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

Новосибирский государственный университет

Международная конференция

МАЛЬЦЕВСКИЕ ЧТЕНИЯ

11–15 ноября 2013 г.

Тезисы докладов

РФФИ Конференция проведена при финансовой поддержке
Российского фонда фундаментальных исследований
(код проекта 13-01-06081-г)

Новосибирск • 2013

Sobolev Institute of Mathematics

Novosibirsk State University

International Conference

MAL'TSEV MEETING

November 11–15, 2013

Collection of Abstracts

РФФИ Supported by
Russian Foundation for Basic Research
(grant 13-01-06081-г)

Novosibirsk • 2013

Содержание

I. Пленарные доклады

Позитивные логики доказуемости

Л. Д. Беклемишев

Рассматривается фрагмент языка модальной логики, состоящий из импликаций $A \to B$, где формулы A и B строятся из пропозициональных переменных и константы «истина» лишь с помощью конъюнкции и модальностей типа $\Diamond$. Такой фрагмент называем строго позитивным.

Более бедный язык позволяет обобщить стандартную интерпретацию связки $\Diamond$ как гёделевской формулы, выражающей непротиворечивость формальной арифметики, на более широкие классы арифметических схем, в частности на так называемые схемы рефлексии. В отличие от стандартного подхода, принятого в логике доказуемости, в позитивной логике переменные могут интерпретироваться как множества арифметических предложений (схемы), а связки — как операции над такими множествами.

Строго позитивные фрагменты стандартных модальных логик, в том числе полимодальных логик доказуемости, как правило значительно проще соответствующих логик в полном языке. В ряде случаев была установлена их разрешимость за полиномиальное время [**3, 2**]. В то же время, строго позитивный язык оказывается достаточно выразительным для некоторых конкретных применений логики доказуемости к исследованию формальных теорий, в частности, к построению систем ординальных обозначений [**1**].

Мы формулируем арифметически полное исчисление с модальностями, занумерованными натуральными числами и символом ω, где ω соответствует полной равномерной схеме рефлексии в арифметике, а $n < \omega$ соответствует ограничению этой схемы арифметическими Π_{n+1}-предложениями. Для этого исчисления устанавливается теорема о полноте относительно подходящего класса конечных шкал Крипке, доказывается полиномиальная разрешимость проблемы выводимости, а также теорема об арифметической полноте, аналогичная известной теореме Р. Соловея для стандартной логики доказуемости [**2**].

Список литературы

[1] Beklemishev L. D. Calibrating provability logic: from modal logic to reflection calculus. In T. Bolander, T. Braüner, S. Ghilardi, and L. Moss, editors, Advances in Modal Logic, v. 9, pages 89–94. College Publications, London, 2012.

[2] Beklemishev L. D. Positive provability logic for uniform reflection principles. Annals of Pure and Applied Logic, published online, August 2013. DOI: 10.1016/j.apal.2013.07.006.

[3] Dashkov E.V. О позитивном фрагменте модальной логики доказуемости GLP. Математические заметки, 91(3):331–346, 2012. English translation: Mathematical Notes 91(3):318–333, 2012.

Математический институт им. В.А. Стеклова РАН, Москва
Московский Государственный Университет им. М.В. Ломоносова, Москва
Национальный исследовательский университет «Высшая школа экономики», Москва
E-mail: bekl@mi.ras.ru

Распознаваемость по спектру знакопеременных групп

И. Б. Горшков

Спектр группы — это множество порядков ее элементов. Две группы называются изоспектральными, если их спектры совпадают. В докладе рассматриваются группы, изоспектральные знакопеременным группам A_n. Основной результат таков. Если G — конечная группа, изоспектральная группе A_n при $n \geq 5$, $n \notin \{6, 10\}$, то G изоморфна A_n.

Новосибирск

Графы простых чисел и группы с факторизацией

Л. С. Казарин

Рассматривается конечная группа G на множестве простых делителей $V = \pi(G)$ порядка которой определен граф $\Gamma = (V, E)$, связанный с ее строением. Например, вершины p и q соединены ребром $(p, q) \in E$, если G содержит элемент порядка pq. Соответствующий граф носит название графа Грюнберга - Кегеля $GK(G)$. Исследованиям свойств таких графов для конечных простых неабелевых групп посвящено целое направление в теории конечных групп как в России, так и за ее пределами.

Другой граф $\Gamma_{Sol}(G)$ на $V = \pi(G)$ определяется свойством $(p, q) \in E(\Gamma_{Sol}(G))$ для $p, q \in V$, если группа G имеет разрешимую подгруппу, порядок которой делится на pq. Графы такого типа введены в обиход японскими математиками С.Абе и Н.Йори, докаавшими связность таких графов для любых конечных неабелевых простых групп.

Наконец, М.-Д. Перес - Рамос определила граф $\Gamma_A(G)$ на множестве $V = \pi(G)$ свойством $(p, q) \in E(\Gamma_A(G))$, если $p \in \pi(N_G(Q)/QC_G(Q))$ для силовской q-подгруппы Q группы G. Все указанные графы неориентированные. Свойства этих графов оказываются весьма полезными для изучения конечных групп, обладающих факторизациями различного типа. В докладе приведены результаты, касающиеся приложений графов простых чисел для изучения конечных групп с факторизацией.

Этот подход наиболее полезен для групп с факторизацией вида $G = AB$. Приведем один результат о группах, обладающих ABA – факторизацией, т.е. о группах G, имеющих такие собственные подгруппы A и B, у которых каждый элемент $g \in G$ записывается в виде $g = aba'$ для подходящих $a, a' \in A$ и $b \in B$.

Теорема. *Спорадические простые группы J_2, McL, HS, Ru и Suz обладают факторизациями вида $G = ABA$ для некоторых собственных своих подгрупп A и B.*

Последний результат получен автором при финансовой поддержке РФФИ (проект 13-01-00469) совместно с И. Рассадиным и Д. Сахаровым.

Ярославский госуниверситет и. П.Г.Демидова, Ярославль
E-mail: kazarin@uniyar.ac.ru

Дистанционно регулярные графы, в которых окрестности вершин — сильно регулярные графы с собственным значением 3

А. А. Махнев

Дж. Кулен предложил задачу описания дистанционно регулярных графов, в которых окрестности вершин — сильно регулярные графы с неглавным собственным значением r. Ранее эта задача была решена в случаях $r = 1, 2$.

А.А. Махневым [1] начато изучение дистанционно регулярных графов, в которых окрестности вершин — сильно регулярные графы с собственным значением 3. В частности, им получена редукция к графам, в которых окрестности вершин — исключительные графы. А.А. Махнев и Д.В. Падучих нашли параметры исключительных сильно регулярных графов с собственным значением 3. Там же было доказано, что граф, в котором окрестности вершин — графы из пунктов (7-10) заключения теоремы не являются вполне регулярными. Позднее они установили, что вполне регулярный граф, в котором окрестности вершин — графы из пунктов (3-6) заключения теоремы является сильно регулярным с параметрами $(490, 297, 168, 198)$, $(616, 287, 126, 140)$, $(640, 243, 66, 73)$, $(961, 320, 99, 110)$ или $(1331, 850, 513, 595)$.

С другой стороны, в работах Белоусова И.Н., Гутновой А.К., Ефимова К.С., Исаковой М.М., Кабанова А.А., Кагазежевой А.М., Махнева А.А., Падучих Д.В., Токбаевой А.А. были классифицированы регулярные графы, в которых окрестности вершин — графы из пункта (1) заключения теоремы. Таким образом, задача сведена к изучению графов, в которых окрестности вершин — сильно регулярные графы с параметрами:

$(35, 18, 9, 9)$, $(36, 21, 12, 12)$, $(40, 27, 18, 18)$, $(50, 28, 15, 16)$, $(56, 45, 36, 36)$, $(64, 27, 10, 12)$, $(81, 30, 9, 12)$, $(85, 54, 33, 36)$, $(96, 75, 58, 60)$, $(96, 35, 10, 14)$, $(99, 84, 71, 72)$, $(100, 33, 8, 12)$, $(119, 54, 21, 27)$, $(120, 63, 30, 36)$, $(120, 51, 18, 24)$, $(121, 36, 7, 12)$, $(126, 45, 12, 18)$, $(133, 108, 87, 90)$, $(136, 105, 80, 84)$, $(147, 66, 25, 33)$, $(148, 77, 36, 44)$, $(148, 63, 22, 30)$;

Работа выполнена при поддержке РФФИ (грант 12-01-00012), программы отделения математических наук РАН (проект 12-Т-1-1003) и программ совместных исследований УрО РАН с СО РАН (проект 12-С-1-1018) и с НАН Беларуси (проект 12-С-1-1009).

Список литературы

[1] Махнев А. А. О сильно регулярных графах с собственным значением 3 и их расширениях. Доклады академии наук. 451:5, 2013, С. 501–504.

Институт Математики и механики УрО РАН, Екатеринбург
E-mail: makhnev@imm.uran.ru

Размерные функции над алгебраическими системами

В. Н. Ремесленников

Для пары объектов (M, A), где M – частично упорядоченное множество, а A – линейно упорядоченная абелева группа, вводится понятие размерной функции $d : M \to A^+$, здесь d отображение из M в A^+, а A^+ – полугруппа неотрицательных элементов в A, с помощью единственной аксиомы:

$$\text{если } m_1 < m_2 \text{ в } M, \text{ то } d(m_1) < d(m_2).$$

В докладе будут продемонстрированы два приложения этого понятия. Первое, для произвольного алгебраического множества над произвольной алгебраической системой будет введено понятие размерности, обобщающее понятие размерности алгебраического множества из классической алгебраической геометрии над полем.

Второе приложение связано с введением оценок сложности на множестве всех регулярных подмножеств фиксированного свободного моноида конечного ранга.

Омский филиал Института математики им. С.Л. Соболева СО РАН, Омск
E-mail: remesl@ofim.oscsbras.ru

О процессах и структурах

А. И. Стукачев

Доклад посвящен результатам, описывающим взаимосвязи между классами обобщенно конструктивных процессов и относительно конструктивных структур. Основными используемыми инструментами являются две сводимости на структурах: Σ-сводимость (как релятивизация понятия "конструктивизируемая структура") и $s\Sigma$-сводимость (как релятивизация понятия "конструктивная структура"). Кроме того, для произвольного допустимого множества вводятся понятия Σ-процесса, относительно Σ-допустимого семейства и компоненты вычислимости. Указанные понятия находятся на стыке теории допустимых множеств и теории аппроксимационных пространств Ершова–Скотта. Рассматриваются такие классы процессов, как Σ-функции, Σ-предикаты и Σ-операторы, и исследуются взаимосвязи между этими классами (в частности, свойства униформизации и вложимости). Рассматриваются также следующие вопросы:

1. Какие вычислимости порождаются структурами?
2. Какие структуры порождаются вычислимостями?

Подробно рассматриваются HF-вычислимости над структурами и их компоненты. Наиболее наглядной иллюстрацией ответов на вопросы второго типа является теорема об обращении скачка для минимальных компонент HF-вычислимостей, которая существенно обобщает известную теорему Фридберга и имеет серию приложений. Найдены также естественные связи максимальной компоненты HF-вычислимости над 0 с действительными числами.

Список литературы

[1] Ершов Ю. Л. Определимость и вычислимость. Новосибирск: Научная книга, 1996.

[2] Ershov Yu. L., Puzarenko V. G., and Stukachev A. I. HF-computability // Computability in Context: Computation and Logic in the Real World / Eds. S. B. Cooper and A. Sorbi. Imperial College Press/World Scientific, 2011. P. 173–248.

[3] Stukachev A. Effective model theory: an approach via Σ-definability // Lecture Notes in Logic. 2013. V. 41. P. 164–197.

[4] Stukachev A. On processes and structures // Lecture Notes in Computer Science. 2013. V. 7921. P. 393–402.

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

Неразрешимая и не-p-разрешимая длина конечных групп

Е. И. Хухро

Результаты данного доклада получены в совместной работе с П. Шумяцким (Бразилия).

Любая конечная группа обладает нормальным рядом, каждый фактор которого либо разрешим, либо является прямым произведением конечных простых групп. Число неразрешимых факторов самого короткого такого ряда называется *неразрешимой длиной* группы. Аналогично вводится понятие *не-p-разрешимой длины*. Ограничения не-p-разрешимой и неразрешимой длины входят в редукционные теоремы Холла–Хигмэна для ослабленной проблемы Бернсайда и Уилсона для проблемы локальной конечности периодических проконечных групп. (Обе проблемы, как известно, были решены Зельмановым.)

Мы доказываем, что не-p-разрешимая длина конечной группы ограничена в терминах максимальной p-длины её p-разрешимых подгрупп. В частности, неразрешимая длина ограничена в терминах максимальной 2-длины разрешимых подгрупп. Эти результаты применяются для изучения вербальных подгрупп конечных и проконечных групп в задачах, обобщающих ослабленную проблему Бернсайда.

Ставится вопрос об ограниченности не-p-разрешимой длины конечных групп, силовские p-подгруппы которых лежат в заданном собственном многообразии. Получено положительное решение этого вопроса для любого многообразия, являющегося произведением нескольких разрешимых многообразий и многообразий конечного периода.

Институт математики им. С. Л. Соболева СО РАН, Новосибирск
E-mail: khukhro@yahoo.co.uk

On Brouwer–Heyting–Kolmogorov provability semantics

Sergei N. Artemov

According to Brouwer, intuitionistic truth is provability; this leads to the informal Brouwer-Heyting-Kolmogorov (BHK) semantics of proofs which has been widely accepted as the intended semantics for intuitionistic logic. Whereas a desired interpretation of BHK-proofs via *proof objects* turned out to be elusive, a variety of BHK-inspired semantics based on *computational programs* (cf., Kleene realizability, Curry-Howard isomorphism, Martin-Löf Type Theory) have been around since the 1940s. They reveal the computational content of constructive reasoning and constitute a major development in logic and computer science. However, such computational semantics does not capture the original provability nature of BHK. In particular, it fails to compensate for some well-known omissions in the original BHK semantics and merely reproduces them formally:

> *In BHK, anything vacuously "proves" the negation of an unprovable sentence; this dubious feature ruins a constructive connection between a sentence and its proof. Original BHK's treating of universal quantifiers admits unacceptable bogus "proofs" for any true* Π_1*-sentence, e.g., for Fermat's Last Theorem or the consistency statement.*

In the 1930s, Gödel suggested to define intuitionistic logic via classical provability (represented by modal logic) and interpret the latter as a system of explicit proofs. Recent developments of the logic of proofs opened the door to realizing Gödel's approach. In this talk, we present a resulting *provability BHK semantics* which satisfies the BHK requirements and, in addition, naturally analyzes and resolves the aforementioned issues with the original BHK.

The provability BHK finds applications far beyond its original foundational scope, e.g., in formal epistemology where it offers a long anticipated theory of justification.

CUNY Graduate Center, New York City (USA)
E-mail: sartemov@gc.cuny.edu

On interpolation in n-transitive modal logics

A. V. Karpenko

Firstly we will observe the problem of interpolation in the extensions of weak transitive modal logics. After that we will try to extend results to n-transitive modal logics. As usual we will study interpolation with the help of criterions wich were found by Larisa Maksimova. These criterions are based on the existence of one-to-one correspondence between classes of extensions of a logic and classes of the corresponding varietes of algebras.

Novosibirsk state university, Novosibirsk (Russia)
E-mail: anastasia.v.karpenko@gmail.com

Operads of decorated trees

P. S. Kolesnikov

These results were obtained in collaboration with V. Yu. Gubarev.

We observe relations between several classes of algebraic systems appeared in areas including algebraic topology, homological algebra, K-theory, combinatorics, and mathematical physics. A general categorical approach to the definition of these classes involves considering free operads of trees with decorated leaves. In this talk, we will focus on a general approach to two types of decoration (called replication and splitting).

In the binary quadratic case, one may observe Koszul duality between replication and splitting algebras, which is very natural since the corresponding operads may be obtained as Manin products with Koszul-dual operads Perm and pre-Lie, respectively. We observe a general method how to deduce the identities defining replication and splitting algebras for an arbitrary operad, not necessarily binary or quadratic.

Further, we consider a relation between algebras in these decorated classes and ordinary algebras with additional operators. The idea of Koszul duality works here and provides a way to embed a replication algebra into an ordinary algebra with an averaging operator, i.e., a linear map T such that

$$T(x)T(y) = T(xT(y)) = T(T(x)y).$$

Similarly, a splitting algebra may be embedded into an ordinary algebra with a Rota–Baxter operator, i.e., a linear map R such that

$$R(x)R(y) = R(xR(y)) + R(R(x)y).$$

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

Naturalness in formal mathematics

Peter Koepke

In this talk I shall first survey the field of *formal mathematics*, emphasizing that:

- every mathematical statement can be translated into a formula in a strictly formal symbolic language, using e.g. standard first-order set-theoretic foundations of mathematics;
- every mathematical proof can be turned into a drivation in a strictly formal symbolic calculus, due to Gödel's completeness theorem;
- formalization is a highly complex process that requires computer assistance;
- there are several powerful formal mathematics systems which allow proofs of significant theorems and the development of extensive mathematical theories;
- formalizations resemble computer languages;
- computer generated derivations are based on resolution proofs found by extensive search.

The last two items demonstrate that up to now there is a huge difference between statements and proofs in the mathematical literature and their formal counterparts. The Naproche (Natural Proof Checking; `www.naproche.net`) at Bonn aims at understanding and bridging that gap by analysing the natural language of mathematics and natural mathematical arguments. Naproche combines:

- techniques from Natural Language Processing (NLP) to parse and represent ordinary mathematical language;
- automatic reasoning tools and Automatic Theorem Provers (ATP) for filling gaps in natural proofs.

We shall give examples of proofs of non-trivial theorems which are formulated in ordinary mathematical language and which are at the same time strict derivations in a computer-implemented formal proof system. We shall present details involved in the formalizations and discuss future technical work.

Finally we shall discuss some general issues brought up by the project:

- how faithful are formalizations of mathematical notions, statements and arguments?
- what is the ontology of mathematical statements? is there a mathematical universe?
- which implicit background theories should be employed, and how should they be implemented in formal systems?
- what is an ordinary mathematical proof?

We propose to view ordinary proofs as coercive arguments for the existence of formal derivations of claims, but without actually carrying them out. If the language of mathematics is restricted to a controlled natural sublanguage computer systems may be able to actually produce such derivations, using cues from the ordinary proof. This will make formal mathematics more accessible and practicable, and it will show that (parts of) mathematics can be developed naturally, yet in complete formality.

Mathematical Institute, University of Bonn, Bonn (Germany)

Hall subgroups and the pronormality

D. O. Revin

A subgroup H of a group G is said to be *pronormal* if H and H^g are conjugate in $\langle H, H^g \rangle$ for every $g \in G$.

Let π be a set of primes. A subgroup H of a finite group G is called *a Hall π-subgroup* if every prime divisor of $|H|$ belongs to π while $|G : H|$ is divisible by no prime in π.

The well-known Hall's Theorem implies that, in the finite solvable groups, Hall π-subgroups exist and all of them are pronormal for every set π of primes.

In non-solvable finite groups, the existence of Hall π-subgroups is not guaranteed.

Let a set π of primes is given. In the talk, we will discuss the following questions:

- Under what conditions is every Hall π-subgroup of a finite group G pronormal?
- Do there exist examples of non-pronormal Hall π-subgroups?
- Is it true that if a finite group G possesses a Hall π-subgroup then G possesses a pronormal Hall π-subgroup?
- What can one say about the class of finite groups G such that G includes a Hall π-subgroup and every Hall π-subgroup of G is pronormal.

The results of the talk are obtained by the author in collaboration with E. Vdovin and W. Guo.

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

Quantifying over Bernoulli random variables in probability logic

Stanislav O. Speranski

Assume $\mathscr{X} = \{x_i\}_{i=1}^{\infty}$ is the set of *variables*, and C is a decidable set of *constants*. Define the collection of *e-terms* to be the smallest set containing $\mathscr{X} \cup C$ such that if t_1 and t_2 are e-terms, then $\overline{t_1}$ and $t_1 \cap t_2$ are e-terms as well. Next, by a $\mathscr{L}_{\mu}^{C}$*-atom* we mean an expression of the sort

$$f\,(\mu\,(t_1), \ldots, \mu\,(t_n)) \;\leqslant\; g\,(\mu\,(t_{n+1}), \ldots, \mu\,(t_{n+m}))\,,$$

where f and g are polynomials with coefficients in $\mathbb{Q}$, and $t_1, \ldots, t_{n+m}$ are e-terms. Finally, $\mathscr{L}_{\mu}^{C}$*-formulas* are obtained from $\mathscr{L}_{\mu}$-atoms by closing under $\neg$, $\wedge$ and applications of $\forall x$, with $x \in \mathscr{X}$; we abbreviate $\neg \forall x \, \neg \Phi$ as $\exists x \, \Phi$.

Suppose that $\mathfrak{A} = \langle \Omega, \mathscr{A}, \mathsf{P} \rangle$ is a discrete probability space. For a quantifier-free $\mathscr{L}_{\mu}$-formula Φ and a valuation $v : \mathscr{X} \cup C \to \mathscr{A}$, we define $\mathfrak{A} \Vdash \Phi\,[v]$ recursively (in a first-order fashion) by interpreting $\overline{t_1}$ as the complement of t_1, $t_1 \cap t_2$ as the intersection of t_1 and t_2, and μ as P — this leads to a minor extension of decidable quantifier-free probability logic from [**1**] (with $C := \{c_i\}_{i=1}^{\infty}$ and no variables).

The above semantics can be further expanded to arbitrary $\mathscr{L}_{\mu}^{C}$-formulas if quantifiers are viewed as ranging over: i) all events of $\mathscr{A}$; ii) all events of $\mathscr{A}$ expressible by ground e-terms (which essentially corresponds to considering $\mathfrak{A}$ being a finitely additive probability space with $\mathscr{A}$ countable). In the latter case the validity problem for $\mathscr{L}_{\mu}^{C}$, where C is infinite, is known to be Π_1^1-complete [**2**] (and easily shown to be decidable whenever C is finite), while in the former it turns out to be m-equivalent to the second-order theory of $\langle \mathbb{N}, +, \times \rangle$ (even with no constants). Also, a number of results on prefix fragments are established here.

Note that every $E \in \mathscr{A}$ is uniqely determined by its characteristic function, i. e., by a Bernoulli random variable on $\mathfrak{A}$, and vice versa. In this way, our probabilistic languages expand the basic quantifier-free logic of [**1**] by adding quantification over Bernoulli random variables (either all, or only those definable via ground e-terms). The present talk is devoted to various aspects of these quantified probabilistic languages, focusing on issues of expressibility and computability.

References

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

[2] Speranski S. O. Complexity for probability logic with quantifiers over propositions, Journal of Logic and Computation 23:5 (2013), 1035–1055.

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

Primitive and measure-preserving system of elements on the varieties of soluble groups

E. I. Timoshenko

Let $\{v_1, \dots, v_m\}$ be a system of elements in a free group F_n of rank n, $m \leq n$. The system of elements $\{v_1, \dots, v_m\}$ is called *primitive system* in a free group $F_n(\mathfrak{M})$ of a variety $\mathfrak{M}$ if its image by the natural homomorphism $F_n \to F_n(\mathfrak{M})$ can be complemented to a basis of $F_n(\mathfrak{M})$. Let G be a finite group in the variety $\mathfrak{M}$. Define the verbal mapping $\varphi_{\{v_1,\dots,v_m\}}$ from G^n into G^m by assigning to each $\overline{g} = (g_1, \dots, g_n) \in G^n$ the element $(v_1(g_1, \dots, g_n), \dots, v_l(g_1, \dots, g_n))$ in G^m. A system of elements $\{v_1, \dots, v_m\}$ *preserves measure on* G if every $\overline{g} \in G^m$ appears as an image under $\varphi_{\{v_1,\dots,v_m\}}$ with probability $|G|^{-m}$. A system of elements $\{v_1, \dots, v_m\}$, $1 \leq m \leq n$, that preserves measure on every finite group $G \in \mathfrak{M}$ is called *measure-preserving* on the variety $\mathfrak{M}$. Let a variety $\mathfrak{M}$ be the product $\mathfrak{M} = \mathfrak{A}\mathfrak{B}$ of the variety $\mathfrak{A}$ of all Abelian groups and some variety $\mathfrak{B}$. We can calculate the Fox derivatives $\partial_i v \in \mathbb{Z}(F_n(\mathfrak{B}))$ for each $v \in F_n(\mathfrak{A}\mathfrak{B}))$. Denote by $J(v)$ the matrix $(\partial_i(v_j))_{m\times n}$ over the rink $\mathbb{Z}(F_n(\mathfrak{B}))$.

Theorem 1. *The following conditions are equivalent:*

1. the system of elements $\{v_1, \dots, v_m\}$ is primitive in the free metabelian group $F_n(\mathfrak{A}^2)$; 2. the system of elements $\{v_1, \dots, v_m\}$ is measure-preserving on the variety $\mathfrak{A}^2$ of all metabelian groups; 3. there is a matrix $B_{n\times m}$ over the ring $\mathbb{Z}(F_n(\mathfrak{A}))$ such that $J(v)B$ is the identity matrix $E_{m\times m}$.

Let R be a ring with unity. The vector $(u_1, \dots, u_n)$, $u_i \in R$, be known as *unimodular* if $u_1 r_1 + \ldots + u_n r_n = 1$ for some $r_i \in R$.

Corollary. *The following conditions are equivalent:*

1. an element $v \in F_n(\mathfrak{A}^2)$ is primitive; 2. v is measure-preserving element on $\mathfrak{A}^2$; 3. $(\partial_1 v, \dots, \partial_n v) \in \mathbb{Z}(F_n(\mathfrak{A}))^n$ is an unimodular vector.

Let $\mathfrak{N}_c$ be a variety of all nilpotent groups of class $\leq$ c. On the other hand, the Corollary is not true for the variety $\mathfrak{A}\mathfrak{N}_2$.

Theorem 2. *There is an element v such that 1. v is not primitive element of the group $F_2(\mathfrak{A}\mathfrak{N}_2)$; 2. v is measure-preserving element on the variety $\mathfrak{A}\mathfrak{N}_2$.*

Theorem 3. *A system of elements $\{v_1, \dots, v_m\}$ is measure-preserving on the variety $\mathfrak{N}_c\mathfrak{A}$ iff it is measure-preserving system on the variety of all metabelian groups $\mathfrak{A}^2$.*

Theorem 4. *A system of elements $\{v_1, \dots, v_m\}$ is measure-preserving on the variety $\mathfrak{N}_c\mathfrak{A}$ iff it is primitive system in the group $F_n(\mathfrak{N}_c\mathfrak{A})$.*

Theorem 5. *A system of elements $\{v_1, \dots, v_m\}$ is measure-preserving on the variety of all profinite metabelian groups iff it is primitive system in the free metabelian profinite group $\widehat{F}_n(\mathfrak{A}^2)$.*

Theorem 6. *A system of elements $\{v_1, \dots, v_m\}$ is primitive in the group $F_n(\mathfrak{A}^2)$ iff it is primitive in the free metabelian profinite group $\widehat{F}_n(\mathfrak{A}^2)$.*

Novosibirsk, NGTU
E-mail: eitim45@gmail.com

Atomic rule refinement in the tableau synthesis framework

D. E. Tishkovsky, R. A. Schmidt

Tableau algorithms play a very important role in the mainstream of current research on automated reasoning, proof theory, semantic web and ontology reasoning. They provide a uniform and flexible way of defining decision procedures for logical formalisms which underlie beneath various applications.

We are interested in generic principles for developing tableau decision procedures. In [**1**], we developed a framework which formalises a process for automatically transforming the definition of the semantics of a logic into a tableau calculus which is sound and complete for the logic.

Initially, some rules of the generated calculus can have branches which are not necessary for guaranteeing completeness. This decreases the performance of tableau algorithms based on the calculus. The tableau synthesis framework, addressing the problem, defines a refinement procedure of the generated tableau calculus. In order to preserve completeness of the calculus, the rule refinement requires the verification of a general rule refinement condition which is inductive and needs to be checked manually. For the purposes of automating rule refinement it is therefore important to find other less generic conditions which are sufficient to preserve completeness and, yet, can be automatically verified.

In this talk, we discuss a special atomic rule refinement condition [**2**] and prove that it implies the general rule refinement condition. Consequently, this guarantees that the atomic rule refinement preserves completeness of the tableau calculus.

In brief, given a tableau rule, the atomic rule refinement allows to move negated atomic formulae from the conclusions of the rule to the rule premises by inverting their sign. We identify three important cases when the atomic rule refinement condition is satisfied automatically. The first case automates refinement of the generated rule for the box (necessity) operator in standard modal logics to the usual box propagation rule. The second case allows to refine rules which are generated from frame conditions for arbitrary combinations of modal-like logics. In the third case, using the atomic rule refinement, we show how to transform the generated tableau calculus into a hypertableau-like calculus and prove that the transformation preserves completeness of the calculus.

References

[1] Schmidt R. A., Tishkovsky D. Automated synthesis of tableau calculi. Log. Methods Comput. Sci., 7(2:6):1–32, 2011.

[2] Tishkovsky D., Schmidt R. A. Refinement in the tableau synthesis framework. CoRR, abs/1305.3131, 2013.

University of Manchester, Manchester (UK)
E-mail: dmitry@cs.man.ac.uk

Mereotopology III: Whiteheadean type of point-free theories of space and time

Dimiter Vakarelov

Alfred North Whitehead is well-known as a co-author with Bertrand Russell of the famous book "Principia Mathematica". The authors intended to write a special part of the book related to the foundation of geometry, but due to some disagreements between them this part has not been written. Later on Whitehead formulated his own program for a new, relational theory of space and time, which appeared in print for the first time in his book *The Organization of Thought*, London, William and Norgate, 1917, page 195. This theory should be *point-free* in a double sense, that neither the notion of space point, nor the notion of time moment should be taken as primitives. Instead they have to be defined by a more realistic primitive notions related to the existing things in reality. In his later book, *Process and Reality*, New York, MacMillan, 1929, Whitehead presented a detailed program of how to build a point-free mathematical theory of space, based on the primitive notions *region*, formalizing the notion of physical body, and some relations between regions like mereological relations *part-of*, *overlap* and the mereotopological relation *contact*. He developed also a very interesting philosophical theory of time, called by him *epochal theory of time*, but unfortunately he did not present any program for its mathematical formalization. Whitehead's epochal theory of time was presented rather informally in an unusual philosophical terminology, which makes extremely difficult its mathematical formalization.

The present paper is a third one in a series of papers [**1, 2**] devoted to an Whiteheadean type of point-free theories of space and time. We will present first a natural model of spatial regions changing in time (*dynamic regions*) with operations between them forming a Boolean algebra and various natural relations between dynamic regions of space like *space contact*, *time contact*, *precedence relation* and some others. The resulting point-free formalizations are abstract Boolean algebras with some additional relations between their elements. The main results for such abstract systems is a kind of Stone-like representation theorems, showing in certain sense the equivalence between the point-free and point based formalizations.

References

[1] Vakarelov D. Dynamic Mereotopology: A point-free Theory of Changing Regions. I. Stable and unstable mereotopological relations. Fundamenta Informaticae, vol 100, (1-4) (2010), 159-180.

[2] Vakarelov D. Dynamic Mereotopology II: Axiomatizing some Whiteheadean Type Space-time logics. In: Th. Bolandwer, T. Braüner, S. Ghilardi and L. Moss Eds., Advances in Modal Logic, vol. 9, 538-558, 2012.

Sofia University, Sofia, Bulgaria
E-mail: dvak@fmi.uni-sofia.bg

A variant of bi-intuitionistic logic

Heinrich Wansing

A variant of bi-intuitionistic propositional logic, called 2Int, is introduced and shown to be faithfully embeddable into intuitionistic propositional logic with respect to validity and into dual intuitionistic logic with respect to a notion of dual validity. The difference between bi-intuitionistic logic, 2Int, and Nelsons's constructive logic with strong negation N4 extended by a falsity constant is explained. Moreover, the system 2Int is shown to be sound and complete with respect to a natural deduction calculus that comprises proof rules and dual proof rules.

Ruhr-University Bochum (Germany)
E-mail: Heinrich.Wansing@rub.de

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

Дескриптивная сложность конечных множеств регулярных языков

С. А. Афонин

В качестве меры сложности $C(L)$ регулярного языка L можно выбрать (минимально возможное) число состояний состояний соответствующего детерминированного или недетерминированного автомата, длину регулярного выражения и другие аналогичные характеристики. В данном докладе рассматривается вопрос определения сложности конечного множества регулярных языков.

Пусть задано мультимножество $\mathbf{S} = \{L_1, \ldots, L_n\}$ регулярных языков в алфавите Σ. Каждый элемент может иметь относительно большое значение $C(L)$, однако между различными элементами может существовать зависимость, например $L_i = L_{i-1}L_{i-1}$, и сложность описания всего набора не является суммой по его элементам.

Рассмотрим отображение из некоторого алфавита Δ в множество регулярных языков, $\varphi : \Delta \to \mathrm{Reg}(\Sigma)$, которое может быть расширено до гомоморфизма $\varphi : \Delta^+ \to \mathrm{Reg}(\Sigma)$. Пусть образом пустого слова $\varphi(\varepsilon)$ является язык $\{\varepsilon\}$. Для любого языка $R \subseteq \Delta^*$ положим $\varphi(\Delta) = \cup_{w \in R} \varphi(w)$.

Сложность регулярной подстановки φ определим как $C(\varphi) = \sum\limits_{\delta \in \Delta} C(\varphi(\delta))$. Для заданной подстановки φ разрешима задачи проверки принадлежности языка $L \in \mathrm{Reg}(\Sigma)$ множеству $\mathbf{L}(\varphi) = \{\varphi(R) \mid R \in \mathrm{Reg}(\Delta)\} \subseteq \mathrm{Reg}(\Sigma)$.

Сложность описания конечного множества регулярных языка определим как

$$C(\mathbf{S}) = \min_{\varphi, R_1, \ldots, R_n} \left(C(\varphi) + \sum_{i=1}^{n} C(R_i) \right),$$

где минимум берется по всем подстановкам φ для которых $\mathbf{S} \subseteq \mathbf{L}(\varphi)$.

Очевидно, что вследствие разрешимости проверки принадлежности $L \in \mathbf{L}(\varphi)$ функция $C(\mathbf{S})$ вычислима. Достаточно перебрать все наборы подстановок, сложность которых не превосходит суммарной сложности элементов $\mathbf{S}$. В докладе рассматривается возможность построения более эффективного алгоритма вычисления $C(\mathbf{S})$.

МГУ имени М.В. Ломоносова, Москва
E-mail: serg@msu.ru

Пример протокола интерактивного доказательства

М. И. Бекенов, Р. М. Оспанов

Рассматривается пример протокола интерактивного доказательства.

Пусть A - квадратная матрица большого порядка, d - вещественное число. P утверждает, что $detA = d$ (т.е. обладает достаточными вычислительными ресурсами, чтобы вычислить $detA$), V не может самостоятельно вычислить $detA$ (не обладает достаточными ресурсами). P хочет убедить V в истинности этого утверждения, не раскрывая вычислений (по разным причинам), а V хочет быть уверенным, что число d действительно является значением $detA$.

1-ый вариант. Общий вход: A - квадратная матрица большого порядка, вещественное число d.

1) Первый шаг проверяющего: V преобразовывает A так, чтобы $detA$ не изменился, применяя соответствующие свойства определителей достаточное количество раз (предполагается, что на такие преобразования у него достаточно ресурсов). Получает матрицу A_1 такую, что $detA_1 = detA$. Затем преобразовывает A так, чтобы $detA$ изменился, т.е. получает A_2 такую, что $detA_2 \neq detA$. V отправляет A_1 и A_2 доказывающему и просит его вычислить их определители.

2) Первый шаг доказывающего: P вычисляет определители полученных матриц и отправляет их значения проверяющему.

3) Второй шаг проверяющего: V проверяет, если $detA_1 \neq d$ или $detA_2 = d$, то останавливает проверку и отвергает доказательство.

P и V повторяют шаги 1) и 3) m раз. Проверяющий принимает доказательство, если он завершит m итераций шагов 1) - 3). В противном случае, отвергает.

2-ой вариант (в котором участники выполняют меньше вычислений). Общий вход: A - квадратная матрица большого порядка, вещественное число d.

1) Первый шаг проверяющего: V наугад выбирает бит $\alpha \in \{0, 1\}$. Если $\alpha = 1$, то V преобразовывает A так, чтобы $detA$ не изменился, применяя соответствующие свойства определителей достаточное количество раз (предполагается, что на такие преобразования у него достаточно ресурсов). Получает матрицу A_1 такую, что $detA_1 = detA$. Если $\alpha = 0$, то V преобразовывает A так, чтобы $detA$ изменился, т.е. получает A_0 такую, что $detA_0 \neq detA$. V отправляет A_α доказывающему и просит его вычислить определитель матрицы A_α.

2) Первый шаг доказывающего: P вычисляет определитель полученной матрицы и отправляет его значение проверяющему.

3) Второй шаг проверяющего: V проверяет, если $detA_1 \neq d$ или $detA_2 = d$, то останавливает проверку и отвергает доказательство.

P и V повторяют шаги 1) и 3) m раз. Проверяющий принимает доказательство, если он завершит m итераций шагов 1) - 3). В противном случае, отвергает.

Евразийский Национальный Университет им. Л.Н.Гумилева, Астана
E-mail: bekenov50@mail.ru, hamza13@mail.ru

Об оптимальных композициях алгоритмов кластеризации, основанных на логических правилах

В. Б. Бериков

Рассматривается следующая задача кластерного анализа: требуется разбить множество объектов, информация о которых имеет форму таблицы "объект-признак", на некоторое число групп в соответствии с заданным критерием однородности. Предполагается, что признаки, описывающие объекты наблюдения, могут быть разнотипными: вещественными, порядковыми, булевыми или измеренными в шкале наименований. Число признаков может быть достаточно большим: сравнимо с числом объектов или намного больше. Задачи такого рода возникают, например, в биоинформатике или при анализе медицинских данных. Для решения подобного рода задач в существуют методы, основанные на коллективе логических правил (таксономических решающих деревьях). Коллективный (ансамблевый) подход позволяет снижать зависимость результатов группировки от выбора параметров алгоритма, получать более устойчивые решения в условиях зашумленных данных, при наличии в них пропусков. 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 признака X_j для объекта a.

В докладе предлагается метод построения композиции коллективных решений с учетом весов алгоритмов, основанный на нахождении матрицы попарных классификаций объектов. Нахождение оптимальных весов основано на минимизации верхней оценки вероятности ошибки классификации, найденной в рамках модели ансамблевого кластерного анализа с латентными классами [**1, 2**]. Указанная (непосредственно ненаблюдаемая) ошибка оценивается по наблюдаемым характеристикам ансамбля.

Работа поддержана грантом РФФИ, проект № 11-07-00346а.

Список литературы

[1] Бериков В. Б. Построение ансамбля деревьев решений в кластерном анализе // Вычислительные технологии. 2010. Т. 15. № 1. С. 40-52.

[2] Berikov V. A latent variable pairwise classification model of a clustering ensemble // Lecture Notes on Computer Science, LNCS 6713. 2011. P. 279-288.

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

Достаточное условие предписанной 3-раскрашиваемости 4-регулярных графов

А. Ю. Бернштейн

Предположим, что для каждой вершины u графа $G(V,E)$ задан список $L(u)$ допустимых цветов. Раскраска c вершин графа G называется *L-раскраской*, если $c(u) \in L(u)$ для каждой вершины $u \in V$. Граф G называется *предписанно k-раскрашиваемым*, если он обладает L-раскраской для каждого набора предписаний L такого, что $|L(u)| \geq k$ для всех $u \in V$. Наименьшее k, для которого G предписанно k-раскрашиваем, называется *предписанным числом* графа G и обозначается $\chi_\ell(G)$.

Легко видеть, что предписанное число не может быть меньше хроматического: $\chi_\ell(G) \geq \chi(G)$. Изучение свойств графов, для которых достигается равенство $\chi_\ell(G) = \chi(G)$, представляет значительный интерес [**2**]. В докладе это равенство рассматривается для случая, когда граф G 4-регулярен.

Мощным методом оценки предписанных чисел графов служит так называемый *полиномиальный метод*, предложенный Алоном и Тарси [**1**]. Он позволяет сводить некоторые задачи существования к проверке равенства нулю определённого коэффициента специально сконструированного многочлена. Для 4-регулярных графов с его помощью можно установить связь между предписанной 3-раскрашиваемостью графа и структурой множества его эйлеровых ориентаций.

Автором было показано, что полученный с помощью полиномиального метода критерий предписанной 3-раскрашиваемости 4-регулярного графа можно сформулировать в терминах его обычных правильных раскрасок в 3 цвета. Именно, пусть $G(V,E)$ — 4-регулярный граф. Его правильную раскраску в цвета $\{1,2,3\}$ будем отождествлять с упорядоченной тройкой (X,Y,Z) множеств вершин первого, второго и третьего цвета соответственно. Множество всех правильных 3-раскрасок графа G специальным образом разбивается на два класса $A(G)$ и $B(G)$, после чего доказывается следующее утверждение.

Теорема. *Пусть G — 4-регулярный мультиграф без петель, причём $\chi_\ell(G) > 3$. Тогда*

$$\sum_{(X,Y,Z)\in A(G)} \left(-\frac{1}{8}\right)^{|X|} = \sum_{(X,Y,Z)\in B(G)} \left(-\frac{1}{8}\right)^{|X|}.$$

Доказательство этого результата использует линейную алгебру над полем $\mathbb{Z}_2$.

Список литературы

[1] Alon N., Tarsi M. Colorings and orientations of graphs. Combinatorica, Volume 12, no. 2, 1992. Pages 125–134.

[2] Bollobás B., Harris A.J. List-colourings of graphs. Graphs and Combinatorics, Volume 1, Issue 1, 1985. Pages 115–127.

Новосибирский Государственный Университет, Новосибирск
E-mail: bahtoh@gmail.com

Применение полей Q и F(X) в параллельных вычислениях и для верификации программ

В. А. Васенин, В. А. Роганов

Вычисления с плавающей точкой традиционно доминируют при решении прикладных задач. Однако, при переходе ко все более точным и масштабным расчетам, зачастую проявляются недостатки, связанные с ошибками округления и переполнения. При разработке численных методов приходится следить за накоплением ошибок ([**1**], [**2**]); из-за нарушения аксиом поля сужается круг допустимых алгебраических преобразований и вычислительных схем.

Применение "масштабируемых" полей типа рациональных чисел и функций в качестве базовой арифметики делает возможным создание высокопараллельных программ по следующей схеме:

1. Выделяется объект с набором характеристик X, которые достаточно найти;
2. Проводится разносторонний анализ алгебраических свойств данного объекта;
3. Подбираются легко вычислимые характеристики Y, связанные с X;
4. Параллельно вычисляется набор характеристик Y объекта;
5. Восстанавливаются искомые характеристики X по известной связи с Y.

В случае использования обычной арифметики с плавающей точкой количество информации, содержащейся в каждом числовом значении, ограничено сверху, что в случае масштабных задач приводит к потере существенной доли сведений об объекте.

Арифметика с масштабируемой точностью ([**3**]), которая требуется при данном подходе, утяжеляет расчет, но на современных массивно-параллельных архитектурах это можно компенсировать, задействовав достаточно большое количество счетных ядер.

К практически значимым задачам, которые можно решать с применением данного подхода, можно отнести задачу решения систем линейных уравнений с разреженными матрицами некоторых видов ([**4**]), задачу вычисления части спектра и собственных функций в задачах математической физики, верификацию участков программ для решения систем нелинейных уравнений.

Теорема. *Систему линейных алгебраических уравнений с несимметричной разреженной матрицей, соответствующей расчетной сетке N x N x N, можно решить прямым методом за время $O(N^4)$ используя N^2 процессоров и операции с масштабируемой точностью. Повторные решения СЛАУ с той же матрицей, но с произвольными правыми частями можно получать за время $O(N^3)$ при тех же условиях.*

Теорема. *Корректность алгоритма линейного участка программы, явно решающего систему нелинейных алгебраических уравнений, можно доказать, выполнив конечное число контрольных вычислений с повышенной точностью, зависящей от конкретного вида системы.*

Возможность обобщения последней теоремы для других классов программ представляется весьма интересным вопросом, связанным с разрешимостью теорий для более сложных алгебраических структур ([**5**]).

Список литературы

[1] Годунов С.К. Компьютерные вычисления и проблемы оценки погрешностей в пакетах прикладных программ // Доклад на IV форуме СИИС-2013, Новосибирск, 2013.

[2] Годунов С.К., Антонов А.Г., Кирилюк О.П., Костин В.И. Гарантированная точность решения систем линейных уравнений в евклидовых пространствах // Новосибирск, Наука, 2-е. изд., перераб. и доп., 1992.

[3] Дональд Кнут. Искусство программирования, том 2, Получисленные алгоритмы, гл. Арифметика многократной точности.

[4] Vasenin V.A., Krivchikov M.A., Kroshilin A.E., Kroshilin V.E., Roganov V.A. Scalable Three-Dimensional Thermal-Hydraulic Best-Estimate Code BAGIRA // Proceedings of International Congress on Advances in Nuclear Power Plants, 2012, Chicago, USA.

[5] Ершов Ю.Л. Проблемы разрешимости и конструктивные модели // Москва, изд. "Наука", 1980.

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

Σ – спецификация иерархизированных мультиагентных систем

В. Н. Глушкова

В парадигме агентного моделирования система представляется в виде отдельно специфицируемых активных подсистем (агентов). Все такие модели децентрализованы и агенты имеют индивидуальные правила поведения. Глобальное поведение всей системы является результатом деятельности многих агентов, каждый из которых по своим собственным правилам взаимодействует с другими агентами и окружающей их средой. Эти принципы естественно поддерживаются при использовании в качестве языка спецификации поведения агентов многосортного языка исчисления предикатов первого порядка с ограниченными кванторами, выделенного в концепции Σ – программирования [1].

Особенность предлагаемого подхода состоит в том, что ограниченные кванторы действуют на иерархических списках, представляющих деревья вывода в КС-грамматике, правила которой иерархизируют пространство состояний и действий агентов. В модели определяется несколько независимых иерархий с разными КС-грамматиками, отражающими поведение разных агентов. В спецификации простого промышленного агрегата [2] используется 4 грамматики: для роботов D и G; для обрабатывающего устройства; для описания перемещений ящика.

Логическая спецификация состоит из $\Delta_0 T$–формул вида:

$$(\forall x_1 \dot{\in} t_1) \ldots (\forall x_m \dot{\in} t_m)(y_1 \prec z_1) \ldots (y_p \prec z_p)\varphi(\bar{x}, \bar{t}) \to \psi(\bar{x}, \bar{t})$$

$m \geq 1$, $p \geq 0$, $y_j, z_j \in < \bar{x}, \bar{t} >$, $1 \leq j \leq p$; $\dot{\in}$ обозначает отношение принадлежности элемента КС-списку или его транзитивное замыкание, $\prec$ – отношение ”левее”. Теория модели состоит из нескольких ”подтеорий” для разных агентов. Теории взаимодействующих агентов содержат общие предикаты. Интерпретатор аксиом теории реализует прямой логический вывод. Вычисления для разных теорий могут осуществляться асинхронно с задержкой обработки тех аксиом с общими предикатами, значения которых еще не известны. Аксиомы теорий, предикаты и функции согласованы с символами и правилами соответствующих грамматик. Это позволяет при интерпретации построить деревья, отражающие иерархию действий агентов с конкретными значениями констант, вычисленными в процессе интерпретации. Для верификации модели используются произвольные $\Delta_0 T$–формулы, которые проверяются на построенных деревьях за полиномиальное время.

Список литературы

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

[2] Daws C., Yovine S. Two examples of verification of multirate timed automata with Kronos. in Proc. IEEE RTSS, 1995, p. 66–75.

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

Отношения по направлению и истинностная семантика

Б. Н. Дроботун

1. Пусть M - произвольное непустое множество, $1 \leq i_1 < i_2 < i_3 ... < i_3$, $i_j \in N$ и $M_{i_j} = M$, $j = 1; 2; ...n$. Декартово произведение $E = \mathbf{X}_{k=1}^{n} M_{j_k}$ будем называть n-мерным декартовым M-пространством направления $(i_1; i_2; ...; i_n)$, а декартовы сомножители M_{i_j} - его i_j-ми координатными осями. Подмножества множества E назовем n-местными отношениями направления $(i_1; i_2; ...; i_n)$, заданными на множестве M. Пусть $A_{(i_1;i_2;...;i_n)}(M)$ - совокупность всех таких отношений. Положим $\mathbf{A}(M) = \cup_{n \in N}(\cup_{(i_1;i_2;...i_n)} A_{(i_1;i_2;...i_n)}(M))$.

2. В работе на множестве $\mathbf{A}(M)$ вводятся унарные операции ${}^{(t)}A$ и $A_{(t)}$-проектирования и цилиндрификации вдоль t-ой координаты, как аналоги соответствующих операций, определяемых в теории рекурсивных функций [1]. С использований этих операций вводится понятие t-цилиндра, даются описания t-цилиндров с экстремальными свойствами и содержательная характеризация формульных предикатов в истинностной семантике.

3. Отношение $A \in A(M)$ назовем t-цилиндром, если $A = ({}^{(t)}A)^{(t)}$.

Предложение 1.*Пусть $A \in A_{(i_1;i_2;...;i_n)}(M)$. Тогда для любого $t \in \{i_1; i_2; ...; i_n\}$:*

а) отношение ${}^{(t)}A \ X_t M_t$ есть наименьший t-цилиндр, содержащий отношение A;

б) отношение $\overline{({}^{(t)}(\overline{A}))^{(t)}}$ есть наибольший t-цилиндр, содержащийся в отношении A.

4. Через $\mathbf{P}^{(n)}(M)$ обозначим множество всех n-местных предикатов, определенных на множестве M. Положим $\mathbf{P}(M) = \cup_{n=1}^{\infty} \mathbf{P}^{(n)}(M)$. Через S^* будет обозначаться далее область истинности предиката $S \in \mathbf{P}(M)$. Дадим описание областей истинности $(P_{\exists_{i_k}})^*$ и $(P_{\forall_{i_k}})^*$ предикатов $(\exists x_{i_k})P(x_{i_k})$ и $(\forall x_{i_k})P(x_{i_k})$, исходя из области истинности P^* предиката P.

Предложение 2.. *Пусть $P = P(x_{i_1}; x_{i_2}; ...; x_{i_n}) \in \mathbf{P}(M)$ и $1 \leq k \leq n$. Тогда:*

а) область истинности предиката $P_{\exists_{i_k}}$ совпадает с i_k-проекцией области истинности P^* предиката P;

б) область истинности $(P_{\forall_{i_k}})^*$ предиката $P_{\forall_{i_k}}$ есть i_k-проекция наибольшего i_k-цилиндра, содержащегося в области истинности P^* предиката P

Список литературы

[1] Роджерс Х. Теория рекурсивных функций и эффективная вычислимость.- М.: Мир, 1972.

Павлодарский государственный университет, Павлодар
E-mail: drobotun.nina@mail.ru

Обращение перестановочных дифференцируемых функций над модулями

А. В. Карпов

Пусть R — кольцо с единицей, C — центр R и G — правый R-модуль. Функция $f : G \to G$ называется *дифференцируемой*, если для любого $x \in G$ существует такое значение $f'(x) \in R$, что для любого идеала $J \trianglelefteq C$ и всех $a \in GJ$ выполняется $f(x+a) = f(x) + af'(x) \pmod{GJ^2}$. Функцию называют *перестановочной*, если она индуцирует перестановку элементов G.

Частным случаем перестановочных дифференцируемых функций являются, например, перестановочные полиномиальные функции над кольцами, представляющие интерес в связи с их применениями в криптографии и теории кодирования. В докладе делается обобщение результатов, полученных в [**1**] на случай дифференцируемых функций над модулями, а именно рассматривается задача нахождения *обратной* к $f : G \to G$ функции $g : G \to G$, т.е. такой, что для произвольного $x \in G$ выполняется $g(f(x)) = x$.

Теорема 1. *Пусть функции $f : G \to G$, $g_k : G \to G$ являются дифференцируемыми и взаимно обратными над G/GJ^k, тогда функции $g_{k+\lfloor k/2 \rfloor}$ и f — взаимно обратны над $G/GJ^{k+\lfloor k/2 \rfloor}$, где*

$$g_{k+\lfloor k/2 \rfloor}(x) = 2g_k(x) - g_k(f(g_k(x))).$$

Доказывается следующая теорема, позволяющая изменять вид функции, обратную к которой необходимо найти, а также строить целый класс пар взаимно обратных функций на основе одной такой пары.

Теорема 2. *Пусть функции $f_p : G \to G$, $g_p : G \to G$ и $f_0 : G \to G$ являются дифференцируемыми, причем f_p и g_p — взаимно обратные над GJ^k, а f_0 такая, что для любого $x \in G$ выполняется:*

(1) $f_0(x) \in GJ^{\lceil k/2 \rceil}$

(2) $f_0'(x) \in Ann(GJ^k : GJ^{\lceil k/2 \rceil})$.

Тогда обратной к $f(x) = f_p(x) + f_0(x)$ над GJ^k является функция

$$g(x) = g_p(x) - f_0(g_p(x))g_p'(x).$$

Здесь под $Ann(GJ^k : GJ^{\lceil k/2 \rceil})$ понимается множество $\{r \in R \mid GJ^{\lceil k/2 \rceil}r \subseteq GJ^k\}$.

Список литературы

[1] Карпов А.В. Перестановочные многочлены над примарными кольцами // Прикладная дискретная математика. 2013. No. 4(22). (в печати)

Томский государственный университет, Томск
E-mail: karpov@isc.tsu.ru

Алгоритмическое обеспечение алгебраического анализа информативности кинетических измерений

С. И. Спивак, А. С. Исмагилова, А. А. Ахмеров

В [**1**], [**2**] построена общая теория анализа информативности. В качестве математического аппарата используется теория неявных функций и теория непрерывных групповых преобразований. Трудность состоит в том, что использование этой теории связано со сложными аналитическими вычислениями, применение которых сильно затрудняется из-за большой размерности в реальных задачах построения кинетических моделей практически значимых реакций. Возникает вопрос о построении системы автоматизации анализа информативности.

Основной результат данной работы – построение алгоритмов [**3**]-[**5**], допускающих компьютерную интерпретацию. В качестве инструментария выбран аппарат теории графов поскольку механизм сложной реакции может быть представлен следующими эквивалентными формами: в виде системы химических уравнений в символьной форме, с перечислением всех участников и стадий реакции, в виде системы обыкновенных дифференциальных уравнений, матричное представление систем стехиометрических и кинетических уравнений, а также в виде связного ориентированного двудольного графа.

Разработанные алгоритмы легли в основу математического обеспечения решения обратных задач химической кинетики. Создан комплекс компьютерных программ анализа информативности кинетических измерений при решении обратных задач химической кинетики. Результаты иллюстрируются конкретными примерами определения кинетических параметров для реакции пиролиза этана, механизма гетерогенно-каталитического дегидрирования бутана, реакции окисления сероводорода с учетом адсорбции кислорода и сероводорода.

Список литературы

[1] Спивак С.И., Горский В.Г. О полноте доступных кинетических измерений при определении констант скоростей сложной химической реакции // Химическая физика. 1982. Т.1. №2. С.237-243.

[2] Спивак С.И., Исмагилова А.С. Информативность кинетических измерений при определении параметров математических моделей химической кинетики // Журнал СВМО. 2009. Т.11. №2. С.131-136.

[3] Спивак С.И., Исмагилова А.С., Хамитова И.А. // ДАН. 2010. Т. 434. № 4. С.499-501.

[4] Спивак С.И., Исмагилова А.С., Хамитова И.А. // ДАН. 2012. Т. 443. № 6. С.1-3.

[5] Спивак С.И., Исмагилова А.С. // ДАН. 2013. Т. 451. № 3. С.1-3.

Башкирский государственный университет, г.Уфа
E-mail: IsmagilovaAS@rambler.ru

Алгебраическая интерпретация проблемы информативности кинетических измерений при идентификации механизмов сложных химических реакций

С. И. Спивак, А. С. Исмагилова

Основная задача, решаемая в настоящей работе – создание метода, позволяющего существенно упростить исследование на информативность кинетических моделей сложных реакций. Этот метод основан на теоретико-графовом анализе независимых маршрутов [**1**], [**2**].

Маршрут есть вектор, умножение элементов которого на соответствующие стадии механизма сложной реакции вместе с последующим сложением стадий приводит к суммарному уравнению реакции, которое не содержит промежуточных веществ [**1**].

Теорема 1. *Маршрут реакции есть циклический подграф исходного графа. Объединение таких подграфов образует полный граф, т.е. граф исходной системы реакции. Число независимых маршрутов равно числу независимых циклов графа Вольперта* [**3**].

Теорема 2. *Существует преобразование, переводящее граф закона сохранения массы атомов в граф, часть вершин которого не имеет исходящих дуг. Указанные вершины достижимы из базиса ключевых веществ* [**4**].

Совокупность стадий химической реакции можно разложить на подсистемы, в которые входят части стадий исходного механизма. Число таких подсистем равно числу независимых маршрутов. Тогда вместо анализа всей сложной системы реакций расматриваются те, которые отвечают за протекание по каждому из независимых машрутов. Доказаны теоремы 3 и 4:

Теорема 3. *Объединение множеств базисов ключевых веществ для каждой из подсистем совпадает с базисом ключевых веществ исходной системы реакций.*

Теорема 4. *Объединение базисов нелинейных параметрических функций для каждой из подсистем, позволяет выписать базис НПФ исходной сложной системы реакций* [**5**].

Список литературы

[1] Вольперт А.И., Худяев С.И. Анализ в классах разрывных функций и уравнения математической физики. М: Наука, 1975. 394 с.

[2] Альбина Исмагилова, Семен Спивак. Обратные задачи химической кинетики. Каталитические реакции. Germany: LAP LAMBERT Acad. Publ., 2013. 125 p.

[3] Спивак С.И., Исмагилова А.С., Хамитова И.А. // ДАН. 2010. Т. 434. № 4. С.499-501.

[4] Спивак С.И., Исмагилова А.С., Хамитова И.А. // ДАН. 2012. Т. 443. № 6. С.1-3.

[5] Спивак С.И., Исмагилова А.С. // ДАН. 2013. Т. 451. № 3. С.1-3.

Башкирский государственный университет, г.Уфа
E-mail: IsmagilovaAS@rambler.ru

Язык описания лингвистических шаблонов

П. А. Степанов

В работе проводится исследование проблемы извлечения онтологических знаний из текстов естественного языка [**1**]. В процессе решения этих задач разработан язык описания лингвистических шаблонов и реализован его интерпретатор [**2**]. Язык описания лингвистических шаблонов предназначен для поиска грамматических конструкций и описывает связи между грамматическими значениями слов в искомой конструкции. Интерпретатор языка принимает на вход условия, заданные при помощи выражений языка описания лингвистических шаблонов, а также текст естественного языка, в котором должен производиться поиск.

В основу грамматики языка описания лингвистических шаблонов положена грамматика языка регулярных выражений REGEX [**3**]. В качестве элементарных конструкций выступают условия на словоформу, задающие список грамматических значений, которые должна реализовывать искомая словоформа. Также может быть указана исходная форма искомого слова. Такие элементарные конструкции составляются в более сложные регулярные выражения.

Определение. Рассмотрим недетерминированный автомат-распознаватель $A = \langle S, X, s_0, \delta, F\rangle$ и последовательность символов входного алфавита $x_1...x_N$, где $x_i \in X$. Будем называть множество $I_A(x_1...x_N) = \{\langle i_1, i_2, f\rangle : 1 <= i_1 <= i_2 <= N+1, f \in F \cap \delta^*(s_0, x_{i_1}...x_{i_2-1})\}$ множеством интерпретаций автоматом A входной последовательности $x_1...x_N$.

Теорема. Рассмотрим пару недетерминированных автоматов-распознавателей $A = \langle S^A, X^A, s_0^A, \delta^A, F^A\rangle$ и $B = \langle S^B, X^B, s_0^B, \delta^B, F^B\rangle$, что $F^A \subseteq X^B$ и результаты работы автомата A используются в качестве входных последовательностей автомата B. Рассмотрим входную последовательность $x_1...x_N \in X^A$, а также некоторую $\bar{f}_B = f_1^B...f_K^B \in S_B$. Тогда $\exists \bar{f}_A \in R_A(x_1...x_N) : \bar{f}_B \in R_B(\bar{f}_A)$ тогда и только тогда, когда $\exists n_0...n_K : 1 = n_0 <= n_1 <= ... <= n_K = N+1$, что $\forall i : \langle n_{i-1}, n_i, f_i^B\rangle \in I_B(I_A(x_1...x_N))$.

Таким образом доказано, что множества интерпретаций являются корректным способом хранения результатов анализа последовательностей при помощи автоматов-распознавателями, к которым относится большинство алгоритмов обработки текста.

При поиске участков текста, удовлетворяющих грамматическим условиям, заданным при помощи языка описания лингвистических шаблонов, интерпретатор использует недетерминированные автоматы-распознаватели. На первом этапе анализа текст обрабатывается морфологическим анализатором, который естественным образом порождает альтернативные варианты анализа. Все эти альтернативные варианты анализа представляются в виде множеств интерпретаций, которые затем используется в качестве входа автомата, восстановленного по искомому регулярному выражению. Результаты поиска также представляются в виде множества интерпретаций.

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] Regular expression // Wikipedia The Free Encyclopedia.
URL: http://en.wikipedia.org/wiki/Regular_expression (дата обращения: 05.11.2013).

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

Применение обобщенных нечетких моделей в задачах согласования знаний, извлеченных из разных документов

О. В. Ясинская

Для эффективной защиты от компьютерной угрозы необходимо как можно раньше узнать о её появлении. Один из наиболее актуальных источников такой информации — тексты на естественном языке, представленные в сети Интернет.

Одной из методологий обработки знаний, извлечённых из текстов на естественном языке, является теоретико-модельный подход представления знаний. Он основан на разработанном теоретико-модельном подходе к формализации онтологий предметных областей ([**1**]). В рамках данного подхода знания, извлекаемые из текстов, написанных на естественном языке, представляются в виде алгебраических систем (прецедентов предметной области). На основе прецедентов строится прецедентная модель предметной области ([**2**]). Значением истинности предложения на прецедентной модели является набор тех прецедентов, для которых это предложение является истинным в точном смысле. В результате фазификации прецедентной модели получается нечёткая модель, в которой значениями истинности предложений являются числа из интервала $[0, 1]$. Фазифицируя некоторое множество прецедентных моделей как единое целое, мы получаем обобщенную нечеткую модель ([**3**]).

Одним из путей порождения новых знаний при помощи текстов естественного языка является сравнение и интеграция знаний, содержащихся в разных текстах ([**4**]). В процессе извлечения знаний из текстов на естественном языке, строятся различные обобщенные нечеткие модели, формализующие извлечённое знание. И, соответственно, возникает необходимость в согласовании различных алгебраических систем. Для реализации согласования знаний строится обобщенная нечеткая модель, являющаяся произведением всех хранящихся в базе алгебраических систем ([**5**]). Согласованное значение истинности предложения вычисляется в виде интервала, определенного на отрезке $[0, 1]$. В рамках данной работы разработаны алгоритмы вычисления согласованного значения истинности и реализован модуль программной системы, позволяющий вычислять истинностное значение любого бескванторного предложения, представленного в виде СДНФ.

Список литературы

[1] Пальчунов Д.Е. Решение задач поиска информации на основе онтологий // Бизнес-информатика, т.1, 2008, с. 3-13.

[2] Яхъяева Г.Э., Ясинская О.В. Применение методологии прецедентных моделей в системе риск - менеджмента, направленного на раннюю диагностику компьютерного нападения // Вестник НГУ. Серия: Информационные технологии. 2012. Т.10, вып. 2. С. 106-115.

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

[4] Пальчунов Д.Е. Поиск и извлечение знаний: порождение новых знаний на основе анализа текстов естественного языка // Философия науки. 2009. №4(43). С. 70-90.

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

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

An iterative construction of APN functions

A. A. Gorodilova

Let $GF(2^n)$ be a finite field of order 2^n. A function $F : GF(2^n) \to GF(2^n)$ can be considered as a vectorial Boolean function in n variables. It is known that such a function has the unique representation in the form $F(x) = \sum_{i=0}^{2^n-1} c_k x^k$, where $c_k \in GF(2^n)$.

Vectorial Boolean functions are used in block ciphers as S-boxes (nonlinear components of ciphers). S-boxes should have special properties for guaranteeing security of a cipher against different kinds of cryptanalysis.

A vectorial Boolean function F is called differentially δ-uniform if for every nonzero $a \in GF(2^n)$ and every $b \in GF(2^n)$ the equation $F(x)+F(x+a) = b$ has at most δ solutions. These functions with small δ contribute to a high resistance to differential cryptanalysis. For example, differentially 4-uniform function in 8 variables is used as S-box in cipher AES (Advanced Encryption Standard). The smallest possible value of δ is 2 and in this case such functions are called APN functions.

A vectorial function $F(x) = x^d$ is called monomial function. All known exponents d that lead to APN functions are the following: $d = 2^i + 1$, $\gcd(i, n) = 1$ (Gold function); $d = 2^{2i} - 2^i + 1$, $\gcd(i, n) = 1$ (Kasami function); $2^t + 3$, $n = 2t + 1$ (Welch function); $2^t + 2^{\frac{t}{2}} - 1$ for t even and $2^t + 2^{\frac{3t+1}{2}} - 1$ for t odd (Niho function); $2^{2t} - 1$ $n = 2t+1$ (Inverse function); $2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$, $n = 5t$ (Dobbertin function). Further nonmonomial APN functions can be found in paper [**1**].

In this work we present an iterative construction of APN function.

Theorem. *Let $F, G : GF(2^n) \to GF(2^n)$ be two APN functions and let $f, g : GF(2^n) \to GF(2)$ be two Boolean functions. Consider $GF(2^{n+1})$ and an element $c \in GF(2^{n+1}) \setminus GF(2^n)$. Then the following vectorial Boolean function S from $GF(2^{n+1})$ to $GF(2^{n+1})$, where $x \in GF(2^n)$, $\alpha \in GF(2)$,*

$$S(y) = S(x + \alpha c) = (\alpha + 1)F(x) + \alpha G(x) + c((\alpha + 1)f(x) + \alpha g(x))$$

is APN if the condition holds

$$\text{for all } x, y, a \in GF(2^n),\ a \neq 0, \text{ such that } F(x) + F(x + a) = G(y) + G(y + a)$$
$$\text{we have } f(x) + f(x + a) \neq g(y) + g(y + a).$$

We get the following numerical experiments for small n:

- $n = 1$: this iterative construction generates all 192 APN functions in 2 variables;
- $n = 2$: this iterative construction generates 589824 APN functions from all 668128 APN functions in 3 variables.

References

[1] Budaghyan L. Construction and Analysis of Cryptographic Functions. Habilitation Thesis, University of Paris 8, Sept. 2013.

Novosibirsk State University, Novosibirsk
E-mail: gorodilova.aa@gmail.com

On a property of quadratic Boolean functions

N. A. Kolomeec

A mapping $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is called a Boolean function in n variables. A Boolean function is called *affine* if its algebraic degree (degree of its algebraic normal form) not more than 1 and *quadratic* if its algebraic degree is equal to 2. An *affine subspace* is a shift of a linear subspace. A Boolean function f in n variables is *affine on the set* $D \subseteq \mathbb{Z}_2^n$ if $f|_D(x) = \langle a, x\rangle \oplus c$ for some $a \in \mathbb{Z}_2^n$, $c \in \mathbb{Z}_2$, where $\langle a, x\rangle = a_1x_1 \oplus \ldots \oplus a_nx_n$. A Boolean function f in n variables is called *normal* (*weakly normal*) if there exists an affine subspace of dimension $\lceil \frac{n}{2} \rceil$ that f is constant (affine) on it, see Dobbertin [**2**], Charpin [**1**]. A Boolean function in even number of variables is called a *bent* function if it is at the maximal possible distance from the set of all affine functions, see [**5**].

All quadratic Boolean functions have the following property.

Statement. *Let f be a quadratic Boolean function in n variables and f be affine on an affine subspace L of dimension $\lceil \frac{n}{2} \rceil$. Then f is affine on any shift of L.*

We can choose an affine subspace of any dimension in the previous statement, but in that case not for all quadratic functions there exists at least one L that f is affine on it, while such an affine subspace of dimension $\lceil \frac{n}{2} \rceil$ always exists.

Also, affine subspaces of such dimension can be used to construct bent functions from the given bent functions ([**4**], [**3**]).

A question appears: are there non-quadratic Boolean functions that the statement is right? The following theorem gives an answer on the question.

Theorem. *Let f be a Boolean function in n variables and it holds the following: if f is affine on an affine subspace L of dimension $\lceil \frac{n}{2} \rceil$ then f is affine on any shift of L. Then f is either affine or quadratic or non-weakly normal.*

Statement. *Let f be a bent function in 6 variables. Then there exist affine subspaces L_1, L_2, L_3 of dimension 3, that $f \oplus Ind_{L_1}, f \oplus Ind_{L_1} \oplus Ind_{L_2}, f \oplus Ind_{L_1} \oplus Ind_{L_2} \oplus Ind_{L_3}$ are bent functions and at least one of them is quadratic.*

References

[1] Charpin P. Normal Boolean functions // Journal of Complexity. — 2004. — V. 20. — P. 245–265

[2] Dobbertin H. Construction of bent functions and balanced Boolean functions with high nonlinearity // Fast Software Encryption, Lecture Notes in Computer Science. — 1994. — V. 1008. — P. 61–74.

[3] Kolomeec N.A., Pavlov A.V. Properties of Bent functions that are on the minimal possible distance // Descrete Applied Mathematics. — 2009. — No 4. — P. 5–20. (in Russian).

[4] Logachev O.A., Salnikov A.A., Yaschenko V.V. Boolean functions in coding theory and cryptology. MCCME, Moscow. 2004. — 470. (In Russian)

[5] Rothaus O. On bent functions // J. Combin. Theory, Ser. A. — 1976. — V. 20. No 3. — P. 300–305.

Sobolev Institute of Mathematics, Novosibirsk (Russia)
E-mail: nkolomeec@gmail.com

Verification of multi-state Pfaffian dynamics

M. V. Korovina

The main aim of the ongoing research presented in this talk is to create a logical framework for formal analysis of definable dynamical systems. The key ideas of this framework are based on computing combinatorial types of trajectories of multi-state dynamical systems. Suppose we have multi-state dynamics which is a finite family of dynamical systems and state conditions on switches between them. The state space of every dynamical system has a finite partition, and each element of the partition is labelled by a letter of some alphabet. Then every trajectory of the dynamics is naturally labelled by a word in the joint alphabet. This word is called the combinatorial type of the trajectory. In applications it is important to decide whether among a certain family of trajectories there is at least one trajectory of a given type, or whether all the trajectories in this family have the same type. In this talk we propose algorithms for solving this sort of questions for wide classes of multi-state Pfaffian dynamics, which have elementary (doubly-exponential) upper complexity bounds.

The research is partially supported by EU project PIRSES-GA-2011-294962 “Computable Analysis” and RFBR project 13-01-00015a.

A.P. Ershov Institute of Informatics Systems RAS, Novosibirsk (Russia)
E-mail: rita.korovina@gmail.com

There is a transitive nonpropelinear perfect code

F. I. Solov'eva, I. Yu. Mogilnykh

A *binary code* of length n is a collection of binary vectors of length n. Consider a transformation of type (x, π), where x is a binary vector, and π is a permutation on coordinate positions acting on a binary vector y by the following rule:

$$(x, \pi)(y) = x + \pi(y).$$

The *automorphism group* $Aut(C)$ of a code C is a collection of transformations (x, π) that fixes C setwise. A code C is called *transitive* if there is a subgroup H of $Aut(C)$ acting transitively on codewords of C.

In case when the order of H equals $|C|$, or equivalently H is a regular group [**6**], the code C is called *propelinear* [**7**]. Each regular subgroup naturally induces a group on codewords of C. In general a code yields many different (including nonisomorphic ones) regular subgroups of its automorphism group (for the case of perfect code see [**3**]).

The notion of propelinearity is extremely important in algebraic-combinatorial coding theory because it provides a general view on linear, Z_2Z_4-linear and additive codes.

The inequality of classes of transitive and nonpropelinear codes was supposed in [**1**] and solved later in [**3**] by showing that $(10, 40, 4)$ Best code is transitive nonpropelinear.

In the current work we handle the question for the class of perfect codes by studying the characterization of perfect codes of length 15 given in [**5**].

Theorem. *A transitive nonpropelinear perfect code of length 15 exists.*

The work of the first author was partially supported by the Grant RFBR 12-01-00631-a and the work of the second author was partially supported by the Grants RFBR 12-01-00448, 12-01-31098.

References

[1] Borges J., Rifà J., Solov'eva F. I., On properties of propelinear and transitive binary codes, 3rd International Castle Meeting on Coding Theory and Applications 2011 3ICMCTA, CARDONA CASTLE, Spain, September 10-15, 2011, to appear.

[2] Borges J., Rifa J., A characterization of 1-perfect additive codes, IEEE Trans. Inform. Theory, 1999. V. 45. P. 1688–1697.

[3] Borges J., Mogilnykh I. Yu., Rifà J., Solov'eva F. I., Structural properties of binary propelinear codes, Advances in Mathematics of Communications, Volume 6, No. 3, 2012, pp. 329-346.

[4] Malyugin S. A., On equivalent classes of perfect binary codes of length 15, Preprint 138. Novosibirsk: Inst. of Mathematics of SB RAS. 2004. P. 34 (in Russian).

[5] Östergård P. R. J., Pottonen O., The perfect binary one-error-correcting codes of length 15: Part I – Classification, ArXiv, http://arxiv.org/src/0806.2513v3/anc/perfect15.

[6] Phelps K. T., Rifà J., On binary 1-perfect additive codes: some structural properties, IEEE Trans. on Inform. Theory, vol. 48. pp. 2587–2592, 2002.

[7] Rifà J., Basart J. M., Huguet L., On completely regular propelinear codes, in Proc. 6th Int. Conference, AAECC-6, n. 357 LNCS, pp. 341–355, 1989.

Sobolev Institute of Mathematics and Novosibirsk State University, Novosibirsk, Russia;
E-mail: ivmog,sol@math.nsc.ru;

On the support of a Boolean bent function

N. N. Tokareva

Consider Boolean functions in n variables, i. e. functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$.

The *support* of a Boolean function f is the set of all vectors x such that $f(x) = 1$. It is denoted by $supp(f)$. A *derivative in direction* $y \in \mathbb{Z}_2^n$ of a Boolean function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is the Boolean function $D_y f(x) = f(x) + f(x + y)$. A Boolean function in n variables (n is even) is called *bent* if every its derivative in nonzero direction is balanced (takes values 0 and 1 equally often) [**2**]. Bent functions and their generalizations are used in cryptography for constructing S-boxes resistant to linear and differential cryptanalysis [**3**].

A subset $M \subseteq \mathbb{Z}_2^n$ we call *strongly* (k, λ)*-regular*, if its size is k and cardinality of intersection of M and any its shift $M + y$, where $y \neq 0$, is equal to λ. We call this set *proper*, if $0 < k < 2^n$, $0 < \lambda < 2^n$. It is easy to see that M is strongly (k, λ)-regular iff Cayley graph of a Boolean function f, where $supp(f) = M$, is strongly regular with parameters $(2^n, k, \lambda, \lambda)$.

In this work we obtain the simple proof of the following fact [**1**].

Theorem. *The support of a bent function is a strongly regular set. Every proper strongly regular set in* $\mathbb{Z}_2^n$ *is a support of a certain bent function in* n *variables and has parameters* $(2^{n-1} \pm 2^{(n/2)-1}, 2^{n-2} \pm 2^{(n/2)-1})$.

Then we prove

Proposition. *Let* f *be a bent function. Then every element of* $supp(f)$ *is covered by the same number of sets* $supp(f) + y$*, where* $y \neq 0$.

By definition every function $D_y f$ is balanced if f is bent and y is nonzero. The natural question about the structure of the support of $D_y f$ arises.

Proposition. *The support of a derivative of a bent function is not an affine subspace.*

References

[1] Bernasconi A., Codenotti B., VanderKam J. M. A characterization of bent functions in terms of strongly regular graphs. IEEE Trans. Computers. 2001. V. 50. No. 9. P. 984–985.

[2] Rothaus O. On bent functions. J. Combin. Theory. Ser. A. 1976. V. 20, P. 300–305.

[3] Tokareva N. Nonlinear Boolean functions: bent functions and their generalizations LAP LAMBERT Academic Publishing (Germany), 2011. ISBN: 978-3-8433-0904-2. 180 pages.

Sobolev Institute of mathematics, Novosibirsk (Russia)
E-mail: tokareva@math.nsc.ru
itkup@yandex.ru

On Threshold Implementations of vectorial Boolean functions in cryptographic primitives

V. A. Vitkup

Many cryptographic algorithms are vulnerable to so-called side-channel attacks. *Threshold implementation* is a recent countermeasure against such attacks introduced by S. Nikova *et.al* [1]. This method can be summarized as follows. Consider the vectorial Boolean function (S-box) $S : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, $S = (f_1, \ldots, f_n)$, where $f_1, ..., f_n$ are the coordinate functions of F. Split each variable x_i into r additive Boolean variables: $x_i = \sum_{j=1}^{r} x_{ij}$. Denote the vector $v = (x_{11}, ..., x_{nr})$. Split the vectorial function S into r functions S_i : $\mathbb{Z}_2^{nr} \to \mathbb{Z}_2^n$ to satisfy the following: $S(x) = \sum_i S_i(v)$. This *sharing* of the fucntion S we denote as $P(S)$. It should satisfy two properties:

1. *Non-completeness*: S-box S_i must be independent from variables x_{ki}.
2. *Uniformity*: the function $S^* : \mathbb{Z}_2^{nr} \to \mathbb{Z}_2^{nr}$, $S^* = (S_1, \ldots, S_r)$ is 1-1 function.

The sharing $P(S)$ with these properties is called an *admissible* sharing. The set of S-boxes $\mathbb{Z}_2^3 \to \mathbb{Z}_2^3$ contains four equivalence classes, $\mathcal{A}_1^3, \mathcal{Q}_1^3, \mathcal{Q}_2^3, \mathcal{Q}_3^3$. The main method of representing S-box as a sum $S(x) = \sum_i S_i(v)$ is called the *direct sharing*. It does not necessarily satisfy the property of uniformity. To achieve the uniformity of a sharing the authors in [1] insert pairs of *correction terms*. The admissible sharing for class $\mathcal{Q}_3^3$ with the representative $(xy + xz + yz, x + y + xy + yz, x + z + yz)$ was not found and an exhaustive search requires large number of operations, so in [1] the open question how to find the admissible sharing with 3 shares for $\mathcal{Q}_3^3$ was posed.

Let $S = (f_1, ..., f_n)$, $S : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ and $P(S)$ be the direct sharing of S-box S into r shares $S_i = (f_{1i}, ..., f_{ni})$. Consider the vectorial function $F = (f_{11}, ..., f_{n1}, ..., f_{1r}, ..., f_{nr})$.

We say that the function $C_F = (c_{11}, ..., c_{n1}, ..., c_{1r}, ..., c_{nr})$, $c_{ij} : \mathbb{Z}_2^{nr} \to \mathbb{Z}_2$ is a *correction function* for F, if the function $F + C_F$ has the following properties:

1. $f_i = \sum_{j=1}^{r}(f_{ij} + c_{ij})$ 2. $f_{ij} + c_{ij}$ is independent from variables $x_{1j}, ..., x_{nj}$.

Let $k \in \{1, \ldots, nr\}$ and let $(i_1 j_1, ..., i_k j_k)$ be the tuple of indices of length k. By $C^k_{i_1 j_1,\ldots,i_k j_k}$ denote the following set: $C^k_{i_1 j_1,\ldots,i_k j_k} = \{C_F \mid (f_{i_1 j_1} + c_{i_1 j_1}, ..., f_{i_k j_k} + c_{i_k j_k})$ is a balanced function from $\mathbb{Z}_2^{nr}$ in $\mathbb{Z}_2^k\}$. Consider the set $C = \bigcap_k \bigcap_{i_1 j_1,\ldots,i_k j_k} C^k_{i_1 j_1,\ldots,i_k j_k}$.

Theorem. *The function $F + C_F$ is a bijection if and only if $C_F \in C$.*

This theorem allows us to use the specific algorithm to search the admissible sharing for S-boxes from $\mathcal{Q}_3^3$. We obtained that the set C from the theorem is empty, hence, there is no admissible sharing for the given S-box. This proves the following:

Corollary. *There does not exist an admissible sharing with 3 shares for S-boxes from $\mathcal{Q}_3^3$.*

References

[1] Bilgin B., Nikova S., Nikov V., Rijmen V., Stütz G. Threshold Implementations of all 3x3 and 4x4 S-boxes, CHES 2012, LNCS 7428, Springer-Verlag 2012, pp. 76–91.

Novosibirsk state university, Novosibirsk

VII. Секция «Неклассические логики»

Расширения конечных решеток для модальных и дескрипционных логик

А. О. Башеева, Ю. В. Гребенёва, А. Ж. Сатекбаева, Н. В. Шилов

Определение. Для любой решетки L и любого свойства P решеток (например, дистрибутивность), P-расширение L — это любая решетка L' со свойством P, в которую L может быть вложена как частично упорядоченное множество.

В работах [**3, 2**] были определены и исследованы модальные логики со значениями в конечных дистрибутивных решётках. Поэтому для того, что бы определить модальные логики со значениями в произвольной конечной решётке, возникает интерес исследовать дистрибутивные расширения конечных решёток. В работе [**1**] сформулирована следующая

Теорема 1: *Пусть P — это любое из следующих свойств решеток: или модулярность, или дистрибутивность, или полудистрибутивность. Тогда для любой конечной решетки L существует конечное P-расширение решетки L.*

Дескрипционные логики — это семейство вариантов полимодальной логики для описания «знаний» о предметных областях (представленных в виде терминологических фактов, определений и отношений). В частности, $\mathcal{ALC}$ — это полимодальный вариант логики K. В работе [**4**] определена семантика этой логики со значениями в решётке понятий, порождённой симметричным контекстом и доказана следующая

Теорема 2: *Для любой терминологической интерпретации $I = (D, \Upsilon)$, для любой формулы ϕ логики $\mathcal{ALC}$ значение этой формулы в решётке понятий контекста $(D, D, \neq)$ есть $(I(\phi),\ I(\neg\phi))$.*

Для того, что бы определить дескрипционную логику со значениями в произвольной решётке понятий, возникает необходимость исследовать методы расширения произвольных конечных контекстов до симметричных, которые приводят к симметричным расширениям соответствующих решёток понятий. В работе [**4**] исследовано 16 вариантов таких расширений контекстов.

Список литературы

[1] Башеева А. О., Сатекбаева А. Ж. Расширение решеток и их применение в АФП. Материалы международной научной конференции студентов, магистрантов, аспирантов и молодых ученых «Ломоносов-2013» (8-12 апреля 2013г). Астана 2013, стр.14-15.

[2] Fitting M. C. Many-valued modal logics II. Fund. Inform., 1992, v.17, p. 55–73.

[3] Fitting M. C. Many-valued modal logics. Fund. Inform., 1991, v.15, p. 235–254.

[4] Grebeneva J., Shilov N., Garanina N. Towards Description Logic on Concept Lattices. Accepted for presentation at International Conference on Concept Lattices and Their Applications — CLA'13. To appear in CEUR Workshop Proceedings series, 2013.

Евразийский национальный университет им. Л.Н. Гумилева, г. Астана, Казахстан;
Институт систем информатики им. А.П. Ершова СО РАН, г. Новосибирск, Россия;
Назарбаев Университет, г. Астана, Казахстан
E-mail: basheeva@mail.ru, j.grebeneva@gmail.com, aika_satekbayeva@mail.ru, shilov@iis.nsk.su, nikolay.shilov@nu.edu.kz

Количество разложений числа n, в том числе заданной длины, каждое из которых содержит одновременно все числа $m_1, \ldots, m_s$

А. В. Кошелева

Известно, что количество разложений натурального числа n равно 2^{n-1}, при этом C_{n-1}^{l-1} имеют длину l. В работе, с помощью упорядочивания подмножеств разложений фреймами Крипке, найдено количество разложений числа n, каждое из которых содержит одновременно все числа $m_1, \ldots, m_s < n$. Также найдено количество разложений числа n длины l, каждое из которых содержит все числа $m_1, \ldots, m_s < n$. Под *подмножеством разложения* $a = (x_1, x_2, \ldots, x_k)$ будем понимать такое подмножество $b \in a$, части которого взяты в исходном их порядке. Приведем основную теорему, с помощью которой выводятся все нужные формулы. Пусть $F_{n,k}$ — фрейм Крипке, построенный специальным образом из подмножеств разложений числа n, а $kol(k, i, m_1, m_2, \ldots, m_s)$ означает количество таких подмножеств, содержащих числа $m_1, m_2, \ldots, m_s \in [2,\ i+1]$ на i-ом слое фрейма $F_{n,k}$. Каждый такой фрейм — корневой и нумерация слоев фрейма для удобства начинается с корневого слоя. В теореме подмножества разложений, из которых составлен фрейм, называются просто разложениями.

Теорема. *Количество разложений, содержащих числа* $m_1, m_2, \ldots, m_s \in [2,\ i\ +\ 1\ ]$ *на i-ом слое фрейма* $F_{n,k}$, $2 \leq s \leq k$, *находится по реккурентной формуле*

$$kol(k, i, m_1, m_2, \ldots, m_s) = s\, kol(k-1, i-m_1+2, m_2, \ldots, m_s) +$$

$$+ \sum_{\substack{j=max(m_1, m_2, \ldots, m_s)-1, \\ j \neq i-m_1+2, \\ \vdots \\ j \neq i-m_s+2}}^{i} kol(k-1,\ j,\ m_1,\ m_2,\ \ldots,\ m_s)$$

с базой рекурсии:

если $m_1 + m_2 + \ldots + m_s = 2\,s + j - 1$, *то* $kol(s, j, m_1, m_2, \ldots, m_s) = s\,!$;

если $m_1 + m_2 + \ldots + m_s \neq 2\,s + j - 1$, *то* $kol(s,\ j,\ m_1,\ m_2,\ \ldots,\ m_s) = 0$.

Для $kol(k, i, m)$, то есть в случае одного числа m, найдена и нереккурентная формула.

СФУ, Красноярск
E-mail: koshelevaa@mail.ru

Аксиоматика полных по П.С. Новикову расширений суперинтуиционистской логики L1 в языке с несколькими дополнительными константами

А. К. Кощеева

Пусть Fm — множество формул стандартного пропозиционального языка. Обогатим язык набором дополнительных логических констант $\bar{\varphi} = \{\varphi_1, \varphi_2, ..., \varphi_n\}$.

Логикой Даммета (логикой $L1$) называется суперинтуиционистская логика, полученная добавлением к Int аксиомы линейности $(A \to B) \vee (B \to A)$. Логика $L1$ характеризуется классом конечных линейно упорядоченных шкал (цепей).

$\bar{\varphi}$-Логикой называется множество $\mathcal{L}$ формул расширенного языка, включающее Int и замкнутое относительно правил modus ponens и подстановки. $\bar{\varphi}$-Логика $\mathcal{L}$ называется ***консервативным расширением*** логики L, если $L \subset \mathcal{L}$ и для всякой чистой формулы A выполнено: из $A \in \mathcal{L}$ следует $A \in L$. $\bar{\varphi}$-Логика $\mathcal{L}$ называется ***полным по П.С. Новикову расширением*** логики L, если $\mathcal{L}$ консервативна над L и для любой формулы $A \in Fm(\bar{\varphi}) \setminus \mathcal{L}$, $\bar{\varphi}$-логика $\mathcal{L} + A$ неконсервативна над L. Под ***проблемой Новикова для*** $L1$ понимается описание класса всех полных по Новикову расширений (***пополнений***) $L1$ в конкретном расширении языка, в рассматриваемом случае с новым конечным набором логических констант $\bar{\varphi}$.

Моделями $\bar{\varphi}$-логик являются так называемые *$\bar{\varphi}$-шкалы*, т.е. шкалы с выделенными конусами, которыми интерпретируются константы.

В работе [**1**] для описания полных расширений логики Даммета применяется понятие конечной цепи с наростом определенного типа. Под термином ***нарост*** понимается конечная $\bar{\varphi}$-цепь, в которой все точки имеют разные цвета. Под ***цветом*** точки понимается множество дополнительных констант, приписанных к этой точке. Заметим, что всего существует 2^n цветов. Такой нарост присоединяется «сверху» к произвольной конечной цепи, при этом цвет корня нароста дублируется на точки основы. В качестве типового примера рассмотрим нарост следующего вида: $\bullet - - - \underset{\varphi_1}{\bullet} - - - \underset{\varphi_1\varphi_2}{\bullet} - - - \ldots - - - \underset{\varphi_1, ..., \varphi_n}{\bullet}$

Аксиоматика полного по П.С. Новикову расширения $\bar{\varphi}$-логики, определяемой этим наростом, задается так:

$1^0_k.\ L1 + (\varphi_k \to \varphi_{k+1}) \to \varphi_{k+1}\,, k = [1, n-1]$;

$2^0_k.\ L1 + \varphi_{k+1} \to \varphi_k\,, k = [1, n-1]$;

$3^0.\ L1 + \varphi_1 \to (A \vee (A \to \varphi_2))$;

$4^0.\ L1 + \neg\neg\varphi_n$;

$5^0.\ L1 + \varphi_n \to (p \vee \neg p)$.

Список литературы

[1] Яшин А.Д. О новых константах в двух предтабличных суперинтуиционистских логиках // Алгебра и логика, Т. 50, № 2, 2011, с. 246–267.

Удмуртский государственный университет, Ижевск
Московский городской психолого-педагогический университет, Москва
E-mail: kannakst@mail.ru, kannko@yandex.ru

Об исчислении Ламбека с операцией пересечения и конъюнктивных грамматиках

С. Л. Кузнецов

Исчисление Ламбека, допускающее пустые левые части секвенций, (L^*) определяется следующим образом. Типы (формулы) этого исчисления строятся из примитивных типов $p_1, p_2, \ldots$ с помощью трёх связок: $\backslash$, $/$ и $\cdot$. Секвенции L имеют вид $\Gamma \to A$, где Γ — последовательность типов, A — тип. Аксиомы имеют вид $A \to A$; правила вывода таковы (латинские буквы обозначают типы, греческие — их последовательности):

$$\frac{A\,\Pi \to B}{\Pi \to A \setminus B}\ (\to \setminus) \qquad \frac{\Pi \to A \,\&\, \Gamma\, B\, \Delta \to C}{\Gamma\, \Pi\, (A \setminus B)\, \Delta \to C}\ (\setminus \to);$$

$$\frac{\Pi\, A \to B}{\Pi \to B \,/\, A}\ (\to /) \qquad \frac{\Pi \to A \,\&\, \Gamma\, B\, \Delta \to C}{\Gamma\, (B \,/\, A)\, \Pi\, \Delta \to C}\ (/ \to);$$

$$\frac{\Gamma \to A \,\&\, \Delta \to B}{\Gamma\, \Delta \to A \cdot B}\ (\to \cdot); \qquad \frac{\Gamma\, A\, B\, \Delta \to C}{\Gamma\, (A \cdot B)\, \Delta \to C}\ (\cdot \to);$$

L^*-*грамматика* — это тройка $\mathcal{G} = \langle \Sigma, \rhd, H \rangle$, где Σ — алфавит, H — тип и $\rhd \subset \mathrm{Tp} \times \Sigma$ — конечное соответствие между типами и буквами алфавита. Слово $w = a_1 \ldots a_n$ допускается грамматикой, если существуют такие типы $A_1, \ldots, A_n$, что $L^* \vdash A_1 \ldots A_n \to H$ и $A_i \rhd a_i$ для всех i.

Известно (Х. Гайфман 1960, М. Р. Пентус 1993, С. К. 2012), что L^*-грамматики задают в точности контекстно-свободные языки.

Расширим исчисление L^* новой связкой $\cap$ с правилами

$$\frac{\Gamma\, A_i \Delta \to C}{\Gamma\, (A_1 \cap A_2)\, \Delta \to C}\ (\cap \to)_i,\ i = 1, 2 \qquad \frac{\Pi \to A \,\&\, \Pi \to B}{\Pi \to A \cap B}\ (\to \cap)$$

С другой стороны, рассмотрим предложенное А. Охотиным обобщение контекстно-свободных грамматик — *конъюнктивные грамматики:* правила в них имеют вид $A \to \beta_1 \& \ldots \& \beta_n$ $(n \geqslant 1)$; Слово w можно вывести из A тогда и только тогда, когда оно выводимо из всех β_i.

Конъюнктивная грамматика называется *конъюнктивной грамматикой в форме Грейбах,* если её правила имеют вид $A \to a\beta_1 \& \ldots a\beta_n$ $(a \in \Sigma)$ или $S \to \varepsilon$ (S — стартовый символ, ε — пустое слово). Вопрос о приведении произвольной конъюнктивной грамматики к форме Грейбах остаётся открытым; тем не менее, уже грамматики в форме Грейбах способны порождать некоторые достаточно сложные языки, например $\{a^{4^n} \mid n \geqslant 0\}$ (А. Еж 2008).

Теорема. *Всякий язык, задаваемый конъюнктивной грамматикой в форме Грейбах, может быть задан грамматикой, основанной на расширенном операцией пересечения исчислении* L^*.

Московский государственный университет им. М. В. Ломоносова, г. Москва
E-mail: sk@lpcs.math.msu.su

О технике построения канонических формул модальных логик в случае нетранзитивных шкал

Е. И. Латкин

Известная техника Захарьящева [**1**] для построения канонических формул для **K4** существенным образом опирается на транзитивность шкал Крипке описывающих эту логику. В данной работе рассматриваются расширения логики **BK**, Белнаповского варианта наименьшей нормальной модальной логики **K**. В работе [**2**] с помощью твист-структур над модальными алгебрами была описана алгебраическая семантика для этой логики, а так же семантика в терминах шкал Крипке. Модальные шкалы Крипке, описывающие логику **BK**, не обязаны быть транзитивными, что не позволяет напрямую перенести технику Захарьящева. В процессе разработки алгоритма, который по данной формуле φ строит канонические формулы $\alpha_1, \ldots, \alpha_N$ такие, что $\mathbf{BK} + \varphi = \mathbf{BK} + \alpha_1 + \ldots + \alpha_N$, были получены следующие факты:

Предложение 1

$$\mathbf{BK} = \{\varphi \in For \mid \mathcal{F} \models \varphi \text{ для всех корневых BK-шкал } \mathcal{F}\},$$

здесь и далее, For — это множество всех формул рассматриваемого языка.

Предложение 2

$$\mathbf{BK} = \{\varphi \in For \mid \mathcal{F} \models \varphi \text{ для всех конечных интранзитивных BK-деревьев } \mathcal{F}\}.$$

Список литературы

[1] Chagrov A., Zakharyaschev M. Modal logic. Oxford, 1997.

[2] Odintsov S.P., Wansing H. Modal logics with Belnapian truth values// Journal of Applied Non-Classical Logics V.20, 2010, P.279–301.

[3] Odintsov S.P., Latkin E.I. BK-lattices. Algebraic semantics for Belnapian modal logics // Studia Logica, V. 100, 2012, 319–338.

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

О конечной аксиоматизации линейной логики знания и времени LTK_r с интранзитивным отношением времени

А. Н. Лукьянчук, В.В. Римацкий

Мы продолжаем исследование свойств много-модальной линейной логики Знания и Времени LTK_r с рефлексивным и интранзитивным отношением времени. Логика определяется семантически, как множество формул, истинных на фреймах специального вида. Время рассматриваем как линейную дискретную последовательность моментов. Каждый момент содержит в себе набор информационных узлов, связанных между собой кортежем модальных операций R_i, имитирующих знания агентов.

Представлен конечный набор формул, и доказано, что данный набор образует систему аксиом логики LTK_r.

Аксиомы AS_{LTK_r}:

Аксиомы **CPC** (классического пропозиционального исчисления);
$L_{\Box_T}$: $\Box_T(\Box_T A \to B) \vee \Box_T(\Box_T B \to A)$;
$K_{\Box_\xi}$: $\Box_\xi(A \to B) \to (\Box_\xi A \to \Box_\xi B)$, $\xi \in \{T, \sim, 1, \dots, k\}$;
$T_{\Box_\xi}$: $\Box_\xi A \to A$, $\xi \in \{T, \sim, 1, \dots, k\}$;
$4_{\Box_\xi}$: $\Box_\xi A \to \Box_\xi \Box_\xi A$, $\xi \in \{\sim, 1, \dots, k\}$;
$5_{\Box_\xi}$: $\neg\Box_\xi A \to \Box_\xi \neg\Box_\xi A$, $\xi \in \{\sim, 1, \dots, k\}$;

$M.1$: $\Box_T A \to \Box_\sim A$;
$M.2$: $\Box_\sim A \to \Box_i A$, $1 \leq i \leq k$;
AL: $\Box_\sim A \wedge \Box_\sim B \wedge \Diamond_T(\neg A \wedge \Box_\sim B) \to \Box_T B$.

Правила вывода AS_{LTK_r}:

$$MP : \frac{A, A \to B}{B} \quad Nec : \frac{A}{\Box_\xi A}$$

Определим $LTK_{r_{ax}} := \{A \in Fma(\mathcal{L}^{LTK}) | \vdash_{AS_{LTK_r}} A\}$.

Доказаны следующие результаты:
Теорема 1. *$LTK_{r_{ax}}$ непротиворечиво и $LTK_{r_{ax}} = LTK_r$.*
Следствие 1. *Логика LTK_r является конечно аксиоматизируемой.*

Работа выполнена при поддержке проекта "‘Алгебро-логические структуры и комплексный анализ с приложениями к передаче и защите информации"’, выполняемому в рамках "‘Задание Минобрнауки РФ"’.

Список литературы

[1] ukyanchuk A., Decidability of multi-modal logic LTK of linear time and knowledge. Journal of Siberian Federal University, 6(2): 220-226, 2013.

Сибирский федеральный университет, Красноярск
E-mail: a.lukyanchuk@inbox.ru, gemmeny@rambler.ru

Обратный метод Маслова и метод входной клаш-резолюции

А. В. Лялецкий

Очевидно, что в классической логике первого порядка установление невыполнимости любого множества обычных формул можно свести, при помощи скулемизации и последующего, после опускания кванторов, применения операции приведения к дизъюнктивной нормальной форме, к установлению невыполнимости множества S так называемых конъюнктивных дизъюнктов (к-дизъюнктов [**1**]), под которыми понимаются выражения вида $C_1 \vee \ldots \vee C_n$, где $C_1, \ldots, C_n$ — конъюнкты, т. е. конъюнкции атомарных формул или их отрицаний.

Для установления невыполнимости S предлагается использовать резолюционную трактовку обратного метода С. Ю. Маслова в формулировке из [**2**], имеющую вид специальной стратегии метода входной клаш-резолюции [**3**], обобщенной на случай к-дизъюнктов и обозначаемой здесь ОМ.

Правило **А** из [**2**] в резолюционных терминах позволяет по конечному S строить конечное множество исходных благоприятных дизъюнктов (в обычном смысле [**3**]), обладающих тем свойством, что каждый из них содержит хотя бы одну атомарную формулу вместе с ее отрицанием.

Правило **Б** из [**2**] трактуется как ограничение правила резолюционного типа IR из [**1**] на случай, когда в качестве ядерного к-дизъюнкта может выступать только вариант к-дизъюнкта из S, а в качестве сателлитных – только варианты уже порожденных (т. е. благоприятных) дизъюнктов, причем их число должно совпадать с числом конъюнктов в ядерном к-дизъюнкте, из-за чего в результате такого применения IR может быть выведен только (благоприятный) дизъюнкт.

ОМ-стратегия заключается в порождении всевозможных исходных благоприятных дизъюнктов вначале по правилу **А**, а затем только по правилу **Б**.

Теорема. *Конечное множество S к-дизъюнктов невыполнимо в классической логике первого порядка без равенства тогда и только тогда, когда посредством ОМ-стратегии из S выводим пустой дизъюнкт.*

Список литературы

[1] Лялецкий А. В. Об одном исчислении к-дизъюнктов. В кн.: Математические вопросы теории интеллектуальных машин, ИК АН УССР, Киев, 1975, 34–48.

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

[3] Robinson J. A. An overview of mechanical theorem proving, Lecture notes in operations research and mathematical systems, 28, 1970, 2–20.

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

Логика Хинтикки и реализуемость по Нельсону

С. П. Одинцов, И. Ю. Шевченко

Отправным пунктом для построения IF (independence friendly) логики являет ся теоретико-игровая семантика для классической логики первого порядка. Если в этой семантике допустить игры с неполной информацией, а в язык ввести соответствующие конструкции, то мы придем к семантическому заданию IF логики Хинтикки [**1**]. В начале десятой главы [**1**] Хинтикка отмечает: "One of the basic ideas of constructivists like Michael Dummett (1978,1993) is that meaning has to be mediated by teachable, learnable, and practicable human activities." Семантические игры как раз являются примерами деятельности такого рода, поэтому мы рассмотрим связь логики Хинтикки с одной из традиционных конструктивных семантик, реализуемостью по Нельсону [**2**].

Сначала мы рассмотрим ограниченный вариант логики реализуемости по Нельсону в языке без импликации и интуиционистского отрицания и проведем реконструкцию теоретико-игровой семантики Хинтикки (GTS) для логики первого порядка, определив особым образом выигрышные стратегии для верификатора и фальсификатора в играх Хинтикки как абстрактные теоретико-множественные объекты. Это позволит выделить эффективные стратегии среди всех стратегий. Далее будет показано, что эффективные стратегии верикатора (фальсификатора) — это в точности позитивные (негативные) реализации по Нельсону. Таким образом, ограниченная реализуемость по Нельсону — это в точности эффективная версия GTS для логики первого порядка. Введенная реконструкция понятия стратегии позволит распространить GTS на язык с импликацией (при этом импликация интерпретируется в терминах стратегий, а не игр). Эту семантику мы обозначим $GTS^{\rightarrow}$. И опять, можно доказать, что реализуемость по Нельсону — это в точности эффективная версия семантики $GTS^{\rightarrow}$. Наконец, отправляясь от полученной реконструкции GTS, мы определим аналогичную реконструкцию для IF логики, обогащенной импликацией, а ее эффективный вариант будет IF версией реализуемости по Нельсону. Это дает точный ответ на вопрос из 10-й главы [1]: как IF логика была бы определена конструктивистами?

Список литературы

[1] Hintikka J. The Principles of Matematics Revisited. Cambridge, Cambridge University Press, 1998.

[2] Nelson D. Constructible falsity. J. Symb. Log., V. 14, 1949, 16-26.

Институт математики СО РАН, Новосибирск; Новосибирский Государственный Университет, Новосибирск

E-mail: odintsov@math.nsc.ru, igorec-08@mail.ru

О свойствах α-пополнений одной системы трехзначной логики

А. Л. Шабунин

Понятия α-пополнения и α-полноты множества функций k-значной логики были введены М.М. Глуховым в [**1**]. Там же для $k \geq 7$ построены конечные α-полные системы функций. В [**2**] для $k \geq 5$ построены α-полные системы из двух бинарных операций с правым сокращением; для $k = 2$ доказано отсутствие конечных α-полных систем; для $k \geq 2$ установлено, что в P_k отсутствуют α-полные системы, состоящие из одной функции.

В [**3**] построены конечные α-полные системы для $k = 3, 4$. В [**4**] доказано, что при любом $k \geq 2$ множество функций $F \subseteq P_k$ α-замкнуто тогда и только тогда, когда F замкнуто.

В данной работе продолжается исследование системы F функций трехзначной логики, состоящей из всех одноместных функций и операции сложения по модулю 3, начатое в [**5**].

Пусть $F' = [F]_\alpha$, $F'' = [F']_\alpha$. Одноместными подфункциями функции $f(x, y)$ из P_3 называются функции $f^{(0)}(x) = f(x, 0)$, $f^{(1)}(x) = f(x, 1)$, $f^{(2)}(x) = f(x, 2)$.

Предложение 1. *Пусть $f(x, y) \in F'$. Тогда $f(x, y)$ удовлетворяет следующим условиям:*

1) если одна из подфункций $f^{(0)}(x)$, $f^{(1)}(x)$, $f^{(2)}(x)$ функции $f(x, y)$ является константой, то среди остальных подфункций этой функции нет подстановки;

2) если среди подфункций $f^{(0)}(x)$, $f^{(1)}(x)$, $f^{(2)}(x)$ функции $f(x, y)$ есть подстановки, то все они имеют одинаковую четность.

Предложение 2. *Бинарная операция с правым сокращением $f(x, y) \in F'$ тогда и только тогда, когда подфункции $f^{(0)}$, $f^{(1)}$ и $f^{(2)}$ функции f являются подстановками одной и той же четности.*

Предложение 3. $F'' = [[F]_\alpha]_\alpha = P_3$. *Другими словами, однократное α-пополнение системы F является α-полной системой.*

Список литературы

[1] Глухов М.М. Об α-замкнутых классах и α-полных системах функций k-значной логики. Дискретная математика. 1989. Т. 1, № 1. С. 16–21.

[2] Чернышов А.Л. Условия α-полноты систем функций многозначной логики. Дискретная математика. 1992. Т. 4, № 4. С. 117–130.

[3] Шабунин А.Л. Примеры α-полных систем k-значной логики при $k = 3, 4$. Дискретная математика. 2006. Т. 18, № 4. С. 45–55.

[4] Шабунин А.Л. Об α-суперпозиции функций k-значной логики. Сиб. матем. журнал. 2007. Т. 48, № 2. С. 441–457.

[5] Шабунин А.Л. Об α-полноте одной системы трехзначной логики. Тезисы докладов международной конф. “Мальцевские чтения”, Новосибирск, Институт математики СО РАН, 12-16 ноября 2012 г. – Новосибирск, 2012, С. 165.

Чувашский государственный университет, Чебоксары
E-mail: a.shabunin@gmail.com

Об одном вычислимо полном регулярном простом комбинаторном исчислении

Л. В. Шабунин

Простые комбинаторные исчисления изучались в [**2**]. Эти исчисления возникают естественным образом в теории комбинаторов [**3, 1**].

Простое комбинаторное исчисление C задается набором *базисных комбинаторов* $\mathbf{a}_1, \ldots, \mathbf{a}_r$ с определяющими их равенствами

$$\begin{cases} \mathbf{a}_1 x_1 \ldots x_{n_1} = X_1, \\ \qquad \ldots \\ \mathbf{a}_r x_1 \ldots x_{n_r} = X_r, \end{cases} \tag{1}$$

где X_i — терм над множеством переменных $\{x_1, \ldots, x_{n_i}\}$, $1 \leq i \leq r$. При записи термов внешние скобки опускаем и используем группировку скобок влево: запись $\mathbf{a}xyz$ служит сокращением для $(((\mathbf{a}x)y)z)$.

Исчисление C называется регулярным, если каждая переменная, входящая в левую часть одного из равенств (1), входит и в правую часть этого же равенства.

Исчисление C называется вычислимо полным, если существует последовательность попарно не эквивалентных (в этом исчислении) замкнутых термов

$$Z_0, Z_1, Z_2, \ldots$$

таких, что для любой частично рекурсивной функции f от k переменных $(k \geq 1)$ существует замкнутый терм F такой, что для всех целых неотрицательных чисел m_1, $\ldots$, m_k имеет место

$$C \vdash FZ_{m_1} \ldots Z_{m_k} = Z_{f(m_1,\ldots,m_k)}$$

всякий раз, когда определено $f(m_1, \ldots, m_k)$.

Если, в добавление, все Z_n имеют нормальную форму и терм $FZ_{m_1} \ldots Z_{m_k}$ не имеет нормальной формы, когда $f(m_1, \ldots, m_k)$ не определено, то исчисление C называется вычислимо полным в сильном смысле.

Пусть исчисление CI задается базисными комбинаторами **B**, **C**, **S**, **I** с определяющими равенствами

$$\mathbf{B}xyz = x(yz), \quad \mathbf{C}xyz = xzy, \quad \mathbf{S}xyz = xz(yz), \quad \mathbf{I}xy = xy,$$

где x, y, z — переменные. Исчисление CI регулярно, но не комбинаторно полно.

Теорема. *Исчисление CI вычислимо полно в сильном смысле.*

Список литературы

[1] Барендрегт Х. Лямбда-исчисление. Его синтаксис и семантика. — М.: Мир, 1985. — 606 с.
[2] Шабунин Л.В. Простые комбинаторные исчисления // Вестн. МГУ, матем., механ., 1973, N 6, С. 30–35.
[3] Curry H.B., Feys R. Combinatory logic. Vol. 1. — North-Holland, Amsterdam, 1958.

Чувашский государственный университет, Чебоксары
E-mail: lvsh@mail.ru

Применение недетерминированных монадических схем программ к исследованию свойств программных логик с неподвижными точками

Н. В. Шилов, А. Ю. Бернштейн, С. О. Шилова

Памяти Сергея Ильича Мардаева (6.04.1962-10.04.2013)

Сергей Ильич Мардаев уделял много внимания изучению неклассических логик с неподвижными точками (см. список работ в [**1**]). В нашей работе описан подход к доказательству разрешимости и аксиоматизируемости так называемого μ-исчислени (μC)[**5**], которое можно определить как полимодальный вариант логики **K** с неподвижными точками по пропозициональным переменным с позитивными вхождениями.

В первоначальной работе [**5**] было определено μ-исчисление и доказана его корректность. Первая полная и корректная синтаксическая аксиоматизация для μC была построена в работе [**7**], а полнота и корректность исходной аксиоматизации была доказана только в [**8**]. Разрешимость μC с экспоненциальной верхней оценкой сложности была доказана независимо в работе [**6**] (с использованием трансляции формул μC в недетерминированные схемы Янова [**2**] на основе разрешающего алгоритма для обобщенной тотальности таких схем из работ [**3**], и в работе [**4**] (методом сведения к проблеме непустоты автоматов на бесконечных деревьях). В настоящей работе метод доказательства разрешимости из [**6**] распространен для построения полной и корректной аксиоматизации μ-исчисления.

Работа выполнена в рамках проекта РФФИ №13-01-00645-а.

Список литературы

[1] Алаев П.Е., Богопольский О.В., Васильев А.В. и др. СЕРГЕЙ ИЛЬИЧ МАРДАЕВ. Сибирские электронные математические заметки, 2013, т.10, стр. А.30–А.34.

[2] Котов В.Е. Введение в теорию схем программ. Новосибирск: Наука, Сиб. отд-ние, 1978.

[3] Непомнящий В.А., Шилов Н.В. Недетерминированные схемы программ и их отношение к программным логикам. Кибернетика, 1988, №3, стр.12-18, 28.

[4] Emerson E.A. and Jutla C.J. The Complexity of Tree Automata and Logics of Programs. SIAM J. Comput., v. 29, 1999, p.132-158

[5] Kozen D. Results on the Propositional Mu-Calculus. Theoretical Computer Science, v.27, 1983, p.333-354.

[6] Snilov N.V. Program Schemata vs. Automata for Decidability of Program Logics. Theor. Comput. Sci., v.175, 1997, p.15-27.

[7] Walukiewicz I. A Complete Deductive System for the mu-Calculus. Proceedings of IEEE LICS'93, p.136-147.

[8] Walukiewicz I. Completeness of Kozen's axiomatisation of the propositional Mu-calculus. Information and Computation, v.157, 2000, p.142-182.

Институт систем информатики им. А.П. Ершова СО РАН, г. Новосибирск, Россия; Назарбаев Университет, г. Астана, Казахстан; Новосибирский Государственный Университет, г. Новосибирск, Россия

E-mail: shilov@iis.nsk.su, nikolay.shilov@nu.edu.kz, bahtoh@gmail.com, shilov61@inbox.ru

О числе полных по П.С. Новикову расширений логики Даммета в языке с дополнительной одноместной логической связкой

А. Д. Яшин

Рассматривается оценка снизу числа полных по П.С. Новикову расширений суперинтуиционистской логики Даммета LC, характеризуемой классом конечных цепей и аксиоматизируемой как

$$LC = Int + (A \to B) \vee (B \to A),$$

в языке с одноместной дополнительной связкой $\varphi(\cdot)$.

Связку φ интерпретируем на цепях как *иррефлексивную модальность*:

$$x \Vdash \varphi(A) :\Leftrightarrow \forall y > x(y \Vdash A).$$

При такой интерпретации общезначима *аксиома замены*

$$(A \leftrightarrow B) \to (\varphi(A) \leftrightarrow \varphi(B))$$

(её наличие является одним из условий в подходе П.С. Новикова к понятию *новой* логической связки в данной с.и. логике [**1, 2**]).

Рассматриваем шкалы порядковых типов $\omega + n$, где ω — порядковый тип множества натуральных чисел, и n — натуральное число. Пусть $\mathcal{L}_n$ — φ-логика шкалы $\omega + n$ (т.е. множество формул расширенного языка, общезначимых в этой шкале).

Теорема 1. *(а) Каждая из φ-логик $\mathcal{L}_n$ является консервативным расширением с.и. логики LC;*

(б) Каждая из φ-логик $\mathcal{L}_n$ определяет новую по П.С. Новикову неконстантную логическую связку в LC.

Теорема 2. *При $m \neq n$ φ-логики $\mathcal{L}_m$ и $\mathcal{L}_n$ несовместимы над LC, т.е. их объединение порождает неконсервативную над LC φ-логику.*

Семейство консервативных над LC φ-логик является индуктивным в смысле леммы Цорна, поэтому всякая такая φ-логика включена в некоторую максимальную консервативную ($\equiv$ полную по П.С.Новикову) φ-логику.

Следствие. *Семейство полных по П.С.Новикову расширений LC является, как минимум, счётным.*

Является ли это семейство континуальным — открытый вопрос.

Список литературы

[1] Сметанич Я.С. О полноте исчисления высказываний с дополнительной операцией от одной переменной, Тр. Моск. матем. об-ва, т. 9, (1960), 357–371.

[2] Сметанич Я.С. Об исчислениях высказываний с дополнительной операцией, Докл. АН СССР, т. 139, № 2 (1961), 309–312.

Московский городской психолого–педагогический университет, Москва
E-mail: yashin.alexandr@yandex.ru

A unification-based approach to automatic theorem proving for the extension of infinite-valued first-order Lukasiewicz logic

A. S. Gerasimov

Infinite-valued first-order Łukasiewicz logic Ł∀ is one of the most important many-valued logics that provide foundations for approximate reasoning [**1**]. The only known approach to automatic theorem proving for Ł∀ is [**2, 3**].

In [**2, 3**], the author defines the extension Ł∀q of Ł∀ and formulates the sequent calculus Ł∀qS for the extension. In short, a sequent is an axiom iff a corresponding system of linear inequalities with rational coefficients is infeasible. The proof search algorithm for Ł∀qS constructs a preproof in a bottom-up manner introducing metavariables instead of witnessing terms and checks from time to time whether the preproof is closable. The infinite search of witnessing terms is eliminated by means of minus-normalization. Let $\mathcal{A}$ denote the algorithm that checks whether a preproof is closable and is based on minus-normalization.

Striving for a more efficient algorithm that checks preproof closability, now we investigate the complexity of the problem PREPROOF CLOSABILITY (given a preproof, decide whether it is closable) and propose a straightforward unification-based algorithm $\mathcal{B}$ for the problem.

Theorem 1. *If the Ł∀q language contains at least 2 nonzero-place predicate symbols, then the problem PREPROOF CLOSABILITY is NP-complete.*

Given a preproof, the algorithm $\mathcal{B}$ generates all partitions of the set of all atomic formulas in (the so-called basic subsequents of) the leaf sequents of the preproof. For each partition the algorithm simultaneously unifies its subsets, and if a unifier is found, $\mathcal{B}$ tests whether it is correct (according to the eigenvariable condition on the quantifier inference rules) and all the systems of linear inequalities corresponding to the leaf sequents are infeasible. (The algorithm $\mathcal{B}$ is subject to further improvements.)

Proposition 1. *The running time of the algorithm $\mathcal{A}$ is $\Omega(n^m \cdot p)$, the running time of the algorithm $\mathcal{B}$ is $O((n/\ln n)^{2n-3} \cdot q)$, where n is the number of distinct atomic formulas in the leaf sequents of the preproof, m is the number of metavariables in the preproof (m may be $\geqslant 1000n$), p and q are polynomials in the length of the preproof.*

References

[1] Cintula P., Hájek P., and Noguera C., eds. Handbook of Mathematical Fuzzy Logic. College Publications, 2011.

[2] Gerasimov A. S. A sequent calculus-based predicate logic meant for modeling of continuous scales (in Russian). In: Proceedings of the Tenth national conference on artificial intelligence CAI-06, pp. 339–347, 2006.

[3] Gerasimov A. S. Design and implementation of a proof search algorithm for an extension of infinite-valued predicate Lukasiewicz logic (in Russian). PhD thesis, Saint Petersburg State University, 2007.

Saint Petersburg State University, Saint Petersburg
E-mail: alexander.s.gerasimov@ya.ru

Strong equivalence theorem for paraconsistent answer set semantics

Z. V. Makridin, S. P. Odintsov

In [**1**], it was proved that the logic $\mathbf{KC} = \mathbf{Int} + \{\neg\mathbf{p} \vee \neg\neg\mathbf{p}\}$ is the smallest superintuitionistic logic for which the strong equivalence theorem holds. The main goal of our work is to prove the analogue of De Jong and Hendriks theorem for the logic programs with two kinds of negation: the traditional for logic programming default negation ($\neg$) and the strong negation ($\sim$). Let us define the logic **NKC** as follows:

$$\mathbf{NKC} = \mathbf{N4}^{\perp} + \{\neg\mathbf{p} \vee \neg\neg\mathbf{p}\},$$

where $\mathbf{N4}^{\perp}$ denotes the paraconsistent Nelson's logic.

Suppose that Π is a program without $\neg$ and *Lit* is the set of literals, i.e. the set of all atoms and its strong negations. A set $S \subseteq Lit$ is called an *answer set* of Π if and only if for all $Y \subseteq S$ it is true that $Y \vDash \Pi \;\Leftrightarrow\; Y = S$.

The *Gelfond and Lifschitz reduct* (GL-*reduct* [**2**]) Π^S of a program Π wrt a set of literals $S \subseteq Lit$ is a program obtained from Π in two steps. First, we exclude from Π all rules containing subformula of the form $\neg L$ with $L \in S$. Second, from the rest of rules we delete all subformulas $\neg L$.

A set of literals S is an *answer set* of a program Π if S is an answer set of Π^S.

Two programs Π_1 and Π_2 are called *strongly equivalent* if for any program Π, the programs $\Pi_1 \cup \Pi$ and $\Pi_2 \cup \Pi$ have the same answer sets.

Theorem. *Let Π_1 and Π_2 are logic programs. Then Π_1 and Π_2 are strongly equivalent if and only if they are equivalent viewed as propositional theories in* **NKC**. *Moreover,* **NKC** *is a smallest extension of* $\mathbf{N4}^{\perp}$ *for which strong equivalence theorem holds.*

The work is supported by Russian Foundation of Basic Research, projects No. 12-01-00168-a and No. 11-07-00560-a.

References

[1] De Jong D., Hendriks L. Characterization of strongly equivalent logic programs in intermediate logics. Theory and Practice of Logic Programming, 2003, Vol.3, P.259—270.

[2] Lifschitz V. Introduction to Answer Set Programming. Manuscript, available at http://www.cs.utexas.edu/users/vl/papers/esslli.ps, 2004.

Novosibirsk State University, Novosibirsk; Sobolev Institute of Mathematics, Novosibirsk
E-mail: skrol_z@mail.ru, odintsov@math.nsc.ru

III. Секция «Теория вычислимости»

О Δ^0_α-размерности вычислимых структур

П. Е. Алаев

Пусть $\mathfrak{A}$ — вычислимая структура. Её *вычислимой размерностью* называется супремум множества натуральных чисел n т. ч. существуют вычислимые модели $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$, изоморфные $\mathfrak{A}$ и такие, что между $\mathfrak{A}_i$, $\mathfrak{A}_j$ нет вычислимого изоморфизма при $i \neq j$. Эта размерность находится в пределах от 1 до ω. Если она равна 1, структура $\mathfrak{A}$ называется *автоустойчивой*, или *вычислимо категоричной*.

Заменяя в этом определении вычислимые изоморфизмы на Δ^0_α-вычислимые, мы получим определение Δ^0_α-*размерности*: это супремум множества натуральных чисел n т.ч. существуют вычислимые модели $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$, изоморфные $\mathfrak{A}$ и такие, что между $\mathfrak{A}_i$, $\mathfrak{A}_j$ нет Δ^0_α-вычислимого изоморфизма при $i \neq j$. Если размерность равна 1, то $\mathfrak{A}$ называется Δ^0_α-*категоричной*.

В Теореме 1 указаны достаточные условия, при которых Δ^0_α-размерность вычислимой структуры равна ω. Соединяя её с теоремой Эша, мы получаем широкий класс вычислимых структур, для которых Δ^0_α-размерность равна либо 1, либо ω.

Пусть $\Rightarrow$ — бинарное отношение на множестве конечных наборов из $\mathfrak{A}$, α — счётный ординал. Определим отношение $\mathrm{Free}^{\Rightarrow}_\alpha(\bar{a}, \bar{c})$ на наборах из $\mathfrak{A}$ так:

$$\forall \beta < \alpha\, \forall \bar{a}_1 \exists \bar{a}'\, \exists \bar{a}'_1\, [\, |\bar{a}| = |\bar{a}'|,\ \bar{c}, \bar{a}, \bar{a}_1 \leqslant_\beta \bar{c}, \bar{a}', \bar{a}'_1, \text{ и } \bar{c}, \bar{a} \not\Rightarrow \bar{c}, \bar{a}'].$$

Если отношение $\Rightarrow$ фиксировано, то будем говорить, что набор $\bar{a}$ *α-свободен над $\bar{c}$*.

Если $\Rightarrow$ равно $\geqslant_\alpha$, это определение совпадает с приведённым в [1], §17.4. Там же можно найти определение α-дружественной структуры.

Теорема 1. *Пусть $\alpha \geqslant 1$ — вычислимый ординал, и $\mathfrak{A}$ — вычислимая α-дружественная структура. Предположим, что $\Rightarrow$ — отношение на конечных наборах из $\mathfrak{A}$, обладающее свойствами:*

a) *$\Rightarrow$ транзитивно, т.е. из $\bar{a} \Rightarrow \bar{b}$ и $\bar{b} \Rightarrow \bar{c}$ следует $\bar{a} \Rightarrow \bar{c}$;*

b) *если $g : \mathfrak{A} \to \mathfrak{A}$ — автоморфизм, то $\bar{a} \Rightarrow g(\bar{a})$ для любого $\bar{a}$ in $\mathfrak{A}$.*

Если отношение $\not\Rightarrow$ вычислимо перечислимо, и для каждого $\bar{c}$ из $\mathfrak{A}$ можно эффективно найти $\bar{a}$ т.ч. $\mathrm{Free}^{\Rightarrow}_\alpha(\bar{a}, \bar{c})$, то существует вычислимая последовательность $\{\mathfrak{B}_i\}_{i\in\omega}$ вычислимых представлений $\mathfrak{A}$ т.ч. между $\mathfrak{B}_i$ и $\mathfrak{B}_j$ нет Δ^0_α-вычислимого изоморфизма при $i \neq j$.

Список литературы

[1] Ash C. J., Knight J. F. Computable structures and the hyperarithmetical hierarchy. Elsevier, 2000.

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

Структуры непрерывных и дифференцируемых функций

В. С. Амстиславский

Пусть X – совершенно нормальное пространство (определение можно найти, например, в [**3**]). Через $C(X)$ обозначим множество непрерывных функций из X в $\mathbb{R}$; через $O(X)$ – множество всех открытых подмножеств топологического пространства X. Через $\leq$ – поточечный порядок для непрерывных функций. Отношение $<$ определим для пары непрерывных функций $f, g \in C(X)$ следующим образом: $f < g \Leftrightarrow f(x) < g(x)$ *для всех* $x \in X$. При введенных обозначениях справедливо следующее утверждение.

Теорема 1. *Теории структур* $\mathfrak{A}_X \rightleftharpoons (C(X), \leq, <)$ *и* $\mathfrak{B}_X \rightleftharpoons (O(X), \subseteq, \emptyset)$ *–* m*-эквивалентны.*

Если для некоторого пространства X из класса совершенно нормальных пространств известно, что теория $\mathfrak{B}_X$ разрешима, то по теореме 1 получаем разрешимость теории $\mathfrak{A}_X$. Например, можно доказать, что теории $\mathfrak{B}_{\mathfrak{R}^n} \rightleftharpoons (O(\mathbb{R}^n), \subseteq, \emptyset)$ для $n \geq 1$ являются разрешимыми, значит разрешимы и теории $(C(\mathbb{R}^n), \leq, <)$.

Рассмотрим также теорию структуры $\mathfrak{C} \rightleftharpoons (C^1(\mathbb{R}), \leq)$, где $C^1(\mathbb{R})$ – множество непрерывно-дифференцируемых функций из $\mathbb{R}$ в $\mathbb{R}$; $\leq$ – поточечный порядок.

Теорема 2. *Теория структуры* $\mathfrak{C}$ *– разрешима.*

Эти теоремы удалось доказать, используя обобщенный метод интерпретаций, предложенный О. В. Кудиновым (изложение метода приведено в [**1**]). Ранее, этим методом доказана $m-$сводимость теории $\mathfrak{A} \rightleftharpoons (C(\mathbb{R}), \leq)$ к разрешимой теории структуры $\mathfrak{B} \rightleftharpoons (O(\mathbb{R}), \subseteq, \emptyset)$. В теореме 1 этот результат переносится на случай совершенно нормального пространства и классическим методом доказывается обратная $m-$сводимость. При доказательстве теоремы 2 проверяются условия обобщенного метода интерпретации, и, тем самым, $m-$сводимость теории структуры $\mathfrak{C}$ к разрешимой теории второго порядка структуры $\mathfrak{D}$ разностей открытых подмножеств $\mathbb{R}$. Идея и метод доказательства разрешимости теории $\mathfrak{B}$ кратко изложены в [**2**]. Более подробное доказательство этого результата, а также доказательство разрешимости теорий $\mathfrak{B}_{\mathbb{R}^n}$ можно найти в [**1**]. Аналогичным образом доказывается разрешимость теории $\mathfrak{D}$. Новые примеры применения обобщенного метода интерпретаций позволяют считать его хорошим инструментом доказательства разрешимости теорий.

Список литературы

[1] Амстиславский В. С. Элементарные теории пространств непрерывных функций // Вестник НГУ. Серия: математика, механика, информатика. 2012. Т. 12, № 3. С. 22–34.

[2] Рабин М. О. Разрешимые теории // Справочная книга по математической логике. Часть III / Ред. Дж. Барвайс. М.: Наука, 1982. С. 77–111.

[3] Энгелькинг Р. Общая топология. М.: Мир, 1986.

Институт математики им. С. Л. Соболева СО РАН, Новосибирск
E-mail: amvladislav@yandex.ru

Булевы алгебры с выделенными эндоморфизмами и порождающие деревья

Н. А. Баженов

Конструктивизируемость моделей различных естественных классов изучалась в работах А. И. Мальцева, Ю. Л. Ершова, С. С. Гончарова, Н. Г. Хисамиева, В. П. Добрицы и многих других авторов. С. С. Гончаров [**1**] доказал, что суператомная булева алгебра является конструктивизируемой в том и только том случае, когда ее ранг Фреше равен вычислимому ординалу. Н. Т. Когабаев [**2**] получил описание вычислимых булевых алгебр с конечным числом выделенных идеалов в терминах порождающих деревьев и идеальных подмножеств деревьев. В [**3**] получен критерий конструктивизируемости булевой алгебры $\mathfrak{B}(\omega)$ с выделенным автоморфизмом.

Данная работа посвящена исследованию конструктивизируемости E-алгебр, т. е. булевых алгебр с конечным числом выделенных эндоморфизмов. Получено описание вычислимых E-алгебр в терминах порождающих деревьев и отображений, заданных на деревьях. Полученная характеризация применяется для доказательства следующих результатов.

Теорема 1. *Для любого конечного $n \geqslant 1$ существует вычислимая E-алгебра с выделенным множеством атомов, имеющая вычислимую размерность n.*

Теорема 2. *Существует E-алгебра с выделенным множеством атомов, спектр степеней которой состоит в точности из всех ненулевых тьюринговых степеней.*

Работа выполнена при финансовой поддержке Совета по грантам Президента РФ для государственной поддержки ведущих научных школ (проект НШ-276.2012.1), ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (Соглашение № 8227), и РФФИ (проект 11-01-00236).

Список литературы

[1] Гончаров С. С. Конструктивизируемость суператомных булевых алгебр. Алгебра и логика. 1973. Т. 12, № 1. С. 31–40.

[2] Когабаев Н. Т. Универсальная нумерация конструктивных I-алгебр. Алгебра и логика. 2001. Т. 40, № 5. С. 561–579.

[3] Баженов Н. А., Тухбатуллина Р. Р. Конструктивизируемость булевой алгебры $\mathfrak{B}(\omega)$ с выделенным автоморфизмом. Алгебра и логика. 2012. Т. 51, № 5. С. 579–607.

Институт математики им. С. Л. Соболева СО РАН, Новосибирск
E-mail: nickbazh@yandex.ru

О Σ_2^0-начальных сегментах вычислимых линейных порядков

Р. И. Бикмухаметов

Одно из направлений исследований вычислимых линейных порядков сосредоточено на изучении алгоритмической сложности начальных сегментов. М. Роу [**1**] показал, что Π_1^0-начальный сегмент вычислимого линейного порядка имеет вычислимое представление. С другой стороны, им был построен пример вычислимого линейного порядка с Π_3^0-начальным сегментом, не имеющим вычислимой копии. Р. Коулз, Р. Доуни и Б. Хусаинов [**2**] показали, что существует вычислимый линейный порядок с Π_2^0 -начальным сегментом, не изоморфным никакому вычислимому линейному порядку. К. Амбос - Шпис, С. Б. Купер, С. Лемпп [**3**] в совместной работе показали, что Σ_2^0-начальный сегмент любого вычислимого линейного порядка имеет вычислимую копию. Мы покажем, что любой вычислимый порядок, не имеющий наибольшего элемента, является Σ_2^0-начальным сегментом, наперед заданной Σ_2^0-степени, некоторого вычислимого линейного порядка.

Теорема. *Для любого вычислимого линейного порядка $\mathcal{L} = \langle L, <_L \rangle$ без наибольшего элемента и любого множества $M \in \Sigma_2^0$, существует такой вычислимый линейный порядок $\tilde{\mathcal{L}} = \mathcal{A} + \eta$, что $\mathcal{A} \cong \mathcal{L}$ и $\mathcal{A} \equiv_T M$.*

Список литературы

[1] Raw M. J. S. Complexity of automorphisms of recursive linear orders. Ph. D. Thesis. University of Wisconsin-Madison, 1995.

[2] Coles R. J., Downey R., Khoussainov B. On Initial Segments of Computable Linear Orders // Order. 1997. V. 14, No. 2. P. 107–124.

[3] Ambos-Spies K., Cooper S. B., Lempp S. Initial Segments of Recursive Linear Orders // Order. 1997. V. 14, No. 2. P. 101–105.

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

Вычислимые нумерации в аналитической иерархии

М. В. Доржиева

Изучаются минимальные нумерации аналитической иерархии. Главным образом, нас интересует однозначная нумерация всего класса. Как оказалось, в арифметической иерархии и иерархии Ершова однозначная нумерация для максимального класса есть, но неожиданный результат получен для аналитической иерархии: однозначная нумерация для любого уровня Π^1_n отсутствует.

Теорема 1. *У семейства S Π^1_n-множеств есть универсальная нумерация.*

Теорема 2. *Пусть S — бесконечное семейство Π^1_n-множеств, ν — Π^1_n-нумерация семейства S, M — максимальное множество, $A \in S$. Нумерация*

$$\nu^A_M(m) = \begin{cases} \nu(i), \text{если } m = m_i; \\ A, \text{иначе.} \end{cases} \tag{1}$$

будет минимальной.

Теорема 3. *Не существует Π^1_n-вычислимой последовательности $\nu(n)$ такой, что каждое Π^1_n-множество* A *в этой последовательности встречается только один раз.*

Список литературы

[1] Owings J. C., Jr., The meta-r. e. sets, but not the Π^1_1 sets, can be enumerated without repetition // The Journal of Symbolic Logic. 1970. V. 35, No. 2. P. 223–229.

[2] Роджерс Х. Теория рекурсивных функций и эффективная вычислимость. М.: Мир, 1972.

Новосибирский государственный университет, Новосибирск
E-mail: dm-3004@inbox.ru

Условное и безусловное моделирование формулами длинных вычислений

И. В. Латкин

Автор приносит извинения редакции и читателям журнала «Алгебра и логика» за допущенную им серьёзную ошибку при доказательстве основной теоремы в [**2**]. Теперь она исправлена и более того, теорема может быть слегка усилена:

Теорема 1. *Пусть $m(n)$ — функция, и $m(n) \geqslant n$ для каждого $n \in \omega$; $\boldsymbol{B_0}$ — двухэлементная булева алгебра. По любой программе детерминированной P машины Тьюринга и всякому входу X на ленте машины, можно эффективно построить $\forall\exists$-предложение $\Omega(X,P)$, обладающее свойствами: а) его код строится за время $g(m(|X|)+|cP|)$ для некоторого многочлена g, фиксированного для всех $m(n), X$ и P; б) $\boldsymbol{B_0} \models \Omega(X,P)$ равносильно тому, что машина с программой P допускает X менее, чем за $\exp(2, m(|X|))$ шагов; в) имеется константа $D > 0$, независящая от P и $m(n)$ (но зависящая от кодировки формул и программ), что при всех достаточно длинных X верно $m(|X|) \leqslant |c\,\Omega(X,P)| \leqslant D|cP| \cdot (m(|X|))^{2+\varepsilon}$, для всякого наперёд заданного $\varepsilon > 0$.*

Исследуется возможность усиления теоремы 1 на недетерминированный случай. Любопытно, что возможность подобного моделирования по сути давно известна. Например, опираясь на известную теорему Кука, несложно выводится

Теорема 2 (об условном моделировании). *Для каждого языка L класса $\boldsymbol{\mathcal{NP}}$ существует алгоритм, который по любому входу машины w строит $\exists$-формулу $C(L,w)$ со свойствами: а) код формулы строится за время $g_L(|w|)$ для некоторого многочлена g_L, фиксированного для всех w; б) $\boldsymbol{B_0} \models C(L,w)$ равносильно тому, что любая детерминированная машина P допускает w менее чем за $F(|w|)$ шагов, при условии, что эта машина распознаёт язык L за время $F(|w|)$, и при этом не имеет значения, насколько огромна функция F.*

Более того, для некоторых проблем теории сложности, такое моделирование — это по существу единственный способ их решения. Это показывает следующее утверждение, получающееся применением теоремы 7.10 из [**1**].

Теорема 3. *Пусть $\boldsymbol{\mathcal{EXP}}$ — класс языков, распознаваемых за экспоненциальное время, $\boldsymbol{\mathcal{P}}$-space — класс языков, распознаваемых с полиномиальной памятью. Эти классы совпадают в том и только том случае, когда для всякого многочлена $m(n)$ имеется алгоритм, который по всякому входу X на ленте машины Тьюринга и любой программе P машины строит предложение $\Omega_m(X,P)$ со свойствами а) и б) из теоремы 1, но многочлен g_m может зависеть от m.*

Список литературы

[1] Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.

[2] Латкин И. В. О сложности распознавания теорий и их вычислительной выразительности // Алгебра и логика. 2012. Т. 51, № 2. С. 216–238.

Восточно-Казахстанский гос. тех. университет, г. Усть-Каменогорск (Казахстан)
E-mail: lativan@yandex.ru

Совершенная локальная вычислимость суператомных булевых алгебр

Д. А. Луппов

В работе рассматривается новый подход к обобщению понятия конструктивизации, основанный на понятии совершенной локальной вычислимости структур, введенном Расселом Миллером и Дастином Мулкахей в [**1**]. Алгебраическая система S теории T называется совершенно локально вычислимой если для нее существуют: равномерно вычислимый класс $\mathfrak{A}$ конечно порожденных моделей теории T, изоморфных всем конечно порожденным подструктурам из S, множества I инъективных гомоморфизмов для любых двух моделей из $\mathfrak{A}$, множество M вложений элементов из $\mathfrak{A}$ в S; и для $\mathfrak{A}$, I и M выполняется ряд свойств описанный в [**1**].

Особенности данного подхода рассматриваются здесь на примере класса суператомных булевых алгебр в том числе и несчетных. В работе получен критерий того что суператомная булева алгебра является совершенно локально вычислимой.

Теорема. *Суператомная булева алгебра совершенно локально вычислима тогда и только тогда, когда ее ранг является вычислимым ординалом.*

В некотором смысле эта теорема является обобщением критерия существования вычислимого представления для счетных суператомных булевых алгебр из [**2**]: счетная суператомная булева алгебра обладает вычислимым представлением тогда и только тогда, когда ее ранг является вычислимым ординалом.

Список литературы

[1] Miller R., Mulcahey D. Perfect Local Computability and Computable Simulations // Fourth Conference on Computability in Europe (CiE 2008), Lecture Notes in Computer Science 5028. Berlin: Springer-Verlag, 2008. P. 388–397.

[2] Гончаров С. С. Конструктивизируемость суператомных булевых алгебр // Алгебра логика. 1973. Т. 12, № 1. С. 31–40.

Институт математики им. С. Л. Соболева СО РАН, Новосибирск
E-mail: dima2703@yandex.ru

Новое доказательство теоремы нормализации для бестипового экстенсионального λ-исчисления

А. А. ЛЯЛЕЦКИЙ

Рассматривается бестиповый вариант λ-исчисления. Через $f_{\beta\eta}^{left}$ обозначим одношаговую стратегию $\beta\eta$-левой редукции, которая в каждом λ-терме t сворачивает самое левое вхождение $\beta\eta$-редекса в t, если таковое имеется; аналогично, через f_{β}^{left} будем обозначать стратегию β-левой редукции. В 1980 г. Я. Клопом был получен следующий известный результат.

Теорема нормализации для $\beta\eta$-редукции**.** *Стратегия $f_{\beta\eta}^{left}$ – нормализующая.*

Первоначальное доказательство Я.Клопа громоздкое и технически очень сложное. Изучая вводимое ниже свойство абстрактности для произвольного понятия редукции, можно построить другое, более короткое и прозрачное доказательство.

Через S_X обозначим полную симметрическую группу множества X, где X – совокупность всех переменных языка λ-термов. По индукции продолжим каждую перестановку $\pi \in S_X$ до перестановки множества Λ всех λ-термов:

$$(t_0 t_1)^\pi = t_0^\pi t_1^\pi; \qquad (\lambda x.t)^\pi = \lambda x^\pi.t^\pi.$$

Отношение R произвольной арности на множестве Λ называется *абстрактным*, если R выдерживает применение любой перестановки $\pi \in S_X$. Поскольку любое понятие редукции и любая стратегия являются бинарными отношениями на Λ, то можно говорить об абстрактных понятиях редукции и стратегиях. Например, абстрактными являются понятия β- и η-редукций, а также стратегии f_{β}^{left} и $f_{\beta\eta}^{left}$.

Лемма. *Пусть даны абстрактное понятие R редукции и абстрактная нормализующая R-стратегия f. Для каждого натурального числа s существует такое натуральное число $m = m(f,s)$, что $f^m(t)$ находится в R-н.ф., если только λ-терм t имеет R-н.ф. и размер t равен s.*

Схема нового доказательства теоремы нормализации для $\beta\eta$-редукции:

1. Предполагаем противное. Тогда существует такой λ-терм t, имеющий $\beta\eta$-н.ф., но $f_{\beta\eta}^{left}$-редукционная цепочка σ которого не ведет к $\beta\eta$-н.ф. Так как $\eta \models SN$, цепочка σ содержит бесконечное число сворачиваемых β-редексов.

2. По теореме о $\beta\eta$-нормальной форме, терм t имеет какую-то β-н.ф. Стратегия f_{β}^{left} является абстрактной и, по теореме нормализации для β-редукции, нормализующей. Поэтому мы *придем к противоречию с леммой*, если сможем перестроить какой-то начальный отрезок σ в $\beta\eta$-редукционную цепочку, которая начинается термом t и в которой, для какого-то $n > m(f_{\beta}^{left}, s)$, где s равно размеру t, первые n сворачиваемых редексов являются β-редексами.

3. С помощью техники откладывания η-редукции начальный отрезок цепочки σ, оканчивающийся сворачиванием $(m(f_{\beta}^{left}, s)+1)$-го β-редекса в σ (существующий в силу п.1), перестраиваем в $\beta\eta$-редукционную цепочку с указанными в п.2 свойствами.

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

О вычислимых подгруппах $UT_n(Q)$

М. К. Нуризинов, Р. К. Тюлюбергенев, Н. Г. Хисамиев

Пусть $UT_n(Q)$ – группа всех унитреугольных матриц размерностей $n \times n$ над полем рациональных чисел Q, $n \in \omega$, ω – множество всех натуральных чисел, γ_n – ее некоторая геделева нумерация, т. е. по данному числу $m \in \omega$ эффективно находится матрица $\gamma_n m$ и, наоборот, по данной матрице – ее γ_n-номер.

В данной работе получены критерии вычислимости нильпотентных групп без кручения конечных размерностей. Как следствие получено существование главной вычислимой нумерации класса всех вычислимых нильпотентных групп без кручения конечных размерностей. Построен пример группы $G \le UT_3(Q)$, которая невычислима, но секции любого ее центрального ряда вычислимы.

Пусть дана абелева группа A без кручения и ее базис $a_0, ..., a_{n-1}$. Характеристикой $\chi(A)$ группы A назовем множество целых чисел

$$\chi(A) = < m, s_0, ..., s_{n-1} >| \ \exists a \in A(a_0^{s_0} \cdot \ldots \cdot a_{n-1}^{s_{n-1}} = a^m)$$

Пусть даны группы G, $H \lhd G$ и G/H – абелева группа, $\bar{g}_0, \ldots, \bar{g}_{n-1}$ – базис фактор-группы G/H. Тогда для любой последовательности $æ =< m, s_0, \ldots, s_{n-1} >\in \chi(G/H)$ существуют элементы $h_æ \in H$ и $g_æ \in G$ такие, что $g_0^{s_0} \cdot \ldots \cdot g_{n-1}^{s_{n-1}} h_æ = g_æ$.

Если для каждой $æ \in \chi(G/H)$ каким-то способом сопоставлен однозначно определенный элемент $h_æ$, то будем говорить, что определена функция выбора $ch : \chi(G/H) \to H$.

Теорема 1. *Пусть подгруппа $G \le UT_n(Q)$ вычислима, ν – некоторая ее вычислимая нумерация и $1 = G_0 < G_1 < \ldots < G_{k-1} = G$ – ее некоторый центральный ряд, секции которого не имеют кручения. Тогда каждая погруппа G_i вычислима перечислима в $(UT_n(Q), \gamma_n)$ и $\nu \le_m \gamma_n$, где γ_n – геделева нумерация группы $UT_n(Q)$*

Следствие 1. *Нильпотентная группа без кручения конечной размерности вычислима тогда и только тогда, когда она изоморфна вычислимо перечислимой подгруппе $(UT_n(Q), \gamma_n)$ при некотором n*

Следствие 2. *Существует главная вычислимая нумерация семейства всех вычислимых нильпотентных групп без кручения конечных размерностей.*

Теорема 2. *Пусть G – подгруппа $(UT_n(Q), \gamma_n)$, $1 = G_0 < G_1 < \ldots < G_{k-1} = G$ – ее центральный ряд, секции которого без кручения, и $\bar{g}_{i0}, \ldots, \bar{g}_{in_i-1}$ – базис группы $\overline{G}_i = G_i/G_{i-1}$. Тогда G вычислима если и только если справедливы: 1. Для любого $i < k$ характеристика $\chi(\bar{G}_i)$ секции $\bar{G}_i$ – вычислимо перечислимое множество; 2. Существует частично вычислимая функция выбора.*

Теорема 3. *Существует невычислимая подгруппа $G \le UT_3(Q)$ такая, что все секции любого ее центрального ряда вычислимы.*

Отсюда следует, условие 2 теоремы 2 не зависит от условия 1.

Восточно-Казахстанский государственный университет им. Д. Серикбаева, г. Усть-Каменогорск
E-mail: marat.nurizinov@gmail.com

Об изоморфных полурешетках Роджерса в иерархии Ершова

С. С. Оспичев

Одним из основных направлений исследований в теории нумераций является изучение полурешеток Роджерса в различных иерархиях множеств [**1**]. Цель данной работы – построение семейства Σ_a^{-1}-множеств $\mathcal{S}$ с полурешеткой Роджерса $\mathcal{R}_a^{-1}(\mathcal{S})$ [**2**], изоморфной некоторым уже изученным объектам.

Построены примеры конечных семейств вычислимо-перечислимых множеств, полурешетка Роджерса которых, изоморфна полурешетке m-степеней Σ_a^{-1}-множеств. Также доказана

Теорема. *Пусть $\mathcal{S}$ – Σ_a^{-1}-вычислимое семейство, и $|\mathcal{S}| = k$. Для любого $n \in \omega \cup \{\omega\}$, $n \geqslant k$ найдется Σ_a^{-1}-вычислимое семейство $\mathcal{T}$, такое что $|\mathcal{T}| = n$, а $\mathcal{R}_a^{-1}(\mathcal{T})$ изоморфна $\mathcal{R}_a^{-1}(\mathcal{S})$.*

Работа выполнена при финансовой поддержке Совета по грантам Президента РФ для государственной поддержки ведущих научных школ (проект НШ-276.2012.1) и при поддержке ФЦП "Научные и научно-педагогические кадры инновационной России" на 2009-2013 годы (Соглашение № 8227).

Список литературы

[1] Goncharov S. S., Badaev S. Theory of numberings, open problems // Contemporary Mathematics. V 257. P. 23–38.

[2] Арсланов М. М. Иерархия Ершова. Казань: Казанский государственный университет, 2007.

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

Generic complexity and compression

Alexander N. Rybalov

Let G be a finitely generated group (semigroup) and $g \in G$. Denote by $sl(g)$ the set of all straight line programs computing element g. For $S \subseteq G$ denote

$$sl(S) = \bigcup_{g \in S} sl(g).$$

We are interested in developing of generic computability over set of all straight line programs over G. By the size of a straight line program we mean the number of variables (assignments) in the program.

Denote by P_n the set of straigh line programs of size n and by $sl(g)_n$ the set of programs of size n computing n.

Theorem 1. *If $S \subseteq G$ is undecidable set, then $sl(S) \subseteq sl(G)$ is strongly undecidable set.*

Theorem 2. *If for $S \subseteq G$ the set $sl(S)$ is strongly generically decidable in polynomial time then S is decidable by a probabilistic polynomial algorithm.*

OB IM SB RAS, Omsk
E-mail: alexander.rybalov@gmail.com

Definability in the local theories of the ω-enumeration and the ω-Turing degree structures

A. C. Sariev, H. Ganchev

The structure $\mathcal{D}_\omega$ of the ω-enumeration degrees is introduced by Soskov in [**3**]. In this talk first we shall investigate the definability in the local structure of $\mathcal{D}_\omega$, continuing the studying which was started in the work of Ganchev and Soskova [**1**]. Namely, we shall show the first order definability of the class $\mathbf{H} = \bigcup \mathbf{H}_n$ of the ω-enumeration degrees below the first jump of the least element which are high$_n$ for some n and of the class $\mathbf{L} = \bigcup \mathbf{L}_n$ of the ω-enumeration degrees below the first jump of the least element which are low$_n$ for some n. Then we have the definition of the class $\mathbf{I}$ of the intermediate degrees.

The second structure we investigate, the one of the ω-Turing degrees $\mathcal{D}_{\omega,T}$, was raised as an analogue of $\mathcal{D}_\omega$ over the Turing reducibility, [**2**]. We shall show connections between definability of the first jump of the least element and its minimal low splittings.

The authors were partially supported by BNSF grant No. DMU 03-07/12.12.2011.

References

[1] Ganchev H., Soskova M. I. The high/low hierarchy in the local structure of the ω-enumeration degrees // Annals of Pure and Applied Logic. 2012. V. 163, No. 5. P. 547–566.

[2] Sariev A. C., Ganchev H. The ω-Turing degrees. To appear in Annals of Pure and Applied Logic.

[3] Soskov I. N. The ω-enumeration degrees. To appear in Journal of Logic and Computation.

Sofia University, Sofia (Bulgaria)
E-mail: andreys@fmi.uni-sofia.bg, ganchev@fmi.uni-sofia.bg

IV. Секция «Теория групп»

Об одном свойстве подгрупп фраттиниева типа

Л. П. Авдашкова, С. Ф. Каморников, О. Л. Шеметкова

Рассматриваются только конечные группы, используются определения и обозначения, принятые в [**1, 2**]. Напомним только, что если θ — подгрупповой m-функтор, то $\Phi_\theta(G)$ — это пересечение всех максимальных подгрупп из $\theta(G)$ (если таких подгрупп нет, то полагают, что $\theta(G) = G$).

Хорошо известно (см., например, [**1**]), что если N — нормальная подгруппа конечной группы G, то подгруппа Фраттини $\Phi(N)$ подгруппы N содержится в подгруппе Фраттини $\Phi(G)$ группы G. В связи с этим результатом Л.А. Шеметковым была предложена задача нахождения других подгрупп фраттиниева типа, обладающих описанным свойством. Один из вариантов этой задачи зафиксирован в [**2**] как вопрос 4.4.10:

Для каких регулярных подгрупповых m-функторов θ выполняется включение $\Phi_\theta(N) \subseteq \Phi_\theta(G)$ для каждой конечной группы G и любой ее нормальной подгруппы N?

Простые примеры показывают, что существуют подгрупповые m-функторы θ, для которых θ-подгруппа Фраттини не обладает отмеченным свойством вложения. В частности, это имеет место для подгруппового m-функтора θ, который сопоставляет каждой группе саму группу и множество всех ее ненормальных максимальных подгрупп.

Определение. *Подгрупповой m-функтор θ называется нормально вложенным, если для любой группы G и каждой ее нормальной подгруппы N всегда из $M \in \theta(G)$ и $M \cap N \neq N$ следует, что найдется максимальная подгруппа $H \in \theta(N)$, отличная от N, для которой выполняется условие $M \cap N \subseteq H$.*

В работе устанавливается связь нормально вложенных подгрупповых m-функторов с m-функторами, удовлетворяющими условиям отмеченного вопроса 4.4.10, и строятся серии регулярных и нерегулярных подгрупповых m-функторов θ, для которых θ-подгруппа Фраттини обладает свойством $\Phi_\theta(N) \subseteq \Phi_\theta(G)$.

Список литературы

[1] Doerk K., Hawkes T. Finite soluble groups. Berlin – New-York: Walter de Gruyter, 1992.

[2] Каморников С. Ф., Селькин М. В. Подгрупповые функторы и классы конечных групп. Мн., 2003.

Белорусский торгово-экономический университет потребительской кооперации, Гомель, Гомельский филиал Международного университета «МИТСО», Российский экономический университет им. Г. В. Плеханова

E-mail: avdashkova@mail.ru, sfkamornikov@mail.ru, ol-shem@mail.ru

О почти аппроксимируемости конечными p-группами некоторых классов групп

Д. Н. Азаров

Пусть $\mathcal{K}$ — некоторый класс групп. Группа G называется $\mathcal{K}$-аппроксимируемой, если для любого ее неединичного элемента a существует гомоморфизм группы G на группу из класса $\mathcal{K}$, при котором образ элемента a отличен от 1. Группа G называется почти $\mathcal{K}$-аппроксимируемой, если она содержит $\mathcal{K}$–аппроксимируемую подгруппу конечного индекса. Обозначим через $\mathcal{F}$ и $\mathcal{F}_p$ класс всех конечных групп и класс всех конечных p-групп. А. И. Мальцев доказал $\mathcal{F}$-аппроксимируемость конечно порожденных линейных групп. Следствием этого результата является теорема Гирша о $\mathcal{F}$-аппроксимируемости полициклических групп. Д. М. Смирнов и Г. Баумслаг доказали, что группа автоморфизмов конечно порожденной $\mathcal{F}$-аппроксимируемой группы сама является $\mathcal{F}$-аппроксимируемой.

Перечисленные результаты и большинство других известных результатов о $\mathcal{F}$-аппроксимируемости не могут быть распространены на $\mathcal{F}_p$-аппроксимируемость. С другой стороны, любая полициклическая группа почти $\mathcal{F}_p$-аппроксимируема для каждого простого p. Этот, ставший уже классическим, результат был доказан А. Л. Шмелькиным. В дальнейшем он обобщался в различных направлениях. Так В. П. Платонов доказал, что конечно порожденная линейная группа над полем нулевой характеристики почти $\mathcal{F}_p$-аппроксимируема для всех достаточно больших простых p. Нами доказано, что *группа автоморфизмов конечно порожденной линейной группы над полем нулевой характеристики почти $\mathcal{F}_p$-аппроксимируема для всех достаточно больших простых p.* Для группы автоморфизмов конечно порожденной свободной группы это свойство недавно доказано Л. Паризом.

Рассмотрим теперь обобщения теоремы А. Л. Шмелькина на разрешимые группы конечного ранга. Напомним, что группа G имеет конечный ранг, если существует число r такое, что любая конечно порожденная подгруппа группы G порождается не более чем r элементами. Д. Робинсон доказал, что разрешимая группа конечного ранга $\mathcal{F}$-аппроксимируема тогда и только тогда, когда она редуцирована. Он же доказал, что редуцированная разрешимая минимаксная группа почти $\mathcal{F}_p$-аппроксимируема для всех достаточно больших прстых p. Мы обобщаем этот результат и результат А. Л. Шмелькина следующим образом: *разрешимая группа конечного ранга является почти $\mathcal{F}_p$-аппроксимируемой тогда и только тогда, когда ее периодический радикал конечен и она не содержит подгрупп, изоморфных группе p-ичных дробей.* Лубоцкий и Манн доказали, что $\mathcal{F}$-аппроксимируемая группа конечного ранга почти локально разрешима. В связи с этим напомним один опубликованный результат автора: *если группа конечного ранга $\mathcal{F}_p$-аппроксимируема для всех простых p, то она нильпотентна.* Ранее такая теорема была доказана Сексенбаевым для полициклических групп.

ИвГУ, Иваново
E-mail: azarovdn@mail.ru

Полугруппа эндоморфизмов свободной периодической группы

В. С. Атабекян

Д.Дайер и Э.Форманек доказали, что если F свободная группа конечного ранга $m > 1$, то ее группа автоморфизмов $Aut(F)$ совершенна, т.е. центр группы $Aut(F)$ тривиален и каждый автоморфизм группы $Aut(F)$ – внутренний. В дальнейшем разные усиления и обобщения этого результата получили Д.Храмцов, В.Толстых, М.Бридсон и К.Вогтман. Позднее Э.Форманек показал, что каждый автоморфизм полугруппы $End(F)$ задается сопряжением некоторым элементом из $Aut(F)$ (see [**1**]). Заметим, что вопрос об описании группы $Aut(End(F))$ для относительно свободных групп был поставлен Б.Плоткиным (see [**1**], [**2**]).

Мы получили полное описание группы $Aut(End(B(m, n)))$ для свободных бернсайдовых групп $B(m, n)$ нечетного периода $n \geq 1003$.

Теорема. *Если $S : End(B(m, n)) \to End(B(m, n))$ некоторый автоморфизм полугруппы $End(B(m, n))$, то существует $\alpha \in Aut(B(m, n))$ такая, что $S(\beta) = \alpha \circ \beta \circ \alpha^{-1}$ для всех $\beta \in End(B(m, n))$, где $n \geq 1003$ – произвольное нечетное число и $m > 1$.*

Список литературы

[1] Formanek E., A question of B. Plotkin about the semigroup of endomorphisms of a free group, Proc. Amer. Math. Soc. 130:935–937, 2002.

[2] Mashevitzky G., Plotkin B., On Automorphisms of the endomorphisms of a free universal algebras, Int. J. Algebra Comput., 17(5/6): 1085–1106, 2007.

Факультет математики и механики, Ереванский гос.университет, Ереван
E-mail: varujan@atabekyan.com

О бесконечной дистрибутивности в решетке многообразий m-групп

Н. В. Баянова, А. В. Зенков

Напомним, 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 $\langle G, \vee, \wedge\rangle$. 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.

Основным результатом является пример, показывающий, что в решетке M не всегда выполнено равенство $\mathcal{V}(\bigvee\limits_i \mathcal{U}_i) = \bigvee\limits_i(\mathcal{V}\mathcal{U}_i)$ для бесконечного множества индексов и это дает отрицательный ответ на вопрос М. Жираде и Й. Рахунека из [**1**]. При построении примера мы использовали идеи и конструкции Н.Я. Медведева из [**2**] и [**3**].

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.

[2] Медведев Н.Я.О бесконечной дистрибутивности в решетке многообразий ℓ-групп//Сибирский матем.журнал.1989.Т.30.№ 2.С.216-220.

[3] Медведев Н.Я.О решетке o-аппроксимируемых многообразий ℓ-групп//Czech.Math.J.1984.V.34.№ 2.P.6-17.

Алтайский государственный аграрный университет, Барнаул, Россия
E-mail: alexey_zenkov@yahoo.com

Доминионы абелевых подгрупп в классе метабелевых групп

А. И. Будкин

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

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

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

Несложно заметить, что $\mathrm{dom}_A^{\mathcal{M}}(-)$ является оператором замыкания на решетке подгрупп данной группы A, 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.

Группа H называется 1- замкнутой в классе $\mathcal{M}$, если для каждой группы A=гр(a, H) из $\mathcal{M}$, порожденной по модулю H одним элементом, имеем: $\mathrm{dom}_A^{\mathcal{M}}(H) = H$.

Группа H называется абсолютно замкнутой в классе $\mathcal{M}$, если для любой группы A из $\mathcal{M}$ из каждого включения $H \leq A$ следует, что $\mathrm{dom}_A^{\mathcal{M}}(H) = H$.

Направление исследований, представленное в данной работе, связано с нахождением всех групп H, замкнутых в любой метабелевой группе, содержащей H в качестве подгруппы.

Теорема 1. *Неединичная абелева группа без кручения не является абсолютно замкнутой в классе метабелевых групп.*

Теорема 2. *Пусть G — метабелева группа, $H = (h)$ — циклическая p-группа и нормальное замыкание H^G подгруппы H в группе G совпадает с коммутантом G' группы G. Предположим, что H^G разлагается в прямое произведение некоторых своих подгрупп вида H^f $(f \in G)$. Тогда доминион H в G (в классе метабелевых групп) равен H.*

Теорема 3. *Циклическая группа простого порядка является 1-замкнутой в классе метабелевых групп.*

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

О представлениях m-групп

С. В. Вараксин

Напомним, что *m-группой* называется алгебраическая система G сигнатуры $m = \langle \cdot, e, ^{-1}, \vee, \wedge, \varphi \rangle$, где $\langle G, \cdot, e, ^{-1}, \vee, \wedge \rangle$ является ℓ-группой и одноместная операция φ есть автоморфизм второго порядка группы $\langle G, \cdot, e, ^{-1} \rangle$ и антиизоморфизм решетки $\langle G, \vee, \wedge \rangle$, т.е. для любых $x, y \in G$ верны соотношения $\varphi(xy) = \varphi(x)\varphi(y), \varphi(\varphi(x)) = x, \varphi(x \vee y) = \varphi(x) \wedge \varphi(y), \varphi(x \wedge y) = \varphi(x) \vee \varphi(y)$. Будем записывать m-группу G с фиксированным автоморфизмом φ как пару (G, φ). Пусть F_m – свободная m-группа многообразия m-групп $\mathfrak{V}_m$ с порождающими $x_1, \ldots, x_r$, F_0 – свободная группа квазимногообразия $\mathfrak{Q}_g$ групп, вложимых в m-группы из $\mathfrak{V}_m$ с порождающими $s_1^0, \ldots, s_r^0, s_1^1, \ldots, s_r^1$. Пусть P^γ – правый порядок на F_0, F_0^γ – правоупорядоченная группа F_0 с правым порядком P^γ, V_0^γ – выпуклая подгруппа в F_0^γ, линейно упорядоченное множество $X_0 = R_{F_0^\gamma}(V_0^\gamma)$ с индуцированным порядком, $X_1 = \overleftarrow{R}_{F_0^\gamma}(V_0^\gamma)$ с противоположным порядком. Определим действие $\mathcal{R}$ порождающих группы F_0^γ на X_0:

$$\mathcal{R}(s_i^0)(V_0^\gamma g) = V_0^\gamma g s_i^0 \quad \text{и} \quad \mathcal{R}(s_i^1)(V_0^\gamma g) = V_0^\gamma g s_i^1$$

и на X_1:

$$\mathcal{R}(s_i^0)(V_0^\gamma g) = V_0^\gamma g s_i^1 \quad \text{и} \quad \mathcal{R}(s_i^1)(V_0^\gamma g) = V_0^\gamma g s_i^0,$$

и антиавтоморфизм $a_0 : X_0 \rightleftarrows X_1$, действующий на $R_{F_0^\gamma}(V_0^\gamma)$ тождественно. Этот антиавтоморфизм индуцирует реверсивный автоморфизм φ_0 на $A_0^\gamma = Aut(X_0) \times Aut(X_1)$ по правилу $\varphi_0(g_0; g_1) = (g_1; g_0)$, превращая ℓ-группу A_0^γ в m-группу. Обозначим через r_i^0 и r_i^1 элементы m-группы $(A_0^\gamma; \varphi_0) : r_i^0(x_0; x_1) = (\mathcal{R}(s_i^0)(x_0); \mathcal{R}(s_i^0)(x_1))$ и $r_i^1(x_0; x_1) = (\mathcal{R}(s_i^1)(x_0); \mathcal{R}(s_i^1)(x_1))$. При этом $\varphi_0(r_i^\delta) = r_i^{1-\delta}$. Обозначим m-подгруппу в $(A_0^\gamma; \varphi_0)$, порожденную $\{r_i^\delta\}_{i,\delta}$, через $(R_0^\gamma; \varphi_0)$. Рассмотрим только те m-группы $(R_0^\gamma; \varphi_0)$, которые лежат в $\mathfrak{V}_m$, обозначим через R^* их прямое произведение, $R^* = \overline{\prod\limits_{R_0^\gamma \in \mathfrak{V}_m}} R_0^\gamma$. Пусть $\psi : F_m \to R^*$ – m-гомоморфизм, продолжающий отображение $\psi_0(x_i)|_{R_0^\gamma} = r_i^0$, а $F^* = \psi(F_m) \leq R^*$ – его гомоморфный образ.

Теорема. Отображение $\psi : F_m \to F^*$ является m-изоморфизмом m-групп F_m и F^*.

Список литературы

[1] Giraudet M.,Lukas F. Groupes á motié ordonnés// Fundam.Math.1991.139,№2.P.75-89.

[2] Курош А.Г. Теория групп.М.:Наука,1967.

[3] Kopytov V.M., Medvedev N.Ya. The theory of lattice-ordered groups.Dordrecht;Boston;London: Kluwer Academic Publishers, 1994.

[4] Вараксин С.В., Зенков А.В. О представлениях m-групп.// Сиб.матем.журнал, 2013, Т.54. № 2. С.298-302.

АлтГУ, Барнаул
E-mail: varaksins@yandex.ru

О конечных группах с обобщенно субнормальными критическими подгруппами

В. Ф. Велесницкий, В. Н. Семенчук

В работе [**1**] Семенчуком В.Н. было начато изучение строения конечных групп, у которых группы Шмидта субнормальны. Дальнейшее исследование было продолжено Княгиной В.Н., Монаховым В.С. [**2**]. Полное описание таких групп было получено Ведерниковым В.А. [**3**]. В теории классов конечных групп естественным обобщением понятия субнормальности является понятие $\mathfrak{F}$-достижимости. При изучении строения конечных групп, у которых любая минимальная не $\mathfrak{F}$-подгруппа $\mathfrak{F}$-достижима ($\mathfrak{F}$ — насыщенная наследственная формация с решеточным свойством), были получены следующие результаты.

Теорема 1. *Пусть $\mathfrak{F}$ — насыщенная наследственная формация с решеточным свойством, $\pi(\mathfrak{F})$ — множество всех простых чисел и любая минимальная не $\mathfrak{F}$-группа разрешима. Если в группе G все подгруппы Шмидта $\mathfrak{F}$-достижимы, то $G/G_{\mathfrak{F}}$ абелева.*

Следствие 1.1. *Пусть $\mathfrak{F}$ — формация всех p-разложимых групп. Если в группе G все подгруппы Шмидта $\mathfrak{F}$-достижимы, то $G/G_{\mathfrak{F}}$ абелева.*

Теорема 2. *Пусть $\mathfrak{H}$ — насыщенная наследственная формация, содержащая $\mathfrak{N}$, $\mathfrak{F}$ — насыщенная наследственная формация с решеточным свойством, причем $\mathfrak{F} \subseteq \mathfrak{H}$. Если все минимальные не $\mathfrak{H}$-подгруппы группы G разрешимы и $\mathfrak{F}$-достижимы в G, то $G/F(G) \in \mathfrak{H}$.*

Следствие 2.1. *Пусть $\mathfrak{F}$ — насыщенная наследственная формация с решеточным свойством и $\pi(\mathfrak{F})$ — множество всех простых чисел. Если в группе G все подгруппы Шмидта $\mathfrak{F}$-достижимы, то $G/F(G) \in \mathfrak{F}$.*

Следствие 2.2. *Если в группе G все минимальные не $\mathfrak{F}$-подгруппы $\mathfrak{F}$-достижимы ($\mathfrak{F}$ — класс всех p-разложимых групп), то $G/F(G)$ — p-разложима.*

Следствие 2.3. *Пусть $\mathfrak{F}$ — насыщенная наследственная формация с решеточным свойством. Если все минимальные не $\mathfrak{F}$-подгруппы группы G разрешимы и $\mathfrak{F}$-достижимы в G, то $G \in \mathfrak{N}\mathfrak{F}$.*

Список литературы

[1] Семенчук В.Н. Конечные группы с системой минимальных не $\mathfrak{F}$-подгрупп / В.Н. Семенчук // Подгрупповое строение конечных групп. – Минск: Наука и техника. – 1981. – С. 138–149.

[2] Княгина В.Н. О конечных группах с некоторыми субнормальными подгруппами Шмидта / В.Н. Княгина, В.С. Монахов // Сибирский матем. журн. – 2004. – Т. 45, № 6. – С. 1316–1322.

[3] Ведерников В.А. Конечные группы с субнормальными подгруппами Шмидта / В.А. Ведерников // Алгебра и логика. – 2007. – Т. 46, № 6. – С. 669–687.

УО "Гомельский государственный университет имени Ф. Скорины", Гомель
E-mail: velogos@rambler.ru

Неприводимые системы колец и полей расщепления локальных групп без кручения

С. В. Вершина, В. Х. Фарукшин

Рассматриваются сильно неразложимые p-локальные группы без кручения конечного ранга, полями расщепления которых являются конечные алгебраические расширения поля рациональных чисел.

Определение 1. *Назовем кольцо R p-ранга 1 кольцом расщепления для p-локальной неразложимой группы A без кручения p-ранга $\geqslant 2$, если $A \otimes R \cong A_1 \oplus R^k$, где R^k — прямая сумма аддитивной группы кольца R и $k \geqslant 1$. Поле частных $\mathbb{Q}(R)$ кольца расщепления R назовем полем расщепления группы A.*

Теорема 1. *Всякая редуцированная сильно неразложимая p-локальная группа без кручения p-ранга $\geqslant 2$ обладает кольцом расщепления, полем расщепления.*

Определение 2. *Систему колец расщепления $R_1, \ldots, R_n$ для группы A назовем неприводимой системой колец расщепления для A, если n является минимальным числом, для которого имеет место сервантное вложение группы A в прямую сумму $R_1 \oplus \ldots \oplus R_n$, их поля частных $K_1 = \mathbb{Q}(R_1), \ldots, K_n = \mathbb{Q}(R_n)$ назовем неприводимой системой полей расщепления группы A.*

Теорема 2. *Всякая редуцированная сильно неразложимая p-локальная группа без кручения конечного ранга и p-ранга $\geqslant 2$ имеет неприводимую систему колец расщепления.*

Определение 3.[**1**] *Кольцо R p-ранга 1 назовем универсальным кольцом расщепления для группы A, если $A \otimes R \cong D \oplus F$, где D — делимый R-модуль, F — свободный R-модуль, а его поле частных $K = \mathbb{Q}(R)$ назовем универсальным полем расщепления группы A.*

Теорема 3. *Если $R_1, \ldots, R_k$ — неприводимая система колец расщепления для сильно неразложимой p-локальной группы без кручения A конечного ранга и p-ранга $\geqslant 2$, то существует такое натуральное число n, что универсальное кольцо расщепления $R \cong \circledast^n (R_1 \circledast \ldots \circledast R_k)$, где $\circledast$ — редуцированное тензорное произведение аддитивных групп колец.*

Теорема 4. *Если подполя $K_1, \ldots K_n$ поля p-адических чисел образуют неприводимую систему полей расщепления группы A, то их композит является универсальным полем расщепления для группы A.*

Работа выполнена при поддержке ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 годы. Государственный контракт №14.B37.21.0363.

Список литературы

[1] Lady E. L., Splitting fields for torsion-free modules over discrete valuation rings. I, J.Algebra, 49, 261–275 (1977).

Московский Педагогический Государственный Университет, Москва
E-mail: svetlanavershina@gmail.com, fvkh@mail.ru

О реализуемости заданного графа как графа простых чисел подходящей конечной группы

А. Л. Гаврилюк, А. С. Кондратьев, Н. В. Маслова, И. В. Храмцов

Пусть G — конечная группа. Обозначим через $\omega(G)$ *спектр* группы G, т.е. множество порядков всех ее элементов, а через $\pi(G)$ — множество всех простых делителей числа $|G|$. Множество $\omega(G)$ определяет *граф простых чисел* (или *граф Грюнберга—Кегеля*) $\Gamma(G)$ группы G, в котором множество вершин есть $\pi(G)$, и две различные вершины p и q смежны тогда и только тогда, когда число pq принадлежит $\omega(G)$.

Граф простых чисел конечной группы G можно понимать как некоторый абстрактный обыкновенный граф на $|\pi(G)|$ вершинах, все вершины которого помечены различными простыми числами из $\pi(G)$ так, что две вершины, помеченные простыми числами p и q, смежны тогда и только тогда, когда $pq \in \omega(G)$. В связи с таким пониманием графа простых чисел возникает следующая

Проблема. Пусть Γ — обыкновенный граф с конечным числом вершин. Можно ли пометить вершины графа Γ различными простыми числами так, что полученный помеченный граф будет графом простых чисел подходящей конечной группы?

Ранее в [**1**] было показано, что данная проблема решается положительно для всех графов с количеством вершин не более, чем 4, и для некоторых графов на 5 вершинах. В настоящей работе данная проблема исследуется для графов с 5 вершинами. Доказана следующая

Теорема. *Пусть Γ — обыкновенный граф с 5 вершинами. Тогда*
(1) *если Γ является кокликой, то проблема решается отрицательно*;
(2) *если Γ не является кокликой, то проблема решается положительно.*

Работа выполнена при финансовой поддержке РФФИ (проект 13-01-00469), РФФИ-ГФЕН Китая (проект 12-01-91155), программы Отделения математических наук РАН (проект 12-Т-1-1003), программ совместных исследований УрО РАН с СО РАН (проект 12-С-1-1018) и с НАН Беларуси (проект 12-С-1-1009), совета по грантам Президента РФ (проект МК-3395.2012.1) и гранта ИММ УрО РАН для молодых ученых за 2013 г.

Список литературы

[1] Гаврилюк А. Л., Маслова Н. В., Храмцов И. В. О реализуемости заданного графа как графа Грюнберга-Кегеля некоторой группы// Теория групп и ее приложения: Тез. Международной школы-конференции, посвященной 90-летию со дня рождения З.И. Боревича. Владикавказ: изд-во СОГУ, 2012. С. 38-40.

Институт математики и механики им. Н.Н.Красовского УрО РАН, Екатеринбург
E-mail: alexander.gavriliouk@gmail.com, a.s.kondratiev@imm.uran.ru, butterson@mail.ru, ihramtsov@gmail.com

Об аппроксимируемости корневыми классами групп некоторых свободных конструкций

Д. В. Гольцов, Д. Н. Азаров

Пусть $\mathcal{K}$ — непустой класс групп. Группа G называется $\mathcal{K}$-аппроксимируемой, если для любого неединичного элемента a группы G существует гомоморфизм группы G на некоторую группу из класса $\mathcal{K}$, при котором образ элемента a отличен от 1. Группа G называется почти $\mathcal{K}$-аппроксимируемой, если она содержит некоторую $\mathcal{K}$-аппроксимируемую подгруппу конечного индекса. Класс $\mathcal{K}$ называется корневым, если он замкнут относительно подгрупп и для любой субнормальной последовательности $C \leq B \leq A$ из того, что факторы A/B и B/C принадлежат классу $\mathcal{K}$, следует, что в группе A существует нормальная подгруппа D такая, что $D \subseteq C$ и A/D принадлежит классу $\mathcal{K}$. Примером корневого класса может служить класс $\mathcal{F}$ всех конечных групп и класс $\mathcal{F}_p$ всех конечных p-групп.

В. Магнус, А. Каррас и Д. Солитэр в своей книге "Комбинаторная теория групп" приводят следующий результат К. Грюнберга: для того, чтобы любое свободное произведение групп, аппроксимируемых данным корневым классом $\mathcal{K}$, само было $\mathcal{K}$-аппроксимируемой группой необходимо и достаточно, чтобы любая свободная группа была $\mathcal{K}$-аппроксимируемой. Д. Н. Азаров доказал, что любая свободная группа аппроксимируема любым корневым классом. Поэтому результат Грюнберга принимает следующий вид.

Теорема 1. *Свободное произведение любого семейства групп, аппроксимируемых корневым классом $\mathcal{K}$, само является $\mathcal{K}$-аппроксимируемой группой.*

Г Баумслаг доказал, что свободное произведение двух $\mathcal{F}$-аппроксимируемых групп с конечными объединенными подгруппами является $\mathcal{F}$-аппроксимируемой группой. Аналогичный результат справедлив и для HNN-расширений. Однако эти результаты не могут быть обобщены на аппроксимируемость произвольным корневым классом. Тем не менее, нами доказаны следующие теоремы.

Теорема 2. *Пусть $P = (A * B, H = K)$ — свободное произведение групп A и B с конечными объединёнными подгруппами H и K. Если группы A и B $\mathcal{F}$-аппроксимируемы и почти аппроксимируемы корневым классом $\mathcal{K}$, то и группа P почти $\mathcal{K}$-аппроксимируема. В частности, если группы A и B почти аппроксимируемы корневым классом $\mathcal{K}$, состоящим из конечных групп, то группа P почти $\mathcal{K}$-аппроксимируема.*

Теорема 3. *Пусть $C^* = (C, t, t^{-1}Ht = K)$ — HNN-расширение группы C с конечными связанными подгруппами H и K. Если группа C $\mathcal{F}$-аппроксимируема и почти аппроксимируема корневым классом $\mathcal{K}$, то и группа C^* почти $\mathcal{K}$-аппроксимируема. В частности, если группа C почти аппроксимируемы корневым классом $\mathcal{K}$, состоящим из конечных групп, то группа C^* почти $\mathcal{K}$-аппроксимируема.*

ИвГУ, Иваново
E-mail: goltsov_89@mail.ru, azarovdn@mail.ru

Об оценках числа автотопий n-арных квазигрупп порядка 4

Е. В. Горкунов, Д. С. Кротов, В. Н. Потапов

Рассмотрим множество Σ^n всех упорядоченных наборов длины n, образованных элементами множества $\Sigma = \{0, 1, 2, 3\}$. Алгебраическая система (Σ, f), в которой n-арная операция $f\colon \Sigma^n \to \Sigma$ обратима по каждой переменной, называется *n-арной квазигруппой порядка* 4. Также n-арной квазигруппой называется и сама операция f.

Квазигруппы f и g называются *изотопными*, если найдется набор перестановок $\bar\theta = (\theta_1, \dots, \theta_n, \theta_{n+1})$ из симметрической группы S_4, действующей на Σ, такой, что на Σ^n имеет место тождество

$$f(x_1, \dots, x_n) \equiv g\theta_{n+1}^{-1}(x_1\theta_1, \dots, x_n\theta_n). \tag{1}$$

Автотопией квазигруппы f называется любая изотопия $\bar\theta \in S_4^{n+1}$, для которой (1) имеет место при $g = f$. Группу автотопий f обозначим через $\mathrm{Atp}(f)$.

Пусть Σ и бинарная операция $*\colon \Sigma^2 \to \Sigma$ образуют группу, изоморфную $\mathbb{Z}_2^2$. Квазигруппа f *линейна*, если она изотопна квазигруппе $\ell(\bar x) = x_1 * \ldots * x_n$. Если для некоторых $a, b \in \Sigma$ множество $S_{a,b}(f) = \{\bar x \in \Sigma^n \mid f(\bar x) \in \{a, b\}\}$ содержит подмножество, изотопное булеву кубу, то f называется *полулинейной*.

Теорема 1. *Группа автотопий линейной n-арной квазигруппы порядка* 4 *изоморфна полупрямому произведению $S_3 \leftthreetimes \left(\mathbb{Z}_2^2\right)^n$.*

Линейная структура существенно влияет на симметрию квазигруппы.

Лемма. *Если n-арная квазигруппа f нелинейна, то $|\mathrm{Atp}(f)| \leqslant 2 \cdot 4^n$.*

Таким образом, справедлива

Теорема 2. *В множестве n-арных квазигрупп порядка* 4 *только линейные имеют группы автотопий максимального порядка, равного $6 \cdot 4^n$.*

С другой стороны, любая квазигруппа порядка 4 в определенной степени регулярна, поскольку, согласно результатам [**1**], она либо полулинейна, либо представляется в виде суперпозиции квазигрупп меньшей арности. Этой регулярности оказывается достаточно, чтобы группа автотопий квазигруппы отличалась от тривиальной.

Теорема 3. *Для произвольной n-арной квазигруппы f порядка* 4 *имеет место неравенство $|\mathrm{Atp}(f)| \geqslant 2^{[n/2]+2}$, причем эта оценка точна.*

Настоящая работа выполнена при поддержке Российского фонда фундаментальных исследований (грант № 13-01-00463а).

Список литературы

[1] Krotov D. S., Potapov V. N. n-Ary quasigroups of order 4 // SIAM J. Discrete Math. — 2009. — V. 23, № 2. — P. 561–570.

Институт математики им. С. Л. Соболева, Новосибирск
Новосибирский государственный университет
E-mail: gorkunov@math.nsc.ru, krotov@math.nsc.ru, vpotapov@math.nsc.ru

О линейных группах с ограничениями на систему собственных подгрупп

О. Ю. Дашкова

Группа G всех автоморфизмов векторного пространства A над полем F называется полной линейной группой и обозначается $GL(F, A)$. Подгруппы группы $GL(F, A)$ называются линейными группами. Конечномерные линейные группы играют важную роль в различных областях математики и изучались достаточно много. В случае, когда размерность векторного пространства A над полем F бесконечна, подгруппы группы $GL(F, A)$ исследовались значительно меньше, и, как правило, при дополнительных ограничениях на рассматриваемые группы.

В [**1**] авторы ввели в рассмотрение понятие центральной размерности линейной группы. Если H — подгруппа группы $GL(F, A)$, то H действует на фактор–пространстве $A/C_A(H)$ естественным образом. Размерность фактор–пространства $A/C_A(H)$ называется центральной размерностью группы H [**1**].

Естественно возникает вопрос об исследовании бесконечномерных линейных групп, у которых система подгрупп бесконечной центральной размерности "достаточно мала". В [**1**] изучались почти локально разрешимые линейные группы бесконечной центральной размерности, у которых каждая собственная подгруппа имеет конечную центральную размерность. Как оказалось, в этом случае бесконечномерная линейная группа изоморфна квазициклической q–группе C_{q^∞} для некоторого простого числа q. В [**1**] авторами построен пример бесконечномерной линейной группы над бесконечным полем простой характеристики p, удовлетворяющей указанным условиям и изоморфной $C_{q^\infty}, q \neq p$.

Основным результатом работы является следующая теорема.

Теорема. *Пусть $G \leq GL(F, A)$, $G \neq G'$, F — конечное поле. Если каждая собственная подгруппа группы G имеет конечную центральную размерность, и $|G| \neq q^k$, где q — простое число, то G имеет конечную центральную размерность.*

Следствие. *Пусть $G \leq GL(F, A)$, $G \neq G'$, F — конечное поле простой характеристики p. Если каждая собственная подгруппа группы G имеет конечную центральную размерность, и $|G| \neq q^k$, где q — простое число, то группа G содержит элементарную абелеву p–подгруппу H, такую, что факторгруппа G/H изоморфна некоторой подгруппе $GL_n(F)$.*

Литература

[1] Dixon M. R., Evans M. J., Kurdachenko L. A., Linear groups with the minimal condition on subgroups of infinite central dimension // J. Algebra. – 2004. — V. 277. – № 1. – P. 172–186.

Днепропетровский национальный университет, Днепропетровск
E-mail: odashkova@yandex.ru

О пересечениях нильпотентных подгрупп в конечных группах с цоколем $L(2,q)$

В. И. Зенков

Пусть G — конечная группа, A и B — подгруппы из G и пусть $M = \{A\cap B^g | g \in G$ и подгруппа $A\cap B^g$ минимальна по включению среди всех подгрупп такого вида$\}$, а $m \subseteq M$ и m состоит из тех элементов в M, порядок которых минимален. По определению $\mathrm{Min}_G(A,B) = \langle M\rangle$, а $\mathrm{min}_G(A,B) = \langle m\rangle$ и, таким образом, $\mathrm{Min}_G(A,B) \geq \mathrm{min}_G(A,B)$. Заметим, что если в группе G для любого элемента q справедливо неравенство $A\cap B^g \neq 1$, то это эквивалентно тому, что $\mathrm{Min}_G(A,B) \neq 1$, что, в свою очередь, эквивалентно тому, что $\mathrm{min}_G(A,B) \neq 1$.

В работе [**1**] доказано, что $\mathrm{Min}_G(A,B) \leq F(G)$ для любой пары абелевых подгрупп A и B из G, а в работе [**2**] доказано, что в простой неабелевой группе G подгруппа $\mathrm{Min}_G(A,B) = 1$ для любой пары примарных подгрупп A и B. Нами доказана следующая

Теорема. *Пусть G — конечная почти простая группа с цоколем, изоморфным $L(2,q)$, $q > 3$, A и B — нильпотентные подгруппы из G. Тогда следующие условия эквивалентны:*

(1) *$Min_G(A,B) \neq 1$;* (2) $G = \mathrm{Aut}(K)$, *где либо*

(2a) $K \simeq L(2,q)$, $q = 2^n - 1 > 3$ — *простое число Мерсенна и* $(A,B) = (S,S)$, *где* $S \in Syl_2(G)$, *либо*

(2b) $K \simeq L(2,9)$ *и* $(A,B) \in \{(\mathrm{min}_G(S,S),S),(S,\mathrm{min}_G(S,S)),(S,S) \big| S \in Syl_2(G)$, $\mathrm{min}_G(S,S) \simeq D_{16}$ *и* $\mathrm{min}_G(S,S) = \langle i,j\rangle$, $i^2 = j^2 = 1$, $i,j \in G\backslash G'$ *и* $|C_S(i)| = |C_S(j)| = 8\}$.

Заметим, что при $n = 2$ в пункте (2a) теоремы подгруппа $K \simeq L(2,5)$ имеет четверную силовскую 2-подгруппу V с $N_K(V) \simeq A_4$ и $|K : N_K(V)| = 5$. Для силовской 5-подгруппы из K имеем $N_K(T) \simeq Z_5\lambda Z_2$ — группа Фробениуса. Следовательно, подгруппа $M = N_K(T)$ нетривиально пересекается с каждой силовской 2-подгруппой из G. Этот пример дает отрицательный ответ на вопрос 16.29 из “Коуровской тетради” [**3**].

Работа выполнена при поддержке РФФИ (проект 13-01-00476), Программы Отделения математических наук РАН (проект 12-Т-1-1003), Программы совместных исследований УрО РАН с СО РАН (проект 12-С-1-1018) и с НАН Беларуси.

Список литературы

[1] Зенков В.И. Пересечения абелевых подгрупп в конечных группах // Мат. заметки. 1994. № 56. С. 869–871.

[2] Мазуров В.Д., Зенков В.И. О пересечении силовских подгрупп в конечных группах // Алгебра и логика. 1996. Т. 35, № 4. С. 424–432.

[3] Коуровская тетрадь. Нерешенные задачи теории групп. Изд. 17-е. Новосибирск: ИМ СО РАН. 2010.

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

О пересечениях примарных подгрупп нечетного порядка в почти простых группах

В. И. Зенков, Я. Н. Нужин

Пусть G — конечная группа, A и B — подгруппы из G и пусть $M = \{A \cap B^g | g \in G$ и подгруппа $A \cap B^g$ минимальна по включению среди всех подгрупп такого вида$\}$, а $m \subseteq M$ и m состоит из тех элементов в M, порядок которых минимален. По определению $\mathrm{Min}_G(A,B) = \langle M \rangle$, а $\mathrm{min}_G(A,B) = \langle m \rangle$ и, таким образом, $\mathrm{Min}_G(A,B) \geq \mathrm{min}_G(A,B)$. Заметим, что если в группе G для любого элемента q справедливо неравенство $A \cap B^g \neq 1$, то это эквивалентно тому, что $\mathrm{Min}_G(A,B) \neq 1$, что, в свою очередь, эквивалентно тому, что $\mathrm{min}_G(A,B) \neq 1$.

В работе [**1**] доказано, что $\mathrm{Min}_G(A,B) \leq F(G)$ для любой пары абелевых подгрупп A и B из G, а в работе [**2**] доказано, что в простой неабелевой группе G подгруппа $\mathrm{Min}_G(A,B) = 1$ для любой пары примарных подгрупп A и B. В следующей теореме используются введенные обозначения.

Теорема. *Пусть G — конечная неразрешимая почти простая группа, A и B — примарные подгруппы нечетного порядка из G. Тогда следующие условия эквивалентны:*

(1) *$Min_G(A,B) \neq 1$;*

(2) *$F^*(G) = E(G) \simeq \Omega_8^+(3)$, $G/E(G) \simeq Z_3$ или S_3 и $(A,B) \in \{(S,S),(S,S_0),(S_0,S),(S_0,S_0)\}$, где $S \in Syl_3(N_G(P))$, а $S_0 = O_3(N_G(P))$ и P — параболическая подгруппа из $E(G)$, соответствующая центральной вершине в диаграмме Дынкина для $\Omega_8^+(3)$ и $S_0 = \mathrm{min}_G(S,S)$.*

Работа первого автора выполнена при поддержке Программы Отделения математических наук РАН (проект 12-Т-1-1003), Программы совместных исследований УрО РАН с СО РАН (проект 12-С-1-1018) и с НАН Беларуси, РФФИ (проект 13-01-00476).

Список литературы

[1] Зенков В.И. Пересечения абелевых подгрупп в конечных группах // Мат. заметки. 1994. № 56. С. 869–871.

[2] Мазуров В.Д., Зенков В.И. О пересечении силовских подгрупп в конечных группах // Алгебра и логика. 1996. Т. 35, № 4. С. 424–432.

ИММ УрО РАН, Екатеринбург, СФГУ, Красноярск
E-mail: v1i9z52@mail.ru, nuzhin2008@rambler.ru

Факторизации конечных групп r-разрешимыми подгруппами с заданными вложениями

В. Н. Княгина, В. Н. Тютянов

Рассматриваются только конечные группы. В работе [**1**] было введено следующее определение. Пусть $\mathbb{N}$ и $\mathbb{P}$ — множества всех натуральных и всех простых чисел соответственно. Для фиксированного натурального числа t положим $\mathbb{P}^t = \{p^k \mid p \in \mathbb{P},\ k \in \{0\} \cup \mathbb{N}, k \leq t\}$. Подгруппа H называется $\mathbb{P}^t$-субнормальной подгруппой группы G, если существует цепочка подгрупп $H = H_0 \subseteq H_1 \subseteq \ldots \subseteq H_n = G$ такая, что $|H_i : H_{i-1}| \in \mathbb{P}^t$ для всех i. При $t = 1$ получается понятие $\mathbb{P}$-субнормальной подгруппы, введенное в [**2**].

Обозначим $\mathbb{P}^\infty = \{p^k \mid p \in \mathbb{P},\ k \in \{0\} \cup \mathbb{N}\}$. Подгруппа H называется $\mathbb{P}^\infty$-субнормальной подгруппой группы G, если существует цепь подгрупп $H = H_0 \subseteq H_1 \subseteq \ldots \subseteq H_n = G$ такая, что $|H_i : H_{i-1}| \in \mathbb{P}^\infty$ для всех i.

Для фиксированных чисел $t \in \mathbb{N}$ и $r \in \mathbb{P}$ обозначим

$$\mathbb{P}_r^t = \{p^k \mid p \in \mathbb{P} \setminus \{r\},\ k \in \{0\} \cup \mathbb{N}\} \cup \{r^k \mid k \in \{0\} \cup \mathbb{N}, k \leq t\}.$$

Подгруппа H называется $\mathbb{P}_r^t$-субнормальной, если существует цепь подгрупп $H = H_0 \subseteq H_1 \subseteq \ldots \subseteq H_n = G$ такая, что $|H_i : H_{i-1}| \in \mathbb{P}_r^t$ для всех i.

В [**1**] изучались конечные группы $G = AB$ при условии что A и B разрешимые $\mathbb{P}^2$-субнормальные подгруппы группы G. Установлено, что в этом случае группа G разрешима. Развивая данную тематику мы доказали следующие теоремы.

Теорема 1. *Пусть G — конечная группа и $r \in \pi(G) \setminus \{2, 3, 7\}$. Если A и B — $\mathbb{P}^\infty$-субнормальные r-разрешимые подгруппы группы G и $G = AB$, то G является r-разрешимой группой.*

Теорема 2. *Пусть G — конечная группа и $r \in \pi(G)$. Если A и B — $\mathbb{P}_2^2$-субнормальные r-разрешимые подгруппы G и $G = AB$, то G является r-разрешимой группой.*

Простая неабелева группа $PSL_2(7)$ является произведением $\mathbb{P}^3$-субнормальной подгруппы $[Z_7]Z_3$ индекса 2^3 и $\mathbb{P}^1$-субнормальной симметрической подгруппы S_4. Однако $PSL_2(7)$ не является r-разрешимой для всех $r \in \{2, 3, 7\}$. Поэтому в теореме 1 условие $r \in \pi(G) \setminus \{2, 3, 7\}$ отбросить нельзя, а в теореме 2 условие $\mathbb{P}_2^2$-субнормальности нельзя заменить условием $\mathbb{P}_2^3$-субнормальности.

Список литературы

[1] Княгина В.Н., Монахов В.С. Конечные факторизуемые группы с разрешимыми $\mathbb{P}^2$-субнормальными подгруппами // Сиб. мат. журн. 2013. Т.54, N. 1. С. 77–85.

[2] Васильев А. Ф., Васильева Т. И., Тютянов В. Н. О конечных группах сверхразрешимого типа // Сиб. мат. журнал. 2012. Том 53, N. 1. С. 59–67.

Гомельский инженерный институт МЧС Республики Беларусь, Гомельский филиал Международного университета "МИТСО", Беларусь
E-mail: knyagina@inbox.ru, tyutyanov@front.ru

О Минимально полных нильполугруппах

О. В. Князев

В [**1**] предлагается обширная программа по исследованию алгебр, различных классов универсальных алгебр, например, многообразий, псевдомногообразий. Одной из задач этой программы является проблема (проблема 10): *охарактеризовать минимальные полные алгебры данного многообразия.* Здесь мы сообщаем одно свойство минимально полных нильполугрупп.

Напомним некоторые определения. Пусть $\mathbf{V}$ — многообразие всех полугрупп с выделенным нулем 0; $\mathbf{L}(\mathbf{V})$ — решетка подмногообразий многообразия $\mathbf{V}$, $\mathbf{X} \in \mathbf{L}(\mathbf{V})$, $A \in \mathbf{V}$. В дальнейшем под словом "полугруппа" понимается алгебра из многообразия $\mathbf{V}$. Единственным классом $\mathbf{X}-$вербальной конгруэнции $\rho(\mathbf{X}, A)$ на полугруппе A ($\rho(\mathbf{X}, A)$ — наименьшая из конгруэнций на A, фактор-полугруппы по которым принадлежат $\mathbf{X}$), являющимся подполугруппой полугруппы A, будет класс, содержащий нуль 0. Обозначают его через $\mathbf{X}(A)$ и называют $\mathbf{X}-$*вербалом* полугруппы A.

Полугруппу A называют *полной*, если равенство $\mathbf{X}(A) = A$ имеет место для любого атома $\mathbf{X}$ из решетки $\mathbf{L}(\mathbf{V})$. Если полная полугруппа не имеет собственных, отличных от нуля, полных подполугрупп, то ее называют *минимально полной* полугруппой.

Элемент a полугруппы A называют нильэлементом, если найдется натуральное число n такое, что $a^n = 0$. Полугруппу, у которой все элементы суть нильэлементы, называют *нильполугруппой.*

Имеет место следующая

Теорема. *Минимально полная нильполугруппа не имеет нетривиального коммутативного гомоморфного образа.*

Автору не известны нетривиальные примеры минимально полных нильполугрупп.

Список литературы

[1] Мартынов Л. М. О понятиях полноты, редуцированости, примарности и чистоты для произвольных алгебр // Универсальная алгебра и ее приложения. Труды междунар. семинара. Волгоград: Перемена. 2000. С. 179–190.

Омский государственный педагогический университет, Омск
E-mail: knyazev50@rambler

О конечных группах, все n-максимальные подгруппы которых $\mathfrak{F}$-субнормальны

В. А. Ковалева

Все рассматриваемые в сообщении группы являются конечными. Символами $\mathfrak{U}$, $\mathfrak{N}$ and $\mathfrak{N}^r$ обозначаются классы всех сверхразрешимых групп, всех нильпотентных групп и всех разрешимых групп с нильпотентной длиной не более r $(r \geq 1)$ соответственно. 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. Пусть $\mathfrak{F}$ — класс групп. Тогда подгруппа H группы G называется $\mathfrak{F}$-субнормальной в G, если либо $H = G$, либо найдется такая цепь $H = H_0 < \ldots < H_n = G$, что H_{i-1} — максимальная подгруппа в H_i и $H_{i-1}/(H_{i-1})_{H_i} \in \mathfrak{F}$ для всякого $i = 1, 2, \ldots, n$.

Нами исследовались группы, все n-максимальные подгруппы которых $\mathfrak{F}$-субнормальны, где $\mathfrak{F}$ — такая r-кратно насыщенная формация, что $\mathfrak{N} \subseteq \mathfrak{F} \subseteq \mathfrak{N}^{r+1}$ для некоторого $r \geq 0$. В частности, было доказано, что если $|\pi(G)| \geq n + r + 1$, то $G \in \mathfrak{F}$; если $|\pi(G)| \geq n$ и $\mathfrak{F} \subseteq \mathfrak{U}$, то G ϕ-дисперсивна для некоторого упорядочения ϕ множества всех простых чисел. Для случая же, когда $|\pi(G)| \geq n + 1$ и $\mathfrak{F} \subseteq \mathfrak{U}$, было получено полное описание группы G.

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

О распознаваемости по графу простых чисел группы $E_7(2)$

А. С. Кондратьев

Пусть G — конечная группа. Обозначим через $\omega(G)$ *спектр* группы G, т. е. множество всех порядков ее элементов. Множество $\omega(G)$ определяет *граф простых чисел* (*граф Грюнберга — Кегеля*) $\Gamma(G)$ группы G, в котором вершинами служат простые делители порядка группы G и две различные вершины p и q соединены ребром тогда и только тогда, когда $pq \in \omega(G)$.

В теории конечных групп сложилось и динамично развивается направление исследования распознаваемости конечных групп по спектру или графу простых чисел.

Конечная группа G называется *распознаваемой по спектру* (соотв. *графу простых чисел*), если она определяется своим спектром (соотв. графом простых чисел) с точностью до изоморфизма. Ясно, что из распознаваемости конечной группы по графу простых чисел следует ее распознаваемость по спектру.

В [**1**] автором была доказана распознаваемость группы $E_7(2)$ по спектру.

В настоящей работе доказана

Теорема. *Если G — конечная группа и $\Gamma(G) = \Gamma(E_7(2))$, то $G/O_2(G) \cong E_7(2)$.*

Заметим, что граф $\Gamma(E_7(2))$ имеет точно 12 вершин и три компоненты связности.

Работа выполнена при финансовой поддержке РФФИ (проект 13-01-00476), РФФИ-ГФЕН Китая (проект 12-01-91155), программы Отделения математических наук РАН (проект 12-Т-1-1003), и программ совместных исследований УрО РАН с СО РАН (проект 12-С-1-1018) и с НАН Беларуси (проект 12-С-1-1009).

Список литературы

[1] Кондратьев А.С. Об одном вопросе В.Д. Мазурова // Алгебра и геометрия. Тез. межд. конф., посвященной 80-летию со дня рождения А.И. Старостина. Екатеринбург: издательство "УМЦ-УПИ", 2011. С. 82–83.

ИММ УрО РАН, Екатеринбург
E-mail: a.s.kondratiev@imm.uran.ru

Необходимые условия конечности для групп с инволюцией

О. А. Коробов

Централизаторы инволюций накладывают жёсткие ограничения на строение группы. В классе групп, рассмотренных Шунковым, группы с наименьшим централизатором почти регулярной инволюции начал исследовать В.Бусаркин [**1**]. Автором был получен новый результат о группах с маленьким централизатором инволюции.

Теорема 1. *Пусть G — бесконечная группа, содержащая инволюцию a, и $\forall g \epsilon G$ $|гр(a, a^g)| < \infty$, и пусть $|C_G(a)| = 4r$, где r — нечетное число. Тогда группа G разрешима.*

Знаменитая теорема Шункова - Беляева утверждает, что группа с почти регуляной инволюцией является локально конечной. При некоторых дополнительных условиях автором было получено усиление этого результата.

Определение. *Пусть C — конечная группа такая, что $C = [C, C]$. Говорят, что C удовлетворяет условию $\mathcal{K}$, если в C существует нормальная подгруппа N, которая является 2-группой, такая, что C/N — простая неабелевая группа неизоморфная A_7 и $PSL_2(q)$, где $q > 3$ — нечетное число.*

Отметим ещё одно следствие полученного результата.

Теорема 2. *Пусть G — группа, содержащая инволюцию a, $\forall g \epsilon G$ $|гр(a, a^g)| < \infty$, и пусть $C_G(a)$ удовлетворяет условию $\mathcal{K}$. Тогда G есть конечная группа.*

Б.Хартли и Мейкснер [**3**]. показали, что индекс некоторой нильпотентной подгруппы ступени ≤ 2 любой периодической группы с централизатором инволюции, порядок которого равен m, можно ограничить функцией от m. В 1982 году В.В.Беляев и Н.Ф.Сесекин [**4**] продолжили изучение строения периодической группы с почти регулярной инволюцией. Также автором получены теоремы, усиливающие эти результаты.

Список литературы

[1] Бусаркин В. М. Изолированные покрытия и расщепления групп : Автореф. канд. дисс. - Урал.ГУ, 1963.

[2] Шунков В. П. T_0-группы. Новосибирск: Наука, 2000.

[3] Hartley B., Meihner Th. Periodic groups in which the centralizer of an involution has bounded order // J. Algebra. - 1980. - Vol. 64, N 1. - P. 285-291.

[4] Беляев В. В., Сесекин Н. Ф. Периодические группы с почти регулярным инволютивным автоморфизмом // Studia Scientiarum Mathematicarum Hungarica. - 1982. - Vol. 17, N 1-4. - P. 137-141.

Новосибирский государственный университет
E-mail: oleg0101@ngs.ru

Наследуемость свойства D_π надгруппами π-холловых подгрупп четного порядка

Н. Ч. Манзаева

Пусть π — некоторое множество простых чисел. Конечная группа G называется π-группой, если множество простых делителей её порядка лежит в π. Подгруппа H конечной группы G называется π-холловой, если H является π-группой и все простые делители её индекса не лежат в π. Следуя Ф.Холлу [**1**], будем говорить, что группа G является D_π-группой (или, короче, $G \in D_\pi$), если все её максимальные π-подгруппы сопряжены.

В «Коуровской тетради» [**2**] под номером 17.44(б) записана следующая

Проблема. *Всегда ли в D_π-группе надгруппа π-холловой подгруппы является D_π-группой?*

Обозначим через U_π класс всех конечных D_π-групп, в которых всякая надгруппа π-холловой подгруппы обладает свойством D_π. Тогда проблему 17.44(б) можно переформулировать эквивалентным образом: верно ли, что $U_\pi = D_\pi$?

С помощью классификации конечных простых групп доказана следующая

Теорема. *Пусть π — некоторое множество простых чисел и $2 \in \pi$. Тогда $U_\pi = D_\pi$.*

Работа выполнена при финансовой поддержке РФФИ (проекты № 12-01-33102, № 12-01-31222) и ФЦП «Научные и научно-педагогические кадры инновационной России» (гос. контракт №14.740.11.1510).

Список литературы

[1] Hall P., Theorems like Sylow's // Proc. London Math. Soc. Ser. 3. **6** № 22 (1956), 286–304.

[2] Mazurov V. D., Khukhro E.I. (editors), The Kourovka notebook. Unsolved problems in group theory // RAS Siberian Division, Sobolev Institute of Mathematics, Novosibirsk, **17** (2010).

НГУ, Новосибирск
E-mail: manzaeva@mail.ru

О совпадении графа Грюнберга-Кегеля конечной простой группы и ее собственной подгруппы

Н. В. Маслова

Всюду в работе мы будем употреблять термин «группа» в значении «конечная группа». Пусть G — группа, и $\pi(G)$ — множество всех простых делителей ее порядка. *Спектром* группы G называется множество $\omega(G)$ порядков всех ее элементов. Вершинами *графа простых чисел* (или *графа Грюнберга-Кегеля*) $\Gamma(G)$ группы G являются простые числа из $\pi(G)$, и две вершины r и s соединены ребром тогда и только тогда, когда число rs принадлежит множеству $\omega(G)$. Доказана следующая

Теорема 1. *Пусть G — конечная простая группа и H — собственная подгруппа в G. Тогда, за конечным числом исключений, $\Gamma(G) = \Gamma(H)$, в том и только в том случае, когда выполняется одно из следующих утверждений*:

(1) *$G = A_n$, где n и $n-4$ — нечетные не простые числа, и $H = A_{n-1}$*;

(2) *$G = PSp_4(q)$ и $H = PSL_2(q^2).\langle t\rangle$, где $q \in \{3, 2^w\}$ и t — полевой автоморфизм порядка 2 группы $PSL_2(q^2)$*;

(3) *$G = PSp_8(2^w)$ и $H = SO_8^-(2^w)$*;

(4) *$G = P\Omega_8^+(q)$ и $H = P\Omega_7(q)$.*

Пункт (1) *теоремы был получен по модулю расширенной гипотезы Гольдбаха.*

Группа G называется *$\omega(G)$-критической*, если для любых ее подгрупп K и L таких, что $K \trianglelefteq L$, из равенства $\omega(L/K) = \omega(G)$ следует, что $L = G$ и $K = 1$. В работе [**1**] было введено понятие $\omega(G)$-критической группы и был поставлен вопрос: верно ли, что конечная простая группа G, не изоморфная $P\Omega_8^+(2)$ и $P\Omega_8^+(3)$, является $\omega(G)$-критической? В настоящей работе получен отрицательный ответ на этот вопрос. Доказана следующая

Теорема 2. *Пусть G — конечная простая группа, K и L — собственные подгруппы G такие, что $K \trianglelefteq L$. Тогда, за конечным числом исключений, $\omega(G) = \omega(L/K)$, в том и только в том случае, когда либо $G = PSp_4(q)$, $L = PSL_2(q^2).\langle t\rangle$, где q четно и t — полевой автоморфизм порядка 2 группы $PSL_2(q^2)$, и $K = 1$, либо $G = PSp_8(2^w)$, $H = SO_8^-(2^w)$ и $K = 1$.*

Работа выполнена при финансовой поддержке РФФИ (проект 13-01-00469), Совета по грантам Президента РФ (проект МК-3395.2012.1), программ совместных исследований УрО РАН с СО РАН (проект 12-С-1-1018) и УрО РАН с НАН Беларуси (проект 12-С-1-1009), и гранта для молодых ученых ИММ УрО РАН за 2013 г.

Список литературы

[1] Мазуров В. Д., Ши В. Критерий нераспознаваемости конечной группы по спектру // Алгебра и логика. 2012. Т. 51, № 2. С. 239–243.

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

Неабелевы композиционные факторы группы, минимальной относительно простого спектра

Н. В. Маслова, Д. О. Ревин

Пусть $\pi(G)$ — множество всех простых делителей порядка конечной группы G. Конечная группа G *минимальна относительно простого спектра,* если $\pi(H) \neq \pi(G)$ для любой собственной подгруппы H в G. Класс таких групп обозначим через $\mathfrak{Y}$. П. Шумяцкий записал в "Коуровскую тетрадь" гипотезу 17.125, эквивалентную следующей **гипотезе 1**: *любая группа из класса $\mathfrak{Y}$ порождается двумя сопряженными элементами.* В [**1**] было получено частичное подтверждение гипотезы 1, а именно, была доказана ее справедливость для конечных групп с холловыми максимальными подгруппами. Этот результат основывается, в том числе, на результатах работы [**2**]. Поэтому представляет интерес проблема: *каковы неабелевы композиционные факторы группы из класса $\mathfrak{Y}$?*

Теорема. *Среди неабелевых композиционных факторов группы из класса $\mathfrak{Y}$ нет групп, изоморфных следующим конечным простым группам*:

(1) A_n *при непростом* n;

(2) $P\Omega_{2m+1}(q)$, *где* $m \geq 4$ *и* q *нечетны*;

(3) $PSp_{2m}(q)$, *где* $m = 2$ *и* q *нечетно или* $m \geq 4$ *и* m *и* q *четны*;

(4) M_{11}, M_{12}, M_{24}, HS, Co_3, Co_2, ${}^2F_4(2)'$, $PSU_3(3)$, $PSU_4(2)$, $PSU_5(2)$, $PSp_6(2)$, $PSL_6(2)$, $G_2(3)$.

Замечание. Для групп $P\Omega^+_{4k}(q)$, $PSp_4(2^m)$, $PSU_3(5)$, $PSU_4(3)$ и $PSU_6(2)$ вопрос изоморфизма неабелеву композиционному фактору группы из класса $\mathfrak{Y}$ открыт, для группы McL он решается положительно. Остальные конечные простые группы, не перечисленные в теореме, принадлежат классу $\mathfrak{Y}$ ввиду [**3**].

Работа выполнена при финансовой поддержке РФФИ (проекты 13-01-00469 и 13-01-00505), Совета по грантам Президента РФ (проект МК-3395.2012.1), программ совместных исследований УрО РАН с СО РАН (проект 12-С-1-1018) и УрО РАН с НАН Беларуси (проект 12-С-1-1009), ФЦП «Научные и научно-педагогические кадры инновационной России» (проект 14.740.11.0346), целевой программы СО РАН на 2012–2014 гг. (интеграционный проект No. 14) и гранта для молодых ученых ИММ УрО РАН за 2013 г.

Список литературы

[1] Маслова Н. В., Ревин Д. О. Порождаемость конечной группы с холловыми максимальными подгруппами парой сопряженных элементов // Тр. Ин-та математики и механики УрО РАН. 2013. Т. 19, № 3. С. 199–206.

[2] Маслова Н. В. Неабелевы композиционные факторы конечной группы, все максимальные подгруппы которой холловы. Сиб. матем. ж. 2012. Т 53, № 5. С. 1065–1076.

[3] Liebeck M.W., Praeger C.E., Saxl J. Transitive Subgroups of Primitive Permutation Groups// J. Algebra. 2000. V. 234. P. 291–361.

ИММ УрО РАН, Екатеринбург, ИМ СО РАН, Новосибирск
E-mail: butterson@mail.ru, revin@math.nsc.ru

Конечные группы с заданными циклическими примарными подгруппами

В. И. Мурашко

Рассматриваются только конечные группы.

Определение 1 [**1**]. *Подгруппа H группы G называется $\mathbb{P}$-субнормальной, если либо $H = G$, либо существует цепь подгрупп $H = H_0 < H_1 < \cdots < H_n = G$ такая, что $|H_i : H_{i-1}|$ является простым числом для $i = 1, \ldots, n$.*

В работе [**2**] В.Н. Князина и В.С. Монахов ввели и изучили класс $\mathfrak{X}$ всех групп, у которых всякая циклическая примарная подгруппа является $\mathbb{P}$-субнормальной. Ими было показано, что $\mathfrak{X}$ является разрешимой наследственной насыщенной формацией и $\mathfrak{U} \subset \mathfrak{X}$, где $\mathfrak{U}$ — формация всех сверхразрешимых групп. Заметим, что класс $\mathfrak{X}$ совпадает с классом всех групп, у которых всякая циклическая примарная подгруппа $\mathfrak{U}$-субнормальна в смысле следующего определения.

Определение 2 [**3**]. *Пусть $\mathfrak{F}$ — формация. Подгруппа H группы G называется $\mathfrak{F}$-субнормальной, если либо $H = G$, либо существует максимальная цепь подгрупп $H = H_0 < H_1 < \cdots < H_n = G$ такая, что $H_i/Core_{H_i}(H_{i-1}) \in \mathfrak{F}$ для $i = 1, \ldots, n$.*

Нами для заданной формации $\mathfrak{F}$ введен и изучается класс $v\mathfrak{F}$ всех групп, у которых каждая циклическая примарная подгруппа, в том числе и единичная подгруппа, является $\mathfrak{F}$-субнормальной.

Теорема 1. *Если $\mathfrak{F}$ — наследственная (насыщенная) формация, то $v\mathfrak{F}$ — наследственная (насыщенная) формация.*

Напомним [**3**], что подгруппа $\tilde{F}(G)$ определяется следующими двумя условиями: 1) $\tilde{F}(G) \supseteq \Phi(G)$; 2) $\tilde{F}(G)/\Phi(G)$ — цоколь группы $G/\Phi(G)$.

Теорема 2. *Пусть $\mathfrak{F}$ — наследственная насыщенная формация. Тогда и только тогда $v\mathfrak{F} = \mathfrak{F}$, когда $G/\tilde{F}(G)$ является циклической примарной группой для любой минимальной не $\mathfrak{F}$-группы G.*

Список литературы

[1] Васильев А.Ф. О конечных группах сверхразрешимого типа / А.Ф. Васильев, Т.И. Васильева, В.Н. Тютянов // Сиб. мат. журн. — 2010. — Т.51, № 6. — С.1270-1281.

[2] Monakhov V.S. Finite groups with $\mathbb{P}$-subnormal subgroups / V.S. Monakhov, V.N. Kniahina // Ricerche di Matematica, Springer, DOI 10.1007/s11587-013-0153-9.

[3] Шеметков Л.А. Формации конечных групп / Л.А. Шеметков. — Наука, 1978 — 272 с.

Гомельский государственный университет имени Франциска Скорины, Гомель
E-mail: mvimath@yandex.ru

О p-дополнениях в конечных группах

М. Н. Нестеров

Пусть p — простое число. Подгруппа H конечной группы G называется *p-дополнением*, если её порядок не делится на p, а индекс является степенью числа p.

Обозначим через $\mathcal{N}C$ множество всех простых чисел p таких, что для некоторых натурального числа s, степени q простого числа и нечетного простого числа l справедливо равенство

$$p^s = \frac{q^l - 1}{q - 1},$$

Справедлива следующая

Теорема. *Для данного простого числа p следующие утверждения эквивалентны.*

(1) *В каждой конечной группе любые два p-дополнения сопряжены.*

(2) *В каждой конечной группе G любые два p-дополнения сопряжены в* $\mathrm{Aut}(G)$.

(3) *В каждой конечной группе любые два p-дополнения изоморфны.*

(4) $p \notin \mathcal{N}C$.

Для доказательства теоремы используется описание p-дополнений в конечных простых группах [**1**], полученное с помощью классификации конечных простых групп.

Доказано, что числа Ферма, а также числа 2, 19, 37 и 487 не принадлежат множеству $\mathcal{N}C$, в то время как числа Мерсенна принадлежат множеству $\mathcal{N}C$. Кроме того, с помощью компьютерных вычислений найден ряд чисел из $\mathcal{N}C$, среди них числа 11, 13 и 73 не превосходят 100.

Список литературы

[1] Казарин Л.С., О произведении конечных групп, Доклады АН СССР, 269 (1983), №3, 528–531.

Новосибирский государственный университет, Новосибирск
E-mail: mauk00@mail.ru

К теории локально конечных групп

И. И. Павлюк

В сообщении дается описание локально конечных групп, в которых собственные подгруппы имеют черниковский коммутант, а так же описание локально конечных минимальных непочти FC-групп, в которых индексно эквивалентны [**1**] нетривиальные элементы.

Теорема 1. *Локально конечная группа, в которой собственные подгруппы имеют черниковские коммутанты сама имеет черниковский коммутант.*

Теорема 2. *Локально конечная минимальная непочти FC-группа с индексно эквивалентными нетривиальными элементами непроста.*

Работа выполнена при поддержке грантового финансирования научных исследований Комитетом науки Министерства образования и науки Республики Казахстан (№ 92 от 04.02.2013 г. Астана) по теме "Разработка теории сравнений в группах".

Список литературы

[1] Павлюк И. И. Локально-конечные минимальные не FC-группы и проблема минимальности в классе локально-конечных групп. Часть 1//Вестник ПГУ им. С. Торайгырова. Серия физ.-мат. - Павлодар. - 2010. - № 2. - С. 58-72.

Павлодарский государственный университет, Павлодар, Казахстан
E-mail: Ivan.Pavlyuk@mail.ru

О некоторых полуполях нечетного порядка p^3

С. В. Панов

Квазителом, в соответствии с [**1**, II.6.1], или *полуполем* называют кольцо $S =< S, +, \circ >$ с единицей $e \neq 0$, в котором каждое из уравнений $a \circ x = b$ и $y \circ a = b$ $(a, b \in S,\ a \neq 0)$ однозначно разрешимо, т.е. $S^* = S \setminus \{0\}$ – лупа с единицей.

Построение и классификация конечных полуполей тесно связана с классификацией конечных полуполевых плоскостей [**2**]. Известно, что полуполя порядка p и p^2 ($p-$простое число) являются полями [**3**].

Нашей целью является исследование полуполя S порядка p^3, $p > 2$. Элементы ke $(k \in Z)$ образуют в S единственное минимальное подполе $F \simeq Z_p$ для подходящего простого числа p, причем S есть 3-х мерное линейное пространство над F. Если элемент $x \in S \setminus F$ есть корень квадратичного многочлена над F, то он лежит в подполе порядка p^2.

Далее предполагаем, что каждый элемент из S однозначно записывается как многочлен от x степени ≤ 2 над F. Очевидно, коммутативность в S равносильна условию $xx^2 = x^2x$; тогда степень x^3 определена однозначно и x есть корень многочлена $f(z)$ третей степени над F. Если в S выполняется ассоциативность степеней, то S – поле. Более того, полуполе S есть поле, если оно коммутативно и $x^2x^2 = x^3x$.

Оставшийся случай $x^2x^2 \neq x^3x$ подробно исследован, когда $p = 3$, см. [**4**].

Работа выполнена при поддержке Российского фонда фундаментальных исследований (код проекта 12-01-00968).

Список литературы

[1] Курош А.Г. Лекции по общей алгебре. – М., Наука, 1973.
[2] Hughes D. R., Piper F. C. Projective planes //Springer - Verlag: New-York Inc. 1973.
[3] Knuth D.E. Finite semifields and projective planes. – J. Algebra, 2 (1965), 182-217.
[4] Левчук В.М., Панов С.В., Штуккерт П.К. Перечисления полуполевых плоскостей и латин- ских прямоугольников // сб. научных статей "Механика и моделирование". - Красноярск: СибГАУ, 2012, с. 56-70.

каф. АиМЛ ИМФИ СФУ, Красноярск
E-mail: pansevakrasn@mail.ru

О группах Михайлова – Рипса

М. С. Петухова

Р. Михайлов и И. Рипс определили группы $G(\sigma,\tau,\lambda,\mu)$. Эти группы порождаются $4n$, $n \geq 2$, элементами

$$a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n, c_1, c_2, \ldots, c_n, d_1, d_2, \ldots, d_n,$$

и определяется соотношениями

$$a_i c_j = b_{\sigma(i,j)} d_{\tau(i,j)},$$
$$a_i d_j = b_{\lambda(i,j)} c_{\mu(i,j)},$$

для всех i, j и некоторых функций

$$\sigma, \tau, \lambda, \mu : \{1, 2, \ldots, n\}^2 \longrightarrow \{1, 2, \ldots, n\},$$

таких, что их пары

$$(\sigma,\tau), (\lambda,\mu) : \{1, 2, \ldots, n\}^2 \longrightarrow \{1, 2, \ldots, n\}^2$$

задают биекции множества $\{1, 2, \ldots, n\}^2$, т. е. для любой пары индексов (i', j') существует единственная пара индексов (i, j) таких, что $i' = \sigma(i,j)$, $j = \tau(i,j)$, аналогично для функций λ, μ.

Эти группы интересны тем, что групповое кольцо $k[G]$ имеет делители нуля:

$$(a_1 + a_2 + \ldots + a_n + b_1 + b_2 + \ldots + b_n)(c_1 + c_2 + \ldots + c_n - d_1 - d_2 - \ldots - d_n) = 0.$$

Основным результатом работы является

Теорема. *При $n = 2$ всякая группа $G(\sigma,\tau,\lambda,\mu)$ изоморфна некоторой группе из следующего списка*

$$F_2 * \mathbb{Z}_2,\ F_2 * \mathbb{Z}_4,\ F_2 * \mathbb{Z}_8,\ F_3 * \mathbb{Z}_2,\ F_3 * \mathbb{Z}_4,\ F_4 * \mathbb{Z}_2,\ F_2 * \mathbb{Z}_2 * \mathbb{Z}_2,\ F_2 * (\mathbb{Z}_2 \times \mathbb{Z}_2),$$
$$\mathbb{Z} * \langle c, d, f \mid\mid f^2 = ((c^{-1}d)^2 f)^2 = 1\rangle,\ \mathbb{Z} * \langle c, d, f \mid\mid f^2 = ((c^{-1}d)^3 f)^2 = 1\rangle,$$
$$\mathbb{Z} * \langle c, d, f \mid\mid f^2 = c^{-1}d(c^{-1}df)^3 = 1\rangle.$$

НГАУ, Новосибирск
E-mail: russian_basket11@mail.ru

Общее строение мультипликативных групп полей

К. Н. Пономарёв

Хорошо известно строение мультипликативных групп локально конечных полей. Они представляют прямые суммы квазициклических групп.

Для любого не локально конечного поля L определим его *группу единиц* $U(L)$ следующим образом. Если L – поле алгебраических чисел нулевой характеристики, тогда обозначим $U(L)$ – группа алгебраических единиц (обратимых элементов) целого замыкания кольца целых чисел в поле L. А если в поле L имеются трансцендентные элементы, то обозначим алгебраическое замыкание простого поля Q в поле L через $\overline{Q}$. В этом случае группой единиц называем мультипликативную группу этого поля, $U(L) = \overline{Q}^*$.

Теорема. *Рассмотрим поле L, которое не является локально конечным. Утверждается, что в мультипликативной группе поля найдётся подгруппа D не имеющая кручения, которая определяет прямое разложение мультипликативной группы поля L^*:*

$$L^* = U(L) \times D.$$

НГТУ, Новосибирск
E-mail: ponomaryov@ngs.ru

О почти аппроксимируемости конечными p–группами свободного произведения полициклических групп с нормальной объединенной подгруппой

А. В. Розов

Пусть $\mathcal{K}$ — некоторый класс групп. Напомним, что группа G называется аппроксимируемой группами из класса $\mathcal{K}$ (или, короче, $\mathcal{K}$–аппроксимируемой), если для каждого неединичного элемента x из G существует гомоморфизм группы G на группу из класса $\mathcal{K}$, образ элемента x относительно которого отличен от единицы. Если $\mathcal{F}$ обозначает класс всех конечных групп, то понятие $\mathcal{F}$–аппроксимируемой группы совпадает с классическим понятием финитно аппроксимируемой группы. Наряду с финитной аппроксимируемостью изучается также свойство $\mathcal{F}_p$–аппроксимируемости, где p — простое число, $\mathcal{F}_p$ — класс всех конечных p–групп. Будем рассматривать также свойство почти $\mathcal{F}_p$–аппроксимируемости, являющееся промежуточным между финитной аппроксимируемостью и $\mathcal{F}_p$–аппроксимируемостью. Напомним, что группа G обладает некоторым свойством почти, если она содержит подгруппу конечного индекса, обладающую этим свойством.

В 1952 г. К. Гирш [**1**] доказал, что любая полициклическая группа финитно аппроксимируема. А. Л. Шмелькин [**2**] в 1968 г. обобщил этот результат, доказав, что любая полициклическая группа почти $\mathcal{F}_p$–аппроксимируема для каждого простого числа p. Несложные примеры показывают, однако, что аналогичное утверждение для $\mathcal{F}_p$–аппроксимируемости уже не имеет места.

В 1963 г. Г. Баумслаг [**3**] доказал, что свободное произведение двух полициклических групп с нормальной объединенной подгруппой является финитно аппроксимируемой группой. Этот результат не может быть распространен с финитной аппроксимируемости на $\mathcal{F}_p$–аппроксимируемость. Иными словами, свободное произведение двух полициклических $\mathcal{F}_p$–аппроксимируемых групп с нормальным объединением уже не обязано быть $\mathcal{F}_p$–аппроксимируемой группой.

Иначе дело обстоит с почти $\mathcal{F}_p$–аппроксимируемостью. Нами был получен следующий результат.

Теорема. *Пусть G — свободное произведение полициклических групп A и B с нормальной объединенной подгруппой H. Тогда группа G почти $\mathcal{F}_p$–аппроксимируема для любого простого числа p.*

Список литературы

[1] Hirsh K. A. On infinite soluble groups // J. London Math. Soc. 1952. Vol. 27. P. 81–85.
[2] Шмелькин А. Л. Полициклические группы // Сиб. мат. ж. 1968. Том 9. С. 234–235.
[3] Baumslag G. On the residual finiteness of generalized free products of nilpotent groups // Trans. Amer. Math. Soc. 1963. Vol. 106. P. 193–209.

Ивановский государственный университет, Иваново
E-mail: post-box023@mail.ru

Алгебраически, вербально и экзистенциально замкнутые подгруппы свободных нильпотентных групп

В. А. Романьков, Н. Г. Хисамиев

Подгруппа H группы G называется *алгебраически замкнутой* в G, если любая конечная система уравнений с константами из H разрешима в G тогда и только тогда, когда она разрешима в H. Подгруппа H *вербально замкнута* в группе G, если любое уравнение вида $w(x_1, ..., x_n) = h$, где $w(x_1, ..., x_n)$ – произвольное групповое слово от обозначенных переменных и h – произвольный элемент подгруппы H, имеющее решение в группе G, имеет решение в подгруппе H. Подгруппа H *экзистенциально замкнута* в группе G, если любая конечная система уравнений и неравенств с константами из H, имеющая решение в группе G, имеет решение в подгруппе H.

Теорема 1. *Для любой подгруппы N свободной нильпотентной группы $N_{r,c}$ ранга $r \geq 1$ ступени нильпотентности $c \geq 1$ следующие свойства равносильны:*

- *N – вербально замкнутая подгруппа группы $N_{r,c}$;*
- *N – ретракт группы $N_{r,c}$;*
- *N – алгебраически замкнутая подгруппа группы $N_{r,c}$;*
- *N – свободный множитель группы $N_{r,c}$ в многообразии $\mathbf{N}_c$ всех нильпотентных групп ступени нильпотентности $\leq c$.*

Теорема 2. *Подгруппа N свободной нильпотентной группы $N_{r,c}$ ранга $r \geq 3$ ступени нильпотентности $c \geq 2$ экзистенциально замкнута в $N_{r,c}$ тогда и только тогда, когда N является свободным множителем группы $N_{r,c}$ относительно многообразия $\mathbf{N}_c$ всех нильпотентных групп ступени нильпотентности $\leq c$, следовательно, $N \simeq N_{m,c}, 1 \leq m \leq r$, и $m \geq c-1$. Для $c = 2$ последнее ограничение следует заменить на $m \geq 2$.*

Заметим, что экзистенциально замкнутыми подгруппами свободных абелевых групп $N_{r,1}$ являются их нетривиальные прямые множители. Группа $N_{2,c}$ при $c \geq 2$ не имеет собственных экзистенциально замкнутых подгрупп.

Омский государственный университет им. Ф. М. Достоевского, Омск;
Восточно-Казахстанский государственный технический университет им. Д. Серикбаева, Усть-Каменогорск, Республика Казахстан
E-mail: romankov48@mail.ru, hisamiev@mail.ru

Об аппроксимируемости относительно сопряженности некоторыми классами конечных групп обобщенных свободных произведений и HNN-расширений

Е. В. Соколов

Пусть $\mathcal{C}$ — произвольный класс конечных групп, содержащий хотя бы одну неединичную группу и замкнутый относительно взятия подгрупп и расширений. Следуя общему определению, будем говорить, что некоторая группа X аппроксимируема классом $\mathcal{C}$ (или, короче, $\mathcal{C}$-аппроксимируема) относительно отношения ρ, связывающего элементы этой группы, если для любых элементов, не состоящих в данном отношении, найдется гомоморфизм группы X на группу из класса $\mathcal{C}$, при котором образы указанных элементов по-прежнему не состоят в отношении ρ.

Автором доказаны следующие утверждения.

Теорема 1. *Произвольное расширение свободной группы при помощи $\mathcal{C}$-группы аппроксимируется классом $\mathcal{C}$ относительно сопряженности.*

Теорема 2. *Пусть G — свободное произведение двух $\mathcal{C}$-аппроксимируемых относительно сопряженности групп с конечной объединенной подгруппой или HNN-расширение $\mathcal{C}$-аппроксимируемой относительно сопряженности группы с конечными связанными подгруппами. Если группа G $\mathcal{C}$-аппроксимируема (относительно равенства), то она $\mathcal{C}$-аппроксимируема относительно сопряженности.*

Поскольку обычное свободное произведение двух групп можно рассматривать как обобщенное с тривиальной объединенной подгруппой, из теоремы 2 вытекает

Следствие. *Свободное произведение двух групп, $\mathcal{C}$-аппроксимируемых относительно сопряженности, само аппроксимируется относительно сопряженности классом $\mathcal{C}$.*

Отметим, что если $\mathcal{C}$ совпадает с классом всех конечных групп, утверждения, доставляемые теоремами 1, 2 и следствием, известны и доказаны в работах [**1**], [**2**] и [**3**], соответственно. В случае, когда $\mathcal{C}$ — класс всех конечных p-групп, результаты, аналогичные теореме 1 и следствию, получены в [**4**].

Список литературы

[1] Dyer J. L. Separating conjugates in free-by-finite groups // J. Lond. Math. Soc. (2). 1979. V. 20. P. 215–221.

[2] Dyer J. L. Separating conjugates in amalgamated free products and HNN extensions // J. Australian Math. Soc. 1980. V. 29. P. 35–51.

[3] Stebe P. F. A residual property of certain groups // Proc. Amer. Math. Soc. 1970. V. 26. P. 37–42.

[4] Иванова Е. А. Аппроксимируемость относительно сопряженности конечными p-группами свободных произведений двух групп // Вестник Иван. гос. ун-та. Сер. “Биология, Химия, Физика, Математика”. 2005. Вып. 3. С. 83–91.

Ивановский государственный университет, г. Иваново
E-mail: ev-sokolov@yandex.ru

О ядре сопряжения элементов группы

Л. И. Теняева, И. И. Павлюк

Пусть H - подмножество группы G.

Введем бинарное отношение " $\equiv_L^H$ ", базирующееся на отношении равенства выражений в группе.

Определение 1. [1] $(\forall a, b \in G)(\forall H \subset G)\left(\left(a \equiv_L^H b\right) \overset{\text{Def}}{\Leftrightarrow} (a = hb, h \in H)\right)$.

Лемма 1. *Если отношение " $\equiv_L^H$ " является отношением эквивалентности на элементах группы G, то H подгруппа группы G.*

Определение 2. *Ядром сопряжения элемента a группы G в группе G назовем множество $S(a)$ элементов h группы G, удовлетворяющее равенству $a = hb$, где элементы a, b принадлежат классу $\overset{c\equiv}{a}$ сопряженных элементов с a, т. е. аналитически ядро сопряжения определяется формулой $S(a) = \{h/a = hb, a, b \in \overset{c\equiv}{a}\}$.*

Лемма 2. *(Корректность введенного понятия). В группе G ядра сопряжения сопряженных элементов равны между собой.*

Теорема 1. *Для любого элемента a группы G ядро сопряжения $S(a)$ является нормальным делителем группы G.*

Теорема 2. *Группа G тогда и только тогда абелева, когда для любого ее элемента g ядро сопряжения $S(g) = \{e\}$.*

Лемма 3. *Для любого элемента z из центра $Z(G)$ группы G ядро сопряжения $S(z) = \{e\}$.*

Теорема 3. *Группа G обладает нетривиальным центром $Z(G)$ тогда и только тогда, когда в G существует нетривиальный элемент z такой, что $S(z) = \{e\}$.*

Работа выполнена при поддержке грантового финансирования научных исследований Комитетом науки Министерства образования и науки Республики Казахстан (№ 92 от 04.02.2013 г. Астана) по теме "Разработка теории сравнений в группах".

Список литературы

[1] Павлюк И.И., Лукьянчук О.И. Отношение эквивалентности и смежные классы группы по подгруппе // Международная научная конференция "Ломоносов 2011". - Астана. - 2011. - С. 63-65.

Павлодарский государственный университет, Павлодар, Казахстан
E-mail: Ivan.Pavlyuk@mail.ru

Разрешимые группы с ограничениями на небициклические силовские подгруппы фиттинговых факторов

А. А. Трофимук

Рассматриваются только конечные группы. Все обозначения и используемые определения соответствуют [**1**].

Бициклической называют группу $G = AB$, факторизуемую циклическими подгруппами A и B.

Из результата Бэра [**1**, с. 720] следует сверхразрешимость разрешимой группы G, обладающей цепочкой подгрупп

$$\Phi(G) = G_0 \subset G_1 \subset \ldots \subset G_{m-1} \subset G_m = F(G), \tag{1}$$

такой, что G_i нормальна в G и $|G_{i+1}/G_i|$ является простым числом для всех i. Здесь $\Phi(G)$ — подгруппа Фраттини группы G, а $F(G)$ — подгруппа Фиттинга группы G. Очевидно, что группа останется сверхразрешимой, если силовские подгруппы в факторах цепочки вида (1) будут циклическими.

В работе [**2**] исследовались разрешимые группы, у которых силовские подгруппы в факторах цепочки вида (1) бициклические.

В настоящей работе продолжено изучение разрешимых групп, у которых силовские подгруппы в факторах цепочки вида (1) имеют заданные ограничения. Доказана следующая теорема.

Теорема. *Предположим, что в разрешимой группе G существует цепочка подгрупп вида (1) такая, что G_i нормальны в G и силовские p-подгруппы в факторах G_{i+1}/G_i являются либо бициклическими, либо порядка p^3 для каждого $p \in \pi(G)$. Тогда нильпотентная длина группы G не превышает 4, а производная длина фактор-группы $G/\Phi(G)$ не превышает 6.*

Разрешимые группы из работы [**2**] и группы, исследуемые в теореме, имеют одинаковые оценки нильпотентной длины, а для производной длины оценки различны (в работе [**2**] производная длина $G/\Phi(G)$ не превышает 5). Оказалось, что если порядки небициклических силовских подгрупп в факторах цепочки вида (1) будут равны кубам простых чисел $p \in \{2, 3, 5, 11, 17\}$, либо 16, либо 32, то оценка производной длины фактор-группы $G/\Phi(G)$ останется равной 5.

Работа выполнена при финансовой поддержке БРФФИ (грант № Ф13М-113).

Список литературы

[1] Huppert B. Endliche Gruppen I. Berlin-Heidelberg-New York: Springer, 1967. 793 p.

[2] Трофимук А. А. Конечные группы с бициклическими силовскими подгруппами в фиттинговых факторах // Труды Института математики и механики УрО РАН. 2013. № 3(19). С. 304–307.

Брестский гос. университет им. А.С. Пушкина, Брест
E-mail: alexander.trofimuk@gmail.com

Об аппроксимируемости корневыми классами групп обобщенных свободных произведений с нормальным объединением

Е. А. Туманова

В данной работе рассматриваются условия аппроксимируемости произвольным корневым классом групп обобщенного свободного произведения двух групп с нормальной объединенной подгруппой.

Напомним, что класс групп $\mathcal{K}$ называется корневым [**1**], 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 $X/T \in \mathcal{K}$. Можно показать, что класс групп является корневым тогда и только тогда, когда он замкнут относительно взятия подгрупп и декартовых сплетений [**2**].

Далее будем предполагать, что $G = (A * B;\ H)$ — обобщенное свободное произведение двух групп A и B с объединенной подгруппой H, нормальной в A и в B. Тогда подгруппа H является нормальной в группе G, и потому ограничение на H любого внутреннего автоморфизма группы G оказывается автоморфизмом группы H. Обозначим множество всех таких автоморфизмов через $\mathrm{Aut}_G(H)$.

Г. Хигман доказал, что если A и B являются конечными p-группами, то группа G аппроксимируется конечными p-группами тогда и только тогда, когда $\mathrm{Aut}_G(H)$ — конечная p-группа [**3**]. Приводимые далее результаты показывают, что данное утверждение можно распространить на свойство аппроксимируемости произвольным классом конечных групп, замкнутым относительно взятия подгрупп, фактор-групп и расширений.

Теорема. *Пусть $\mathcal{K}$ — произвольный корневой класс групп, A, $B \in \mathcal{K}$. Если A/H, B/H, $\mathrm{Aut}_G(H) \in \mathcal{K}$, то группа G является $\mathcal{K}$-аппроксимируемой.*

Следствие 1. *Пусть $\mathcal{K}$ — замкнутый относительно факторизации корневой класс групп, A, $B \in \mathcal{K}$, подгруппа H конечна. Группа G является $\mathcal{K}$-аппроксимируемой тогда и только тогда, когда $\mathrm{Aut}_G(H) \in \mathcal{K}$.*

Следствие 2. *Пусть $\mathcal{K}$ — замкнутый относительно факторизации корневой класс групп, A, $B \in \mathcal{K}$, подгруппа H является циклической или лежит в центре хотя бы одного свободного множителя. Тогда группа G $\mathcal{K}$-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 // ArXiv math.GR: 1308.1039.
[3] Higman G. Amalgams of p-groups // J. Algebra. 1963. V. 1. P. 301 — 305.

Ивановский государственный университет, г. Иваново
E-mail: helenfog@bk.ru

О конечных группах с независимыми подгруппами

А. А. Цирхов

Подгруппа H группы G называется независимой подгруппой, если $N_G(K) \leqslant N_G(H)$ для любой нетривиальной подгруппы K из H.

Независимыми подгруппами, очевидно, являются группы простых порядков, нормальные подгруппы, дополнения групп Фробениуса. Другими примерами независимых подгрупп служат силовские 2-подгруппы в простых группах $L_2\left(2^m\right)$, $Sz\left(2^{2m+1}\right)$ и $U_3\left(2^m\right)$.

М. Сузуки (Ann. Mathem., 1980) классифицировал конечные группы четного порядка с независимыми силовскими 2-подгруппами.

Л.И. Шидов (Сибирск. Матем. Ж., 1980) описал конечные группы, в которых независима каждая нильпотентная подгруппа.

Одной из целей данного сообщения является изучение класса конечных групп, в каждой из которых любая неабелева подгруппа независима. Очевидно, рассматриваемому классу принадлежат все конечные метагамильтоновы группы, т.е. группы, в которых нормальны все неабелевы подгруппы.

Начало изучению метегамильтоновых групп положила работа (Г.М. Ромалиса и Н.Ф. Сесекина Т.М. Ромалис, Н.Ф. Сесекин. О метагамильтоновых группах. Матем. Зап. Уральского Университета, 5, №3 (1966), 45-49).

Конечные ненильпотентные метагамильтоновы группы классифицировал В.Т. Нагребецкий (В.Т. Нагребецкий. Конечные ненильпотентные группы, любая неабелева подгруппа которых инвариантна. Матем. Зап. Уральского Университета, 6, №1 (1967), 80-88).

Конечные нильпотентные метагамильтоновы группы описаны в работе А.А. Махнева (А.А. Махнев. О конечных метагамильтоновых группах. Матем. Зап. Уральского Университета, 10, №1 (1976), 60-75).

Бесконечные метагамильтоновы группы, а также обобщения как конечных, так и бесконечных метагамильтоновых групп рассматривались в работах различных авторов, из которых отметим работы С.Н. Черникова (С.Н. Черников. Группы с заданными свойствами систем подгрупп. М.: Наука, 1980), Н.Ф. Кузенного и Н.Н. Семко (Н.Ф. Кузенный, Н.Н. Семко. Строение разрешимых ненильпотентных метагамильтоновых групп. Матем. Заметки, 34, №2 (1983), 179-188), F. De Mari, F. De Giovanni (F. De Mari, F. De Giovanni. Groups with finitely many normalizers of non-abelian subgroups. Ricerche di matematica, 55, №2 (2006), 311-317). Наиболее "свежие" результаты на эту тему содержатся в работе Bollester-Bolinches, J. Cossey (J. Algebra, 2009).

Нами получены следующие результаты:

Теорема 1. *В конечной группе G любая неабелева подгруппа независима тогда и только тогда, когда G метагамильтонова.*

Теорема 2. *Конечная группа, в которой независима любая абелева подгруппа, является либо двуступенно нильпотентной группой, либо группой Фробениуса с нильпотентным дополнительным множителем, либо группой, изоморфной одной из следующих групп*: S_4, A_6, $L_2(7)$, $L_2(2^m)$, $m \geqslant 2$.

Следующий результат дает полное описание нильпотентных конечных групп, в которых независимы все абелевы подгруппы.

Теорема 3. *В конечной нильпотентной группе G все абелевы подгруппы независимы тогда и только тогда, когда выполнено одно из условий:*

(1) *G – абелева или гамильтонова группа, т.е. группа, в которой все подгруппы нормальны;*
(2) *G – p-группа нечетного порядка, являющаяся центральным произведением экстраспециальной группы периода p и порядка p^3 на циклическую группу;*
(3) *G изоморфна $\left\langle a, b \mid a^p = b^{p^m} = 1,\ a^{-1}ba = b^{1+p^{m-1}} \right\rangle$ для некоторого $m \geqslant 2$. Здесь p – простое число;*
(4) *G – центральное произведение группы диэдра порядка 8 на циклическую 2-группу или группу кватернионов порядка 8.*

Следующий результат завершает описание всех конечных групп с независимыми абелевыми подгруппами.

Скажем, что циклическая группа $\langle h \rangle$ действует скалярно на абелевой группе K, если найдется такое целое число α, что $k^h = k^\alpha$ для любого $k \in K$.

Теорема 4. *Пусть G – конечная группа Фробениуса с ядром K и дополнением H. В G тогда и только тогда все абелевы подгруппы независимы, когда выполнено одно из следующих условий:*

(1) *$H = \langle h \rangle$, K – экстраспециальная группа периода p, т.е.*
$$K = \langle a, b \mid a^p = b^p = [[a, b], a] = [[a, b], b] = 1 \rangle,$$
где p – нечетное простое число, и существует целое число α такое, что $a^h = a^\alpha$, $b^h = b^\alpha$;
(2) *K – абелева группа, а H – циклическая подгруппа, действующая скалярно на K;*
(3) *$K = \langle k_1 \rangle \times \langle k_2 \rangle$ – элементарная абелева группа, $H = \langle h \rangle$, $k_1^h = k_1^{\alpha_1}$, $k_2^h = k_2^{\alpha_2}$ для некоторых целых α_1, α_2;*
(4) *H – циклическая группа, K – нециклическая элементарная абелева группа, H действует неприводимо на K при сопряжении, а любая собственная подгруппа из H действует на K либо неприводимо, либо скалярно;*
(5) *K – элементарная абелева группа порядка p^2 для некоторого нечетного простого числа p, $H = Q \times H_0$, где Q – группа кватернионов порядка 8, H_0 – циклическая группа, действующая скалярно на K.*

Результаты опубликованы во Влад. Мат. Ж. (2010, 2013) и в Трудах ИММ УрО РАН (2011). Докладывались на школах-конференциях (2010, 2012). Они составляют основное содержание моей кандидатской диссертации.

О замкнутости аддитивной группы рациональных чисел в классах нильпотентных групп без кручения

С. А. Шахова

Доминионом [**1**] подгруппы H группы G в квазимногообразии $\mathfrak{M}$ ($G \in \mathfrak{M}$), обозначаемом $dom_G^{\mathfrak{M}}(H)$, называется следующее множество элементов группы G: $dom_G^{\mathfrak{M}}(H) = \{g \in G \mid \forall M \in \mathfrak{M}\ \forall \varphi, \psi : G \to M,$ если $\varphi\,|_H = \psi\,|_H,$ то $\varphi(g) = \psi(g)\}$, где $\varphi, \psi : G \to M$ — гомоморфизмы группы G в группу M; $\varphi\,|_H$, $\psi\,|_H$ — сужение φ, ψ на H; $\varphi(g)$, $\psi(g)$ — образы элемента g при гомоморфизмах φ, ψ.

Согласно [**2**] группа $H \in \mathfrak{M}$ называется $n-$замкнутой в $\mathfrak{M}$, если $dom_G^{\mathfrak{M}}(H) = H$ для любой группы G из $\mathfrak{M}$, содержащей H в качестве подгруппы и порождённой по модулю H n элементами.

Пусть s — фиксированное натуральное число. В настоящей работе доказана

Теорема. *Аддитивная группа рациональных чисел 1-замкнута в произвольном квазимногообразии нильпотентных ступени $\leq s$ групп без кручения и 3-замкнута в произвольном квазимногообразии нильпотентных ступени ≤ 2 групп без кручения.*

Список литературы

[1] Isbell J. R., Epimorphisms and dominions, Proceedings of the Conference on Categorical Algebra, La Jolla, 1965, New York, Springer-Verlag, 1966, 232–246.

[2] Будкин А. И., Доминионы универсальных алгебр и проективные свойства, Алгебра и логика, 47, № 5 (2008), 541–557.

Алтайский государственный университет, г. Барнаул
E-mail: sashakhova@gmail.com

Об объединении решений систем уравнений в конечных простых полугруппах

А. Шевляков

Пусть S — вполне простая полугруппа. Согласно классической теореме Риса, полугруппа S имеет представление $(G, \mathbb{P}, \Lambda, I)$, и S изоморфна дизъюнктному объединению копий группы G. Результат умножения элементов из различных копий группы G определяется с помощью сэндвич-матрицы $\mathbb{P}$ и множеств индексов Λ, I. Вполне простые мы будем рассматривать в языке $\mathbb{L}_S = \{\cdot, ^{-1}\} \cup \{s | s \in S\}$, где $^{-1}$ — операция взятия обратного элемента (в соответствующей копии группы G) и все элементы полугруппы S отмечены как константы в языке $\mathbb{L}$.

Согласно [**1**], полугруппа S является эквациональной областью, если любое конечное объединение решений систем уравнений над S является решением некоторой системы уравнений.

Мы доказываем следующий результат.

Теорема. *Вполне простая полугруппа $S = (G, \mathbb{P}, \Lambda, I)$ языка $\mathbb{L}_S$ является эквациональной областью тогда и только тогда, когда группа G — эквациональная область в языке $\mathbb{L}_G = \{\cdot, ^{-1}\} \cup \{g | g \in G\}$ и нормализованная матрица $\mathbb{P}$ не содержит одинаковых строк и столбцов.*

Список литературы

[1] Daniyarova E., Miasnikov A., Remeslennikov V., Algebraic geometry over algebraic structures IV: эквациональная областьs and co-domains, Algebra & Logic, v. 49, 6, pp.715–756.

О свойствах полуполей четного порядка

П. К. Штуккерт

Определение. *Полуполем называют кольцо* $S = \langle S, +, \circ \rangle$ *с единицей* $e \neq 0$ *и однозначно разрешимыми уравнениями* $a \circ x = b$ *и* $y \circ a = b$ *при любых* $a, b \in S$, $a \neq 0$, *т.е.* $S^* = (S \setminus \{0\}, \circ)$ *есть лупа.*

Порядком элемента x в лупе будем называть наименьшее целое число $n \geq 1$ такое, что хотя бы одно произведение длины n с сомножителями x равно e. В остальных случаях считаем порядок бесконечным.

Классификация конечных полуполевых плоскостей и полуполей тесно связаны. Во всяком конечном полуполе S кратные единичного элемента образуют единственное минимальное подполе $F \simeq Z_p$ для подходящего простого числа p (характеристика полуполя S), причем $|S| = p^n$, n – размерность S над F. Известно, что полуполя порядков p, p^2 и 8 являются полями, [**1**].

С другой стороны, неассоциативные полуполя порядка 16 существуют. Число их изотопных классов равно 2, как показывается с использованием компьютерных вычислений, [**1**], [**2**], [**3**], [**4**]. Оказывается, уже для них проявляются аномальные свойства по сравнению с конечными полями.

Аналог теоретико-групповой теоремы Лагранжа для лупы S^* полуполя S не обязан выполняться даже для порядков ее элементов. Типична следующая теорема, установленная для полуполя S, соответствующего полуполевой плоскости ранга 2 порядка 16, построенной в [**3**].

Теорема. *а) Порядки элементов лупы* S^* *образуют множество* $\{1, 3, 4, 5, 6\}$*;*

б) всякий элемент порядка ≤ 3 *лупы* S^* *лежит в подходящем подполе порядка 4 полуполя* S*, а любой другой ее элемент порождает* S^**;*

в) полуполе S *имеет, в точности, два подполя порядка 4.*

Список литературы

[1] *Knuth D.E.* Finite semifields and projective planes. // J. Algebra. 2, 1965, pp. 182-217.

[2] E. Kleinfeld. Techniques for enumerating Veblen-Wedderburn systems. // J. Assoc. Comput. Mach. 7, 1960, pp. 330-337.

[3] *Кравцова О.В., Куршакова (Штуккерт) П.К.* К вопросу об изоморфизме полуполевых плоскостей // Красноярск: вестник КГТУ, 2005, с.13-21.

[4] *В.М. Левчук, С.В. Панов, П.К. Штуккерт.* Перечисления полуполевых плоскостей и латинских прямоугольников // сб. научных статей "Механика и моделирование". - Красноярск: СибГАУ, 2012, с. 56-70.

Сибирский федеральный университет, Красноярск
E-mail: Poli422@yandex.ru

Distance regular colorings of the infinite hexagonal grid

S. V. Avgustinovich, D. S. Krotov, A. Yu. Vasil'eva

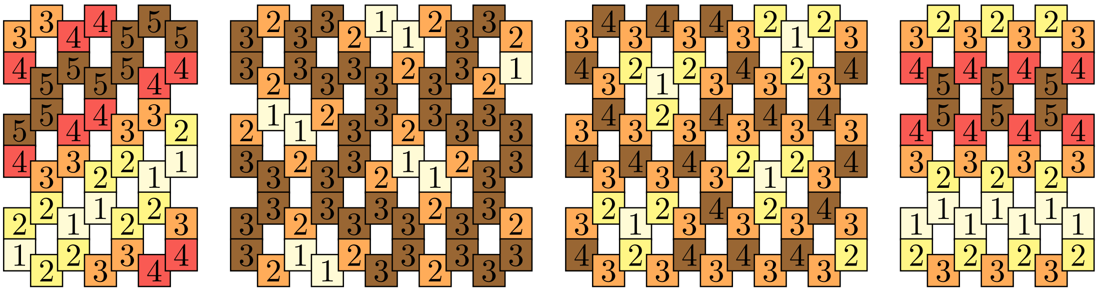
A vertex partition $(V_1, \ldots, V_k)$ of a graph G is called a *perfect coloring* (equitable partition, regular partition, partition design) if for every $i, j \in \{1, \ldots, k\}$ there is a number a_{ij} such that every vertex from V_i has exactly a_{ij} neighbors from V_j. The matrix $A = (a_{ij})$ will be called the *parameter matrix* of the coloring. A perfect coloring $(V_1, \ldots, V_k)$ is called *distance regular* if its parameter matrix is three-diagonal (equivalently, if the perfect coloring $(V_1, \ldots, V_k)$ is the distance coloring with respect to V_1; the set V_1 is known to be a *distance regular code* in this case). We study the distance regular colorings of the infinite cubic graph of the hexagonal grid.

A matrix $(a_{ij})_{i,j=1}^{k}$ will be written as $[a_{11}a_{12}|a_{21}a_{22}a_{23}|a_{32}a_{33}a_{34}|\ldots|a_{k\,k-1}a_{kk}]$.

Theorem. *Up to the central symmetry, the parameter $k \times k$ matrices of nontrivial ($k > 1$) distance regular colorings of the infinite hexagonal grid are divided into:*

- 5 *matrices* [03|30], [03|12], [12|21], [12|12], [21|12], $k = 2$*;*
- 6 *classes* [12|111|...|111|12], [12|111|...|111|21], [21|111|...|111|12], $k = 3, 4, 5, \ldots$*;*
  [12|201|102|201|...|201|12], $k = 3, 5, 7, \ldots$*;*
  [12|201|102|201|...|102|21], [21|102|201|102|...|201|12], $k = 4, 6, 8, \ldots$*;*
- 9 *"sporadic" matrices* [03|102|30], [03|111|12], [12|102|12], [21|102|12],
  [03|102|102|30], [03|102|201|30], [03|111|111|30], [12|102|111|21],
  [03|102|102|201|30], [03|102|111|201|12].

Each of the matrices [03|111|12], [12|201|12] *corresponds to two nonequivalent colorings; each of* [01|12], [12|21], [21|12], [12|111|21], [03|102|201|30], *to infinite number of colorings; every other matrix corresponds to one colorings, up to equivalence.*



This research was supported by the Target program of SB RAS for 2012-2014 (integration project No. 14).

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. N 3. P. 3–10.

[2] Puzynina, S. A. On periodicity of perfect colorings of the infinite hexagonal and triangular grids // Sib. Math. J. 2011. Vol. 52. N 1. P. 91–104.

Sobolev Institute of Mathematics, Novosibirsk
E-mail: avgust@math.nsc.ru, krotov@math.nsc.ru, vasilan@math.nsc.ru

Finite groups in which all 2-maximal subgroups are π-decomposable

V. A. Belonogov

Finite groups in which all maximal subgroups are nilpotent was described by O. Ju. Schmidt in 1924. 2-maximal subgroup of a group is a maximal subgroup of a maximal subgroup of this group. Finite non-solvable groups in which all 2-maximal subgroups are nilpotent was studied by Z. Janko in [**1**]; there are only two such groups: $SL_2(5)$ and A_5. Finite solvable groups in which all 2-maximal subgroups are nilpotent was described in the author's paper [**2**].

Let π be a set of primes. A group is called π-*decomposable* (or (π, π')-decomposable) if it is the direct product of a π-group and a π'-group.

Theorem. *Let π be a set of primes and G be a finite not π-decomposable group in which all 2-maximal subgroups are π-decomposable. Then*

or G is solvable and $|\pi(G)| \in \{2, 3\}$ (the complete description of G given in [**3**]*),*

or $G/\Phi(G)$ is isomorphic to one of the following simple groups:

(1) *A_r, where r and $(r-1)/2$ are primes, $r \notin \{7, 11, 23\}$;*

(2) *$PSL_2(q)$ for some $q > 5$;*

(3) *$PSL_r(q)$ for odd primes r and $t/(t, q-1)$, where $t = (q^r - 1)/(q-1)$;*

(4) *$PSU_r(q)$ for odd primes r and $t/(t, q+1)$, where $t = (q^r + 1)/(q+1)$;*

(5) *the Mathieu group M_{23} and the Baby Monster F_2.*

Some additional restrictions on parameters of the groups from conditions (1)–(5) and corresponding sets π are obtained. In particular, in (5) one of sets $\pi \cap \pi(G)$ and $\pi' \cap \pi(G)$ is $\{23\}$ for $G = M_{23}$ and $\{47\}$ for $G = F_2$.

The proof of Theorem is based on the results of the author's paper [**4**] about the control of the prime spectrum of the finite simple groups.

This work was supported by RFBR (project no. 13-01-00469), RFBR–GFEN of China (project no. 12-01-91155), Program DMS of RAS (project no. 12-T-1-1003), Programs of JR of UB RAS with SB RAS (project no. 12-S-1-10018) and Belarusian NAS (project no. 12-S-1-1009).

References

[1] Janko. Z. Endliche Gruppen mit lauter nilpotenten zweitmaximalen Untergruppen// Math. Z., 1962, vol. 79, no. 5, pp. 422–424.

[2] Belonogov. V. A. Finite solvable groups with nilpotent 2-maximal subgroups // Math. Notes., 1968, vol. 3, no. 1, pp. 15–21.

[3] Belonogov. V. A. On finite groups saturated with (π, π')-decomposable subgroups // Siberian Math. J., 1969, vol. 10, no. 3, pp. 354–362.

[4] Belonogov. V. A. On control of the prime spectrum of finite simple group // Trudy Inst. Mat. i Mekh. UrO RAN, Ekaterinburg, 2013, vol. 19, no. 3, pp. 29–44. (in Russian).

Inst. Math. Mech., Ural Branch of RAS, Ekaterinburg (Russia)
E-mail: belonogov@imm.uran.ru

Completely regular codes in the Johnson graphs $J(v, 3)$

A. L. Gavrilyuk, S. V. Goryainov, I. Yu. Mogilnykh

The *Johnson graph* $J(v, k)$ is a graph whose vertex set consists of all k-subsets of a fixed v-set. Two k-subsets are adjacent if and only if they share k-1 elements exactly. Since the graphs $J(v, k)$ and $J(v, v-k)$ are isomorphic, we assume that $k \leq v/2$. The Johnson graph is distance-regular, see [1], has diameter k and $k+1$ distinct eigenvalues $\theta_i = (k-i)(v-k-i) - i, i = 0, \ldots, k$.

A *perfect coloring* with r colors of a graph Γ (r-coloring, for short) is a partition of the vertex set of Γ into r parts (colors) $C_1, \ldots, C_r$ such that, for all $i, j \in 1, \ldots, r$ every vertex in C_i is adjacent to the same number of vertices, namely, c_{ij}, in C_j. The matrix $C = (c_{ij})_{i,j=1,\ldots,r}$ is called the *quotient matrix* of a perfect r-coloring. It is well known [1] that the eigenvalues of the quotient matrix are eigenvalues of the graph.

Given a perfect r-coloring, if an appropriate ordering of its colors determines a distance partition of the vertex set with respect to C_i, then C_i is called a completely regular code. In this case, the number $\rho := r-1$ is called the *covering radius* of the code. The set of vertices at maximal distance from a completely regular code also is a completely regular code and is called the *opposite code* [4].

A t-design is a set $\mathcal{B}$ of vertices of $J(v, k)$ (usually called blocks) such that every tЦsubset of vЦset belongs to the constant number of blocks in $\mathcal{B}$. The strength of $\mathcal{B}$ is the largest t such that $\mathcal{B}$ is a t-design.

One may show [4] that the strength of a completely regular code of $J(v, k)$ is t such that θ_{t+1} is the second largest eigenvalue of the quotient matrix.

Completely regular codes of strength 0 in the Hamming graphs and Johnson graphs have been described in [3]. Completely regular codes of strength 1 with the assumption that a code or its opposite induces a disconnected subgraph in $J(v, k)$ have been described in [4]. Completely regular codes with covering radius 1 in $J(v, k)$ for $v \leq 8$ or $k = 2$ are studied in [2,5,6].

Given a completely regular code in $J(v, k)$, the inequality $t + \rho \leq k$ holds [1], where t is its strength, and ρ is its covering radius. We also recall, see [2], that any $(k-1)$-design is a completely regular code in $J(v, k)$. Hence, for $k = 3$, the parameters $(t, \rho) \in (1, 1), (1, 2)$ remain unsolved.

Completely regular codes in $J(v, 3)$ with $(t, \rho) = (1, 1)$ and under the assumption that the quotient matrix is symmetric or v is even have been classified in [7].

In the present work, we finish the classification of completely regular codes in $J(v, 3)$.

Theorem. *The quotient matrix of a perfect* 2*-coloring that corresponds to a completely regular code of strength* 1 *and radius* 1 *in* $J(v, 3)$ *is one of the following:*

$$\begin{pmatrix} 3(v-5) & 6 \\ 4(\frac{v}{2}-2) & v-1 \end{pmatrix}, \begin{pmatrix} 3(\frac{v}{2}-3) & \frac{3v}{2} \\ \frac{v}{2}-2 & \frac{5v}{2}-7 \end{pmatrix}, \begin{pmatrix} 3(\frac{v}{2}-1) & 3(\frac{v}{2}-2) \\ \frac{v}{2}+4 & \frac{5v}{2}-13 \end{pmatrix}$$

in particular, v *is even. Conversely, for any of the matrices above, there is a perfect* 2*-coloring of* $J(v, 3)$ *with corresponding quotient matrix.*

Conclusion. Recently, there have been several results on the perfect colorings of various graphs, utilizing the local structure of the graphs [5,7,8]. In this work, using the approach, we obtain the classification of completely regular codes in $J(v, 3)$ with covering radius $\rho = 1$ of strength 1. Moreover, we announce that the case where $\rho = 2$ in $J(v, 3)$ can be also solved using the approach.

Acknowledgement. The work is supported by RFBR (project 12-01-31098), and by the grant of the President of Russian Federation for young scientists (project MK-1719.2013.1).

References

[1] Brouwer A. E., Cohen A. M., Neumaier A. Distance-regular graphs, Springer-Verlag, Berlin, 1989.

[2] Avgustinovich S. V., Mogilnykh I. Yu. Perfect colorings of the Johnson graphs $J(8,3)$ and $J(8,4)$ with two colors, J. of Applied and Industrial Math. **5** (2011), 19–30.

[3] Meyerowitz A. D. Cycle-balanced partitions in distance-regular graphs, Discrete Math **264** (2003), 149–165.

[4] Martin W. J. Completely regular designs of strength one, J. Algebr. Comb. **3** (1994), 170–185.

[5] Mogilnykh I. Yu. On the nonexistence of some perfect 2-colorings of Johnson graphs (*Russian*), Diskretn. Anal. Issled. Oper. **16** (5) (2009), 52–68.

[6] Avgustinovich S.V., Mogilnykh I.Yu. Perfect 2-colorings of Johnson graphs $J(6,3)$ and $J(7,3)$, Lect. Notes Comp. Sci. **5228** (2008), 11–19.

[7] Gavrilyuk A. L., Goryainov S. V. On Perfect 2-Colorings of Johnson Graphs $J(v,3)$, Journal of Combinatorial Designs **21** (6) (2013), 232–252.

[8] Gavrilyuk A. L., Mogilnykh I. Yu. Cameron-Liebler line classes in $PG(n,4)$, Des. Codes Cryptogr. (2013). (accepted)

Krasovsky Institute of Mathematics and Mechanics, Ekaterinburg, Russia,
Graduate School of Information Sciences, Tohoku University, Sendai, Japan,
Sobolev Institute of Mathematics, Novosibirsk, Russia
E-mail: alexander.gavriliouk@gmail.com

On generalized embedded subgroups of a finite group

Xiaoyu Chen, Wenbin Guo, A. N. Skiba

Recently, there are many researches of embedded subgroups (for example, n-embedded, S-embedded, weakly S-embedded, weakly τ-embedded, $\mathfrak{F}$-quasinormal, $\mathfrak{F}_n$-quasinormal, $\mathfrak{F}_s$-quasinormal, $\mathfrak{F}_n$-normal, $\mathfrak{F}_h$-normal, $\mathfrak{F}_s$-normal and so on). A problem naturally arises: *Whether one can give a notion which develops and unifies all the above concepts and related results* ?

In order to resolve the above problem, we introduce the notion of $\mathfrak{F}_\tau$-embedded subgroups as follows.

A function τ which assigns to each group G a set of subgroups $\tau(G)$ of G satisfying that $1 \in \tau(G)$ and $\theta(\tau(G)) = \tau(\theta(G))$ for any isomorphism $\theta : G \to G^*$ is said to be a *subgroup functor*. If $H \in \tau(G)$, then we say that H is a τ-subgroup of G.

Definition 1. Let τ be a subgroup functor. Then we say that τ is:

(1) *inductive* if for any group G, $HN/N \in \tau(G/N)$ whenever $H \in \tau(G)$ is a p-group and $N \trianglelefteq G$.

(2) *hereditary* if for any group G, $H \in \tau(E)$ whenever $H \in \tau(G)$ is a p-group and $H \leq E \leq G$.

(3) *regular* (*quasiregular*, respectively) if for any group G, whenever $H \in \tau(G)$ is a p-group and N is a minimal normal subgroup (a minimal abelian normal subgroup, respectively) of G, then $|G : N_G(H \cap N)|$ is a power of p.

(4) Φ-*regular* (Φ-*quasiregular*, respectively) if for any primitive group G, whenever $H \in \tau(G)$ is a p-group and N is a minimal normal subgroup (a minimal abelian normal subgroup, respectively) of G, then $|G : N_G(H \cap N)|$ is a power of p.

Definition 2. Let $\mathfrak{F}$ be a non-empty formation, τ a subgroup functor and H a subgroup of G. Let $\bar{G} = G/H_G$ and $\bar{H} = H/H_G$. Then we say that that H is $\mathfrak{F}_\tau$-*embedded* in G if for some quasinormal subgroup $\bar{T}$ of $\bar{G}$ and some τ-subgroup $\bar{S}$ of $\bar{G}$ contained in $\bar{H}$, $\bar{H}\bar{T}$ is S-quasinormal in $\bar{G}$ and $\bar{H} \cap \bar{T} \leq \bar{S}Z_{\mathfrak{F}}(\bar{G})$.

By using the above idea, we established the theory of generalized embedded subgroups, which develops and unifies all the above subgroups and related results.

Research is supported by a NNSF grant of China (grant #11371335) and Research Fund for the Doctoral Program of Higher Education of China (Grant 20113402110036).

Department of Mathematics, University of Science and Technology of China, Hefei, China, Department of Mathematics, Francisk Skorina Gomel State University, Gomel, Belarus
E-mail: jelly@mail.ustc.edu.cn, wbguo@ustc.edu.cnalexander.skiba49@gmail.com

Φ-isolators of finite groups

S. F. Kamornikov, O. L. Shemetkova, Yi Xiaolan

All groups considered in the paper are finite. We use standard definitions and notations from [**1, 2**].

Definition 1. *An element x of a group G is called Q-superfrattini if it satisfies one of the following two equivalent conditions:*

1) *each chief factor A/B of G for which $x \in A \setminus B$ is Frattini;*

2) *each chief factor of G having a form $< x^G > /B$ is Frattini.*

By definition, the identity element of G is Q-superfrattini.

Definition 2. *A subgroup H of a group G is called a Φ-isolator if it covers all Frattini chief factors and avoids all non-Frattini chief factors of G.*

A connection of Q-superfrattini elements with Φ-isolators is investigated.

Theorem. *For a group G, the following conditions hold:*

1) *any two Φ-isolators of G have the equal order;*

2) *if H is a Φ-isolator of G, then:*

a) *all elements of H are Q-superfrattini in G;*

b) *H is not contained properly in any subgroup of G whose elements are all Q-superfrattini in G;*

c) $Core_G(H) = \Phi(G)$;

d) *if $H \trianglelefteq G$, then $H = \Phi(G)$.*

In 1962 Gaschütz in [**3**] introduced the concept of the prefrattini subgroup of a finite soluble group. In the original presentation the prefrattini subgroup is defined as the intersection of complements of the crowns of all non-Frattini chief factors of a fixed chief series of the group.

By definition, every soluble group has at least one prefrattini subgroup. As shown in [**3**], each prefrattini subgroup covers all Frattini and avoids all non-Frattini chief factors of a soluble group G, i.e. it is a Φ-isolator of G.

Proposition 1. *Let H be a prefrattini subgroup of a soluble group G. Then all elements of H are Q-superfrattini in G.*

Proposition 2. *Let H be a Φ-isolator of a soluble group G. Then H is a prefrattini subgroup if and only if H permutes with every element of a Hall system of G.*

References

[1] Shemetkov L. A. Formations of Finite Groups. Moscow: Nauka, 1978.
[2] Doerk K., Hawkes T.O. Finite Soluble Groups. Berlin - New-York: Walter de Gruyter, 1992.
[3] Gaschütz W. Praefrattinigruppen // Arch. Math. 1962. Bd. 13, № 3. S. 418-426.

Gomel Branch of International University MITSO, Belarus, Russian Economic University, Moscow, Russia, Zhejiang Sci-Tech University, Hangzhou, China
E-mail: sfkamornikov@mail.ru, ol-shem@mail.ru, yixiaolan2005@126.com

On Π-property and Π-normality of subgroups of finite groups

Baojun Li

Let H be a subgroup of group G. H is said satisfying Π-property in G, if $|G/K : N_{G/K}(HK/K \cap L/K)|$ is a $\pi(HK/K \cap L/K))$-number for any chief factor L/K of G, and, if there is a subnormal supplement T of H in G such that $H \cap T \leq I \leq H$ for some subgroup I satisfying Π-property in G, then H is said Π-normal in G. These properties are essential properties satisfied by many subgroups which satisfy some known embedding property. Groups can be described when some primary subgroups are Π-normal, and many known results are generalized.

College of Applied Mathematics, Chengdu University of Information Technology, Chengdu (China)
E-mail: baojunli@cuit.edu.cn

A geometric interpretation of the infinite wreath powers of P. Hall

Vahagn H. Mikaelian

Wreath powers are one of the most elegant structures developed by P. Hall, and used to construct characteristically simple groups, verbally complete groups and other types of groups [**2, 3, 4**]. Although wreath powers are flexible constructions, they are not used as widely as many of other arguments of Hall due to their rather complicated structure. The aim of our recent work [**5**] is to suggest a simpler interpretation for wreath powers, since some of the analytical proofs of Hall can in easier manner be explained in geometrical terms. As an application of our approach we construct a group, which was already announced in [**1**, Remark 5.6] to answer the question: *Is there a 2-generator group* $G = \langle x, y\rangle$ *such that* G *is not soluble (and, thus, even not locally soluble), but the normal closure* $\langle x\rangle^G$ *of* x *in* G *is locally soluble?*

Here is the context in which existence of such a group was considered. [**1**] considers some "local-global" conditions in the sense that properties of a group G can be determined by its 2-generator subgroups and by normal closures of single elements in G. This is motivated by earlier result of Thompson [**6**], who proved that a finite group is soluble if and only if any of its 2-generator subgroup is soluble. [**1**] generalizes this and offers the notion of a *locally radical element* $x \in G$ (if $\langle x\rangle^{\langle x,y\rangle}$ is locally soluble for any $y \in G$) and the notion of a *globally radical element* $x \in G$ (if $\langle x\rangle^G$ is locally soluble). For such elements Problem 5.5 in [**1**] asks: *which are the groups in which every locally radical element is globally radical; which are the groups in which every radical element is globally radical; and which are the groups in which every locally radical element is a radical?* The 2-generator group we build in [**5**], also mentioned in [**1**, Remark 5.6], is in some sense a "minimal" example of a group G which is not locally soluble, but contains an element which is both locally radical and globally radical. This example shows that, unlike the case of finite groups, in the case of infinite groups the properties of locally radical and globally radical elements can be "very far" from the properties of the whole group.

References

[1] Guralnick R., Plotkin E., Shalev A., Burnside-type problems related to solvability, Internat. J. Algebra Comput. 17 (2007), no. 5–6, 1033Ц-1048.

[2] Hall P., Some constructions for locally finite groups, J. Lond. Math. Soc. 34, 305–319 (1959).

[3] Hall P., Wreath powers and characteristically simple groups, Proc. Camb. Philos. Soc. 58, 170–184 (1962).

[4] Hall P., On non-strictly simple groups, Proc. Camb. Philos. Soc. 59, 531-533 (1963).

[5] Mikaelian V. H., A Geometrical Interpretation of Infinite Wreath Powers, Algebra Discrete Math, accepted to publication, to appear in 2014.

[6] Thompson J., Non-solvable finite groups all of whose local subgroups are solvable, Bull. Amer. Math. Soc. 74 (1968) 383Ц437.

Yerevan State University, Yerevan (Armenia)
E-mail: v.mikaelian@gmail.com

Φ-Harmonic Functions on Discrete Groups and First ℓ^Φ-Cohomology

Roman Panenko

Inspired by works of Puls and Martin–Valette (see [**1**], [**2**] and [**3**]) on first L^p-cohomology of discrete groups and p-harmonic functions, we introduce by analogy the notion of the discrete Φ-Laplacian and prove a decomposition theorem for the space of Φ-Dirichlet functions, where Φ is an N-function belonging to the class $\Delta_2(0) \cap \nabla_2(0)$. According to the idea, we study the nonreduced and reduced first cohomology of a (finitely generated) discrete group G with coefficients in the left regular representation of G in the Orlicz space $\ell^\Phi(G)$ and show that if G contains an infinite normal amenable subgroup with infinite centralizer then the cohomology space $H^1(G, \ell^\Phi(G)) = 0$. We also prove a theorem about the triviality of the first cohomology space for a wreath product of two groups the first of which is nonamenable.

References

[1] Bourdon M., Martin F., and Valette A., Vanishing and non-vanishing for the first L^p-cohomology of groups, Comm. Math. Helv., **80** (2005), no. 2, 377–389.

[2] Martin F. and Valette A., On the first L^p-cohomology of discrete groups, Groups Geom. Dyn. **1** (2007), no. 1, 81–100.

[3] Puls M., The first L^p-cohomology of some finitely generated groups and p-harmonic functions, J. Funct. Anal. **237** (2006), no. 2, 391–40.

Sobolev Institute of Mathematics, Pr. Akad. Koptyuga 4, 630090, Novosibirsk, Russia
E-mail: panenkora@gmail.com

About Shunkov group center with one saturation condition

A. A. Shlyopkin, I.V. Sabodakh

The structure of periodic Shunkov Group center, saturated by full linear groups of dimension two on finite fields, was obtained in present work.

Group G is saturated by groups from the set X, if any finite subgroup K from G is contained in subgroup of group G, isomorphic to some group from X [**1**].

Let K be finite subgroup from G saturated by the set X. Define $X(K)$ as a set of all subgroups from G containing K and isomorphic to groups from X. In particular, if 1 is an unity subgroup from G, then $X(1)$ is the set of all subgroups of G isomorphic to groups from X [[**2**]].

We continue studies started in the articles: [**3, 4, 5**]. Define $\Im = \{GL_2(p^n)\}$, where p is fixed prime number and n varies. We proved the following result.

Theorem. *Let G be a periodic Shunkov group, saturated by the set $\Im$ and $K \in \Im(1)$. Then $Z(K) \subset Z(G)$ and $Z(G)$ is locally cyclic group.*

References

[1] Shlyopkin A.K., Shunkov groups, contains finite unsolvable subgroups A.K. Shlyopkin, Book of abstracts of the third international conference on algebra, Krasnoyarsk, (1993), 363.

[2] Kuznezov A.A., Filippov K.A., Groups, saturated by given set of groups, Siberian electronic mathematical reports, **8**(2011), 230-246.

[3] Panushkin D.N., Shunkov groups, saturated by direct products of different groups, phd dissertation - Krasnoyarsk, (2010), 66.

[4] Shlyopkin A.A., Periodic groups saturated by the groups $GL_2(p^n)$, book of abstracts of the international conference on algebra, Kyiv, Ukraine, (2012), 144.

[5] Shlyopkin A.A., About groups, saturated by the groups $GL_2(p^n)$, Journal of SibSAU, **1**(2013), 100-108.

Krasnoyarsk
E-mail: shlyopkin@gmail.com

A new infinite family of arc-transitive distance-regular covers of cliques with $\lambda = \mu$ related to Ree groups ${}^2G_2(q)$

L. Yu. Tsiovkina

Let Γ be a distance-regular graph of diameter 3 and let μ denote the number of common neighbours for any two vertices of Γ at distance 2. Recall that if graph Γ is antipodal then Γ is a r-fold cover of $(k+1)$-clique, Γ has intersection array $\{k, \mu(r-1), 1; 1, \mu, k\}$, and any two adjacent vertices of Γ have exactly $\lambda = k - 1 - \mu(r-1)$ common neighbours, where parameter k is the degree of graph Γ, see [**2**].

A graph is called arc-transitive (or edge-symmetric) if its automorphism group acts transitively on ordered pairs of adjacent vertices.

Arc-transitive antipodal distance-regular graphs of diameter 3 with $\lambda = \mu$ were described in [**1**]. In particular, in [**1**] there were found three new potential series of graphs corresponding to groups $Sz(q), U_3(q), {}^2G_2(q)$. The problem of the existence of one of those series of distance-regular graphs, which is related to groups $Sz(q)$, where $q = 2^{2a+1} > 2$, was positively settled by the author, and this was announced in [**3**].

In the present work we prove the existence of infinite series of distance-regular graphs related to groups ${}^2G_2(q)$, where $q = 3^{2a+1} > 3$, which is new.

The following theorem holds.

Theorem. *Let $G = {}^2G_2(q)$, where $q = 3^{2a+1} > 3$, and let $S \in Syl_3(G)$. Suppose that g is an involution of G not contained in $N_G(S)$ and let h be an involution contained in $N_G(S) \cap N_G(S)^g$. Let $H = S\langle h \rangle$ and let $\Gamma(G, H, HgH)$ denote the graph with vertex set $\{Hx \mid x \in G\}$ whose edges are the pairs $\{Hx, Hy\}$ such that $xy^{-1} \in HgH$. Then $\Gamma(G, H, HgH)$ is arc-transitive antipodal distance-regular graph with intersection array $\{q^3, q^3 - 2q^2 - 2q - 3, 1; 1, 2(q^2 + q + 1), q^3\}$.*

Acknowledgement. The research was supported by RFBR (project 13-01-00469), by the Program of the Division of Mathematical Sciences of RAS (project 12-T-1-1003), by the Joint Research Program of UB RAS with SB RAS (project 12-C-1-10018) and with NAS of Belarus (project 12-C-1-1009), and by a grant from the IMM of UB RAS for young scientists in 2013.

References

[1] Makhnev A. A, Paduchikh D. V., Tsiovkina L. Yu. Edge-symmetric distance-regular covers of cliques with $\lambda = \mu$. Dokl. Akad. Nauk, 448, №1 (2013), 22-26. (Russian)

[2] Brouwer A. E., Cohen A. M., Neumaier A. Distance-Regular Graphs. Berlin etc: Springer-Verlag, 1989.

[3] Tsiovkina L. Yu. On the existence of arc-transitive distance-regular covers of cliques with $\lambda = \mu$ related to Suzuki groups. Abstracts of the International Conference on Group Theory in Honor of the 70th Birthday of Professor V. D. Mazurov, http://www.math.nsc.ru/conference/groups2013/eng/prog.htm (2013).

Krasovsky Institute of Mathematics and Mechanics of UB RAS, Yekaterinburg
E-mail: l.tsiovkina@gmail.com

Exact structures on categories of locally convex spaces

Sven-Ake Wegner

The class of all locally convex spaces constitutes an example of a category which is not abelian but allows for the use of homological methods in an intuitive way, see e.g. Wengenroth (2003). This is due to the fact that the collection of all its kernel cokernel pairs forms an exact structure in the sense of Quillen (1973). Indeed, the latter category is even quasi-abelian, see e.g. Schneiders (1999) for a detailed exposition and Rump (2008) for comments on the history of this notion.

Unfortunately, many subcategories of the locally convex spaces are not quasi-abelian. In order to make such a subcategory accessible for homological methods it is necessary to determine an appropriate exact structure. In particular, this structure should fit into the framework of the analytic problem under consideration.

In this talk we review some recent results on the hierarchy of pre-abelian categories as well as on the existence of exact structures. We illustrate these results by examples arising from functional analysis.

Sobolev Institute of Mathematics, Novosibirsk (Russia) / University of Wuppertal, Wuppertal (Germany)
E-mail: wegner@math.uni-wuppertal.de

Spectrum of automorphic extensions of simple symplectic groups over fields of characteristic 2

M. A. Zvezdina

The *spectrum* of a finite group G denoted by $\omega(G)$ is the set of its element orders. Non-isomorphic groups are called *isospectral* if they have the same spectrum. We deal with the spectrum of automorphic extensions of simple symplectic groups over a field of characteristic 2. A. V. Vasil'ev formulated a problem in [**1**]:

Problem 17.36 *Two groups are called isospectral if they have the same set of element orders. Find all finite non-abelian simple groups G for which there is a finite group H isospectral to G and containing a proper normal subgroup isomorphic to G. For every simple group G determine all groups H satisfying this condition.*

It is easy to show that a group H must satisfy the condition $G < H \leq AutG$. In other words, the problem is to describe all the automorphic extensions H of a simple group G such that $\omega(H) = \omega(G)$ for every simple group G.

The main result is the following:

Theorem. *Let $G = Sp_{2n}(q)$, $n \geq 2$, $q = 2^k \geq 2$ be a finite simple symplectic group over a field of characteristic 2. If $G < H \leq \operatorname{Aut} G$, then $\omega(H) \neq \omega(G)$.*

The work was partially supported by RFBR grant 13-01-00505.

References

[1] Mazurov V. D. and Khukhro E. I. (editors), The Kourovka notebook. Unsolved problems in group theory. 1 7th. ed. – Novosibirsk: Russian Academy of Sciences Siberean Division, Sobolev Institute of Mathematics. 2010.

Novosibirsk state university
E-mail: maria.a.zvezdina@gmail.com

V. Секция «Теория колец»

$\mathbb{Z}S_n$-модули и целочисленные тождества

А. С. Гордиенко

Полиномиальные тождества и их числовые и теоретико-представленческие характеристики хорошо изучены в случае алгебр над полями характеристики 0. Однако тождества с целыми коэффициентами также находят своё применение в теории колец.

Оказывается, что, как и в случае алгебр над полями характеристики 0, изучение полилинейных тождеств колец с единицей может быть сведено к изучению их *собственных* тождеств, т.е. линейных комбинаций произведений длинных коммутаторов. В частности, зная факторы в рядах подмодулей $\mathbb{Z}S_n$-модулей полилинейных функций, представляемых собственными многочленами, можно, пользуясь аналогом правила Юнга (или Пиери), вычислить факторы в рядах подмодулей $\mathbb{Z}S_n$-модулей полилинейных функций, представляемых обычными многочленами.

Кроме того, существует связь между коразмерностями колец и коразмерностями алгебр. Эта связь позволяет доказать для колец без кручения аналог гипотезы Амицура, а для колец без кручения, имеющих единицу, "— аналог гипотезы Регева.

Даже в случае алгебр над полями известно лишь несколько примеров, в которых явно вычислены коразмерности и кохарактеры тождеств. Среди этих примеров "— алгебра Грассмана и алгебра верхнетреугольных матриц 2×2. В докладе будет показано, как вычислить коразмерности, базис тождеств, а также факторы в рядах подмодулей соответствующих $\mathbb{Z}S_n$-модулей полилинейных функций, представляемых обычными многочленами, для колец верхнетреугольных матриц 2×2 и бесконечнопорождённых алгебр Грассмана над коммутативными кольцами с единицей.

Работа поддержана грантами Fonds Wetenschappelijk Onderzoek — Vlaanderen Pegasus Marie Curie post doctoral fellowship (Бельгия) и РФФИ 13-01-00234a.

Список литературы

[1] Gordienko A. S., Janssens G. $\mathbb{Z}S_n$-modules and polynomial identities with integer coefficients. `arXiv:1307.0733v1 [math.RA] 2 Jul 2013`

Vrije Universiteit Brussel, Belgium
E-mail: alexey.gordienko@vub.ac.be

Существование PI-экспонент роста тождеств

М. В. Зайцев

Каждой алгебре A над полем F нулевой характеристики можно сопоставить целочисленную последовательность $c_n(A)$, называемую последовательностью коразмерностей тождеств (или просто последовательностью коразмерностей) алгебры A. Во многих случаях эта последовательность растет не быстрее экспоненциальной функции от n. Например, если $\dim A = d < \infty$, то $c_n(A) \le d^{n+1}$. Аналогичное ограничение выполняется для любой ассоциативной PI-алгебры. В конце 80-х годов прошлого века Амицур выдвинул гипотезу, что предел

$$\lim_{n\to\infty} \sqrt[n]{c_n(A)} \qquad (1)$$

существует и является целым числом для любой ассоциативной PI-алгебры. Эта гипотеза получила свое подтверждение в конце 90-х годов [**1**]. Позднее аналогичная гипотеза была подтверждена для широкого класса алгебр — конечномерных йордановых и альтернативных алгебр, алгебр Ли и ряда других. Однако в общем случае предел (1) может быть любым вещественным числом (см. [**2**]).

За последние десятилетия появилось большое число работ, в которых изучалось асимптотическое поведение последовательности $c_n(A)$. При этом основное внимание уделялось вопросу о существовании предела (1) и его возможных значениях для различных типов алгебр. Ни одного контрпримера к гипотезе существования предела (1) до сих пор не удавалось построить.

Главным результатом доклада является следующее утверждение.

Теорема. *Для любого вещественного числа $\alpha > 1$ существует алгебра A_α, такая, что*

$$\underline{\lim}_{n\to\infty} \sqrt[n]{c_n(A_\alpha)} = 1\ , \qquad \overline{\lim}_{n\to\infty} \sqrt[n]{c_n(A_\alpha)} = \alpha.$$

С основами теории коразмерностей тождеств линейных алгебр можно познакомиться в [**3**].

Список литературы

[1] Giambruno A., Zaicev M. Exponential codimension growth of P.I. algebras: an exact estimate // Adv. Math. 1999. 142. 221–243.

[2] Giambruno, A., Mishchenko, S., Zaicev, M. Codimensions of algebras and growth functions // Adv. Math. 2008. 217. 1027–1052.

[3] Giambruno A., Zaicev M. Polynomial Identities and Asymptotic Methods // Mathematical Surveys and Monographs. Vol. 122. Providence, RI: Amer. Math. Soc., 2005.

МГУ им. М.В. Ломоносова, Москва
E-mail: zaicevmc@mail.ru

Тождества векторных пространств, вложенных в ассоциативные алгебры

И. М. Исаев, А. В. Кислицин

Пусть F – некоторое поле, A – линейная (не обязательно ассоциативная) алгебра над полем F, E – подпространство алгебры A.

Пусть $F\langle X\rangle$ – свободная неассоциативная алгебра от множества порождающих X. Тождеством векторного пространства E называется неассоциативный полином $f(x_1, x_2, \ldots, x_n) \in F\langle X\rangle$ такой, что $f(e_1, e_2, \ldots, e_n) = 0$ в алгебре A для всех элементов $e_1, e_2, \ldots, e_n \in E$. Тождество $f(x_1, x_2, \ldots, x_n)$ является следствием множества тождеств $G = \{g_i(x_1, \ldots, x_{m_i})|i \in I\}$, если многочлен $f(x_1, x_2, \ldots, x_n)$ лежит в идеале алгебры $F\langle X\rangle$, порожденном многочленами, полученными из многочленов множества $G = \{g_i(x_1, \ldots, x_{m_i})|i \in I\}$ с помощью линейных замен переменных.

Обозначим через $\mathfrak{A}$ класс всех векторных пространств, вложенных в ассоциативные алгебры. Ясно, что векторное пространство E, являющееся подпространством некоторой алгебры A, лежит в этом классе, если E удовлетворяет всем тождествам вида $(uv)w = u(vw)$ для всех неассоциативных одночленов из $F\langle X\rangle$.

В настоящей работе доказано следующее утверждение:

Теорема. *Тождества класса $\mathfrak{A}$ векторных пространств, вложенных в ассоциативные алгебры, не следуют из конечного набора тождеств, выполняющихся в этом классе.*

Список литературы

[1] Исаев И. М., Кислицин А. В. О тождествах пространств линейных преобразований // Мальцевские чтения: тезисы докладов международной конференции по математике. 2010. http://www.math.nsc.ru/conference/malmeet/10/abstracts.pdf.

[2] Исаев И. М. Тождества векторных пространств и примеры конечномерных линейных алгебр, не имеющих конечного базиса тождеств // Мальцевские чтения: тезисы докладов международной конференции по математике. 2012. http://math.nsc.ru/conference/malmeet/12/malmeet_2012.pdf.

Алтайская государственная педагогическая академия, Барнаул
E-mail: isaev@uni-altai.ru, kislitsin@uni-altai.ru

О конечной базируемости тождеств некоторых классов векторных пространств

А. В. Кислицин

Пусть F – поле нулевой характеристики, A – ассоциативная алгебра над полем F, E – подпространство (не обязательно являющееся подалгеброй) алгебры A. Пусть $F[X]$ – свободная ассоциативная алгебра от множества порождающих X. Тождеством векторного пространства E называется многочлен $f(x_1, x_2, \ldots, x_n) \in F[X]$ такой, что $f(e_1, e_2, \ldots, e_n) = 0$ в алгебре A для всех элементов $e_1, e_2, \ldots, e_n \in E$. Если все тождества пространства E следуют из конечной совокупности тождеств E, то пространство E называют конечно базируемым. В противном случае говорят, что E – не конечно базируемое пространство.

В работе [**1**] доказано, что любое векторное пространство, вложенное в ассоциативно-коммутативную алгебру, имеет конечный базис тождеств. В [**2, 3**] показано, что векторные пространства $A_1 = \langle e_{11}, e_{12}\rangle_F$ и $A_2 = \langle e_{11}, e_{21}\rangle_F$, удовлетворяющие тождествам $[x, y]z = 0$ и $x[y, z] = 0$ соответственно, конечно базируемы. В то же время, векторное пространство, удовлетворяющее тождеству $x[y, u]v = 0$ может оказаться как конечно базируемым, так и не конечно базируемым [**2, 3, 4**].

В настоящей работе исследован вопрос конечной базируемости тождеств произвольных векторных пространств над полем нулевой характеристики, удовлетворяющих тождествам $[x, y]z = 0$ и $x[y, z] = 0$, а именно, доказаны следующие утверждения.

Теорема 1. *Векторное пространство V над полем F нулевой характеристики (вложенное в ассоциативную F-алгебру), удовлетворяющее тождеству $x[y, z] = 0$, имеет конечный базис тождеств.*

Теорема 2. *Векторное пространство V над полем F нулевой характеристики (вложенное в ассоциативную F-алгебру), удовлетворяющее тождеству $[x, y]z = 0$, имеет конечный базис тождеств.*

Список литературы

[1] Исаев И. М., Кислицин А. В. О тождествах векторных пространств, вложимых в ассоциативно-коммутативные алгебры // материалы I международной научно-практической конференции «Фундаментальные науки и образование» (Бийск, февраль 2012 г.). – Бийск: ФГБОУ ВПО «АГАО», 2012.

[2] Исаев И. М., Кислицин А. В. О тождествах пространств линейных преобразований // Мальцевские чтения: тезисы докладов международной конференции по математике. 2010. http://www.math.nsc.ru/conference/malmeet/10/abstracts.pdf.

[3] Кислицин А. В. О тождествах пространств линейных преобразований над бесконечным полем // Известия Алтайского государственного университета. – 2010. – № 1/2(65).

[4] Исаев И. М., Кислицин А. В. О вложениях бесконечно базируемых векторных пространств в конечно базируемые // Материалы 15-й региональной конференции по математике «МАК-2012» (Барнаул, июнь 2012 г.). – Барнаул: Изд-во АлтГУ, 2012.

Алтайская государственная педагогическая академия, Барнаул
E-mail: kislitsin@uni-altai.ru

Проектирования колец Галуа

С. С. Коробков

Все рассматриваемые в данном сообщении кольца предполагаются ассоциативными. Всюду ниже R и R^{φ} — кольца с изоморфными решетками подколец, а φ — решеточный изоморфизм (иначе – проектирование) кольца R на кольцо R^{φ}. Кольцо R^{φ} будем называть проективным образом кольца R. Одной из задач изучения решеточных изоморфизмов колец является получение описания проективных образов колец, принадлежащих конкретному классу колец $\mathbf{K}$. Другая задача заключается в нахождении колец из $\mathbf{K}$, изоморфных своим проективным образам (иными словами — нахождение колец, определяющихся своими решетками подколец). В данной работе в качестве $\mathbf{K}$ рассматривается класс колец Галуа. *Кольцом Галуа* называется кольцо $GR(p^n, m)$, изоморфное факторкольцу $K[x]/(f(x))$, где $K = Z/p^nZ$, p — простое число, $f(x)$ — неприводимый над K многочлен степени m и $(f(x))$ — главный идеал, порожденный многочленом $f(x)$ в кольце $K[x]$. Кольца Галуа играют важную роль в теории конечных колец. Свойства решетки подколец кольца Галуа зависят от значений чисел n и m. Наиболее простое строение решетка подколец L кольца $GR(p^n, m)$ имеет при $m = 1$ (L является цепью) и при $n = 1$ (L дистрибутивна). Только в этих случаях существуют примеры проектирований колец Галуа на кольца, не являющиеся кольцами Галуа. Доказана следующая теорема:

Теорема. *Пусть $R = GR(p^n, m)$, где $n > 1, m > 1$. Тогда $R^{\varphi} \cong R$.*

Решеточные изоморфизмы полей Галуа рассматривались в работе [**1**]. Описание колец, решетки подколец которых являются цепями, приведено в работе [**2**]. Сформулированная теорема обобщает результат автора, полученный ранее (см. [**3**]). Содержащиеся в работах [**1**] и [**2**] результаты вместе с приведенной теоремой дают полное решение указанных выше задач для класса колец Галуа.

Приведем два важных свойства решеточных изоморфизмов колец Галуа.

Предложение 1. *Пусть $R = GR(p^n, m)$, $n > 1$, $m > 1$ и e — единичный элемент кольца R. Тогда $\langle e\rangle^{\varphi} = \langle e'\rangle$, где e' — единичный элемент кольца R^{φ}.*

Предложение 2. *Пусть $R = GR(p^n, m)$, $n > 1, m > 1$. Тогда $(pR)^{\varphi} = pR^{\varphi}$.*

Список литературы

[1] Коробков С. С. Решеточные изоморфизмы конечных колец без нильпотентных элементов. Известия УрГУ. Математика и механика № 22, вып. 4. Екатеринбург, 2002. С. 81 – 93.

[2] Фрейдман П. А., Коробков С. С. Ассоциативные кольца и их решетки подколец. Исследование алгебраических систем по свойствам их подсистем. Сборник научных трудов. Ураль-ский гос. пед. ун-т, Екатеринбург, 1998. С. 4 – 45.

[3] Коробков С. С. О решеточных изоморфизмах колец Галуа. Международная алгебраическая конференция, посвященная 100-летию со дня рождения А.Г. Куроша. Тезисы докладов. М.: Изд-во механико-математического фак-та МГУ, 2008 г. С. 135.

Уральский государственный педагогический университет, Екатеринбург
E-mail: ser1948@gmail.com

О представлении некоторых конечных колец матрицами над коммутативными кольцами

А. Мекей, Л. Оюунцэцэг

В работе дано полное описание подпрямо неразложимых конечных ассоциативных колец нильпотентные элементы которых перестановочным. Основным результатом является теорема.

Теорема. Любое конечное ассоциативное кольцо, нильпотентные элементы которых перестановочным, представимо матрицами над коммутативным кольцом.

Список литературы

[1] Мальцев Ю. Н. О представлении конечных колец матрицами над коммутативным кольцом, Математический сборник, 1985, 128 (170), N 3 (11), 383-340.

[2] Ратинов В. А. Структура полусовершенных колец с коммутативным радикалом Джекобсона, Математический сборник, 1979, том 110(152), N 3(11), стр. 456-470.

[3] Нечаев А. А. Конечные кольца главных идеалов, Математический сборник, 1973, том 91(133), N 3(7), стр. 350-366.

[4] Raghavendran R. Finite associative ring, Compositio Mathematica, tome 21, No. 2, 1969, pp.195-229

[5] Wilson R. S. On the structure of finite rings II, Pacific.J.Math, 51, 1974, pp.317-325.

Алгебры Пуассона и алгебры Филиппова

А. П. Пожидаев

Пусть A — алгебра Пуассона $(A; \{\ ,\ \}, \cdot)$, где $\{\ ,\ \}$ — скобка Ли, $\cdot$ — ассоциативная коммутативная операция. Пусть D — линейное отображение на A (обозначим $D(a) = \bar{a}$). Определим на векторном пространстве алгебры A новую тернарную операцию правилом

$$[x, y, z] \quad = \quad \{x, y\} \cdot \bar{z} + \{z, x\} \cdot \bar{y} + \{y, z\} \cdot \bar{x}$$

для любых $x, y, z \in A$. Обозначим получившуюся тернарную алгебру через A_D.

Теорема 1. *Пусть* $(A; \{\ ,\ \}, \cdot)$ *— алгебра Пуассона с дифференцированием* D (*относительно обеих операций*) *и тождеством*

$$\{xy\}\{zu\} + \{zx\}\{yu\} + \{yz\}\{xu\} \quad = \quad 0.$$

Тогда $(A_D; [\ ,\ ,\ ])$ *является тернарной алгеброй Филиппова.*

Теорема 2. *Пусть* $(A; \{\ ,\ \}, \cdot)$ *— либо алгебра Пуассона над полем* F *характеристики* 2, *либо алгебра Пуассона с тождеством*

$$\{xy\}\{zu\} + \{zx\}\{yu\} + \{yz\}\{xu\} \quad = \quad 0.$$

Тогда $(A_D; [\ ,\ ,\ ])$ *является тернарной алгеброй Филиппова, если* D *— тождественное отображение на* A.

Теорема 3. *Пусть* $(A; \{\ ,\ \}, \cdot)$ *— алгебра Пуассона с тождествами*

$$\{ab\}\bar{c} + \{ca\}\bar{b} + \{bc\}\bar{a} = 0,$$
$$\{d\bar{c}\}\{ab\} + \{d\bar{b}\}\{ca\} + \{d\bar{a}\}\{bc\} = 0.$$

Тогда $(A_D; [\ ,\ ,\ ])$ *является тернарной алгеброй Филиппова.*

Работа частично поддержана фондом РФФИ (гранты 11-01-00938-а, 12-01-33031).

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

О структуре факторизаций линейных обыкновенных дифференциальных операторов в случае перестановочности всех факторов

А. В. Пургин

Рассматриваются факторизации в кольце линейных обыкновенных дифференциальных операторов (ЛОДО) с коэффициентами из поля рациональных функций $Q(x)$, [**1**] – [**2**]. Символом P будем обозначать линейный обыкновенный дифференциальный оператор $P = D^n + f_1(x)D^{n-1} + \ldots + f_n(x), \quad D = d/dx$, где $f_s(x)$ принадлежат полю $Q(x)$. Введем отношение частичного порядка на множестве всех правых делителей произвольного ЛОДО P следующим образом: пусть P_1 и P_2 — некоторые правые делители оператора P, будем говорить, что $P_1 \leqslant P_2$, если оператор P_1 является правым делителем оператора P_2. Частично упорядоченное множество правых делителей произвольного ЛОДО P является решеткой с операциями взятия точной нижней грани $\inf\{P_1, P_2\} = \mathrm{rGCD}(P_1, P_2)$ и точной верхней грани $\sup\{P_1, P_2\} = \mathrm{rLCM}(P_1, P_2)$, где $\mathrm{rGCD}(P_1, P_2)$ обозначает оператор, являющийся правым наибольшим общим делителем ненулевых операторов P_1 и P_2, а $\mathrm{rLCM}(P_1, P_2)$ — оператор, являющийся их правым наименьшим общим кратным. Пусть $P = P_1 \circ P_2 \circ \ldots P_i \circ P_{i+1} \circ P_{i+2} \circ \ldots \circ P_k$ — некоторая факторизация линейного обыкновенного дифференциального оператора P на неприводимые множители P_i. Для любого $i \in \{1, \ldots, k\}$ обозначим символом $\langle P_i \rangle$ следующий оператор: $\langle P_i \rangle = P_i \circ P_{i+1} \circ P_{i+2} \circ \ldots \circ P_k$ — именно он и является элементом решетки правых делителей оператора. Два (для простоты неразложимых) оператора P и Q будем называть перестановочными в произведении $P \circ Q$, если $P \circ Q = Q_1 \circ P_1$, $Q_1 \neq P, \quad P_1 \neq Q$[**1**]. Будем говорить, что у ЛОДО P все факторы перестановочны, если в любой факторизации оператора P для любых двух соседних правых делителей $\langle P_i \rangle$ и $\langle P_{i+1} \rangle$ операторы P_i и P_{i+1} перестановочны.

Теорема 1. *Пусть у оператора P все факторы перестановочны. Тогда существует факторизация*

$$P = P_1 \circ P_2 \circ \ldots \circ P_l \circ P_{k_{11}} \circ \ldots \circ P_{k_{1s_1}} \circ P_{k_{21}} \circ \ldots \circ P_{k_{2s_2}} \circ \ldots \circ P_{k_{r1}} \circ \ldots \circ P_{k_{rs_r}}$$

(в которой мы имеем l (где $l \geqslant 0$) попарно несходных факторов и r (где $r \geqslant 0$) множеств факторов, в каждом из которых все факторы сходные), и решетка L_P изоморфна прямому произведению l экземпляров **2** *и r экземпляров решеток $M_\infty^{k_i}$ подпространств k_i-мерных векторных пространств $(i = 1, \ldots, r)$.*

Список литературы

[1] Tsarev, S. P. An algorithm for complete enumeration of all factorizations of a linear ordinary differential operator. Proceedings of ISSAC'96 (1996), ACM Press, pp. 226–231.

[2] Абрамов С. А., Царев С. П. О периферийной факторизации линейных дифференциальных операторов.// Программирование, 1997, N 1, с. 59-67.

Красноярский Государственный Педагогический Университет, Красноярск
E-mail: pav1972@yandex.ru

Абелевы группы с инвариантными справа изометриями

А. Р. Чехлов

Мономорфизмы группы, сохраняющие p-высоты ее элементов будем называть ее *изометриями*. Будем говорить, что изометрии группы *инвариантны справа*, если для любых ее изометрий α, β найдется такая изометрия γ, что $\alpha\beta = \beta\gamma$. Автоморфизмы любой группы инвариантны справа; следовательно, к рассматриваемому классу групп относятся все группы, изометрии которых являются автоморфизмами.

Теорема 1. *Для делимой группы D эквивалентны следующие условия*:

(а) *ее изометрии инвариантны справа*;

(б) *любая ее изометрия является автоморфизмом*;

(в) *часть без кручения группы D, а также каждая ее p-компонента имеют конечный ранг.*

Теорема 2. *У нередуцированной группы $A = D \oplus G$, где D — делимая часть группы A, изометрии инвариантны справа тогда и только тогда, когда этим свойством обладают группы D и G.*

Теорема 3. *Для редуцированной p-группы A следующие условия* (а)–(в) *эквивалентны*:

(а) *изометрии группы A являются ее автоморфизмами*;

(б) *изометрии группы A инвариантны справа*;

(в) *A не имеет собственных чистых подгрупп, изоморфных самой группе A.*

Если к тому же группа A периодически полна, то каждое из условий (а)–(в) *равносильны тому, что все инварианты Ульма-Капланского группы A конечны.*

Теорема 4. *Для редуцированной вполне разложимой группы без кручения A следующие условия эквивалентны*:

(а) *изометрии группы A являются ее автоморфизмами*;

(б) *изометрии группы A инвариантны справа*;

(в) *множество типов всех прямых слагаемых ранга* 1 *группы A удовлетворяет условию максимальности и каждая однородная компонента группы A имеет конечный ранг.*

Теорема 5. *У редуцированной алгебраически компактной группы A изометрии инвариантны справа тогда и только тогда, когда A имеет строение $A = B \oplus G$, где B — алгебраически компактная группа, служащая алгебраически компактным замыканием периодической группы, каждая примарная компонента которой является периодически полной группой с конечными инвариантами Ульма-Капланского, а G — алгебраически компактная группа без кручения, каждая p-адическая компонента которой имеет конечный p-ранг.*

Томский госуниверситет, Томск
E-mail: cheklov@math.tsu.ru

Тернарные дифференцирования полупростых йордановых супералгебр над полем характеристики ноль

А. И. Шестаков

Тернарные дифференцирования, а также связанные с ними обобщенные дифференцирования изучались в различных классах алгебр, см. например [**1**] -[**6**]. В настоящей работе эта задача изучается для конечномерных йордановых супералгебр.

Пусть A — супералгебра над полем Φ, т. е. $A = A_0 + A_1$ — Z_2-градуированная Φ-алгебра.

Тройка (D, F, G) однородных линейных отображений $D, F, G \in \mathrm{End}(A)$ называется *тернарным дифференцированием* супералгебры A, если для любых $x, y \in A$ выполняется равенство

$$D(xy) = F(x)y + (-1)^{deg(x)deg(G)}xG(y).$$

Первая компонента D тернарного дифференцирования (D, F, G) называется также *обобщенным дифференцированием.* Понятие тернарного/обобщенного дифференцирования обобщает обычные дифференцирования при $D = F = G$, а также δ-дифференцирования при $F = G = \delta D$, $(\delta \in \Phi)$, см. например [**7**]-[**8**].

Заметим, что тройки отображений следующего вида, очевидно, являются тернарными дифференцированиями в любой супералгебре:

$$\Delta = (\phi + \psi + D^0,\ \phi + D^0,\ \psi + D^0), \tag{1}$$

где ϕ, ψ — произвольные элементы центроида супералгебры A, а D^0 — любое обыкновенное дифференцирование в A, т. е.

$$D^0(xy) = D^0(x)y + (-1)^{deg(x)deg(D^0)}xD^0(y),$$

при этом $deg\,\phi = deg\,\psi = deg\,D^0 = deg\,\Delta$. Назовем приведенные тернарные дифференцирования вида (1) — *стандартными.* Соответственно, определяются и стандартные обобщенные дифференцирования как главные компоненты стандартных тернарных дифференцирований.

Показано, что, за определенным исключением, всякое тернарное (обобщенное) дифференцирование в полупростых йордановых супералгебрах над алгебраически замкнутым полем характеристики ноль является стандартным. Исключение связано с простой супералгеброй невырожденной билинейной формы f, определенной на полностью нечетном двухмерном векторном пространстве V, т. е.

$$J(V, f) = \Phi \cdot 1 + V_0 + V_1 \quad \text{при} \quad V_0 = 0,\ V_1 = V, \quad dim\,V = 2. \tag{2}$$

Все четные дифференцирования данной супералгебры являются стандартными, а все нечетные дифференцирования находятся во взаимно однозначном соответствии с векторами из V, следующим образом:

$$\{\ \Delta_v \mid \Delta_v(1) = (v, \frac{v}{2}, \frac{v}{2}), \quad \Delta_v(x) = (\frac{f(x,v)}{2}, f(x,v), f(x,v))\ \forall\, x \in V\ \}_{v \in V}.$$

Это единственный случай простых йордановых супералгебр с нестандартными тернарными (обобщенными) дифференцированиями. Поэтому если полупростая йорданова супералгебра над алгебраически замкнутым полем характеристики ноль не содержит прямых слагаемых вида (2), то всякое тернарное(обобщенное) дифференцирование в ней является стандартным.

Работа поддержана грантом РФФИ 11-01-00938-а.

Список литературы

[1] Jimenez-Gestal C., Perez-Izquierdo J. M. Ternary derivations of finite-dimensional real division algebras. Linear Algebra Appl., 428 (2008), N. 8-9, 2192–2219.

[2] Bresar M. On the distance of the composition of two derivations to the generalized derivations. Glasgow Math. J. 33 (1991).

[3] Komatsu H., Nakajima A. Generalized derivations of associative algebras. Quaest. Math., 26 (2003), N. 2, 213–235.

[4] Leger G., Luks E. Generalized derivations of Lie Algebras. J. of Algebra, 228 (2000), 165–203.

[5] Zhang R., Zhang Y. Generalized derivations of Lie superalgebras. Comm. Algebra, 38 (2010), N. 10, 3737–3751.

[6] Шестаков А. И. Тернарные дифференцирования сепарабельных ассоциативных и йордановых алгебр, Сиб. матем. журн., 53:5 (2012), 1178–1195.

[7] Филиппов В. Т. О δ-дифференцированиях альтернативных первичных и мальцевских алгебр. Алгебра и Логика, 39 (2000).

[8] Желябин В. Н., Кайгородов И. Б. О δ-супердифференцированиях простых супералгебр йордановой скобки. Алгебра и Анализ, 23 (2011), N. 4, 40–58.

Новосибирский госуниверситет, г.Новосибирск
E-mail: shestalexy@yandex.ru

Quantizations of Kac—Moody algebras

V. K. Kharchenko

We analyze the extent to which a quantum universal enveloping algebra of a Kac-Moody algebra $\mathfrak{g}$ is defined by multidegrees of its defining relations. To this end, we consider a class of character Hopf algebras defined by the same number of defining relations of the same degrees as the Kac-Moody algebra $\mathfrak{g}$. We demonstrate that if the generalized Cartan matrix A of $\mathfrak{g}$ is connected then the algebraic structure, up to a finite number of exceptional cases, is defined by just one "continuous" parameter q related to a symmetrization of A, and one "discrete" parameter $\mathfrak{m}$ related to the modular symmetrizations of A. The Hopf algebra structure is defined by $n(n-1)/2$ additional "continuous" parameters. We also consider the exceptional cases for Cartan matrices of finite or affine types in more detail, establishing the number of exceptional parameters values in terms of the Fibonacci sequence.

FES-C UNAM, México; Sobolev IM, Novosibirsk, Russia
E-mail: vlad@unam.mx

On basic superrank for varieties of algebras

A. M. Kuz'min, I. P. Shestakov

The term "algebra" means an algebra over a field of characteristic 0. Let $\mathcal{V}$ be a variety of algebras and $\mathcal{V}_n$ be the subvariety of $\mathcal{V}$ generated by the free $\mathcal{V}$–algebra of rank n; then we have $\mathcal{V}_1 \subseteq V_2 \subseteq \cdots \subseteq \mathcal{V}_n \subseteq \cdots \subseteq \mathcal{V}$, where $\mathcal{V} = \bigcup_n \mathcal{V}_n$. Recall [**1**] that the *basic rank* $r_b(\mathcal{V})$ of the variety $\mathcal{V}$ is a minimal cardinal number n such that $\mathcal{V} = \mathcal{V}_n$. Let us denote by Assoc, Lie, Alt, Jord, Malc, Ralt, $\mathrm{Var}(-1,1)$, and SJord, respectively, the varieties of associative, Lie, alternative, Jordan, Malcev, right alternative, $(-1,1)$–algebras, and the variety generated by the special Jordan algebras. It is known that $r_b(\mathrm{Assoc}) = 2$ (A. I. Mal'cev [**1**]), $r_b(\mathrm{Lie}) = r_b(\mathrm{SJord}) = 2$ (A. I. Shirshov [**2**]), $r_b(\mathrm{Alt}) = \aleph_0$ and $r_b(\mathrm{Malc}) = \aleph_0$ (I. P. Shestakov [**3**]), $r_b\big(\mathrm{Var}(-1,1)\big) = \aleph_0$ (S. V. Pchelintsev [**4**]). The values $r_b(\mathrm{Jord})$ and $r_b(\mathrm{Ralt})$ are still unknown.

In order to have a certain finite analog of the basic rank for a given variety $\mathcal{V}$ in the case when $r_b(\mathcal{V})$ is infinite, one can consider a basic superrank. Briefly, *finite basic superrank* $r_s(\mathcal{V})$ of the variety $\mathcal{V}$ is a minimal (in the right side lexicographical order) pair (r_0, r_1) of nonnegative integers such that $\mathcal{V}$ can be generated by the Grassmann envelope $\mathrm{G}(\mathcal{A})$ of a convenient $\mathcal{V}$–superalgebra $\mathcal{A} = \mathcal{A}_0 \oplus \mathcal{A}_1$ (see [**5**]), where r_i is a number of generators of $\mathcal{A}$ that lie in $\mathcal{A}_i$ for $i = 0, 1$. In particular, if $\mathcal{V}$ has a finite basic rank, then by definition we have $r_s(\mathcal{V}) = \big(r_b(\mathcal{V}), 0\big)$.

The Kemer's theorem [**6**] implies that every variety of associative algebras possesses a finite basic superrank. Apparently, the solutions of the open finite basis problems for varieties of nearly associative algebras could be related with the studying of the conditions of finiteness of basic superrank for their subvarieties. Some results about finite basic superranks for varieties of Lie algebras were obtained by M. V. Zaitsev [**7**].

We prove that $r_s\big(\mathrm{Alt}^{(2)}\big) = (1,1)$, $r_s\big(\mathrm{Jord}^{(2)}\big) = (0,2)$, *and* $r_s\big(\mathrm{Malc}^{(2)}\big) = (1,1)$, where $\mathcal{V}^{(2)}$ denotes the subvariety of metabelian (solvable of step 2) algebras of $\mathcal{V}$. Observe that all these varieties have infinite basic rank. We also prove that the variety of all metabelian algebras does not have any finite basic superrank and, moreover, contains certain subvarieties of right alternative and right symmetric algebras that do not possess finite basic superranks. The work is supported by FAPESP 2010/51880–2.

References

[1] Mal'cev A. I. Algebraic systems, Posthumous edition. Die Grundlehren der mathematischen Wissenschaften, Band 192. Springer–Verlag, New York-Heidelberg, 1973. 317 pp.

[2] Zhevlakov K. A., Slin'ko A. M., Shestakov I. P., Shirshov A. I. Rings that are nearly associative. Academic Press, Inc., New York–London, 1982. 371 pp.

[3] Shestakov I. P. A problem of Shirshov, Algebra and Logic, 16:2 (1978), 153–166.

[4] Pchelintsev S. V. Nilpotency of the associator ideal of a free finitely generated $(-1,1)-$ring, Algebra and Logic, 14:5 (1976), 334–353.

[5] Shestakov I. P. Superalgebras and counterexamples, Sib. Math. Journal, 32:6 (1991), 1052–1060.

[6] Kemer A. R. Finite basis property of identities of associative algebras, Algebra and Logic 26:5 (1987), 362–397.

[7] Zaitsev M. V. A superrank of varieties of Lie algebras, Algebra and Logic 37:4 (1998), 223–233.

Institute of Mathematics and Statistics, University of Sao Paulo, Sao Paulo (Brazil)
E-mail: amkuzmin@ya.ru; ivan.shestakov@gmail.com

On finite rings with regular zero-divisor graphs

A. S. Kuzmina, Yu. N. Maltsev

The zero-divisor graph $\Gamma(R)$ of an associative ring R is the graph whose vertices are all nonzero zero-divisors (one-sided and two-sided) of R, and two distinct vertices x and y are joined by an edge iff either $xy = 0$ or $yx = 0$ [**1**].

In the present paper, we give full description of finite rings with regular zero-divisor graphs. Also, some properties of finite rings such that their zero-divisor graphs satisfy the Dirak's condition are proved.

Main results of this thesis are Theorem 1 and Theorem 2.

Theorem 1. *Let R be a finite ring. $\Gamma(R)$ is regular iff R satisfies one of following conditions:*

(1) $R^2 = (0)$;
(2) $R \cong GF(q) \oplus GF(q)$, *where $GF(q)$ is a field with q elements;*
(3) *R is a local ring with $J(R)^2 = (0)$, where $J(R)$ is the Jacobson radical of R.*

Theorem 2. *Let R be a non-zero finite ring without identity such that $\Gamma(R)$ satisfies the Dirak's condition and order of R is degree of a prime number p. Then $R^3 = (0)$. Moreover, $R^2 = (0)$ for $p > 3$.*

The work is supported by RFFI (grant 12-01-00329) and by RF Ministry of Education and Science via project 1.4311.2011.

References

[1] Redmond S. P. The zero-divisor graph of a noncommutative ring. Int.J.Commut.Rings (2002) 1(4), 203–211.

Altai State Pedagogical Academy, Barnaul
E-mail: akuzmina1@yandex.ru, maltsevyn@gmail.com

δ-derivations of semisimple finite-dimensional structurable algebras.

E. Okhapkina

The concept of δ-derivation first appeared in papers by V. Filippov, as a generalization of ordinary derivations. Recall that for a fixed δ of the main field F, under δ-derivation of algebra A we mean a linear mapping ϕ, which satisfies the condition

$$\phi(xy) = \delta(\phi(x)y + x\phi(y)) \tag{1}$$

for arbitrary elements $x, y \in A$. V. Filippov proved that every prime Lie algebra has no nonzero δ-derivations, if $\delta \neq -1, 0, \frac{1}{2}, 1$. The big cycle of articles according to the description of δ-derivations can be found in works of I. Kaygorodov such as δ-derivations of semisimple finite-dimensional Jordan algebras [**1**].

The class of structurable algebras was introduced in 1978 by B. Allison. This class of algebras is of interest because it contains such objects as tensor multiplication of composition algebras, a 35-dimensional algebra $T(C)$. Structurable algebras are algebras with the unit e and involution $^{-}$, which satisfy the identity:

$$[T_z, V_{x,y}] = V_{T_z x,y} - V_{x,T_{\overline{z}} y}, \text{ where } T_z, V_{x,y} \in End(A), \tag{2}$$
$$V_{x,y}(z) = (x\overline{y})z + (z\overline{y})x - (z\overline{x})y, T_z = V_{z,e} \text{ for } x, y, z \in A.$$

In the work [**2**] O. Smirnov proved that the whole class of simple finite-dimensional structurable algebras is isomorphic to six specific algebras like an unital associative algebra with the involution, the algebra of Hermitian form and some other. Jordan algebras with the unit and identical involution are also structurable, so we will receive the generalization of the results of I. Kaygorodov in more general (structurable) case.

Let us note that the linear mapping χ is called a generalized δ-derivation if it is related with δ-derivation ϕ by the following correlations

$$\chi(xy) = \delta(\chi(x)y + x\phi(y)) = \delta(\phi(x)y + x\chi(y)).$$

Now we can pass to the main results of this paper.

Theorem 1. *A semisimple finite-dimensional structurable algebra over an algebraically closed field of characteristic $p \neq 2, 3, 5$ has no nontrivial δ-derivations.*

Theorem 2. *Let χ be the generalized δ-derivation of the semisimple finite-dimensional structurable algebra A over an algebraically closed field of the characteristic $p \neq 2, 3, 5$, then $\chi \in Der(A) + \Gamma(A)$. Here $\Gamma(A)$ is centroid of A.*

References

[1] Kaygorodov I. On δ-derivations of simple finite-dimensional Jordan superalgebras, Algebra and Logic, 46 (2007), 5, 318–329.

[2] Smirnov O. Simple and semisimple structurable algebras, Algebra and Logic, 29 (1990), 5, 377–394.

Sobolev Institute of Mathematics Novosibirsk and Novosibirsk State University, Russia
E-mail: eliza_okhapkina@mail.ru

Alternative and Jordan algebras admitting derivations with invertible values

Yu. Popov

Let A be an algebra with unit element 1 over field F. By $U(A)$ We will denote the set of invertible elements of A. A nonzero derivation d of A is called a *derivation with invertible values*, if for every $x \in A$ we have $d(x) \in U(A)$ or $d(x) = 0$.

In 1983, Bergen, Herstein and Lanski initiated the study which purpose is to relate the structure of a ring to the special behavior of one of its derivations. Namely, in their article [**1**] they described associative rings with derivations with invertible values. They proved that such ring is either a division ring, or the ring of 2×2 matrices over a division ring, or a factor of a polynomial ring over a division ring of characteristic 2. Further, associative rings with derivations with invertible values (and their generalizations) were discussed in variety of works. Nevertheless, the problem of specification of algebras from classical non-associative varieties (such as alternative, Jordan, etc.), admitting derivations with invertible values, remains unconsidered. The purpose of our work is to make up this gap by generalizing the results of Bergen, Herstein and Lanski to alternative [**2**] and Jordan cases.

Theorem 1. *Let A be an alternative nonassociative algebra with unit element* 1*, admitting derivation with invertible values d. Then one of the following holds*:
1) *A is a Cayley–Dickson algebra over its center $Z(A)$;*
2) *A is a factor–algebra $C[x]/(x^2)$ of polynomial algebra over a Cayley–Dickson division algebra C of characteristic* 2.

Theorem 2. *Let J be a Jordan algebra of characteristic $\neq 2, 3$ with unit element* 1*, admitting derivation with invertible values d. Then one of the following holds*:
1) *J is an algebra $A^{(+)}$, where $A = D$ or D_2, D is an associative division algebra;*
2) *J is an algebra $H(A, *)$, where $A = D$ or D_2, D is an associative division algebra, or A is either F_4 or a central order in F_4, $* = Symp$;*
3) *J is an algebra of symmetric bilinear form $J(V, f)$ over field F that does not allow square root extraction;*
4) *J is an algebra of Albert type;*
5) *J is an extension of cases* 1) – 4) *by $M = \mathbf{P}(J)$ – the prime radical of J, $M \subseteq \ker d$, M is the largest ideal of J.*

For types of algebras presented in theorems, we also obtain the necessary and sufficient conditions for them to admit a derivation with invertible values.

References

[1] Bergen J., Herstein I. N., Lanski C. Derivations with invertible values, Canad. J. Math., 35 (1983), 2, 300–310.

[2] Kaygorodov I., Popov Y. Alternative algebras with invertible derivations // arXiv:1212.0615

Novosibirsk State University (Russia)
E-mail: yuri.ppv@gmail.com

On multiplicative length of Jordan algebras

S. Sverchkov

Let A be algebra over a field F of characteristic 0. We will denote by $R(A)$ the algebra of multiplications of A with the operators of right and left multiplications $R_a, L_a \in R(A)$. We will define a natural graduation on $R(A)$ by the length of words as follows

$$R(A)_k = l(\{M_{a_1} \dots M_{a_s} : s \leq k, a_i \in A, M \in \{R, L\}\}), \quad R(A) = \sum_{k=1}^{\infty} R(A)_k.$$

The minimal number $l_m(A) = k$, such that $R(A) \subseteq R(A)_k$, is called m-length of the algebra A. There are simple examples. Let $F[X_n]$, $F[X_n]$, be the absolutely free algebra and the free Jordan algebras with set of generators $X_n = \{x_1, \dots, x_n\}$. It is easily seen that $l_m(F[X_1]) = \infty$ and $l_m(J[X_1]) = 1$.

Let J be Jordan algebra with a basis $Y = \{f_\alpha, \alpha \in I\}$ over F. We will denote by $Ass[J]$ the free associative algebra with the set of generators Y. The universal multiplicative envelope of J will be denoted by $Um(J)$. Let I be the ideal of $Ass[J]$ generated by

$$abc + cba, \quad [a \cdot b, c] + [b \cdot c, a] + [c \cdot a, b]$$

for $a, b, c \in J$. We call $AUm(J) = Ass[J]/I$, the *associated algebra* of $Um(J)$.

Theorem 1. *Algebra $AUm(J[X_n])$ is nilpotent of index $2n+3$, i.e. in the algebra $AUm(J[X_n])$ the following identity is valid:*

$$\forall a_1, \dots, a_{n+2}, b_1, \dots, b_{n+1} \in J[X_n] \quad a_1 b_1 \dots a_{n+1} b_{n+1} a_{n+2} = 0.$$

Corollary. $l_m(Um(J[X_n])) \leq 2n+2$. *Equivalently, any n-generated Jordan algebra has m-length less then $2n+3$.*

By the results of [1], we can get a lower estimation of m-length of the free Jordan algebras.

Theorem 2. $2n - 1 \leq l_m(Um(J[X_n])) \leq 2n + 2$, for $n \geq 2$.

Supported by RFBR (Grant 11-01-00938-a)

References

[1] Sverchkov S. R., Varieties of special algebras, Comm. in Alg., http://www.tandfonline.com/toc/lagb20/current#.UntiYFRouXk, (1988) 1877–1919.

Russian Presidential Academy of National Economy and Public Administration, Siberian Branch, Novosibirsk, Russia
E-mail: sverchkovsr@yandex.ru

On alternators of free algebras

S. Sverchkov

Let $F[X]$ be an absolutely free algebra with the set of generators $X = \{x_1, \dots, x_n, \dots\}$ over a field of characteristic 0. We will denote by $M[X]$ the vector space of Malcev polynomials, i.e. the subalgebra of $F^{(-)}[X]$ generated by the set X with respect to commutator operation.

Set $(a \wedge b, c) = (a, b, c) + (b, a, c),\ c, a \wedge b) = (c, a, b) + (c, b, a),\ a, b, c \in F[X]$ for the associator $(a, b, c) = (ab)c - a(bc)$. We will denote by $Alt(F[X])$ the alternator ideal of the algebra $F[X]$, i.e. $Alt(F[X]) = id_{F[X]}((a \wedge b, c), (c, a \wedge b) \mid a, b, c \in F[X])$. The elements of $Alt(F[X])$ are called the alternators.

In 2004, Perez-Izquierdo and Shestakov [1] extended the famous Poincare-Birkho-Witt theorem from Lie algebras to Malcev algebras. For any Malcev algebra they constructed a universal nonassociative enveloping algebra, which inherits many properties of the universal associative enveloping algebras of Lie algebras. The properties of the alternators play an important role in their proof. We specify the structure of the alternator ideal of the algebra $F[X]$.

Theorem. $Alt(F[X]) = id_{F[X]}((a \wedge b, c), (c, a \wedge b), (a, b, c) \circ [a, b] \mid a, b, c \in F[X])$.

Supported by RFBR (Grant 11-01-00938-a)

References

[1] Perez-Izquierdo J. M., Shestakov I. P. An envelope for Malcev algebras, J. Algebra, 272 (2004) 379–393.

Russian Presidential Academy of National Economy and Public Administration,
Siberian Branch, Novosibirsk, Russia
E-mail: sverchkovsr@yandex.ru

VI. Секция «Теория моделей и универсальная алгебра»

Алгебраические системы в классе моделей счетного языка первого порядка

М. И. Бекенов

Пусть L — счетный язык первого порядка. Рассмотрим класс K_L всех бесконечных моделей языка L. T — теория языка L. T^M — множество всех моделей теории T. $A \prec B$ означает, что A — элементарная подмодель модели B.

Определение 1. *Пусть $\omega \leq \lambda \leq \mu$, A и B модели теории T языка L, $|A| = |B| = \mu$. Модели A и B назовем λ-подобными, если для любой модели $A' \prec A$ из $|A'| \leq \lambda$ следует $A' \prec B$ и для любой модели $B' \prec B$ из $|B'| \leq \lambda$ следует $B' \prec A$.*

Отношение λ-подобия является отношением эквивалентности. Таким образом, отношение $E_{\lambda\mu}$ разбивает множество моделей класса K на непересекающиеся классы λ-подобных моделей мощности μ.

В данной статье рассматривается отношение $E_{\mu\mu}$ в каждой мощности μ.

Факторизуем класс K_L по отношению $E_{\mu\mu}$, и будем говорить просто о b-подобии в каждой бесконечной мощности μ. Ограничимся рассмотрением картины для достаточно большого кардинала $\aleph$. Этот факторкласс обозначим через K_L^b. Отношение элементарной вложимости моделей естественно индуцирует частичный b-порядок на факторклассе K_L^b. Обозначим эту факторалгебраическую систему через $[K_L^b, \leq_b]$.

Существуют интересные связи подсистем этой алгебраической системы со свойствами соответствующих теорий классов моделей [**4**].

На этой факторалгебрической системе также естественно индуцируются ультрапроизведения по различным ультрафильтрам.

Пусть $s \in [K_L^b, \leq_b]$. Возьмем множество всех ультрастепеней элемента s и замкнем его относительно b-порядка. Полученную подсистему назовем B_s-деревом, порожденным элементом s. Таким образом, $[K_L^b, \leq_b]$ — множество различных непересекающихся B-деревьев.

Определение 2. *Подсистему K_1 системы $[K_L^b, \leq_b]$ назовем аксиоматизируемой, если существует теория T, у которой соответствующая алгебраическая система совпадает с K_1.*

Доказаны различные свойства об аксиоматизируемых подсистемах системы $[K_L^b, \leq_b]$.

Список литературы

[1] Ершов Ю. Л., Палютин Е. А., Математическая логика. М.: Наука, 1987.
[2] Кейслер Г., Чен Ч. Ч. Теория моделей. М.: Мир, 1977.
[3] Сакс Дж. Теория насыщенных моделей. М.: Мир, 1976.
[4] Бекенов М. И. Концепция подобия в теории моделей // Мальцевские чтения, Новосибирск, 2012.

Евразийский Национальный Университет им. Л.Н.Гумилева, Астана
E-mail: bekenov50@mail.ru

О группоидах отношений с операцией бинарной цилиндрофикации

Д. А. Бредихин

Множество бинарных отношений, замкнутое относительно некоторой совокупности Ω операций над ними, образует алгебру, называемую *алгеброй отношений*. Основы абстрактно-алгебраического подхода к изучению алгебр отношений были заложены в работах А.Тарского. Представляет интерес рассмотрение алгебр отношений с операциями, выразимыми через операции алгебр отношений Тарского. Такие алгебры называются редуктами алгебр отношений Тарского. Предметом нашего рассмотрения будут редукты с одной бинарной операцией, то есть группоиды бинарных отношений.

Важным классом операций над отношениями являются так называемые диофантовые операции. Операция называется диофантовой, если она может быть задана с помощью формулы, которая в своей предваренной нормальной форме содержит лишь операции конъюнкции и кванторы существования.

Сосредоточим свое внимание на следующей диофантовой операции над бинарными отношениями, определяемой формулой:

$$\rho * \sigma = \{(x, y) \in X \times X : (\exists z, w)(x, z) \in \rho \wedge (z, w) \in \sigma\}.$$

Отношение $\rho * \sigma$ представляет собой результат применения операции цилиндрофикации к произведению $\rho \circ \sigma$ бинарных отношений ρ и σ. По этой причине назовем ее операцией *бинарной цилиндрофикации*. Заметим, что эта операция может быть выражена через операции алгебр отношений Тарского и, следовательно, соответствующий группоид может быть рассмотрен как редукт алгебр отношений Тарского.

Обозначим через $Var\{\Omega\}$ — многообразие, порожденное классом алгебр отношений с операциями из Ω.

Теорема. *Группоид* $(A, \cdot)$ *принадлежит многообразию* $Var\{*\}$ *тогда и только тогда, когда он удовлетворяет тождествам* $(xy)x = xy$, $(xy)y = xy$, $(x^2y)z = (x^2z)y$, $(xy^2)z = x(y^2z)$ *и для каждого натурального* $k > 2$ *тождеству*

$$x_{i_1}(x_{i_2}\dots(x_{i_{k-1}}x_{i_k})\dots) = (x_{i_1}(x_{i_2}\dots(x_{i_{k-1}}x_{i_k})\dots)(x_{i_1}(x_{i_2}\dots(x_{i_{k-2}}x_{i_{k-1}})\dots).$$

Заметим, что приведенный в теореме базис тождеств является бесконечным. В связи с этим естественно возникает следующая проблема.

Проблема. *Является ли многообразие* $Var\{*\}$ *конечно базируемым?*

Саратовский технический университет, Саратов
E-mail: bredikhin@mail.ru

О богатых семействах типов в многосортных многозначных системах и кластеризации конечных типов и формул в логических исчислениях

А. А. Викентьев

Доклад посвящен *переносу и уточнению результатов теорем о богатых семействах типов,* доказанных ранее в стабильном случае или с условиями стабильности *на случай богатых семейств типов с параметрами для многосортных и многозначных 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.* Некоторые из доказанных ранее результатов 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, 70-летию акад. Ю.Л. Ершова и 60-летию чл.-к. РАН С.С. Гончарова.

Основными инструментами доказательств являются теоремы типа компактности, развитая техника современной теории моделей и стабильности, логических исчислений (Шелах, Лахлан, Балдвин, Пуаза, Пиллай, Хрушовский, Невельский, Бен Яков, Зильбер, Палютин, Судоплатов, Перетятькин, Морозов, Еримбетов, Кудайбергенов, Байжанов и многих др.) и наличия (даже локально) нужных компактных измеримых (подходящих мощностей $\varkappa$) моделей теории со свойствами $\varkappa$–отделимости над реализациями семейств стабильных (определимых) типов. Рассмотрены вопросы определимости систем в наследственно конечных надстройках, и о мощностях типово определимых подмножеств. Интерес к этим вопросам и моделям имеет прикладной характер в поиске наиболее информативных (сильно достоверных) типов, закономерностей для кластеризации, для упорядочения таких знаний с помощью привлечения упорядоченных или измеримых систем, для введения метрик на классах эквивалентных типов с помощью измеримых подклассов измеримых (метрических) моделей теории, необходимых для алгоритмов распознавания образов, поиска закономерностей, обнаружения редких событий и кластеризации многозначных знаний. Найдены различные методы кластеризации для множеств формул различных логик. Работа выполнена при финансовой поддержке РФФИ, проект № 11–07–00346а, кафедры ДМИ ММФ НГУ.

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

Кластеризация логических высказываний с учетом мер достоверностей

А. А. Викентьев, Р. А. Викентьев, Е. С. Кабанова

В работе рассматривается одна из актуальных задач — анализ логических высказываний. Мера значений истинности формулы на модели может служить степенью достоверности формулы. При анализе требуется найти близкие высказывания, выявить достоверные и т.д. Для кластеризации знаний, построения решающих функций на основе формул, надо ввести расстояние между формулами. В работе высказывания записаны в виде формул n-значной логики. С привлечением теории моделей определяются: новое расстояние между формулами:

$$\rho(\varphi,\psi)=\frac{1}{n^{|S(\Sigma)|}}\sum_{k=0}^{n-1}\sum_{l=0}^{n-1}\frac{|k-l|}{n-1}\,M\left(\frac{k}{n-1},\frac{l}{n-1}\right),$$

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 мера недостоверности:

$$I(\varphi)=\rho(\varphi,1)=\frac{1}{n^{|S(\Sigma)|}}\sum_{k=0}^{n-2}\frac{n-1-k}{n-1}\,M\left(\frac{k}{n-1}\right),$$

где $M\left(\frac{k}{n-1}\right)$ — количество моделей, на которых формула φ принимает значение $\frac{k}{n-1}$. В работе доказаны особые свойства метрики для расстояний и недостоверности; они учитывают многозначность, схожи со свойствами величин в случае 2, 3–значных логик Лукасевича, отвечают на вопросы Г.С.Лбова и применяются для алгоритмов кластеризации формул. Рассмотрены различные методы кластеризации знаний на основе новых расстояний и мер достоверности, а также коллективные решения. Работа выполнена при поддержке гранта РФФИ, проект 11-07-00346а, кафедры ДМИ ММФ НГУ.

Список литературы

[1] Лбов Г. С., Старцева Н. Г. Логические решающие функции и вопросы статистической устойчивости решений. Новосибирск: Изд-во Ин-та математики СО РАН, 1999.

[2] Кейслер Г., Чэн Ч. Ч. Теория моделей. М.: Мир, 1977.

[3] Викентьев А. А, Лбов Г. С. О метризации булевой алгебры предложений и информативности высказываний 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 СПб: Лань, 2004.

[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

Линейные над группой обратимые алгебры и ядра

С. С. Давидов

Бинарная алгебра $(Q;\Sigma)$ называется обратимой, если каждая операция из Σ квазигрупповая.

Обратимая алгебра $(Q;\Sigma)$ называется линейной, если существует группа $Q(+)$ такая, что любая операция A из Σ имеет вид:

$$A(x,y)=\varphi_A x+t_A+\psi_A y,$$

где $\varphi_A,\psi_A\in AutQ(+)$, а $t_A\in Q$. В [**1**] дана характеризация линейных обратимых алгебр с помощью формул второго порядка, а именно $\forall\exists(\forall)$-тождеств.

Имеется несколько понятий левого и правого ядра в квазигруппах (см. [**2, 3**]). Переходя от квазигрупп к обратимым алгебрам мы сталкиваемся с необходимостью рассматривать различные сверхтождества ассоциативности. Согласно [**4**], если в нетривиальной обратимой алгебре выполняется сверхтождество ассоциативности, то оно может быть только ранга два и одного из следующих видов:

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

В работе вводятся понятия ядер обратимой алгебры относительно каждого из приведенных выше сверхтождеств и исследуются их свойства для линейных над группой обратимых алгебр. Доказывается, что для линейных обратимых алгебр ядра, определенные относительно приведенных выше сверхтождеств, совпадают. Более того, имеет место следующая теорема.

Теорема *Обратимая алгебра линейна над группой тогда и только тогда, когда она совпадает со своим ядром.*

Список литературы

[1] Davidov S. S. A charactorization of binary invertible algebras linear over a group // Quasigroup and Related Systems, 2011, V. 19. P. 207–222.

[2] Белоусов В. Д. Основы теории квазигрупп и луп. М.: Наука, 1967.

[3] Белявская Г. Б. Ядра и центр квазигруппы // Мат. исследования, 102 (1988), Кишинев: Штиинца. С. 37–52.

[4] Мовсисян Ю. М. Введение в теорию алгебр со сверхтождествами. Ереван: Изд-во ЕГУ, 1986.

Ереванский Государственный Университет, Ереван
E-mail: davidov@ysu.am

Алгебраическая геометрия над дистрибутивными решетками

Ю. С. Дворжецкий

В работах Э.Ю. Данияровой, А.Г. Мясникова и В.Н. Ремесленникова [**1, 2**] по универсальной алгебраической геометрии доказаны две Объединяющие Теоремы в терминологии авторов, дающие 7 эквивалентных подходов к проблеме описания координатных алгебр (для систем без предикатных символов). В работе [**3**] все результаты и определения обобщаются для систем с предикатными символами. Данные теоремы применимы только к определённым классам алгебраических систем: классам $\mathbf{N}$ и $\mathbf{N}'$ — нётеровых и слабо нётеровых по уравнениям алгебр и классам $\mathbf{Q}$ и $\mathbf{U}$ — q_ω и u_ω компактных алгебр, соответствено. Чтобы применить результаты к определённой системе, нужно проверить, в каком из классов лежит рассматриваемая система.

А.Н. Шевляковым были доказаны критерии принадлежности булевых алгебр к классам $\mathbf{Q}$, $\mathbf{U}$, $\mathbf{N}$ и $\mathbf{N}'$ [**4**]. Также доказан критерий принадлежности к классу $\mathbf{N}$ для дистрибутивных решёток.

В докладе же будут показаны критерии нётеровости (класс $\mathbf{N}$) и слабой нётеровости (класс $\mathbf{N}'$) по уравнениям для алгебр Ершова и булевых алгебр с выделенным идеалом, рассматриваемых Пальчуновым в [**5**].

Теорема. *$\mathcal{C}$-алгебра Ершова $\mathcal{A}$ нётерова по уравнениям тогда и только тогда, когда подалгебра констант $\mathcal{C}$ конечна.*

Теорема. *Булева $\mathcal{C}$-решётка $\mathcal{B}$ с предикатом $P_I^{(1)}$ принадлежности к простому $\wedge$-идеалу $I \subseteq \mathcal{B}$ слабо нётерова по уравнениям тогда и только тогда, когда для любого множества констант $K \subseteq \mathcal{C}$ идеал $\{a \in \mathcal{B} | a \leq b, \forall b \in K\}$ конечно порождён константами из $\mathcal{C}$ или может быть представлен в виде пересечения идеала I и идеала, конечно порождённого константами из $\mathcal{C}$.*

Список литературы

[1] Daniyarova E., Myasnikov A., Remeslennikov V. Unification theorems in algebraic geometry // Algebra and Discrete Mathematics. 2008, № 1. P. 80–112.

[2] Daniyarova E., Myasnikov A., Remeslennikov V. Algebraic geometry over algebraic structuresIII: Equationally Noetherian Property and Compactness, Southeast Asian Bulletin of Mathematics. 2011, V. 35. P. 35–68. arXiv: 1002.4243.

[3] Daniyarova E., Myasnikov A., Remeslennikov V. Algebraic geometry over algebraic structures V: The case of arbitrary signature // Algebra and Logic. 2012, V. 51 №1. P. 28–40.

[4] Shevlyakov A. Algebraic geometry over Boolean algebras in the language with constants, arXiv: 1305.6844.

[5] Пальчунов Д. Е. О неразрешимости теорий булевых алгебр с выделенными идеалами // Алгебра и логика. 1986, Т. 25, № 3. С. 326–346.

Омский государственный университет им. Ф. М. Достоевского, Омск
E-mail: dvorzhetskij@mail.ru

О ядерных моделях сильно выпуклых позитивных робинсоновских теорий

А. Р. Ешкеев, О. И. Ульбрихт

Пусть T — произвольная Δ-R-теория в языке сигнатуры σ. Пусть C — семантическая модель теории T, $A \subseteq C$. Пусть $\sigma_\Gamma(A) = \sigma \cup \{c_a | a \in A\} \cup \Gamma$, где $\Gamma = \{g\} \cup \{c\} \cup \{P\}$. Рассмотрим следующую теорию $T_\Gamma^{PgM}(A) = Th_{\forall^+}(C,a)_{a\in A} \cup \{g(a) = a | a \in A\} \cup g(c) \cup T_g \cup \{P(c)\} \cup \{"P \subseteq "\}$, где T_g выражает тот факт, что для любой модели $(M, g^M) \models T_g$ имеет место:

1) g^M — автоморфизм M;

2) $\{m \in M | g^M(m) = m\}$ есть универсум некоторой экзистенциально замкнутой подмодели M, для любой модели M сигнатуры σ.

Для предиката P мы записываем выражение $\{"P \subseteq "\}$, что по своей сути есть бесконечное множество предложений, которое говорит, что интерпретация символа P есть позитивно экзистенциально замкнутая подмодель в сигнатуре σ. В силу неполноты мы не записываем точную связь между элементами $\Gamma = \{g\} \cup \{c\} \cup \{P\}$, но предполагается их согласованность в рамках теории $T_\Gamma^{PgM}(A)$.

Эта теория необязательно полная. Рассмотрим все пополнения центра T^* теории T в новой сигнатуре σ_Γ, где $\Gamma = \{c\}$. В силу Δ-R-ности теории T^* существует её центр, и мы обозначим его как T^c.

В рамках вышеуказанных определений и в обогащенной сигнатуре мы имеем следующие результаты.

Пусть $\Delta = B^+(At)$.

Предположение о некоторой полноте рассматриваемой теории необходимо в связи с следующим фактом.

Лемма. *В случае позитивной робинсоновской теории из позитивной экзистенциальной полноты следует Δ-JEP, обратное неверно.*

Теорема 1. *Пусть T — Δ-R-совершенная йонсоновская сильно выпуклая теория и она позитивно экзистенциально полна.*

Тогда следующие условия эквивалентны:

1) теория T^* имеет ядерную структуру;

2) теория T^c имеет ядерную модель;

3) всякий раз, когда $\varphi(x)$ есть позитивно-экзистенциальная формула, выводимая в T, существует некоторая позитивно-экзистенциальная формула $\psi(x)$ и целое число n такие, что в T выводимо $\exists^{=n} x\varphi \wedge \exists x(\varphi \wedge \psi)$, а также если $\mathrm{T} \models (\delta_1 \vee \delta_2)$, где δ_1, δ_2 — некоторые экзистенциальные предложения, то $\mathrm{T} \models \delta_1$ или $\mathrm{T} \models \delta_2$.

Теорема 2. *Пусть T — Δ-R-сильно выпуклая теория и она совершенная йонсоновская, причем она позитивно экзистенциально полна. Тогда M является ядерной структурой T^* тогда и только тогда, когда M является ядерной моделью центра T^* в вышеуказанном обогащении.*

Карагандинский государственный университет имени академика Е.А.Букетова, РГКП “Институт прикладной математики” КН МОН РК, Караганда
E-mail: modth1705@mail.ru, ulbrikht@mail.ru

О решетках квазимногообразий

А. Замойска-Дженио, М. В. Швидефски

А. М. Нуракунов показал, что существует квазимногообразие $\mathbf{K}$ унаров (алгебр с одной унарной операцией), такое что множество (с точностью до изоморфизма) конечных подрешеток его решетки квазимногообразий $Lq(\mathbf{K})$ невычислимо. Хорошо известно, что класс всех унаров является Q-универсальным. Основываясь на этом результате А. М. Нуракунова, а также на результатах В. А. Горбунова о решетках квазимногообразий и А. В. Кравченко о квазимногообразиях графов, мы показываем, что класс $\mathbf{K}(\sigma)$ всех систем сигнатуры σ Q-универсален тогда и только тогда, когда существует класс $\mathbf{K} \subseteq \mathbf{K}(\sigma)$, такой что множество конечных подрешеток его решетки квазимногообразий $Lq(\mathbf{K})$ невычислимо. Попутно мы устанавливаем несколько интересных фактов, касающихся решеток конгруенций (например, что любая конечная решетка изоморфна решетке относительных конгруенций некоторого конечного графа).

В связи с этим интересно было бы найти ответы на такие вопросы: верно ли, что для любого Q-универсального класса $\mathbf{K}'$ существует подкласс $\mathbf{K} \subseteq \mathbf{K}'$, такой что множество конечных подрешеток его решетки квазимногообразий $Lq(\mathbf{K})$ невычислимо? существует ли не Q-универсальный класс $\mathbf{K}'$ с таким свойством?

Нами установлено, что для класса всех дифференциальных группоидов ответ на первый вопрос положителен.

Варшавская Политехника, Варшава
E-mail: A.Zamojska-Dzienio@mini.pw.edu.pl
Институт математики им. С. Л. Соболева СО РАН, Новосибирский государственный университет, Новосибирск
E-mail: udav17@gmail.com

Алгебры унарных мультиопераций

А. С. Казимиров, Н. А. Перязев

Алгебраический подход к изучению функциональных систем впервые был предложен А.И. Мальцевым [**1**]. Введем в рассмотрение следующий класс алгебр, который связан с суперклонами [**2**].

Пусть $B(A)$ — множество всех подмножеств A. Отображение из A в $B(A)$ называется унарной мультиоперацией на A. Для множества всех унарных мультиопераций на A используем обозначение M_A^1.

Пусть $S \subseteq M_A^1$. Алгебра $\mathfrak{F} =< S; *, \cap, \mu, \varepsilon, \theta, \pi >$ типа $\langle 2,2,1,0,0,0\rangle$ 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:

$(f * g)(a) = \{b \mid \text{существует } c \in g(a) \ \text{ такой, что } b \in f(c)\}$;
$(f \cap g)(a) = f(a) \cap g(a)$;
$(\mu f)(a) = \{b \mid a \in f(b)\}$;
$\varepsilon(a) = \{a\}$; $\theta(a) = \varnothing$; $\pi(a) = A$.

При A — двухэлементном множестве имеется 19 алгебр унарных мультиопераций. Среди них 3 максимальных, 4 минимальных.

При A — трехэлементном множестве имеется 2079040 алгебр унарных мультиопераций. Из них максимальных – 46, минимальных – 16. Количественное распределение алгебр по мощности минимального базиса приведено ниже:

Размер базиса	Количество алгебр
1	266
2	10830
3	92619
4	314466
5	570519
6	596809
7	357138
8	116418
9	18676
10	1275
11	24

Работа выполнена при поддержке РФФИ, проекты № 12-01-00351, № 13-01-00621.

Список литературы

[1] Мальцев А. И. Итеративные алгебры Поста. / А.И. Мальцев // Новосибирск, 1976. — 100 с.
[2] Перязев Н. А. Суперклоны и клоны / Н. А. Перязев // Международная конференция "‘Мальцевские чтения"’. Тезисы докл. — Новосибирск, 2009. — С.164.

Восточно-Сибирская государственная академия образования, г. Иркутск.
E-mail: a.kazimirov@gmail.com, nikolai.baikal@gmail.com

Свойство расширения как квазитермальные условия Мальцева

А. М. Нуракунов

Пусть $\mathbf{R}$ – квазимногообразие алгебр конечной сигнатуры и $A \in \mathbf{R}$. Конгруэнция θ на алгебре A называется $\mathbf{R}$-*конгруэнцией*, если $A/\theta \in \mathbf{R}$. Через $Cg_R(X)$ обозначим наименьшую $\mathbf{R}$-конгруэнцию, содержащую множество X, $X \subseteq A \times A$.

Квазимногообразие $\mathbf{R}$ имеет *свойство расширениях*, если $Cg_{\mathbf{R}}(\alpha \cap \beta) = Cg_{\mathbf{R}}(\alpha) \cap Cg_{\mathbf{R}}(\beta)$ для любых $\alpha, \beta \in ConA$, $A \in \mathbf{R}$. Формула первого порядка на языке клонов вида $\exists(\wedge atomics \to atomic)$ называется *квазитермальным условием Мальцева.* Говорим, что квазимногообразие $\mathbf{R}$ удовлетворяет сильным квазитермальным условиям Мальцева, если клон операций любой алгебры из $\mathbf{R}$ удовлетворяет этим условиям. В работе мы покажем, что квазимногообразие $\mathbf{R}$ имеет свойство расширений тогда и только тогда, когда $\mathbf{R}$ удовлетворяет множеству сильных квазитермальных условий Мальцева специального вида.

Институт теоретической и прикладной математики НАН КР, Бишкек, Кыргызстан
E-mail: a.nurakunov@gmail.com

Максимальные в одной последовательности мультиклоны

В. И. Пантелеев

Пусть A — конечное множество, содержащее k элементов, n-местной мультифункцией на множестве A называется отображение $f : A^n \to 2^A$, а n-местной мультипроекцией — отображение $e_n^i : (x_1, ..., x_n) \to \{x_i\},\ 1 \leq i \leq n$.

Суперпозиция $f(f_1(x_1, ..., x_n), ..., f_m(x_1, ..., x_n))$ определяет мультифункцию $h_1(x_1, ..., x_n)$ следующим образом:

$$h_1(a_1, ..., a_n) = \bigcup_{b_i \in f_i(a_1, ..., a_n)} f(b_1, ..., b_m).$$

Мультиклоном называется множество мультифункций, содержащее все мультипроекции и замкнутое относительно суперпозиции. Замыкание множества мультифункций и максимальные мультиклоны определяются обычным образом.

В докладе приводятся примеры максимальных мультиклонов и фрагменты решетки всех мультиклонов.

В частности, справедлив следующий результат.

Пусть m-местный предикат G_m $(m \geq 1)$ определяется следующим образом: G_m состоит из всех наборов $(\alpha_1, ..., \alpha_m)$ длины m таких, что либо для некоторого $i \in \{1, ..., m\}$ выполняется $\alpha_i = \varnothing$ либо для всех $i \in \{1, ..., m\}$ выполняется $\alpha_i \in A$ и при этом $\alpha_i \neq \alpha_j$ если $i \neq j$.

Пусть F_m — множество мультифункций, сохраняющих предикат G_m. Известно, что F_m — мультиклон, F_k — максимальный мультиклон. Для остальных значений m $(1 \leq m < k)$ справедливо:

Теорема 1) *F_m содержится в F_{m+1};*
2) *F_m — максимальный мультиклон в F_{m+1}.*

Работа выполнена при поддержке РФФИ, проекты № 13-01-00621, № 12-01-00351.

Восточно-Сибирская государственная академия образования, Иркутск
E-mail: vl.panteleyev@gmail.com

Подпрямо неразложимые базисные алгебры

А. Пинус, И. Хайда, Р. Халаш

Понятие базисной алгебры было введено в работах [**1**]–[**3**] как обобщение MV-алгебр (алгебраической структуры, связанной с аксиоматизацией многозначной логики Лукасевича) и ортомодулярных решеток (такой же структуры, связанной с аксиоматизацией логики квантовой механики). Подробнее о базисных алгебрах см. [**4**]. Существует стандартная процедура ([**4**]), сопоставляющая базисной алгебре частично упорядоченное множество с наименьшим элементом и самодвойственными его главными фильтрами. Верно и обратное: любому подобному множеству, с фиксированными антиизотонными биекциями на себя его главных фильтров, соответствует некоторая базисная алгебра. При этом базисная алгебра называется линейной, если это частично упорядоченное множество линейно.

Имеют место следующие утверждения.

Теорема 1 (GCH). *Для любого бесконечного кардинала k существуют плотные как коммутативные, так и не коммутативные, как подпрямо неразложимые, так и подпрямо разложимые линейные базисные алгебры мощности k плотного порядкового типа.*

Теорема 2. *Для любого бесконечного кардинала k существует, по крайней мере k^+ подпрямо неразложимых линейных, рассеянных попарно неизоморфных MV-алгебр мощности k.*

Теорема 3. *Для любого бесконечного кардинала k существует, по крайней мере k^+ подпрямо неизоморфных, рассеянных, подпрямо неразложимых не коммутативных базисных алгебр мощности k.*

Список литературы

[1] Chajda I., Halash R., Kuhr J. Semilattice structures. Lempo: Heldermann Verlag, 2007.

[2] Chajda I., Halash R., Kuhr J. Many-valued quantum algebras // Alg. univ. 2009, V. 60. P. 63–90.

[3] Chajda I., Kolarik M. Indepedence of axsiom system of basic algebras // Soft computing. 2009, V. 13. P.41–43.

[4] Chajda I. Basic algebras and their applications, an overview // Contributions to General Algebra, 20. Klagenfurt: Verlag J.Heyn, 2011.

Новосибирский государственный технический университет, Новосибирск
E-mail: ag.pinus@gmail.com
Оломоуцкий университет, Оломоуц
E-mail: ivan.chajda@upol.cz, radomir.halas@upol.cz

О группах матриц с нестандартным умножением

А. А. Симонов

Кольцо квадратных матриц $M_n(R)$ над полем или кольцом R естественным образом появляется как группа автоморфизмов векторов или модулей над R. Умножение матриц строится при помощи билинейной функции

$$f^{(1)}(x_1,\dots,x_n,y_1,\dots,y_n)=\sum_{i=1}^{n}x_iy_i.$$

Возникает естественный вопрос о возможности построения умножения матриц при помощи функции $f : R^n \times R^n \to R$ отличной от билинейной. В теории физических структур [**1**] возникает решение, приводящее к группе матриц с умножением

$$f^{(2)}(x_1,\dots,x_n,y_1,\dots,y_n)=\sum_{i=1}^{n-1}(x_i-x_n)(y_i-y_n)+x_n+y_n.$$

Можно рассмотреть более общий случай, когда в качестве f–умножения двух матриц $A=(a_{ij})$ и $B=(b_{jk})$ рассматривается матрица $C=(c_{jk})$, построенная при помощи функции

$$f:\widehat{R^n\times R^m}\to R.$$

Функция f определена на подмножестве $\widehat{R^n\times R^m}\subset R^n\times R^m$. Будем рассматривать перемножения матриц одного размера — $m\times n$. В результате умножения матриц A и B получается матрица C с элементами:

$$c_{ij}=f(a_{i1},a_{i2},\dots,a_{in},b_{1j},b_{2j},\dots,b_{mj}).$$

Лемма. *Если число строк и столбцов не равно* 1, *то умножение матриц можно записать при помощи f^n-умножения матриц-столбцов или f^m-умножения матриц-строк.*

Физическую структуру ранга $(m+1,n+1)$ можно определить как частичную многосортную алгебру $\langle\mathfrak{M},\mathfrak{N},R;f,g\rangle$, где

$$f:\mathfrak{M}\times\mathfrak{N}\to R,\ g:R^{m+mn+n}\to R$$

— частичные операции с некоторыми дополнительными условиями.

Теорема. *Категория физических структур $\overrightarrow{K}\langle R^n,R^m,R;f,g\rangle$ и категория f-умножения матриц эквивалентны.*

Список литературы

[1] Кулаков Ю. И. О теории физических структур // Краевые задачи математической физики и смежные вопросы теории функций. 15, Зап. научн. сем. ЛОМИ, 127, Изд-во “Наука”, Ленинград. отд., Л., 1983. С. 103–151.

Новосибирск
E-mail: Andrey.Simonoff@gmail.com

Моноиды с аксиоматизируемым классом инъективных полигонов над группой

А. А. Степанова, П. А. Заморова

В работах [**1, 2**] приводится описание моноидов S, класс плоских, проективных, свободных и регулярных S-полигонов над которыми аксиоматизируем. В данной работе решена задача описания группы S, над которым класс инъективных S-полигонов аксиоматизируем.

Для формулировки данного результата напомним некоторые понятия и утверждения из теории моделей и теории полигонов (см. [**3, 4**]). Под правым S-полигоном A_S над моноидом S (или просто S-полигоном) понимается множество A, на котором моноид S действует справа, причем единица S действует тождественно. Пусть S — группа, A_S — правый S-полигон. Элемент $\theta \in A_S$ называется нулем полигона A_S, если $\theta \cdot s = \theta$ для любого $s \in S$. Правый S-полигон Q_S называется инъективным, если для любого правого S-полигона A_S, любого мономорфизма $\imath\colon A_S \to B_S$, где B_S — правый S-полигон, и для любого гомоморфизма $f\colon A_S \to Q_S$ существует гомоморфизм $f'\colon B_S \to Q_S$ такой, что $f = f' \circ \imath$. Класс инъективных правых S-полигонов обозначается Inj.

Утверждение [**3**]. *Пусть S — группа. Правый S-полигон A_s инъективен тогда и только тогда, когда в A_s существует нуль.*

Класс K структур языка L называется аксиоматизируемым (см. [**4**]), если существует множество предложений Σ языка L такое, что структура A принадлежит классу K тогда и только тогда, когда каждое предложение из Σ истинно в A.

Теорема. *Пусть S — группа. Класс Inj инъективных правых S-полигонов аксиоматизируем тогда и только тогда, когда S является конечно порожденной группой.*

Работа выполнена при поддержке РФФИ, проект 12-01-00460-а.

Список литературы

[1] Гоулд В., Михалёв А. В., Палютин Е. А., Степанова А. А. Теоретико-модельные свойства свободных, проективных и плоских s-полигонов // Фундаментальная и прикладная математика. 2008, Т. 14, № 7. С. 63–110.

[2] Михалёв А. В., Овчинникова Е. В., Палютин Е. А., Степанова А. А. Теоретико-модельные свойства регулярных полигонов // Фундаментальная и прикладная математика. 2004. Т. 10, № 4. С. 107–157.

[3] Kilp M., Knauer U., Mikhalev A. V. Monoids, Acts and Categories. Walter De Gruyter. Berlin, New York, 2000.

[4] Кейслер Г., Чен Ч. Теория моделей. М.: Мир, 1977.

Дальневосточный федеральный университет, Владивосток
E-mail: stepltd@mail.ru, korovka_07@mail.ru

Об одном максимальном частичном ультраклоне ранга 2

Т. Ю. Халбашкеева

В работе рассматривается система мультифункций ранга 2 с операцией суперпозиции, определенной в [**1**].

Пусть $E_2 = \{0, 1\}$. Мультифункцией ранга 2 называется отображение вида $f : E_2^n \to 2^{E_2}$. Множество всех мультифункций ранга 2 обозначается $P_2^{\widetilde{*}}$.

Пусть $f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)$, $f(x_1, \dots, x_m) \in P_2^{\widetilde{*}}$.

Суперпозиция $f(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n))$ определяет мультифункцию $g(x_1, \dots, x_n)$ следующим образом:
для любого набора значений переменных $(\alpha_1, \dots, \alpha_n) \in {E_2}^n$

$$g(\alpha_1, \dots, \alpha_n) = \begin{cases} \bigcap\limits_{\beta_i \in f_i(\alpha_1, \dots, \alpha_n)} f(\beta_1, \dots, \beta_m), & \text{если пересечение не пусто;} \\ \bigcup\limits_{\beta_i \in f_i(\alpha_1, \dots, \alpha_n)} f(\beta_1, \dots, \beta_m), & \text{иначе.} \end{cases}$$

Данное определение фактически позволяет находить значение мультифункции $f(x_1, x_2, \dots, x_n) \in P_2^{\widetilde{*}}$ на наборе $(\gamma_1, \gamma_2, \dots, \gamma_n) \in {2^{E_2}}^n$. На наборах, содержащих $\varnothing$, мультифункция обязательно принимает значение $\varnothing$, на остальных наборах значение мультифункции вычисляется в соответствии с описанием.

Частичным ультраклоном называется множество мультифункций, содержащее все проекции и замкнутое относительно суперпозиции. Частичный ультраклон U называется максимальным в некотором классе K, если из $U \subseteq K_1 \subseteq K$, где K_1 – частичный ультраклон, следует $U = K_1$ или $K_1 = K$.

Ставится вопрос поиска максимальных в $P_2^{\widetilde{*}}$ частичных ультраклонов. Решение данного вопроса проводится на языке сохранения предиката функциями. Обозначим через $PolR$ частичный ультраклон, сохраняющий предикат R.

На 2^{E_2} определим предикат R:

$$R = \begin{pmatrix} \{0\} & \{0\} & \{1\} & \{1\} & \{0,1\} & \{1\} & \{0\} & \{1\} & \{0,1\} & \varnothing & \varnothing & \varnothing & \epsilon & \varnothing \\ \{0\} & \{1\} & \{0\} & \{1\} & \{1\} & \{0,1\} & \{0,1\} & \{0,1\} & \{0,1\} & \alpha & \varnothing & \delta & \varnothing & \varnothing \\ \{0\} & \{1\} & \{1\} & \{1\} & \{1\} & \{1\} & \{0,1\} & \{0,1\} & \{0,1\} & \beta & \gamma & \varnothing & \varnothing & \varnothing \end{pmatrix},$$

где $\alpha, \beta, \gamma, \delta, \epsilon \in 2^{E_2} \setminus \varnothing$

Теорема. *$PolK$ является максимальным частичным ультраклоном в $P_2^{\widetilde{*}}$.*

Список литературы

[1] Пантелеев В. И. Критерий полноты для доопределяемых булевых функций // Вестник Самарского государственного университета. Естественнонаучная серия. – № 2 (68). – 2009. – С.60–79.

Восточно-Сибирская государственная академия образования, Иркутск
E-mail: infinityxxx@gmail.com

О мощности решетки клонов мультиопераций, сохраняющих нуль и единицу

С. Ю. Халтанова

Пусть $E_2 = \{0,1\}$, тогда операция $f : E_2^n \to 2^{E_2}$ называется мультиоперацией, $P^{\widetilde{*}}$ — множеством всех мультиопераций. Если для любого набора $(\alpha_1,\ldots,\alpha_n) \in E_2^n$ выполняется:
$\mid f(\alpha_1,\ldots,\alpha_n) \mid = 1$, то операция называется операцией алгебры логики;
$\mid f(\alpha_1,\ldots,\alpha_n) \mid \leq 1$ — частичной операцией;
$\mid f(\alpha_1,\ldots,\alpha_n) \mid \geq 1$ — гипероперацией.

Операция $f(x_1,\ldots,x_n) : f(\alpha_1,\ldots,\alpha_n) = \{\alpha_i\}$ называется селекторной.

Пусть $t \in \{2, *, \sim, \widetilde{*}\}$, определим следующие множества операций
$T^t_{0,0} = \{f \in P^t \mid f(0,\ldots,0) = \{0\}\}$, $\quad T^t_{1,1} = \{f \in P^t \mid f(1,\ldots,1) = \{1\}\}$,
$T^{\widetilde{*}}_{0,*} = \{f \in P^{\widetilde{*}} \mid f(0,\ldots,0) = \varnothing\}$, $\quad T^{\widetilde{*}}_{1,*} = \{f \in P^{\widetilde{*}} \mid f(1,\ldots,1) = \varnothing\}$,
$T^t_{01} = T^t_{0,0} \cap T^t_{1,1}$,

Пусть даны мультиоперации $f(x_1,\ldots,x_n), f_1(x_1,\ldots,x_m),\ldots,f_n(x_1,\ldots,x_m)$, тогда суперпозиция $f(f_1(x_1,\ldots,x_m),\ldots,f_n(x_1,\ldots,x_m))$ определяет мультиоперацию $g(x_1,\ldots,x_m)$ следующим образом:

$$g(a_1,...,a_m) \quad = \quad \begin{cases} \bigcap\limits_{b_i \in f_i(a_1,\ldots,a_m)} f(b_1,...,b_n), & \text{если это пересечение не равно } \varnothing; \\ \bigcup\limits_{b_i \in f_i(a_1,\ldots,a_m)} f(b_1,...,b_n), & \text{иначе.} \end{cases}$$

Клоном называется множество мультиопераций, замкнутое относительно суперпозиции и содержащее все селекторные операции.

Интервалом $I(A,B)$ называется частично упорядоченное по включению множество всех клонов, содержащих клон A и являющихся подмножествами клона B.

Лемма 1. *Интервал $I(T^2_{01}, T^{\sim}_{01} \cup T^{\widetilde{*}}_{1,*} \cup T^{\widetilde{*}}_{0,*})$ содержит 42 клона.*

Лемма 2. *Интервал $I(T^2_{01}, T^{\sim}_{01} \cup T^{\widetilde{*}}_{1,*} \cup T^{\widetilde{*}}_{0,*})$ изоморфен интервалу $I(T^*_{01}, T^{\widetilde{*}}_{01} \cup T^{\widetilde{*}}_{1,*} \cup T^{\widetilde{*}}_{0,*})$.*

Лемма 3. *Интервалы $I(T^2_{0,0}, P^{\widetilde{*}})$ и $I(T^2_{1,1}, P^{\widetilde{*}})$ содержат по 14 клонов .*

Теорема. *Интервал $I(T^2_{01}, P^{\widetilde{*}})$ содержит 108 клонов .*

Восточно-Сибирская государственная академия образования, Иркутск
E-mail: soelabad@mail.ru

The technique of definable terms in Boolean valued analysis

A. E. Gutman

Let Φ be a set of first-order formulas of set-theoretic signature. A formula φ is said to be *of class* Φ ("φ is Φ" for short) whenever $\mathrm{ZFC} \vdash [\varphi \Leftrightarrow \varphi']$ for some φ' in Φ. Let $\tau(\bar{x})$ be any term introduced in (a conservative extension of) ZFC by means of a definition of the form $\tau(\bar{x}) = y \Leftrightarrow \varphi(\bar{x}, y)$. Say that τ is *of class* Φ ("τ is Φ") whenever φ is of class Φ. Say that τ is Φ-*definable* via a term σ ("τ is $\Phi(\sigma)$") whenever there is a formula $\varphi(\bar{x}, y, z)$ of class Φ such that $\mathrm{ZFC} \vdash \big[\tau(\bar{x}) = y \Leftrightarrow \varphi\big(\bar{x}, y, \sigma(\bar{x})\big)\big]$.

In what follows, we denote formulas and terms by φ and τ, σ, ρ with possible indices; Δ_0 is the smallest set containing the formulas $x \in y$ and closed under the connectives $\vee$, $\neg$, $(\exists\, x \in y)$; Σ_1 is constituted by the formulas $(\exists\, x)\, \varphi$, with φ in Δ_0. A formula φ is *of class* Δ_1 ("φ is Δ_1") whenever φ and $\neg\varphi$ are Σ_1.

Lemma. (1) *If φ, τ, $\tau_1, \ldots, \tau_n$ are Σ_1 then so are $\varphi(\tau_1, \ldots, \tau_n)$ and $\tau(\tau_1, \ldots, \tau_n)$.*

(2) *If $\tau_1, \ldots, \tau_n$ are Σ_1 and φ is Δ_1 then $\varphi(\tau_1, \ldots, \tau_n)$ is Δ_1.*

(3) *If τ is Σ_1 and φ is Δ_1 then $\{\tau(\bar{x}) : \bar{x} \in y,\ \varphi(\bar{x}, y)\}$ is Σ_1.*

(4) *If τ is $\Sigma_1(\sigma)$ and ρ is $\Sigma_1(\tau)$ then ρ is $\Sigma_1(\sigma)$.*

(5) *If τ, $\tau_1, \ldots, \tau_n$ are $\Sigma_1(\sigma)$ then so is $\tau(\tau_1, \ldots, \tau_n)$.*

(6) *If τ is Σ_1 then $\tau(\sigma)$ is $\Sigma_1(\sigma)$.*

(7) *If τ is Σ_1 and φ is Δ_1 then $\{\tau(\bar{x}) : \bar{x} \in \sigma,\ \varphi(\bar{x}, \sigma)\}$ is $\Sigma_1(\sigma)$.*

(8) *If τ is Σ_1 and φ is Δ_1 then $\{\tau(\bar{x}) : \bar{x} \in \sigma,\ \varphi(\bar{x}, \sigma)\}^{\mathbb{N}}$ is $\Sigma_1(\sigma^{\mathbb{N}})$.*

The following example shows that statements (3) and (7) do not extend to the case in which φ is Σ_1.

Example. *Assume that ZFC is consistent and put $\varphi(x) := (\exists\, z)(z \subseteq \mathbb{N} \wedge z \notin x)$. Then φ is Σ_1, φ is not Δ_1, and $\{x \in y : \varphi(x)\}$ is not Σ_1.*

In what follows, $(\cdot)^\wedge$ stands for the canonical embedding of $\mathbb{V}$ into the Boolean valued universe $\mathbb{V}^{(B)}$.

Theorem. *If ρ is Σ_1, τ is $\Sigma_1(\sigma)$, and all the parameters of ρ, σ, τ are in $\bar{x}$ then the following is provable in ZFC: for every complete Boolean algebra B and all $\bar{x}$*

(1) $\mathbb{V}^{(B)} \models \big[\, \rho(\bar{x})^\wedge = \rho(\bar{x}^\wedge) \,\big]$;

(2) $\mathbb{V}^{(B)} \models \big[\, \sigma(\bar{x})^\wedge = \sigma(\bar{x}^\wedge) \,\big] \ \Rightarrow\ \mathbb{V}^{(B)} \models \big[\, \tau(\bar{x})^\wedge = \tau(\bar{x}^\wedge) \,\big]$.

Let $\mathbb{R}_{\mathrm{D}}$ and $\mathbb{R}_{\mathrm{C}}$ stand for the set of reals defined as Dedekind cuts and, respectively, classes of Cauchy sequences in $\mathbb{Q}$.

Corollary (ZFC). *Let B be a complete Boolean algebra.*

(1) $\mathbb{V}^{(B)} \models \big[\mathbb{R}_{\mathrm{D}}^\wedge \subseteq \mathbb{R}_{\mathrm{D}}\big]$; $\mathbb{V}^{(B)} \models \big[\mathcal{P}_{\mathrm{fin}}(X)^\wedge = \mathcal{P}_{\mathrm{fin}}(X^\wedge)\big]$ *for all* X.

(2) *The following properties of B are pairwise equivalent: B is σ-distributive*; $\mathbb{V}^{(B)} \models \big[\mathcal{P}(\mathbb{N})^\wedge = \mathcal{P}(\mathbb{N})\big]$; $\mathbb{V}^{(B)} \models \big[(\mathbb{N}^{\mathbb{N}})^\wedge = \mathbb{N}^{\mathbb{N}}\big]$; $\mathbb{V}^{(B)} \models \big[\mathbb{R}_{\mathrm{D}}^\wedge = \mathbb{R}_{\mathrm{D}}\big]$; $\mathbb{V}^{(B)} \models \big[\mathbb{R}_{\mathrm{C}}^\wedge \subseteq \mathbb{R}_{\mathrm{C}}\big]$; $\mathbb{V}^{(B)} \models [\mathbb{R}^\wedge$ *and* $\mathbb{R}$ *are isomorphic ordered fields*$]$.

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

On circularly ordered groups that are weakly circularly minimal

B. Sh. Kulpeshov

We continue studying the notion of *weak circular minimality* originally studied by D. Macpherson and me 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) $\forall x \forall y \forall z (K(x,y,z) \wedge K(y,x,z) \Leftrightarrow x = y \vee y = z \vee z = x)$;
(co3) $\forall x \forall y \forall z (K(x,y,z) \to \forall t [K(x,y,t) \vee K(t,y,z)])$;
(co4) $\forall x \forall y \forall z (K(x,y,z) \vee K(y,x,z))$.

A set A of a circularly ordered structure M is said to be *convex* if for any $a, b \in A$ the following holds: for any $c \in M$ with $K(a,c,b)$ we have $c \in A$ or for any $c \in M$ with $K(b,c,a)$ we have $c \in A$. 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 intervals and points (convex sets). Any weakly o-minimal structure is weakly circularly minimal, but the inverse is not true in general. Some of interesting examples of weakly circularly minimal structures that are not weakly o-minimal were studied in [**1, 2, 3**].

In [**4**] circularly minimal groups have been studied, and was proved that they are abelian, divisible and densely ordered.

The talk is based on joint work with Viktor V. Verbovskiy, Institute for Problems of Informatics and Control (Almaty, Kazakhstan). Here we discuss some properties of weakly circularly minimal groups. We have obtained the following resutls:

Theorem 1. *Any weakly circularly minimal group is abelian and densely ordered.*

Proposition 2. *There exists a weakly circularly minimal group which is non-divisible.*

It had been proved before that a circularly minimal group does not have any proper infinite definable subgroups (Claim 5.1.1, [**4**]). However for the weakly circularly minimal group the claim doesn't hold in general. Moreover, we have the following:

Proposition 3 *For each natural number n there exists a weakly circularly minimal group having an infinite $\emptyset$–definable subgroup with n convex components.*

References

[1] Kulpeshov B. Sh., Macpherson H. D. Minimality conditions on circularly ordered structures // Mathematical Logic Quarterly, 2005, V. 51. P. 377–399.
[2] Kulpeshov B. Sh. On $\aleph_0$-categorical weakly circularly minimal structures // Mathematical Logic Quarterly, 2006, V. 52. P. 555–574.
[3] Kulpeshov B. Sh. Definable functions in the $\aleph_0$-categorical weakly circularly minimal structures // Siberian Mathematical Journal, 2009, V. 50. P. 282–301.
[4] Macpherson H. D., Steinhorn Ch. On variants of o-minimality // Annals of Pure and Applied Logic, 1996, V. 79. P. 165–209.

International Information Technologies University, Almaty
E-mail: kulpesh@mail.ru

Stone type representations for q-lattices and interlaced q-bilattices

Yu. M. Movsisyan, D. S. Davidova

The algebra, $(L; \wedge, \vee)$, with two binary operations is called q-lattice (or quantum-lattice), if it satisfies the following identities: 1. $a \wedge b = b \wedge a, a \vee b = b \vee a$ (commutativity); 2. $a \wedge (b \wedge c) = (a \wedge b) \wedge c, a \vee (b \vee c) = (a \vee b) \vee c$ (associativity); 3. $a \wedge (b \wedge b) = a \wedge b, a \vee (b \vee b) = a \vee b$ (weak idempotency); 4. $a \wedge (b \vee a) = a \wedge a, a \vee (b \wedge a) = a \vee a$ (weak absorption); 5. $a \wedge a = a \vee a (equalization)$.

For example, the $(Z \setminus \{0\}; \wedge, \vee)$ (where $x \wedge y = (|x|, |y|)$ and $x \vee y = [|x|, |y|]$, for which $(|x|, |y|)$ and $[|x|, |y|]$ are the greatest common division (gcd) and the least common multiple (lcm) of $|x|$ and $|y|$) is a q-lattice, which is not a lattice, since: $x \wedge x \neq x$ and $x \vee x \neq x$.

We say that the algebra with four binary operations, $(L; \wedge, \vee, *, \triangle)$ is a q-bilattice, if the reducts, $L_1 = (L; \wedge, \vee)$ and $L_2 = (L; *, \triangle)$, are q-lattices and it satisfies the following identity, $a \wedge a = a * a$, as well.

Any q-lattice corresponds to a quasiorder (both a reflexive and a transitive relation) θ, which is defined in the following manner:

$$a \theta b \leftrightarrow a \wedge b = a \wedge a \leftrightarrow a \vee b = b \vee b.$$

Since the q-bilattice has the structure of the two q-lattices, then any q-bilattice corresponds to two quasiorders. Let us denote the quasiorder of the first reduct, L_1, of the q-bilattice, $(L; \wedge, \vee, *, \triangle)$, by $\leq_\wedge$, and that of the second reduct, L_2, by $\leq_*$.

The q-bilattice is called interlaced if all basic q-bilattice operations are quasiorders preserving with respect to the both quasiorders, i.e.

$a \leq_\wedge b, c \leq_\wedge b \rightarrow a * c \leq_\wedge b * d, a \triangle c \leq_\wedge b \triangle d$; $a \leq_* b, c \leq_* b \rightarrow a \wedge c \leq_* b \wedge d, a \vee c \leq_* b \vee d$.

Note that a q-bilattice is interlaced, iff it satisfies all hyperidentities of the variety of q-lattices.

*F*or example, any q-lattice, $(L; \wedge, \vee)$, can be considered as an interlaced q-bilattice, in the following manner: $(L; \wedge, \vee, \wedge, \vee)$.

We prove Stone's type representation theorems for arbitrary q-lattices and interlaced q-bilattices. The problems of similar representations for q-lattices with a unary operation, and for interlaced q-bilattices with unary operation are still open.

References

[1] Movsisyan Yu. M. Hyperidentities in algebras and varieties // Uspekhi Matematicheskikh Nauk, 1998, V. 53, P. 61–114. English translation in Russian Mathematical Surveys, 1998, V. 53. P. 57–108.

[2] Movsisyan Yu. M. Bilattices and hyperidentities // Proceedings of the Steclov Institute of Mathematics, 2011, V. 274. P. 174–192.

[3] Movsisyan Yu. M., Romanowska A. B., Smith J. D. H. Superproducts, hyperidentities, and algebraic structures of logic programming // Comb. Math. and Comb. Comp., 2006, V. 58. P. 101–111.

Yerevan State University, Yerevan
E-mail: yurimovsisyan@yahoo.com, di.davidova@yandex.ru

Ranks of generalized semi-isolation

S. V. Sudoplatov

We generalize the rank si of semi-isolation [**1**] for sets of types.

Let T be a complete theory, $\mathcal{M} \models T$. We consider *closed* sets (under the natural topology) sets $\mathbf{p}(x) \subseteq S^1(\varnothing)$, i. e., sets $\mathbf{p}(x)$ such that $\mathbf{p}(x) = \bigcap\limits_{i\in I}[\varphi_{\mathbf{p},i}(x)]$, where $[\varphi_{\mathbf{p},i}(x)] \rightleftharpoons \{p(x) \in S^1(\varnothing) \mid \varphi_{\mathbf{p},i}(x) \in p(x)\}$ for some formulas $\varphi_{\mathbf{p},i}(x)$ of T. For closed sets $\mathbf{p}(x), \mathbf{q}(y) \subseteq S(\varnothing)$ of types, realized in $\mathcal{M}$, we take all $(\mathbf{p},\mathbf{q})$-*preserving* $(\mathbf{p},\mathbf{q})$-*semi-isolating*, or $(\mathbf{p} \to \mathbf{q})$-formulas $\varphi(x,y)$ of T, i. e., formulas for which if $a \in M$ realizes a type in $\mathbf{p}(x)$ then every solution of $\varphi(a,y)$ realizes a type in $\mathbf{q}(y)$.

For triples $(\mathbf{p},u,\mathbf{q})$, where $\mathbf{p},\mathbf{q} \subseteq S^1(\varnothing)$, u is a label for a $(\mathbf{p} \to \mathbf{q})$-formula with respect to a labelling function $\nu(\mathbf{p},\mathbf{q})$, we define inductively the *rank* $\mathrm{si}_1(\mathbf{p},u,\mathbf{q})$ *of semi-isolation*: (1) $\mathrm{si}_1(\mathbf{p},u,\mathbf{q}) = 0$ if $u \notin \rho_{\nu(\mathbf{p},\mathbf{q})}$ or $u = \varnothing$; (2) $\mathrm{si}_1(\mathbf{p},u,\mathbf{q}) \geq 1$ if $u \in \rho_{\nu(\mathbf{p},\mathbf{q})} \setminus \{\varnothing\}$; (3) for a positive ordinal α, $\mathrm{si}_1(\mathbf{p},u,\mathbf{q}) \geq \alpha+1$ if there is a set $\{v_i \mid i \in \omega\}$ of pairwise inconsistent labels such that $v_i \vdash u$ and $\mathrm{si}_1(\mathbf{p},v_i,\mathbf{q}) \geq \alpha$, $i \in \omega$; (4) for a limit ordinal α, $\mathrm{si}_1(\mathbf{p},u,\mathbf{q}) \geq \alpha$ if $\mathrm{si}_1(\mathbf{p},u,\mathbf{q}) \geq \beta$ for any $\beta \in \alpha$. As usual, we write $\mathrm{si}(\mathbf{p},u,\mathbf{q}) = \alpha$ if $\mathrm{si}(\mathbf{p},u,\mathbf{q}) \geq \alpha$ and $\mathrm{si}(\mathbf{p},u,\mathbf{q}) \not\geq \beta$ for $\alpha \in \beta$; $\mathrm{si}(\mathbf{p},u,\mathbf{q}) \rightleftharpoons \infty$ if $\mathrm{si}(\mathbf{p},u,\mathbf{q}) \geq \alpha$ for any ordinal α.

Now we define the *rank* $\mathrm{si}_2(\mathbf{p},u,\mathbf{q})$. For $u \in \rho_{\nu(\mathbf{p},\mathbf{q})}$ and $p \in \mathbf{p}$, we denote by u_p the label $v \in \rho_{\nu(\{p\},\mathbf{q})}$ such that $\theta_{\mathbf{p},u,\mathbf{q}}(a,y) \equiv \theta_{\{p\},v,\mathbf{q}}(a,y)$ for a realizing p. We set $\mathrm{si}_2(\mathbf{p},u,\mathbf{q}) \rightleftharpoons \sup\limits_{p\in\mathbf{p}} \mathrm{si}_1(\{p\},u_p,\mathbf{q})$. By the definition, $\mathrm{si}_2(\mathbf{p},u,\mathbf{q}) \leq \mathrm{si}_1(\mathbf{p},u,\mathbf{q})$ for any label u and this inequality can be strict. For singletons $\mathbf{p}$ and $\mathbf{q}$, $\mathrm{si}_1(\mathbf{p},u,\mathbf{q}) = \mathrm{si}_2(\mathbf{p},u,\mathbf{q})$ and this value equals to the si-rank of correspondent label.

Theorem.
(1) *Each* si_1*-rank in a theory* T *is either equal to* ∞ *or less than* $\min\{|T|^+, (\mathrm{MR}'(x \approx x)+1)^+\}$*, where* MR' *is the Morley rank with respect to formulas* $\bigvee\limits_{\models\mathbf{p}(a)} \theta_{\mathbf{p},u',\mathbf{q}}(a,y)$*, representing* $(\mathbf{p} \to \mathbf{q})$*-formulas for labels* $u' \in \rho_{\nu(\mathbf{p},\mathbf{q})}$*. If the Morley rank* $\mathrm{MR}'(x \approx x)$ *is equal to an ordinal* α *then any* si_1*-rank in* T *is not more than* $\alpha+1$*.*

(2) *Each* si_2*-rank in a theory* T *is either equal to* ∞ *or less than* $\min\{|T|^+, (\mathrm{MR}(x \approx x)+1)^+\}$*. If the Morley rank* $\mathrm{MR}(x \approx x)$ *is equal to an ordinal* α *then any* si_2*-rank in* T *is not more than* $\alpha+1$*.*

A series of results and the hierarchy of structures with respect to the rank of semi-isolation [**1**] are generalized for the ranks si_1 and si_2.

The work is supported by RFBR grant No. 12-01-00460-a.

References

[1] Sudoplatov S. V. Algebras of distributions for binary semi-isolating formulas of a complete theory // arXiv:1210.4049v1 [math.LO]. 35 p.

Sobolev Institute of Mathematics, Novosibirsk State Technical University, Novosibirsk State University, Novosibirsk
E-mail: sudoplat@math.nsc.ru

Δ-M-λ and S^M_Γ-λ-stabilities for Δ-M-theories

A. R. Yeshkeyev

Let T be an arbitrary Δ-M-theory in the language of the signature σ. Δ-M-theory differs from the Δ-PM-theory, the fact that the morphisms considered only immersions, as in the [**1**]. Let C be a semantic model of T, $A \subseteq C$. Let $\sigma_\Gamma(A) = \sigma \bigcup \{c_a | \, a \in A\} \bigcup \Gamma$, where $\Gamma = \{g\} \bigcup \{c\} \bigcup \{P\}$.

Consider the following theory

$$T_\Gamma^{PgM}(A) = Th_{\Pi^+_{\alpha+2}}(C,\ a)_{a\in A} \bigcup \{g(a) = a \mid a \in A\} \bigcup g(c) \bigcup T_g \bigcup \{P(c)\} \bigcup \{\text{"}P \subseteq \text{"}\},$$

where T_g expresses the fact that for any model $(M,\ g^M) \models T_g$ we have:

1) g^M is an automorphism of M;

2) $\{m \in M \,|\, g^M(m) = m\}$ is a universe of some existentially closed submodel of M, for any model M of signature σ.

For a predicate P, we write an expression $\{\text{"}P \subseteq \text{"}\}$, that is essentially an infinite set of sentences, which says that the interpretation of the character P is positive existentially closed submodel in the signature σ. Because of the incompleteness we do not write the exact relationships between the elements $\Gamma = \{g\} \bigcup \{c\} \bigcup \{P\}$, but it is assumed that they are consistent within the framework of $T_\Gamma^{PgM}(A)$.

Below we work in this enrichment of signature.

Definition 1. We say that the Δ-M theory T is Δ-M-λ-stable if for any model $A \in \Sigma^+_{\alpha+1}T$, any subset X of the set A, $|X| \leq \lambda \Rightarrow \left| S^M_{\Sigma^+_{\alpha+1}}(X) \right| \leq \lambda$. Δ-M-theory T Δ-M-stable if it is Δ-M-λ stable for some λ.

Theorem 1. *Let T be a Δ-M-theory, perfect, complete for the $E_{\alpha+1}$ sentences, $\lambda \geq \omega$. Then the following conditions are equivalent:*

1) T^* is Δ-M-λ-stable;

2) T^c is λ-stable (in classical meaning), where T^* is the center of the theory T.

Definition 2. We denote by S^M_Γ the set of all $\Sigma^+_{\alpha+1}$-completions of the theory $T_\Gamma^{PgM}(A)$. The theory T is S^M_Γ-λ-stable if $\left|S^M_\Gamma\right| \leq \lambda$ for any A such that $|A| \leq \lambda$.

Theorem 2. *Let T be a $\Sigma_{\alpha+1}$-complete, perfect Δ-M-theory. Then the following conditions are equivalent:*

1) The theory T^c is λ-stable in the sense of [**2**]*;*

2) The theory T^* is S^M_Γ-λ-stable.

All notions undefined in this thesis can be found in [**3**].

References

[1] Ben-Yaacov I. Compactness and independence in non first order frameworks // Bulletin of Symbolic logic. 2005, V. 11, no. A. P. 28–50.

[2] Mustafin T. G. New concepts of stability theories // Sat "Proceedings of the Soviet-French symposium on model theory", Karaganda, 1990. P. 112–125.

[3] Yeshkeyev A. R. Jonsson's theories. Textbook. Karaganda: Karaganda State University, 2009.

Karaganda State University, The Institution of Applied Mathematics, Karagandy
E-mail: modth1705@mail.ru

On free n-nilpotent dimonoids

A. V. Zhuchok

An element 0 of a dimonoid $(D, \dashv, \vdash)$ (see, e.g., [1, 2]) will be called zero, if $x * 0 = 0 = 0 * x$ for all $x \in D$ and $* \in \{\dashv, \vdash\}$.

As usual, $\mathbb{N}$ denotes the set of all positive integers. A dimonoid $(D, \dashv, \vdash)$ with zero will be called nilpotent, if for some $n \in \mathbb{N}$ and any $x_i \in D$, $1 \le i \le n+1$, and $*_j \in \{\dashv, \vdash\}$, $1 \le j \le n$, any parenthesizing of

$$x_1 *_1 x_2 *_2 \ldots *_n x_{n+1}$$

gives $0 \in D$. The least such n we shall call the nilpotency index of $(D, \dashv, \vdash)$. For $k \in \mathbb{N}$ a nilpotent dimonoid of nilpotency index $\le k$ is said to be k-nilpotent.

It is obvious that operations of any 1-nilpotent dimonoid coincide and it is a zero semigroup.

Note that the class of all n-nilpotent dimonoids is a subvariety of the variety of all dimonoids. A dimonoid which is free in the variety of n-nilpotent dimonoids will be called a free n-nilpotent dimonoid.

Let X be an alphabet, $F[X]$ be the free semigroup over X. Denote the length of a word $w \in F[X]$ by l_w. Fix $n \in \mathbb{N}$ and assume

$$FN_n = \{(w, m) \in F[X] \times \mathbb{N} \,|\, m \le l_w \le n\} \cup \{0\}.$$

Define operations $\dashv$ and $\vdash$ on FN_n by

$$(w_1, m_1) \dashv (w_2, m_2) = \begin{cases} (w_1 w_2, m_1), & l_{w_1 w_2} \le n, \\ 0, & l_{w_1 w_2} > n, \end{cases}$$

$$(w_1, m_1) \vdash (w_2, m_2) = \begin{cases} (w_1 w_2, l_{w_1} + m_2), & l_{w_1 w_2} \le n, \\ 0, & l_{w_1 w_2} > n, \end{cases}$$

$$(w_1, m_1) * 0 = 0 * (w_1, m_1) = 0 * 0 = 0$$

for all $(w_1, m_1), (w_2, m_2) \in FN_n \backslash \{0\}$ and $* \in \{\dashv, \vdash\}$. The algebra $(FN_n, \dashv, \vdash)$ will be denoted by $FN_n(X)$.

Theorem. *$FN_n(X)$ is the free n-nilpotent dimonoid.*

Corollary. *The free n-nilpotent dimonoid $FN_n(X)$ generated by a finite set X is finite. Specifically, $|FN_n(X)| = \sum_{i=1}^{n} i|X|^i + 1$.*

In addition, we introduce the notion of a 0-diband of subdimonoids and in terms of 0-dibands of subdimonoids describe the structure of free n-nilpotent dimonoids. We also present the least n-nilpotent 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] Zhuchok A.V., Dimonoids, Algebra and Logic **50** (2011), no. 4, 323–340.

Luhansk Taras Shevchenko National University, Luhansk (Ukraine)
E-mail: zhuchok_a@mail.ru

VIII. Авторский указатель