Novosibirsk State Technical University

Algebra and Model Theory *6*

Collection of papers
edited by A.G. Pinus and K.N. Ponomarev

Novosibirsk
2007

512(06)

Algebra and Model Theory. Collection of papers. Edited by A.G. Pinus and K.N. Ponomarev. Novosibirsk State Technical University, 2007. — 121 p.

ISBN 5–7782–0175–3

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

Technical editor I.D. Chernykh.

Introduction

Algebra and Model Theory 6

The Seventh Summer School "Intermediate problems of Model Theory and Universal Algebra" was held on 26–30 of June 2007 in the camping center "Erlogol" in Altai mountains. The School was organized by Algebra and Math Logic department of Novosibirsk State Technical University (NSTU). Fifty participants took part in the conference.

Unfortunately during the last two years since the former School some active participants and authors of Erlogol collections of papers had passed away. Organizing Committee recalls with gratitude the time of collaboration with prof. Eugeny Sukhanov (Ekaterinburg, Russia), prof. Nikolay Medvedev (Barnaul, Russia), prof. Kazimierz Głazek (Zielena Góra, Poland).

The School was supported by RFBR (grant N 07-01-06046).

The book is composed from some articles of the participants. Organizing Committee of the conference thanks director of Institute of Distant Education Prof. Z.S. Temljakova for financial support of this edition.

Erlogol 2007

Intermediate Problems of Model Theory and Universal Algebra

(June, 26–30)

26 June. Chairman Semen Rososhek

V.G. Bardakov (*Novosibirsk, Russia*).

Braids, knots and linear representations.

K.N. Ponomaryov (*Novosibirsk, Russia*).

Factor-morphisms and centroids of algebraic groups.

V.A. Churkin (*Novosibirsk, Russia*).

Groups of rotations and matrices's diagonalizeability.

Chairman Valery Churkin

A.A. Buturlakin (*Novosibirsk, Russia*).

Spectrums of linear and unitar groups.

S.A. Zyubin (*Tomsk, Russia*).

Flag-transitiveness of groups on projective varieties.

M.A. Grechkoseeva (*Novosibirsk, Russia*).

On recognition of simple linear groups by their spectrums.

27 June. Chairman David Stanovsky

S.V. Sudoplatov (*Novosibirsk, Russia*).

Graphs in models and Ehrenfeucht theories.

V.M. Kopytov (*Novosibirsk, Russia*).

On normal subgroups of l-groups.

N.A. Peryazev (*Irkutsk, Russia*).

Algebra of not completely defined partial functions.

Chairman Valery Kopytov

I.A. Dolguntseva (*Barnaul, Russia*).

On cogomologies' group of some simple associative comform algebras.

N.V. Bayanova (*Barnaul, Russia*).

Free pseudo-MV-algebras.

O.A. Kuryleva (*Barnaul, Russia*).

Discriminative l-groups.

V.V. Lodeyshchikova (*Barnaul, Russia*).

On Levi's quasivarieties.

O.V. Bryukhanov (*Novosibirsk, Russia*).

On residual nilpotency of fundamental groups of 3-dimentional *Sol*-varieties.

28 June. Chairman A? Borodin

S.K. Rososhek (*Tomsk, Russia*).

Cryptosystems of group rings.

S.V. Sudoplatoff (*Paris, France*).

Human network, technological network.

E.A. Palyutin (*Novosibirsk, Russia*).

Elementary questions of structures' classes closed for product.

Chairman Sergey Sudoplatoff

A.P. Pozhidaev (*Novosibirsk, Russia*).

Dialgebras and triplet systems.

A.M. Popova (*Novosibirsk, Russia*).

Automorphisms of the ring ZS_3.

E.V. Grachev (*Novosibirsk, Russia*).

Construction units group of integral ring of cycle group of prime order.

A.N. Borodin (*Russia*).

On method of coordinatisation of physical principals by universal algebras.

29 June. Chairman Alexander Pozhidaev

S.I. Mardaev (*Novosibirsk, Russia*).

Natural numbers and fixed points.

D. Stanovsky (*Prague, Chesh Republic*).

Park hypothesis.

L.A. Shalomov (*Moscow, Russia*).

Application of model theory methods to mathematical decision theory.

I.B. Gorshkov (*Novosibirsk, Russia*).

On groups with composition quotient groups isomorphic to S_7.

Chairmen Valery Bardakov

E.S. Chibrikov (*Novosibirsk, Russia*).

On intersection of onegenerated ideals of free Lie algebras.

M.A. Rusaleev (*Novosibirsk, Russia*).

Properties of extended stable theories.

КОДЫ И СМЕЖНОСТЬ В ОРГРАФАХ КОРНЕВЫХ СИМПЛЕКСОВ ВЕЩЕСТВЕННЫХ МНОГОЧЛЕНОВ

А.А. Воевода, А.В. Чехонадских

Новосибирский государственный технический университет,
Россия, 630092, Новосибирск, пр. К.Маркса 20
e-mail: algebra@nstu.ru

1 Введение

При решении задач синтеза систем автоматического регулирования операторным методом важнейшие свойства пары *объект* $\longleftrightarrow$ *компенсатор* определяются значениями корней характеристического многочлена. Оптимизация системы корней по отношению к заданной целевой области наиболее естественно производилась бы при рассмотрении корневого вектора как элемента — n-мерного пространства над полем R действительных чисел во взаимно однозначном соответствии с вектором коэффициентов многочлена. Такое представление, однако, наталкивается на ряд трудностей: как принципиальных (неупорядоченность корневых наборов), так и технических (структурная сложность расположения корней именно вещественных многочленов в комплексном пространстве C^n). Предпринятая авторами ранее попытка построения взаимно однозначного соответствия *корни* $\longleftrightarrow$ *коэффициенты* корректна только локально [1]. В серии работ [2-4] сегментарные симплексы многочленов произвольной степени были представлены с помощью графов; для многочленов степени не выше 5 соответствующие орграфы были построены явно [3, 5]. Однако уже для степени 6 и выше явное представление становится неэффективным в связи с быстрым ростом мощности. В настоящей работе предлагается кодировка корневых сегментов (вершин орграфов), позволяющая легко выяснить их смежность для произвольной степени.

2 Корневые сегменты и вершины графа

Корневые наборы вещественных многочленов допускают любые перестановки своих элементов. Однако с практической точки зрения было бы удобнее располагать множеством в C^n, содержащим только один корневой набор для каждого многочлена. Хотя последнее оказывается недостижимо (замечание о двулистности подмножеств, отвечающих двум и более комплексным парам корней см. в [2, 3]), мы будем сопоставлять каждому набору корней некоторую точку в пространстве R^n, причём в определённом его **сегменте**, ограниченном несколькими линейными неравенствами. Это делает естественным и практически удобным использование *действительных координат* для данного корневого набора. Все возможные сегменты образуют **симплекс**; границы между сегментами, в свою очередь, также являются *сегментами* — k-мерными подмножествами пространства R^n, задающимися некоторыми линейными неравенствами и равенствами. Структура этого симплекса, сводящаяся к многоуровневому соответствию областей и границ, может представляться в виде ориентированного графа.

Например, для приведённого многочлена 3-й степени $f_3[z] = z^3 + a_2z^2 + a_1z + a_0$ возможно, во-первых, наличие трёх действительных корней: $x_1 \leq x_2 \leq x_3$, во-вторых, одного действительного корня вместе с комплексно сопряжённой парой. Первый случай отвечает сегменту A_0, отсекаемому плоскостями $x_1 = x_2$ и $x_2 = x_3$ — это "треть" пространства R^3 (двугранный угол при ребре $x_1 = x_2 = x_3$, соответствующий этому сегменту, равен 120°). Второй случай естественно соотносится с A_1 — "правым" полупространством $OXYZ$ (при условии $y \geq 0$): $z_{1,2} = x \pm iy, x_3 = z$ (или $x_1 = z$). При $y = 0$ это переходит в кратную действительную пару $z_{1,2} = x$ вместе с третьим, возможно, отличным от них корнем $x_3 = z$ (или $x_1 = z$). Случай $x \leq z$ соответствует полуплоскости B_01, задаваемой неравенством $x_1 = x_2 \leq x_3$; если же $x \geq z$, то полуплоскости $B_02 : x_1 \leq x_2 = x_3$. Из-за этого естественно считать область A_1 объединением двух сегментов: в первом, A_11 выполняется неравенство $Rez_{1,2} \leq z$; во втором, A_12 — неравенство $Rez_{1,2} \geq z$. Между собой они разграничены полуплоскостью $B_1 : Rez_{1,2} = z \& Imz_{1,2} = y \geq 0$. Сами же полуплоскости B_01 и B_02 — это двумерные сегменты, которые, в свою очередь, разграничены одномерной прямой $C : x = z \& y = 0 \Longleftrightarrow x_1 = x_2 = x_3$, которая соответствует трёхкратным корням и служит общим пересечением также и со слоем B_1.

Таким образом, возникает граф G_3 (рис.1) — единственный, позво-

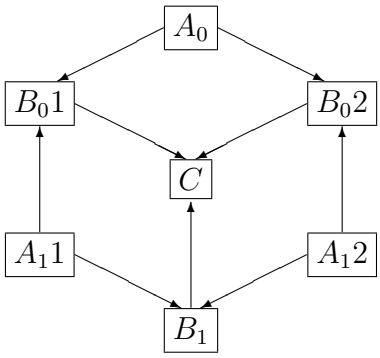

Рис. 1: G_3

ляющий взаимно однозначно сопоставить каждому корневому набору определённую точку пространства R^3. Дуги в нём проведены от областей к границам.

В общем случае будут использоваться схожие обозначения. Поскольку число комплексно сопряжённых пар корней для многочлена степени nне превосходит числа $[n/2]$, то *сегментарные слои* будем нумеровать по числу этих пар: $A_0, A_1, ..., A_{[n/2]}$, каждый из которых складывается из n-мерных действительных сегментов; для рассматриваемых ниже многочленов 4-й и 5-й степени это A_0, A_1 и A_2.

Слой A_0 включает единственный сегмент, описывающийся неравенствами $x_1 \leq x_2 \leq ... \leq x_n$. Допуская равенство в k-ом из неравенств: $x_1 \leq ... \leq x_k = x_{k+1} \leq ...x_n$, попадаем на n-1-мерный граничный сегмент B_0k. Таким образом, на каждом из сегментов B_0k располагается пара кратных действительных корней, которая при малой вариации коэффициентов многочлена может "отклониться назад", возвращаясь к паре различных действительных корней в сегменте A_0, а, отклоняясь "в другую сторону", переходит в пару комплексно сопряжённых корней $z_{k,k+1} = x_k \pm iy_k$ в составе корневого набора из n-мерного сегмента A_1k, описывающегося системой неравенств

$$x_1 \leq ... \leq x_k \leq x_{k+2} \leq ... \leq x_n \& y_k \geq 0 \text{ (где, разумеется,} x_k = Rez_{k,k+1}).$$

Заметим, что сегменты B_lk при нечётном l оказываются границами внутри одного слоя, а при чётном — между сегментами соседних слоёв.

Сегментов 1-го слоя всего $n-1$: $A_11 - A_1(n-1)$; их объединение образует симплекс A_1, а между собой они разделяются $n-1$-мерными границами $B_11 - B_1(n-2)$, которых всего $n-2$:

$B_1 1 : Rez_{1,2} = x_3 \leq ... \leq x_n \& y_1 \geq 0 \Longleftrightarrow x_1 = Rez_{2,3} \leq ... \leq x_n \& y_2 \geq 0$;

$\vdots$

$B_1(n-2) : x_1 \leq ... \leq x_{n-3} \leq Rez_{n-2,n-1} = x_n \& y_{n-2} \geq 0 \Longleftrightarrow x_1 \leq ... \leq x_{n-2} = Rez_{n-1,n} \& y_{n-1} \geq 0$;

(конечно, $y_k = Imz_{k,k+1}$).

Важно отметить, что *перенумерации на стыках сегментов* $B_1 k$ *и* $B_1(k+1)$ *бесконфликтны.*

Сегменты 1-го слоя однолистны. Когда ещё одно неравенство $x_k \leq x_{k+1}$ обращается в равенство, корневой набор переходит на границу $B_2 l$ со слоем A_2, все сегменты которого n-мерны, двулистны и разделены между собой граничными $n-1$-мерными сегментами $B_3 m$.

Легко видеть, что для многочленов 4-й и 5-й степени "слойность" орграфа исчерпывается слоем A_2, причём в случае 4-й степени он состоит из единственного сегмента: двулистной четырёхмерной "полуплоскости в квадрате" (где координаты x_k, отвечающие действительным частям корней, принимают любые значения, а "мнимые" координаты неотрицательны: $y_{1,3} \geq 0$); а в случае степени 5 — из трёх двулистных сегментов:

$A_2 1 : Rez_{1,2}, Rez_{3,4} \leq x_5$;

$A_2 2 : Rez_{1,2} \leq x_3 \leq Rez_{4,5}$;

$A_2 3 : x_1 \leq Rez_{2,3}, Rez_{4,5}$.

Для многочлена же шестой степени появляется слой A_3 — шестилистная "полуплоскость в кубе", где "действительные" координаты x_k любые, а "мнимые" неотрицательны: $y_{1,3,5} \geq 0$.

Далее, пересечение двух $n-1$ – мерных граничных сегментов *всегда непусто*, так как содержит одномерную прямую $L : x_1 = ... = x_n$, и оказывается граничным сегментом $C_k l$, как правило, размерности $n-2$. В рассмотренных выше примерах только в одном случае пересечение четёхмерных сегментов оказывается не трёхмерно, а двумерно — это множество $B_1 1 \cap B_1 3$ для многочлена 5-й степени; в самом деле, система неравенств:

$B_1 1 : Rez_{1,2} = x_3 \leq x_4 \leq x_5 \Longleftrightarrow x_1 = Rez_{2,3} \leq x_4 \leq x_5$;

$B_1 3 : x_1 \leq x_2 \leq Rez_{3,4} = x_5 \Longleftrightarrow x_1 \leq x_2 \leq x_3 = Rez_{4,5}$, — удовлетворяется, только когда все действительные части равны, например,

$Rez_{1,2} = x_{3,4,5} \Longleftrightarrow x_{1,2,3} = Rez_{4,5}$.

В свою очередь, сегменты $C_k l$ ограничены $n-3$ - мерными сегментами $D_k l$, которые для многочлена степени 4 уже оказываются единственной прямой $L : x_1 = ... = x_4$.

Литеральный рост буквенного символа соответствует понижению размерности граничных сегментов.

Дуги в орграфе проводятся от областей к границам. Если две вершины, обозначенные одной и той же буквой, инцидентны некоторой вершине следующей по алфавиту буквы, то сегмент последней имеет размерность $k-1$ и оказывается границей между сегментами двух первых, размерность которых k.

3 Коды вершин графа

Кодировка вершин графа осуществляется по задающим неравенствам соответствующего сегмента. Кодами являются целочисленные матрицы $K_{2\times m} = \begin{pmatrix} k_{11} & \cdots & k_{1m} \\ k_{21} & \cdots & k_{2m} \end{pmatrix}$, где $m \le n, k_{1j} \ge 1, 0 \le k_{2j} \le k_{1j}, \sum k_{ij} = n$.

Число столбцов m равно количеству различных действительных частей в корневых наборах данного сегмента — или, что то же самое, на единицу больше числа значков $\le$ в системе неравенств, задающей данный сегмент и вершину графа. Например, для задающих неравенств

$Rez_{1,2} = x_3 \le x_4 = x_5 = x_6 \le Rez_{7,8} = Rez_{9,10} = x_{11}$ оказывается, что $m = 3$.

Строка $(k_{11\ldots}k_{1m})$ составляется из чисел равных между собой членов задающей системы. Для вышеприведённой системы это будет строка (2 2 3). Элементы второй строки указывают, сколькие из этих равных между собой действительных частей соответствуют комплексным парам; сумма второй строки $\Sigma k_{2j} = l$ — это число комплексных пар набора, или, что то же самое, номер слоя. В указанном случае вторая строка окажется такой: (1 0 2); её сумма равна 3 — это число комплексных пар; а сумма всех элементов матрицы равна 11 — степени многочлена и общему числу корней.

В целом код системы неравенств и вершины графа оказывается таким: $\begin{pmatrix} 2 & 3 & 3 \\ 1 & 0 & 2 \end{pmatrix}$. Его расшифровка может привести как к самой вышеприведённой системе, так и к любой равносильной ей системе неравенств (за счёт перенумерации корней их может быть несколько), например, $x_1 = Rez_{2,3} \le x_4 = x_5 = x_6 \le Rez_{7,8} = x_9 = Rez_{10,11}$. Благодаря этому коды представляют собой более удобный способ описания сегментов и вершин, чем сами задающие системы неравенств.

Нелишне отметить, что код конкретного корня x_k или пары корней $z_{k,k+1} = x_k \pm iy_k$ находится в столбце с минимальным номером l — самом левом, для которого выполняется условие $\sum\limits_{j\leqslant l}(k_{1j} + k_{2j}) \ge k$.

Заметим, что слой вершины определяется как сумма 2-й строки её

кода $\sum\limits_j k_{2j}$; а размерность сегмента легко устанавливается по его коду как сумма $m + \sum\limits_j k_{2j} = \sum\limits_j (sign(k_{1j}) + k_{2j})$.

4 Смежность в орграфе

Коды вершин сегментарного орграфа позволяют легко устанавливать смежность вершин и, тем самым, отношение область — граница для сегментов разных размерностей, а опосредованно — и отношение сопредельности (т.е. граничат ли они между собой) для сегментов равной размерности.

При переходе на межслойную границу с "действительной" стороны одно из нестрогих неравенств меняется на равенство: $x_1 \le ... \le x_k \le \le x_{k+1} \le ... \mapsto x_1 \le ... \le x_k = x_{k+1} \le ... \le x_n$, или для более "кратного" варианта $x_1 \le ... = x_k \le x_{k+1} = ... \le x_n \mapsto x_1 \le ... = x_k = x_{k+1} = ... \le x_n$.

В обоих случаях число столбцов сокращается на единицу, причём в коде складываются l-ый и $l+1$-ый столбцы — именно те, в которых закодированы k-й и $k+1$-й корни (поскольку они разделены неравенством, они находятся обязательно в соседних столбцах):

$$\begin{pmatrix} k_{11} & ... & k_{1l} & k_{1\,l+1} & ... & k_{1m} \\ k_{21} & ... & k_{2l} & k_{2\,l+1} & ... & k_{2m} \end{pmatrix} \mapsto \begin{pmatrix} k_{11} & ... & (k_{1l} & +k_{1\,l+1}) & ... & k_{1\,m-1} \\ k_{21} & ... & (k_{2\,l} & +k_{2\,l+1}) & ... & k_{2\,m-1} \end{pmatrix}.$$

Назовём эту операцию *столбцовым сложением.*

При возвращении на межслойную границу с "мнимой" стороны одна из комплексно сопряжённых пар обращается в кратную действительную пару:

$$x_1 \le ... \le Rez_{k,k+1} \le x_{k+2} \le ... \le x_n \& y_k \ge 0 \mapsto x_1 \le ... \le x_k =$$

$$= x_{k+1} \le x_{k+2} \le ... \le x_n \& y_k = 0;$$

число столбцов при этом не меняется, но единица l-го столбца, в котором закодирована пара $z_{k,k+1} = x_k \pm iy_k$, поднимается из 2-й строки в 1-ю:

$$\begin{pmatrix} k_{11} & ... & k_{1l} & ... & k_{1m} \\ k_{21} & ... & k_{2l} & ... & k_{2m} \end{pmatrix} \mapsto \begin{pmatrix} k_{11} & ... & (k_{1l}+1) & ... & k_{1\,m-1} \\ k_{21} & ... & (k_{2l}-1) & ... & k_{2\,m-1} \end{pmatrix}.$$

Назовём эту операцию *строчным сложением.*

Нетрудно видеть, что и выходы из сегмента на внутрислойные границы, как, например,

$x_1 \le ... \le x_k \le Rex_{k+1} \le ... \le x_n \mapsto x_1 \le ... \le x_k = Rex_{k+1} \le ... \le x_n$,

или даже $x_1 \le ... \le Rex_k \le Rex_{k+2} \le ... \le x_n \mapsto x_1 \le ... \le Rex_k = Rex_{k+2} \le ... \le x_n$ — выражаются в столбцовом сложении кода.

Обе возможности сложения: строчного и столбцового — будем вместе называть просто *сложением.* Разумеется, каждый код допускает множественные возможности сложения, — исключение составляют только двухстолбцовые коды с нулями во второй строке или одностолбцовый код $(n-1\ 1)^T$ (для них есть единственный вариант сложения), а для одностолбцового кода $(n\ 0)^T$ никаких возможностей сложения вообще нет. Нетрудно видеть, что операция сложения понижает найденную по формуле $m + \sum\limits_j k_{2j}$ размерность сегмента как раз на единицу.

Назовём *суммой кода* множество всевозможных кодов, получающихся из него тем или иным сложением.

Обратная операция — *разложение кода* — позволяет ответить и на вопрос, границей каких сегментов предшествующей литеры является сегмент с данным кодом. Естественно, здесь также следует учитывать все возможности разложения (пример 2 в п. 5).

Таким образом, установлен ***критерий смежности***:

Вершины симплектического орграфа соседствующих литер смежны, если код вершины следующей литеры входит в сумму кода вершины предшествующей литеры.

Следствие. Сегменты симплектического неорграфа размерности k граничат по сегменту размерности $k-1$, если пересечение сумм их кодов непусто.

5 Некоторые примеры

Пример 1. Как указывалось в пункте 2, для многочлена 5-й степени пересечение 4-мерных сегментов

$B_1 1 : Rez_{1,2} = x_3 \le x_4 \le x_5 \Longleftrightarrow x_1 = Rez_{2,3} \le x_4 \le x_5$;

$B_1 3 : x_1 \le x_2 \le Rez_{3,4} = x_5 \Longleftrightarrow x_1 \le x_2 \le x_3 = Rez_{4,5}$

оказывается двумерно. Действительно, коды соответствующих сегментов таковы: $\begin{pmatrix} 2 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ и $\begin{pmatrix} 1 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$.

Суммы этих кодов оказываются непересекающимися множествами

$\left\{\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 3 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 1 & 0 \end{pmatrix}\right\}$ и $\left\{\begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 3 \\ 0 & 0 & 0 \end{pmatrix}\right\}$ соответственно.

А вот суммы сумм уже содержат общий элемент $\begin{pmatrix} 4 \\ 1 \end{pmatrix}$ — код сегмента $Rez_{1,2} = x_{3,4,5} \Longleftrightarrow x_{1,2,3} = Rez_{4,5}$.

Пример 2. Рассмотрим сегмент для многочлена 11-й степени, задающийся неравенствами

$Rez_{1,2} = x_3 \leq x_4 = x_5 = x_6 \leq Rez_{7,8} = Rez_{9,10} = x_{11}$

(или $x_1 = Rez_{2,3} \leq x_4 = x_5 = x_6 \leq Rez_{7,8} = x_9 = rez_{10,11}$).

Как уже указывалось, его кодом будет матрица $\begin{pmatrix} 2 & 3 & 3 \\ 1 & 0 & 2 \end{pmatrix}$. Сумма этого кода состоит из матриц $\begin{pmatrix} 3 & 3 & 3 \\ 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 5 & 3 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 6 \\ 1 & 2 \end{pmatrix}$ и $\begin{pmatrix} 2 & 3 & 4 \\ 1 & 0 & 1 \end{pmatrix}\}$. Задающими неравенствами для последнего из них будет, например, система $x_1 = Rez_{2,3} \leq x_{4,5,6} \leq Rez_{7,8} = x_{9,10,11}$.

А разложения данного кода приводят к кодам сегментов, чьей границей он, в свою очередь, является. Поскольку этот код не мог быть получен сложением строк (в этом случае элемент второй строки был бы больше вышележащего), остаются разложения столбцов:

$\begin{pmatrix} 1 & 1 & 3 & 3 \\ 0 & 1 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 3 & 3 \\ 1 & 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 3 & 3 \\ 1 & 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 & 2 & 3 \\ 1 & 0 & 0 & 2 \end{pmatrix}$,
$\begin{pmatrix} 2 & 2 & 1 & 3 \\ 1 & 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 3 & 1 & 2 \\ 1 & 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 3 & 2 & 1 \\ 1 & 0 & 2 & 0 \end{pmatrix}$ и, наконец,
$\begin{pmatrix} 2 & 3 & 2 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$ и $\begin{pmatrix} 2 & 3 & 1 & 2 \\ 1 & 0 & 1 & 1 \end{pmatrix}$. Соответствующие системы неравенств без труда выписываются.

СПИСОК ЛИТЕРАТУРЫ

[1] **Воевода А.А., Плохотников В.В., Чехонадских А.В.** О совмещённых декартовых координатах в пространстве корней многочленов с действительными коэффициентами // Сб. науч. тр. НГТУ. — Новосибирск: Изд-во НГТУ, 2001.— №1 (23).— с.153–156.

[2] **Воевода А.А., Чехонадских А.В.** Координатизация системы корней вещественных многочленов малых степеней// Науч. вестн. НГТУ. — Новосибирск: Изд-во
НГТУ, 2005. — №3(21). — С.177–180.

[3] **Воевода А.А., Чехонадских А.В.** Координатизация системы корней вещественных многочленов степени 5// Науч. вестн. НГТУ. — Новосибирск: Изд-во НГТУ, 2006. — №1(22). — С.176–179.

[4] **Чехонадских А.В.** Свойства корневых симплексов многочленов с действительными коэффициентами // Науч. вестн. НГТУ. — Новосибирск: Изд-во НГТУ, 2007. — №1(26). — С.101–108.

[5] **Воевода А.А., Чехонадских А.В.** Орграфы граничных сегментов корневых симплексов вещественных многочленов. // Науч. вестн. НГТУ. — Новосибирск: Изд-во НГТУ, 2007. — №1(26). — С.191–196.

ВЕРОЯТНОСТЬ ДИАГОНАЛИЗИРУЕМОСТИ МАТРИЦЫ НАД КОНЕЧНЫМ ПОЛЕМ

В.А. Чуркин

Институт математики СО РАН
Россия, 630090, Новосибирск, пр. Коптюга 4
Новосибирский государственный университет
Россия, 630090, Новосибирск, пр. Коптюга 2
e-mail: churkin@math.nsc.ru

Пусть $M_n(F)$ – алгебра квадратных матриц порядка n над полем F. Матрица A называется диагонализируемой над полем F, если существует такая обратимая матрица C из $M_n(F)$, что матрица $D = C^{-1}AC$ — диагональна. Равносильное условие — векторное пространство размерности n над полем F относительно линейного оператора с матрицей A обязательно имеет базис, состоящий из собственных векторов оператора. Характеристический многочлен диагонализируемой матрицы разлагается над полем F на линейные множители. Имеется два препятствия к диагонализируемости: 1) характеристический многочлен имеет корни, не принадлежащие полю F, 2) жорданова форма матрицы может быть недиагональной.

Пусть теперь $F = F_q$ — конечное поле порядка q. Обозначим через $GL_n(F) = GL_n(q)$ — группу обратимых матриц, а через $D_n(F) = D_n(q)$ — множество всех диагонализируемых над $F = F_q$ матриц из $M_n(F) = M_n(q)$. Цель работы — подсчитать долю

$$P_n(q) = \frac{|D_n(q|}{|M_n(q)|}$$

диагонализируемых матриц в алгебре $M_n(q)$ и найти асимптотическую вероятность диагонализируемости

$$P_n = \lim_{q \to \infty} P_n(q)$$

матриц порядка n над большими конечными полями.

Прежде, чем сформулировать ответ, введём обозначения. Пусть дано монотонное разбиение натурального числа n в сумму s натуральных слагаемых

$$n = k_1 + k_2 + \cdots + k_s, \quad k_1 \geqslant k_2 \geqslant \cdots \geqslant k_s.$$

Оно определяет r блоков совпадений длин $n_1,\ n_2, \ldots, n_r$:

$$k_1 = k_2 = \ldots = k_{n_1} > k_{n_1+1} = \ldots = k_{n_1+n_2} > \ldots > k_{n_1+\ldots+n_{r-1}+1} = \ldots =$$

$$= k_{n_1+\ldots+n_r}.$$

Обозначим

$$N(k_1, \ldots, k_s) = n_1!\, n_2! \cdots n_r!$$

— число всевозможных перестановок, сохраняющих блоки совпадений.

Теорема 1.

$$P_n(q) = \frac{|GL_n(q)|}{|M_n(q)|} \sum_{s=1}^{n} \sum_{\substack{k_1 + \cdots + k_s = n, \\ k_1 \geqslant \cdots \geqslant k_s}} \frac{q(q-1)\ldots(q-s+1)}{N(k_1, \ldots, k_s) \prod_{i=1}^{s} |GL_{k_i}(q)|}.$$

Теорема 2.

$$\lim_{q\to\infty} P_n(q) = \frac{1}{n!}.$$

Доказательство теоремы 1. Класс матриц, подобных диагональной, однозначно задается характеристическим многочленом матрицы, причем все корни многочлена лежат в данном поле. В свою очередь такой многочлен определяется множеством корней $\lambda_1, \ldots, \lambda_s$ и их кратностей $k_1, \ldots, k_s$, при этом $k_1 + \cdots + k_s = n$ — степень многочлена или порядок матрицы . Можно также предполагать, что набор кратностей монотонен $k_1 \geqslant \cdots \geqslant k_s$. Если набор кратностей строго монотонен: $k_1 > k_2 > \cdots > k_s$, то выборка корней образует размещение из q элементов по s и однозначно определяет характеристический многочлен

$$\prod_{i=1}^{s} (\lambda - \lambda_i)^{k_i}.$$

Таких многочленов $q(q-1)\cdots(q-s+1)$. Если же набор кратностей не строго монотонен, то он разбивается на блоки совпадений длин $n_1,\ n_2,$ $\ldots, n_r$. В пределах одного блока совпадений кратностей корни можно переставлять без изменения характеристического многочлена. Поэтому

в общем случае число характеристических многочленов диагонализируемых матриц над полем из q элементов с монотонным набором кратностей $k_1, \ldots, k_s$ равно

$$\frac{q(q-1)\cdots(q-s+1)}{N(k_1,\ldots,k_s)}.$$

Фиксируем диагональную матрицу $D = Diag(\lambda_1, \ldots, \lambda_1, \lambda_2, \ldots, \lambda_2, \ldots \lambda_s, \ldots, \lambda_s)$ с указанным характеристическим многочленом. Тогда мощность класса сопряженных (или подобных) матриц $A = CDC^{-1}$ с матрицей D в алгебре $M_n(q)$ равно индексу централизатора матрицы D в группе $GL_n(q)$. Поскольку матрица D составлена из диагональных клеток различных скалярных матриц порядков $k_1, \ldots, k_s$, то любая обратимая коммутирующая с ней матрица тоже клеточно диагональна с обратимыми клетками порядков $k_1, \ldots, k_s$. Таким образом, порядок централизатора матрицы D в $GL_n(q)$ равен $\prod_{i=1}^{s} |GL_{k_i}(q)|$, а его индекс —

$$\frac{|GL_n(q)|}{\prod_{i=1}^{s} |GL_{k_i}(q)|}.$$

Суммируя мощности классов матриц, подобных диагональным матрицам в алгебре $M_n(q)$ по всем характеристическим многочленам, получим

$$|D_n(q)| = \sum_{s=1}^{n} \sum_{\substack{k_1+\cdots+k_s=n,\\ k_1 \geqslant \cdots \geqslant k_s}} \frac{q(q-1)\ldots(q-s+1)|GL_n(q)|}{N(k_1,\ldots,k_s)\prod_{i=1}^{s}|GL_{k_i}(q)|}.$$

Доля $P_n(q)$ диагонализируемых матриц получается отсюда делением на $|M_n(q)|$.

Доказательство теоремы 2 получается из теоремы 1 с использованием известной леммы.

Лемма. $|M_n(q)| = q^{n^2}$, $|GL_n(q)| = \prod_{i=0}^{n-1}(q^n - q^i)$.

Отсюда сразу получается, что

$$\lim_{q\to\infty} \frac{|GL_n(q)|}{|M_n(q)|} = \lim_{q\to\infty} \prod_{i=0}^{n-1}(1 - q^{i-n}) = 1.$$

Кроме того, как многочлен от q числитель в формуле из теоремы 1 имеет вид

$$q(q-1)\cdots(q-s+1) = q^s + \ldots,$$

где многоточием обозначена сумма младших степеней q с коэффициентами, зависящими только от $0, 1, \ldots, s-1 < n$. С другой стороны, в знаменателе произведение

$$\prod_{i=1}^{s} |GL_{k_i}(q)| = q^{k_1^2+\ldots+k_s^2} + \ldots$$

является многочленом от q степени $k_1^2 + \ldots + k_s^2$, причем коэффициенты при младших степенях q зависят только от разложения n в сумму натуральных чисел. Поскольку $s \leqslant n = k_1 + \ldots + k_s \leqslant k_1^2 + \ldots + k_s^2$ с учётом натуральности $k_1, \ldots, k_s$, то равенство степеней числителя и знаменателя возможно только лишь в случае, когда $k_1 = \ldots = k_s = 1$ и $s = n$. В этом случае $N(1, \ldots, 1) = n!$. Соответствующее слагаемое суммы из теоремы 1 стремится к $1/n!$ при q, стремящемся к бесконечности, а остальные слагаемые стремятся к нулю, число слагаемых зависит только от n. Теорема 2 доказана.

Мы видим, что больше всего диагонализируемых матриц, характеристический многочлен которых не имеет кратных корней.

Теперь оценим роль факторов недиагонализируемости. Обозначим через $J_n(q)$ множество матриц из $M_n(q)$ с недиагональной жордановой формой, характеристические корни которых принадлежат F_q. Найдем асимптотическую долю таких матриц для больших конечных полей, т.е.

$$\lim_{q\to\infty} \frac{|J_n(q)|}{|M_n(q)|}.$$

Снова предположим, что матрица A имеет характеристический многочлен с различными корнями $\lambda_1, \ldots, \lambda_s$ из F_q кратностей $k_1 \geqslant \ldots \geqslant k_s$, $k_1 + \cdots + k_s = n$ — степень многочлена или порядок матрицы. Пусть жорданова форма J матрицы A состоит из жордановых клеток $J_1, \ldots, J_m$ порядков $l_1, \ldots, l_m$, $l_1 + \ldots + l_m = n$. Известно, что централизатор жордановой клетки порядка l в алгебре $M_n(q)$ состоит из многочленов над F_q от этой клетки и имеет порядок q^l. Поэтому централизатор матрицы J имеет порядок, не меньший, чем $q^{l_1+\ldots+l_m} = q^n$. Отсюда мощность класса сопряженности матрицы J не больше, чем $|GL_n(q)|/q^n$. С другой стороны, поскольку жорданова форма недиагональна, то характеристический многочлен обязательно имеет кратные корни и с фиксированным набором кратностей $k_1 \geqslant \ldots \geqslant k_s$ число таких многочленов равно

$$\frac{q(q-1)\cdots(q-s+1)}{N(k_1, \ldots, k_s)},$$

где $s < n$. Следовательно, частное $|J_n(q)|/|M_n(q)|$ не больше, чем сумма слагаемых типа

$$C_n \cdot \frac{|GL_n(q)|}{|M_n(q)|} \cdot \frac{q(q-1)\dots(q-s+1)}{q^n}.$$

Здесь количество слагаемых суммы и коэффициент C_n определяются разбиением n в сумму кратностей корней и количеством неподобных жордановых форм порядка n. т. е ограничены в зависимости от n. Поскольку $s < n$, то верна

Теорема 3.

$$\lim_{q\to\infty} \frac{|J_n(q)|}{|M_n(q)|} = 0.$$

Следовательно, главный фактор недиагонализируемости матрицы над конечным полем состоит в том, что характеристический многочлен имеет корни вне данного конечного поля.

В заключение стоит отметить, что интересно было бы найти при фиксированном конечном поле асимптотику соответствующих долей матриц $D_n(q)$ и $J_n(q)$ при порядках матриц, стремящихся к бесконечности.

О ГРУППАХ С КОМПОЗИЦИОННЫМ ФАКТОРОМ, ИЗОМОРФНЫМ ЗНАКОПЕРЕМЕННОЙ ГРУППЕ СТЕПЕНИ 7

И.Б. Горшков

Новосибирский государственный университет
e-mail: ilygor@ngs.ru

1 Введение

Пусть G — конечная группа, $\pi(G)$ — множество всех простых делителей ее порядка и $\omega(G)$ — спектр группы G, т. е. множество порядков всех ее элементов. Для произвольного подмножества ω множества $\mathbb{N}$ натуральных чисел обозначим через $h(\omega)$ число попарно неизоморфных конечных групп G таких, что $\omega(G) = \omega$. Мы будем говорить, что для конечной группы G *проблема распознаваемости решена*, если мы знаем значение $h(\omega(G))$ (для краткости, $h(G)$). В частности, группа G называется *распознаваемой по спектру* (кратко, распознаваемой), если $h(G) = 1$. Последний по времени обзор результатов в этой области см. в [1].

Граф $GK(G) = \langle V(GK(G)), E(GK(G))\rangle$, где $V(GK(G))$ — множество вершин и $E(GK(G))$ — множество ребер, называется *графом Грюнберга — Кегеля* (или *графом простых чисел*) группы G, если $V(GK(G)) = \pi(G)$ и ребро (r, s) лежит в $E(GK(G))$ тогда и только тогда, когда $rs \in \omega(G)$. Простые числа $r, s \in \pi(G)$ называются *смежными*, если они смежны как вершины графа $GK(G)$, т. е. $(r, s) \in E(GK(G))$. В противном случае, r и s называются *несмежными*. Обозначим через $s(G)$ число связных компонент этого графа и через $\pi_i(G)$, $i = 1, ..., s(G)$, его i-ю компоненту. Если группа G имеет четный порядок, то положим $2 \in \pi_1(G)$. Обозначим через $\omega_i(G)$ множество, состоящее из $n \in \omega(G)$ таких, что каждый простой делитель числа n принадлежит $\pi_i(G)$.

Большинство групп, для которых проблема распознаваемости решена, имеют несвязный граф простых чисел, поскольку теорема Грюнбер-

га — Кегеля и классификация конечных простых групп с несвязным графом простых чисел, полученная Уильямсом и Кондратьевым[3, 2], являются важной частью доказательства их распознаваемости.

Теорема А *(Грюнберг – Кегель). Если конечная группа G имеет несвязный граф $GK(G)$, то выполняется одно из следующих условий:*

(а) $s(G) = 2$ *и* G *– группа Фробениуса;*

(б) $s(G) = 2$ *и* G *– двойная группа Фробениуса;*

(в) существует неабелева простая группа S *такая, что* $S \leq \overline{G} = G/K \leq Aut(S)$*, где* K *– максимальная нормальная разрешимая подгруппа группы* G*. Кроме того, группа* K *нильпотентна,* K *и* $\overline{G}/S$ *являются* $\pi_1(G)-$*группами, граф* $GK(S)$ *несвязен,* $s(S) \geq s(G)$*, и для любого числа* i*,* $2 \leq i \leq s(G)$*, существует* j*,* $2 \leq j \leq s(S)$*, такое, что* $\omega_i(G) = \omega_j(S)$*.*

Доказательство. См. [2].

При использовании теоремы Грюнберга — Кегеля применительно к проблеме распознаваемости конечных простых групп полезной оказывается работа Алеевой [4], в которой описаны конечные простые группы со спектром как у группы Фробениуса или двойной группы Фробениуса, что позволяет исключить из рассмотрения случаи (а) и (б) заключения теоремы.

Доказательство теоремы Грюнберга — Кегеля существенно использует тот факт, что в группе G найдется элемент простого нечетного порядка, не связанный в $GK(G)$ с простым числом 2. Оказывается (см. теорему Б), что требование несвязности графа простых чисел в большинстве случаев может быть заменено более слабым требованием несмежности числа 2 с хотя бы одним нечетным простым числом.

Обозначим через $t(G)$ неплотность графа простых чисел, т. е. наибольшее число попарно несмежных вершин. Через $t(2, G)$ обозначим 2-неплотность, т. е. наибольший порядок независимого множества вершин, содержащего 2 (множество вершин графа называется *независимым*, если его вершины попарно несмежны).

Теорема Б *(Васильев). Пусть G – конечная группа, удовлетворяющая двум условиям:*
(а) существует три простых числа из $\pi(G)$, попарно несмежных в $GK(G)$, т.е. $t(G) \geq 3$.
(б) существует нечетное простое число из $\pi(G)$, несмежное в $GK(G)$ с 2, т.е. $t(2, G) \geq 2$.

Тогда существует конечная неабелева простая группа S такая, что $S \leq \overline{G} = G/K \leq Aut(S)$ для максимальной нормальной разрешимой подгруппы K группы G. Кроме того, $t(S) \geq t(G) - 1$, и выполнено одно из следующих условий.
(1) *$S \simeq Alt_7$ или $A_1(q)$ для некоторого нечетного числа q и $t(S) = t(2, S) = 3$.*
(2) *Для каждого простого числа $p \in \pi(G)$, несмежного с 2 в $GK(G)$, силовская p-подгруппа группы G изоморфна силовской p-подгруппе группы S. В частности $t(2, S) \geq t(2, G)$.*

Доказательство. См. [5]

При использовании теоремы Б для решения проблемы распознаваемости конечных простых групп возникает естественный вопрос: когда в конечной группе, удовлетворяющей условию теоремы, выполняется пункт (1) заключения теоремы? В настоящей работе получен частичный ответ на этот вопрос.

Теорема. *Пусть L — конечная неабелева простая группа, G — конечная группа такая, что $\omega(G) = \omega(L)$, и $S \leq G/K \leq Aut(S)$, где K – максимальная нормальная разрешимая подгруппа группы G, $S \simeq Alt_7$ и $Aut(S) \simeq Sym_7$. Тогда $L \simeq G \simeq Alt_7$.*

Следствие. *Пусть L — неабелева конечная простая группа, отличная от групп Alt_7, Alt_n, где n таково, что среди чисел $n, n-1, n-2, n-3$ нет простых. Если G — конечная группа, удовлетворяющая условию $\omega(G) = \omega(L)$, то среди композиционных факторов группы G нет фактора, изоморфного Alt_7.*

2 Предварительные результаты

Лемма 1. *Пусть L — конечная простая группа, отличная от групп $A_2(3)$, ${}^2A_3(3)$, $C_2(3)$, Alt_{10} и групп Alt_n, где n выбрано так, что среди чисел $n, n-1, n-2, n-3$ нет простых. Пусть G — конечная группа, удовлетворяющая условию $\omega(G) = \omega(L)$. Тогда для группы G имеет место заключение теоремы Б. В частности, G имеет единственный неабелев композиционный фактор.*

Доказательство. См. [6, следствие 7.2].

Лемма 2. *Если $t(G) \geq 3$, то группа G — неразрешима.*

Доказательство. См. [5, предложение 1].

Лемма 3. *Пусть G — конечная неразрешимая группа и $t(2,G) \geq 2$, S – конечная простая неабелева группа такая, что $S \leq \overline{G} = G/K \leq Aut(S)$ для максимальной нормальной разрешимой подгруппы K группы G. Тогда $t(S) \geq t(G) - 1$. Более того, для каждого подмножества ρ простых чисел из $\pi(G)$ такого, что $|\rho| \geq 3$ и все числа из ρ попарно несмежны в $GK(G)$, не более чем одно число из ρ делит произведение $|K| \cdot |\overline{G}/S|$.*

Доказательство. См. [5, предложение 3].

Поскольку множество $\omega(G)$ частично упорядочено по делимости, оно однозначно определяется множеством $\mu(G)$ своих максимальных по делимости элементов.

Лемма 4. *Пусть G — конечная простая группа и $s(G) \geq 2$. Тогда $|\mu(G) \cap \omega_i(G)| = 1$ при $i > 1$.*

Доказательство. См. [7, лемма 2].

Лемма 5. *Пусть G — конечная группа, $N \lhd G$, G/N – группа Фробениуса с ядром F и циклическим дополнением C. Если $(|F|, |N|) = 1$ и F не содержится в $NC_G(N)/N$ то $p|C| \in \omega(G)$ для некоторого простого делителя p числа $|N|$.*

Доказательство. См. [8, лемма 1].

Лемма 6. *Пусть p и q – различные простые числа. $H\langle a\rangle$ – такое полупрямое произведение нормальной $\{2,q,p\}'$-группы H и группы $\langle a\rangle$ порядка p, что $[H,a] \neq 1$. Если $H\langle a\rangle$ действует точно на некотором векторном пространстве V над полем порядка q, то $C_V(a) \neq 0$.*

Доказательство. См. [9].

Лемма 7. *(Жигмонди). Пусть a, s — натуральные числа, $a, s \geq 2$. Тогда верно одно из следующих утверждений:*
(а) существует простое число r такое, что r делит $a^s - 1$ и r не делит $a^t - 1$ при любом натуральном $t < s$;
(б) $s = 6$ и $a = 2$;
(в) $s = 2$ и $a = 2^t - 1$ для некоторого натурального числа t.

Доказательство. См. [10].

Число r, отличное от 2 и удовлетворяющее пункту (а) теоремы, называется примитивным делителем числа $a^s - 1$. Следуя [6], будем считать, что число 2 есть примитивный делитель числа $a-1$, если $a \equiv 1(\mod 4)$, и 2 есть примитивный делитель числа a^2-1, если $a \equiv -1(\mod 4)$. Если число a фиксировано, будем обозначать примитивный делитель числа $a^s - 1$ через r_s (ясно, что таких делителей может быть несколько).

Лемма 8. *Пусть $S = A_1(q)$, где $q = p^k$, p — простое число, и группа G такова, что $S \leq G \leq Aut(S)$. Тогда $t(G) \leq 3$. Если $t(G) = 3$, то каждое максимальное независимое множество ρ из $V(GK(G))$ содержит примитивные делители r_1 и r_2 чисел $q-1$ и q^2-1 соответственно.*

Доказательство. Из [6] вытекает, что каждое максимальное независимое множество вершин графа $GK(S)$ имеет вид $\{p, r_1, r_2\}$, где r_1 и r_2 — примитивные делители чисел $q-1$ и q^2-1 соответственно. Пусть ρ — некоторое максимальное независимое подмножество вершин графа $GK(G)$. По лемме 3 не более чем одно из чисел из ρ делит порядок G/S. Следовательно, если $t(G) > 3$, то $\rho = \{p, r_1, r_2, s\}$, где s — нечетный простой делитель числа $|G/S|$. Однако в централизаторе любого автоморфизма группы S нечетного порядка содержится элемент порядка p, следовательно, $t(G) \leq 3$. Аналогично, если $t(G) = 3$ и ρ содержит лишь одно из чисел r_1, r_2, то ρ содержит и p, и s одновременно, что невозможно.

Лемма 9. *Если $p^a - r^b = 1$, где p и r — простые числа, то выполняется одно из утверждений:*
1) $a = 1$
2) $b = 1$
3) $p = 3,\ a = 2,\ r = 2,\ b = 3$.

Доказательство. Утверждение является следствием леммы 7.

Лемма 10. *Если $p^{4k} + p^{2k} + 1 = q^l$, где p и q — простые числа, то $k = 0$.*

Доказательство. Имеет место следующая цепочка равенств: $p^{4k} + p^{2k} + 1 = p^{4k} + 2 \cdot p^{2k} + 1 - p^{2k} = (p^{2k}+1)^2 - p^{2k} = (p^{2k} + p^k + 1)(p^{2k} - p^k + 1)$.

Допустим $k \neq 0$, в этом случае $(p^{2k} - p^k + 1) > 1$. Следовательно, $(p^{2k} - p^k + 1)$ и $(p^{2k} + p^k + 1)$ делятся на q. Поэтому разность $(p^{2k} - p^k + 1)$

и $(p^{2k}+p^k+1)$, равная $2\cdot p^k$, тоже делится на q. Получаем, что q равно либо 2, либо p, но $p^{4k}+p^{2k}+1$ не делится на 2 и на p; противоречие.

Лемма 11. *Если* $p^{2n}+1=2\cdot 5^k$ *и* p *— простое, то* $p=3$ *или* $p=7$.

Доказательство. Решим уравнение $x^2-a\cdot y^2=(-1)^n$. Формула вычисления $n\cdot k$-ого решения имеет вид (см. [11, стр 341]): $x_{n\cdot k}=\frac{a_{k+}^n+a_{k-}^n}{2}$, $y_{n\cdot k}=\frac{a_{k+}^n-a_{k-}^n}{2\sqrt{a}}$, где $a_{k+}=x_k+\sqrt{a}y_k$, $a_{k-}=x_k-\sqrt{a}y_k$. Пусть $a=2$. Тогда, решение можно записать в рекуррентной форме (см. [12, стр 43]): $x_n=x_{n-1}+ay_{n-1}$, $y_n=x_{n-1}+y_{n-1}$, $x_0=1$, $y_0=0$. Первое решение такое, что $y=5^l$, имеет вид $x_3=7, y_3=5$. С помощью рекуррентной записи решения, легко показать, что решения y_{3n+1} и y_{3n-1} не делятся на 5. Таким образом, общий вид решений таких, что $y=5g$, можно записать так: $y_{3n}=\frac{a_{3+}^n-a_{3-}^n}{2\sqrt{2}}=\frac{((x_3+\sqrt{2}y_3)-(x_3-\sqrt{2}y_3))(a_{3+}^{n-1}\ldots a_{3-}^{n-1})}{2\sqrt{2}}=y_3(a_{3+}^{n-1}+\ldots+a_{3-}^{n-1})=5(a_{3+}^{n-1}+\ldots+a_{3-}^{n-1})$. У чисел $s=a-b$ и $f=a^{n-1}+ba^{n-2}+\ldots+b^{n-2}a+b^{n-1}$, если хотя бы одно из них нечетно, существует взаимно простые делители. Следовательно, $y_t=5^l$ только в том случае, если $n=1$. В этом случае $t=3$, $x=7$, $y=5$, а значит, $p^2+1=2\cdot 5^2$. Случай, когда $a=10$, разбирается аналогично, и возможен только, если $y=1, x=3$. Лемма доказана.

Лемма 12. *Для любого числа* x*, большего* 12*, существуют не меньше трех различных простых чисел* p_1, p_2, p_3 *таких, что* $p_i\le x$, $p_i+p_j>x$, *где* $0<i,j\le 3$ *и* $i\ne j$.

Доказательство. Пусть $\pi(x)$ – число простых чисел, меньших или равных x. Существует оценка $0,921\cdot(x/ln(x))<\pi(x)<1,106\cdot(x/ln(x))$ (см. [13, глава 35, §1]). Пусть $\psi(x)$ — число простых чисел в интервале $[x/2,x]$, тогда $\psi(x)=\pi(x)-\pi(x/2)$, $\phi(x)=\frac{x(0{,}368\cdot ln(x)-1)}{ln(x)(ln(x)-ln(2))}$, тогда $\psi(x)\ge\frac{0{,}921\cdot x}{ln(x)}-\frac{1{,}106\cdot x/2}{ln(x/2)}=\frac{x(0{,}368\cdot ln(x)-1)}{ln(x)(ln(x)-ln(2))}=\phi(x)$. Функция $\phi(x)$ монотонно возрастает и при $x\ge 51$ выполнено неравенство $\phi(x)>3$. Следовательно, и $\psi(x)>3$ при $x>51$. Проверяем значения $\psi(x)$ для $x<51$: $\psi(6)=2$, $\psi(7)=2$, $\psi(8)=2$, $\psi(9)=2$, $\psi(10)=2$, $\psi(11)=3$, $\psi(12)=2$, $\psi(x)\ge 3$, где $13\le x\le 51$. Лемма доказана.

3 Исключительные случаи

В этом пункте мы докажем основную теорему для тех простых групп L, рассмотрение которых не укладывается в общую схему доказательства.

Лемма 13. *Если группа L удовлетворяет условиям теоремы, то L не изоморфна следующим группам: $A_3(4)$, $C_4(2)$,${}^2A_3(5)$, $B_3(3)$, $D_4(3)$.*

Доказательство. Допустим, L изоморфна одной из групп $A_3(4)$, $C_4(2)$,${}^2A_3(5)$, $B_3(3)$, $D_4(3)$, и группа G удовлетворяет условиям теоремы. Пусть $\widetilde{G}$ некоторая секция группы G. Очевидно, что $\omega(\widetilde{G}) \subseteq \omega(G)$. Если мы покажем, что $\omega(\widetilde{G}) \nsubseteq \omega(L)$, то $\omega(G) \nsubseteq \omega(L)$, и получится требуемое противоречие.

Пусть $r = 17$, если $L \simeq A_3(4)$ или $C_4(2)$, и $r = 13$, если $L \simeq B_3(3)$, ${}^2A_3(5)$ или $D_4(3)$. Пусть $R = Syl_r(K)$, $N = N_G(R)$. В силу аргумента Фраттини $G/K \simeq N/N \cap K \simeq \overline{G}$. Таким образом, $\omega(N) \supseteq \omega(S)$. Следовательно, в N есть элемент порядка 3. Пусть H силовская 3-подгруппа группы N. Тогда H действует на R без неподвижных точек, так как в N нет элемента порядка $3r$. Следовательно HR — группа Фробениуса с дополнением H. Значит, силовская 3-подгруппа группы N циклическая, следовательно, и в $\overline{G}$ силовская 3-подгруппа должна быть циклической; противоречие.

Лемма 14. *Если L такая как в условии теоремы, то L не изоморфна группе ${}^2A_2(5)$.*

Доказательство. Допустим $L \simeq {}^2A_2(5)$. Тогда $\mu(L) = \{10, 8, 7, 6\}$. Поскольку $12 \in \omega(Sym_7)$, имеем $G/K = S \simeq Alt_7$. Группа K нильпотентна по теореме A, так как граф группы L, а значит, и группы G несвязен. Обозначим через R силовскую r-подгруппу группы K. Заметим, что группа S действует на R точно, иначе $C_G(R)K = G$, и в G найдется элемент порядка $7r$ при $r \neq 7$ или элемент порядка 35 при $r = 7$, что сразу приведет нас к противоречию. Пусть $r = 5$ или 7. Поскольку силовская 3-подгруппа в S есть элементарная абелева группа порядка 3^2, то она не может действовать на R без неподвижных точек. Следовательно, в расширении RS, а значит, и в расширении KS, есть элемент порядка $3r$; противоречие. Пусть $r = 3$. Группа S содержит подгруппу Фробениуса с ядром порядка 7 и дополнением порядка 3. Поэтому по лемме 5 в G найдется элемент порядка 9, что невозможно. Таким образом, мы можем считать, что K является 2-группой. Рассматривая факторгруппу G по подгруппе Фраттини группы K, можно полагать, что K — элементарная абелева 2-группа, которую можно рассматривать как векторное пространство над полем характеристики 2. Рассмотрим представление S над K. Переходя при необходимости к S-инвариантному подмодулю, можно считать, что это представление неприводимо. Поскольку в группе L нет элемента порядка 14, то любой элемент порядка

7 из группы S не может иметь в указанном представлении неподвижных точек. Используя таблицу брауэровых 2-характеров группы Alt_7 несложно установить, что единственное неприводимое представление, в котором элемент порядка 7 группы S не имеет неподвижных точек, имеет размерность 6. Это представление может быть получено из естественного подстановочного 7-мерного представления группы S над полем характеристики 2 факторизацией исходного пространства по одномерному подпространству, порожденному вектором, равным сумме всех семи базисных векторов. Если мы обозначим через $v_1, \ldots, v_6$ базис полученного 6-мерного пространства, а через v_7 вектор, равный их сумме, то в этом представлении действие преобразования $\varphi(g)$, соответствующего подстановке $g \in S$, на данных векторах определено следующим образом: $v_i\varphi(g) = v_{ig}$. Предположим, что в группе G нет элементов порядка 12. Это означает, что каждый элемент $a \in S$ порядка 6 аннулируется многочленом $x^5+x^4+x^3+x^2+x+1$. Однако матрица элемента $a = (123)(45)(67)$ порядка 6 имеет в указанном базисе вид:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Непосредственно вычисляя матрицу $a^5 + a^4 + a^3 + a^2 + a + 1$, определяем, что она не является нулевой. Таким образом, в G найдется элемент порядка 12. Поскольку $12 \notin \omega(L)$, лемма доказана.

Лемма 15. *Если группа L удовлетворяет условию теоремы, то L не изоморфна группе J_2.*

Доказательство. Допустим $L \simeq J_2$. Тогда $\mu(L) = \{15, 12, 10, 8, 7\}$ и, следовательно, $2 \in \omega(K)$, а также $3 \in \omega(K)$ или $5 \in \omega(K)$. В частности, группа K нетривиальна. По теореме А группа K нильпотентна. Допустим, что $5 \in \pi(K)$, тогда группа S действует на силовской 5-подгруппе группы K точно (иначе в G есть элемент порядка $7 \cdot 5$). Пусть $R_5 \simeq Syl_5(K)$. Переходя к фактор-группе по подгруппе Фраттини группы R_5, мы можем рассматривать R_5 как точный $\overline{G}$-модуль над полем характеристики 5. Воспользуемся таблицей брауровых 5-характеров группы S (см. [14]). Имеется лишь два неприводимых модуля V_1 и V_2, в которых элемент порядка 7 группы S не имеет неподвижных точек, оба размерности 6. Пусть элемент $x \in S$ имеет порядок 6. Тогда $\dim C_{V_1}(x) =$

$\dim C_{V_2}(x) = 2$, поэтому в группе G есть элемент порядка 30; противоречие. Следовательно, в K нет элемента порядка 5. Значит, $3 \in \pi(K)$.

Предположим вначале, что $\overline{G} = G/K \simeq Alt_7$. В L, а значит, и в G, существуют элементы порядков 10 и 15. Поскольку все группы порядка 5 в Alt_7 сопряжены, и в Alt_7 нет элементов порядка 10 и 15, то найдется элемент $x \in G$ порядка 5, централизующий элементы $y \in R_2$ и $z \in R_3$ порядков 2 и 3 соответственно. Тогда элемент $xyz \in G$ имеет порядок 30. Поскольку в L нет элемента такого порядка, мы пришли к потиворечию.

Пусть $\overline{G} = G/K \simeq Sym_7$. Группа $\overline{G}$ действует на группе R_3 точно. Переходя к фактор-группе по подгруппе Фраттини группы R_3, мы можем рассматривать R_3 как точный $\overline{G}$-модуль над полем характеристики 3. Пусть V — неприводимый $\overline{G}$-подмодуль этого модуля. Воспользуемся таблицей брауровых 3-характеров группы Sym_7 (см. [14]). Имеется лишь два неприводимых модуля V_1 и V_2, в которых элемент порядка 7 группы Sym_7 не имеет неподвижных точек, оба размерности 6. Пусть элемент $x \in Sym_7$ имеет порядок 10. Тогда $\dim C_{V_1}(x) = \dim C_{V_2}(x) = 1$, поэтому в группе G есть элемент порядка 30; противоречие. Лемма доказана.

Лемма 16. *Если группа L удовлетворяет условию теоремы, то L не изоморфна группе Alt_{10}.*

Доказательство. Допустим $L \simeq Alt_{10}$. Тогда $\mu(L) = \{21, 15, 12, 10, 9, 8\}$. Поскольку $9, 8 \notin \omega(\mathrm{Aut}(\mathrm{Alt}_7))$, порядок K делится на 6.

Если порядок K делится на 7, то холлова $\{2, 7\}$-подгруппа группы K является группой Фробениуса или двойной группой Фробениуса, поскольку в G нет элемента порядка 14. Если K является группой Фробениуса и ее ядро R – 7-группа, то силовская 2-подгруппа из K — группа с единственной инволюцией и по аргументу Фраттини в G есть элемент порядка $14 \notin \omega(Alt_{10})$. Поэтому силовская 7-подгруппа из K — группа порядка 7 и снова по замечанию Фраттини в G есть элемент порядка 14. Итак, порядок K не делится на 7.

Предположим, что порядок K делится на 5. Если R — силовская 7-подгруппа из G, то R нормализует холлову $\{2, 5\}$-подгруппу H из K и действует на ней без неподвижных точек. По теореме Томпсона H нильпотентна. По замечанию Фраттини $G = N_G(H) \cdot K$, поэтому $N_G(H)/N_K(H) \simeq G/K$. Понятно, что $N_K(H)/H$ — 3-группа. Пусть T — силовская 3-подгруппа из $N_K(H)$. Тогда $K = HT$ и $C_K(H) \cap T = 1$. По замечанию Фраттини некоторая силовская 7-подгруппа U из $N_G(H)$ нормализует T. Предположим, что $[K, T] \neq 1$. Ясно, что $[K, T]$ не централизует некоторую силовскую q-подгруппу Q из H для q, равного

одному из чисел 2 или 5. По лемме 6 (в ней p =7, $\langle a\rangle = U, H = T/C_T(P)$) имеем $C_p(K) \neq 1$, что неверно. Поэтому $[K,T]$ =1 и, следовательно, $C_G(T)\cap N_G(H)$ обладает композиционным фактором, изоморфным Alt_7.

Таким образом, в G есть секция вида $(H_2 \times H_5).3.Alt_7$ или $(H_2 \times H_5).Alt_7$, где H_2, H_5 — силовские 2- и 5-подгруппы группы H.

Из таблиц 2- и 5-модулярных характеров группы $3.Alt_7$ вытекает, что любое неприводимое представление группы $3.Alt_7$ над полем характеристики 2 или 5, в котором элемент порядка 7 действует без неподвижных точек, обладает тем свойством, что в $3.Alt_7$ или в Alt_7 существует элемент порядка 3, который обладает неподвижной точкой в этом представлении. Поэтому в G есть элемент порядка $30 \notin \omega(Alt_{10})$. Итак, K является {2,3}-группой, порядок которой делится на 6.

Положим S_0 =1, $S_1 = O_3(G)$, $S_2 = O_{3,2}(G)$, $S_3 = O_{3,2,3}(G)$, ... Пусть t — первое число, для которого $S_t = K$. Понятно, что $t \geq$2. Пусть $\widehat{G} = G/S_{t-2}$, $\widehat{K} = K/S_{t-2}$. Тогда $\widehat{K}$ — группа, в которой инвариантна её силовская p-подгруппа для p =2 или p =3.

Пусть вначале $p = 3$. Тогда $\widetilde{G} = G/S_{t-1}$ обладает нетривиальной нормальной 2-подгруппой $\widetilde{S} = S_t/S_{t-1}$, фактор-группа по которой содержит в качестве нормальной подгруппу, изоморфную Alt_7. Так как в G нет элементов порядка 14, то элемент порядка 7 из G действует при сопряжении без неподвижных точек в $\widetilde{S}$ и, как следует из таблицы 2-модулярных характеров Alt_7, любой композиционный фактор группы G в $\widetilde{S}$ является неприводимым 6-мерным представлением над полем порядка 2, в котором размерность пространства неподвижных точек элемента порядка 5 равна 2. Так как к $\widetilde{S}$ в $\widehat{G}'$ есть дополнение, то Alt_7 действует на $\overline{S}_{t-1} = S_{t-1}/S_{t-2} \neq 1$. Таблица 3-модулярных характеров для Alt_7 показывает, что $C_{\overline{S}_{t-1}}(x) \neq 1$ для элемента x порядка 5, и поэтому $C_{\overline{S}_{t-1}}(x)$ является расширением нетривиальной 3-группы с помощью 2-группы ранга большего либо равного 2, следовательно, $C_{\overline{S}_{t-1}}(x)$ содержит элемент порядка 6. Это означает, что в G есть элемент порядка 30, что неверно.

Итак, $p = 2$. По построению $\overline{S}_{t-1} = S_{t-1}/S_{t-2}$ является 2-группой, содержащей свой централизатор в $\overline{S} = S/S_{t-2}$. С помощью леммы 6 легко показать, что $\widetilde{G}_0 = N(\widetilde{S}) = C(\widetilde{S}) \cdot \widetilde{S}$, где как и раньше $\widetilde{G} = G/S_{t-1}$, а G_0 — полный прообраз $(G/K)'$ в G. Поэтому $N(\widetilde{S}) = \widetilde{S} \cdot \widetilde{A}$, где $\widetilde{A}$ централизует $\widetilde{S}$ и $\widetilde{A} \simeq Alt_7$. Поскольку в G нет элементов порядка $9\cdot7$, группа $\widetilde{S}$ имеет период 3. Если некоторый нетривиальный элемент $\widetilde{y}$ из $\widetilde{S}$ централизует нетривиальный элемент из $\overline{S}_{t-1}$, то $\widetilde{A}$ действует на $C_{\overline{S}_{t-1}}(\widetilde{y}) \neq 1$. Как и раньше, элемент порядка 5 из G централизует в $C_{\overline{S}_{t-1}}(\widetilde{y})$ некоторый нетривиальный элемент и, следовательно, в G есть элемент поряд-

ка 30; противоречие. Поэтому $\widetilde{S}$ — группа порядка 3, действующая на $C_{\overline{S}_{t-1}}$ без неподвижных точек. Отсюда вытекает, что $C_{\overline{G}_0}(\overline{S}) = \overline{S} \cdot \overline{A}$, где $\overline{A} \simeq Alt_7$ или $3.Alt_7$. Поскольку в $\overline{G}$ нет элемента порядка 9, то $S_{t-2} \neq 1$ и S_{t-2}/S_{t-3} — нетривиальная 3-подгруппа. Теперь рассуждения, использовавшиеся для p =3, показывают, что для элемента x порядка 5 централизатор $C_{S_{t-1}/S_{t-3}}(x)$ содержит элемент порядка 6, то есть G содержит элемент порядка 30; противоречие. Лемма доказана.

4 Доказательство теоремы

Ниже мы последовательно рассмотрим все возможные варианты для группы L. Заметим, что L не может быть изоморфна распознаваемой и даже квазираспознаваемой группе. Конечная неабелева простая группа L называется *квазираспознаваемой по спектру* (или просто квазираспознаваемой), если каждая конечная группа с тем же спектром имеет ровно один неабелев композиционный фактор S и этот фактор изоморфен L. Ввиду класификационной теоремы, если L — простая группа, то L является либо группой лиева типа, либо знакопеременной группой, либо спорадической группой. В [6, таблицах 2, 8, 9] указана неплотность каждой конечной простой группы. Также легко видеть, что $\omega(G/K) \subseteq \omega(G)$.

Предложение 1. *L не может быть изоморфна ни одной из спорадических групп и исключительных групп лиева типа.*

Доказательство. Все спорадические группы кроме J_2 распознаваемы. Группа J_2 разобрана в лемме 15. Все группы исключительного лиева типа являются квазираспознаваемыми (см. [15]).

Таким образом, L может быть изоморфна либо классической группе лиева типа, либо знакопеременной группе.

Из леммы 2.1 следует, что L может быть изоморфна только группе с неплотностью, не превосходящей 4. Так как группа Alt_7 имеет индекс 2 в группе $Aut(Alt_7) \simeq Sym_7$, то $G/K \simeq Alt_7$ либо $G/K \simeq Sym_7$.

Покажем, что L не может быть изоморфна классической группе лиева типа.

Предложение 2. *L не может быть изоморфна $A_n(q)$.*

Доказательство. Допустим, что $L \simeq A_n(q)$ для некоторых n и q.

1. Пусть $L \simeq A_1(q)$. Группы $A_1(q)$ распознаваемы (см. [16]), если $q \neq 9$. В группе $A_1(9)$ нет элемента порядка 7. Следовательно, L не может быть изоморфна $A_1(q)$.

2. Пусть $L \simeq A_2(q)$. Группа L является квазираспознаваемой группой, если $q \neq 3$ (смотри [17, теорема B]). В группе $A_2(3)$ нет элемента порядка 7.

3. Пусть $L \simeq A_3(q)$. Тогда $\rho(L) = \{p,\ r_3,\ r_4\}$. Справедлива следующая цепочка равенств: $(q^3-1)/(q-1) = q^2+q+1 = q(q-1)+2(q-1)+3$. Таким образом, у q^2+q+1 и $q-1$ общим делителем может быть только 3. Число q^2+q+1 взаимно просто с $q+1$. Обозначим за $\overline{r}_n$ произведение всех примитивных делителей степени n, взятых с максимальными степенями. Тогда $\overline{r}_3$ равно q^2+q+1 или $(q^2+q+1)/3$, а $\overline{r}_2$ равно $(q+1)/2$. По лемме 3 не более чем одно число из ρ делит $|K| \cdot |Aut(S)|$. Значит, оставшиеся два числа из ρ должны делить порядок S.

Допустим, что p и r_3 делят порядок S, значит, $r_3 \in \{5,7\}$, $p \in \{2,3,5,7\}$. Несложно понять, что в этом случае $\overline{r}_3$ должно быть степенью 5 или 7. Дальнейшее рассуждение разобьем на ряд случаев в зависимости от p.

i.a. Пусть $p = 3,\ q = 3^k$. Число $3^{2k} + 3^k + 1$ не делится на 5, а при $k = 6t+2$ или $k = 6t+4$ делится на 7. По лемме 10 число $\overline{r}_3$ не является степенью простого числа.

i.b.Пусть $p = 5,\ q = 5^k$. Число $5^{2k} + 5^k + 1$ не делится на 5, и при $k = 6t+2$ или $k = 6t+4$ делится на 7. Из леммы 10 следует, что $\overline{r}_3$ не является степенью простого числа.

i.c. Пусть $p = 7,\ q = 7^k$. Число $7^{2k} + 7^k + 1$ не делится на 5 и на 7.

i.d. Пусть $p = 2,\ q = 2^k$. Число $2^{2k} + 2^k + 1$ не делится на 5, следовательно, $2^{2k}+2^k+1 = 3 \cdot 7^l$ при четных k, и $2^{2k}+2^k+1 = 7^l$ при нечетных k. Допустим, $k = 2t$ четно. Тогда справедлива следующая цепочка равенств: $2^{4t}+2^{2t}+1 = (2^{2t}+1)^2-2^{2t} = (2^{2t}+1-2^t)(2^{2t}+1+2^t) = 3 \cdot 7^l$. У чисел $2^{2t}+1-2^t$ и $(2^{2t}+1+2^t)$ есть взаимно простые делители, если одно из них не равно 1. Допустим, что 3 делит $2^{2t}+1-2^t$. Значит, $2^{2t}+1-2^t = 3$, следовательно $t = 1$, $q = 4$. По лемме 13 группа L не может быть изоморфна $A_3(4)$. Допустим, что 3 делит $2^{2t}+1+2^t$. Тогда $2^{2t}+1+2^t = 3$ и, следовательно, $t = 0$; противоречие. Значит k нечетно, $k = 2t+1$. Тогда $2^{4t+2} + 2^{2t+1} + 1 = 7^l$. Справедлива следующая цепочка равенств: $2^{2t+1}(2^{2t+1}+1) = 7^l - 1 = 6(7^{l-1}+...+1)$. Таким образом, если l нечетно, то $(7^{l-1}+...+1)$ не делится на 2, следовательно, $2t+1 = 1$. Группа $A_3(2)$ является распознаваемой, следовательно, $L \not\simeq A_3(2)$. Значит l четно, $l = 2s$. Тогда $2^{4t+2}+2^{2t+1}+1 = 7^{2s}$. Справедлива следующая цепочка равенств: $2^{2t+1}+1 = 7^{2s}-2^{4t+2} = (7^s+2^{2t+1})(7^s-2^{2t+1}) > 2^{2t+1}+1$; противо-

речие. Таким образом, доказано, что либо p, либо r_3 делит $|K| \cdot |Aut(S)|$. Следовательно, r_4 делит порядок S.

Допустим, что p и r_4 делят $|S|$. Заметим, что примитивный простой делитель разности $q^4 - 1$ не может равняться 3 или 7. Поэтому $r_4 = 5$.

ii.a. Пусть p нечетно. Из леммы 11 следует, что $q = 3$ или $q = 7$. В группе $A_3(3)$ нет элемента порядка 7. Если $q = 7$, то $\overline{r}_4 = 25$, и в группе L есть элемент порядка 25. В S нет элемента порядка 25, следовательно, 5 делит порядок K. Но $r_4 = 5$, следовательно, два числа из ρ делят порядок K; противоречие.

ii.b. Пусть $p = 2$. Тогда $2^{2k} + 1 = 5^l$. По лемме 9 имеем $l = 1$, $k = 1$, $q = 2$, а группа $|A_3(2)| \simeq Alt_8$ распознаваема. Отсюда следует, что r_3 делит $|S|$.

Осталось рассмотреть случай, когда числа r_3 и r_4 делят $|S|$.

iii. Пусть $p \neq 2$. Так как $r_4 = 5$, по лемме 11 либо $q = 3$, либо $q = 7$. В этих случаях $r_3 = 13$ или $r_3 = 29$ соответственно и, следовательно, r_3 не делит $|S|$. Случай, когда $p = 2$ разобран в пункте i.d.

4. Пусть $L \simeq A_4(q)$. Тогда $\rho(L) = \{r_3,\ r_4,\ r_5\}$, $\rho(2, A_4(q)) = \{2, r_5\}$. Разберём этот случай аналогично предыдущему. Пусть r_3 и r_4 делят порядок S. Если $p = 2$, то r_4 должно быть равно 5. По лемме 9 это возможно только в одном случае, когда $q = 2$. Группа $A_4(2)$ распознаваема. Если p нечетно, то числа r_3 и r_4 смежны с 2, значит равны 3 или 5. Ни r_4, ни r_3 не могут равняться 3; противоречие. Следовательно, r_5 делит порядок S. Однако r_5 не может лежать в множестве $\{3, 5, 7\}$.

5. Пусть $L \simeq A_5(q)$. Тогда $\rho(L) = \{r_4,\ r_5,\ r_6\}$, $\rho(2, L) = \{2, r_5\}$, или $\rho(2, L) = \{2, r_6\}$, или $\rho(2, L) = \{2, r_5, r_6\}$. Поскольку $r_5 \notin \{3, 5, 7\}$, то $r_4 = 5$, $r_6 = 7$. Из леммы 11 вытекает, что r_4 может быть равно 5 только при $q \in \{4, 3, 7\}$. В этих случаях $r_7 \neq 7$.

6. Пусть $L \simeq A_6(q)$. Тогда $\rho(L) = \{r_4,\ r_5,\ r_6,\ r_7\}$, $\rho(2, L) = \{2, r_7\}$. Числа $r_5, r_6, r_7 \notin \{3, 5\}$, но хотя бы два из них делят $|S|$.

7. Пусть $L \simeq A_7(q)$. Тогда $\rho(L) = \{r_5,\ r_6,\ r_7,\ r_8\}$, $\rho(2, L) = \{2, r_7\}$ или $\rho(2, L) = \{2, r_8\}$, или $\rho(2, L) = \{2, r_8, r_{14}\}$. Числа $r_5, r_6, r_7, r_8 \notin \{3, 5\}$, но хотя бы два из них делят $|S|$.

Линейные группы размерности, большей 8, имеют неплотность, большую 4. Предложение доказано.

Предложение 3. *L не может быть изоморфна ${}^2A_n(q)$.*

Доказательство. 1. Пусть $L \simeq {}^2A_2(q)$. Группа L является квазираспознаваемой группой, если $q \neq 3$ и 5 (см. [18]). Группа ${}^2A_2(5)$ разобрана в лемме 14. В группе ${}^2A_2(3)$ нет элемента порядка 5.

2. Пусть $L \simeq {}^2A_3(q),\ q > 2$. Тогда $\rho(L) = \{p,\ r_4,\ r_6\}$, $t(2, L) = \{2, r_6\}$, если $q + 1$ не делится на 4, $\rho(2, L) = \{p, r_4\}$, если $q + 1$ делится на 8, $\rho(2, L) = \{p, r_4, r_6\}$, если $q + 1$ делится на 4, но не делится на 8.

i. Пусть p и r_4 делят $|S|$. Этот случай рассмотрен в пункте 3.ii предложения 1, и возможен только при $q = 3$. Группа ${}^2A_3(3)$ распознаваема. Противоречие.

ii. Пусть p и r_6 делят $|S|$. Если $p = 2$, то $2^{2k} - 2^k + 1$ не делится на 7. Следовательно, $r_6 \in \{3, 5, 7\}$. Значит, p нечетно. Так как r_6 не может быть равно ни 3, ни 5 при любых значениях q, то $r_6 = 7$, значит, $p \in \{3, 5\}$. Несложно понять, что $\overline{r}_6 = (q^2 - q + 1)/3^i$, где $i \in \{0, 1\}$. Допустим, $p = 3$. Тогда, $\overline{r}_6 = q^2 - q + 1 = 3^{2t} - 3^t + 1 = 7^l$. Покажем, что это возможно только при $k = 1$ и $q = 3$. Число $3^{2t} - 3^t + 1$ делится на 7 при $t = 6k - 1$ или $t = 6k - 5$, т.е. t нечетно. Значит, справедлива следующая цепочка равенств: $7^l = 3^{2(2h+1)} - 3^{2h+1} + 1 = 3^{2(2h+1)} + 2 \cdot 3^{2h+1} + 1 - 3 \cdot 3^{2h+1} = (3^{2h+1} + 1)^2 - 3^{2(h+1)} = (3^{2h+1} + 1 - 3^{h+1})(3^{2h+1} + 1 + 3^{h+1})$. Если $h \neq 0$, у чисел $3^{2h+1} + 1 - 3^{h+1}$ и $3^{2h+1} + 1 - 3^{h+1}$ есть взаимно простые делители. Следовательно, $h = 0$ и $l = 1, q = 3$, что и требовалось доказать. Группа ${}^2A_3(3)$ распознаваема. Аналогичным способом можно показать, что если $p = 5$, то $q = 5$. По лемме 13 группа L неизоморфна ${}^2A_3(5)$.

iii. Пусть r_4 и r_6 делят $|S|$. Случай, когда p четно, рассмотрен в ii, следовательно, p нечетно. По лемме 11 $q \in \{3, 7\}$. При $q = 7$ выполнено $r_6 = 43$ и, следовательно, r_6 не делит $|S|$. При $q = 3$ группа $S = {}^2A_3(3)$ распознаваема.

3. Пусть $L \simeq {}^2A_4(q),\ q \neq 2$. Тогда $\rho(L) = \{r_4, r_6, r_{10}\}$, $\rho(2, L) = \{2,\ r_{10}\}$. Несложно понять, что $r_{10} \notin \{3, 5, 7\}$. Следовательно, $r_4 = 5$, $r_6 = 7$. Легко показать, что этот случай тоже невозможен.

4. Пусть $L \simeq {}^2A_5(q)$. Тогда $\rho(L) = \{r_3, r_4, r_{10}\}, \rho(2, L) = \{2,\ r_{10}\}$. Число $r_{10} \notin \{3, 5, 7\}$. Значит, r_3 и r_4 делят $|S|$. Этот случай разобран в пункте 3.iii предложения 1.

При n, большем 5, группы ${}^2A_n(q)$ имеют неплотность большую 3, и несложно показать, что L не может быть изоморфна ни одной из этих групп.

Предложение 4. *L не может быть изоморфна $B_n(q)$ и $C_n(q)$.*

Доказательство. Пусть $n = 2$. По теореме Грюнберга – Кегеля $(q^2 + 1)/(2, q - 1) = \mu(L) \cap \omega_2(L) = \mu_2(L) = \mu_i(S)$, где $i = 2$ или 3. Следовательно, $(q^2 + 1)/(2, q - 1) = 5$ или 7. Это возможно только при $q = 2$. Но тогда 7 не делит порядок L.

Пусть $n = 3,\ q = 2$ или $n = 4,\ q = 2$. Эти группы являются распознаваемыми.

Пусть $n = 3,\ q \neq 2$. Тогда $\rho(L) = \{r_3, r_4, r_6\}$, $\rho(2, L) = \{2, r_3\}$. Как и в пункте 2 предложения 3, несложно показать, что этот случай возможен только при $q = 3$. Группы $C_3(3)$ и $B_3(3)$ разобраны в лемме 13.

Пусть $n = 4$. Тогда $\rho(L) = \{r_3, r_4, r_6, r_8\}$. Так же, как в пункте 7 предложения 2, можно показать, что этот случай невозможен.

При $n > 4$ неплотность группы L больше 4.

Предложение 5. *L не может быть изоморфна $D_n(q)$ и ${}^2D_n(q)$.*

Доказательство. Пусть $n = 4$. Тогда $\rho(L) = \{r_3, r_4, r_6\}$. Легко показать, что этот случай возможен только при $q = 3$. Случай $q = 3$ разобран в лемме 13. При $n > 4$ число $t(L) \geq 4$, и ни одно из чисел, лежащих в $\rho(L)$, не равно 3 или 2, но хотя бы три из них делят порядок S. Противоречие.

Предложение 6. *L не может быть изоморфна ${}^2B_2(q)$.*

Доказательство. В противном случае $|\rho(L)| \geq 4$ и ни одно из чисел, лежащих в $\rho(L)$, не равно 3 или 2.

Предложение 7. *L не может быть изоморфна ${}^3D_4(q)$.*

Доказательство. В противном случае $\rho(L) = \{r_3, r_6, r_{12}\}$. Легко показать, что этот случай невозможен.

Таким образом, из предложений 2 — 7 следует, что L не может быть изоморфна классической группе лиева типа.

Предложение 8. *L не может быть изоморфна Alt_n при $n \neq 7$.*

Доказательство. Для любого простого числа $p \leq n$ в Alt_n существует элемент порядка p. По лемме 12 при $n > 12$ существуют три простые числа $p_1, p_2, p_3 \leq n$ такие, что $p_i + p_j > n$. Из этого следует, что в $GK(Alt_n)$ существует три попарно несмежных простых числа p_1, p_2, p_3. Порядок группы $|K|$ может делиться только на одно из них . Поскольку $|G| = |K| \cdot |\overline{G}|$, то оставшиеся два числа должны делить порядок S. При $n \geq 13$ числа $p_1, p_2, p_3 \geq 7$, следовательно, $n < 13$. Группы Alt_8, Alt_9, Alt_{11}, Alt_{12} распознаваемы, группа Alt_{10} разобрана в лемме 16. Отсюда $n = 7$.

Если $L \simeq Alt_7$, то из распознаваемости L следует заключение теоремы. Теорема доказана.

Докажем следствие. Допустим, что L — простая группа и G удовлетворяет условию следствия. Тогда из [6] и леммы 1 следует, что если L

отлична от групп $A_2(3)$, ${}^2A_3(3)$, $C_2(3)$ и Alt_n, где n таково, что среди чисел $n, n-1, n-2, n-3$ нет простых, то выполнено заключение теоремы Б. Следовательно, выполнено заключение основной теоремы. Значит, группа L изоморфна Alt_7, $A_2(3)$, ${}^2A_3(3)$ или $C_2(3)$. В группах $A_2(3)$ и ${}^2A_3(3)$ нет элемента порядка 7. Случай, когда L изоморфна $C_2(3)$, разобран в лемме 13. Следовательно, $L \simeq Alt_7$. Следствие доказано.

Список литературы

[1] Мазуров В.Д. Группы с заданным спектром // Изв. УрГУ. 2005. Т. 36. N 7. С. 119–138.

[2] Williams J. S. Prime graph components of finite groups // J. Algebra. 1981. V. 69, N 2. P. 487–513.

[3] Кондратьев А.С. О компонентах графа простых чисел для конечных простых групп // Матем. сб. 1989. Т. 180. N 6. С. 787–797.

[4] Алеева М.Р. О конечных простых группах с множеством порядков элементов, как у группы Фробениуса или двойной группы Фробениуса // Мат. заметки. 2003. Т. 73, N 3. С. 323–339.

[5] Васильев А.В. О связи между строением конечной группы и свойствами ее графа простых чисел // Сиб. мат. журн. 2005. Т. 46, N 3. С. 511–522.

[6] Васильев А.В., Вдовин Е.П. Критерий смежности двух вершин в графе простых чисел конечной простой группы. //Алгебра и логика. 2005. Т. 44, N 6. С. 682–725.

[7] Мазуров В.Д. Распознавание конечных простых групп $S_4(q)$ по порядку их элементов // Алгебра и логика. 2002. Т.41, N 2. С. 166–198.

[8] Мазуров В.Д. Характеризация конечных групп множествами порядков их элементов // Алгебра и логика. 1997. Т. 36, N 1. С. 23–32.

[9] Khukhro E.I., Mazurov V.D. Finite groups with an automorphism of prime order whose centralizer has small rank // J. Algebra. 2006. T. 301, N 2, 474–492.

[10] Zsigmondy K. Zur Theorie der Potenzreste // Monatsh. Math. Phys. 1982. V. 3. P. C. 265–284.

[11] Айерлэнд К., Роузен М. Класическое введение в современную теорию чисел // Мир, 1987.

[12] Эдвардс Г., Последняя Теорема Ферма. Генетическое введение в алгебраическую теорию чисел // Мир, 1980.

[13] Бухштаб А.А. Теория чисел // Москва. 1966

[14] *The GAP Group*, GAP — Groups, algorithms, and programming. Version 4.4. 2004 (http://www.gap-system.org).

[15] Васильев А.В О распознаваемости конечных простых исключительных групп лиева типа // Алгебра и логика (в печати)

[16] Brandl R., Shi W. The characterization of $PSl(2,q)$ by its element orders // J. Algebra 1994 V.163. P. 109–114.

[17] Заварницин А. В. Веса неприводимых $Sl_3(q)$ — модулей в характеристике определения // Сиб. мат. журн. 2004. Т 45, N 2. С. 320–328.

[18] Алеева М. Р. О композиционных факторах конечных групп с множеством порядков элементов, как у группы $U_3(q)$ // Сиб. мат. журн. 2002. Т 43, N 2. С. 250–265.

СТРОЕНИЕ ГРУППЫ ЕДИНИЦ ЦЕЛОЧИСЛЕННОГО ГРУППОВОГО КОЛЬЦА ЦИКЛИЧЕСКОЙ ГРУППЫ ПРОСТОГО ПОРЯДКА

Е.В. Грачев

Новосибирский государственный технический университет,
Россия, 630092, Новосибирск, пр. К.Маркса 20
e-mail: algebra@nstu.ru

Определение. Пусть $G = \{e, g_1, g_2, \ldots, g_n\}$ — конечная группа. Целочисленным групповым кольцом ZG называется множество формальных линейных комбинаций $\sum z_i g_i$ с обычной операцией сложения и операцией умножения, определяемой умножением элементов группы.

Обратимые элементы кольца ZG образуют группу, которая называется группой единиц и обозначается $U(ZG)$. Подгруппа $V(ZG) = \{\sum z_i g_i \in U(ZG) : \sum z_i = 1\}$ называется нормализованной группой единиц кольца ZG.

Первый вопрос, на который нужно ответить, является ли заданный элемент кольца ZCp обратимым.

Если Cp циклическая группа порядка p, то известно, что ее представление имеет вид $D(a) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \xi & 0 & 0 \\ 0 & 0 & \xi^2 & 0 \\ 0 & 0 & 0 & \xi^{p-1} \end{pmatrix}$, где a порождающий элемент группы и ξ первообразный корень степени p из единицы. При этом $ZCp \cong ZD(Cp)$. Произвольный элемент кольца ZCp имеет вид $\beta = \sum_{i=0}^{p-1} z_i a^i$. Рассмотрим кольцо $Z[\xi] = \sum_{i=0}^{p-1} z_i \xi^i$. Заметим ряд равенств

$$\bar{\xi} = \xi^{p-1}, \bar{\xi}^2 = \xi^{p-2}, ..., \bar{\xi}^{\frac{p-1}{2}} = \xi^{\frac{p+1}{2}}, \sum_{i=0}^{p-1} \xi^i = 0(1). \qquad (1)$$

Из этих равенств следует, что любой элемент кольца Z[ξ] можно представить в виде: $\alpha = \sum_{i=0}^{p-2} z_i \xi^i$. Нас интересуют такие обратимые элементы кольца $Z[\xi]$, для которых $\sum_{i=0}^{p-2} z_i \equiv \pm 1 mod p$.

Рассмотрим изоморфизмы кольца $Z[\xi]$ $\sigma_1(\xi) = \xi, \sigma_2(\xi) = \xi^2, ..., \sigma_{p-1}(\xi) = \xi^{p-1}$. В силу равенств (1) имеем, что элемент кольца Z[ξ] обратим тогда и только тогда, когда его норма $N(\alpha) = \prod_{i=1}^{\frac{p-1}{2}} |\sigma_i(\alpha)|^2 = 1$. При вычислении числа $N(\alpha)$ заметим, что его множители можно представить в виде

$$|\sigma_i(\alpha)|^2 = A_0 + A_1^i(\xi + \xi^{p-1}) + ... + A^i_{\frac{p-1}{2}}(\xi^{\frac{p-1}{2}} + \xi^{\frac{p+1}{2}}), A_j^i \in Z.$$

При этом

$$\xi + \xi^{p-1} = 2\cos(\frac{2\pi}{p}), \xi^2 + \xi^{p-2} = 2\cos(\frac{4\pi}{p}), ..., (\xi^{\frac{p-1}{2}} + \xi^{\frac{p+1}{2}}) = 2\cos(\frac{2\pi(p-1)}{p}).$$

Здесь A_j^i представляют собой квадратичные формы от коэффициентов z_j.

Второй вопрос на который нужно ответить следующий: построить подгруппу конечного индекса группы $V(ZCp)$.

Обозначим $r = \frac{p-1}{2} - 1$.

Каждому элементу α кольца $Z[\xi]$ поставим в соответствие вектор логарифмического пространства $l(\alpha) = (\ln(|\sigma_1(\alpha)|^2), \ln(|\sigma_2(\alpha)|^2), .., \ln(|\sigma_r(\alpha)|^2))$.

Обозначим через $\eta_1, \eta_2, ..., \eta_r$ элементы, для которых векторы $l(\eta_1), l(\eta_2)$, $..., l(\eta_r)$ линейно независимы.

Из известной теоремы Дирихле следует, что группа единиц кольца $Z[\xi]$ конечно порождена, а именно любая единица представляется в виде $\xi^k \eta_1^{z_1} ... \eta_r^{z_r}$. Для нахождения порождающих $\eta_1, \eta_2, .., \eta_r$, нужно в логарифмическом пространстве найти базис $l(\eta_1), l(\eta_2), ..., l(\eta_r)$ с минимальным объемом параллелепипеда, натянутого на векторы базиса. Если же объем не минимален, то получаем порождающие подгруппы конечного индекса.

Таким образом нами получен алгоритм, который позволяет находить порождающие подгруппы конечного индекса группы единиц кольца $Z[\xi]$. После этого мы можем эффективно решать поставленные нами задачи.

1) Умножение. Если $\alpha_1 = \xi^k \eta_1^{z_1} ... \eta_r^{z_r}, \alpha_2 = \xi^s \eta_1^{l_1} ... \eta_r^{l_r}$. Тогда $\alpha_1 \alpha_2 = \xi^{k+s} \eta_1^{z_1 + l_1} ... \eta_r^{z_r + l_r}$.

2) Обращение. $\alpha_1^{-1} = \xi^{p-k} \eta_1^{-z_1} ... \eta_r^{-z_r}$.

3) Извлечение корня. $\sqrt[m]{\alpha_1} = \xi^{\frac{k}{m}} \eta_1^{\frac{z_1}{m}} ... \eta_r^{\frac{z_r}{m}}$, при условии что $m/z_1, z_2, ..., z_r$.

Эта задача решена нами для простых p от 5 до 53. Т.е. для этих p нами построены порождающие подгруппы конечного индекса группы $V(ZCp)$.

НЕПОДВИЖНЫЕ ТОЧКИ МОДАЛЬНЫХ DS-ФОРМУЛ

С.И. Мардаев*

Институт математики СО РАН,
Новосибирский государственный университет,
Новосибирск
e-mail: mardaev@math.nsc.ru

Ранее [1] было доказано, что наименьшие неподвижные точки оператора, соответствующего модальной Σ-формуле, определимы некоторой итерацией этой формулы. Такой способ построения определяющей формулы идейно прост и при этом сохраняется позитивность параметров. Заметим, однако, что число итераций может быть велико и не исключено, что более изощренный алгоритм может дать более короткую формулу.

Теорема, доказанная в этой статье, обобщает результат из [1]. Введено понятие DS-формул, которое обобщает понятие Σ-формул. Доказано, что наименьшие неподвижные точки оператора, соответствующего DS-формуле, определимы итерацией этой формулы.

Модальные пропозициональные формулы составляются из пропозициональной константы $\bot$ (ложь) и пропозициональных переменных $p, q, r, \ldots$ с помощью бинарных связок $\wedge$, $\vee$ и унарных связок $\neg$, $\Box$ и $\Diamond$. Будем использовать сокращения $\top = \neg\bot$, $\Diamond\!\!\!\cdot\,\alpha = \alpha \vee \Diamond\alpha$.

Шкала Крипке $\langle W, R \rangle$ состоит из непустого множества W и бинарного отношения R на W. *Модель Крипке* $\langle W, R, v \rangle$ состоит из шкалы Крипке $\langle W, R \rangle$ и означивания v. *Означивание* v — это функция, которая каждой переменной q ставит в соответствие подмножество $v(q)$ множества W. Значение переменной q_i будем обозначать соответствующей прописной буквой Q_i. Функция v естественным образом продолжается на формулы: константе $\bot$ всегда соответствует пустое множество, связкам $\neg$, $\wedge$, $\vee$, $\Box$, $\Diamond$ соответствуют дополнение, пересечение, объединение и следующие операции на множествах:

$$\Box A = \{x \,|\, \forall y(xRy \Rightarrow y \in A)\},\ \Diamond A = \{x \,|\, \exists y(xRy \wedge y \in A)\}.$$

*Работа поддержана Российским Фондом Фундаментальных Исследований, грант N.06-01-00358

Пусть дана формула $\varphi(p, q_1, \ldots, q_n)$ от переменных $p, q_1, \ldots, q_n$ и модель Крипке $\langle\, W, R, v \,\rangle$, в которой заданы значения $Q_1, \ldots, Q_n$ переменных $q_1, \ldots, q_n$, а значение переменной p не задано. Формула φ определяет на модели $\langle\, W, R, v \,\rangle$ оператор $F_\varphi(P) = \varphi(P, Q_1, \ldots, Q_n)$. Множество P называется неподвижной точкой оператора F, если выполняется $P = F(P)$. Если неподвижная точка P совпадает со значением некоторой формулы $\omega(q_1, \ldots, q_n)$, то формула ω *определяет* неподвижную точку P.

Введем обозначения

$$\varphi^0(q_1, \ldots, q_n) = \bot,$$
$$\varphi^{k+1}(q_1, \ldots, q_n) = \varphi(\varphi^k(q_1, \ldots, q_n), q_1, \ldots, q_n).$$

Кроме того, положим $P^k = \varphi^k(Q_1, \ldots, Q_n)$.

DS-формулой назовем модальную формулу, составленную с помощью связок $\wedge$, $\vee$ из формул с главной связкой $\Diamond$ и формул, не содержащих модальных связок. Это понятие обобщает понятие Σ-формулы. Напомним, что модальной Σ-формулой называется формула, составленная с помощью связок $\wedge$, $\vee$, $\Diamond$ из формул, не содержащих модальных связок.

Пусть $\varphi(p, q_1, \ldots, q_n)$ является DS-формулой и переменная p входит в нее только позитивно. Рассмотрим вхождение $\vee$, участвующее в построении φ из формул с главной связкой $\Diamond$ и формул, не содержащих модальных связок. Вынесем все такие вхождения $\vee$ через $\wedge$ наружу. Получим, что наша формула φ представлена в виде $(\alpha_1 \wedge \beta_1) \vee \cdots \vee (\alpha_k \wedge \beta_k) \vee \alpha_{k+1} \vee \cdots \vee \alpha_r$, где α_i является конъюнкцией формул с главной связкой $\Diamond$, либо является $\top$, а β_i не содержит модальностей.

Теорема. *Формула $\varphi^{k+1}(q_1, \ldots, q_n)$ определяет наименьшую неподвижную точку оператора F_φ в любой транзитивной модели Крипке.*

Доказательство. Зафиксируем транзитивную модель Крипке $\langle\, W, R, v \,\rangle$. На j-том шаге значение P^{j-1} подставляется вместо p в формулу φ и получается новое значение P^j. Через A_i^j, B_i^j обозначим значения формул α_i и β_i на j-том шаге, т.е. после подставления P^{j-1}, $j \geqslant 1$. Через A^j обозначим $A_{k+1}^j \cup \cdots \cup A_r^j$. Итак, $P^j = (A_1^j \cap B_1^j) \cup \cdots \cup (A_k^j \cap B_k^j) \cup A^j$. Обозначим $C_i^j = (A_i^j \cap B_i^j) \setminus P^{j-1}$.

Идея доказательства состоит в том, что для каждой формулы $\alpha_i \wedge \beta_i$ ее значение не может увеличиться за счет тех частей значений $\alpha_s \wedge \beta_s$, которые появились за счет самой $\alpha_i \wedge \beta_i$.

Если, как в нашем случае, R транзитивно, то любое множество вида $\Diamond A$ является нижним конусом. Ясно, что пересечение и объединение

нижних конусов — нижние конусы. Поэтому, множества A_i^j и A^j являются нижними конусами.

Сделаем $j+1$-ый шаг. Рассмотрим приращение $P^{j+1} \setminus P^j$ и его часть $C_i^{j+1} = (A_i^{j+1} \cap B_i^{j+1}) \setminus P^j$. Так как β_i не содержит модальностей, то B_i^{j+1} может отличаться от B_i^1, получающегося подстановкой $\varnothing$, только внутри множества P^j. Поэтому, $B_i^{j+1} \setminus P^j = B_i^1 \setminus P^j$ и

$$C_i^{j+1} = (A_i^{j+1} \cap B_i^{j+1}) \setminus P^j = (A_i^{j+1} \cap B_i^1) \setminus P^j.$$

Множество A_i^{j+1} может увеличиться по сравнению с A_i^j только внутри множества $\Diamond(P^j \setminus P^{j-1})$. Тогда $A_i^{j+1} \setminus A_i^j \subseteq \Diamond(P^j \setminus P^{j-1}) = \Diamond C_1^j \cup \cdots \cup \Diamond C_k^j \cup \Diamond(A^j \setminus P^{j-1})$. Так как A^j - конус, то $\Diamond(A^j \setminus P^{j-1}) \subseteq A^j \subseteq P^j$. Поэтому

$$C_i^{j+1} = (A_i^{j+1} \cap B_i^1) \setminus P^j = (A_i^{j+1} \cap (B_i^1 \setminus P^j)) \setminus P^j \subseteq$$
$$\subseteq (A_i^{j+1} \cap (B_i^1 \setminus A_i^j)) \setminus P^j \subseteq (A_i^{j+1} \setminus A_i^j) \setminus P^j \subseteq \Diamond C_1^j \cup \cdots \cup \Diamond C_k^j.$$

Здесь в первом включении использовали $B_i^1 \setminus P^j \subseteq B_i^1 \setminus A_i^j$, это следует из $A_i^j \cap B_i^1 \subseteq P^j$.

Определим индукцией по j разложение каждого множества C_i^j, $2 \leqslant i \leqslant k$, в объединение некоторых множеств $C_i^j(t_1, \ldots, t_{j-1})$:

$$C_i^j = \bigcup_{1 \leqslant t_1, \ldots, t_{j-1} \leqslant k} C_i^j(t_1, \ldots, t_{j-1}).$$

Базис $j = 2$. Полагаем $C_i^2(t_1) = C_i^2 \cap \Diamond C_{t_1}^1$.

Шаг. Допустим, что каждое из C_i^j, $2 \leqslant i \leqslant k$ имеет указанное разложение в объединение множеств $C_i^j(t_1, \ldots, t_{j-1})$.

Ранее показали, что $C_i^{j+1} \subseteq \Diamond C_1^j \cup \cdots \cup \Diamond C_k^j$. Поэтому

$$C_i^{j+1} \subseteq \bigcup_{1 \leqslant t_1, \ldots, t_{j-1}, s \leqslant k} \Diamond C_s^j(t_1, \ldots, t_{j-1}).$$

Отсюда

$$C_i^{j+1} = \bigcup_{1 \leqslant t_1, \ldots, t_j \leqslant k} C_i^{j+1}(t_1, \ldots, t_j),$$

где по определению $C_i^{j+1}(t_1, \ldots, t_j) = C_i^{j+1} \cap \Diamond C_{t_j}^j(t_1, \ldots, t_{j-1})$.

Лемма 1. *Если $f \leqslant j$, то $C_{t_j}^j(t_1, \ldots, t_{j-1}) \subseteq \Diamond C_{t_f}^f(t_1, \ldots, t_{f-1})$.*

Доказательство. Если $f = j$, то утверждение выполняется. Если $f < j$, то последовательность включений

$$C_{t_j}^j(t_1, \ldots, t_{j-1}) \subseteq \Diamond C_{t_{j-1}}^{j-1}(t_1, \ldots, t_{j-2}) \subseteq \cdots \subseteq \Diamond C_{t_f}^f(t_1, \ldots, t_{f-1})$$

доказывает лемму.

Лемма 2. *Если $f < j$ и $t_f = t_j$, то $C^j_{t_j}(t_1, \ldots, t_{j-1}) = \varnothing$.*

Доказательство. По лемме 1 выполняется

$$C^j_{t_j}(t_1, \ldots, t_{j-1}) \subseteq \Diamond C^f_{t_f}(t_1, \ldots, t_{f-1}) \subseteq \Diamond A^f_{t_f} = A^f_{t_f},$$

последнее равенство следует из того, что $A^f_{t_f}$ - конус. Так как $C^j_{t_j}(t_1, \ldots, t_{j-1}) \subseteq B^1_{t_j}$, то пересекая с $B^1_{t_j} = B^1_{t_f}$, получим $C^j_{t_j}(t_1, \ldots, t_{j-1}) \subseteq A^f_{t_f} \cap B^1_{t_f} \subseteq P^f \subseteq P^{j-1}$. Так как элементов из P^{j-1} в $C^j_{t_j}(t_1, \ldots, t_{j-1})$ нет, то $C^j_{t_j}(t_1, \ldots, t_{j-1}) = \varnothing$. Лемма доказана.

Лемма 3. *Выполняется $C^{k+1}_{t_{k+1}}(t_1, \ldots, t_k) = \varnothing$.*

Доказательство. Среди чисел $t_1, \ldots, t_{k+1}$ найдутся два одинаковых, например $t_f = t_j$, где $f < j$. По лемме 2 выполняется $C^j_{t_j}(t_1, \ldots, t_{j-1}) = \varnothing$, поэтому и $\Diamond C^j_{t_j}(t_1, \ldots, t_{j-1}) = \varnothing$. Утверждение леммы следует из включения

$$C^{k+1}_{t_{k+1}}(t_1, \ldots, t_k) \subseteq \Diamond C^j_{t_j}(t_1, \ldots, t_{j-1}),$$

которое выполняется по лемме 1, так как $j \leqslant k+1$.

Продолжим доказательство теоремы. По лемме 3 на $k+1$-ом шаге $C^{k+1}_i = \varnothing$. Поэтому, $P^{k+1} \setminus P^k = A^{k+1} \setminus P^k$, т.е. $P^{k+1} = P^k \cup A^{k+1}$. На $k+2$-ом шаге P^{k+2} может увеличится по сравнению с P^{k+1} только в $\Diamond A^{k+1} = A^{k+1}$, а так как $A^{k+1} \subseteq P^{k+1}$, то $P^{k+2} = P^{k+1}$. Итак, P^{k+1} — неподвижная точка. Она определяется формулой φ^{k+1}. Теорема доказана.

В некоторых случаях оценку, по-видимому, можно улучшить, учитывая, какие слагаемые содержат p, а какие – не содержат. Например, если φ вообще не содержит p, то достаточно одной итерации.

Конечно, число итераций невозможно ограничить для класса всех DS-формул. Следующая формула является и DS-формулой и Σ-формулой.

$$\varphi = q_1 \vee (q_2 \wedge \Diamond(q_1 \wedge p)) \vee (q_3 \wedge \Diamond(q_2 \wedge p)) \vee \cdots \vee (q_n \wedge \Diamond(q_{n-1} \wedge p)) \vee \Diamond(q_n \wedge p).$$

В качестве модели возьмем линейно упорядоченное множество с элементами $n+1 \leqslant \cdots \leqslant 2 \leqslant 1$. Для всех i положим $Q_i = \{i\}$. Нетрудно проверить, что $P^1 = \{1\}$, $P^2 = \{1, 2\}, \ldots$, $P^{n+1} = \{1, \ldots, n+1\}$. Наименьшей неподвижной точкой является P^{n+1}.

Известно, что модальная логика **K4** характеризуется классом всех транзитивных шкал. Поэтому из теоремы 1 получаем

Следствие. *Логика* **K4** *содержит формулу $\varphi^{k+2} \leftrightarrow \varphi^{k+1}$.*

Литература

[1]. Мардаев С.И. Неподвижные точки модальных схем. Алгебра и логика, 31, n.5 (1992), 493 - 498.

О РАСШИРЕНИЯХ ЧАСТИЧНЫХ ИЗОМОРФИЗМОВ КОНЕЧНЫХ ПОЛИГОНОВ НАД ЛИНЕЙНО УПОРЯДОЧЕННЫМИ МОНОИДАМИ

Е.В. Овчинникова*

Кафедра алгебры и математической логики,
Новосибирский государственный технический университет,
пр. К. Маркса, 20,
630092, Новосибирск, РОССИЯ.
e-mail: algebra@nstu.ru, eovchin@ngs.ru

Е. Хрушовский [1] доказал, что для любого конечного графа Γ и любых его частичных изоморфизмов $\varphi_1, \ldots, \varphi_n$ существует конечный граф Γ', расширяющий Γ и имеющий продолжения частичных изоморфизмов $\varphi_1, \ldots, \varphi_n$ до автоморфизмов из $\mathrm{Aut}(\Gamma')$. Б. Херциг [3] обобщил результат Хрушовского для произвольной конечной предикатной алгебраической системы.

В настоящей работе показано, что любой конечный полигон над линейно упорядоченным моноидом вложим в конечный полигон, у которого любой частичный изоморфизм продолжается до автоморфизма.

Левым *S-полигоном* называется алгебра ${}_SA = \langle A, \{f_s \mid s \in S\}\rangle$ с одноместными операциями, в которой для всех $s, t \in S$ выполняются следующие тождества:

$$\forall x\ (f_1(x) = x),$$

$$\forall x\ (f_s(f_t(x)) = f_{st}(x)).$$

Пусть ${}_SA$ — полигон. Для любого элемента $a \in A$ множество $\{sa \mid s \in S\}$ будем обозначать через Sa и называть *орбитой* элемента a. Очевидно, что ${}_SSa$ — подполигон полигона ${}_SA$, порожденный элементом a.

*Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 05-01-00411).

Моноид S называется *линейно упорядоченным* (*ЛУ-моноидом*), если для любого $b \in S$ множество $\{Sa \mid Sa \subseteq Sb\}$ линейно упорядочено по включению.

ЛЕММА 1. *Если S — ЛУ-моноид, ${}_SA$ — полигон, то для любого элемента $a \in A$ множество $\{Sb \mid Sb \subseteq Sa\}$ линейно упорядочено по включению.*

ДОКАЗАТЕЛЬСТВО. Пусть множества Sb и Sc содержатся в Sa. Тогда существуют элементы $s_1, s_2 \in S$, для которых $b = s_1a$ и $c = s_2a$. Так как S — ЛУ-моноид, то выполняется $Ss_1 \subseteq Ss_2$ или $Ss_2 \subseteq Ss_1$. Если $Ss_1 \subseteq Ss_2$, то найдется элемент $t \in S$, для которого $ts_2 = s_1$. Тогда $ts_2a = s_1a$, т.е. $tc = b$, следовательно, $Sb \subseteq Sc$. Аналогично показывается, что если $Ss_2 \subseteq Ss_1$, то $Sc \subseteq Sb$. □

Пусть ${}_SA$ — полигон, ${}_SB$, ${}_SC$ — подполигоны полигона ${}_SA$. Тогда любой изоморфизм $\varphi :_S B \xrightarrow{\sim} {}_SC$ называется *частичным изоморфизмом* полигона ${}_SA$.

Очевидным является следующее

ЗАМЕЧАНИЕ 1. Если φ — частичный изоморфизм полигона ${}_SA$, $\varphi(a) = b$ для некоторых $a, b \in A$, то $\varphi(Sa) = Sb$.

Для семейства $\{{}_SA_i\}_{i\in I}$ непересекающихся S-полигонов обозначаем через $\bigsqcup\limits_{i\in I} {}_SA_i$ дизъюнктное объединение полигонов ${}_SA_i$.

ЛЕММА 2. *Пусть ${}_SA = \bigsqcup\limits_{i\in I} {}_SA_i$ — конечный полигон и φ — его частичный изоморфизм такой, что если $\varphi(a_i) = a_j$ для $a_i \in {}_SA_i$, $a_j \in {}_SA_j$, то $\varphi({}_SA_i) = {}_SA_j$. Тогда существует автоморфизм $\hat{\varphi}$ полигона ${}_SA$, продолжающий φ.*

ДОКАЗАТЕЛЬСТВО. Доопределим φ до искомого автоморфизма $\hat{\varphi}$ следующим образом: если $a \notin \mathrm{Rang}\varphi \cup \mathrm{Dom}\,\varphi$, то $\hat{\varphi}(a) = a$, а если $a \in \mathrm{Rang}\varphi \setminus \mathrm{Dom}\,\varphi$, то $\hat{\varphi}(a) = (\varphi^{-1}(a))^n$, где n таково, что $(\varphi^{-1}(a))^n \in \mathrm{Dom}\,\varphi \setminus \mathrm{Rang}\varphi$ (в силу конечности полигона ${}_SA$ такое конечное n существует). Поскольку полигон ${}_SA$ представляется в виде дизъюнктного объединения полигонов с носителями $\mathrm{Dom}\,\varphi \cap \mathrm{Rang}\varphi$, $\mathrm{Dom}\,\varphi \setminus \mathrm{Rang}\varphi$, $\mathrm{Rang}\varphi \setminus \mathrm{Dom}\,\varphi$ и $A \setminus (\mathrm{Rang}\varphi \cup \mathrm{Dom}\,\varphi)$, то по построению $\hat{\varphi}$ изоморфно переводит $\mathrm{Dom}\,\varphi$ в $\mathrm{Rang}\varphi$, $\mathrm{Rang}\varphi \setminus \mathrm{Dom}\,\varphi$ — в $\mathrm{Dom}\,\varphi \setminus \mathrm{Rang}\varphi$, а $A \setminus (\mathrm{Rang}\varphi \cup \mathrm{Dom}\,\varphi)$ оставляет поэлементно на месте. □

Высотой $h(a)$ элемента $a \in_S A$ назовем мощность множества $\{Sb \mid Sb \subset Sa\}$, а *высотой $h({}_SA)$ полигона ${}_SA$* — $\max\{h(a) \mid a \in_S A\}$.

Корнем элемента $a \in_S A$ назовем множество $K(a) \rightleftharpoons \{b \mid a = sb$ для некоторого $s \in S\}$.

Очевидным является следующее

ЗАМЕЧАНИЕ 2. 1. Корень $K(a)$ совпадает с множеством $\{b \mid Sa \subset Sb\}$.

2. Если $Sb = Sa$, то $K(a) = K(b)$.

3.Если $Sb \subseteq Sa$, то $K(b) \subseteq K(a)$.

Если S — ЛУ-моноид, то из леммы 2 следует справедливость следующего утверждения.

ЛЕММА 3. *Пусть S — ЛУ-моноид.*

1. Если $Sb \neq Sa$ и $Sb \nsubseteq Sa$ и $Sa \nsubseteq Sb$, то $K(a) \cap K(b) = \emptyset$.

2. Если Sa — минимальная орбита полигона ${}_SA$, то ${}_SK(a)$ является подполигоном полигона ${}_SA$ и образует его компоненту связности. Верно ${}_SA = \bigsqcup_{i \in I} {}_SK(a_i)$, где $\{Sa_i \mid i \in I\}$ — множество всех минимальных орбит полигона ${}_SA$.

3. Если $h(a) = n$, то $h(b) \geq n$ для любого $b \in K(a)$.$\square$

Деревом элемента a назовем полигон ${}_SD(a) \rightleftharpoons {}_S(Sa \cup K(a))$.

Очевидно, что для минимальной орбиты Sa полигоны ${}_SD(a)$ и ${}_SK(a)$ совпадают.

На элементах полигона ${}_SA$ введем две эквивалентности $\sim$ и $\approx$. Положим $a \sim b$ (соответственно $a \approx b$), если существует частичный изоморфизм φ полигона ${}_SA$ такой, что $\varphi(a) = b$ (и $\varphi({}_SD(a)) = {}_SD(b)$).

Если $a \approx b$, $\varphi :_S Sa \simeq\!\!\rightarrow {}_SSb$ — частичный изоморфизм полигона ${}_SA$ такой, что $\varphi(a) = b$, $\psi :_S D(a) \simeq\!\!\rightarrow {}_SD(b)$ — продолжение φ, то для любого $x \in D(a)$ через $x_{\varphi,\psi,a}$ будем обозначать элемент $\psi(x)$.

Напомним [3], что конгруэнция θ, отождествляющая элементы из разных компонент связности полигона, называется *амальгамной*.

ТЕОРЕМА. *Если S — ЛУ-моноид, то для любого конечного полигона ${}_SA$ существует конечный полигон ${}_S\hat{A}$ высоты $h({}_SA)$ и такой, что ${}_SA$ вложим в ${}_S\hat{A}$ и в полигоне ${}_S\hat{A}$ любой частичный изоморфизм продолжается до автоморфизма ${}_S\hat{A}$.*

ДОКАЗАТЕЛЬСТВО Пусть ${}_SA$ — полигон высоты n. Строим цепочку полигонов ${}_SA_1 \subseteq \ldots \subseteq {}_SA_n$. Положим ${}_SA_1 \rightleftharpoons {}_SA$. Если полигон ${}_SA_k$ построен, то обозначим через C_k множество $\{a \in A_k \mid h(a) = n - k\}$.

Для любых двух элементов $a, b \in C_k$ таких, что $a \sim b$ и $a \not\approx b$, обозначим через ${}_SD(a, b)$ изоморфную копию дерева ${}_SD(b)$, а элемент, соответствующий элементу $x \in {}_SD(b)$ в копии ${}_SD(a, b)$ обозначим через $x_{a,b}$.

На полигоне ${}_SE_k \rightleftharpoons {}_SA_k \bigsqcup \left(\bigsqcup_{a\sim b, a\not\approx b} {}_SD(a,b) \right)$ определим конгруэнцию θ_k, порожденную парами $(a, b_{a,b})$. Так как полигоны ${}_SSa$ и ${}_SSb_{a,b}$ изоморфны и элементы a и $b_{a,b}$ не связаны, конгруэнция θ_k является амальгамной конгруэнцией. Полагаем ${}_SA_{k+1} \rightleftharpoons {}_SE_k/\theta_k$ и ${}_S\hat{A} \rightleftharpoons {}_SA_n$.

В полигоне A_k выполняется свойство: для любых элементов a и b если $a \sim b$ и $h(a) = h(b) \geq n - k + 1\}$, то $a \approx b$. Следовательно, в полигоне ${}_S\hat{A}$ это свойство верно для элементов a и b любой высоты.

Пусть φ — произвольный частичный изоморфизм полигона ${}_S\hat{A}$, $\hat{A} = \{a_1, \ldots, a_m\}$. Строим частичные изоморфизмы $\varphi_0 \subseteq \varphi_1 \subseteq \ldots \subseteq \varphi_m$. Положим $\varphi_0 \rightleftharpoons \varphi$. Предположим, что $\varphi_1, \ldots, \varphi_{k-1}$ уже построены. Если $a_k \in \mathrm{Dom}\,\varphi_{k-1}$, то $\varphi_k \rightleftharpoons \varphi_{k-1}$. Если $a_k \notin \bigcup_{b\in \mathrm{Dom}\,\varphi_{k-1}} D(b)$, то для любого $x \in \mathrm{Dom}\varphi_{k-1}$ полагаем $\varphi_k(x) \rightleftharpoons \varphi_{k-1}(x)$, а для любого $x \in Sa_k$ — $\varphi_k(x) \rightleftharpoons x$. Таким образом, в этом случае $\mathrm{Dom}\,\varphi_k = \mathrm{Dom}\,\varphi_{k-1} \cup Sa_k$. Если $a_k \in D(b) \setminus \mathrm{Dom}\,\varphi_{k-1}$ для некоторого $b \in \mathrm{Dom}\,\varphi_{k-1}$, то рассмотрим элемент b_k такой, что Sb_k — максимальный элемент в ч.у.множестве

$$U_k \rightleftharpoons \langle \{Sx \mid x \in \mathrm{Dom}\,\varphi_{k-1}, a_k \in D(x)\}; \subseteq \rangle.$$

В силу замечания 2 такой элемент b_k существует. Так как $b_k \in \mathrm{Dom}\varphi_{k-1}$, то $b_k \sim \varphi_{k-1}(b_k)$. Следовательно, по построению полигона ${}_S\hat{A}$ справедливо $b_k \approx \varphi_{k-1}(b_k)$, т. е. существует изоморфизм $\psi_k : D(b_k) \xrightarrow{\sim} D(\varphi_{k-1}(b_k))$ такой, что $\psi_k(b_k) = \varphi_{k-1}(b_k)$. Для любого $x \in \mathrm{Dom}\,\psi_k$ (в частности для a_k) полагаем $\varphi_k(x) \rightleftharpoons \psi_k(x)$. Так как Sb_k — максимальный элемент в множестве U_k, то $\mathrm{Dom}\,\psi_k \cap \mathrm{Dom}\,\varphi_{k-1} = Sb_k$ и определение φ_k корректно. Изоморфизм $\hat{\varphi} \rightleftharpoons \varphi_m$ является автоморфизмом полигона ${}_S\hat{A}$ и расширяет φ . □

Список литературы

[1] *Hrushovski E.* Extending partial isomorphisms of graphs // Combinatorica. 1992. V. 12. P. 204–218.

[2] *Herwig B.* Extending Partial Automorphisms on Finite Structures // Combinatorica. 1995. V. 15. P. 365–371.

[3] *Михалев 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.

ОБ АЛГЕБРАХ С ТЕРМАЛЬНЫМИ $\mathcal{R}$-КОНСЕРВАТИВНЫМИ ФУНКЦИЯМИ

А.Г.Пинус*

Новосибирский государственный технический университет,
Россия, 630092, Новосибирск, пр. К.Маркса 20
e-mail: algebra@nstu.ru

В универсальной алгебре известна (см., к примеру [1] - [3]) целая иерархия конечных алгебр $\mathcal{A} = \langle ; \sigma \rangle$, близких к примальным и определяемых как алгебры, термальные функции которых суть функции сохраняющие те или иные производные отношения алгебры $\mathcal{A}$: квазипримальные (сохраняющие внутренние изоморфизмы), семипримальные (сохраняющие подалгебры), демисемипримальные (сохраняющие подалгебры и автоморфизмы), хемипримальные (сохраняющие конгруэнции) и т.д.

Напомним, что любой клон функций на конечном множестве (в частности клон термальных функций любой конечной алгебры) может быть определен как совокупность функций на множестве, сохраняющих некоторые отношения на этом множестве [4].

Напомним так же, что если R некоторое m - местное отношение на основном множестве A универсальной алгебры $\mathcal{A} = \langle ; \sigma \rangle$ и g — n - местная функция на A, то g сохраняет отношение R($g-$ R - *консервативна*), если для любых $a^i_j \in A$ при $1 \leq i \leq m$ $1 \leq j \leq n$ отношения $R(a^1_j, a^2_j, ..., a^m_j)$ при $1 \leq j \leq n$ влекут отношение $R(g(a^1_1, ..., a^1_n), ..., g(a^m_1, ..., a^m_n))$. Если $\mathcal{R}$ - некоторая совокупность отношений на A, то функция g $\mathcal{R}$ - *консервативна*, если она R - консервативна для любого $R \in \mathcal{R}$. Далее будем считать, что одноместные отношения "быть подалгеброй алгебры $\mathcal{A}$"входят в любую совокупность $\mathcal{R}$ (не указывая на это специально в обозначениях для $\mathcal{R}$), т.е. $\mathcal{R}$ - консервативные функции алгебры $\mathcal{A}$ будут сохранять подалгебры алгебры $\mathcal{A}$. Конечную алгебру $\mathcal{A}$ будем называть $\mathcal{R}$ - *семипримальной*, если термальные функции алгебры $\mathcal{A} = \langle A; \sigma \rangle$ суть $\mathcal{R}$ - консервативные функции этой алгебры. Таким образом, в этих терминах, семипримальные алгебры это — $\varnothing$ - семипримальные, квазипримальные это — Iso - семипримальные, демисемипримальные это —

*Работа выполнена при финансовой поддержке РФФИ (грант 06-01-00159)

Aut - семипримальные.

Заметим так же, что, в силу определений, для любых совокупностей отношений $\mathcal{R}_1, \mathcal{R}_2$ таких, что $\mathcal{R}_1 \subseteq \mathcal{R}_2$ любая $\mathcal{R}_1$ - семипримальная алгебра будет и $\mathcal{R}_2$ - семипримальной.

Для любых $\overline{a} = \langle a_1, ..., a_n \rangle \in A^n$ через $\langle \overline{a} \rangle_{\mathcal{A}}$ обозначим подалгебру алгебры $\mathcal{A}$ порожденную совокупностью $\{a_1, ..., a_n\}$. Пусть $\mathcal{R}$ - совокупность некоторых отношений на основном множестве A алгебры $\mathcal{A} = \langle A; \sigma \rangle$. Для любого $\overline{a} \in A^n$ пусть $c_{\overline{a}}$ - некоторый фиксированный элемент из $\langle \overline{a} \rangle_{\mathcal{A}}$. Совокупность $J = \{\langle \overline{a}, c_{\overline{a}} \rangle | \overline{a} \in A^n\}$ назовем $\mathcal{R}$ - n — *спектром* алгебры $\mathcal{A}$, если для любого m - местного отношения $R \in \mathcal{R}$ и любых $\overline{a}^1 = \langle a_1^1, ..., a_n^1 \rangle, ..., \overline{a}^m = \langle a_1^m, ..., a_n^m \rangle$ отношения $R(a_1^1, ..., a_1^m), ..., R(a_n^1, ..., a_n^m)$ влекут отношение $R(c_{\overline{a}^1}, ..., c_{\overline{a}^m})$. Таким образом, если $g(x_1, ..., x_n)$ R - консервативная функция на $\mathcal{A}$ (напомним про условие $\overline{g}(\overline{a}) \in \langle \overline{a} \rangle_{\mathcal{A}}$ для любого $\overline{a} \in A^n$), то $J_g = \{\langle \overline{a}, g(\overline{a}) \rangle | \overline{a} \in A^n\}$ является $\mathcal{R} - n$ — спектром алгебры $\mathcal{A}$ и обратно, для любого $J = \{\langle \overline{a}, c_{\overline{a}} \rangle | \overline{a} \in A^n\}$ $\mathcal{R} - n$ — спектра n - местная функция $g(x_1, ..., x_n)$ определенная на A как $g(\overline{a}) = c_{\overline{a}}$ для любого $\overline{a} \in A^n$ является $\mathcal{R}$ - консервативной и, при этом, $J_g = J$.

$\mathcal{R}-n$ — спектр $J = \{\langle \overline{a}, c_{\overline{a}} \rangle | \overline{a} \in A^n\}$ назовем *ко - альмагируемым*, если существуют алгебра $\mathcal{B} = \langle B; \sigma \rangle$, элементы $\overline{b} = \langle b_1, ..., b_n \rangle \in B^n, c \in \langle \overline{b} \rangle_{\mathcal{B}}$ и гомоморфизмы $\varphi_{\overline{a}}$ алгебры $\langle \overline{b} \rangle_{\mathcal{B}}$ на алгебры $\langle \overline{a} \rangle_{\mathcal{A}} (\overline{a \in A^n})$ такие, что для $\overline{a} = \langle a_1, ..., a_n \rangle \in A^n \varphi_{\overline{a}}(b_i) = a_i$ и $\varphi_{\overline{a}}(c) = c_{\overline{a}}$.

УТВЕРЖДЕНИЕ 1. $\mathcal{R}$ - консервативная функция $g(x_1, ..., x_n)$ на алгебре $\mathcal{A}\langle A; \sigma \rangle$ является термальной функцией алгебры $\mathcal{A}$ тогда и только тогда, когда ее $\mathcal{R} - n$ — спектр J_g ко-амальгируем.

Доказательство. Пусть алгебра $\mathcal{B}$, ее элементы $\overline{b} \in B^n, c \in \langle \overline{b} \rangle_{\mathcal{B}}$ и гомоморфизмы $\varphi_{\overline{a}}$ ко-амальгамируют спектр J_g функции g. Тогда, так как $c \in \langle \overline{b} \rangle_{\mathcal{B}}$, то существует терм $t(x_1, ..., x_n)$ сигнатуры σ такой, что $c = t(b_1, ..., b_n)$, где $\overline{b} = \langle b_1, ..., b_n \rangle$. Но тогда для любых $\overline{a} = \langle a_1, ..., a_n \rangle \in A^n$

$$g(a_1, ..., a_n) = c_{\overline{a}} = \varphi_{\overline{a}}(c) = \varphi_{\overline{a}}(t(b_1, ..., b_n)) = t(\varphi_{\overline{a}}(b_1), ..., \varphi_{\overline{a}}(b_n)) = t(a_1, ..., a_n),$$

т.е функция g - термальная функция алгебры $\mathcal{A}$.

Обратное, пусть g определена на $\mathcal{A}$ термом $t(x_1, ..., x_n)$ и $\mathcal{B} - n$ — порожденная свободная алгебра многообразия $\mathcal{M}(\mathcal{A})$ порожденного алгеброй $\mathcal{A}$ и $b_1, ..., b_n$ свободные порождающие алгебры $\mathcal{B}, c = t(b_1, ..., b_n), \varphi_{\overline{a}}$ — гомоморфизмы алгебры $\mathcal{B}$ на алгебры $\langle \overline{a} \rangle_{\mathcal{A}}$ продолжающие отображения $b_i \longrightarrow a_i$ для $i = 1, ..., n$. Здесь $\overline{a} = \langle a_1, ..., a_n \rangle$. Тогда $\mathcal{B}, \overline{b}, c$ и $\varphi_{\overline{a}}$ ко-амальгируют $\mathcal{R} - n$ — спектр J_g функции g. Утверждение доказано.

СЛЕДСТВИЕ 1. Конечная алгебра $\mathcal{A}$ является $\mathcal{R}$ - семипримальной

тогда и только тогда, когда для любого $n \in \omega$, любой $\mathcal{R} - n$ — спектр алгебры $\mathcal{A}$ ко-амальгируем.

Рассмотрим теперь ряд конкретных примеров совокупностей $\mathcal{R}$.

1. Напомним, что через $Iso\mathcal{A}$ обозначается полугруппа внутренних изоморфизмов алгебры $\mathcal{A}$ (изоморфизмов между подалгебрами алгебры $\mathcal{A}$). Так же через $Iso\mathcal{A}$ обозначим совокупность двухместных отношений на основном множестве A алгебры A — графиков отображений из $Iso\mathcal{A}$.

Алгебра $\mathcal{A}$ называется дискриминаторной, если трехместная функция дискриминатора термальна для $\mathcal{A}$. С помощью следствия 1 покажем известный факт (доказанный А.Пиксли в [5]), что конечная алгебра $\mathcal{A}$ Iso - семипримальна (квазипримальна) тогда и только тогда, когда она дискриминаторна. Пусть $\mathcal{A}$ дискриминаторная конечная алгебра и $J = \{\langle \overline{a}, c_{\overline{a}}\rangle | \overline{a} \in A^n\}$ некоторый $Iso - n$ — спектр алгебры $\mathcal{A}$. На множестве A^n введем отношение эквивалентности $\simeq$, для $\overline{a}, \overline{e} \in A^n : \overline{a} \simeq \overline{e}$ тогда и только тогда, когда существует изоморфизм $\varphi_{\overline{e}}^{\overline{a}}$ алгебры $\langle \overline{a}\rangle_{\mathcal{A}}$ на алгебру $\langle \overline{e}\rangle_{\mathcal{A}}$ такой, что $\varphi_{\overline{e}}^{\overline{a}}(a_i) = e_i$ для $i = 1, ..., n$. В классах эквивалентности $\overline{a}/\simeq$ выделим по одному представителю $k(\overline{a})$. Пусть $K = \{k(\overline{a}) | \overline{a} \in A^n\}$. Положим $\mathcal{B} = \prod\limits_{\overline{a} \in K} \langle \overline{a}\rangle_{\mathcal{A}}$, элементы $b_i (i \leq n)$ и c из $\mathcal{B}$ определим следующим образом $b_i(\overline{a}) = a_i, c(\overline{a}) = c_a$, где $\overline{a} = \langle a_1, ..., a_n\rangle$. В силу конечности K, дискриминаторности алгебр $\langle \overline{a}\rangle_{\mathcal{A}}$ и того, что отображения $\varphi_{\overline{a}_2}^{\overline{a}_1} g$, для $\overline{a}_1, \overline{a}_2 \in K$, не продолжимы до изоморфизмов между алгебрами $\langle \overline{a}_1\rangle_{\mathcal{A}}$ и $\langle \overline{a}_2\rangle_{\mathcal{A}}$, элементы $b_1, ..., b_n$ (как известно, см., к примеру, [6]) порождают всю алгебру $\mathcal{B}$ и, в частности, $c \in \langle \overline{b}\rangle_{\mathcal{B}}$. Пусть $\pi_{\overline{a}}$ - проекция алгебры $\mathcal{B}$ на алгебру $\langle \overline{a}\rangle_{\mathcal{A}}$. Для $\overline{e} \in A^n$ определим гомоморфизм $\varphi_{\overline{e}} = \varphi_{\overline{e}}^{k(\overline{e})} \cdot \pi_{k(\overline{e})}$ алгебры $\mathcal{B}$ на алгебру $\langle \overline{e}\rangle_{\mathcal{A}}$. Тогда, очевидно, что $\mathcal{B}, b_1, ..., b_n, c, \varphi_{\overline{e}} (\overline{e} \in A^n)$ ко-амальгамируют $Iso - n$ — спектр J. То-есть, согласно следствию 1, алгебра $\mathcal{A}$ Iso - семипримальна. С другой стороны, очевидно, что функция дискриминатора Iso - консервативна и, значит, если алгебра $\mathcal{A}$ Iso - семипримальна, то дискриминатор термален на $\mathcal{A}$, что и требовалось показать.

Напомним также, что как доказано А Пиксли [5] конечная алгебра $\mathcal{A}$ дискримиаторна тогда и только тогда, когда многообразие $\mathcal{M}(\mathcal{A})$ ею порожденное арифметично и $\mathcal{A}$ наследственно проста (все подалгебры алгебры $\mathcal{A}$ просты).

2. Так как $\phi \subseteq Iso$, то, в силу отмеченного выше ϕ - семипримальные алгебры будут и Iso - семипримальными, т.е. в силу предыдущего пункта, дискриминаторными. Внутренний изоморфизм алгебры называется нетривиальным, если он отличен от тождественного отображения некоторой ее подалгебры на себя.

А.Фостером и А.Пиксли [5] доказано, что конечная алгебра $\mathcal{A}$ семи-

примальна (ϕ - семипримальна в нашей терминологии) тогда и только тогда, когда $\mathcal{A}$ дискриминаторна и не имеет нетривиальных внутренних изоморфизмов. Докажем это на основе следствия 1. Итак, пусть $\mathcal{A}$ ϕ - семипримально и, в частности, как отмечено выше, $\mathcal{A}$ - дискриминаторна. Допустим, от противного, что φ - некоторый нетривиальный внутренний изоморфизм алгебры $\mathcal{A}$ с областью определения $\mathcal{A}_1$ и пусть $\overline{a} = \langle a_1, ..., a_n \rangle$ некоторая система порождающих алгебры $\mathcal{A}_1$, а $\varphi(\overline{a}) = \langle \varphi(a_1), ..., \varphi(a_n) \rangle$. $\phi - n$ — спектр J алгебры $\mathcal{A}$ определим произвольным выбором $\overline{c}_{\overline{e}} \in \langle \overline{e} \rangle_{\mathcal{A}}$ для любого $\overline{e} \neq \varphi(\overline{a})$ и $c_{\varphi(\overline{a})} \neq \varphi(c_{\overline{a}})$. Очевидно, что подобный $\phi - n$ — спектр J не может быть ко-амальгамируемым в противоречии с ϕ - семипримальностью алгебры $\mathcal{A}$. Таким образом, ϕ - семипримальные алгебры являются дискриминаторными не имеющими нетривиальных внутренних изоморфизмов. Обратное так же очевидно, т.к. если $\mathcal{A}$ дискриминаторная алгебра без нетривиальных внутренних изоморфизмов, то любой $\phi - n$ — спектр алгебры $\mathcal{A}$ является $Iso - n$ — спектром для $\mathcal{A}$ и в силу дискриминаторности $\mathcal{A}$, а значит и Iso - семипримальности $\mathcal{A}$, этот спектр будет ко-амальгамируемым, т.е. $\mathcal{A}$ — ϕ - семипримальна.

3. Докажем теперь, на основе следствия 1, результат Р.Квакенбуша [8], что конечная алгебра $\mathcal{A}$ деми - семипримальна (Aut - семипримальна в нашей терминологии) тогда и только тогда, когда $\mathcal{A}$ дискриминаторна и все ее внутренние изоморфизмы продолжимы до автоморфизмов. Если $\mathcal{A}$ имеет свойство продолжимости внутренних изоморфизмов до автоморфизмов, то совокупность $Iso - n$ — спектров и $Aut - n$ — спектров алгебры $\mathcal{A}$ совпадают и если при этом $\mathcal{A}$ дискриминаторна, то, как показано выше в пункте 1 все $Iso - n$ — спектры, а значит и $Aut - n$ — спектры этой алгебры, ко-амальгамируемы, то есть $\mathcal{A}$ Aut - семипримальна. Обратное, если $\mathcal{A}$ Aut - семипримальна, то т.к. $Aut \subseteq Iso, \mathcal{A}$ Iso - примальна то есть, дискриминаторна. Пусть, от противного, φ - внутренний изоморфизм алгебры $\mathcal{A}$ с областью определения $\mathcal{A}_1$ не продолжимый до автоморфизма $\mathcal{A}$. Пусть $\overline{a} = \langle a_1, ..., a_n \rangle$ некоторая система порождающих для $\mathcal{A}_1$. $Aut - n$ — спектр J алгебры $\mathcal{A}$ определим произвольным выбором $c_{\overline{e}}$ для любых $\overline{e} \neq \varphi(\overline{a})$ и $c_{\varphi(\overline{a})} \neq \varphi(c_{\overline{a}})$. Тогда очевидно, что подобный $Aut - n$ — спектр J не может быть ко-амальгамируемым в противоречии со следствие 1 и Aut - семипримальностью $\mathcal{A}$.

4. Через $Ihm\mathcal{A}$ обозначим полугруппу внутренних изоморфизмов алгебры $\mathcal{A}$ (гомоморфизмов подалгебр алгебры $\mathcal{A}$ на ее же подалгебры). Так же через $Ihm\mathcal{A}$ будем обозначать совокупность двухместных отношений - графиков отображений из $Ihm\mathcal{A}$. Аналогичным образом $End\mathcal{A}$ будет обозначать и полугруппу эндоморфизмов алгебры $\mathcal{A}$ и совокуп-

ность отношений - графиков этих эндоморфизмов.

На множестве A^n рассмотрим два отшения квазипорядка $:\leq$ и $\leq^1$, для $\overline{a},\overline{e} \in A^n \overline{a} \leq \overline{e}(\overline{a} \leq^1 \overline{e})$ тогда и только тогда, когда существует $\varphi \in Ihm\mathcal{A}(\varphi \in End\mathcal{A})$ такой, что $\varphi(e_i) = a_i$. Эквивалентность порожденная квазипорядком $\leq$ на A^n является отношением $\simeq$ определенным выше, через $\simeq^1$ обозначим отношение эквивалентности порожденное квазипорядком $\leq^1$. Через M и M^1 соответственно обозначим совокупности представителей из $\simeq$ и $\simeq^1$ - классов являющихся максимальными в конечных частично упорядоченных множествах $\langle A^n/\simeq;\leq\rangle$ и $\langle A^n/\simeq^1;\leq^1\rangle$. Пусть J произвольный $Ihm-n$ — спектр ($End-n$ — спектр) алгебры $\mathcal{A}$ тогда очевидно, что набор $\mathcal{B}, b_1, ..., b_n, c \in \mathcal{B}$ и $\varphi_{\overline{a}}(\overline{a} \in A^n)$ ко-амальгамирует спектр J тогда и только тогда, когда он ко-амальгамирует фрагмент $J \restriction M(J \restriction M^1)$ этого спектра, т.е. когда существуют гомоморфизмы $\varphi_{\overline{a}}$, при $\overline{a} \in M(\overline{a} \in M^1)$ алгебры $\langle\overline{b}\rangle_{\mathcal{B}}$ на алгебры $\langle\overline{a}\rangle_{\mathcal{A}}$ такие, что $\varphi_{\overline{a}}(b_i) = a_i$ и $\varphi_{\overline{a}}(c) = c_{\overline{a}}$. Таким образом алгебра $\mathcal{A}$ Ihm - семипримальна (End - семипримальна) тогда и только тогда, когда соответствующие фрагменты любых $Ihm-n$ — спектров ($End-n$ — спектров) ко-амальгамируемы.

Представляет интерес характеризации Ihm - семипримальных и End - семипримальных алгебр в рамках самих этих алгебр наподобие приведенных выше характеризаций ϕ - семипримальных, Aut - семипримальных и Iso - семипримальных алгебр.

Заметим также, что Iso - консервативные функции алгебры $\mathcal{A}$ это так называемые условно термальные функции этой алгебры, Ihm - консервативные - позитивно условно термальные, End - консервативные — $\exists^+$ - условно термальные. Различным соотношениям между классами этих функций посвящена, в частности, работа автора [9].

ЛИТЕРАТУРА

1. H. Werner. Discriminotor Algebras, - Akademie - Verlag, Berlin, 1978.

2. G.Gratzez. Universal Algebra, 2 En. - Springer Verlag, New - York - Heidelberg - Berlin, 1979.

3. А.Г.Пинус. Производные структуры универсальных алгебр, Из-во НГТУ, Новосибирск, 2007.

4. В.Г.Бондарчук, Л.А.Калужнин, В.Н.Котов, Б.А.Ромов. Галуа теория для алгебр Поста I, II. - Кибернетика, №3, 1969, с. 1-10, №5, 1969, с. 1 - 9.

5. A.F.Pixley. The ternary discriminator function in universal algebra. - Math. Ann., v. 191, 1971, p. 167 - 180.

6. A.G.Pinus. Boolean Constructions in Universal Algebra. - Kluver Acad. Publ., Dordrecht - Boston -London, 1993.

7. A.L.Foster, A.F. Pixley. Semi - categorical algebras I, II. - Math. Zeits., v. 83, 1964, p. 147-169. v. 84, 1964, p. 169-184.

8. R.W.Quackonbuch. Semi - simple equational classes with distributive congruence lattices. - preprint, 1974.

9. А.Г.Пинус. О диаграмме классов условно термальных функций. - Фундаментальная и прикладная математика, т. 8, №4, 2002, с. 1099-1109.

ON SOME QUESTIONS IN THE THEORY OF ORDERED SETS, MODEL THEORY AND UNIVERSAL ALGEBRA

A.G. Pinus*

Novosibirsk State Technical University
e-mail: algebra@nstu.ru

In this work the author attempted to collect and remind his colleagues of problems published in a number of his works that are still open (as far as the author knows).

These questions are concerned with theory of ordered sets, lattices, boolean algebras, model theory of logics with generalized quantifiers, universal algebra. The author attempted to classify there problems according to the fields mentioned although some of the problems could be attributed to several fields at once.

The problems discussed have different importance, but the author thinks that the answers to these problems will prove to be interesting. The author does not justify the importance of stated problems. He only gives a brief commentaries and links to papers where these problems were first formulated. The author uses standard notation of model theory and universal algebra.

1. *Logics with generalized quantifiers.*

In [1] the language $L(I)$ with the Hartig quantifier has been introduced. The set of formulas of $L(I)$ is inductively defined as an extension of the set of elementary formulas with the following additional rule: if $\varphi(x, \overline{y})$ and $\psi(x, \overline{z})$ are formulas of $L(I)$ with free variables $x, \overline{y}$ and $x, \overline{z}$ respectively then $Ix(\varphi(x, \overline{y}), \psi(x, \overline{z}))$ is also $L(I)$-formula with $\overline{y}, \overline{z}$ occurring as free variables. For any elements $\overline{a}, \overline{b}$ of an algebraic system M we have

$$M \models Ix(\varphi(x, \overline{a}), \psi(x, \overline{b})) \Longleftrightarrow |\{c \in M | M \models \varphi(c, \overline{a})\}| =$$

$$= |\{d \in M | M \models \psi(d, \overline{b})\}|.$$

*The paper was supported by the Russian Foundation of Fundamental Researches (06-01-00159).

The survey of the basic results connected with the language $L(I)$ is given in [2]. Some of open questions formulated in [2] are.

Question 1. a) What classes of cardinals are the spectors of $L(I)$-formulas?

b) What are the structural properties of the spectors of $L(I)$-formulas?

c) Is the statement that the spector of any second order formula is the spector of some $L(I)$-formula, consistent with ZF?

A more particular question has been formulated in [3].

Question 2. Is it true that the Hanf-numbers (Lowenheim-numbers) of second order logic and the language $L(I)$ are equal?

Note that in [4] this equation for the Hanf-numbers has been proved assuming $V = L$.

Among open questions there are some questions from [5] on the decidability of $L(I)$-theories.

Question 3. Are the following $L(I)$-theories decidable

a) of all abelian groups,

b) one unary function f with the following condition:

$$\forall x \neg \exists x_1, ..., x_{n+1} (\underset{i \neq j}{\&} x_i \neq x_j \& f(x_i) = x)$$

for fixed number $n \geq 2$?

Note, that in works [6] and [7] the decidability of $L(I)$-theory of all abelian p-groups and the undecidability of $L(I)$-theory of unary function were proved respectively.

By analogy with the set of $L(I)$-formulas, substituting the symbol I with the symbol A, work [7] has defined the set of the formulas $L(A)$ — the set of the formulas of the language with the automorphism-quantifier. Here $M \models \forall x(\varphi(x, \overline{a}), \psi(x, \overline{b})) \Longleftrightarrow$ there exist some automorphism η of the algebraic system M such that

$$\eta(\{c \in M | M \models \varphi(c, \overline{a})\}) = \{d \in M | M \models \psi(d, \overline{b})\}.$$

Some open questions formulated in [7] are

Question 4. a) Is the $L(A)$-theory of the class of all linear orders decidable?

b) Is the language $L(A)$ projective equivalent to the second order logic?

A special case of question 2 b) was mentioned in [8].

Question 5. Is class of all well orderings a projective class of the language $L(A)$?

The paper [9] by A.Mostowsky has introduced languages $L(Q_\alpha)$ with the power-quantifiers Q_α as an extension of the set of elementary formalas by the following additional rule: if $\varphi(x, \overline{y}) \in L(Q_\alpha)$ then $Q_\alpha x \varphi(x, \overline{y}) \in L(Q_\alpha)$ and $M \models Q_\alpha x \varphi(x, \overline{a}) \Longleftrightarrow |\{c \in M | M \models \varphi(c, \overline{a})\}| \geq \aleph_\alpha$.

In [10] it was proven that the quantifiers Q_0 and Q_1 can be eliminated for a class of all symmetric groups and was formulated

Question 6. Which quantifiers $Q_\alpha(\alpha > 1)$ can be eliminated for a class of all symmetric groups?

We have also formulated the following questions:

From [11]

Question 7. Find Hanf-number and Lowenheim-number for the first order theory of the class of rings of continuous real-valued functions on topological spaces.

From [18]

Question 8. Is the universal theory of the operation of lexicographic addition (of lexicographic product) on the class of all isomorphisms types of linear orders decidable?

The elementary theories of this operations are undecidable [12].

Universal Algebra.

a) *The derived structures of universal algebras.*

In the study of epimorphism skeletons of varieties of universal algebras the important role plays the concept of quasisimple algebra which was introduced in [13] and which is some generalization of concepts of simple and pseudosimple algebras. The structure of congruence lattices of pseudosimple algebras is well known (it is ordinals $\omega^\alpha + 1$, see [14]). The question on the structure of congruence lattices of quasisimple algebras is open. Remember, that the algebra $\mathcal{A}$ defined as quasisimple if for any its not largest congruence θ there exists some congruence θ' such that $\theta \leq \theta'$ and $\mathcal{A}/\theta' \cong \mathcal{A}$. The lattice L with 1 is defined as up-indecomposable if for any $a \in L\backslash\{1\}$ there exists $b \in L$ such that $a \leq b$ and $L \cong L \restriction \geq b = \{c \in L | b \leq c\}$.

The work [13] contains

Question 9. Is it true that for any algebraic up-indecomposable algebraic lattice L there exists some quasisimple algebra $\mathcal{A}$ such that $Con\mathcal{A} \cong L$?

Particular cases with positive answers are considered in [13].

The work [15] introduced the lattice $Qord\mathcal{A}$ — the lattice of all quasiorders on the universal algebra $\mathcal{A}$ (quasiorders that are preserved by signature operations of the algebra $\mathcal{A}$). In [16] it was proven that any algebraic lattice is isomorphic to the lattice $Qord\mathcal{A}$ for some algebra $\mathcal{A}(Qord\mathcal{A} = Con\mathcal{A}$ in this proof). In connection with this result in work [16] formulated

Question 10. a) Describe pairs of algebraic lattices $\langle L_1, L_2\rangle$ such that $L_2 \subseteq L_1$ and there exists some universal algebra $\mathcal{A}$ such that $\langle Qord\mathcal{A}, Con\mathcal{A}\rangle \cong \langle L_1, L_2\rangle$.

b) Describe pairs $\langle L, f\rangle$ where L is some algebraic lattice and f is some involution on L such that for some universal algebra $\mathcal{A}$ the pairs $\langle Qord\mathcal{A}, *\rangle$

and $\langle L, f\rangle$ are isomorphic.

Here $\leq^*$ is quasiorder dual to the quasiorder $\leq$.

Note, that some particular answers to these questions are given in the work [17].

In [18] a filter $EQord\mathcal{A}$ on the lattice $Qord\mathcal{A}$ for any algebra $\mathcal{A}$ has been defined (the filter of natural quasiorders on $\mathcal{A}$) which is generated by some naturalized quasiorder $\preceq^{\mathcal{A}}$ on the algebra $\mathcal{A}$ (the smallest quasiorder on $\mathcal{A}$ that contain the algebraic relation $\preceq^{\mathcal{A}}$ on the algebra $\mathcal{A}$). In [18] some properties of the quasiorder $\leq^{\mathcal{A}}$ and the filter $EQord\mathcal{A}$ are given and some open questions are formulated. The algebra $\mathcal{A}$ for which relations $\preceq^{\mathcal{A}}$ and $\leq^{\mathcal{A}}$ coinsides is defined as natural algebra.

Question 11. a) Find the characterization of lattices which are isomorphic to the lattice $EQord\mathcal{A}$ for some algebra $\mathcal{A}$.

b) Is it true, that for any quasiorder $\langle A; \leq\rangle$ with the property: for any $a, b \in A$ if there exists $c \in A$ such that $c \leq a, b$ there exists $d \in A$ such that $a, b \leq d$, there exists a natural algebra $\mathcal{A} = \langle A; \sigma\rangle$ such that the quasiorder $\leq$ is the algebraic relation $\preceq^{\mathcal{A}}$ on $\mathcal{A}$?

c) Is it true that for any algebra $\mathcal{A}$ there exists its naturalization?

Here the naturalization of the algebra $\mathcal{A} = \langle A; \sigma\rangle$ is an enrichmend $\mathcal{A}' = \langle A; \sigma'\rangle (\sigma \subseteq \sigma')$ of the algebra $\mathcal{A}$ such that the algebra $\mathcal{A}'$ is natural and the relations $\leq^{\mathcal{A}'}$ and $\preceq^{\mathcal{A}}$ coinside.

By the studying positive-conditional terms (see below) in [19] the question been formulated.

Question 12. Describe the pairs $\langle S, H\rangle$ of families of subsets of the set A and families H of maps of sets from S on to sets from S such that there exists some universal algebra $\mathcal{A} = \langle A; \sigma\rangle$ satisfying $S = Sub\mathcal{A}$ and $H = Ihm\mathcal{A}$.

Here $Ihm\mathcal{A}$ is the semigroup of inner homomorphisms of the algebra $\mathcal{A}$, that is homomorphisms of subalgebras of the algebra $\mathcal{A}$ on its subalgebras.

A series of work study the relation of elementary equivalence of derived structures of free algebras of varieties. The survey of these results is given in [20]. For any variety $\mathcal{M}$ of universal algebras we denote the k-generation $\mathcal{M}$-free algebra as $\mathcal{F}_{\mathcal{M}}(k)$. On the class of all infinite cardinals we consider the following equivalence relations

$$k \equiv^{\mathcal{M}}_{Sub} \lambda \Longleftrightarrow Sub\mathcal{F}_{\mathcal{M}}(k) = Sub\mathcal{F}_{\mathcal{M}}(\lambda);$$

$$k \equiv^{\mathcal{M}}_{Aut} \lambda \Longleftrightarrow Aut\mathcal{F}_{\mathcal{M}}(k) = Aut\mathcal{F}_{\mathcal{M}}(\lambda);$$

$$k \equiv^{\mathcal{M}}_{Con} \lambda \Longleftrightarrow Con\mathcal{F}_{\mathcal{M}}(k) = Con\mathcal{F}_{\mathcal{M}}(\lambda);$$

$k \nabla \lambda$ for any k and λ;

$k \equiv_2 \lambda \Longleftrightarrow$ theories of the cardinals k and λ coinsides in the second order logic;

$k \equiv_p \lambda \Longleftrightarrow$ theories of the cardinals k and λ coinsides in the second order language with quantifiers on permutations.

Note, that the relation $k \equiv_p \lambda$ coinsides with the fact that full symmetric groups on k and on λ are elementary equivalent.

A number of open questions about relations $\equiv^{\mathcal{M}}_{Sub}, \equiv^{\mathcal{M}}_{Aut}, \equiv^{\mathcal{M}}_{Con}$ has been formulated in [20].

Question 13. Let $\mathcal{M}$ be some nontrivial finite based variety of universal algebras of finite signatures

a) Is it true that $\equiv^{\mathcal{M}}_{Sub}, \equiv^{\mathcal{M}}_{Aut}, \equiv^{\mathcal{M}}_{Con} \in \{\nabla, \equiv_p, \equiv_2\}$?

b) *Let* $\langle \equiv^1, \equiv^2, \equiv^3 \rangle$ be some triple of equivalence relations such that $\equiv^i \in \{\nabla, \equiv_p, \equiv_2\}$. Is it true, that there exists some variety $\mathcal{M}$ such that $\langle \equiv^1, \equiv^2, \equiv^3 \rangle = \langle \equiv^{\mathcal{M}}_{Sub}, \equiv^{\mathcal{M}}_{Aut}, \equiv^{\mathcal{M}}_{Con} \rangle$?

Question 14. a) Is it true that equivalence relations $\equiv^{\mathcal{M}}_{Con}$ and $\equiv_\alpha$ coinside for varieties of unars? Describe the relations $\equiv^{\mathcal{M}}_{Aut}$ for such varieties.

b) Is it true that relations $\equiv^{\mathcal{M}}_{Sub}, \equiv^{\mathcal{M}}_{Con}, \equiv_\alpha$ coinside for varieties of all groups. of all abelian groups?

c) Is it true that $\equiv^{\mathcal{M}}_{Con}$ and $\equiv_2$ coinside for normal varieties? Describe the relation $\equiv^{\mathcal{M}}_{Sub}$ for normal nonunars varieties.

d) Is it true that $\equiv^{\mathcal{M}}_{Con}$ and $\equiv_\alpha$ conside for regular varieties? Describe the relation $\equiv^{\mathcal{M}}_{Aut}$ for such varieties.

e) Describe relations $\equiv^{BA}_{Sub}, \equiv^{BA}_{Aut}, \equiv^{BA}_{Con}$. Here BA is the variety of Boolean algebras.

f) Describe relations $\equiv^{\mathcal{M}}_{Aut}$ and $\equiv^{\mathcal{M}}_{Con}$ for various varieties of lattices. For which varieties $\mathcal{M}$ of lattices (except the variety of distributive lattices, for which see -[21]) relations $Con'\mathcal{F}_{\mathcal{M}}(k) \equiv Con'\mathcal{F}_{\mathcal{M}}(\lambda)$ and $\equiv_2$ coinside? Here $Con'\mathcal{A}$ is a enrichment of the lattice $Con\mathcal{A}$ by addition of partial multiplication operation $\circ$ of congruences (the value of operation $\circ$ is defined for permutables congruences).

Note that the answer to the question 14 a) on the relation $\equiv^{\mathcal{M}}_{Aut}$ for varieties of unars is dependent on the answer to the following pure group-theoretical question: is it true that for any finite or countable group G and any infinite cardinals k and λ the relation $Symk \equiv Sum\lambda$ implies the relation $G\imath\, Symk \equiv G\imath\, Sym\lambda$. Here $Symk$ is the full symmetric group on the cardinal k.

The work [22] introduced subgroups $SAut\mathcal{A}$ and $PSAut\mathcal{A}$ of proper and pure proper automorphisms of the universal algebra $\mathcal{A}$. The automorphism φ of the algebra $\mathcal{A}$ is proper (pure proper) if it can be represented as a product

of automorphisms of the type $x \longrightarrow t(x, \overline{a})(x \longrightarrow t'(x))$ and their inverses, here $t'(x), t(x, \overline{y})$ are terms of the algebra $\mathcal{A}$ and $\overline{a}$ are elements from $\mathcal{A}$. The same work [22] has also proved that for any groups $G_3 \trianglelefteq G_2 \trianglelefteq G_1$ such that $G_3 \subseteq G_2 \cap Z(G_1)$ (here $Z(G_1)$ is the center of G_1) there exists some universal algebra $\mathcal{A}$ such that $\langle G_3, G_2, C_1\rangle \cong \langle PSAut\mathcal{A}, SAut\mathcal{A}, Aut\mathcal{A}\rangle$. This work [22] has formulated the following.

Question 15. Is it true, that for any groups $G_3 \trianglelefteq G_2 \trianglelefteq G_1 \trianglelefteq G$ such that $G_3 \subseteq G_2 \cap Z(G_1)$ there exists some universal algebra $\mathcal{A}$ such that $\langle G_3, G_2, G_1, G\rangle \cong \langle PSAut\mathcal{A}, SAut\mathcal{A}, WAut\mathcal{A}\rangle$?

Here $WAut\mathcal{A}$ is the group of weak automorphisms of the algebra $\mathcal{A}$. Note that in [23] it was proven that for any groups $G_1 \trianglelefteq G$ there exits some algebra $\mathcal{A}$ such that $\langle G_1, G\rangle \cong \langle Aut\mathcal{A}, WAut\mathcal{A}\rangle$.

Let $FCon\mathcal{A}$ be the down-subsemilattice of the lattice $Con\mathcal{A}$ which consists of congruences of the algebra $\mathcal{A}$ that are defined by some first order formulas on the algebra $\mathcal{A}$ and $OFCon\mathcal{A}$ be the analogue down-subsemilattice of congruences that are defined by the quantifierfree first order formulas on $\mathcal{A}$.

The work [24] formulated

Question 16. For which 0-1-down-subsemilattices $L_0 \subseteq L_1$ of the algebraic lattice L there exists some algebra $\mathcal{A}$ such that $\langle L_0, L_1, L\rangle \cong \langle OFCon\mathcal{A}$, $FCon\mathcal{A}, Con\rangle$?

Answers for some special cases of this problem are given in [24].

For any algebra $\mathcal{A} = \langle A : \sigma\rangle$ its subalgebra $\mathcal{B}$ is open formulae definable (paremetric open formulae definable) if there exists some quantifierfree formula $\phi(x)$ of the signature σ (some quantifierfree formula $\phi(x, \overline{y})$ and some elements $\overline{c}$ from $\mathcal{A}$) such that

$$\mathcal{B} = \langle b \in \mathcal{A} | \mathcal{A} \models \phi(b)\}(\mathcal{B} = \{b \in \mathcal{A} | \mathcal{A} \models \phi(b, \overline{c})\}).$$

Similarly the concept of formulae definable and parametric formulae definable subalgebras of the algebra $\mathcal{A}$ are defined for first order formulas $\phi(x), \phi(x, \overline{y})$.

Let $PSub\mathcal{A}(PPSub\mathcal{A}, ESub\mathcal{A}, PESub\mathcal{A})$ be families of all open formulae (parametric open formulae, formulae and parametric formulae definable subalgebras of he algebra $\mathcal{A}$.

The work [25] has several results on the realization of algebraic lattices and theirs 0-1-down-subsemilattices as triples $\langle PSub\mathcal{A}, PPSub\mathcal{A}, Sub\mathcal{A}\rangle$ for some algebras $\mathcal{A}$ and has formulated the open

Question 17. Is it that for any algebraic lattice L and its 0-1-down-subsemilattices L_0, L_1, L_2, L_3 such that

$$\begin{array}{ccc} L_0 & \subseteq & L_1 \\ \subseteq & & \subseteq \\ L_2 & \subseteq & L_3 \end{array} \subseteq L$$

there exists some universal algebra $\mathcal{A}$ such that $\langle L_0, L_1, L_2, L_3, L\rangle \cong \langle PSub\mathcal{A}, ESub\mathcal{A}, PPSub\mathcal{A}, PESub\mathcal{A}, Sub\mathcal{A}\rangle$?

b) *The varieties of universal algebra and some construction on universal algebras.*

For any class $\mathcal{K}$ of universal algebras we denote as $J\mathcal{K}$ the class of all isomorphism types of $\mathcal{K}$-algebras. On $J\mathcal{K}$ we define the two quasiorder relations $\leq, \ll$ and some operation $\times : a, b, c \in J\mathcal{K}$, i.e. are isomorphism types of some $\mathcal{K}$-algebras $\mathcal{A}, \mathcal{B}, \mathcal{Z}$ correspondingly, then

$a \leq b \Longleftrightarrow \mathcal{A}$ is isomorphicaly embeddable in $\mathcal{B}$,

$a \ll b \Longleftrightarrow \mathcal{A}$ is homomorphic image of $\mathcal{B}$,

$a \times b = c \Longleftrightarrow \mathcal{C}$ is isomorphic to the cartesian product of algebras $\mathcal{A}$ and embeddable in $\mathcal{B}$.

Let $\mathcal{K}_{\aleph 0} = \{\mathcal{A} \in \mathcal{K} || \mathcal{A}| \leq \aleph 0\}$. The quasiorder family $\langle J\mathcal{K}; \leq\rangle(\langle J\mathcal{K}_{\aleph 0}; \leq\rangle)$ will be called the embedding skeleton (the countable embedding skeleton) of the class $\mathcal{K}$; $\langle J\mathcal{K}; \ll\rangle(\langle J\mathcal{K}_{\aleph 0}; \ll\rangle)$ — the (countable) epimorphism skeleton of $\mathcal{K}$; the commutative semigroup $\langle J\mathcal{K}; \times\rangle(\langle J\mathcal{K}_{\aleph 0}; \times\rangle)$ — the cartesian (countable cartesian) skeleton of $\mathcal{K}$; $\langle J\mathcal{K}; \ll, \leq\rangle(\langle J\mathcal{K}_{\aleph 0}; \ll, \leq\rangle)$ — the double (countable double) skeleton of $\mathcal{K}$. Basic results for skeletons of varieties of algebras are given in the monography [26] and in the survey [27]. In particular the author has several results on embedding quasiordered sets into skeletons of congruence-distributive varieties and a classification of such varieties by structure of their countable skeletons.

The following questions are open.

Question 18. Let $\mathcal{M}$ be some nontrivial congruence distributive variety

a) [27] is any quasiordered set isomorphicaly embedded in $\langle J\mathcal{M}; \leq\rangle$?

b) [28] has any $\mathcal{M}$-algebra some cover in $\langle J\mathcal{M}; \ll\rangle$?

c) [29] is any automorphism of skeletons $\langle J\mathcal{M}; \ll\rangle, \langle J\mathcal{M}; \leq\rangle, \langle J\mathcal{M}; \times\rangle, \langle J\mathcal{M}; \ll, \leq\rangle$ trivial ?

Jn particular, this question arises for the variety BA of Boolean algebras.

Question 19. Let $\mathcal{M}$ be some nontrivial discriminator variety

a) [30] describe the structure of $\langle J\mathcal{M}_{\aleph 0}; \leq\rangle$ for locally finite and not finitely generated variety $\mathcal{M}$ (for other cases the structure of $\langle J\mathcal{M}_{\aleph 0}; \leq\rangle$ is described in [26], [27]. In particular, is it true that $\langle J\mathcal{M}_{\aleph 0}; \leq\rangle$ is the better quasiorder if $\langle J(\mathcal{M}_S)_{\aleph 0}; \leq\rangle$ is the better quasiorder?

Here $\mathcal{M}_S$ is a family of simple $\mathcal{M}$-algebras.

In [31] by continuum-hypothesis (CH) it was proven that any finite set with two quasiorders is isomorphicaly embedded in $\langle J\mathcal{M}; \leq, \ll\rangle$ for any nontrivial congruence-distributive variety $\mathcal{M}$ with congruence-extension property. In connection with this result works [31], [27] contain following open questions

Question 20. a) Is it possible to prove, that any finite set with two quasiorders is isomorphicaly embeddable in the double skeleton of any nontrivial congruence-distributive variety with the congruence-extension property without continuum-hypothesis?

b) Is the analogous result (under assumption of the CH or without it) for any countable sets with two quasiorders?

The work [32] on the basis of D. Ketonen's result [33] from $\langle JBA_{\aleph 0}; \times\rangle$ has proved that for any nontrivial congruence-distributive variety $\mathcal{M}$ any countable commutative semigroup is isomorphicaly embeddable into the countable cartesian skeleton of $\mathcal{M}$. In connection with this result [27] has formulated

Question 21. Describe the commutative semigroups which are isomorphicaly embeddable in cartesian skeletons of any nontrivial congruence distributive variety.

In connection with previous results on cartesian, embedding and epimorphism skeletons of congruence distributive varieties, [34] has formulated following questions

Question 22. a) Is it true that any countable commutative quasiordered semigroup is isomorphically embededdable in $\langle J\mathcal{M}; \times, \ll\rangle$ for any nontrivial congruence distributive variety $\mathcal{M}$?

b) Is it true that any countable commutative quasiordered semigroup is isomorphically embeddable in $\langle J\mathcal{M}; \times, \leq\rangle$ for any nontrivial congruence distributive variety $\mathcal{M}$ with the congruence-extension property?

Question 23. Is the elementary theory of the skeletons $\langle J\mathcal{M}; \leq\rangle$ decidable for any congruence distributive variety $\mathcal{M}$ with the congruence-extension property?

Other results on the decidability of the elementary theories of skeletons of congruence distributive varieties are in [27], [34].

In [35] by the proposition of negation of Vopenka-principle it was proven that for any nontrivial congruence distributive variety $\mathcal{M}$ with congruence-extension property and zero-element in the skeleton $\langle J\mathcal{M}; \leq\rangle$ there exists a class of pairwise incomparable elements which is not a set. In connection with this result [35] has formulated

Question 24. a) Is it true that negation of Vopenka-principle is equivalent (relative to ZFC) to the following statement: for any nontrivial congruence distributive variety $\mathcal{M}$ with congruence-extension property in $\langle J\mathcal{M}; \leq\rangle$ (in $\langle JBA; \leq\rangle$) there exists a proper class of pairwise incomparable elements?

b) Is it true that the skeleton $\langle J\mathcal{M}; \ll\rangle$ (in $\langle JBA; \ll\rangle$) of any congruence distributive variety $\mathcal{M}$ contains a proper class of pairwise incomparable elements?

Note that for not risidual small discriminator varieties the answer to the last question is positive.

The work [35] formulated following questions on varieties of lattices.

Question 25. Is the countable epimorphism (countable embedding) skeleton of any finite generated variety of lattices the best quasiorder? Is the answer to this question positive for the variety of distributive lattices?

While studying skeletons of varieties the following open question ([37]) naturally arises.

Question 26. Is it true that any nontrivial quasivariety with Fraser-Horn property contains a nontrivial congruence distributive variety?

Let $\mathcal{A}^{\mathcal{B}}$ denote the boolean power of universal algebra $\mathcal{A}$ with boolean exponent $\mathcal{B}$ and $\mathcal{A}^{\mathcal{B}}(\theta)$ (here θ is a congruence of the algebra $\mathcal{A}$) — the congruence-boolean power of algebra $\mathcal{A}$, that is subalgebra of algebra $\mathcal{A}^{\mathcal{B}}$ with basic set $\{f \in \mathcal{A}^{\mathcal{B}} |$ for any $i, j \in \mathcal{B}^*$ $\theta(f(i), f(j))\}$. Here $\mathcal{B}^*$ is the Stone space of Boolean algebra $\mathcal{B}$. See [26], [27] of these constructions. These works contain following questions.

Question 27. Given a description of Boolean-separable universal algebras, i.e. such algebras $\mathcal{A}$ that for any Boolean algebras $\mathcal{B}_1, \mathcal{B}_2$ the isomorphism of $\mathcal{A}^{\mathcal{B}_1}$ and $\mathcal{A}^{\mathcal{B}_2}$ implies the isomorphism of $\mathcal{B}_1$ and $\mathcal{B}_2$.

b) Given a description of first order formulas which hold when switching to congruence-boolean powers, i.e. such formulas φ that for any algebra $\mathcal{A}$ any Boolean algebra $\mathcal{B}$ and any $\theta \in Con\mathcal{A}$ from $\mathcal{A} \models \varphi$ follows that $\mathcal{A}^{\mathcal{B}}(\theta) \models \varphi$.

c) Given a description of all algebras $\mathcal{A}$ such that $\mathcal{M}(\mathcal{A}) = \{\mathcal{A}^{\mathcal{B}} | \mathcal{B}$ any Boolean algebra$\}$. Here $\mathcal{M}(\mathcal{A})$ is the variety generated by $\mathcal{A}$ and $I\mathcal{K}$ is the class of all algebras that are isomorphic to some $\mathcal{K}$ algebra.

c) *Conditional terms and the scales of computability potentials.*

The concepts of conditional, positive conolitional, $\exists^+$-conditional and elementary conditional terms was introduced by the author was studied in a long series of his work. The essential part of results connected to these concepts can be found in the monography [38] and in survey [39]. For any universal algebra $\mathcal{A} = \langle A; \sigma \rangle$ we denote as $T(\mathcal{A})$ the set of all termal functions of algebra $\mathcal{A}$, as $CT(\mathcal{A})$-the set of all conditional termal functions of algebra $\mathcal{A}$, as $PCT(\mathcal{A})$-the set all positive conditional termal functions, as $\exists^+CT(\mathcal{A})$-the set of all $\exists^+$-conditional termal functions and as $ECT(\mathcal{A})$-the set of all elementary conditional termal functions of algebra $\mathcal{A}$. The considence of sets $CT(\mathcal{A}_1)$ and $CT(\mathcal{A}_2)$ for algebras $\mathcal{A}_1 = \langle A; \sigma_1 \rangle$ and $\mathcal{A}_2 = \langle A; \sigma_2 \rangle$ with the common basic set (by analogy to the definition of the rational equivalence of $\mathcal{A}_1$ and $\mathcal{A}_2$ when $T(\mathcal{A}_1) = T(\mathcal{A}_2)$) we define as conditionally rational equivalence of algebras $\mathcal{A}_1$ and $\mathcal{A}_2$. By analogy we

define relations of positive conditionally rational equivalence, $\exists^+$-conditionally rational equivalence and elementary conditionally rational equivalence relations. The using bijections between basic sets of universal algebras gives a possibility of expansion of the concepts of these equivalences to any algebras and classes of algebras.

In [40] an analog of the Malcev's theorem [41] (on rational equivalence of varieties and equivalence of categories of these varieties) was proven for the relation of the elementary conditionally rational equivalence of elementary classes of universal algebras and some categories of these classes connected with some enrichment of categories of elementary embeddings algebras of these classes. The work [40] has formulated the following open question

Question 28. Is it possible, and if it is, how the concept of elementary condition in the definition of the elementary conditional terms should be changed so that after the change the elementary conditionally rational equivalence relation on the elementary classes of algebras would correspond to equivalence of categories of elementary embeddings on this classes?

In [42] has described universal algebras $\mathcal{A}$ for that satisfy various equations between sets $PCT(\mathcal{A}), CT(\mathcal{A}), \exists^+CT(\mathcal{A})$ and $ECT(\mathcal{A})$ and has formulated

Question 29. Give an algebraic characterization of finite (uniformly locally finite of finite signature) algebras for which we have the equation $PCT(\mathcal{A}) = \exists^+CT(\mathcal{A})$.

Question 30. Is the equation $[\mathcal{A}]_{re} = [\mathcal{A}]_{pcre}$ possible for some finite algebra $\mathcal{A}$?

Here $[\mathcal{A}]_{re}([\mathcal{A}]_{pcre}, [\mathcal{A}]_{cre})$ is the class of all algebras which are rational (positive conditionally rational, conditionally rational) equivalent to the algebra $\mathcal{A}$.

The work [43] has studied partitions of classes $[\mathcal{A}]_{cre}$ on classes of rational equivalent algebras and has formulated

Question 31. Find a description of all finite algebras $\mathcal{A}$ such that $[\mathcal{A}]_{cre}$ is a union of infinite set of classes $[\mathcal{B}]_{re}$ for some algebras $\mathcal{B}$.

For any universal algebra $\mathcal{A}$ the clone of functions $CT(\mathcal{A})$ is an extension of clone $T(\mathcal{A})$ with a single function $d(x, y, z)$ — the discriminator function. In [44] it was proved that there exist some infinite algebra $\mathcal{A}$ such that clones $PCT(\mathcal{A}), ECT(\mathcal{A})$ are not finite extensions of the clone $T(\mathcal{A})$. The work [39] has formulated

Question 32. Is it true that for any finite algebra $\mathcal{A}$ clones $PCT(\mathcal{A}), \exists^+CT(\mathcal{A})$, $CT(\mathcal{A})$ are finite extensions of the clone $T(\mathcal{A})$?

The work [45] has

Question 33. a) Is it true that there exist (not locally finite) conditionally rational equivalent discriminator varieties that are not rational equivalent?

b) Is it true that there exist (not locally finite) conditionally rational equivalent varieties $\mathcal{M}_1$ and $\mathcal{M}_2$ such that the algebras $\mathcal{F}_{\mathcal{M}_1}(\aleph 0)$ and $\mathcal{F}_{\mathcal{M}_2}(\aleph 0)$ are not conditionally rational equivalent and inverse?

In [46] there is a question on analogs of Lovash's-theorem (for any finite algebras $\mathcal{A}$ and $\mathcal{B}$ the isomorphism of algebras $\mathcal{A}^2$ and $\mathcal{B}^2$ implies the isomorphism of algebras $\mathcal{A}$ and $\mathcal{B}$ for relations of conditionally (elementary conditionally) rational equivalence.

Question 34. Is it true that for any finite algebras $\mathcal{A}$ and $\mathcal{B}$ the conditionally (elementary conditionally) rational equivalence of algebras $\mathcal{A}^2$ and $\mathcal{B}^2$ implies the conditionally (elementary conditionally) rational equivalence of algebras $\mathcal{A}$ and $\mathcal{B}$?

The invariants of relation of conditionally rational equivalence of finite algebras are pairs $\langle Sub\mathcal{A}, Iso\mathcal{A}\rangle$. In some works the author describes (for example, see [38]) these invariants for semilattices, lattices, Boolean algebras, fields, unares.

In [47] the following question was formulated

Question 35. Describe pairs $\langle Sub\mathcal{A}, Iso\mathcal{A}\rangle$ for groups and for rings.

The concept of the scale of computability potentials on n-element algebras was introduced in [39]. Two algebras $\mathcal{A}_1 = \langle A; \sigma_1\rangle$ and $\mathcal{A}_2 = \langle B; \sigma_2\rangle$ have the same computability potentials ($\mathcal{A}_1 \sim \mathcal{A}_2$) if there exists a bijection g of set A on set B such that $CT(\mathcal{A}_1) = g^{-1}CT(\mathcal{A}_2)g$. Further we assume that $A = \{0, 1, ..., n-1\}$ for any n-element set A. On the set $CT_n = \{\mathcal{A}/\sim | A = \{0, 1, ..., n-1\}\}$ we define order relation $\leq$: $\mathcal{A}_1/\sim \leq \mathcal{A}_2/\sim$ if there exists some permutation π on the set $\{0, 1, ..., n-1\}$ such that $CT(\mathcal{A}_1) \subseteq \pi^{-1}CT(\mathcal{A}_2)\pi$. The partially ordered set $\langle CT_n; \leq\rangle$ we define as the scale of computability potentials of n-element algebras. The survey of the basic results on the scales $\langle CT_n; \leq\rangle$ can be found in [48]. Similarly instead of $CT(\mathcal{A})$ the scale $\langle ECT_n; \leq\rangle$ is defined based on set $ECT(\mathcal{A})$. The work [48] list several open questions on these scales that were formulated is earlier works by the author.

Question 36. a) Find "confidence"intervals for numbers $|CT_n|$, that is, find recursive sequence $a_1 < a_2 < a_3 < ... < a_n < ...$ such that $a_n \leq |CT_n| < a_{n+1}$ for any $n \in \omega$.

b) Find a "good"assimptotic exponential estimate of the sequence $|CT_1|$, $|CT_2|, ..., |CT_n|, ...$

Question 37. a) Find the width of the partially ordered set $\langle CT_n; \leq\rangle$.

b) Find maximal up — and down-valence of points in $\langle CT_n; \leq\rangle$.

Question 38. Is it true that all automorphisms of scales $\langle CT_n; \leq\rangle$ and $\langle ECT_n; \leq\rangle$ are trivial?

Partial results on these question are in [49], [50].

There concept of the fattiness of points from $\langle CT_n; \leq \rangle$ is connected to a natural map of the clone lattice on n-element set on the scale $\langle CT_n; \leq \rangle$ and was introduced in [51].

There following question appears in [51]

Question 39. a) Describe all values of fattiness of points from $\langle CT_n; \leq \rangle$.

b) For any number k which is the value of fattiness of a point from $\langle CT_n; \leq \rangle$ find a number of points from $\langle CT_n; \leq \rangle$ that have fattiness equal to k.

We denite as $Iso^*\mathcal{A}$ an enrichment of the semigroup Iso with one unary predicate which defines the idempotents of $Iso\mathcal{A}$ that correspond to oneelement subalgebras of algebra $\mathcal{A}$. Finite algebras $\mathcal{A}_1$ and $\mathcal{A}_2$ for which these enriched semigroups $Iso^*\mathcal{A}_1$ and $Iso^*\mathcal{A}_2$ are isomorphic, we define as similar. Similar algebras can be constructed in some standard way one from another (see, for example, [39]).

We consider the relation $\simeq$ on the scale $\langle CT_n; \leq \rangle : \mathcal{A}_1/\sim \simeq \mathcal{A}_2/\sim$ iff algebras $\mathcal{A}_1$ and $\mathcal{A}_2$ are similar.

In [48] there is

Question 40. a) Find the number $|CT_n/\simeq|$ and possible powers of classes from $CT_n/\simeq$.

b) Is the relation $\simeq$ definable in $\langle CT_n; \leq \rangle$ by some first order formula?

The point $\mathcal{A}/\sim$ from $\langle CT_n; \leq \rangle$ is defined as original point if there exists no algebra $\mathcal{B}$ similar to $\mathcal{A}$ and such that $|\mathcal{B}| < |\mathcal{A}|$.

In [48] there is

Question 41. Define the ratio of original points of scale $\langle CT_n; \leq \rangle$ relative to the power of set CT_n.

Algebra $\mathcal{A}$ is m-ar if aryty of its every signature operations is not bigger that m. Let $CT_n^m = \{\mathcal{A}/\sim | \mathcal{A}/\sim \in CT_n$ and $\mathcal{A}$ is m-ar$\}$. Than $CT_n^n = CT_n$. Most of the questions stated earlier for scale $\langle CT_n; \leq \rangle$ apply for scales $\langle CT_n^m; \leq \rangle$ with $m < n$ (For particular answers for scales $\langle CT_n^1; \leq \rangle$ see [48]). Among open questions for $\langle CT_n^m; \leq \rangle$ ($2 \leq m < n$, the answer is known for $m = 1, n$) is the question on the number of atoms and coatoms of scales $\langle CT_n^m; \leq \rangle$.

The algebra $\mathcal{A}$ is defined as superrigid if it has no nontrivial inner isomorphisms. We denote as $\alpha(n)$ the number of pairwise non conditionally rational equivalent superrigid unars. [52] has formulated the following question connected to the number of pairwise different representations of finite distributive lattices as the families of subsets of the finite sets.

Question 42. Find the assimptotic exponential estimate of the sequence $\alpha(1), \alpha(2), ..., \alpha(n), ...$.

The minimal number of generators of a finite algebra is invariant to

conditionally rational equivalence relation. Let $G_n(\mathcal{A}/\sim)$ denote the function which is defined on the set CT_n and which value is the minimal number of generators of algebra $\mathcal{A}$. The work [53] has formulated

Question 43. For any natural n find numbers $|G_n^{-1}(k)|$ of computability potentials of k-generated n-element algebras.

3. Partially ordered sets and graphs.

Let $J\mathcal{L}$ be the class of isomorphism types of all linear ordered sets. The work [54] has studied epimorphism $\langle J\mathcal{L}; \ll\rangle$ and embedding $\langle J\mathcal{L}; \ll\rangle$ skeletons of this class and has formulated

Question 44. a) Is it true that any (any countable) better quasiordered set is isomorphically embedded in $\langle J\mathcal{L}; \ll\rangle(\langle J\mathcal{L}_{\aleph 0}; \ll\rangle)$?

b) Which quasiordered sets are embedded in $\langle J\mathcal{L}; \ll\rangle$?

A series of work by the author has studied partially orders with unique (the biggest, the smallest) linear extensions relative to the isomorphical embedding relation. Work [55], [56] have formulated

Question 45. a) Describe, for the class of all partially orders of infinite width which contains no infinite sets of pairwise incomparable elements, those sets that have a unique (relative to isomorphical embedding relation) linear extension?

b) When countable almost linear partially orders have the biggest (relative to isomorphically embedding relation) linear extension?

Note that a partially ordered set is almost linear if it contains finite set of maximal (for inclusion) chains.

Let α be isomorphism type of some linear ordered set. Any linear extension $\langle A; \leq_1\rangle$ of partially ordered set $\langle A; \leq\rangle$ which is embedding in α is defined as α-realization of $\langle A; \leq\rangle$. A partially ordered set $\langle A; \leq\rangle$ have α-dimension if the order $\leq$ is an intersection of some α-realizations of the set $\langle A; \leq\rangle$. The existence of α-realization of the set $\langle A; \leq\rangle$ is a necessary condition for existence of α-dimension for $\langle A; \leq\rangle$. The question of description of linear orders α such that any partially ordered set which has α-realization also has α-dimension was formulated in [57]. Some special cases of this question were studied by V. Novak, the author and others. The work [58] has formulated the following question.

Question 46. Describe linear orders α such that any up-directed partially orders (any lattice) that have α-realization also hove α-dimension.

In [59] the well known concept of Rudin-Keisler order $\leq$ on the set of ultrafilters of Boolean algebra $\mathcal{P}(\lambda)$ (algebra of all subsets of the cardinal λ) was generalized to the order relation $\leq$ on ultrafilters of any complete Boolean algebra $\mathcal{B}$. We denote as $RK(\mathcal{B})$ partially ordered set of all ultrafilters of any complete Boolean algebra $\mathcal{B}$ with this order $\leq$. In [59] following open

questions were formulated.

Question 47. a) Describe complete Boolean algebras $\mathcal{B}, \mathcal{C}$ and their ultrafilters D, E for which the relation $D \leq E$ is equivalent to the existence of complete homomorphism φ of $\mathcal{B}$ in $\mathcal{C}$ such that $\varphi(D) \subseteq E$.

b)Is it true that ZFC implies the following statement: for any complete Boolean algebra $\mathcal{B}$ and for any infinite cardinal k the partially ordered set $RK(\mathcal{P}(\lambda))$ is isomorphicaly embedded in $RK(\mathcal{B}^k)$ for $\lambda \leq k$?

In [59] this statement was proven using the assumption of existence of k^+-complete ultrafilter.

We work [60] has defined concepts of programm movement and programm equivalence of multigraphs with colored edges on the base of conditionally termal functions of unars that correspond to this graphs.

This work [60] has formulated.

Question 48. a) Find the number of pairwise programm nonequivalent multiorgraphs of bounded degree with colored edges and n vertices (for any natural n).

b) The problem of minimization of the number of edges for multiorgraph G of bounded degree with the colored edges in the class of multiorgraphs that are programm equivalent to the graph G.

c) The problem of minimization of number of colors with restriction on the number of edges for multiorgraph G of bounded degree in the class of the multiorgraphs that are programm equivalent to the graph G.

References

1.K.Hartig. Uber einen Quantifikator mit zwei Wirkungsbereichen. — Colloq. on the foundations of mathemat., mathemat. machines and their appl., Akadem. Kiado, Budapest, 1962, p. 31-36.

2. H.Herre, M.Krynicki, A.Pinus, J.Vaananen. The Hartig Quantifier: A survey. — J.Symbol Logic, v. 56, 1991, №4, p. 1153-1183.

3. А.Г.Пинус. Мощность моделей теорий исчисления с квантором Хартига. — Сиб. матем. журнал, т. XIX, 1978, №6, с. 1349-1356.

4. А.Г.Пинус. Число Ханфа для исчисления с квантором Хартига. — Сиб.матем. журнал, т. XX, 1979, №2, с. 440-441.

5. A.Baudisch. The theory of abelian p-groups with the quantifier I is decidable. — Fund. Math., v. 108, 1980, №1, p. 183-197.

6. H.Herre, A.Pinus. Zum Entscheidungsproblem fur Theorien in Logiken mit monadischen verallegemeinerten Quantoren. — Zeitschr. fur Math. Logik und Grundlagend. Math., v. 2, 1978, №3, p. 375-384.

7. А.Г.Пинус. Исчисление с квантором автоморфности. — "Алгебраические системы, алгоритмические вопросы и ЭВМ". - Из-во ИрГУ, Иркутск, 1985, с. 102-120.

8. A.G.Pinus. Generalized Quantifiers in Algebra. — "Quantifiers: Logic, Models and Computation. v. II", Kluwer Acad. Publ., Dordrecht-Boston-London, 1955, p. 215-228.

9. A.Mostowski. On a generalization of quantifiers. — Fund. Math., v. 44, 1957, №1, p. 12-36.

10. А.Г.Пинус. Элиминируемость кванторов Q_0 и Q_1 на симметрческих группах. — Известия вузов. Математика, 1979, №12, с. 45-47.

11. А.Г.Пинус. Об элементарной эквивалентности топологических пространств. — Сиб. матем. журнал, т. XX, 1979, №2, с. 433-439.

12. А.Г.Пинус. Элементарные теории полугрупповых операций на классе линейных порядков. — Деп. в ВИНИТИ, №4161-82, с. 11

13. А.Г.Пинус. О квазипростых алгебрах. — Исследование алгебраических систем по свойствам их подсистем. - Из-во УрГУ, Свердлвск, 1987, с. 108-118.

14. D. Monk. On psendo-simple universal algebras. — Proc. Amer. Math. Soc, v. 13, 1962, p. 543-546.

15. А.Г.Пинус., И.Хайда. О квазипорядках на универсальных алгебрах. — Алгебра и логика, т. 32, 1993, №3, с. 308-325.

16. А.Г.Пинус. О решетках квазипорядков на универсальных алгебрах. — Алгебра и логика, т. 34, 1995, №3, с. 327-328.

17. I.Chajda, G.Czedli. Four notes on quasiorder lattices. — Math Slovaca, v. 46, 1996, №4, p. 371-378.

18. А.Г.Пинус. О естественных квазипорядках на алгебрах. — Универсальная алгебра и ее приложения. Из-во ВГУ, Волгоград, 2000, с. 238-249.

19. А.Г.Пинус. Внутренние гомоморфизмы и позитивно условные термы. — Алгебра и логика, т. 40, 2001, №2, с. 158-173.

20. Ю.М.Важенин, А.Г.Пинус. Элементарная классификация и разрешимость теорий производных структур. — Успехи матем. наук, т. 60, 2005, №3, с. 3-40.

21. А.Г.Пинус. Об элементарной эквивалентности производных структур свободных решеток. — Известия вузов. Математика, 2002, №5, с. 44-47.

22. А.Г.Пинус. О собственных автоморфизмах универсальных алгебр. — Сиб. матем. журнал, т. 45, 2004, №6, с. 1329-1337.

23. J. Sichler. Weak automorphisms of universal algebra. — Alg. univ., v. 3, 1973, №1, p. 1-7.

24. А.Г.Пинус. О подполурешетках формульных и открыто формульных конгруэнций решетки всех конгруэнций универсальных алгебр. — Сиб. матем. журнал, т. 47, 2006, №4, с. 865-872.

25. А.Г.Пинус. О полурешетках формульных подалгебр. — Алгебра и логика, т. 44, 2005, №4, с. 474-482.

26. A.G.Pinus. Boolean constructions in Universal Algebra. — Kluwer Acad. Publ., Dordrecht-Boston-London, 1993.

27. А.Г.Пинус. Булевы конструкции в универсальной алгебре. — Успехи матем. наук, т. 47, №4, с. 145-180.

28. А.Г.Пинус. К вопросу о покрытиях в скелетах эпиморфности многообразий. — Известия вузов. Математика, 1993, №1, с. 48-55.

29. A.G.Pinus. Elementary expressiveness in skeletons of the variety of Boolean algebras and Continuum-hypothesis.

30. A.G.Pinus. The countable skeletons of discriminator varieties. Results and problems. — "Ordered sets and Generalized Algebra", Olomouc, 1995, p. 100-105.

31. А.Г.Пинус. Об отношениях вложимости и эпиморфности на конгруэнц-дистрибутивных многообразиях. — Алгебра и логика, т. 24, 1985, №5, с. 588-607.

32. А.Г.Пинус. О декартовых скелетах конгруэнц-дистрибутивных многообразий. — Известия вузов. Математика, 1990, №6, с. 47-89.

33. J.Ketonen. The structure of countable boolean algebras. — Ann. Math., v. 118, 1978, №1, p. 41-89.

34. A.G.Pinus. Skeletons of congruence distributive varieties of algebras. — Alg. univ., v. 32, 1994, №3, p. 531-544.

35. А.Г.Пинус. Принцип Вопенки и скелеты многообразий. — Известия вузов. Математика, 1993, №3, с. 68-71.

36. А.Г.Пинус, Я.Л.Мордвинов. О скелетах многообразий решеток. — Алгебра и теория моделей 2, Новосибирск, Из-во НГТУ, 1999, с. 111-118.

37. A.G.Pinus. Skeletons of quasivarieties with the Fraser-Horn property. — Alg. univ., v. 46, 2001, №1, p. 7-13.

38. А.Г.Пинус. Условные термы и их применение в алгебре и теории вычислений. — Новосибирск, Из-во НГТУ, 2002

39. А.Г.Пинус. Условные термы и их применение в алгебре и теории вычислений. — Успехи матем. наук, т. 56, 2001, №4, с. 35-72.

40. А.Г.Пинус. n-элементарная вложимость и n-условные термы. — Известия вузов. Математика, 1999, №1, с. 36-40.

41. А.И.Мальцев. Структурная характеристика некоторых классов алгебр. — ДАН СССР, т. 120, 1958, №1, с. 29-32.

42. А.Г.Пинус. О диаграмме класов условно термальных функций. —

Фундаментальная и прикладная математика, т. 8, 2002, №4, с. 1099-1109.

43. А.Г.Пинус. О рационально и условно рационально эквивалентных алгебрах. — Алгебра и логика, т. 41, 2002, №3, с. 326-334.

44. A.G.Pinus. The positive and generalized discriminators don't exist. — Disscussiones Math. Ceneral Algebra and Applications, v. 20, 2000, p. 121-128.

45. А.Г.Пинус. Об условно рационально эквивалентных дискриминаторных многообразиях. — Известия вузов. Математика, 1999, №8, с. 54-59.

46. А.Г.Пинус. Об утверждениях типа теоремы Ловаша. — Алгебра и теория моделей 4, Новосибирск, Из-во НГТУ, 2003, с. 94-98.

47. А.Г.Пинус. Об алгебрах условно рационально эквивалентных полурешеткам и булевым алгебрам. — Сиб. матем. журнал, т. 39, 1998, №1, с. 121-128.

48. А.Г.Пинус, С.В.Журков. Шкалы потенциалов вычислимости конечных алгебр: результаты и проблемы. — Фундаментальная и прикладная математика, т. 9, 2003, №3, с. 145-164.

49. С.В.Журков, А.Г.Пинус. Об автоморфизмах шкал потенциалов вычислимости n-элементных алгебр. — Сиб. матем. журнал, т. 44, 2003, №3, с. 606-621.

50. А.Г.Пинус. Автоморфизмы, формульные отношения и покрытия элементов шкалы потенциалов вычислимости всех конечных алгебр. — в печати.

51. А.Г.Пинус. Слабые автоморфизмы и жирность точек шкал потенциалов вычислимости. — Математические вопросы кибернетики, т. 11, 2002, с. 15-26.

52. А.Г.Пинус. Представления дистрибутивных решеток подмножествами и оценка числа потенциалов вычислимости n-элементных сверхжестких унаров. — Вычислительные системы, т. 173, 2004, с. 32-39.

53. А.Г.Пинус. Порожденность конечных алгебр, базируемость их условно эквиациональных теорий и шкала потенциалов вычислимости n-элементных алгебр. — Алгебра и теория моделей 4, Из-во НГТУ, Новосибирск, 2003, с. 89-93.

54. .Г.Пинус. Об отношениях "вложимости"и "эпиморфности"на линейных порядках. — Упорядоченные множества и решетки. - Некоторые алгебраические приложения теории решеток, Из-во СГУ, Саратов, 1982, с. 81-90.

55. А.Г.Пинус. О единственности линейных продолжений частичных порядков. — Сиб. матем. журнал, т. 24, 1983, №4, с. 131-137.

56. А.Г.Пинус. О наибольших линейных продолжениях частичных

порядков. — Упорядоченные множества и решетки, Из-во СГУ, Саратов, 1986, с. 61-70.

57. H.Komm. On the dimension of partially ordered sets. — Amer. J. Math, v. 70, 1948, №4, p. 507-520.

58. А.Г.Пинус. О некоторых комбинаторных свойствах линейных порядков. — Депонированно в ВИНИТИ, №1223-81, с. 20.

59. P.Jipsen, A.Pinus, H.Rose. Rudin-Keisler Posets of Complete Boolean Algebras. — Math. Log. Quat., v. 47, 2001, №4, p. 447-454.

60. А.Г.Пинус. Программные перемещения на графах и програмная эквивалентность последних. — ДАН ВШ России, 2004, №1(2), с. 28-37.

ЖЁСТКИЕ ГРУППОВЫЕ КОЛЬЦА

К.Н. Пономарёв*

Новосибирский государственный технический университет,
Россия, 630092, Новосибирск, пр. К.Маркса 20
e-mail: algebra@nstu.ru

В выступлении на конференции Эрлогол-2007 профессор С.К.Росошек предложил новую криптосистему, основанную на использовании групповых колец. Ключевой при использовании этой системы оказалась следующая проблема.

Рассмотрим конечное коммутативное кольцо K, конечную группу G и групповое кольцо $KG = \{x = \sum\limits_{g\in G} a_g g \mid a_g \in K\}$. Назовём автоморфизм $\varphi : KG \to KG$ *стандартным* если он определяется некоторым автоморфизмом кольца $\alpha : K \to K$ и автоморфизмом группы $\sigma : G \to G$ так, что при любом $x = \sum\limits_{g\in G} a_g g$ имеем $x^\varphi = \sum\limits_{g\in G} a_g^\alpha g^\sigma$.

Проблема Росошека: при каких конечных коммутативных кольцах K и конечных группах G групповое кольцо KG имеет только стандартные автоморфизмы?

В духе общей концепции жёсткости (см. [1]) естественно групповые кольца KG, обладающие только стандартными автоморфизмами, называть *автоморфно жёсткими* и проблема состоит в определении автоморфно жёстких групповых колец.

Мы решаем эту проблему для групповых колец абелевых групп над конечными полями и доказываем следующее утверждение.

Теорема 1. *Пусть K – конечное поле характеристики p, а G – конечная абелева группа.*

Тогда групповое кольцо KG является автоморфно жёстким тогда и только тогда, когда

либо группа G является тривиальной, $G = 1$;

либо поле K простое поле характеристики p, G циклическая группа простого порядка q, при этом простые числа p и q различные и p служит первообразным корнем по модулю q.

*Работа выполнена при поддержке РФФИ грант N06-01-00159-а.

1 Группа автоморфизмов

Строгое решение проблемы требует определённого формализма в понятиях. Обозначим $AutKG, AutK, AutG$ – группы автоморфизмов группового кольца KG, коммутативного кольца K и группы G.

Определим естественные вложения групп автоморфизмов $AutK \to AutKG, AutG \to AutKG$. Они отвечают вложениям кольца K и группы G в групповое кольцо KG. Для произвольных $\alpha \in AutK$, $\sigma \in AutG$ и $f = \sum a_g g$ полагаем

$$f^\alpha = \sum a_g^\alpha g, f^\sigma = \sum a_g g^\sigma.$$

Будем использовать эти вложения и считать группы $AutK$ и $AutG$ подгруппами группы автоморфизмов группового кольца $AutKG$.

Замечание 1. *Поскольку групповое кольцо KG порождается подкольцом $K = K \cdot 1_G$ и подгруппой группы единиц $G = 1_K \cdot G$, то указанные подгруппы определяются такими условиями:*

$$AutK = \{\varphi \in AutKG |\ \varphi(K) = K,\ \varphi|_G = id_G\},$$

$$AutG = \{\varphi \in AutKG |\ \varphi|_K = id_K,\ \varphi(G) = G\}.$$

Отметим, что элементы этих подгрупп в полной группе автоморфизмов перестановочные, $[AutK, AutG] = 1$.

Произведение $AutK \cdot AutG$ в группе $AutKG$ образует подгруппу *стандартных автоморфизмов*. Таким образом, каждый стандартный автоморфизм φ определяется парой автоморфизмов $\alpha \in AutK$, $\sigma \in AutG$. Для произвольного $f = \sum a_g g$ он определяется формулой

$$f^{(\alpha,\ \sigma)} = \sum a_g^\alpha g^\sigma.$$

Формально проблема Росошека состоит в определении таких колец K и групп G для которых $AutKG = AutK \cdot AutG$. Основное техническое средство решения проблемы доставляет следующее утверждение.

Лемма 1. *Подгруппа стандартных автоморфизмов $AutK \cdot AutG$ группового кольца KG в полной группе его автоморфизмов $AutKG$ выделяется такими условиями:*

$$AutK \cdot AutG = \{\varphi \in AutKG |\ \varphi(K) = K,\ \varphi(G) = G\}.$$

В самом деле, включение $\subseteq$ следует из замечания 1. Установим обратное включение $AutK \cdot AutG \supseteq \{\varphi \in AutKG |\ \varphi(K) = K,\ \varphi(G) = G\}$.

Рассмотрим произвольный автоморфизм $\psi \in AutKG$ с условиями $\psi(K) = K,\ \psi(G) = G$. Определим $\alpha = \psi|_K \in AutK,\ \sigma = \psi|_G \in AutG$. Поскольку K и G порождают групповое кольцо KG, то эта пара автоморфизмов определяет такой стандартный автоморфизм φ, который совпадает с автоморфизмом ψ. Таким образом ψ – стандартный автоморфизм группового кольца. Лемма доказана.

2 Необходимость $(p, m) = 1$

Будем доказывать необходимость всех условий теоремы. Рассмотрим конечное поле K и конечную абелеву группу G для которых групповое кольцо KG является жёстким. Будем предполагать, что для простого числа p и натурального s имеем $|K| = p^s$, также $|G| = m$.

В этом разделе докажем от противного, что выполняется условие $(p, m) = 1$. Предположим $(p, m) \neq 1$ и покажем, что групповое кольцо KG имеет нестандартные автоморфизмы.

Из структуры абелевых групп следует, что в этом случае группа G имеет циклические прямые слагаемые периода степени простого числа p. Пусть скажем $G = G' \times C$ и циклическая группа C имеет период p^n. Тогда групповое кольцо изоморфно групповому кольцу $KG = (KG')C$. Обозначим $R = KG'$, тогда $KG = RC$, при этом кольцо R имеет характеристику кольца K, $chR = chK = p$.

Лемма 2. *Пусть R – кольцо характеристики p, C – циклическая группа периода p^n, а c – образующий этой группы.*

Тогда групповое кольцо RC имеет ненулевое дифференцирование $\theta : RC \to RC$ для которого $1 = \theta(c) \in R$.

Рассмотрим кольцо многочленов $R[X]$ и его стандартное дифференцирование $' : R[X] \to R[X]$ при котором $X' = 1$. Групповое кольцо RC изоморфно фактору кольца многочленов $RC = R[X]/(X^{p^n} - 1)$.

В кольце многочленов имеем $(X^{p^n} - 1)' = p^n X' = 0$. Заметим, что идеал $I = (X^{p^n} - 1)$ инвариантен относительно дифференцирования, $I' \subseteq I$, поскольку при любом $s \in R[X]$ имеем тождество

$$[s(X^{p^n} - 1)]' = s'(X^{p^n} - 1) + s \cdot 0 = s'(X^{p^n} - 1).$$

Поэтому отображение $'$ определяет требуемое дифференцирование θ фактор-кольца $R[X]/I$ и группового кольца RC. Лемма доказана.

Заметим, что элемент $\varepsilon = 1 + c + c^2 + \ldots + c^{p^m-1} \in RC$ нильпотентный, выполняется $\varepsilon^2 = 0$. Несложно проверить, что отображение $\psi : RC \to RC$, определённое формулой $x \to x + \theta(x)\varepsilon$, служит автоморфизмом кольца $KG = RC$. Этот автоморфизм в силу леммы 1 не является стандартным поскольку выполнено неравенство $\psi(c) = c + \varepsilon \notin G$. Получили противоречие. Необходимость условия $(p, m) = 1$ доказана.

Из этого раздела следует, что в силу теоремы Машке жесткое групповое кольцо KG является полупростым, оно разлагается в прямую сумму полей (см. [2]). Будем этим пользоваться далее.

3 Необходимость цикличности группы G

Вначале отметим вариант хорошо известной для областей главных идеалов "китайской теоремы об остатках".

Пусть R произвольное коммутативное кольцо (не обязательно область целостности), а $f, g \in R$. Эти элементы будем называть *взаимно простыми* и обозначать $(f, g) = 1$ если $fR + gR = R$. Это равносильно совместности диофантова уравнения $fx + gy = 1$ в кольце R. Очевидно, что свойство взаимной простоты элементов кольца сохраняется при его гомоморфизмах на другие коммутативные кольца.

Лемма 3. *Рассмотрим коммутативное кольцо R и взаимно-простые элементы этого кольца $f, g \in R$, $(f, g) = 1$. Тогда фактор-кольцо $R/(fg)$ изоморфно прямой сумме колец $R/(fg) = R/(f) \dot{+} R/(g)$.*

Действительно, в условиях леммы рассмотрим естественные проекции, эпиморфизмы $\pi : R/(fg) \to R/(f)$ и $\sigma : R/(fg) \to R/(g)$.

Сумма проекций определяет гомоморфизм на прямое произведение – на прямую сумму $\pi \times \sigma : R/(fg) \to R/(f) \dot{+} R/(g)$. Ядро этого гомоморфмзма совпадает с пересечением $(f) \cap (g)$. Докажем, что в силу взаимной простоты f и g имеем $(f) \cap (g) = (fg)$.

В самом деле, включение $(f) \cap (g) \supseteq (fg)$ очевидно. Проверим обратное включение $(f) \cap (g) \subseteq (fg)$. Используем взаимную простоту и определим такие $r, s \in R$, которые удовлетворяют уравнению $fr + gs = 1$.

Рассмотрим произвольный элемент $z \in (f) \cap (g)$ и представим его в виде произведений $z = fx = gy$ для некоторых x, y из кольца R. Из уравнения выше выводим равенство $fxr + gxs = x$. Отсюда $gyr + gxs + x$. Заключаем, что $x \in (g)$ и $z \in (fg)$. Таким образом выполенено обратное включение и в самом деле $(f) \cap (g) = (fg)$.

Заключаем, что ядро гомоморфизма $\pi \times \sigma$ нулевое, а его образ содержит компоненты прямой суммы. Таким образом этот гомоморфизм является изоморфизмом. Лемма доказана.

По индукции утверждение леммы 3 легко обобщается на случай любого числа попарно взаимно простых элементов. Будем использовать утверждение этой леммы в таком расширенном смысле и применять его к кольцу полиномов $R[X]$ от переменной X с коэффициентами из произвольного коммутативного кольца R. Сформулируем это следствие в явном виде.

Лемма 4. *Рассмотрим произвольное коммутативное кольцо R и унитарные попарно взаимно простые полиномы $f_1, \ldots, f_n$ из кольца полиномов $R[X]$. Тогда фактор-кольцо $R[X]/(f_1 \ldots f_n)$ изоморфно прямой сумме фактор-колец $R[X]/(f_1) \dot{+} \ldots \dot{+} R[X]/(f_n)$.*

Далее будем рассматривать кольца полиномов $R[X]$ над полупростыми коммутативными кольцами R – конечными прямыми суммами полей $R = F_1 \dot{+} \ldots \dot{+} F_n$. Такие кольца не образуют области целостности, однако это – конечные прямые суммы областей главных идеалов, колец полиномов $F_i[X]$ над полями F_i. Обозначим проекции на компоненты $\pi_i : R \to F_i$.

Выполняется алгоритм деления с остатком на унитарные полиномы, поэтому справедливо утверждение теоремы Безу. Таким образом, степень полинома $f(X) \in R[X]$ не превосходит числа его корней $a_1, \ldots, a_m$, различающихся в каждой компоненте, т.е. $\pi_i(a_j) \neq \pi_i(a_k)$ $i = 1, ..., n$.

Лемма 5. *Рассмотрим полупростое коммутативное кольцо R, простое число p взаимно простое с характеристикой кольца и натуральное число n. Предположим, что каждая компонента R содержит первообразный корень из единицы степени p^n.*

Тогда фактор-кольцо $R[X]/(X^{p^n}-1)$ разлагается в конечную прямую сумму колец изоморфных кольцу R: $R[X]/(X^{p^n} - 1) = R \dot{+} \ldots \dot{+} R$ с числом слагаемых p^n. При этом само кольцо R вложено в прямую сумму диагональным образом.

Утверждение следует из леммы 4 и замечаний выше.

Предположим, что групповое кольцо KG является жёстким. Докажем, что абелева группа G циклическая.

Рассмотрим разложение группы в прямое произведение примарных компонент: $G = G_{p_1} \times \ldots \times G_{p_m}$ в котором простые числа p_i различные

и каждая группа G_{p_i} имеет порядок равный степени простого числа p_i. Достаточно доказать, что каждая группа G_{p_i} является циклической. Тогда циклической будет и сама группа G.

Будем рассуждать от противного и предположим, что некоторая примарная компонента разлагается в произведение циклических групп $G_{p_i} = H_1 \times \ldots \times H_k,\ k > 1$. Обозначим через r_j порядок циклической группы H_j. Будем считать число r_k наименьшим. Обозначим $H = H_1 \times \ldots \times H_{k-1}$, тогда $G_{p_i} = H \times H_k$ и $G = G' \times H_k$, где $G' = G_{p_1} \times \ldots \times G_{p_{i-1}} \times H \times G_{p_{i+1}} \times \ldots \times G_{p_m}$.

Группа H, а вместе с ней и группа G' содержит элемент c порядка p^{r_k}. Обозначим $R = KG'$, тогда имеем изоморфизмы групповых колец $KG = (KG')H_k = RH_k$. Полупростое кольцо R в каждой компоненте содержит c – первообразный корень из единицы степени p^k. По лемме 5 имеем разложение группового кольца в прямую сумму p^k слагаемых: $RH_k = R[X]/(X^{p^k} - 1) = R \dot{+} \ldots \dot{+} R$. Значит, имеется $p^k!$ автоморфизмов этого кольца, переставляющих эти слагаемые и неподвижных на диагонали, на кольце R. Однако группа H_k имеет только $\phi(p^k) = p^{k-1}(p-1) < p^k!$ автоморфизмов. В силу леммы 1 групповое кольцо KG имеет нестандартные автоморфизмы, оно не является жёстким. Противоречие.

Необходимость цикличности группы G доказана.

4 Необходимость первообразности p^s по модулю m

Нам следует проверить, что если конечное поле K имеет p^s элементов, а групповое кольцо KG жёсткое, то число p^s является первообразным корнем по модулю порядка группы $m = |G|$. Будем предполагать жёсткость кольца KG. Нам уже известно, что $(p, m) = 1$, а группа G циклическая.

Групповое кольцо KG изоморфно фактор-кольцу кольца полиномов $KG = K[X]/(X^m - 1)$. Автоморфизмы группы G определяются по действию $X \to X^t$, в котором $t \in N, (t, m) = 1$. Таким образом, число автоморфизмов группы определяется по функции Эйлера, $|aut(G)| = \phi(m)$.

Напомним (см. [3]), что полином $X^m - 1$ над кольцом целых чисел разлагается в произведение круговых полиномов:

$$X^m - 1 = \Phi_1(X) \ldots \Phi_m(X) = \prod_{d|m} \Phi_d(X).$$

Все круговые полиномы неприводимы над полем рациональных чисел. Первообразные корни степени m над полем рациональных чисел – корни кругового полинома $\Phi_m(X)$. Над другими полями круговые полиномы могут разлагаться на множители, тогда первообразные корни служат корнями сомножителей круговых полиномов.

Утверждение следующей леммы хорошо известно. Доказательство приводим только для полноты изложения.

Лемма 6. *Пусть K поле в котором p^s элементов, а ζ_m первообразный корень степени m над полем K. Тогда степень расширения полей $K(\zeta_m)/K$ равна показателю числа p^s по модулю m, $|K(\zeta_m) : K| = P_m(p^s)$.*

В частности, такая степень максимальная $|K(\zeta_m) : K| = \phi(m)$ тогда и только тогда, когда p^s – первообразный корень по модулю m.

Действительно, рассмотрим расширение поля L/K, оно является конечным полем характеристики p. Значит, $|L| = p^t$. Поскольку это – расширение поля K. то t делится на s и $|L : K| = t/s$.

Мультипликативная группа поля L циклическая порядка $p^t - 1$. Поэтому она включает первообразный корень степени m только и только если $p^t - 1$ делится на m. Отсюда следует, что $L = K(\zeta_m)$ тогда и только тогда, когда $t = P_m(p^s)$. Заключительное утверждение леммы очевидно. Лемма доказана.

Отметим, что заключение леммы образует критерий неприводимости кругового полинома $\Phi_m(X)$ над конечным полем $\mathbb{F}_{p^s}$. Он состоит в том, что $\Phi_m(X)$ неприводим тогда и только тогда, когда p^s – первообразный корень по модулю числа m.

Поле $K(\zeta_m)$ принято называть *круговым полем* степени m над полем K.

Докажем, что p^s первообразный корень от противного. Предположим, что это не так и придём к противоречию с жёсткостью группового кольца KG. Используем известное строение круговых полей из монографии [4] (теорема 2.47).

По заключительному утверждению леммы заключаем, что $|K(\zeta_m) : K| < \phi(m)$. Значит, круговой полином $\Phi_m(X)$ степени $\phi(m)$ над полем K разлагается на множители: $\Phi_m(X) = G_1(X) \dots G_n(X)$, $n \geqslant 2$. Обозначим $L = K(\zeta_m)$ круговое поле, оно является полем разложения любого многочлена $G_i(X)$ над полем K. По лемме 4 из разложения кругового полинома выводим разложение группового кольца KG в прямую сумму

$KG = K[X]/(X^m - 1) = K[X]/\Phi_1(X) \dot{+} \ldots \dot{+} K[X]/\Phi_m(X) = K \dot{+} \ldots \dot{+} L \dot{+} \ldots \dot{+} L$. В последнем слагаемом $R = L \dot{+} \ldots \dot{+} L$ круговое поле L присутствует n раз.

Круговое поле L имеет $\phi(m)/n$ автоморфизмов неподвижных на поле K. Поэтому кольцо R имеет не менее $(\frac{\phi(m)}{n})^n n!$ автоморфизмов, неподвижных на поле K. Так как $n > 1$, то выполняется неравенство

$$(\frac{\phi(m)}{n})^n n! \geqslant \phi(m)(n-1)!.$$

Вначале рассмотрим случай $n > 2$, тогда $\phi(m)(n-1)! > \phi(m)$ и выполнено строгое неравенство

$$(\frac{\phi(m)}{n})^n n! > \phi(m).$$

Поскольку число стандартных автоморфизмов неподвижных на поле K совпадает с числом $\phi(m)$ автоморфизмов циклической группы G заключаем, что среди автоморфизмов KG есть нестандартные. Это противоречит жёсткости кольца KG.

Предположим теперь, что $n = 2$. Тогда если $\phi(m) > 2$, то также выполняется

$$(\frac{\phi(m)}{n})^n n! > \phi(m)(n-1)! = \phi(m).$$

Доказательство завершается аналогичным рассуждением.

Осталось рассмотреть случай когда $n = \phi(m) = 2$. Такое возможно только для чисел $m = 3,\ 4$ или $m = 6$. В этом случае круговой полином $\Phi_m(X)$ имеет степень $\phi(m) = 2$. Значит, он разлагается на линейные множители. Поэтому, в прямом разложении группового кольца KG указанном выше трижды присутствует основное поле: $KG = K \dot{+} K \dot{+} K \dot{+} \ldots$. Поэтому групповое кольцо имеет не менее $3! = 6 > 2 = \phi(m)$ автоморфизмов, переставляющих эти три слагаемых и неподвижных на поле K. Также имеем нестандартные автоморфизмы и получаем противоречие жёсткости кольца KG.

5 Необходимость простоты поля K и группы G

Рассмотрим конечное поле K с числом элементов p^s. Рассмотрим циклическую группу G порядка m, причём $(m, p) = 1$. Предположим, что p^s – первообразный корень по модулю m. Предполагаем жёсткость группового кольца KG.

Лемма 7. *Пусть целое число q представляет первообразный корень по модулю натурального числа m. Тогда для любого делителя d, $d|m$ число q будет первообразным корнем и по модулю d.*

Здесь нужно разобраться с определением первообразного корня в алгебраических терминах. По определению первообразный корень – порождающий элемент группы обратимых элементов кольца вычетов $\mathbb{Z}/m\mathbb{Z}$. Такие элементы имеются в том и только том случае, когда группа обратимых элементов циклическая.

По условию леммы группа обратимых элементов $(\mathbb{Z}/m\mathbb{Z})^*$ циклическая и число q определяет порождающий элемент этой группы.

Рассмотрим естественный эпиморфизм колец вычетов $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ ядро которого образовано классами вычетов $d\mathbb{Z}/m\mathbb{Z}$. Этот эпиморфизм определяет эпиморфизм групп обратимых элементов колец $(\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/d\mathbb{Z})^*$. Поэтому группа $(\mathbb{Z}/d\mathbb{Z})^*$ циклическая и порождается образом порождающего группы $(\mathbb{Z}/m\mathbb{Z})^*$. Поэтому то же самое число q определяет порождающий и группы $(\mathbb{Z}/d\mathbb{Z})^*$. Лемма доказана.

Из этой леммы следует, что если p^s первообразный корень по модулю m, то над полем $K = \mathbb{F}_{p^s}$ все круговые полиномы $\Phi_d(X),\ d|m$, являются неприводимыми. Поэтому групповое кольцо разлагается в прямую сумму круговых полей

$$KG = K[X]/(X^m - 1) = K_1 \dot{+} \ldots \dot{+} K_d \dot{+} \ldots \dot{+} K_m,$$

в которой числа d пробегают делители числа m, а поле K_d обозначает круговое поле, поле разложения кругового полинома $\Phi_d(X)$. Основное поле K вложено в эту сумму диагональным образом.

Заметим, что $K = K_1$ и круговые поля в указанном разложении образуют решётку всех промежуточных полей расширения K_m/K.

По лемме 1 в силу жёсткости автоморфизмы группового кольца RG переводят элементы поля K в элементы поля K. Поэтому, если выбрать набор произвольных автоморфизмов полей

$$\alpha_1 : K_1 \to K_1, \ldots, \alpha_d : K_d \to K_d, \ldots, \alpha_m : k_m \to K_m,$$

то составной автоморфизм группового кольца $\alpha_1 \times \ldots \times \alpha_m$ должен переводить диагональные элементы из поля K в диагональные элементы этого поля. Иными словами, ограничение действия любых автоморфизмов полей K_d– расширений поля K– на поле K определяет один и тот

же автоморфизм поля K. Если $m \neq 1$, то $K_m \neq K$ и все автоморфизмы поля K_m оказываются неподвижными на поле K.

Значит, либо $m = 1$, группа тривиальна $G = 1$ и первое утверждение теоремы выполняется, либо поле K является простым. В первом случае доказательство теоремы завершается. Поэтому далее будем предполагать, что поле K простое $K = \mathbb{F}_p$ и докажем, что группа G простая, т.е. её порядок $m = q$ – простое число.

Из структуры группового кольца KG вытекает строение группы его обратимых элементов. Имеем разложение в прямое произведение

$$(KG)^* = K_1^* \times \ldots \times K_d^* \times \ldots \times K_m^*$$

в котором каждая группа K_d^* циклическая. Также эти группы образуют решётку всех мультипликативных групп промежуточных полей расширения K_m/K.

По построению циклическая группа G вкладывается в это произведение следующим образом. Пусть g – образующая группы G. Тогда образ (проекция вложения) этого элемента в круговое поле $K_d,\ d|m$, образует первообразный корень ζ_d степени d. Произвольный элемент группы $h \in G$ представляется степенью $h = g^n$ и его проекцией в поле K_d служит элемент ζ_d^n. Таким образом, проекции элемента группы G в любом круговом поле $K_d,\ d|m$, вполне определяется по его значению в максимальном круговом поле K_m.

Поскольку групповое кольцо $KG = \mathbb{F}_pG$ жёсткое, то по лемме 1 автоморфизмы этого кольца должны переводить элементы группы G в элементы этой же группы. Покажем, что это выполняется только если число m является простым.

Будем рассуждать от противного и предположим, что число m составное. Пусть $d|m,\ d \neq 1,\ d \neq m$. Тогда круговое поле K_d не является простым, оно имеет нетривиальные автоморфизмы. Однако, по замечанию выше все автоморфизмы поля K_d должны оставлять на месте некоторый первообразный элемент $\zeta_d \in K_d$, значит имеется только тривиальный автоморфизм этого поля. Противоречие. Таким образом $m = q$ – простое число.

Доказательство необходимости всех условий завершено.

6 Достаточность условий

Предположим, что выполняются все условия теоремы. Если группа G тривиальная, $G = 1$, то доказывать нечего, $KG = K$ и все автомор-

физмы группового кольца есть автоморфизмы поля K, тривиальным образом они являются стандартными. Будем далее предполагать, что поле K является простым, $K = \mathbb{F}_p$, группа G является циклической группой простого порядка q, при этом число p является первообразным корнем по модулю q.

В предыдущем разделе было показано, что при этих условиях имеется разложение группового кольца в прямую сумму $KG = \mathbb{F}_p G = \mathbb{F}_p \dot{+} K_q$. Группа G представляется группой первообразных корней кругового поля K_q

В силу однозначности такого разложения произвольный автоморфизм такого кольца $\alpha \in aut(KG)$ состоит в действии на втором слагаемом некоторого автоморфизма α_q кругового поля $K_q = \mathbb{F}_p[\zeta_q]$, $\alpha = id_K \times \alpha_q$. Такие автоморфизмы переставляют группу первообразных корней – элементы группы G. Они являются стандартными. Доказательство достаточности завершено.

Список литературы

[1] К.Н.Пономарёв. Жёсткие алгебры и неассоциативные кольца. Новосибирск, изд-во НГТУ, 2007.

[2] М.Атья, И.Макдональд. Введение в коммутативную алгебру. М., Мир, 1972.

[3] С.Ленг. Алгебра. М., Мир, 1968.

[4] Р.Лидл, Г.Нидеррайтер. Конечные поля. Том 1. М., Мир, 1988.

ГРУППА АВТОМОРФИЗМОВ КОЛЬЦА ZS_3

А.М. Попова

Кафедра алгебры и математической логики Новосибирский государственный
технический университет
проспект К. Маркса, 20
Новосибирск, Россия
e-mail: algebra@nstu.ru

Рассматривается группа автоморфизмов целочисленного группового кольца симметрической группы S_3, доказывается, что она совпадает с группой внутренних автоморфизмов этого кольца. В работе используется матричное представление группы $D(S_3)$ (см. [1]). Из этого представления легко получаем клеточно - диагональное представление для ZS_3:

$$ZS_3 \cong ZD(S_3) = \left\{ e = \begin{pmatrix} 1 & & \\ & 1 & \\ & & \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix} \end{pmatrix}, a = \begin{pmatrix} 0 & & \\ & -2 & \\ & & \begin{matrix} 0 & 0 \\ -1 & 1 \end{matrix} \end{pmatrix}, \right.$$

$$e_1 = \begin{pmatrix} 0 & & \\ & 0 & \\ & & \begin{matrix} -1 & 1 \\ -1 & 1 \end{matrix} \end{pmatrix}, e_2 = \begin{pmatrix} 0 & & \\ & 0 & \\ & & \begin{matrix} 0 & -3 \\ 0 & 0 \end{matrix} \end{pmatrix},$$

$$\left. e_1e_2 = \begin{pmatrix} 0 & & \\ & 0 & \\ & & \begin{matrix} 0 & 3 \\ 0 & 3 \end{matrix} \end{pmatrix}, e_2e_1 = \begin{pmatrix} 0 & & \\ & 0 & \\ & & \begin{matrix} 3 & -3 \\ 0 & 0 \end{matrix} \end{pmatrix} \right\}_Z$$

Понятно, что любой автоморфизм $\varphi \in AutZS_3$ на первых двух одномерных клетках является тождественным, поэтому вначале изучим действие автоморфизма φ на двумерных клетках элементов матричного кольца $ZD(S_3)$, т.е. на подкольце.

$$K = \{e_1, e_2, e_1e_2, e_2e_1\}_Z.$$

Лемма 1. Пусть $X, Y \in K$ удовлетворяют условиям

$$X^2 = Y^2 = 0, XY + YX = 3E \tag{1}$$

Тогда отображение $\varphi(e_1) = X, \varphi(e_2) = Y, \varphi(e_1e_2) = XY, \varphi(e_2e_1) = YX, \varphi(\alpha_1e_1+\alpha_2e_2+\alpha_3e_1e_2+\alpha_4e_2e_1) = \alpha_1X+\alpha_2Y+\alpha_3XY+\alpha_4YX$ является автоморфизмом подкольца K.

Для любых элементов $u, v \in K$ равенство $\varphi(u \cdot v) = \varphi(u)\varphi(v)$ доказывается простым вычислением. Чтобы доказать, что φ — автоморфизм, достаточно заметить линейную независимость X, Y, XY, YX. Пусть, напротив,

$$\alpha_1X + \alpha_2Y + \alpha_3XY + \alpha_4YX = 0 \tag{2}$$

Из (1) легко получаем, что $XYX = 3X, YXY = 3Y, XYXY = 3XY$, $YXYX = 3YX$. Теперь домножая (2) слева на X а справа на Y, получаем $3\alpha_4XY = 0$, откуда $\alpha_4 = 0$. Аналогично, $\alpha_3 = 0$, т.е. $\alpha_1X + \alpha_2Y = 0$, откуда домножением на X получаем $\alpha_2 = 0$, и, аналогично, $\alpha_1 = 0$. Тем самым лемма доказана.

Пусть теперь

$X = \alpha_1e_1 + \alpha_2e_2 + \alpha_3e_1e_2 + \alpha_4e_2e_1$

$Y = \beta_1e_1 + \beta_2e_2 + \beta_3e_1e_2 + \beta + 4e_2e_1$

Из условий (1) леммы 1 получаем

$$\alpha_3 + \alpha_4 = 0, \beta_3 + \beta_4 = 0$$

$$\alpha_1\alpha_2 + 3\alpha_4^2 = 0 \tag{3}$$

$$\beta_1\beta_2 + 3\beta_4^2 = 0$$

$$\alpha_1\beta_2 + \alpha_2\beta_1 + 6\alpha_4\beta_4 = 1$$

Возникают только три возможных случая

1) $\alpha_2 = 0, \beta_2 \neq 0 \Longrightarrow \alpha_4 = 0, \alpha_1\beta_2 = 1, \beta_1 = \pm 3\beta_4^2$

2)$\alpha_2 \neq 0, \beta_2 = 0 \Longrightarrow \beta_4 = 0, \alpha_2\beta_1 = 1, \alpha_1 = \pm 3\alpha_4^2$

3) $\alpha_2 \neq 0, \beta_2 \neq 0$.

Рассмотрим матрицы автоморфизма φ для всех трех случаев

$$1)[\varphi] = \begin{pmatrix} \alpha_1 & \pm 3\beta_4^2 & 3\alpha_1\beta_4 & -3\alpha_1\beta_4 \\ 0 & \beta_2 & 0 & 0 \\ 0 & -\beta_4 & 1 & 0 \\ 0 & \beta_4 & 0 & 1 \end{pmatrix}$$

$$2)[\varphi] = \begin{pmatrix} \pm 3\alpha_4^2 & \beta_1 & -3\alpha_4\beta_1 & 3\alpha_4\beta_1 \\ \alpha_2 & 0 & 0 & 0 \\ -\alpha_4 & 0 & 0 & 1 \\ \alpha_4 & 0 & 1 & 0 \end{pmatrix}$$

$$3)[\varphi] = \begin{pmatrix} \alpha_1 & \beta_1 & 3\alpha_1\beta_4 - 3\alpha_4\beta_1 & 3\alpha_4\beta_1 - 3\alpha_1\beta_4 \\ \alpha_2 & \beta_2 & -3\alpha_2\beta_4 + 3\alpha_4\beta_2 & 3\alpha_2\beta_4 - 3\alpha_4\beta_2 \\ -\alpha_4 & -\beta_4 & \alpha_1\beta_2 + 3\alpha_4\beta_4 & \alpha_2\beta_1 + 3\alpha_4\beta_4 \\ \alpha_4 & \beta_4 & \alpha_2\beta_1 + 3\alpha_4\beta_4 & \alpha_1\beta_2 + 3\alpha_4\beta_4 \end{pmatrix}$$

Из случая 2) при $\alpha_2 = \beta_1 = 1, \alpha_4 = 0$ получаем матрицу

$$S = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Понятно, что произвольная матрица из 2) получается умножением матрицы из 1) на матрицу S справа. Поэтому рассмотрим матрицы, которые получаются в случаях 1) и 3).

1) $\alpha_2 = 0, \beta_2 \neq 0, \alpha_4 = 0, \alpha_1\beta_2 = 1, \beta_1 = \pm 3\beta_4^2$

Если $\alpha_1 = \beta_2 = 1, \beta_1 = -3\beta_4^2$, то получаем матрицу

$$a = \begin{pmatrix} 1 & -3\beta_4 & 3\beta_4 & -3\beta_4 \\ 0 & 1 & 0 & 0 \\ 0 & -\beta_4 & 1 & 0 \\ 0 & \beta_4 & 0 & 1 \end{pmatrix},$$

которая при $\beta_4 = 1$ дает единичную.

Если $\alpha_1 = \beta_2 = -1, \beta_1 = 3\beta_4^2$, то получаем матрицу

$$\widetilde{a} = \begin{pmatrix} -1 & 3\beta_4^2 & -3\beta_4 & 3\beta_4 \\ 0 & -1 & 0 & 0 \\ 0 & -\beta_4 & 1 & 0 \\ 0 & \beta_4 & 0 & 1 \end{pmatrix},$$

которая при $\beta_4 = 0$ дает матрицу

$$a_1 = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Понятно, что $\widetilde{a} = a_1 \cdot a$

Введем в рассмотрение матрицы

$$A = \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 3 & -3 \\ 0 & 0 \end{pmatrix}, C = \begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix}, a_2 = \begin{pmatrix} A & B \\ C & E \end{pmatrix}$$

Несложно доказать индукцией по β_4, что $a = a_2^{\beta_4}$ при $\beta_4 \geq 1$. Если $\beta_4 < 0$, то очевидно $a^{-1} = a_1 a a_1$. Получили, что матрицы $[\varphi]$ из случаев 1) и 2) получаются как слова от матриц a_1, a_2, S.

3) Пусть теперь $A' = \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix}, B' = \begin{pmatrix} 0 & 0 \\ -3 & 3 \end{pmatrix}, C' = \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix}$.

Тогда из случая 3) при $\alpha_1 = 1, \alpha_2 = -3, \alpha_4 = 1, \beta_1 = 0, \beta_2 = 1, \beta_4 = 0$ получаем матрицу $a_3 = \begin{pmatrix} A' & B' \\ C' & E \end{pmatrix}$.

Из системы равенств (3) следует, что $(\alpha_1, \alpha_2, \alpha_4) = 1$, причем только одно из чисел α_1 или α_2 делится на 3.

Если $\alpha_1 \vdots 3$, то $\alpha_1 = \pm 3\alpha_1'^2, \alpha_2 = \pm \alpha_2'^2, \alpha_4 = \alpha_1'\alpha_2'$.

Если $\alpha_2 \vdots 3$, то $\alpha_1 = \pm \alpha_1'^2, \alpha_2 = \pm 3\alpha_2'^2, \alpha_4 = \alpha_1'\alpha_2'$. Аналогично для $\beta_1, \beta_2, \beta_4$. Если эти равенства подставить в последнее равенство из (3), то получим

$$(\alpha_1'\beta_2' + 3\alpha_2'\beta_1')^2 = 1 \text{ либо } (3\alpha_1'\beta_2' + \alpha_2'\beta_1')^2 = 1$$

Отсюда следует, что $\alpha_1'\alpha_2'\beta_1'\beta_2' < 0$, т.е. $\alpha_4\beta_4 < 0$, поэтому при $\alpha_4 = -\alpha_1'\alpha_2'$ с необходимостью $\beta_4 = -\beta_1'\beta_2'$ и все сводится к сопряжению матрицей a_1, т.е. рассматривать случай $\alpha_4 = -\alpha_1'\alpha_2'$ не нужно. После этих замечаний понятно, что 3) распадается на 4 случая:

а) $\alpha_1 = \alpha_1'^2, \alpha_2 = -3\alpha_2'^2, \alpha_4 = \alpha_1'\alpha_2'$,
$\beta_1 = -3\beta_1'^2, \beta_2 = \beta_2'^2, \beta_4 = \beta_1'\beta_2'$;

б) $\alpha_1 = -\alpha_1'^2, \alpha_2 = 3\alpha_2'^2, \alpha_4 = \alpha_1'\alpha_2'$,
$\beta_1 = 3\beta_1'^2, \beta_2 = -\beta_2'^2, \beta_4 = \beta_1'\beta_2'$;

в) $\alpha_1 = 3\alpha_1'^2, \alpha_2 = -\alpha_2'^2, \alpha_4 = \alpha_1'\alpha_2'$,
$\beta_1 = 3\beta_1'^2, \beta_2 = -\beta_2'^2, \beta_4 = \beta_1'\beta_2'$;

г) $\alpha_1 = -3\alpha_1'^2, \alpha_2 = \alpha_2'^2, \alpha_4 = \alpha_1'\alpha_2'$,
$\beta_1 = \beta_1'^2, \beta_2 = -3\beta_2'^2, \beta_4 = \beta_1'\beta_2'$.

Рассмотрим матрицы $[\varphi]$ из случая 3) при различных вариантах а) — г).

а) при условии $\alpha_1'\beta_2' + 3\alpha_2'\beta_1' = 1$ получаем матрицу

$$[\varphi] = \begin{pmatrix} \alpha_1'^2 & -3\beta_1'^2 & 3\alpha_1'\beta_1' & -3\alpha_1'\beta_1' \\ -3\alpha_2'^2 & \beta_2'^2 & 3\alpha_2'\beta_2' & -3\alpha_2'\beta_2' \\ -\alpha_1'\alpha_2' & -\beta_1'\beta_2' & \alpha_1'\beta_2' & 3\alpha_2'\beta_1' \\ \alpha_1'\alpha_2' & \beta_1'\beta_2' & 3\alpha_2'\beta_1' & \alpha_1'\beta_2' \end{pmatrix}$$

Такая матрица получается как слово от матриц a_2 и a_3. Это проверяется компьютерными вычислениями.

Если $\alpha_1'\beta_2' + 3\alpha_2'\beta_1' = -1$, то получаем $[\varphi] \cdot a_1$.

б)

$$\begin{pmatrix} -\alpha_1'^2 & 3\beta_1'^2 & -3\alpha_1'\beta_1' & 3\alpha_1'\beta_1' \\ 3\alpha_1'^2 & -\beta_2'^2 & -3\alpha_2'\beta_2' & 3\alpha_2'\beta_2' \\ -\alpha_1'\alpha_2' & -\beta_1'\beta_2' & \alpha_1'\beta_2' & 3\alpha_2'\beta_1' \\ \alpha_1'\alpha_2' & \beta_1'\beta_2' & 3\alpha_2'\beta_1' & \alpha_1'\beta_2' \end{pmatrix} = a_1 \cdot [\varphi]$$

Если $\alpha_1'\beta_2' + 3\alpha_2'\beta_1' = -1$, то получаем $a_1[\varphi](-a_1)$.

в)

$$\begin{pmatrix} 3\alpha_1'^2 & -\beta_1'^2 & 3\alpha_1'\beta_1' & -3\alpha_1'\beta_1' \\ -\alpha_2'^2 & 3\beta_2'^2 & 3\alpha_2'\beta_2' & -3\alpha_2'\beta_2' \\ -\alpha_1'\alpha_2' & -\beta_1'\beta_2' & 3\alpha_1'\beta_2' & \alpha_2'\beta_1' \\ \alpha_1'\alpha_2' & \beta_1'\beta_2' & \alpha_2'\beta_1' & 3\alpha_1'\beta_2' \end{pmatrix} = a_1[\varphi]S$$

Если $3\alpha_1'\beta_2' + \alpha_2'\beta_1' = -1$, получаем $a_1[\varphi]S(-a_1)$.

г)

$$\begin{pmatrix} -3\alpha_1'^2 & \beta_1'^2 & -3\alpha_1'\beta_1' & 3\alpha_1'\beta_1' \\ \alpha_2'^2 & -3\beta_2'^2 & -3\alpha_2'\beta_2' & 3\alpha_2'\beta_2' \\ -\alpha_1'\alpha_2' & -\beta_1'\beta_2' & 3\alpha_1'\beta_2' & \alpha_2'\beta_1' \\ \alpha_1'\alpha_2' & \beta_1'\beta_2' & \alpha_2'\beta_1' & 3\alpha_1'\beta_2' \end{pmatrix} = [\varphi] \cdot S$$

Если $3\alpha_1'\beta_2' + \alpha_2'\beta_1' = -1$, получаем $[\varphi] \cdot S(-a_1)$.

Таким образом, нами доказана.

Лемма 2. $AutK \cong \text{гр}(\pm a_1, a_2, a_3, S)$:

Обозначим $e_5 = \begin{pmatrix} 0 & & & \\ & 6 & & \\ & & 0 & 0 \\ & & 0 & 0 \end{pmatrix}$, $e_6 = \begin{pmatrix} 6 & & & \\ & 0 & & \\ & & 0 & 0 \\ & & 0 & 0 \end{pmatrix}$ и рассмотрим конечно порожденный идеал кольца $ZD(S_3)$

$$I = (e_1, e_2, e_1e_2, e_2e_1, e_5, e_6)$$

Очевидно, что I — характеристический идеал, так как для любого автоморфизма φ кольца $ZD(S_3)$ и любого элемента $x \in I, \varphi(x) \in I$.

$$ZD(S_3)/I \cong \{\alpha e + \beta a | \alpha = 0, ..., 5, \beta = 0, 1, 2\}$$

Здесь e, a — матрицы из представления ZS_3. Пусть $x = r + b \in ZD(S_3)$, где $r = \alpha e + \beta a, b \in I$. Тогда для любого автоморфизма φ колца $ZD(S_3)$ имеем $\varphi(x) = \varphi(r + b) = \varphi(r) + \varphi(b), \varphi(r) \notin I, \varphi(b) \in I$. Поэтому

$$\varphi(a) = a + \gamma_1 e_1 + \gamma_2 e_2 + \gamma_3 e_1 e_2 + r_4 e_2 e_1 + \gamma_5 e_5 \tag{4}$$

Из предыдущих рассуждений понятно, что все автоморфизмы кольца K продолжаются до автоморфизмов идеала I, если положить их действие тождественным на одномерных клетках. Осталось понять, какие из автоморфизмов идеала I можно продолжить до автоморфизмов кольца $ZD(S_3)$. Для этого нужно проверить, существуют ли такие $\gamma_1, ..., \gamma_5$ из равенства (4), для которых выполнялись бы равенства

1. $\varphi(ae_1) = \varphi(a)\varphi(e_1)$
2. $\varphi(e_1a) = \varphi(e_1)\varphi(a)$
3. $\varphi(ae_2) = \varphi(a)\varphi(e_2)$
4. $\varphi(e_2a) = \varphi(e_2)\varphi(a)$
5. $\varphi(ae_1e_2) = \varphi(a)\varphi(e_1e_2)$
6. $\varphi(e_1e_2a) = \varphi(e_1e_2)\varphi(a)$
7. $\varphi(ae_2e_1) = \varphi(a)\varphi(e_2e_1)$
8. $\varphi(e_2e_1a) = \varphi(e_2e_1)\varphi(a)$
9. $\varphi(a^2) = (\varphi(a))^2$

Обозначим $\varphi_{a_1}, \varphi_{a_2}...$ — автоморфизмы кольца K, задаваемые матрицами $a_1, a_2...$.

Непосредственным вычислением находим продолжения $\varphi_{a_1}(a) = a - 2e_1, \varphi_{a_2}(a) = a - e_1, \varphi_{a_3}(a) = a - 2e_2 + e_1e_2 - e_2e_1, \varphi_{-a_1}, \varphi_s, \varphi_{-a_1s}$ не продолжаются до автоморфизмов кольца $ZD(S_3)$. Нами получена

Лемма 3. $AutZD(S_3) = \text{гр}(\varphi_{a_1}, \varphi_{a_2}, \varphi_{a_3})$

Рассмотрим группу внутренних автоморфизмов кольца $ZD(S_3)$. Понятно, что она изоморфна группе нормализованных единиц $V(ZD(S_3))$. Из представления [1] легко получить, что

$$V(ZS_3) \cong \text{гр}\left(r = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, s = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, b = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \right)$$

Обозначим $\varphi_r, \varphi_s, \varphi_b$ автоморфизмы, задаваемые на кольце ZS_3 сопряжениями матрицами, соответственно, $\widetilde{r} = diag(1, -1, r), \widetilde{s} = diag(1, 1, s), \widetilde{b} = diag(1, 1, b)$. Простым вычислением находим матрицы этих автоморфизмов в базисе кольца ZS_3. Обозначим их, соответственно, $[\varphi_r], [\varphi_s], [\varphi_b]$.

Поскольку
$[\varphi_{a_1}] = [\varphi_s][\varphi_r][\varphi_b]$,
$[\varphi_{a_2}] = [\varphi_s][\varphi_r][\varphi_b][\varphi_r][\varphi_s]$,
$[\varphi_{a_3}] = [\varphi_b]^{-1}$, справедлива.

Теорема 1. Все автоморфизмы кольца ZS_3 является внутренними.

Литература

[1] Попова А.М., Порошенко Е.Н. Группы единиц групповых колец конечных групп. Algebra and Model Theory 4. Новосибирск, 2003, 99-106.

СВОЙСТВА ОБОБЩЕННО СТАБИЛЬНЫХ ТЕОРИЙ

М.А. Русалеев*

Институт математики им. Соболева,
проспект академика Коптюга, 4
630090, Новосибирск, Россия
e-mail: rusma@ngs.ru

1 Введение

Стабильные теории были введены С.Шелахом [1] для построения теории классификации и являются обобщением понятия тотально трансцендентной теории, введенного М. Морли [2]. С. Шелах доказал (см.[3]), что стабильность теории равносильна определимости любого полного типа. Это свойство играет фундаментальную роль в исследовании стабильных теорий. В статье [4] Е.А.Палютин ввел понятие E^*-стабильности и доказал определимость типов для E^*-стабильных теорий. Следствием этого результата кроме определимости типов для стабильных теорий, доказанной Шелахом, является также определимость типов над любыми P-множествами в P-стабильных теориях, которая была ранее установлена Т.Нурмагамбетовым и Б.Пуаза [5] для типов над P-моделями. Понятие E^*-стабильности представляет собой новую шкалу стабильности, основным параметром которой является некоторое отображение типов полной теории в типы другой теории.

В [6] Русалеевым был исследован случай $(P,1)$-стабильности, одного из простейших частных случаев E^*-стабильности. Для класса $(P,1)$-стабильный теорий была дана полная характеризация, как класса теорий, каждая из которых определимо интерпретируется в некоторой теории языка, состоящего только из одноместных предикатов. В этой работе исследуется другой частный случай — (P,A)-стабильность, и делается попытка доказать некий аналог результата для $(P,1)$-стабильных теорий.

*Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, проект №05-01-00411

2 Определения

Для наших целей более удобно заранее не ограничиваться мощностью множества (предметных) переменных. Будем считать, что в формулах все связанные переменные берутся из фиксированного счетного множества $U = \{u_i | i \in \omega\}$, свободные переменные не принадлежат этому множеству и, когда не говорится противное, будем считать, что переменные не входят в множество U. Выводимость рассматривается в исчислении предикатов с указанными условиями разделения связанных и свободных переменных.

Зафиксируем некоторое счетное множество переменных $V = \{v_i | i \in \omega\}$. Через $S_n(T)$ обозначается множество $S_{\mathbf{v}}(T)$, где $\mathbf{v} = \langle v_0, \ldots, v_{n-1} \rangle$. Пусть $S_\omega(T) = \bigcup\{S_{\mathbf{v}}(T) | \mathbf{v} \in V\}$. Множество формул языка L от переменных из кортежа $\mathbf{v} = \langle v_0, \ldots, v_{n-1} \rangle$ обозначим $F_n(L)$.

Определение. *Пусть даны языки L, L^* и полная теория T языка L. Отображение $E : S_\omega(T) \to S^{\subseteq}_\omega(L^*)$ называется* представлением типов теории T в языке L^*, *если выполнены следующие условия:*

(1) абстрактность *(если w - перестановка множества переменных V, то $E(w(t)) = w(E(t))$ для любого $t \in S_\omega(T)$);*

(2) сохранение равенства *(если $t \in S_\omega(T)$, $x, y \in V$ и $x = y \in t$, то $x = y \in E(t)$);*

(3) консервативность *(если $t \in S_n(T)$ и $t \subseteq t' \in S_\omega(T)$, то $E(t) = (E(t') \cap F_n(L^*))$);*

(4) непрерывность *(если $t \in S_\omega(T)$ и $\varphi \in E(t)$, то существует формула $\Phi \in t$ такая, что $\varphi \in E(t')$ для любого $t' \in S_\omega(T)$ с условием $\Phi \in t'$);*

В дальнейшем представление типов теории T в языке L^* будем обозначать E^*.

Определение. *Расширим отображение E^* на типы от любого множества переменных следующим образом.*

(a) Если $\mathbf{x}$ - произвольный кортеж переменных длины n и $t \in S_{\mathbf{x}}(T)$, то полагаем $E^*(t) = (E^*((t)^{\mathbf{x}}_{\mathbf{v}})^{\mathbf{v}}_{\mathbf{x}}$, где $\mathbf{v} = \langle v_0, \ldots, v_{n-1} \rangle$.

(b) Если X — произвольное множество переменных и $t \in S_X(T)$, то полагаем $E^*(t) = \bigcup\{E^*(t \restriction \mathbf{x}) | \mathbf{x} \in X\}$

Корректность последнего определения (т.е. что это отображение удовлетворяет абстрактности, консервативности, непрерывности, сохраняет равенство, а образ типа $t \in S_X(T)$ при таком отображении является типом из $S^{\subseteq}_X(L^*)$) показана в [4].

Определение. *Пусть E^* — представление типов полной теории T. Теория T называется* E^*-стабильной в мощности λ *, если для каждого множества переменных X с условием $|X| \leq \lambda$ и каждого $t \in S_X(T)$ тип $E^*(t)$ имеет не более λ пополнений из множества $S_X(L^*)$. Теория T называется E^*-стабильной, если она E^*-стабильна в некоторой бесконечной мощности λ.*

Определение. *Пусть L — некоторый язык, X — множество переменных, $t \in S_X^{\subseteq}(L)$. Пусть $\mathbf{X}$, $\mathbf{Y}$ — некоторые множества кортежей переменных из X длины n. Будем говорить, что пара $\langle \mathbf{X}, \mathbf{Y} \rangle$* отделима *в типе t над X, если существует формула $\Phi(\mathbf{z}; \mathbf{x}^0)$ языка L такая, что $l(\mathbf{z}) = n$, $\mathbf{x}^0 \in X$ и множество формул*

$$\{\Phi(\mathbf{x}; \mathbf{x}^0) | \mathbf{x} \in \mathbf{X}\} \cup \{\neg\Phi(\mathbf{x}; \mathbf{x}^0) | \mathbf{x} \in \mathbf{Y}\}$$

совместно с типом t. При этом формула $\Phi(\mathbf{z}; \mathbf{x}^0)$ отделяет $\mathbf{X}$ *от $\mathbf{Y}$ в $t(X)$.*

Мы будем использовать следующую теорему из статьи [4].

Теорема 2.1. *Пусть T — полная теория языка L, и E^* — представление типов теории T в языке L^*. Тогда следующие условия эквивалентны:*

(1) теория T является E^*-стабильной;

(2) для любых множества переменных X и полного типа $t \in S_X(T)$, каждая пара $\langle \mathbf{X}, \mathbf{Y} \rangle$ множеств кортежей переменных из X одинаковой длины, отделимая в типе $E^*(t)$ над X, является отделимой в t над X.

Пусть задан язык L. Тогда расширение языка L с помощью одноместного предиката будем обозначать $L^P = L \cup \{P(x)\}$.

Для полной теории T языка L зададим представление типов в языке L^P. $E^{(P,A)}(t(X))$ — замыкание относительно выводимости множества формул $t \cup \{P(x) | x \in X\}$ с множеством формул, не зависящих от выбора типа t, выражающих, что для любой модели $\mathfrak{A}$ языка L^P множество $P(\mathfrak{A})$ является алгебраически замкнутым подмножеством.

Определение. *Теория T называется (P, A)-стабильной, если она $E^{(P,A)}$-стабильна.*

Для полной теории T, если не оговаривается иного, мы будем предполагать, что все рассуждения производятся в монстр-модели $\mathfrak{M}$, которая достаточно насыщена и все рассматриваемые модели теории T являются её элементарными подмоделями. Вместо $\mathfrak{M} \models$ будем писать просто $\models$.

3 Признак не (P, A) стабильности

Теорема 3.1. *Пусть* $\mathbf{X} = \{\mathbf{x}^\alpha | \alpha \in I\}$, $\mathbf{x}^\alpha = \langle x_0^\alpha, \ldots, x_{k-1}^\alpha \rangle$, $X = \{x_i^\alpha | \alpha \in I, i < k\}$ *— соответственно множество кортежей переменных и множество переменных. Причем,* X *состоит из тех же переменных, что кортежи из* $\mathbf{X}$.
Пусть существует формула $\varphi(z, \mathbf{x})$ *такая, что совместно следующее множество формул:*
$R_0(\mathbf{X}) = T \cup \{\mathbf{X}$ *является неразличимой последовательностью*$\} \cup$
$\cup \{\exists z(\neg((\varphi(z, \mathbf{x}^\alpha) \leftrightarrow \varphi(z, \mathbf{x}^\beta)) \wedge \forall z_1 \ldots \forall z_m(\bigwedge_{i=1}^{m} \neg(\varphi(z_i, \mathbf{x}^{\gamma_i} \leftrightarrow \varphi(z, \mathbf{x}^{\gamma_i}))) \rightarrow$
$((\exists^{\leqslant n} z_0 \theta(z_0, z_1, \ldots, z_m, \mathbf{y})) \rightarrow \neg\theta(z, z_1, dots, z_m, \mathbf{y})))) \mid \alpha, \beta, \gamma_i, n, m \in \omega,\ i \in \{1, \ldots, m\},\ \mathbf{x}^\alpha, \mathbf{x}^\beta, \mathbf{x}^{\gamma_i} \in \mathbf{X},\ \mathbf{y}$ *— кортеж переменных из* X, $\theta-$*формула теории* $T\}$. *Тогда* T *не* (P, A)*-стабильна.*

Доказательство. Рассмотрим монстр-модель $\mathfrak{M}$ теории T. По условию $R_0(\mathbf{X})$ совместно с T, значит найдётся $\mathbf{A} \subset \mathfrak{M}$, такое, что $\models R_0(\mathbf{A})$.

случай 1 Существует $d \in \mathfrak{M}$ такой, что $|\varphi(d, \mathbf{A})| = |\neg\varphi(d, \mathbf{A})| = \omega$. В этом случае обозначим в качестве $\mathbf{A}' = \neg\varphi(d, \mathbf{A})$, а в качестве $\mathbf{A}'\prime = \varphi(d, \mathbf{A})$. Построим модель $\mathfrak{M}^P$, путём добавления одноместного предиката P к языку, а реализацию этого предиката выберем так, что $P(\mathfrak{M}^P) = \mathrm{acl}(\mathbf{A} \cup \{b | \models \varphi(b, \mathbf{a}),$ для некторого $\mathbf{a} \in \mathbf{A}'\})$.

Ясно, что для всякого $\mathbf{a} \in \mathbf{A}'$ выполнено $\models \forall z \varphi(z, \mathbf{a}) \rightarrow P(z)$.

Заметим, что в силу того, что $\models R_0(\mathbf{A})$, определения интерпретации P в $\mathfrak{M}$ и того, что $\models \neg\varphi(d, \mathbf{a})$ для всякого $\mathbf{a} \in \mathbf{A}'$, получаем, что d не может попадать в алгебраическое замыкание $\mathbf{A} \cup \{b | \models \varphi(b, \mathbf{a}),$ для некоторого $\mathbf{a} \in \mathbf{A}'\}$. А значит для всякого $\mathbf{a} \in \mathbf{A}''$ выполнено $\models \neg P(d) \wedge \varphi(d, \mathbf{a})$.

По теореме 2.1 теория T не (P, A)-стабильна.

случай 2 Для каждого $d \in \mathfrak{M}$ одно из множеств $\varphi(d, \mathbf{A})$ и $\neg\varphi(d, \mathbf{A})$ конечно.

Зафиксируем некоторое $d \in \mathfrak{M}$. Без ограничения общности можно считать, что $|\varphi(d, \mathbf{A})| = k_0 < \omega$. Обозначим $q(x) = \mathrm{tp}(d, \mathbf{A})$.

Разобьём $\mathbf{A}$ на две бесконечные части $\mathbf{A}'$ и $\mathbf{A}''$ произвольным образом, с тем условием, что $\varphi(d, \mathbf{A}) \subseteq \mathbf{A}''$.

Разобьём $\mathbf{A}''$ на множества $\mathbf{A}_i''$, такие, что $|\mathbf{A}_i''| = k_0$, $\mathbf{A}_i'' \cap \mathbf{A}_j'' = \varnothing$, $i, j \in \omega$. Возьмём такие реализации d_i типа $q(x)$, что $\varphi(d_i, \mathbf{A}) = \mathbf{A}_i''$ (это можно сделать ввиду неразличимости последовательности $\mathbf{A}$).

Построим модель $\mathfrak{M}^P$, путём добавления одноместного предиката P к языку, а реализацию этого предиката выберем так, что $P(\mathfrak{M}^P) = \mathrm{acl}(\mathbf{A} \cup \{b | \models \varphi(b, \mathbf{a}),$ для некторого $\mathbf{a} \in \mathbf{A}'\})$.

Ясно, что для всякого $\mathbf{a} \in \mathbf{A}'$ выполнено $\models \forall z \varphi(z, \mathbf{a}) \rightarrow P(z)$.

Заметим, что в силу того, что $\models R_0(\mathbf{A})$, определения интерпретации P в $\mathfrak{M}$ и выбора d_i, получаем, что d_i не могут попадать в алгебраическое замыкание $\mathbf{A} \cup \{b| \models \varphi(b, \mathbf{a}),$ для некторого $\mathbf{a} \in \mathbf{A}'\}$. А значит для всякого $\mathbf{a} \in \mathbf{A}''$ выполнено $\models \exists z^{\neg} P(d) \wedge \varphi(z, \mathbf{a})$.

По теореме 2.1 теория T не (P, A)-стабильна. □

Список литературы

[1] *S.Shelah,* Stable theories, Israel J. Math. 7 (1969) 187-202.

[2] *M.D.Morly,* Categoricity in power, Trans. A.M.S., 114 (1965) 514-538.

[3] *S.Shelah,* Classification theory and the number of non-isomorphic models, Amsterdam: North-Holland, 1978.

[4] *Е. А. Палютин,* "E^*-стабильные теории", Алгебра и логика, т.42, N 2(2003), с. 194-210.

[5] *Т. Нурмагамбетов, Б.Пуаза,* О числе элементарных пар над множествами, Труды Французско-казахстанского коллоквиума по теории моделей, Алматы, 1995, с. 73-82.

[6] *М.А.Русалеев,* "Характеризация $(p, 1)$-стабильных теорий", Алгебра и логика, принято к печати.

МЕТОД ИНТЕРПРЕТАЦИЙ В ЗАДАЧЕ СИНТЕЗА ОПЕРАТОРОВ ГРУППОВОГО ВЫБОРА

Л.А. Шоломов*

Московский Государственный Университет
Россия, 119991, Москва, ГСП-1, Ленинские горы
e-mail: sholomov@isa.ru

1 Введение

В формальной логике широко применяется метод интерпретаций. Он поволяет устанавливать относительную непротиворечивость аксиоматических теорий, решать вопрос о независимости аксиом. При использовании этого метода переменным, отношениям и операциям, присутствующим в формулах, принадлежащих теории некоторого класса систем, придается новая интерпретация, и сами формулы (свойства систем) интерпретируются по-новому.

Подход, основанный на возможности другой интерпретации формул, может быть использован и для решения некоторых конструктивных задач в областях, не связанных с формальной логикой. В данной работе он применяется в следующем виде. Пусть имеется класс V объектов некоторой природы и каждый объект из V допускает представление формулой некоторого вида (вообще говоря, неединственное). Будем говорить, что множество формул F описывает класс V, если для каждого $v \in V$ в F есть хотя бы одна представляющая его формула f, и всякая формула $f \in F$ соответствует объекту из V. Пусть задано свойство α объектов из V и требуется указать какое-либо множество формул $F_\alpha \subseteq F$, описывающих множество V_α всех объектов из V, обладающих этим свойством. Тогда, если удастся подобрать другую интерпретацию множества формул F, т. е. другой класс объектов W, для представления которых можно использовать формулы из F, и указать свойство β объектов из W такое,

*Работа выполнена при поддержке Отделения информационных технологий и вычислительных систем РАН (проект 1-1 программы "Фундаментальные проблемы информационных технологий и систем") и Российского фонда фундаментальных исследований (проекты 06-01-00577 и 06-07-89293).

что если v и w ($v \in V$, $w \in W$) представимы одной и той же формулой f, то w обладает свойством β тогда и только тогда, когда v обладает свойством α, то описание объектов класса V со свойством α может быть заменено описанием объектов из W со свойством β. Если объекты из W и свойство β имеют более простую структуру, это может существенно упростить задачу.

В данной работе такой подход используется для нахождения явного вида операторов группового выбора с заданными свойствами. Задача описания таких операторов инициирована известной теоремой невозможности К. Эрроу (см., например, [1]), и эта проблематика занимает одно из центральных мест в теории группового выбора. Данная работа излагает некоторые результаты из [2, 3, 4, 5] и почти не включает доказательств. Более подробный обзор этих результатов имеется в [6].

2 Операторы группового выбора

Пусть задано некоторое множество A, элементы которого называются *вариантами*, и указано правило выбора, определяющее для всякого $X \subseteq A$ подмножество вариантов $Y \subseteq X$, *выбираемых* из X. Будем рассматривать случай, когда правило выбора использует некоторое бинарное отношение $r \subseteq A^2$, характеризующее "предпочтительность" вариантов (xry трактуется как x лучше y). Вид самого правила выбора по отношению для данной работы не существен и его уточнять не будем.

В задаче группового (коллективного выбора) с участием n лиц возникает необходимость выбора по набору отношений $(r_1, \ldots, r_n)$, связанных с участниками. Часто ее решают путем построения агрегированного отношения $r = F(r_1, \ldots, r_n)$ и выбора по нему. Отношения $r_1, \ldots, r_n$ называют *индивидуальными*, отношение r — *групповым*.

Задача синтеза операторов группового выбора состоит в том, чтобы найти явный вид операторов F, удовлетворяющих заданным *характеристическим условиям* и *структурным ограничениям* [7]. Характеристические условия представляют собой аксиоматически заданные требования к операторам. Структурные ограничения вводятся указанием классов отношений $\mathcal{R}_1$ и $\mathcal{R}_2$ (обычно $\mathcal{R}_1 \subseteq \mathcal{R}_2$) и требованием, чтобы при использовании индивидуальных отношений из $\mathcal{R}_1$ групповое принадлежало классу $\mathcal{R}_2$. Будем говорить, что соответствующий оператор имеет тип $\mathcal{R}_1^n \to \mathcal{R}_2$. Если понадобится указать множество A, на котором заданы отношения класса $\mathcal{R}$, будем использовать обозначение $\mathcal{R}(A)$. Дальше множество A будем предполагать конечным.

Приведем характеристические условия и структурные ограничения,

используемые в данной работе. В содержащемся ниже описании характеристических условий под x, y, x', y' понимаются произвольные варианты из A, под $(r_1, \ldots, r_n)$ и $(r'_1, \ldots, r'_n)$ — произвольные наборы индивидуальных отношений, под r и r' — значения $F(r_1, \ldots, r_n)$ и $F(r'_1, \ldots, r'_n)$. Будем рассматривать операторы $F(r_1, \ldots, r_n)$, удовлетворяющие следующему распространенному набору характеристических условий [7]:

$$\begin{array}{l}(xr_iy \Leftrightarrow xr'_iy) \wedge (yr_ix \Leftrightarrow yr'_ix),\ 1 \le i \le n, \Longrightarrow xry \Leftrightarrow xr'y \ -\ , \\ \forall x \forall y \exists (r_1, \ldots, r_n) \exists (r'_1, \ldots, r'_n)(xry \wedge y\bar{r}'x) \quad -\ , \\ (xr_iy \Leftrightarrow x'r_iy') \wedge (yr_ix \Leftrightarrow y'r_ix'),\ 1 \le i \le n, \Longrightarrow xry \Leftrightarrow x'ry' \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad - \quad .\end{array}$$

Нетрудно видеть, что такие операторы (и только они) представимы в виде

$$F(r_1, \ldots, r_n) = \Phi(r_1, \ldots, r_n, r_1^{-1}, \ldots, r_n^{-1}),$$

где Φ — нетривиальная (не дающая тождественно пустого или полного множества) теоретико-множественная операция. Вместо r_i^{-1} удобно иметь дело с отношениями $r_i^* = \overline{(r_i^{-1})}$, которые называются *двойственными* к r_i. Заменив r_i^{-1} на $\overline{r_i^*}$ и модифицировав соответствующим образом оператор Φ, будем рассматривать представления

$$F(r_1, \ldots, r_n) = \Phi(r_1, \ldots, r_n, r_1^*, \ldots, r_n^*). \tag{1}$$

Будем использовать также эквивалентную запись

$$xF(r_1, \ldots, r_n)y = \varphi(xr_1y, \ldots, xr_ny, xr_1^*y, \ldots, xr_n^*y), \tag{2}$$

где $x, y \in A$ произвольны, φ — булева функция, соответствующая операции Φ.

Чтобы указать структурные ограничения, опишем основные классы отношений, используемых в моделях выбора. Отношение r называется (а) *рефлексивным*, (б) *иррефлексивным*, (в) *асимметричным*, (г) *антисимметричным*, (д) *полным*, (е) *связным*, (ж) *транзитивным*, (и) *негатранзитивным*, (к) *ациклическим*, если оно удовлетворяет условию (а) xrx, (б) $x\bar{r}x$, (в) $xry \Rightarrow y\bar{r}x$, (г) $(x \ne y \wedge xry) \Rightarrow y\bar{r}x$, (д) $xry \vee yrx$, е) $x \ne y \Rightarrow (xry \vee yrx)$, (ж) $(xry \wedge yrz) \Rightarrow xrz$, (и) $(x\bar{r}y \wedge y\bar{r}z) \Rightarrow x\bar{r}z$, (к) $x_1rx_2 \wedge x_2rx_3 \wedge \ldots \wedge x_{k-1}rx_k \Rightarrow x_k\bar{r}x_1$, $k = 1, 2, \ldots$

Транзитивное иррефлексивное отношение называется *частичным порядком* (строгим), связный частичный порядок — *линейным порядком*, а негатранзитивное ациклическое отношение — *слабым порядком*. Частичный порядок r со свойством $(xry \wedge zrv) \Rightarrow (xrv \vee zry)$ называется *интервальным порядком*, а интервальный порядок со свойством $(xry \wedge yrz) \Rightarrow$

$(xrv \vee vrz)$ — *полупорядком*. Указанные типы порядков наиболее распространены в задачах выбора. Это связано с тем, что линейные порядки представимы строгим критерием, слабые порядки — нестрогим критерием, интервальные порядки — критерием с погрешностью, полупорядки — критерием с постоянной погрешностью, частичные порядки — совокупностью критериев [8].

Обозначим соответственно через $\mathcal{P}$, $\mathcal{L}$, $\mathcal{W}$, $\mathcal{I}$, $\mathcal{S}$, $\mathcal{T}$ и $\mathcal{A}$ классы отношений частичного, линейного, слабого, интервального порядка, полупорядка, ацикличных и транзитивных отношений. Справедливы строгие включения

$$\mathcal{L} \subset \mathcal{W} \subset \mathcal{S} \subset \mathcal{I} \subset \mathcal{P} \subset (\mathcal{T}, \mathcal{A}).$$

Классы $\mathcal{T}$ и $\mathcal{A}$ не сравнимы по включению и оба содержат $\mathcal{P}$.

В качестве классов $\mathcal{R}_1, \mathcal{R}_2$, задающих структурные ограничения будем использовать произвольные пары классов из $\{\mathcal{L}, \mathcal{W}, \mathcal{S}, \mathcal{I}, \mathcal{P}, \mathcal{T}, \mathcal{A}\}$, удовлетворяющие включению $\mathcal{R}_1 \subseteq \mathcal{R}_2$. Всего имеется 27 типов таких операторов $\mathcal{R}_1^n \to \mathcal{R}_2$. Данная работа содержит их явные представления. Они получены с помощью метода интерпретаций, посредством которого задача описания операторов над отношениями, имеющих нужный тип, сведена к задаче описания более простых объектов — так называемых порядковых отношений, принадлежащих соответствующему классу.

3 Порядковые отношения

Будем рассматривать n-мерное действительное пространство $\mathbb{R}^n$ и под $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n)$ и т. д. будем понимать точки из $\mathbb{R}^n$. Бинарное отношение ρ на $\mathbb{R}^n$ называется *порядковым*, если для любых $\mathbf{x}, \mathbf{y}, \mathbf{u}, \mathbf{v} \in \mathbb{R}^n$

$$(\operatorname{sgn}(x_i - y_i) = \operatorname{sgn}(u_i - v_i),\ 1 \le i \le n) \Longrightarrow \mathbf{x}\rho\mathbf{y} \Leftrightarrow \mathbf{u}\rho\mathbf{v},$$

где $\operatorname{sgn}(z)$ равен -1, 0 и 1 соответственно при $z < 0$, $z = 0$ и $z > 0$. Примером порядкового отношения может служить *лексикография*

$$\mathbf{x}\lambda\mathbf{y} \Longleftrightarrow x_1 > y_1 \vee (x_1 = y_1 \wedge x_2 > y_2) \vee \ldots \vee (x_1 = y_1 \wedge \ldots \wedge x_{k-1} = y_{k-1} \wedge x_k > y_k)$$

при некотором k, $k \le n$. В случае $k = n$ лексикография называется *полной*. Порядковые отношения часто используются в задачах многокритериального выбора, где точки пространства $\mathbb{R}^n$ интерпретируются как наборы оценок вариантов по n заданным критериям.

Порядковые отношения определены на бесконечном множестве $\mathbb{R}^n$, и для решения связанных с ними конструктивных задач необходимо

условиться о конечном способе их задания. Введем бинарные отношения p_i и p'_i $(1 \le i \le n)$ на $\mathbb{R}^n$, положив $\mathbf{x}p_i\mathbf{y} \Leftrightarrow x_i > y_i$, $\mathbf{x}p'_i\mathbf{y} \Leftrightarrow x_i \ge y_i$. Соотношения $x_i \square y_i$, $\square \in \{>, <, =\}$, выразимы через эти отношения:

$$x_i > y_i \Leftrightarrow \mathbf{x}p_i\mathbf{y}, \quad x_i < y_i \Leftrightarrow \mathbf{x}\bar{p}'_i\mathbf{y}, \quad x_i = y_i \Leftrightarrow \mathbf{x}(p'_i \wedge \bar{p}_i)\mathbf{y}.$$

Поскольку порядковое отношение ρ однозначно определяется соотношениями (больше, меньше, равно) одноименных компонент x_i и y_i, $1 \le i \le n$, оно может быть представлено в виде

$$\rho = g_\rho(p_1, \ldots, p_n, p'_1, \ldots, p'_n) = g_\rho(P, P'),$$

где g_ρ – булева функция, называемая *представляющей функцией* отношения ρ. Это равенство означает

$$\mathbf{x}\rho\mathbf{y} \Leftrightarrow g_\rho(\mathbf{x}p_1\mathbf{y}, \ldots, \mathbf{x}p_n\mathbf{y}, \mathbf{x}p'_1\mathbf{y}, \ldots, \mathbf{x}p'_n\mathbf{y}).$$

Аргументы функции g_ρ удовлетворяют неравенству $p_i \le p'_i$, поскольку $\mathbf{x}p_i\mathbf{y} \Rightarrow \mathbf{x}p'_i\mathbf{y}$. Набор $(\Sigma, \Sigma') = (\sigma_1, \ldots, \sigma_n, \sigma'_1, \ldots, \sigma'_n)$ значений аргументов назовем *правильным*, если $\sigma_i \le \sigma'_i$, $1 \le i \le n$. Будем считать булевы функции $g_1(P, P')$ и $g_2(P, P')$ равными и записывать $g_1 = g_2$, если совпадают их значения на правильных наборах (Σ, Σ'). Запись $g_1 \ge g_2$ будет означать, что $g_1(\Sigma, \Sigma') \ge g_2(\Sigma, \Sigma')$ для правильных наборов (Σ, Σ'). Аналогично, эквивалентность формул $F_1(P, P')$ и $F_2(P, P')$ и запись $F_1 = F_2$ понимаются как совпадение значений формул на правильных наборах.

С учетом эквивалентных соотношений $p_i \wedge p'_i = p_i$ и $\bar{p}'_i \wedge \bar{p}_i = \bar{p}'_i$ любая конъюнкция $K \not\equiv 0$ от переменных (P, P') может быть приведена к виду $K = q_1 q_2 \ldots q_n$ (значки $\wedge$ конъюнкции опущены), где $q_i \in \{p_i, p'_i, \bar{p}_i, \bar{p}'_i, p'_i\bar{p}_i, 1\}$ ($q_i = 1$ означает отсутствие соответствующего сомножителя). Такие конъюнкции будем называть *элементарными конъюнкциями*, а сомножители q_i — *элементарными сомножителями*. Дизъюнкцию элементарных конъюнкций назовем *дизъюнктивной нормальной формой* (ДНФ). Всякая функция $g \not\equiv 0$ представима в виде ДНФ, а ДНФ функции $g \equiv 0$ считаем равной 0. Нетрудно видеть, что ДНФ представляющей функции отношения лексикографии имеет вид

$$g_\lambda = p_1 \vee p'_1 p_2 \vee p'_1 p'_2 p_3 \vee \ldots \vee p'_1 \ldots p'_{k-1} p_k. \tag{3}$$

4 Интерпретация операторов порядковыми отношениями

Будем рассматривать операторы вида $F = \Phi(r_1, \ldots, r_n, r_1^*, \ldots, r_n^*)$, а отношения $r_1, \ldots, r_n$, к которым применяются операторы, будем предполагать асимметричными (результатом действия оператора может быть

неасимметричное отношение). Заметим, что из всех введенных выше классов неасимметричные отношения имеются лишь в $\mathcal{T}$. Свойство асимметрии отношения r_i может быть записано в виде $r_i \cap r_i^{-1} = \emptyset$, что эквивалентно включению $r_i \subseteq r_i^*$. Поэтому при вычислении оператора теоретико-множественная операция $\Phi(X_1, \ldots, X_n, X'_1, \ldots, X'_n)$ применяется лишь к наборам множеств, удовлетворяющим условиям $X_i \subseteq X'_i$, $1 \leq i \leq n$. Такие наборы множеств будем называть *правильными*.

С оператором $F = \Phi(r_1, \ldots, r_n, r_1^*, \ldots, r_n^*)$ свяжем функцию $g_F = \varphi(p_1, \ldots, p_n, p'_1, \ldots, p'_n)$, где φ — булева функция, соответствующая теоретико-множественной операции Φ, и обозначим через ρ_F порядковое отношение с представляющей функцией $g_{\rho_F} = g_F$. Один и тот же оператор F может быть представлен разными теоретико-множественными операциями $\Phi(X_1, \ldots, X_n, X'_1, \ldots, X'_n)$, значения которых на правильных наборах множеств совпадают. Соответствующие им булевы функции φ также совпадают на правильных наборах (P, P'), а потому представляют одно и то же порядковое отношение. Это означает, что отношение ρ_F не зависит от того, какое представление оператора F использовано для установления соответствия. Легко видеть, что соответствие между операторами F и порядковыми отношениями ρ_F взаимно однозначно.

Бинарное отношение r можно рассматривать как двуместный предикат $r(x, y) = xry$. Свойства отношений r и классы отношений обычно задаются системами аксиом, которые часто имеют вид

$$\forall x_1 \ldots \forall x_s P(x_1, \ldots, x_s), \tag{4}$$

где P — бесквантворная формула, содержащая (наряду с предметными переменными x_i и логическими операциями) лишь двуместный предикат r. Такие свойства и классы отношений будем называть *универсально аксиоматизируемыми*. Отметим (и это существенно), что предикат равенства не допускается и, таким образом, P является формулой чистого исчисления предикатов [9]. Универсально аксиоматизируемыми являются все введенные выше свойства отношений, исключая антисимметрию и связность, в определении которых участвуют неравенства (отрицания равенств), и все классы отношений кроме $\mathcal{L}$.

Следующая теорема [2] связывает операторы типа $\mathcal{W}^n \to \mathcal{R}$ и порядковые отношения.

Теорема 1. *Если $\mathcal{R}$ — универсально аксиоматизируемый класс отношений, то оператор F вида* (1) *имеет тип $\mathcal{W}^n \to \mathcal{R}$ тогда и только тогда, когда соответствующее ему порядковое отношение ρ_F принадлежит классу $\mathcal{R}$.*

Эта теорема играет ключевую роль в предлагаемом подходе, поэтому приведем ее доказательство. Оно основано на следующей лемме.

Лемма 1. *Если F — оператор вида* (1)*, то*

$$(a)\quad (\forall s)(\forall \mathbf{x}_1 \dots \forall \mathbf{x}_s \in \mathbb{R}^n)(\exists A)(\exists r_1 \dots \exists r_n \in \mathcal{W}(A))(\exists x_1 \dots \exists x_s \in A)$$
$$x_i F(r_1, \dots, r_n) x_j \Leftrightarrow \mathbf{x}_i \rho_F \mathbf{x}_j, \quad 1 \le i, j \le s,$$
$$(b)\quad (\forall s)(\forall A)(\forall r_1 \dots \forall r_n \in \mathcal{W}(A))(\forall x_1 \dots \forall x_s \in A)(\exists \mathbf{x}_1 \dots \exists \mathbf{x}_s \in \mathbb{R}^n)$$
$$x_i F(r_1, \dots, r_n) x_j \Leftrightarrow \mathbf{x}_i \rho_F \mathbf{x}_j, \quad 1 \le i, j \le s.$$

Доказательство. (a) Пусть $\mathbf{x}_i = (x_1^{(i)}, \dots, x_n^{(i)})$, $1 \le i \le s$. Сопоставим каждому $\mathbf{x}_i$ некоторый элемент x_i (например, целое число) и возьмем $A = \{x_1, \dots, x_s\}$. Введем отношения r_t, $1 \le t \le n$, на A, положив $x_i r_t x_j \Leftrightarrow x_t^{(i)} > x_t^{(j)}$, $1 \le i, j \le s$. Из свойств слабых порядков [8] следует, что $r_t \in \mathcal{W}(A)$. Для любых i, j выполнено

$$x_i r_t x_j \Leftrightarrow x_t^{(i)} > x_t^{(j)} \Leftrightarrow \mathbf{x}_i p_t \mathbf{x}_j,$$
$$x_i r_t^* x_j \Leftrightarrow x_j \bar{r}_t x_i \Leftrightarrow x_t^{(i)} \ge x_t^{(j)} \Leftrightarrow \mathbf{x}_i p_t' \mathbf{x}_j.$$

С учетом этого и соотношения (2) получаем

$$x_i F(r_1, \dots, r_n) x_j \Leftrightarrow \varphi(x_i r_1 x_j, \dots, x_i r_n x_j, x_i r_1^* x_j, \dots, x_i r_n^* x_j) \Leftrightarrow$$
$$\varphi(\mathbf{x}_i p_1 \mathbf{x}_j, \dots, \mathbf{x}_i p_n x_j, \mathbf{x}_i p_1' \mathbf{x}_j, \dots, \mathbf{x}_i p_n' \mathbf{x}_j) \Leftrightarrow \mathbf{x}_i \rho_F \mathbf{x}_j.$$

(b) Из $r_t \in \mathcal{W}(A)$ следует, что конечное множество A может быть разбито на множества (уровни) так, что $x r_t y$ тогда и только тогда, когда уровень элемента x выше, чем у элемента y [8]. Обозначим через $x_t^{(i)}$ номер уровня элемента x_i в отношении r_t и положим $\mathbf{x}_i = (x_1^{(i)}, \dots, x_n^{(i)})$. Тогда $x_i r_t x_j \Leftrightarrow x_i^{(t)} > x_t^{(j)}$, т. е. x_i и x_j связаны с $\mathbf{x}_i$ и $\mathbf{x}_j$ тем же способом, что и в (a). Это дает возможность завершить доказательство как в (a) и получить $x_i F(r_1, \dots, r_n) x_j \Leftrightarrow \mathbf{x}_i \rho_F \mathbf{x}_j, 1 \le i, j \le s$. Лемма доказана.

Доказательство теоремы. Пусть F — оператор типа $\mathcal{W}^n \to \mathcal{R}$, где $\mathcal{R}$ — универсально аксиоматизируемый класс. Рассмотрим некоторую аксиому (4), используемую для задания класса $\mathcal{R}$. Пусть $\mathbf{x}_1, \dots, \mathbf{x}_s$ — произвольные точки из $\mathbb{R}^n$. Возьмем гарантируемые пунктом (a) леммы множество A, отношения $r_1, \dots, r_n \in \mathcal{W}(A)$ и элементы $x_1, \dots, x_s$ из A. Отношение $r = F(r_1, \dots, r_n)$ удовлетворяет формуле $P(x_1, \dots, x_s)$ в (4). Согласно (a) имеет место $\mathbf{x}_i \rho_F \mathbf{x}_j \Leftrightarrow x_i r x_j$, а потому формула $P(\mathbf{x}_1, \dots, \mathbf{x}_s)$ истинна для ρ_F. Поскольку эти рассуждения применимы к любой аксиоме, участвующей в определении класса $\mathcal{R}$, получаем $\rho_F \in \mathcal{R}$.

Обратно, покажем что из $\rho_F \in \mathcal{R}$ следует $r = F(r_1, \dots, r_n) \in \mathcal{R}$ для любых $r_1, \dots, r_n \in \mathcal{W}$. Рассмотрим аксиому (4) и произвольные

$x_1, \ldots, x_s \in A$. Возьмем точки $\mathbf{x}_1, \ldots, \mathbf{x}_s \in \mathbb{R}^n$, гарантируемые пунктом (b) леммы. Поскольку ρ_F удовлетворяет формуле $P(\mathbf{x}_1, \ldots, \mathbf{x}_s)$, то $P(x_1, \ldots, x_s)$ истинна для r. Остается учесть, что аксиома (4) и элементы $x_1, \ldots, x_s \in A$ произвольны. Теорема доказана.

Таким образом, формулы, задающие операторы $\mathcal{R}_1^n \to \mathcal{R}_2$ при $\mathcal{R}_1 = \mathcal{W}$ могут быть интерпретированы (с точностью до обозначений) как представляющие функции порядковых отношений из $\mathcal{R}_2$. Это позволяет вместо достаточно сложных объектов (операторов над отношениями) использовать более простые (порядковые отношения), что значительно облегчает исследование. Важно и то, что свойства порядковых отношений из универсально аксиоматизируемых классов заданы явно (аксиомами), в то время как для операторов лишь указано, как они должны воздействовать на отношения. При нахождении явного вида порядковых отношений из заданных классов (см. следующий раздел) будут использоваться некоторые операции над отношениями. Они не имеют содержательной интерпретации в терминах операторов, и рассуждения, связанные с описанием порядковых отношений, напрямую не переносятся на операторы. Модификации данного подхода позволяют найти явный вид операторов $\mathcal{R}_1^n \to \mathcal{R}_2$ и при $\mathcal{R}_1 \neq \mathcal{W}$.

5 Техника исследования порядковых отношений

Существенную роль при исследовании свойств порядковых отношений играет возможность описания основных операций над отношениями в терминах преобразования представляющих функций [2, 5]. Приведем некоторые из них.

1°. *Если* $\rho = F(\rho_1, \ldots, \rho_k)$, *где* F – *теоретико-множественная операция, то*

$$g_\rho(P, P') = \varphi_F(g_{\rho_1}(P, P'), \ldots, g_{\rho_k}(P, P')),$$

где φ_F – *булева функция, соответствующая операции* F.

Скажем, что ρ' получено из ρ *инвертированием оси* 1, если

$$(x_1, x_2, \ldots, x_n)\rho'(y_1, y_2, \ldots, y_n) \Leftrightarrow (y_1, x_2, \ldots, x_n)\rho(x_1, y_2, \ldots, y_n).$$

Аналогично определяется результат инвертирования оси i. Отношение $\hat{\rho}$, полученное из ρ инвертированием некоторых осей, называется *однотипным* с ρ.

Таблица 1:

	p_i	p'_i	$\bar{p}_i$	$\bar{p}'_i$	$p'_i\bar{p}_i$	1
p_i	p_i	p_i	1	1	p_i	1
p'_i	p_i	p'_i	1	1	p'_i	1
$\bar{p}_i$	1	1	$\bar{p}_i$	$\bar{p}'_i$	$\bar{p}_i$	1
$\bar{p}'_i$	1	1	$\bar{p}'_i$	$\bar{p}'_i$	$\bar{p}'_i$	1
$p'_i\bar{p}_i$	p_i	p'_i	$\bar{p}_i$	$\bar{p}'_i$	$p'_i\bar{p}_i$	1
1	1	1	1	1	1	1

2°. *Если ρ' образовано из ρ инвертированием оси i, то представляющая функция $g_{\rho'}$ может быть получена из g_ρ заменой p_i и p'_i соответственно на $\bar{p}'_i$ и $\bar{p}_i$, т. е. при $i = 1$ имеет вид*

$$g_{\rho'}(p_1, \ldots, p_n, p'_1, \ldots, p'_n) = g_\rho(\bar{p}'_1, p_2, \ldots, p_n, \bar{p}_1, p'_2, \ldots, p'_n).$$

В случае однотипных отношений указанную замену нужно произвести для всех инвертированных осей.

3°. *Представляющая функция отношения ρ^{-1}, обратного к ρ, может быть записана в виде*

$$g_{\rho^{-1}}(P, P') = g_\rho(\bar{P}', \bar{P}),$$

где $\bar{P} = (\bar{p}_1, \ldots, \bar{p}_n)$, $\bar{P}' = (\bar{p}'_1, \ldots, \bar{p}'_n)$.

4°. *Представляющая функция отношения ρ^*, двойственного к ρ, имеет вид*

$$g_{\rho^*}(P, P') = g^*_\rho(P', P),$$

где g^*_ρ — булева функция, двойственная к g_ρ. (Напомним, что если f — булева функция, то $f^*(x_1, \ldots, x_n) = \bar{f}(\bar{x}_1, \ldots, \bar{x}_n)$.)

Введем операцию композиции $g \circ \hat{g}$ функций $g(P, P')$ и $\hat{g}(P, P')$ [2], которая позволит найти представляющую функцию произведения отношений. Операцию $\circ$ определим вначале для элементарных сомножителей, затем для элементарных конъюнкций и, наконец, – для функций, заданных посредством ДНФ.

Композиция $q_i \circ \hat{q}_i$ элементарных сомножителей находится согласно таблице 1, содержащей в пересечении строки q_i и столбца $\hat{q}_i$ значение $q_i \circ \hat{q}_i$. Композицией элементарных конъюнкций $K = q_1 \ldots q_n$ и $\hat{K} = \hat{q}_1 \ldots \hat{q}_n$ назовем элементарную конъюнкцию $K \circ \hat{K} = (q_1 \circ \hat{q}_1) \ldots (q_n \circ \hat{q}_n)$. Композицию функций $g, \hat{g} \not\equiv 0$, заданных посредством ДНФ $g = K_1 \vee$

$\ldots \vee K_s$ и $\hat{g} = \hat{K}_1 \vee \ldots \vee \hat{K}_t$, определим равенством

$$g \circ \hat{g} = \bigvee_{1 \le u \le s,\, 1 \le v \le t} K_u \circ \hat{K}_v.$$

Роль операции композиции проясняет следующее утверждение [2].

Теорема 2. *Представляющая функция произведения $\rho_1\rho_2$ находится как композиция $g_{\rho_1} \circ g_{\rho_2}$ представляющих функций для ρ_1 и ρ_2.*

Если определить *степень g^k функции g*, положив $g^1 = g$, $g^k = g^{k-1} \circ g$, $k \ge 2$, то последовательность степеней не убывает, т. е $g \le g^2 \le \ldots \le g^k \le \ldots$, и ограничена [2]. Результат ее стабилизации обозначим $[g]$.

Произведение порядковых отношений обладает рядом свойств, не имеющих места для произвольных отношений. В их числе коммутативность $\rho_1\rho_2 = \rho_2\rho_1$ (вытекающая из коммутативности операции композиции) и свойство неубывания степеней $\rho \subseteq \rho^2 \subseteq \ldots \subseteq \rho^k \subseteq \ldots$, где $\rho^1 = \rho$, $\rho^k = \rho^{k-1}\rho$, $k \ge 2$. Результат стабилизации этой неубывающей ограниченной последовательности, который обозначим $[\rho]$, является транзитивным замыканием отношения ρ. Легко видеть, что оно является порядковым отношением и функция $g_{[\rho]}$ совпадает с $[g_\rho]$.

Следующая теорема [2, 5] связывает свойства порядковых отношений со свойствами представляющих функций. Пусть $\tilde{0} = (0, \ldots, 0)$ и $\tilde{1} = (1, \ldots, 1)$ – наборы длины n, $D_0 = p_1 \vee \ldots \vee p_n \vee \bar{p}'_1 \vee \ldots \vee \bar{p}'_n$.

Теорема 3. *Порядковое отношение ρ а) рефлексивно, б) иррефлексивно, в) асимметрично, г) антисимметрично, д) полно, е) связно, ж)транзитивно, и) негатранзитивно, к) ациклично тогда и только тогда, когда*

а) $g_\rho(\tilde{0}, \tilde{1}) = 1$, б) $g_\rho(\tilde{0}, \tilde{1}) = 0$, в) $g_\rho(P, P') \le g^*_\rho(P', P)$, г) $D_0 g_\rho(P, P') \le D_0 g^*_\rho(P', P)$, д) $g_\rho(P, P') \ge g^*_\rho(P', P)$, е) $D_0 g_\rho(P, P') \ge D_0 g^*_\rho(P', P)$, ж) $g_\rho(P, P') \circ g_\rho(P, P') \le g_\rho(P, P')$, и) $g^*_\rho(P', P) \circ g^*_\rho(P', P) \le g^*_\rho(P', P)$, к) $[g_\rho](\tilde{0}, \tilde{1}) = 0$.

С помощью этой теоремы находится явный вид порядковых отношений из определенных выше классов $\mathcal{L}, \mathcal{W}, \mathcal{S}, \mathcal{I}, \mathcal{P}, \mathcal{T}, \mathcal{A}$. Отношения, однотипные с лексикографиями и полными лексикографиями, т. е. полученные из них инвертированием некоторых осей, будем называть *обобщенными лексикографиями* и *обобщенными полными лексикографиями*. Для лексикографий и полных лексикографий будем использовать обозначения λ и λ^0, а для однотипных с ними отношений — обозначения $\hat{\lambda}$ и $\hat{\lambda}^0$. Отношение λ^*, двойственное лексикографии, будем называть *нестрогой лексикографией*, поскольку оно рефлексивно (в отличие от

лексикографии, которая иррефлексивна). Используя 4°, нетрудно убедиться, что его представляющая функция может быть получена заменой в (3) конъюнкции $p'_1 \dots p'_{k-1} p_k$ конъюнкцией $p'_1 \dots p'_{k-1} p'_k$. Однотипное с ним отношение будем называть *обобщенной нестрогой лексикографией* и обозначать $\hat{\lambda}^*$. Следующая теорема [2, 5] указывает явный вид порядковых отношений из всех рассматриваемых классов.

Теорема 4. *Порядковое отношение является а) линейным порядком; б) слабым порядком, полупорядком, интервальным порядком; в) частичным порядком; г) транзитивным отношением; д) ациклическим отношением тогда и только тогда, когда оно представляет собой а) обобщенную полную лексикографию; б) обобщенную лексикографию; в)пересечение обобщенных лексикографий; г) пересечение обобщенных лексикографий или пересечение обобщенных нестрогих лексикографий; д) может быть дополнено до обобщенной лексикографии.*

Их представляющие функции имеют вид а) $g_{\hat{\lambda}^0}$, б) $g_{\hat{\lambda}}$, в) $g_{\hat{\lambda}_1} \wedge \ldots \wedge g_{\hat{\lambda}_k}$, г) $g_{\hat{\lambda}_1} \wedge \ldots \wedge g_{\hat{\lambda}_k}$ или $g_{\hat{\lambda}_1^*} \wedge \ldots \wedge g_{\hat{\lambda}_k^*}$, д) $g_{\hat{\lambda}} \wedge \psi$, где ψ — произвольная булева функция от набора переменных (P, P').

Из теоремы видно, что для порядковых отношений классы $\mathcal{W}$, $\mathcal{S}$ и $\mathcal{I}$ совпадают. В общем случае отношений имеют место строгие включения $\mathcal{W} \subset \mathcal{S} \subset \mathcal{I}$ [8].

6 Явный вид операторов группового выбора

Введем некоторые специальные типы операторов.

Первый из них хорошо известен. Это *оператор лексикографии* (ср. с (3))

$$\Lambda(r_1, \dots, r_n) = \bigcup_{j=1}^{k} \Big(r_j \cap \bigcap_{i=1}^{j-1} r_i^* \Big), \qquad k \in \{1, \dots, n\}.$$

Оператор транзитивной лексикографии впервые введен в [3] и является оператором одного из двух типов. Первый имеет вид

$$T(r_1, \dots, r_n) = \bigcup_{j=1}^{k} \Big(r_j^* \cap \bigcap_{i=1}^{j-1} r_i \Big), \qquad k \in \{1, \dots, n\},$$

второй получается из него заменой члена $r_1 \cap \ldots \cap r_{k-1} \cap r_k^*$ на $r_1 \cap \ldots \cap r_k$. Для второго оператора также будем использовать обозначение T.

Чтобы описать следующий тип операторов, дадим ряд определений. Булева функция $f(x_1,\ldots,x_n)$ называется *пороговой*, если существуют такие числа $w_1,\ldots,w_n$ (*веса*) и t (*порог*), что

$$f(x_1,\ldots,x_n)=1 \Leftrightarrow w_1x_1+\ldots+w_n\geq 1.$$

Набор $(w_1,\ldots,w_n,t)$ называется *реализацией* функции f. Обозначим через $Th_{1/2}$ класс пороговых функций, для которых существует реализация с $w_1\geq 0,\ldots,w_n\geq 0$, $w_1+\ldots+w_n=1$, $t=1/2$. Функции из $Th_{1/2}$ монотонны. Представим функцию $f\in Th_{1/2}$ в виде $f=\bigvee_{\{i_1,\ldots,i_s\}} x_{i_1}\ldots x_{i_s}$, где отсутствуют поглощения конъюнкций (для монотонных функций такое представление единственно), и сопоставим ей оператор

$$\Theta(r_1,\ldots,r_n)=\bigcup_{\{i_1,\ldots,i_s\}}\ \bigcap_{i\in\{i_1,\ldots,i_s\}} r_i\ \bigcap_{j\notin\{i_1,\ldots,i_s\}} r_j^*.$$

Оператор Θ впервые введен в работе [2].

Однотипным с оператором $F(r_1,\ldots,r_n)$ будем называть всякий оператор, который получается из F заменой некоторых отношений r_i на r_i^{-1}. При этом в представлении оператора необходимо заменить отношение r_i на $\overline{r_i^*}$ и r_i^* — на $\bar{r}_i$. Для оператора, однотипного с F, будем использовать обозначение $\hat{F}$. В частности, $\hat{\Lambda}$ означает оператор, однотипный с лексикографией, а $\hat{r}_i$ представляет собой отношение r_i либо r_i^{-1}.

Двойственным оператору F называется оператор F^*, получающийся заменой в представлении F теоретико-множественной операции Φ двойственной операцией $\Phi^*(Y_1,\ldots,Y_n,Z_1,\ldots,Z_n)=\bar{\Phi}(\bar{Y}_1,\ldots,\bar{Y}_n,\bar{Z}_1,\ldots,\bar{Z}_n)$ (черта означает дополнение множества), а отношений r_i — двойственными отношениями r_i^* (при этом r_i^* заменяются на r_i). Подобно порядковым отношениям λ и λ^*, двойственный оператор Λ^* отличается из Λ лишь тем, что вместо члена $r_1^*\cap\ldots\cap r_{k-1}^*\cap r_k$ в нем присутствует $r_1^*\cap\ldots\cap r_k^*$.

Следующая теорема [2, 3, 4, 6] указывает явный вид всех операторов типа $\mathcal{R}_1^n\to\mathcal{R}_2$, где $\mathcal{R}_1,\mathcal{R}_2\in\{\mathcal{L},\mathcal{W},\mathcal{S},\mathcal{I},\mathcal{P},\mathcal{T},\mathcal{A}\}$, $\mathcal{R}_1\subseteq\mathcal{R}_2$.

Теорема 5. *Оператор вида* (1) *имеет тип* $\mathcal{R}_1^n\to\mathcal{R}_2$, *где* $\mathcal{R}_1,\mathcal{R}_2\in\{\mathcal{L},\mathcal{W},\mathcal{S},\mathcal{I},\mathcal{P},\mathcal{T},\mathcal{A}\}$, $\mathcal{R}_1\subseteq\mathcal{R}_2$, *тогда и только тогда, когда он может быть представлен в виде, указанном в таблице 2.*

Строки таблицы соответствуют классам $\mathcal{R}_1$, столбцы — классам $\mathcal{R}_2$. В клетках таблицы для пар $(\mathcal{R}_1,\mathcal{R}_2)$, таких что $\mathcal{R}_1\not\subseteq\mathcal{R}_2$, проставлен прочерк. Под G понимается произвольный оператор (остальные обозначения введены выше). Часть включенных в теорему результатов, относящаяся к операторам $\mathcal{W}^n\to\mathcal{R}_2$, $\mathcal{R}_2\in\{\mathcal{W},\mathcal{P},\mathcal{T},\mathcal{A}\}$, получена другими методами в [8, 10, 11, 12, 13] (более подробно см. в [6]).

Таблица 2:

	$\mathcal{L}$	$\mathcal{W}$	$\mathcal{S}$	$\mathcal{I}$	$\mathcal{P}$	$\mathcal{T}$	$\mathcal{A}$	$\leftarrow \mathcal{R}_2$
$\mathcal{L}$	$\hat{r}_i$	$\hat{r}_i$	$\hat{r}_i$	$\hat{r}_i$	$\bigcap_i \hat{r}_i$	$\bigcap_i \hat{r}_i \cap \bigcap_j \hat{r}_j^*$	$\hat{r}_i \cap G$	
$\mathcal{W}$	–	$\hat{\Lambda}$	$\hat{\Lambda}$	$\hat{\Lambda}$	$\bigcap_i \hat{\Lambda}_i$	$\bigcap_i \hat{\Lambda}_i \cap \bigcap_j \hat{\Lambda}_j^*$	$\hat{\Lambda} \cap G$	
$\mathcal{S}$	–	–	$\hat{r}_i$	$\hat{r}_i$	$\bigcap_i \hat{r}_i$	$\bigcap_i \hat{r}_i$	$\hat{\Theta} \cap G$	
$\mathcal{I}$	–	–	–	$\hat{r}_i$	$\bigcap_i \hat{r}_i$	$\bigcap_i \hat{r}_i$	$\hat{r}_i \cap G$	
$\mathcal{P}$	–	–	–	–	$\bigcap_i \hat{r}_i$	$\bigcap_i \hat{r}_i$	$\hat{r}_i \cap G$	
$\mathcal{T}$	–	–	–	–	–	$\bigcap_i \hat{T}_i$	–	
$\mathcal{A}$	–	–	–	–	–	–	$\hat{r}_i \cap G$	
$\uparrow$ $\mathcal{R}_1$								

Приведенный в теореме 5 явный вид операторов типа $\mathcal{W}^n \to \mathcal{R}$ вытекает из теоремы 4 о явном виде порядковых отношений в силу теоремы 1, сводящей синтез таких операторов к описанию порядковых отношений класса $\mathcal{R}$.

Явный вид операторов типа $\mathcal{L}^n \to \mathcal{R}$ может быть получен путем следующего сведения к теореме 1, предложенного в [4]. Учитывая, что для отношения $r_i \in \mathcal{L}$ и $x \neq y$ выполнено $x\bar{r}_i y = xr^{-1}y$ и $xr_i y = xr_i^* y$, можно путем эквивалентных преобразований привести оператор $F = \Phi(r_1, \ldots, r_n, r_1^*, \ldots, r_n^*)$ к одному из видов $F = \Psi(r_1, \ldots, r_n, r_1^*, \ldots, r_n^*)$ и $F = \Psi(r_1^*, \ldots, r_n^*, r_1^{-1}, \ldots, r_n^{-1})$, где Ψ — монотонная теоретико-множественная операция. Первая форма оператора возникает, если он порождает иррефлексивные отношения, вторая — если рефлексивные. Такие операторы будем называть *однородными*, а преобразование, которым они получены, — *редукцией*. Следующая теорема доказана в [4].

Теорема 6. *Если $\mathcal{R}$ — универсально аксиоматизируемый класс отношений и множество $\mathcal{F}$ операторов решает проблему синтеза для $\mathcal{W}^n \to \mathcal{R}$, то множество всех однородных операторов $\mathcal{F}'$, полученных редукцией операторов $F \in \mathcal{F}$, решает проблему синтеза для $\mathcal{L}^n \to \mathcal{R}$.*

Отсюда с учетом легко проверяемого факта, что редукция обобщенной лексикографии дает оператор r_i либо r_i^{-1}, получен явный вид операторов $\mathcal{L}^n \to \mathcal{R}$, указанный в теореме 5.

Для других классов отношений $\mathcal{R}_1$ не удалось сформулировать общих результатов о виде операторов $\mathcal{R}_1^n \to \mathcal{R}_2$, подобных теоремам для $\mathcal{W}$ и $\mathcal{L}$. Однако сам подход к описанию операторов $\mathcal{R}_1^n \to \mathcal{R}_2$ на основе

представляющих функций g_ρ отношений $\rho \in \mathcal{R}_2$, применим (в некотором модифицированном виде) и для других классов отношений [2, 3]. Этим способом установлен явный вид всех операторов в теореме 5. Наибольшие трудности вызвали операторы типов $\mathcal{S}^n \to \mathcal{A}$ [2] и $\mathcal{T}^n \to \mathcal{T}$ [3]. В частности, поскольку транзитивные отношения r_i не всегда ассиметричны (т. е. удовлетворяют условию $r_i \subseteq r_i^*$), операторы $\mathcal{T}^n \to \mathcal{T}$ требуют более сложных логических представлений [3].

Список литературы

[1] Миркин Б. Г. Проблема группового выбора. – М.: Наука, 1974.

[2] Шоломов Л.А. Исследование отношений в критериальных пространствах и синтез операторов группового выбора // Математические вопросы кибернетики. Вып. 5. – М.: Физматлит, 1995. С. 109–143.

[3] Шоломов Л. А. Операторы над отношениями, сохраняющие транзитивность // Дискретная математика. 1998. Т. 10. Вып.1. С. 28–45.

[4] Шоломов Л. А. Агрегирование линейных порядков в задачах группового выбора // Автоматика и телемеханика. 1998. N2. С. 113–122.

[5] Шоломов Л. А. Сложность распознавания свойств порядковых отношений в n-мерных пространствах // Дискретный анализ и исследование операций. Сер. 1. 2002. Т. 9, N 4. С. 82–105.

[6] Sholomov Lev A. Explicit form of neutral social decision rules for basic rationality conditions // Mathematical Social Sciences. 2000. V. 39, N 1. P. 81–107.

[7] Айзерман М. А., Алескеров Ф. Т. Выбор вариантов: основы теории. – М.: Наука, 1990.

[8] Фишберн П. Теория полезности для принятия решений. – М.: Наука, 1978.

[9] Мальцев А. И. Алгебраические системы. – М.: Наука, 1970.

[10] Моркялюнас А. Групповой выбор при независимости и слабой симметрии альтернатив // Математические методы в социальных науках. Вильнюс: Ин-т математики и кибернетики АН ЛитССР, 1985. Вып. 18. С. 57–60.

[11] Данилов В. И. Модели группового выбора // Изв. АН СССР. Техническая кибернетика. 1983. N 1. С. 143–164.

[12] Владимиров А. В. Исследование процедур построения коллективных решений. – Автореф. дис. ... канд. техн. наук / Ин-т проблем управления. М., 1987.

[13] Левченков В. С. Алгебраический подход в теории группового выбора. – М.: Наука, 1990.

SMALL STABLE TRIGONOMETRIES WITH INFINITE WEIGHT

S.V. Sudoplatov*

Sobolev Institute of Mathematics,
4, Acad. Koptyug avenue,
Novosibirsk, 630090, Russia
e-mail: sudoplat@math.nsc.ru, sudoplat@ngs.ru

In the paper we continue, started in [1], an investigation of the class of group trigonometries on projective planes having stable theories. Modifying the construction from [1] and applying Hrushovski — Herwig constructions [3] updated in [2], we prove an existence of small stable trigonometries on projective planes induced by acyclic digraphs. As a corollary we establish an existence of trigonometrical powerful digraphs [4] having small stable theories with infinite weights.

Remind [5], that the type $p(\bar{x})$ *has an infinite own weight*, if there is a realization $\bar{a}$ of $p(\bar{x})$ and an infinite independent sequence $(\bar{a}_n)_{n\in\omega}$ of realizations of type $p(\bar{x})$ such, that tuples $\bar{a}$ and $\bar{a}_n$ are dependent for any $n \in \omega$.

It is known [6], that in the assumption of simplicity, and, in particular, of stability of the theory its Ehrenfeuchtness (i.e. finite, but more than one number of pairwise non-isomorphic countable models) implies the presence of a type having an infinite weight.

The considered construction, alongside with known examples of small stable theories with unique 1-type, having infinite weight [2], [3], produces examples of such theories with an additional condition of presence of geometrical structures of projective planes induced by powerful digraphs.

We use without specifications standard notions and notations from [5], [7], [8] as well as the terminology from [1], [2], [4], [9]–[11].

Let $T(\mathrm{pm})$ be the theory of a polygonometry $\mathrm{pm} = \mathrm{pm}(G, \mathcal{P}, g_0)$, where $\mathcal{P} = \langle P, L, \in\rangle$, n be an integer number. We denote by $x \in y \uparrow^n$ a formula, "saying" that for a graph with the signature symbol Q_{g_0} there exists a (y, x)-sequence of length n if $n \geq 0$, and there exists a (x, y)-sequence of length $-n$, if $n < 0$.

*Supported by RFBR grant No. 05-01-00411, and by the Council for Grants (under RF President) and State Aid of Fundamental Science Schools via project NSh-4787.2006.1.

The theory $T(\mathrm{pm})$ is called g_0-*acyclic*, if $T(\mathrm{pm}) \vdash \neg\exists x\,(x \in x\uparrow^n)$ for all $n \in \omega \setminus \{0\}$.

It is obvious, that the theory $T(\mathrm{pm})$ is g_0-acyclic iff there are no cycles in the graph $\langle P, Q_{g_0}\rangle$.

Observe that if the theory $T(\mathrm{pm})$ is g_0-acyclic then the group G is infinite.

As shown in [10], [12], the class of g_0-acyclic polygonometrical theories without nontrivial polygons as well as the class of g_0-acyclic theories of trigonometries on projective planes are nonempty.

Simplest examples of g_0-acyclic theories present theories of polygonometries $\mathrm{pm} = \mathrm{pm}(G * F_1, \mathcal{P}, g_0)$ of free products of groups G with the free two-generated group $F_1 = \langle g_0, g_1\rangle$, defined by the following equality: $\mathbf{S}(\mathrm{pm}) =$

$$= GN\left(\mathbf{\Delta}_e(G * F_1) \cup \left\{\left(\begin{array}{ccc} g_0^{-1} & g_0 & \alpha^{-1} \\ \alpha & g_1 & g_1^{-1}\end{array}\right) \;\middle|\; \alpha \in G * F_1\right\}\right) \setminus S^e(G * F_1).$$

Specified polygonometries will be called *free*.

Remind, that the notion of *free projective closure* $\mathrm{FPC}(\mathrm{pm})$ polygonometry pm is defined in [1].

Proposition 1. *The theory* $T(\mathrm{FPC}(\mathrm{pm}))$ *is* g_0*-acyclic iff the theory* $T(\mathrm{pm})$ *is* g_0*-acyclic.*

Proof. It is obvious that the theory $T(\mathrm{pm})$ is g_0-acyclic if $T(\mathrm{FPC}(\mathrm{pm}))$ is g_0-acyclic. Assuming that the theory $T(\mathrm{pm})$ is g_0-acyclic, we get that $T(\mathrm{FPC}(\mathrm{pm}))$ is g_0-acyclic similarly [12] by the induction on steps of construction of trigonometry $\mathrm{FPC}(\mathrm{pm})$ from the polygonometry pm. □

Let A be a set in a model $\mathcal{M}$ of theory $T(\mathrm{pm})$, a_1 and a_2 be some elements of A. A (a_1, a_2)-sequence S is called a (a_1, a_2)-g_0-*sequence*, if S is a (a_1, a_2)-sequence in the graph $\mathcal{M} \restriction Q_{g_0}$, received by restriction of model $\mathcal{M}$ to the language $\{Q_{g_0}\}$. The (a_1, a_2)-g_0-sequence S is *external* (over A), if S doesn't contain elements from $A \setminus \{a_1, a_2\}$.

Proposition 2. *Let* A *and* B *be nonempty sets of a model* $\mathcal{M}$ *of* g_0*-acyclic theory* $T(\mathrm{trm})$ *of trigonometry* trm *on a projective plane such that there exists an isomorphism* $f : \mathrm{pcl}(A) \xrightarrow{\sim} \mathrm{pcl}(B)$*, satisfying the following conditions:*

1) $f(A) = B$;

2) *if elements* $a_1, a_2 \in \mathrm{pcl}(A)$ *are connected by an external* (a_1, a_2)-g_0-*sequence over* $\mathrm{pcl}(A)$ *then there are no external* $(f(a_2), f(a_1))$-g_0-*sequences over* $\mathrm{pcl}(B)$.

Then the theory $T(\mathrm{trm}_{A\equiv B})$ *is* g_0*-acyclic.*

Proof. By [1, theorem 2.2] the trigonometry $\mathrm{trm}_{A\equiv B}$ exists. By proposition 1 it is enough to show that prime models $\mathcal{M}_c$ of $T(\mathrm{trm}^c_{A\equiv B})$ over elements

$c \in M \setminus \mathrm{pcl}(A)$ don't contain g_0-cycles. An absence of g_0-cycles in $\mathcal{M}_c$ follows from the condition of absence of g_0-cycles in the model $\mathcal{M}$ and from the reason that by the construction and by item 2 g_0-cycles do not arise via extensions of the isomorphism f to isomorphisms $f_c : \mathrm{pcl}(A \cup \{c\}) \xrightarrow{\sim} \mathrm{pcl}(B \cup \{d\})$. □

Using proposition 2 and an existence of trigonometries $\mathrm{trm}_{\equiv\Lambda}$, identifying types for any family of sets $\Lambda = \{A_i \mid i \in \omega\}$ of model $\mathcal{M} \models T(\mathrm{trm})$ such that systems $\mathrm{pcl}(A_i)$, $i \in \omega$, are pairwise isomorphic, we get the following

Proposition 3. *Let $\Lambda = \{A_i \mid i \in \omega\}$ be a family of nonempty sets of model $\mathcal{M}$ of g_0-acyclic theory $T(\mathrm{trm})$ of trigonometry $\mathrm{trm} = \mathrm{trm}(G, \mathcal{P}, g_0)$ on a projective plane $\mathcal{P}$ such that there exist isomorphisms $f_{ij} : \mathrm{pcl}(A_i) \xrightarrow{\sim} \mathrm{pcl}(A_j)$, $i, j \in \omega$, satisfying the following conditions:*

1) *$f_{ij}(A_i) = A_j$, $i, j \in \omega$;*

2) *if elements $a_1^i, a_2^i \in \mathrm{pcl}(A_i)$ are connected by external (a_1^i, a_2^i)-g_0-sequence over $\mathrm{pcl}(A_i)$ then there are no external $(f_{ij}(a_2^i), f_{ij}(a_1^i))$-$g_0$-sequences over $\mathrm{pcl}(A_{ij})$, $i, j \in \omega$.*

Then the theory $T(\mathrm{trm}_{\equiv\Lambda})$ is g_0-acyclic.

AGREEMENT. Further all considered polygonometrical theories $T(\mathrm{pm})$ will be countable, g_0-acyclic and without h.p.-polygons. We will denote by Q the relation Q_{g_0}.

Let A be a *finite* set in a model $\mathcal{M}$ of theory $T(\mathrm{pm})$. As $T(\mathrm{pm})$ is g_0-acyclic the structure $\mathcal{M}$ induces on A a *c-graph* $\mathcal{A}$ [13] with a binary relation Q, i.e. the graph $\langle A, Q\rangle$ with a record W about existence of only external (over A) shortest sequences connecting elements of A. Here the empty set with the empty record W is also considered as a c-graph.

Remind [2], that for a c-graph $\mathcal{A}$ we denote by A_f the set of *furcations* of A, i.e. of vertices of A, for each of which some Q-sequences of nonzero lengths, connecting this vertex with some other vertices from A, comes to and comes from, and moreover for each vertex $a \in A_f$ one can get arcs or only external shortest sequences with the origin a not less than to two vertices of A, or it is possible to get arcs or only external shortest sequences with the end a not less than from two vertices belonging A. The set of vertices from A, not being furcations, is denoted by A_{nf}.

Similarly [2], [11] we define positive coefficients $\alpha_k < \frac{1}{2}$, where $\alpha_{k+1} \ll \alpha_k$, $k \in \omega \setminus \{0\}$. The coefficient α_1 is the *weight* of Q-arcs, and coefficients α_k, $k \geq 2$, are the *weights* of pairs of vertices connected only by external shortest Q-sequences of length k.

Similarly [2], on the basis of coefficients α_k, we define external *compulsory* furcations a of c-graph, such that an addition of them to the c-graph gives

more than one total value of weights for pairs of vertices (a, b) for all vertices b being nearest followers of a, or for pairs of vertices (c, a) for all vertices c being nearest predecessors of a. A *finite* information on presence of compulsory furcations as well as their positions concerning the others vertices in the c-graph is added in the record W of c-graph and, thus an *expanded* c-graph is defined.

Further we shall mean that c-graphs are expanded as well as an information about all possible (probably empty) predicates Q_g of all elements g of considered group is included in records W. The family of these considered predicates in the c-graph $\mathcal{A}$ will be denoted by $Q_{\mathcal{A}}$.

Remind [13], that a c-graph $\mathcal{A} = \langle A, Q_{\mathcal{A}}, W_{\mathcal{A}}\rangle$ is a *c-subgraph* of c-graph $\mathcal{B} = \langle B, Q_{\mathcal{B}}, W_{\mathcal{B}}\rangle$ and it is denoted by $\mathcal{A} \subseteq_c \mathcal{B}$, if $A \subseteq B$, $Q_{\mathcal{A}} = Q_{\mathcal{B}} \restriction A^2$ and the record $W_{\mathcal{A}}$ coincides with the restriction of record $W_{\mathcal{B}}$ on the set A.

A c-graph $\mathcal{A} = \langle A, Q_{\mathcal{A}}, W_{\mathcal{A}}\rangle$ is a *c-subgraph* of model $\mathcal{M}$, if $A \subseteq M$, $Q_{\mathcal{A}} = Q_{\mathcal{M}} \restriction A^2$ and the record $W_{\mathcal{A}}$ is coordinated with the type $\mathrm{tp}_{\mathcal{M}}(A)$. We write $\mathcal{A} \subseteq_c \mathcal{M}$ if the c-graph $\mathcal{A}$ is a c-subgraph of model $\mathcal{M}$.

An injective map $f : A \to B$ is a *c-embedding* of c-graph $\mathcal{A} = \langle A, Q_{\mathcal{A}}, W_{\mathcal{A}}\rangle$ in c-graph $\mathcal{B} = \langle B, Q_{\mathcal{B}}, W_{\mathcal{B}}\rangle$ (it is denoted by $f : \mathcal{A} \to_c \mathcal{B}$), if f is an embedding of the graph $\mathcal{A} = \langle A, Q_{\mathcal{A}}\rangle$ in the graph $\mathcal{B} = \langle B, Q_{\mathcal{B}}\rangle$ such, that the restriction of the record $W_{\mathcal{B}}$ to the set $f(A)$ coincides with the substitution in the record $W_{\mathcal{A}}$ of elements from $f(A)$ instead of corresponding elements of A.

c-Graphs $\mathcal{A}$ and $\mathcal{B}$ are *c-isomorphic*, if there exists a c-embedding $f : \mathcal{A} \to_c \mathcal{B}$ such that $f(A) = B$. Here the map f is called a *c-isomorphism* between $\mathcal{A}$ and $\mathcal{B}$, and the c-graphs $\mathcal{A}$ and $\mathcal{B}$ are called to be *c-isomorphic copies*.

For given c-graph $\mathcal{A}$ we denote by $\mathrm{cfc}(\mathcal{A})$ a c-graph as the result of addition to $\mathcal{A}$ of all its compulsory furcations. The c-graph $\mathrm{cfc}(\mathcal{A})$ is the cf-*closure* of the c-graph $\mathcal{A}$. If $\mathcal{A}$ doesn't have external compulsory furcations, then $\mathcal{A}$ is cf-*closed*.

Similarly [2] we define a *prerank function* $y(\cdot)$, that for every c-graph $\mathcal{A}$ puts in correspondence some real number by the following rule:

$$y(\mathcal{A}) = 2 \cdot |A_f| + |A_{\mathrm{nf}}| - \sum_{k=1}^{\infty} \alpha_k \cdot e_k(\mathcal{A}), \tag{1}$$

where $e_1(\mathcal{A})$ is the number of arcs in $\mathcal{A}$, $e_k(\mathcal{A})$, $k \geq 2$, is the number of pairs $(a, a') \in A^2$, connected only by external shortest (a, a')-sequences of length k and such, that any (a, a')-sequence of length k does not contain $\mathcal{A}$-external $\mathcal{A}$-compulsory furcations.

A *p-approximation* of the prerank function $y(\cdot)$ is a function $y_p(\cdot)$, that for every c-graph $\mathcal{A}$ puts in correspondence a number by the rule

$$y_p(\mathcal{A}) = 2 \cdot |A_f| + |A_{\mathrm{nf}}| - \sum_{k=1}^{p} \alpha_k \cdot e_k(\mathcal{A}).$$

The definition of sequences of numbers b_n^i and k_p, corresponding to the sequence of coefficients α_k, is given in [11].

For c-graph $\mathcal{A}$ we write $\mathcal{A} \in \mathbf{K}_1$ if $y_1(\mathcal{A}') \geq b_n^1$ for any nonempty c-graph $\mathcal{A}' \subseteq_c \mathrm{cfc}(\mathcal{A})$, where $n = 2 \cdot |A'_f| + |A'_{\mathrm{nf}}|$.

For a c-graph $\mathcal{A}$ we write $\mathcal{A} \in \mathbf{K}_{p+1}$ if $\mathcal{A} \in \mathbf{K}_p$ and $y_p(\mathcal{A}') \geq b_n^p$ for any c-graph $\mathcal{A}' \subseteq_c \mathrm{cfc}(\mathcal{A})$, where $n = 2 \cdot |A'_f| + |A'_{\mathrm{nf}}|$, $k_p \leq n < k_{p+1}$.

Now we put $\mathbf{K}_0 \rightleftharpoons \bigcap\limits_{p=1}^{\infty} \mathbf{K}_p$ and denote by $\mathbf{K}$ the class of all models of polygonometrical theories $T(\mathrm{pm})$, for which every c-subgraph belongs to the class $\mathbf{K}_0$.

Let $\mathcal{A}$ be a c-subgraph of a model (of cf-closed c-subgraph) $\mathcal{M}$ (of a model) belonging to the class $\mathbf{K}$. We say that $\mathcal{A}$ is a *self-sufficient* c-subgraph of $\mathcal{M}$ and write $\mathcal{A} \leqslant_c \mathcal{M}$, if

$$y(\mathcal{A}) + |A_{\mathrm{nf}}| \leq y(\mathcal{B}) + |B_{\mathrm{nf}} \cap A|$$

for any c-graph $\mathcal{B}$, where $\mathcal{A} \subseteq_c \mathcal{B} \subseteq_c \mathcal{M}$. If $\mathcal{A} \leqslant_c \mathcal{M}$ and $\mathcal{M}$ is a c-graph, then $\mathcal{A}$ is called a *strong c-subgraph* of $\mathcal{M}$.

Clearly, the self-sufficiency of c-graph implies its cf-closeness.

Using proposition 1 the direct analysis of c-graphs, included in models of polygonometrical theories, shows that models of countable theories of free polygonometries belong to the class $\mathbf{K}$, and a belonging to the class $\mathbf{K}$ is preserved at transition from models of theory $T(\mathrm{pm})$ to models of theory $T(\mathrm{FPC(pm)})$. Repeating the proof of amalgamation lemma (lemma 3.6 of [2]) and using proposition 3 we establish, that a belonging to the class $\mathbf{K}$ is preserved by transitions from models of theory $T(\mathrm{trm})$ to models of theory $T(\mathrm{trm}_{\equiv\Lambda})$, where Λ is a countable family of the sets being universes of pairwise c-isomorphic self-sufficient c-graphs. Repeating the proof of theorem 7.1 of [1] we check a smallness of theories $T(\mathrm{trm}_{\mathrm{gen}})$, received from countable theories of free polygonometries by countable number of alternations of transitions to free projective closures and to results of type identifications of self-sufficient sets. Similarly to the proof of theorem 4.8 of [2] we show the stability of generic theories $T(\mathrm{trm}_{\mathrm{gen}})$.

As any g_0-acyclic trigonometry $\mathrm{trm}_{\mathrm{gen}}$ on a projective plane generates a powerful digraph with the relation Q_{g_0}, repeating the proof of proposition 3

of [4] for the stable theory $T(\mathrm{trm}_{\mathrm{gen}})$, we get the presence of an infinite own weight for (unique) type $p \in S^1(\varnothing)$.

Thus we get the following

Theorem. *Any countable free polygonometry* pm*, having an g_0-acyclic theory, is embeddable in some generic trigonometry* $\mathrm{trm}_{\mathrm{gen}}$ *on a projective plane, possessing a g_0-acyclic small stable theory having a (unique) type $p \in S^1(\emptyset)$ with an infinite own weight.*

As shown in [14, lemma 5.3], the structure of projective plane is contained in the definable closure of any line and pair of points, not laying on this line. Thus, the structure of projective plane is defined by structures of its lines. As known, the structures of lines in models of trigonometrical theories are polygons over groups with additional predicate structures, connecting various components of polygons. It is shown in [14, theorem 5.5], that structures of lines of projective planes, constructed in [14], are strongly minimal. Using aforesaid remarks in conclusion we present the comparative table of properties of structures of projective planes $\mathcal{P}_B$, $\mathcal{P}_\omega$ and $\mathcal{P}_{iw}$, constructed in [14], [1] and in the present paper accordingly.

Structure	Graph, defining projective plane	Theory	Prerank function	Structure of line
$\mathcal{P}_B$	undirected graph	almost strongly minimal	$y = 2 \cdot u - v$	strongly minimal
$\mathcal{P}_\omega$	digraph	ω-stable	$y = 2 \cdot u - v$	polygon with additional structure
$\mathcal{P}_{iw}$	acyclic digraph	small stable with infinite weight	(1)	polygon with additional structure

References

[1] *Sudoplatov S.V.* Stable trigonometries on a projective plane // Siberian Advances in Mathematics. 2002. V. 12, No. 4. P. 97–124.

[2] *Sudoplatov S.V.* Small stable generic graphs with infinite weight. Poerful digraphs // Matematicheskie trudy (submitted in 2006).

[3] *Herwig B.* Weight ω in stable theories with few types // J. of Symbolic Logic. 1995. V. 60, No. 2. P. 353–373.

[4] *Sudoplatov S.V.* Powerful digraphs // Siberian Math. J. 2007. V. 48, No. 1. P. 205–213.

[5] *Shelah S.* Classification theory and the number of non-isomorphic models / Studies in Logic and the Foundations of Mathematics. Amsterdam: North-Holland. 1990. V. 92.

[6] *Pillay A.* Countable models of stable theories // Proc. Amer. Math. Soc. 1983. V. 89, No. 4. P. 666–672.

[7] *Handbook* of Mathematical Logic, Vol. 1, Model Theory, J. Barwise (ed.) [in Russian]. — Moscow: Nauka, 1982.

[8] *Sudoplatov S.V., Ovchinnikova E.V.* Discrete mathematics [in Russian]. — Moscow: INFRA-M, Novosibirsk: Edition of NGTU, 2007.

[9] *Sudoplatov S.V.* Group polygonometries and related algebraic systems // Contributions to General Algebra 11. Klagenfurt: Verlag Johannes Heyn, 1999. P. 191–210.

[10] *Sudoplatov S.V.* On classification of group polygonometries // Siberian Advances in Mathematics. 2001. V. 11, No. 3. P. 98–125.

[11] *Sudoplatov S.V.* Small stable generic graphs with infinite weight. Bipartite Digraphs // Siberian Advances in Mathematics. 2007. V. 17, No. 1. P. 37–48.

[12] *Sudoplatov S.V.* On group trigonometries on a projective plane // Siberian Math. J. 1995. V. 36, No. 2. P. 419–431.

[13] *Sudoplatov S.V.* Complete theories with finitely many countable models. II // Algebra and logic. 2006. V. 45, No. 3. P. 314–353.

[14] *Baldwin J. T.* An almost strongly minimal non-Desarguesian projective plane // Trans. Amer. Math. Soc. 1994. V. 342, No. 2. P. 695–711.

Abstracts

A.V. Chekhonadskih, A.A. Voevoda. *Codes and adjustment in digraphs of root simplexes of real polynomials.*

This article continues the series of author's papers on coordinatiation root sets of polynomials with real coefficients in complex space. Segments of space R^k which represent single-type sets of roots are considered as vertices of digraph, arcs represent relations of areas and borders of segments of different dimentions. We offer the encoding and some methods of processing of codes for vertices of such digraphs which can be applied to polynomials of arbitrary degree.

V.A. Churkin. *The probability with that a matrix may be diagonalized in finite fields.*

Let $M_n(q)$ be an algebra of all $(n \times n)$-matrices with coefficients in the field of order q and $D_n(q)$ be a subset of matrices that may be diagonalized in $M_n(q)$. We proved that $\lim_{q\to\infty} \frac{|D_n(q)|}{|M_n(q)|} = \frac{1}{n!}$.

I.B. Gorshkov. *On groups with composition quotient group isomorphic to S_7.*

A sufficient condition for group's composition quotient group to be isomorphic to S_7 if described.

E.V. Grachev. *Construction units group of integral ring of cycle group of prime order.*

We are going on the description of the groups of units of integeral group rings of cycle groups. We investigate the structure of the group $V(ZCp)$ in this article. A description of subgroup of finite index in terms of generators and an algorithm for determing are presented. The algorithm is completely prepared to be implemented on the computer.

S.I. Mardaev. *Fixed Points of modal DS-formulas.*

Least fixed points of modal DS-formulas are definable by iteration of the main formula. DS-formulas generalize Sigma-formulas.

E.V. Ovchinnikova. *On extensions of partial isomorphisms of finite polygons on linearly ordered monoids.*

It is shown that any finite polygon over linearly ordered monoid is embeddable in a finite polygon such that any its partial isomorphism is

extensible till an automorphism.

A.G. Pinus. *On algebras with termal $\mathcal{R}$-conservative functions.*
Some general approach to description of algebras for which all $\mathcal{R}$-conservative functions are termal is described. $\mathcal{R}$ stands for any set of relations on algebra.

A.G. Pinus. *On some questions in the theory of ordered sets, model theory and universal algebra.*
In this work the author attempted to collect and remind his colleagues of problems published in a number of his works that are still open (as far as the author knows).

K.N. Ponomarev. *Rigid group rings.*
We define the class of authomorphic rigid group rings over abelian groups and finite fields.

A.M. Popova. *Group of automorphisms of the ring ZS_3.*
We show, that $AutZS_3 = InnZS_3$.

M.A. Rusaleev. *Properties of generalized stable theories.*
The work is devoted to investigation of properties of E^*-stable theories, in particular the properties of (P, A)-stable theories. The theorem proved gives a condition for a theory to be non-(P, A)-stable.

L.A. Sholomov. *The technique of interpretations in the group choice operators design.*
The paper deals with operators $F : R_1^n \to \mathcal{R}_2$ which transform any n-tuple $(r_1, \ldots, r_n)$ of relations of the given class $\mathcal{R}_1$ into a relation r of of the given class $\mathcal{R}_2$. We consider as $\mathcal{R}_1$ and $\mathcal{R}_2$ the classes of linear orders, weak orders, semiorders, interval orders, partial orders, transitive relations, acyclic relations. For all pairs $(\mathcal{R}_1, \mathcal{R}_2)$ of the classes such that $\mathcal{R}_1 \subseteq \mathcal{R}_2$, we bring the explicit form of operators $\mathcal{R}_1^n \to \mathcal{R}_2$. The results are obtained on the basis of the approach which interprets the logical form of operator F as the logical representation of a ordinal binary relation ρ_F on R^n. We prove that if the class $\mathcal{W}$ of weak orders is used as $\mathcal{R}_1$, and $\mathcal{R}_2$ is any universally axiomatizable class of relations, then F maps $\mathcal{W}^n$ into $\mathcal{R}_2$ if and only if $\rho_F \in \mathcal{R}_2$. So the description of operators $\mathcal{W}^n \to \mathcal{R}_2$ amounts to a description of the ordinal relations of $\mathcal{R}_2$. The approach can be adapted to classes $\mathcal{R}_1$ other than $\mathcal{W}$. The article is first that presents in Russian the approach as a whole.

S.V. Sudoplatov. *Small stable trigonometries with infinite weight.*

Grounding on Herwig's generic construction that modifies Hrushovski's construction, we prove that for any countable group G and free countably generated group F_ω there exists a small stable trigonometry of group $G * F_\omega$ on a projective plane induced by an acyclic digraph. As a corollary we show an existence of powerful digraph generating a projective plane and having a small stable theory with an infinite weight.

Contents