

Novosibirsk State Technical University

Algebra and Model Theory 4

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

Novosibirsk
2003

512(06)

Algebra and Model Theory. Collection of papers. Edited by A.G. Pinus and K.N. Ponomarev. Novosibirsk State Technical University, 2003. — 189 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 4

The Fifth Summer School “Intermediate problems of Model Theory and Universal Algebra” was held on 19–23 of June 2003 in the camping center “Erlogol” in Altai mountains. The School was organized by Algebra and Math Logic department of Novosibirsk State Technical University (NSTU). Forty six participants of the conference were researchers, postgraduate and graduate students from Britain, Germany, Kazakhstan and Russia.

The book is composed from some articles of the participants. Organizing Committee of the conference thanks director of Institute of Distant Education Dr. V.Yu. Kalpus for financial support of this edition.

Chairmen of Organizing Committee:

Prof. A.G. Pinus (NSTU, Novosibirsk, Russia),
Prof. K.N. Ponomaryov (NSTU, Novosibirsk, Russia).

Organizing Committee:

Prof V.D. Mazurov (Math. Institute, Novosibirsk, Russia),
Prof E.A. Palyutin (Math. Institute, Novosibirsk, Russia),
Dr. S.V. Sudoplatov (NSTU, Novosibirsk, Russia),
Dr. V.G. Puzarenko (Math. Institute, Novosibirsk, Russia).

Erlogol 2003
INTERMEDIATE PROBLEMS
OF MODEL THEORY AND UNIVERSAL ALGEBRA
(JUNE, 19–23)

19 June. Chairman Robin Knight

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

On decidable linearly ordered groups.

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

On homology theory over p-adic numbers.

N.Ya. Medvedev (*Barnaul, Russia*).

Ideals in free vector lattices and free abelian l -groups.

Chairman Bektur Baizhanov

V. Verbovski (*Almaty, Kazakhstan*).

Some questions on the Hrushovski's geometry.

E.V. Orekhova (*Moscow, Russia*).

On an analogue of Slupetski's theorem about implicit expressibility in the many-valued logic.

D.Yu. Vlasov (*Novosibirsk, Russia*).

Structure of algebraic systems with a finite set of theories of infinite subsystems.

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

Recognition of finite simple groups by their spectrums.

20 June. Chairman V.M. Kopytov

R.W. Knight (*Oxford, Great Britain*).

On Vaught conjecture.

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

Classification of complete theories having a finite number of countable models.

V.M. Levchuk (*Krasnoyarsk, Russia*).

Some questions in the theory of Chevalley groups and K -theories.

Chairman V.G. Puzarenko

P.S. Kolesnikov (*Novosibirsk, Russia*).

On the structure of pseudoalgebras.

O. Isaeva (*Barnaul, Russia*).

On varieties of m -groups.

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

Fixed points in temporal models.

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

On groups represented by matrices over fields of arbitrary characteristic.

A.N. Koryukin (*Novosibirsk, Russia*).

On Gröbner-Shirshov bases of simple finite dimensional Lie algebras.

21 June. Chairman N.Ya. Medvedev

B. Baizhanov (*Almaty, Kazakhstan*).

On expansions in stable theories.

A.G. Pinus, S.V. Zhurkov (*Novosibirsk, Russia*).

Scales of computational potentials of finite algebras.

P. Roquette (*Heidelberg, Germany*).

On the problem of A. Weil.

Chairman S.F. Vinokurov

A.G. Pinus (*Novosibirsk, Russia*).

On proper automorphisms of universal algebras.

A.M. Popova, E.N. Poroshenko (*Novosibirsk, Russia*).

Multiplicative groups of integral group rings of finite groups.

N. Bayanova, N.Ya. Medvedev (*Barnaul, Russia*).

Inversing automorphisms of free l -groups.

O. Listova (*Krasnoyarsk, Russia*).

Geometric interpretation of Mathieu group.

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

On inner definability in hereditary finite superstructures.

23 June. Chairman V.M. Levchuk

N.A. Peryazev, V.I. Panteleev (*Irkutsk, Russia*).

Generalized interpretation of variables.

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

On invariants in the theory of computability over admissible sets.

V. Bogdanov (*Novosibirsk, Russia*).

On categorical algebras in HF-logic.

D. Tusupov (*Taras, Kazakhstan*).

Generalized computability and hereditarily computably enumerable relations.

A.A. Voevoda, A.V. Chekhonadskikh (*Novosibirsk, Russia*).

Optimizing problems in the polynomial algebra with a poor set of parameters.

E.N. Poroshenko (*Novosibirsk, Russia*).

On basis of Leibnitz algebras.

НЕОРТОГОНАЛЬНОСТЬ 1-ТИПОВ В СЛАБО О-МИНИМАЛЬНЫХ СТРУКТУРАХ КОНЕЧНОЙ ГЛУБИНЫ

Б. Байжанов, В. Вербовский, Г. Туреханова

Институт проблем информатики и управления,
Министерство образования и науки,
ул. Пушкина 125,
Алматы 480100, Казахстан
e-mail: {baizhanov,vvv,guljan}@ipic.kz

1 Введение

Определение 1.1 (Dickmann). Линейно упорядоченная структура $M = (M, <, \dots)$ называется *слабо о-минимальной*, если любое определимое с параметрами подмножество M равно некоторому конечному объединению выпуклых относительно порядка $<$ множеств. Теория называется *слабо о-минимальной*, если любая ее модель слабо о-минимальна.

Пусть M — произвольная упорядоченная структура, A и B произвольные подмножества для M . Введем следующие обозначения:

$$\begin{aligned} A^+ &\doteq \{x \in M : \text{для всех } a \in A \text{ верно, что } a < x\} \\ A^- &\doteq \{x \in M : \text{для всех } a \in A \text{ верно, что } x < a\} \\ A \leq B &\doteq B^+ \subseteq A^+ \end{aligned}$$

Пусть $\Phi(x, y)$ — M -определимая формула. Тогда согласно с введенными выше обозначениями мы можем написать $\Phi(M, y_1) \geq \Phi(M, y_2)$, то есть мы сравниваем супремумы двух множеств. Обычными средствами мы можем определить строгое неравенство и равенство двух формульных множеств.

Определение 1.2. Если $E(y, z)$ — отношение эквивалентности с выпуклыми классами на множестве I , то формула $\Phi(x, y)$ *строго возрастает* на множестве I/E по y , если $\forall y \forall z [y, z \in I \wedge \neg E(y, z) \wedge y < z \rightarrow \Phi(M, y) <$

$\Phi(M, z)]$. Строгое убывание и постоянство формулы определяются аналогичным образом.

Назовем формулу *строго монотонной*, если она строго возрастает, либо строго убывает.

Скажем, что формула *монотонна* на множестве I , если существует отношение эквивалентности E на I с выпуклыми классами, такое что данная формула строго монотонна на I/E и постоянна на каждом классе эквивалентности E (в частности, E может быть и отношением равенства).

Положим $\text{dom}(\Phi(M, y)) = \{y \in M : M \models (\exists x)\Phi(x, y)\}$

Определение 1.3. [6] Пусть M — линейно упорядоченная структура, $\Phi(x, y)$ — M -определимая формула, $I \subset \text{dom}(\Phi(M, y))$. Говорят, что Φ *вполне хорошая* на множестве I , если выполняется одно из трех нижеперечисленных условий:

1. $\forall y \in I$ существует бесконечный интервал $J \subset I$, такой что $y \in J$ и Φ строго возрастает на J . В этом случае говорят, что Φ *локально возрастает* на I .
2. $\forall y \in I$ существует бесконечный интервал $J \subset I$, такой что $y \in J$ и Φ строго убывает на J . В этом случае говорят, что Φ *локально убывает* на I .
3. $\forall y \in I$ существует бесконечный интервал $J \subset I$, такой что $y \in J$ и Φ постоянна на J , то есть $\forall y_1, y_2 \in J, \Phi(M, y_1)^+ = \Phi(M, y_2)^+$. В этом случае говорят, что Φ *локально постоянна* на I .

Определение 1.4. [8] Пусть Φ и I будут как в определении 1.3. Определим некоторые формулы и понятия по шагам индукции

Шаг 0 $E_0(x, y) \doteq x = y$, $\Phi^{(0)}(x, y) \doteq \Phi(x, y)$. Будем говорить, что формула Φ *0-вполне хорошая* на I , если она либо строго возрастает, либо строго убывает, либо постоянна на I .

Шаг 1

$$\begin{aligned} E_1(z, y) &\doteq E_0(z, y) \vee [[z < y \rightarrow \Phi \upharpoonright [z, y] \text{ строго монотонна или} \\ &\text{постоянна}] \wedge [y < z \rightarrow \Phi \upharpoonright [y, z] \text{ строго монотонна или постоянна}] \\ \Phi^{(1)}(x, y) &\doteq \Phi(x, y) \end{aligned}$$

Будем говорить, что формула Φ *1-вполне хорошая*, если она вполне хорошая в смысле Определения 1.3 и при любом элементе $y \in I$ класс

эквивалентности $E_1(I, y)$ не имеет ни максимума, ни минимума, а само множество I состоит из бесконечного числа классов эквивалентности E_1 .

Шаг n , $n > 0$

$$\begin{aligned} E_n(z, y) &\doteq E_{n-1}(z, y) \vee \\ &\vee \quad [[z < y \wedge \neg E_{n-1}(z, y) \rightarrow \Phi^{(n)} \upharpoonright [z, y] / E_{n-1} \text{ строго монотонна}] \wedge \\ &\quad \wedge \quad [y < z \wedge \neg E_{n-1}(z, y) \rightarrow \Phi^{(n)} \upharpoonright [y, z] / E_{n-1} \text{ строго монотонна}]] \\ \Phi^{(n)}(x, y) &\doteq \exists z [E_{n-1}(y, z) \wedge \Phi(x, z)] \end{aligned}$$

Будем говорить, что Φ n -*вполне хорошая* на I , если выполняется следующее:

1. $\forall z \forall y \forall t [\Phi(M, z) = \Phi(M, y) \wedge z < t < y \rightarrow \Phi(M, z) = \Phi(M, t)]$
2. $\Phi^{(n)}$ 1-*вполне хорошая* на I/E_{n-1} .
3. $(\forall y \in I) E_n(I, y)/E_{n-1}$ не имеет ни максимума ни минимума.
4. $|I/E_n| \geq \omega$.

Заметим, что E_n является отношением эквивалентности на I .

Определение 1.5. [8] Пусть формула Φ и множество I будут как в определении 1.3. Скажем, что Φ *сильно 0-вполне хорошая* на I , если она 0-*вполне хорошая* на I . Скажем, что Φ *сильно n -вполне хорошая* на I , если она n -*вполне хорошая* на I и $\Phi^{(n)}$ *сильно 0-вполне хорошая* на I/E_n . Это число n назовем *глубиной формулы Φ на I* . Скажем, что Φ *сильно вполне хорошая*, если она *сильно n -вполне хорошая* для некоторого $n < \omega$.

Определение 1.6. [6] Пусть M — слабо о-минимальная структура. Будем говорить, что M обладает *монотонностью*, если выполняется следующее: какова бы ни была формула $\Phi(x, y, \bar{a})$, $\bar{a} \in M$, существует $m \in \omega$ и разбиение $\text{dom}(\Phi(M, y, \bar{a}))$ на определимые множества $X, I_1, \dots, I_m$, такие что X конечно, каждое I_i выпукло, и на каждом I_i -том формула $\Phi(x, y, \bar{a})$ *вполне хорошая*.

Определение 1.7. Пусть M — слабо о-минимальная структура. Будем говорить, что M обладает *n -монотонностью*, если выполняется следующее: какова бы ни была формула $\Phi(x, y, \bar{a})$, $\bar{a} \in M$, существует m и разбиение $\text{dom}(\Phi(M, y, \bar{a}))$ на определимые множества $X, I_1, \dots, I_m$, такие что X конечно, каждое I_i выпукло, и на каждом I_i формула $\Phi(x, y, \bar{a})$ n -*вполне хорошая*.

Определение 1.8. [8] Пусть M — слабо о-минимальная структура. Будем говорить, что M обладает *сильной монотонностью*, если выполняется следующее: какова бы ни была формула $\Phi(x, y, \bar{a})$, $\bar{a} \in M$, существует m и разбиение $\text{dom}(\Phi(M, y, \bar{a}))$ на определимые множества $X, I_1, \dots, I_m$, такие что X конечно, каждое I_i выпукло, и на каждом I_i формула $\Phi(x, y, \bar{a})$ сильно вполне хорошая.

Определение 1.9. [8] Пусть M — слабо о-минимальная структура. Скажем, что M имеет *конечную глубину*, если выполняется следующее: для каждой формулы $\Phi(x, y, \bar{z})$ существует $n \in \omega$, такое что для любого $\bar{a} \in M^{l(\bar{z})}$ и для любого выпуклого множества $I \subset \text{dom}(\Phi(M, y, \bar{a}))$, такого что $\Phi(M, y, \bar{a})$ сильно вполне хорошая на I , глубина $\Phi(M, y, \bar{a})$ на I не превосходит n .

Напомним, что в работе [6] было доказано, что если все модели $\text{Th}(M)$ суть слабо о-минимальны, то M обладает монотонностью. Эта теорема была обобщена в статье [8]: относительно тех же посылок было показано, что M обладает сильной монотонностью и конечной глубиной. В той же статье было доказано, что условие слабой о-минимальности теории нельзя ослабить до условия слабой о-минимальности структуры. В другом направлении теорема о монотонности [6] была обобщена Арефьевым в работе [1]:

Теорема 1.10. *Слабо о-минимальная структура обладает монотонностью.*

2 Ортогональность 1-типов

Далее M будет слабо о-минимальной структурой конечной глубины, A — некоторым подмножеством для M , N — $|M|^+$ -насыщенное элементарное расширение модели M .

Определение 2.1. Пусть p и $q \in S_1(A)$. Будем говорить, что тип p слабо ортогонален типу q , и записывать это как $p \perp^w q$, если $p(x) \cup q(y)$ определяет полный 2-тип.

Заметим, что согласно результатам из [7], $p(N)$ — выпуклое множество.

Определение 2.2. Будем говорить, что формула $H(x)$ расщепляет выпуклое множество B (не обязательно формульное), если

$$\neg H(N) = H(N)^+, \quad B \cap H(N) \neq \emptyset \text{ и } B \cap \neg H(N) \neq \emptyset.$$

Теорема 2.3. Пусть M будет слабо o -минимальной структурой конечной глубины, A — некоторым подмножеством для M , $N = |M|^+$ — насыщенное элементарное расширение модели M . Пусть неалгебраические типы p и $r \in S_1(A)$ не слабо ортогональны, и пусть существует A -определимая формула $H(x, y)$, такая что для некоторого (эквивалентно, для всех) $\beta \in r(N)$, $H(x, \beta)$ расщепляет $p(N)$. Тогда существует A -определимая формула $K(x, y)$, такая что:

1. $K(x, y)$ монотонна по y на $\Theta(N)$, $\Theta(y) \in r(y)$;
2. $K(x, y)$ монотонна по x на $\mu(N)$, $\mu(x) \in p(x)$;
3. для любого $\beta \in r(N)$ формула $K(x, \beta)$ расщепляет $p(N)$;
4. для любого $\alpha \in p(N)$ формула $K(\alpha, y)$ расщепляет $r(N)$.

Доказательство. В силу условий теоремы имеем A -определимую формулу $H(x, y)$, такую что для некоторого $\beta \in r(N)$ формула $H(x, \beta)$ расщепляет $p(N)$, то есть существуют $\alpha_1, \alpha_2 \in p(N)$ такие что

$$N \models H(\alpha_1, \beta) \wedge \neg H(\alpha_2, \beta) \wedge \alpha_1 < \alpha_2$$

По теореме 1.10 существует разбиение M на A -определимые подмножества $X, I_1, \dots, I_n$, такое что множество X конечно, и на каждом I_j -том формула $H(x, y)$ вполне хорошая. Тогда $r(N) \subseteq I_j$ для некоторого j .

Возьмем отношение эквивалентности E_1 с выпуклыми классами из определения 1.4 для формула $H(x, y)$. Заметим, что это отношение эквивалентности A -определимо, поэтому если пересечение некоторого E_1 -класса с $r(N)$ не пусто, то либо данный класс содержит $r(N)$, либо строго содержится в $r(N)$.

Если некоторый E_1 -класс содержит $r(N)$, то $H(x, y)$ строго монотонна на $r(N)$. Заметим, что $H(x, y)$ не может быть постоянной по y на $r(N)$. Действительно, в противном случае существует A -определимая формула $\mu(y)$ из типа r , на которой формула $H(x, y)$ постоянна по y . Но тогда верно:

$$N \models \forall y(\mu(y) \rightarrow H(\alpha_1, y)) \wedge \forall y(\mu(y) \rightarrow \neg H(\alpha_2, y))$$

что противоречит определению типа p . Тогда она либо строго возрастает, либо строго убывает по y на $r(N)$. Так как E_1 — A -определимое отношение эквивалентности и $r \in S_1(A)$, то E_1 -класс, содержащий $r(N)$, тоже A -определим, поэтому в качестве Θ мы можем взять данный E_1 -класс, а в качестве $K = H$, что доказывает пункты (1) и (3) теоремы.

Значит, можно предположить, что $E_1(N, \beta) \subset r(N)$.

Пусть $H_1(x, y) \doteq \exists z(E_1(z, y) \wedge H(x, z))$. Рассмотрим поведение формулы $H(x, y)$ или, что тоже самое, формулы $H_1(x, y)$, на I_j/E_1 . Определим структуру $M_1 \doteq (I_j/E_1, <, P^2)$, где порядок наследуется из структуры M , а $P(y_1, y_2) \doteq H(M, y_1) < H(M, y_2)$. Так как M_1 интерпретируется в M , она слабо о-минимальна. Тогда по теореме 1.10 существует разбиение M_1 на определимые подмножества $X^1, I_1^1, \dots, I_n^1$, такое что множество X^1 конечно, и на каждом I_j^1 -том формула $P(x, y)$ вполне хорошая. Тогда $r(N)/E_1 \subseteq I_{j_1}^1$ для некоторого j_1 . Тогда по определению, $H(x, y)$ 2-вполне хорошая на прообразе множества $I_{j_1}^1$ в M .

Возьмем отношение эквивалентности E_2 с выпуклыми классами из определения 1.4 для формулы $H(x, y)$. Заметим, что это отношение эквивалентности A -определимо, поэтому если пересечение некоторого E_1 -класса с $r(N)$ не пусто, то либо данный класс содержит $r(N)$, либо строго содержится в $r(N)$.

Если некоторый E_2 -класс содержит $r(N)$, то $H_1(x, y)$ строго монотонна на $r(N)/E_1$ и постоянна на классах E_1 , что доказывает пункты (1) и (3) теоремы, если в качестве Θ взять E_2 -класс, содержащий $r(N)$, а в качестве K — H_1 .

В противном случае, рассмотрим $H_1(x, y)$ в качестве $H(x, y)$ и повторим рассуждения (для модели M_1).

В силу конечности глубины формулы $H(x, y)$, данный процесс конечен, следовательно, для некоторого $k < \omega$ некоторый класс отношения эквивалентности E_k будет содержать $r(N)$, формула $H_{k-1}(x, y) \doteq \exists z(E_{k-1}(y, z) \wedge H(x, z))$ будет строго монотонной на $r(N)/E_{k-1}$ и постоянной на E_{k-1} -классах, что доказывает пункты (1) и (3) теоремы, если в качестве Θ взять E_k -класс, содержащий $r(N)$, а в качестве K — H_{k-1} .

В качестве $\mu(x)$ возьмем формулу

$$\exists z_1, z_2(\Theta(z_1) \wedge \Theta(z_2) \wedge K(x, z_1) \wedge \neg K(x, z_2))$$

Формула $K(x, y)$ монотонна по x на $\mu(N)$ в силу общих принципов монотонности функции и ее обратной. Таким образом, условия (2) и (4) теоремы выполнены.

Отметим, что выбранное k является числом изменений направлений монотонности для формулы $H(x, y)$ на $r(N)/E_i$ и равно "глубине формулы $H(x, y)$ на $r(N)$ ", определенной в конце доказательства теоремы 33 [2], страница 1398. $\square$

Заметим, что для модели слабо о-минимальной теории для двух не слабо ортогональных 1-типов всегда существует расщепляющая формула $H(x, y)$ из условий теоремы (показано в теореме 33, [2]). В работе [8]

доказано, что модель слабо о-минимальной теории обладает конечной глубиной. Отсюда получаем

Следствие 2.4 (Теорема 33, [2]). Пусть A является некоторым подмножеством $|A|^+$ -насыщенной модели N слабо о-минимальной теории. Пусть неалгебраические типы p и $r \in S_1(A)$ не слабо ортогональны. Тогда существует A -определимая формула $K(x, y)$, такая что:

1. $K(x, y)$ монотонна по y на $\Theta(N)$, $\Theta(y) \in r(y)$;
2. $K(x, y)$ монотонна по x на $\mu(N)$, $\mu(x) \in p(x)$;
3. для любого $\beta \in r(N)$ формула $K(x, \beta)$ расщепляет $p(N)$;
4. для любого $\alpha \in p(N)$ формула $K(\alpha, y)$ расщепляет $r(N)$.

Из работы [8] следует, что существуют слабо о-минимальные структуры, не являющиеся моделью слабо о-минимальной теории, имеющие любую наперед заданную конечную глубину. Таким образом данная теорема является строгим обобщением теоремы 33, [2].

Многократное применение теоремы 1.10 к слабо о-минимальным моделям M_i , введенным в доказательстве теоремы 2.3, позволяет сформулировать

Следствие 2.5. Слабо о-минимальная структура обладает n -монотонностью для любого наперед заданного n .

Список литературы

- [1] Р. Д. Арефьев, *О свойстве монотонности слабо о-минимальных моделей*, **Алгебра и теория моделей**, сборник научных трудов под редакцией А. Г. Пинуса и К. Н. Пономарева, Новосибирск, 1997, стр. 8 – 13.
- [2] B. Baizhanov, *Expansion of a model of a weakly o-minimal theory by a family of unary predicates*, **The Journal of Symbolic Logic**, 66 (2001), стр. 1382 – 1414.
- [3] B. Baizhanov, *Classification of one-types in weakly o-minimal theories and its corollaries*, preprint, 1996.
- [4] B. Baizhanov, *Orthogonality of one-types in weakly o-minimal theories*, **Алгебра и теория моделей**, сборник научных трудов под редакцией А. Г. Пинуса и К. Н. Пономарева, Новосибирск, 1999, стр. 5–28.

- [5] M. Dickmann, *Elimination of quantifiers for ordered valuation rings*, **Proceedings 3rd Easter Model Theory Conference at Gross Koris**, Berlin, 1985.
- [6] D. Macpherson, D. Marker, Ch. Steinhorn, *Weakly o-minimal structures and real closed fields*, **Transaction of American Mathematical Society** 352 (2000), стр. 5435–5483.
- [7] B. Kulpeshov, *Weakly o-minimal structures and some of their properties*, **The Journal of Symbolic Logic**, 63 (1998), стр. 1511 – 1528.
- [8] V. Verbovskiy, *On formula depth of weakly o-minimal structures*, **Алгебра и теория моделей**, сборник научных трудов под редакцией А. Г. Пинуса и К. Н. Пономарева, Новосибирск, 1997, стр. 209 – 224.

МАТРИЧНАЯ ПРЕДСТАВИМОСТЬ И СТРОЕНИЕ ГРУПП

Брюханов О.В.

Сибирский университет потребительской кооперации,
г. Новосибирск

В статье исследуется вопрос о матричной представимости нильпотентных произведений $A(n)B$, $n \geq 2$, линейных групп A , B и изучается строение абстрактных бесконечных групп представимых матрицами над полями различных характеристик.

В теореме 1.1 дан критерий матричной представимости над полями произвольной характеристики нильпотентных произведений $A(n)B$, $n \geq 2$ конечнорожденных групп A и B . В теореме 1.2 вопрос о матричной представимости нильпотентного произведения $A(n)B$, $n \geq 2$ линейных групп A и B сведен к матричной представимости нильпотентной группы, специально построенной по данному произведению $A(n)B$. В качестве следствия теоремы 1.2, показано, что нильпотентное произведение $F(X)(n)F(Y)$, $n \geq 2$ свободных групп $F(X)$ и $F(Y)$ представимо матрицами над полем нулевой характеристики и не представимо матрицами ни над каким полем положительной характеристики.

В теореме 2.4 доказано, что группа G , не содержащая свободных подгрупп, представима матрицами над полями различных характеристик p и q тогда и только тогда, когда она почти абелева, при этом периодическая часть τA , нужной абелевой подгруппы A , конечного ранга, а примарные компоненты $\tau_p A$, $\tau_q A$ конечны.

§ 1 Матричная представимость нильпотентных произведений групп.

Следуя О.Н.Головину [2], n -ым нильпотентным произведением групп A и B называют фактор-группу

$$A(n)B = A * B / [A, B] \cap \gamma_{n+1}(A * B),$$

где $n \geq 2$, $A * B$ — свободное произведение групп A и B , $[A, B]$ — взаимный коммутант подгрупп A и B , $\gamma_m(G)$ — m -й централ группы G .

Перечислим ряд стандартных свойств нильпотентных произведений групп (см. [2]).

Свойство 1.1. Группы A и B изоморфно вложены в своё нильпотентное произведение $A(n)B$, $n \geq 2$ и порождают его как группу.

Свойство 1.2. В нильпотентном произведении $G = A(n)B$ пересечения $A \cap B^G$, $A^G \cap B$ тривиальны.

Свойство 1.3. Всякий элемент из нильпотентного произведения $A(n)B$ однозначно представим в виде произведения $abw(g)$, где $a \in A$, $b \in B$, $w(g) \in [A, B]$.

Свойство 1.4. Если нормальные подгруппы $A_0 \trianglelefteq A$, $B_0 \trianglelefteq B$ нормальны во всей группе $A(n)B$, то гомоморфизмы групп $A \rightarrow A/A_0$, $B \rightarrow B/B_0$ продолжаются до гомоморфизма нильпотентных произведений $A(n)B \rightarrow A/A_0(n)B/B_0$ с ядром $A_0 \cdot B_0$, при этом $A_0B_0 \cap [A, B] = e$.

Приведем несколько вспомогательных лемм.

Лемма 1.1. Пусть подгруппы $A, B \leq G$ такие, что $[A, B] \cap \gamma_{n+1}(G) = e$.

а) Если для любых $a \in A$, $b \in B$ выполнено тождество $[a^k, b] = e$, то $[a, b]^{k^{n-1}} = e$;

б) Если для любых $a \in A$, $b \in B$ выполнено тождество $[a, b]^k = e$, то $[a^{k^{n-1}}, b] = e$.

Доказательство. Докажем индукцией по n . При $n = 1$ утверждение тривиально. Пусть для всех $n < s$ утверждения а) и б) доказаны.

а) Из тождества $[a^k, b] = e$ следует, что $[a, b]^{k^{s-2}} \in [A, B] \cap \gamma_s(G)$. Так как $[A, B] \cap \gamma_{s+1}(G) = e$, то группа $[A, B] \cap \gamma_s(G)$ порождается коммутаторами вида $[x_1, x_2, \dots, x_s]$, где $x_i \in A \cup B$ и не все x_i из одной подгруппы A или B . Далее $[a, b]^{k^{s-1}} = ([a, b]^{k^{s-2}})^k$ и, следовательно, является произведением k -ых степеней коммутаторов вида $[x_1, x_2, \dots, x_s]$. в силу стандартных коммутаторных тождеств выполняются равенства $[x_1, x_2, \dots, x_s]^k = [[x_1, \dots, x_i]^k, x_{i+1}, \dots, x_s] = [x_1, \dots, x_i^k, x_{i+1}, \dots, x_s]$, $1 \leq i \leq s$ при этом всегда можно выбрать индекс i таким, что все $x_1, \dots, x_i$ из одной подгруппы A или B , а x_{i+1} из другой. Таким образом каждый коммутатор из нашего произведения имеет вид $[[a^k, b], x_{i+2}, \dots, x_s]$ или $[b, a^k, x_{i+2}, \dots, x_s]$ и следовательно равен единице.

б) Из тождества $[a, b]^k = e$ следует, что $[a^{k^{s-2}}, b] \in [A, B] \cap \gamma_s(G)$. Так как $[A, B] \cap \gamma_{s+1}(G) = e$, то $[a^{k^{s-1}}, b] = [(a^{k^{s-2}})^k, b] = [a^{k^{s-2}}, b]^k = e$.

Лемма 1.1 доказана.

Обозначим через $C_X(Y)$ централизатор множества Y в множестве X .

Лемма 1.2. В нильпотентном произведении $A(n)B$ групп A и B выполнены следующие утверждения:

а) $\gamma_n(A) \trianglelefteq C_A(B)$, $\gamma_n(B) \trianglelefteq C_B(A)$;

б) $C_A(B), C_B(A) \leq A(n)B$;

в) $C_A(B) \cdot C_B(A) \cap [A, B] = e$.

Доказательство. Утверждение а) очевидно, так как в свободном произведении выполнены включения $[\gamma_n(A), B] \subset [A, B] \cap \gamma_{n+1}(A * B)$ и $[\gamma_n(B), A] \subset [A, B] \cap \gamma_{n+1}(A * B)$.

б) Заметим, что любой автоморфизм групп A и B индуцирует автоморфизм свободного произведения $A * B$. Далее по определению $[C_A(B), B], [C_B(A), A] \leq [A, B] \cap \gamma_{n+1}(A * B)$. Группа $[A, B] \cap \gamma_{n+1}(A * B)$ допустима относительно всех автоморфизмов индуцированных автоморфизмами на сомножителях A и B . Таким образом, если $[a, b] \in [A, B] \cap \gamma_{n+1}(A * B)$, то $[a^\varphi, b^\psi] \in [A, B] \cap \gamma_{n+1}(A * B)$ для всех $\varphi \in \text{Aut } A$, $\psi \in \text{Aut } B$, группы $C_A(B)$ и $C_B(A)$ являются автоморфно допустимыми подгруппами групп A и B соответственно.

в) Непосредственно следует из утверждения б) и свойства 1.4.

Лемма 1.2 доказана.

Будем обозначать фактор-группы $A/C_A(B)$ и $B/C_B(A)$ через $\bar{A}$ и $\bar{B}$ соответственно.

Лемма 1.3. Нильпотентное произведение $A(n)B$ изоморфно вкладывается в прямое произведение групп $A \times B$ и $\bar{A}(n)\bar{B}$.

Доказательство. Следует из Леммы 1.2 и свойства 1.4.

Лемма 1.4. Пусть G — нильпотентная подгруппа ступени n из группы $GL_m(P)$, P — поле.

а) Если $\text{char } P = 0$, то любой элемент $g \in G$, попадающий в центр $\mathbb{Z}(G)$ группы G в некоторой степени k , попадает в $\mathbb{Z}(G)$ в фиксированной степени $l(m, n)$ зависящей только от m и n .

б) Если $\text{char } P = p > 0$, то любой элемент $g \in G$ попадает в центр $\mathbb{Z}(G)$ группы G в некоторой фиксированной степени $l(m, n, p)$, зависящей только от m, n, p .

Доказательство. Из теоремы А.Д. Супруненко (см. [6], теорема 49.3.2) о почти центральности вполне приводимых нильпотентных групп следует, что над алгебраическим замыканием поля P группа G содержит триангулируемую подгруппу конечного индекса не больше $\mu(m, n) = m^{(n+1)(m-1)}$. Тогда имеем вложение $[G^{\mu(m, n)}, G^{\mu(m, n)}] \hookrightarrow UT_m(\bar{P})$, где $\bar{P}$ — алгебраическое замыкание поля P .

а) Пусть $g_0^k \in \mathbb{Z}(G)$, тогда из тождества $[\langle g_0 \rangle^k, G] = e$ по лемме 1.1 (а) получаем тождество $[\langle g_0 \rangle, G]^{k^{n-1}} = e$. Следовательно $[\langle g_0 \rangle^{\mu(m, n)}, G^{\mu(m, n)}] = e$ и снова по лемме 1.1 получаем $[\langle g_0 \rangle^{\mu(m, n)^{(n-1)^2+1}}, G] = e$ или $g_0^{\mu(m, n)^{(n-1)^2+1}} \in \mathbb{Z}(G)$, $l(m, n) = \mu(m, n)^{(n-1)^2+1} = m^{(m-1)(n+1)((n-1)^2+1)}$.

б) Для любых $g_1, g_2 \in G$ имеем равенство $[\langle g_1 \rangle^{\mu(m, n)}, \langle g_2 \rangle^{\mu(m, n)}]^{p^{m-1}} = e$.

Рассуждениями из леммы 1.1 получаем

$$[\langle g_1 \rangle^{p^{(m-1)(n-1)^3} \mu(m,n)(n-1)^2+1}, \langle g_2 \rangle] = e, \text{ или}$$

$$g_1^{p^{(m-1)(n-1)^3} \mu(m,n)(n-1)^2+1} \in \mathbb{Z}(G), l(m, n, p) = p^{(m-1)(n-1)^3} m^{(m-1)(n+1)((n-1)^2+1)}.$$

Лемма 1.4 доказана.

Как следствие из леммы 1.4 получаем, что над полями нулевой характеристики фактор по центру линейной нильпотентной группы обладает конечной периодической частью, а над полями положительной характеристики фактор по центру нильпотентной группы будет ограниченного периода, т.е. почти унитарным.

Лемма 1.5. Пусть группа $A(n)B$ представима матрицами степени m над полем P .

а) Если $\text{char } P = 0$, то периодические части $\bar{\tau A}$, $\bar{\tau B}$ будут группами ограниченного периода $l(m, n)$

б) Если $\text{char } P = p > 0$, то группы $\bar{A}$, $\bar{B}$ будут периодическими группами ограниченного периода $l(n, m, p)$.

Доказательство. а) Пусть $a_0^k \in C_A(B)$, тогда в нильпотентной группе $\text{gr}\{a_0, b\}$, $b \in B$, выполнено включение $a_0^k \in \mathbb{Z}(\text{gr}\{a_0, b\})$. По лемме 1.4 получаем, что $a_0^{l(m,n)} \in \mathbb{Z}(\text{gr}\{a_0, b\})$ или $a_0^{l(m,n)} \in C_A(B)$.

б) Пусть $a \in A$, $b \in B$. В нильпотентной группе $\text{gr}\{a_0, b\}$ по лемме 1.4 выполнены включения $a^{l(m,n,p)} \in \mathbb{Z}(\text{gr}\{a_0, b\})$, $b^{l(m,n,p)} \in \mathbb{Z}(\text{gr}\{a_0, b\})$ и так как a и b — произвольные элементы получаем $a^{l(m,n,p)} \in C_A(B)$, $b^{l(m,n,p)} \in C_B(A)$.

Теорема 1.1. Пусть конечно A , B — порожденные группы матриц над полем P .

а) Если $\text{char } P = 0$, то нильпотентное произведение $A(n)B$ представимо матрицами над полем P .

б) Если $\text{char } P = p > 0$, то нильпотентное произведение $A(n)B$ представимо матрицами над полем характеристики p тогда и только тогда, когда индексы $|A : C_A(B)|$, $|B : C_B(A)|$ конечны.

Доказательство. а) По лемме 1.3 нильпотентное произведение $A(n)B$ изоморфно вкладывается в прямое произведение сумму групп $A \times B$ и $\bar{A}(n)\bar{B}$. Группа $\bar{A}(n)\bar{B}$ конечно порождена и нильпотентна, поэтому представима матрицами (см. [2]). Таким образом всё прямое произведение $A \times B \times \bar{A}(n)\bar{B}$ представляется матрицами над полем P .

б) Заметим сначала, что нильпотентное произведение конечных групп также конечно.

Пусть группа $A(n)B$ представима матрицами, тогда по лемме 1.5 (б) группы $\bar{A}$, $\bar{B}$ периодические ограниченного периода. С другой стороны, группы $\bar{A}$, $\bar{B}$ конечно порождены по условию и нильпотентны по лемме 1.2 (а), а значит конечны, т.е. $|A : C_A(B)|, |B : C_B(A)| < \infty$.

В обратную сторону, если группы $\bar{A}$, $\bar{B}$ конечны, то конечно их нильпотентное произведение $\bar{A}(n)\bar{B}$. Опять получаем, что группа $A \times B \times \bar{A}(n)\bar{B}$ представима матрицами над полем P , а лемма 1.3 позволяет сделать это заключение и для группы $A(n)B$.

Теперь изложим подробнее метод расщепляемых координат Ю.И. Мерзлякова (см.[5],[6]). Матричное представление группы строится, если удастся задать точное действие этой группы в некотором конечномерном векторном пространстве. Естественным полигоном для этого служит алгебра функций действующих из группы G , для которой строится матричное представление, в некоторое поле K . Пусть $A(G, K)$ — алгебра всех K -значных функций на группе G . Если $f \in A(G, K)$, $x \in G$, то пусть

$$f^x(y) = f(xy), \quad y \in G.$$

Легко видеть, что эта формула задает действие группы G на алгебре $A(G, K)$, так как $f^{gh} = (f^g)^h$ и $f^e = f$, где e — единица группы G , $g, h \in G$.

Определение 1.1. Говорят, что на группе G заданы K -значные расщепляемые координаты $t_1, \dots, t_d$, если для них выполнены следующие равенства:

$$t_\alpha(xy) = \sum_{\beta=1}^l f_{\alpha\beta}(x)h_\beta(y), \quad x, y \in G, \quad 1 \leq \alpha \leq d,$$

где $f_{\alpha\beta}, h_\beta$ — некоторые K -значные функции на группе G .

В случае, когда на группе G заданы K -значные расщепляемые координаты $t_1, \dots, t_d$ видно, что векторное пространство V , порожденное G -орбитой множества координатных функций $\{t_\alpha\}$, будет конечномерным, так как лежит в линейной K -оболочке конечного множества $\{h_\beta\}$. Пусть $v_1, \dots, v_n$ — база V над K . Тогда для всякого $x \in G$ имеем

$$v_i^x = \sum_{j=1}^n \rho_{ij}(x)v_j, \quad \rho_{ij}(x) \in K.$$

Матричное представление ρ , определяемое формулой $x \mapsto (\rho_{ij}(x))$, $x \in G$, будет точным. В самом деле, если элементу x из группы G соответствует тождественное линейное преобразование векторного пространства V , то $t_\alpha^x = t_\alpha$, где $1 \leq \alpha \leq d$. В этом случае $t_\alpha(x) = t_\alpha^x(e) = t_\alpha(e)$ при

$1 \leq \alpha \leq d$, что влечет равенство $x = e$. Более точное описание данного представления дает

Лемма 1.6. (Лемма о расщепляемых координатах, см. [5], [6]). Пусть K — поле, G — группа с K -значными координатами $t_1, \dots, t_d$, причем

$$t_\alpha(xy) = \sum_{\beta=1}^l f_{\alpha\beta}(x)h_\beta(y), \quad x, y \in G, \quad 1 \leq \alpha \leq d,$$

где $f_{\alpha\beta}, h_\beta$ — функции со значениями в K . Существует изоморфизм $\rho : G \rightarrow GL_n(K)$ такой, что: 1) ρ^{-1} линейно на G^ρ , 2) если функции $f_{\alpha\beta}$ полиномиальны на G (в координатах t_α), а h_β — на подмножестве $G_1 \subset G$, то ρ полиномиально на G_1 .

Определение 1.2. Будем говорить, что отображение $f : X \times Y \mapsto Mat_n(K)$ расщепляемо, если для всех его компонент f_{ij} выполнены равенства

$$f_{ij}(x, y) = \sum_{\nu=1}^l \varphi_\nu(x)\psi_\nu(y), \quad x \in X, y \in Y,$$

где φ_ν, ψ_ν — функции со значениями в поле K .

Лемма 1.7. (см. [6]). Пусть G — расширение группы A при помощи группы B , задаваемое факторами $f(x, y) \in A$, $x, y \in B$ и автоморфизмами $\hat{x} \in Aut A$, $x \in B$. Если группы A и B представимы матрицами над полем K и отображения

$$(x, y) \mapsto f(x, y), \quad (a, x) \mapsto a^{\hat{x}}$$

расщепляемы, то группа G представима матрицами над K .

Доказательство. По условию леммы, каждому $g \in G$ взаимнооднозначно соответствует пара (b, a) , $b \in B, a \in A$, где произведение задается по правилу

$$(b_1, a_1) \cdot (b_2, a_2) = (b_1 b_2, f(b_1, b_2) a_1^{\hat{b}_2} a_2).$$

Тогда на группе G можно задать координаты:

$$T_{ij}^{(B)}(g) = t_{ij}^{(B)}(b), \quad T_{ij}^{(A)}(g) = t_{ij}^{(A)}(a),$$

где $t_{ij}^{(A)}$ — компоненты матричного представления группы A , $t_{ij}^{(B)}$ — компоненты матричного представления группы B , (b, a) — пара, соответствующая элементу g . Покажем, что определенные таким образом координаты $T_{ij}^{(A)}$, $T_{ij}^{(B)}$ будут расщепляемыми в смысле определения 1.1.

$$T_{ij}^{(A)}(g_1, g_2) = t_{ij}^{(A)}(f(b_1, b_2) a_1^{\hat{b}_2} a_2) = \sum_{k,l} t_{ik}^{(A)}(f(b_1, b_2)) t_{kl}^{(A)}(a_1^{\hat{b}_2}) t_{lj}^{(A)}(a_2) =$$

$$\begin{aligned}
&= \sum_{k,l} \left(\sum_{\nu} \varphi_{\nu ik}(b_1) \psi_{\nu ik}(b_2) \right) \left(\sum_{\mu} \bar{\varphi}_{\mu kl}(a_1) \bar{\psi}_{\mu kl}(b_2) \right) t_{lj}^{(A)}(a_2) = \\
&= \sum_{k,l,\mu,\nu} (\varphi_{\nu ik}(b_1) \bar{\varphi}_{\mu kl}(b_1)) (\psi_{\nu ik}(b_2) \bar{\psi}_{\mu kl}(b_2) t_{lj}^{(A)}(a_2)) = \\
&= \sum_{\alpha} \Phi_{\alpha}(g_1) \Psi_{\alpha j}(g_2), \text{ где } \alpha = (i, k, l, \mu, \nu).
\end{aligned}$$

Набор функций $\{\Psi_{\alpha j}\}$ конечен, так как индексы i, j, k, l, μ, ν принимают конечное число значений.

$$T_{ij}^{(B)}(g_1, g_2) = t_{ij}^{(B)}(b_1, b_2) = \sum_k t_{ik}^{(B)}(b_1) t_{kj}^{(B)}(b_2) = \sum_k T_{ik}^{(B)}(g_1) T_{kj}^{(B)}(g_2).$$

Таким образом, координаты $T_{ij}^{(A)}, T_{ij}^{(B)}$ расщепляемы, и матричная представимость группы G следует из леммы о расщепляемых координатах.

Определение 1.3. Будем говорить, что функция $f \in A(G, K)$ расщепляема в $A(G, K)$, если

$$f(x, y) = \sum_{\nu=1}^l \varphi_{\nu}(x) \psi_{\nu}(y) \text{ для всех } x, y \in G,$$

где $\varphi_{\nu}, \psi_{\nu}$ — некоторые функции из $A(G, K)$.

Пусть N — нормальная подгруппа группы G , тогда алгебра функций $A(G/N, K)$ является подалгеброй алгебры $A(G, K)$.

Лемма 1.8. Функция $f \in A(G/N, K)$ расщепляема в $A(G/N, K)$ тогда и только тогда, когда она расщепляема в $A(G, K)$.

Доказательство. Если f расщепляема в $A(G/N, K)$, то она расщепляема и в $A(G, K)$ в силу включения $A(G/N, K) \subset A(G, K)$. Если f расщепляема в $A(G, K)$ и $\varphi_{\nu}, \psi_{\nu}$ — функции из $A(G, K)$, задающие это расщепление, то, выбрав в каждом смежном классе xN фиксированного представителя x_0 , можно определить новые функции $\Phi_{\nu}(xN) \equiv \varphi_{\nu}(x_0)$, $\Psi_{\nu}(xN) \equiv \psi_{\nu}(x_0)$. Равенства $f(xy) = f(x_0 y_0) = \sum_{\nu=1}^l \varphi_{\nu}(x_0) \psi_{\nu}(y_0) =$

$$\sum_{\nu=1}^l \Phi_{\nu}(x) \Psi_{\nu}(y) \text{ показывает расщепляемость } f \text{ в } A(G/N, K).$$

Лемма 1.9. (см. [11] теорема 6.2.) Пусть G — группа матриц степени n над полем K , H — ее нормальная подгруппа, такая, что $H = C_G(X)$, где $X \subset \text{Mat}_n(K)$. Тогда фактор-группа G/N представима матрицами степени n^2 над полем K .

Доказательство. Выберем максимальное линейно независимое множество матриц $\{m_1, \dots, m_l\}$ вида $m = g^{-1}xg$, $g \in G$, $x \in X$. На линейной K -оболочке $V = \langle m_1, \dots, m_l \rangle_K$ зададим действие группы G по правилу:

$$\hat{g} : v \mapsto g^{-1}vg, \quad v \in V, g \in G.$$

Очевидно, это соответствие задает гомоморфизм группы G в группу автоморфизмов конечномерного векторного пространства V . Вычислим ядро этого гомоморфизма. Пусть элементу $g \in G$ соответствует тождественное преобразование пространства V , тогда выполнены равенства $x = g^{-1}xg$, $x \in X$, то есть $g \in C_G(X)$. Обратно, так как $H \trianglelefteq G$, каждый элемент $h \in H$ оставляет неподвижной каждую матрицу m_i , $i = 1, \dots, l$, то есть задает тождественное линейное преобразование на V . Таким образом, группа G/H изоморфно представима матрицами степени l над полем K . Так как $l \leq n^2$, получаем утверждение леммы.

Из леммы 1.9 непосредственно следует, что, если нильпотентное произведение $A(n)B$, $n \geq 2$, представимо матрицами над полем K , то группы $\bar{A}, \bar{B}$ также представимы матрицами над полем K . Для этого достаточно положить $X = B, H = C_A(B)$ или $X = A, H = C_B(A)$.

Теорема 1.2. Пусть A, B — группы матриц над некоторым полем K . Нильпотентное произведение $A(n)B$, $n \geq 2$, представимо матрицами над полем K тогда и только тогда, когда представимо матрицами над полем K нильпотентное произведение $\bar{A}(n)\bar{B}$.

Доказательство. Пусть группа $A(n)B$ представима матрицами над полем K , t_{ij} — компоненты этого матричного представления. Нильпотентное произведение $A(n)B$, в силу гомоморфизма $A(n)B \rightarrow A \times B$, можно представить как расширение группы $[A, B]$ при помощи группы $A \times B$. Так как элемент $g \in A(n)B$ однозначно представим в виде произведения $abw(g)$, где $a \in A$, $b \in B$, $w(g) \in [A, B]$ (см. свойство 4.3.) и

$$g_1 g_2 = a_1 b_1 w(g_1) a_2 b_2 w(g_2) = a_1 a_2 b_1 b_2 [b_1, a_2]^{b_2} w(g_1)^{a_2 b_2} w(g_2),$$

это расширение задается представителями ab , факторами $f(a_1 b_1, a_2 b_2) = [b_1, a_2]^{b_2}$ и автоморфизмами $\widehat{a \times b} : [A, B]^{\widehat{a \times b}} = [A, B]^{ab}$.

Зададим координаты на группе $A(n)B$ согласованные с этим расширением:

$$T_{ij}^{(1)}(g) = t_{ij}(a), \quad T_{ij}^{(2)}(g) = t_{ij}(b), \quad T_{ij}^{(3)}(g) = t_{ij}(w(g)),$$

где $g = abw(g)$, $a \in A, b \in B, w(g) \in [A, B]$, t_{ij} — компоненты матричного представления группы $A(n)B$.

Координатные функции $T_{ij}^{(1)}, T_{ij}^{(2)}$ расщепляемы в $A(A(n)B, K)$ в силу леммы 1.8, где $N = B[A, B]$ или $N = A[A, B]$. Покажем расщепляемость в $A(A(n)B, K)$ функций $T_{ij}^{(3)}$.

$$\begin{aligned} T_{ij}^{(3)}(g_1 g_2) &= t_{ij}(w(g_1 g_2)) = t_{ij}([b_1, a_2]^{b_2} w(g_1)^{a_2 b_2} w(g_2)) = \\ &= \sum t_{ik_1}(b_2^{-1}) t_{k_1 k_2}(b_1^{-1}) t_{k_2 k_3}(a_2^{-1}) t_{k_3 k_4}(b_1) t_{k_4 k_5}(w(g_1)) t_{k_5 k_6}(a_2 b_2) t_{k_6 j}(w(g_2)) = \\ &= \sum_{\alpha\beta\gamma} F_{\alpha\beta}(g_1) H_{\beta\gamma}(g_2), \end{aligned}$$

где $F_{\alpha\beta}(g_1) = t_{k_1 k_2}(b_1^{-1}) t_{k_3 k_4}(b_1) t_{k_4 k_5}(w(g_1))$, $\alpha\beta = (k_1, k_2, k_3, k_4, k_5)$, $H_{\beta\gamma}(g_2) = t_{ik_1}(b_2^{-1}) t_{k_2 k_3}(a_2^{-1}) t_{k_5 k_6}(a_2 b_2) t_{k_6 j}(w(g_2))$, $\beta\gamma = (k_1, k_2, k_3, k_5, k_6, i, j)$.

Множество функций $\{H_{\beta\gamma}\}$ конечно, по этому координатные функции $T_{ij}^{(3)}$ расщепляемы в $A(A(n)B, K)$.

Заметим, что $[aC_A(B), bC_B(A)] = [a, b]$, $[a, b]^{C_A(B)} = [a, b]^{C_B(A)} = [a, b]$, где $a \in A, b \in B$. По этому каждый элемент смежного класса $gC_A(B)C_B(A)$ будет иметь вид $aC_A(B)bC_B(A)w(g)$, где $g = abw(g)$, $a \in A, b \in B, w(g) \in [A, B]$, а функции $T_{ij}^{(3)}$ будут инвариантными на смежных классах $gC_A(B)C_B(A)$, то есть $T_{ij}^{(3)} \in A(\bar{A}(n)\bar{B}, K)$.

Таким образом, каждому элементу $\bar{g} \in \bar{A}(n)\bar{B}$ можно взаимнооднозначно сопоставить тройку элементов $\{\bar{a}, \bar{b}, w(g)\}$, $\bar{a} \in \bar{A}, \bar{b} \in \bar{B}, w(g) \in [A, B]$, а на самой группе $\bar{A}(n)\bar{B}$ задать координатные функции $\bar{T}_{ij}^{(1)}(\bar{g}) = \bar{t}_{ij}^{(1)}(\bar{a})$, $\bar{T}_{ij}^{(2)}(\bar{g}) = \bar{t}_{ij}^{(2)}(\bar{b})$, $\bar{T}_{ij}^{(3)}(\bar{g}) = T_{ij}^{(3)}(\bar{g})$, где $\bar{t}_{ij}^{(1)}, \bar{t}_{ij}^{(2)}$ — компоненты матричных представлений групп $\bar{A}$ и $\bar{B}$ соответственно, которые существуют в силу леммы 1.9.

Равенства

$$\begin{aligned} \bar{T}_{ij}^{(1)}(\bar{g}_1 \bar{g}_2) &= \bar{t}_{ij}^{(1)}(\bar{a}_1 \bar{a}_2) = \sum_k \bar{t}_{ik}^{(1)}(\bar{a}_1) \bar{t}_{kj}^{(1)}(\bar{a}_2) = \sum_k \bar{T}_{ik}^{(1)}(\bar{g}_1) \bar{T}_{kj}^{(1)}(\bar{g}_2), \\ \bar{T}_{ij}^{(2)}(\bar{g}_1 \bar{g}_2) &= \bar{t}_{ij}^{(2)}(\bar{b}_1 \bar{b}_2) = \sum_k \bar{t}_{ik}^{(2)}(\bar{b}_1) \bar{t}_{kj}^{(2)}(\bar{b}_2) = \sum_k \bar{T}_{ik}^{(2)}(\bar{g}_1) \bar{T}_{kj}^{(2)}(\bar{g}_2) \end{aligned}$$

показывают расщепляемость координатных функций $\bar{T}_{ij}^{(1)}, \bar{T}_{ij}^{(2)}$. Расщепляемость координатных функций $\bar{T}_{ij}^{(3)}$ вытекает из расщепляемости в $A(\bar{A}(n)\bar{B}, K)$ функций $T_{ij}^{(3)}$, в силу леммы 1.8. Существование матричного представления группы $\bar{A}(n)\bar{B}$ следует теперь из леммы о расщепляемых координатах.

Утверждение в обратную сторону следует из леммы 1.3.

Пусть $F(X)$ — свободная группа со свободным порождающим множеством X , $F_m(X) = F(X)/\gamma_{m+1}(F(X))$.

СЛЕДСТВИЕ 1.1. Нильпотентное произведение $F(X)(n)F(Y)$, $n \geq 2$, представимо матрицами над полем нулевой характеристики и не представимо матрицами ни над каким полем положительной характеристики.

Доказательство. Заметим, что $F_n(X \cup Y) = F_n(X)(n)F_n(Y)$, а в группах $F(X)(n)F(Y)$, $F_n(X)(n)F_n(Y)$ выполнены равенства

$$C_{F(X)}(F(Y)) = \gamma_n(F(X)), \quad C_{F(Y)}(F(X)) = \gamma_n(F(Y)),$$

$$C_{F_n(X)}(F_n(Y)) = \gamma_n(F_n(X)), \quad C_{F_n(Y)}(F_n(X)) = \gamma_n(F_n(Y)).$$

Поэтому матричная представимость групп $F(X)(n)F(Y)$ и $F_n(X \cup Y)$ равносильна, по теореме 1.2, матричной представимости нильпотентного произведения $F_{n-1}(X)(n)F_{n-1}(Y)$. Известно, что свободная нильпотентная группа представима матрицами над полем нулевой характеристики. С другой стороны, она не может быть группой матриц над полем положительной характеристики, так как в этом случае ее фактор по центру был бы группой ограниченного периода (см. лемма 1.4). Таким образом, группа $F(X)(n)F(Y)$ представима матрицами над полем нулевой характеристики и не представима матрицами над полями положительной характеристики.

Отметим, что хотя свободные группы $F(X)$, $F(Y)$ представимы матрицами над полями произвольной характеристики (см. [7],[11]), их нильпотентное произведение представимо матрицами только над полями нулевой характеристики.

§ 2 Группы представимые матрицами над полями различных характеристик.

Рангом группы G называют наименьшее число r , обладающее тем свойством, что всякая ее конечно порожденная подгруппа может быть порождена не более чем r элементами. Если такое число существует, будем писать $\text{rank} G = r$, в противном случае $\text{rank} G = \infty$. Через F_n будем обозначать свободную группу со свободным порождающим множеством из n элементов.

Возможность представления группы матрицами конечной степени над некоторым полем накладывает ограничение на ее строение. Так

из альтернативы Титса следует, что линейная группа, не содержащая свободной подгруппы F_2 , является расширением линейной разрешимой группы при помощи линейной периодической. В абелевом случае полное описание строения групп, представимых матрицами конечной степени над полем, дает теорема А.И. Мальцева.

Теорема 2.1. ([4], теорема 1) Пусть G — абелева группа.

а) Группа G представима матрицами степени n над полем нулевой характеристики тогда и только тогда, когда ранги ее примарных компонент не превосходят n , т.е. $\text{rank}(\tau G) \leq n$.

б) Группа G представима матрицами степени n над полем положительной характеристики p тогда и только тогда, когда ее примарная компонента $\tau_p G$ конечного периода не больше p^s , а ранги остальных примарных компонент ограничены числом $n - s$.

Из теоремы 2.1 непосредственно следует что абелева группа G представима матрицами над полями различных характеристик p и q тогда и только тогда, когда ранги ее примарных компонент ограничены в совокупности, а примарные компоненты $\tau_p G$, $\tau_q G$ конечны. В этом случае $\text{rank}(\tau G) < \infty$ и группа G представима матрицами над полем нулевой характеристики.

Лемма 2.1. Пусть G — p -группа представимая матрицами степени n над полем характеристики p и матрицами степени m над полем характеристики q , $p \neq q$. Тогда $|G| \leq p^{em^3} \leq (np)^{m^3}$, где $e = [\log_p n] + 1$.

Доказательство. Как p -группа матриц степени n над полем характеристики p , G унитаризуема и является группой конечного периода p^r . В этом случае выполнены неравенства $p^{r-1} < n \leq p^r$, а на группе G верно равенство $G^{p^e} = 1$, где $e = [\log_p n] + 1$.

По теореме Бернсайда $|G : U_q(G)| \leq (p^e)^{m^3}$, где $U_q(G)$ — унипотентный радикал группы G , как группы матриц степени m над полем характеристики q .

Так как G — p -группа и $(p, q) = 1$, то $U_q(G)$ тривиален и $|G| \leq p^{em^3}$, где $e = [\log_p n] + 1$. Из неравенства $p^e \leq np$ получаем $|G| \leq (np)^{m^3}$.

Лемма 2.2. Пусть G — группа конечного периода l представимая матрицами степени n над полем характеристики $p > 0$, и матрицами степени m над полем характеристики $q \geq 0$, $p \neq q$. Тогда $|G| \leq l^{n^3} p^{em^3}$, где $e = [\log_p n] + 1$, или $|G| \leq l^{n^3} (np)^{m^3}$.

Доказательство. По теореме Бернсайда $|G : U_p(G)| = l^{n^3}$, где $U_p(G)$ — унипотентный радикал группы G , как группы матриц степени n над полем характеристики p . По лемме 2.1 $|U_p(G)| \leq p^{em^3}$, где $e = [\log_p n] + 1$, и, следовательно, $|G| \leq l^{n^3} p^{em^3}$ или $|G| \leq l^{n^3} (np)^{m^3}$.

Теорема 2.2. Периодическая группа G допускает точное представление матрицами над полями различных характеристик p и q тогда и только тогда, когда в ней найдется нормальная абелева подгруппа A конечного индекса, ранги примарных компонент которой ограничены в совокупности, а примарные компоненты $\tau_p A$, $\tau_q A$ конечны. Индекс нужной группы A ограничен целозначной функцией $f(m, n, p)$, где m, n — степени данных представлений, p — ненулевая характеристика.

Доказательство. а) Пусть группа G представима матрицами степени n над полем характеристики $p > 0$ и матрицами степени m над полем характеристики $q \geq 0$, $p \neq q$. Как линейная периодическая, группа G является локально конечной. По лемме 2.1, силовские p -подгруппы конечно порожденных подгрупп группы G имеют порядок не больше p^{em^3} , где $e = [\log_p n] + 1$. Тогда, по теореме Брауэра-Фейта (см. [11], теорема 9.6.) о почти абелевости конечных групп матриц над полем ненулевой характеристики, имеем, что каждая конечно порожденная подгруппа группы G содержит нормальный абелев делитель индекса не больше $i(p^{em^3}, n)$, где $i(p^{em^3}, n)$ — целозначная функция, зависящая от порядка силовской p -подгруппы p^{em^3} и степени матричного представления n . По локальной теореме Мальцева (см. [3], упражнение 27.3.2) этот вывод можно сделать и для всей группы G . Положим $f(m, n, p) = i(p^{em^3}, n)$.

б) Если A — абелева подгруппа из условия теоремы, то она по теореме 2.1 представима матрицами над полями характеристики p и q . Так как A конечного индекса в группе G , то и вся группа G допускает изоморфное представление матрицами над полями характеристики p и q . Если, при этом, $\text{rank } A = r$, $|G : A| = i$, $(\tau_p A)^{p^{s_1}} = 1$, $(\tau_q A)^{q^{s_2}} = 1$, то G представима матрицами степени $i(r + s_1)$ над полем характеристики p и матрицами степени $i(r + s_2)$ над полем характеристики q .

Лемма 2.3. Пусть G — нильпотентная группа ступени s , представимая матрицами степени n над полем характеристики $p > 0$ и матрицами степени m над полем характеристики q , $q \neq p$. Тогда $|G : \mathbb{Z}(G)| \leq l(m, n, p, s)$, где $\mathbb{Z}(G)$ — центр группы,

$$l(m, n, p, s) = (np)^{n^6(s-1)^5+m^6} n^{n^6(n-1)^5(s+1)((s-1)^2+1)+m^6}.$$

Доказательство. По лемме 1.4 имеем, что $G^{l(n,s,p)} \leq \mathbb{Z}(G)$, где $l(n, s, p) = p^{(n-1)(s-1)^3} n^{(n-1)(s+1)((s-1)^2+1)}$, а по лемме 1.9 фактор-группа $G/\mathbb{Z}(G)$ представима матрицами степени n^2 над полем характеристики p и матрицами степени m^2 над полем характеристики q . Из леммы 2.2 следует, что $|G/\mathbb{Z}(G)| \leq l(n, s, p)^{n^6} (pn^2)^{m^6}$. Заметим, что в доказательстве леммы 1.4 (б) тождество $[G^{\mu(n,s)}, G^{\mu(n,s)}]^{p^{n-1}} = 1$ можно заменить на

тождество $[G^{\mu(n,s)}, G^{\mu(n,s)}]^{p^e} = 1$, где $e = [\log_p n] + 1$. Тогда $l(n, s, p) \equiv p^{e(s-1)^3} n^{(n-1)(s+1)((s-1)^2+1)}$, а с учетом неравенства $p^e \leq pn$ получаем неравенство $|G/\mathbb{Z}(G)| \leq ((pn)^{(s-1)^3} n^{(n-1)(s+1)((s-1)^2+1)})^{n^6} (pn^2)^{m^6}$, что влечет оценку $|G/\mathbb{Z}(G)| \leq (pn)^{n^6(s-1)^3+m^6} n^{n^6(n-1)(s+1)((s-1)^2+1)+m^6}$.

Теорема 2.3. Разрешимая группа G допускает точное представление матрицами над полями различных характеристик p и q тогда и только тогда, когда в ней найдется абелева подгруппа A конечного индекса, ранги примарных компонент которой ограничены в совокупности, а примарные компоненты $\tau_p A, \tau_q A$ конечны. Индекс нужной группы A ограничен целозначной функцией $f(m, n)$, где m, n — степени данных матричных представлений.

Доказательство. Без ограничения общности, можно считать, что поля, над которыми группа G представима матрицами, являются алгебраически замкнутыми. Тогда по теореме Мальцева о почти триангулируемости разрешимых линейных групп, в группе G найдутся подгруппы T_p и T_q конечного индекса представимые треугольными матрицами степени n над полем характеристики p и матрицами степени m над полем характеристики q . При этом $|G : T_p| = \mu(n) \leq (n^2!)^{n^2} (n!)^n n^{2n^2}$, $|G : T_q| = \mu(m) \leq (m^2!)^{m^2} (m!)^m m^{2m^2}$ (см. [6], теорема 45.1.1). Их пересечение $T_{pq} = T_p \cap T_q$ будет конечного индекса не больше $\mu(n) \cdot \mu(m)$. Коммутант $[T_{pq}, T_{pq}]$ унитаризуем и является одновременно и p -группой и q -группой. Так как p и q взаимнопросты, то $[T_{pq}, T_{pq}]$ тривиален, а группа T_{pq} абелева. В этом случае $f(m, n) = (m^2!)^{m^2} (m!)^m m^{2m^2} (n^2!)^{n^2} (n!)^n n^{2n^2}$.

В обратную сторону, если нашлась нужная абелева группа A , то она по теореме 2.1 представима матрицами над полями характеристики p и q . Так как A конечного индекса в группе G , то этот вывод верен и для всей группы G .

Теорема 2.4. Пусть группа G не содержит свободной группы F_2 . Группа G представима матрицами над полями различных характеристик p и q тогда и только тогда, когда в ней найдется абелева подгруппа A конечного индекса, ранги примарных компонент которой ограничены в совокупности, а примарные компоненты $\tau_p A, \tau_q A$ конечны.

Доказательство. Пусть группа G представима матрицами над полями различных характеристик p и q , $R(G)$ — ее разрешимый радикал, т. е. максимальная нормальная разрешимая подгруппа. По альтернативе Титса (см. [10]) фактор-группа $G/R(G)$ периодическая, представима матрицами над тем же полем, что и G , при этом $G/R(G)$ уже не содержит нормальных разрешимых подгрупп. Из теорем 2.2 и 2.3 следует, что $G/R(G)$ конечна, а $R(G)$ почти абелева. Таким образом, группа G

содержит некоторую абелеву подгруппу A конечного индекса. Ограничения на ранги примарных компонент абелевой группы A и конечность примарных компонент $\tau_p A$, $\tau_q A$ вытекает из теоремы 2.1.

Обратно, пусть в группе G нашлась абелева подгруппа A конечного индекса i , такая, что $\text{rank}(\tau A) = r$, $(\tau_p A)^{p^{s_1}} = 1$, $(\tau_q A)^{q^{s_2}} = 1$. По теореме 2.1 группа A представима матрицами степени $r + s_1$ над полем характеристики p и матрицами степени $r + s_2$ над полем характеристики q . Тогда вся группа G представима матрицами степени $i(r + s_1)$ и $i(r + s_2)$ над полями характеристики p и q , соответственно.

Отметим, что группы из условия теоремы 2.4 всегда представимы матрицами над полем нулевой характеристики.

Требование, чтобы группа G из условия теоремы 2.4 не содержала свободной группы F_2 , существенно. Как показал В.Л. Нисневич [7], свободная группа F_n представима матрицами над полем любой характеристики, а свободное произведение $A * B$ двух линейных групп представляется матрицами над некоторым чисто трансцендентным расширением поля представления групп A и B . В частности, свободное произведение $A * B$ групп A и B , допускающих точное представление матрицами над полями характеристик p и q , само допускает точное представление матрицами над полями тех же характеристик. Ясно, что свободное произведение $A * B$ содержит подгруппу, изоморфную свободной группе F_2 , и не является почти абелевой группой. Очевидно, что и конечные расширения групп, допускающих матричное представление над полями различных характеристик, так же обладают этим свойством.

Литература

1. Вапнэ Ю.Г. О матричной представимости нильпотентных произведений групп // Матем. заметки, т. 14, N 3, с.383–394
2. Головин О.Н. Нильпотентные произведения групп // Матем. сб. 1950, т. 27, N 3, с. 427–454.
3. Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. 3-е изд. М.:Наука, 1982.
4. Мальцев А.И. Об изоморфном представлении бесконечных групп матрицами. // Матем. сб. 1940. т.8, N 3, с. 405–422.
5. Мерзляков Ю.И. О матричном представлении автоморфизмов, расширений и разрешимых групп // Алгебра и логика. 1968. т.7, N 3, с. 63–104.

6. Мерзляков Ю.И. Рациональные группы.— М.: Наука, 1980.
7. Нисневич В.Л. О группах изоморфно представимых матрицами над коммутативным полем Матем.сб. 1940. т.8, N 3, с. 405–422.
8. Супруненко Д.А. Группы матриц.- М.:Наука, 1972.
9. Swan R. Representation of polycyclic groups// Proc. Amer. Math. Soc., 1967, v. 18. N 3. P.573–574
10. Tits J. Free subgroups in linear groups.- J.Algebra, 1972, 20, N 2, p. 250–270
11. Wehrfritz B.A.F. Infinite linear groups. — Berlin, 1973.

О КОРРЕКТНОСТИ ОПТИМИЗАЦИОННЫХ ЗАДАЧ НА МНОЖЕСТВЕ ХАРАКТЕРИСТИЧЕСКИХ КОРНЕЙ

А.А. Воевода, А.В. Чехонадских

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

1. Введение. Решение ряда задач синтеза систем автоматического управления требует оптимизации параметров системы или перемещения их в заданную область. При переходе к операторной форме эти параметры оказываются непосредственно связанными не с коэффициентами характеристических многочленов, а с их корнями, тогда как регулировке подаются именно коэффициенты. Хорошо известные связи корней (вообще говоря, комплексных) и действительных коэффициентов многочленов (см., напр. [1]) не позволяют, однако, указать условий корректной постановки оптимизационных задач, равно как и естественного подхода к самому понятию оптимизации. Это связано, во-первых, с отсутствием «естественной» метрики на пространстве многочленов, которая по близости многочленов позволяла бы судить о близости корневых наборов; во-вторых, с тем, что сами корневые наборы являются неупорядоченными множествами и, более того, не допускающими «естественного» порядка, поскольку случай комплексных корней нельзя исключить из рассмотрения. Некоторые способы метризации множества многочленов и оптимизации системы корней были предложены в работе [2]. После того, как сформировалась концепция совмещённых корневых координат [3], появилась возможность рассмотрения соответствия *коэффициенты* $\leftrightarrow$ *корни* как биекции пространств над полем действительных чисел. Однако для того, чтобы осуществлять оптимизацию системы корней за счёт изменения коэффициентов многочлена, требовалось выяснить, когда под действием этого отображения выпуклое множество переходит в выпуклое. В настоящей работе указываются достаточные условия

на целевую область в пространстве совмещённых корневых координат, которые гарантируют выпуклость соответствующего множества коэффициентов и обеспечивают корректность постановки оптимизационной задачи для характеристических многочленов.

2. Постановка задачи. Даже в случае квадратного трёхчлена задание естественной целевой области для корней часто не позволяет получить выпуклой области коэффициентов. Например, если брать действительные или комплексно сопряжённые пары корней из трапеции $-3 \leq \operatorname{Re} z_{1,2} \leq -1$, $|\operatorname{Im} z_{1,2}| \leq |\operatorname{Re} z_{1,2}|$, обеспечивающей заданное качество переходных процессов, то коэффициенты b и c действительного трёхчлена

$$f[z] = (z - z_1)(z - z_2) = z^2 + bz + c$$

попадают в невыпуклую область $-6 \leq b \leq -2$; $\max(-1 - b; -9 - 3b) \leq c \leq b^2/4$; точно так же задание области для таких же корней в виде круга $(x - 2)^2 + y^2 \leq 1$ в комплексной плоскости приводит к треугольнику $-6 \leq b \leq -2$; $\max(-1 - b; -9 - 3b) \leq c \leq -3 - 2b$; для пар корней, расположенных в эллипсе $(x - 2)^2 + y^2/4 \leq 1$ — к выпуклой области $-6 \leq b \leq -2$; $\max(-1 - b; -9 - 3b) \leq c \leq 28/3 - 3/4(b + 16/3)^2$ для коэффициентов, а для пар корней, расположенных в эллипсе $(x - 2)^2 + 4y^2 \leq 1$ — к невыпуклой области $-6 \leq b \leq -2$; $\max(-1 - b; -9 - 3b) \leq c \leq (-12 - 8b + 3b^2)/16$ для коэффициентов.

Для многочленов большей степени граница области коэффициентов оказывается довольно сложной и с трудом поддаётся анализу на выпуклость.

Естественно поставить вопрос в общем случае так: какие условия на область прообразов и заданный на ней диффеоморфизм должны выполняться, чтобы выпуклое множество под его действием переходило в выпуклое?

3. Поток диффеоморфизма через поверхность. Следующее определение восходит к классическому понятию потока векторного поля. Пусть $\Gamma \subset R^n$ — гладкая замкнутая поверхность в n -мерном действительном пространстве с обычной метрикой, в некоторой окрестности которой определён диффеоморфизм $\varphi : R^n \rightarrow R^n$, и Φ — его производное отображение, специализацию которого для точки X поверхности Γ будем обозначать Φ_X . Если $\mathbf{n}$ — единичная внешняя нормаль в точке X , то назовём **потоком** отображения φ в точке X величину нормальной составляющей вектора $\Phi_X(\mathbf{n})$ по отношению к поверхности $\Gamma^* = \varphi(\Gamma)$ в пространстве образов:

$$\Pi_\varphi(X) = |\Phi_X(\mathbf{n})_\perp|.$$

Пусть $\mathbf{e}_1, \dots, \mathbf{e}_{n-1}$ — некоторый базис (не обязательно ортонормиро-

ванный) в касательной гиперплоскости K к поверхности Γ в точке X , дополним его до базиса $\mathbf{e}_1, \dots, \mathbf{e}_{n-1}, \mathbf{n}$ всего пространства. Тогда справедливо следующее:

Предложение 1. $\Pi_\varphi(X) = \frac{|\mathbf{f}_1 \wedge \dots \wedge \mathbf{f}_{n-1} \wedge \mathbf{f}_n|}{|\mathbf{f}_1 \wedge \dots \wedge \mathbf{f}_{n-1}|}$, где $\mathbf{f}_1 = \Phi_X(\mathbf{e}_1), \dots, \mathbf{f}_{n-1} = \Phi_X(\mathbf{e}_{n-1}), \mathbf{f}_n = \Phi_X(\mathbf{n})$.

Прежде всего, заметим, что векторы $\mathbf{f}_1, \dots, \mathbf{f}_{n-1}$ линейно независимы и знаменатель дроби отличен от нуля. Пусть теперь $\mathbf{e}_1^*, \dots, \mathbf{e}_{n-1}^*$ — некоторый о.н.б в плоскости K^* , касательной к поверхности Γ^* в точке $\varphi(X)$. Поскольку $\mathbf{f}_1, \dots, \mathbf{f}_{n-1} \in K^*$, имеем $|\mathbf{f}_1 \wedge \dots \wedge \mathbf{f}_{n-1}| = |\det(f_{ij})|$, где f_{ij} — коэффициенты разложения векторов $\mathbf{f}_1, \dots, \mathbf{f}_{n-1}$ по базису $\mathbf{e}_1^*, \dots, \mathbf{e}_{n-1}^*$ [4]. Дополнив этот базис до о.н.б пространства с помощью единичного вектора внешней нормали $\mathbf{e}_n^*$, получим разложение $\mathbf{f}_n = f_{1n}\mathbf{e}_1^* + \dots + f_{nn}\mathbf{e}_n^*$, причём $f_{nn} = |(\mathbf{f}_n)_\perp| = \Phi_X(\mathbf{n})_\perp$. Теперь наше утверждение следует из очевидного соотношения

$$\begin{aligned} |\mathbf{f}_1 \wedge \dots \wedge \mathbf{f}_{n-1} \wedge \mathbf{f}_n| &= \left| \det \begin{pmatrix} f_{11} & \dots & f_{1n-1} & f_{1n} \\ \vdots & & & \\ f_{n-11} & \dots & f_{n-1n-1} & f_{n-1n} \\ 0 & \dots & 0 & f_{nn} \end{pmatrix} \right| = \\ &= f_{nn} \left| \det \begin{pmatrix} f_{11} & \dots & f_{1n-1} \\ \vdots & \vdots & \\ f_{n-11} & \dots & f_{n-1n-1} \end{pmatrix} \right| = |\Phi_X(\mathbf{n})_\perp| |\mathbf{f}_1 \wedge \dots \wedge \mathbf{f}_{n-1}|. \end{aligned}$$

4. Выпуклость образа выпуклого множества. Предположим, что область $D(\Gamma)$, ограниченная поверхностью Γ , выпукла, а сама поверхность — второго порядка гладкости. По-прежнему считая, что $X \in \Gamma$ — некоторая точка, $\mathbf{n}$ — единичная внешняя нормаль в ней, проведём сечение поверхности Γ некоторой двумерной нормальной плоскостью P , проходящей через точку X . Тогда плоская кривая $L = \Gamma \cap P$ локально может быть представлена в виде $y_n = f(y_1)$, где в системе координат, связанной с точкой X , координатная ось OY_1 направлена вдоль прямой $P \cap K$, касательной к поверхности Γ , а ось OY_n сонаправлена с нормалью $\mathbf{n}$. Очевидно, функция $y_n = f(y_1)$ второго порядка гладкости, а в окрестности точки $y_1 = y_n = 0$ она выпукла вверх, причём в самой этой точке ось OY_1 оказывается касательной к графику этой функции — т.е. кривой L . Предположим, что кривая L имеет в точке X ненулевую кривизну

$$k(X) = \frac{|f''(0)|}{(1 + f'(0)^2)^{3/2}} = |f''(0)| > 0.$$

Представим функцию $y_n = f(y_1)$ в виде $y_n = \frac{a_2}{2}y_1^2 + O_3(y_1)$, где в силу того, что выпуклость направлена вверх, выполняется неравенство $a_2 = f''(0) < 0$. Тогда в координатах $\mathbf{y} = (y_1; \dots; y_n)^T$ кривая L локально принимает вид

$$\mathbf{y}_L = (y_1; 0; \dots; 0; \frac{a_2}{2}y_1^2 + O_3(y_1))^T.$$

В исходных координатах кривая L запишется как $\mathbf{x}_L = \mathbf{x}_0 + S \mathbf{y}_L$, где S — матрица соответствующего ортогонального преобразования, а $\mathbf{x}_0$ — столбец координат точки X . Обозначим через $\mathbf{s}_1, \dots, \mathbf{s}_n$ столбцы матрицы S , которые являются координатами векторов о.н.б, соответствующего системе координат $\mathbf{y} = (y_1; \dots; y_n)^T$, в исходном базисе, соответствующем координатам $\mathbf{x}$; тогда для кривой получится представление

$$\mathbf{x}_L = \mathbf{x}_0 + \mathbf{s}_1 y_1 + \mathbf{s}_n (\frac{a_2}{2} y_1^2 + O_3(y_1)).$$

Пусть $z = (z_1, \dots, z_n)^T$ — координаты в пространстве образов диффеоморфизма φ , так что его представление формулой Тейлора 2-го порядка в точке X имеет вид:

$$z = \varphi(\mathbf{x}) = \varphi(\mathbf{x}_0) + \Phi_X(\mathbf{x} - \mathbf{x}_0) + (\mathbf{x} - \mathbf{x}_0)^T Q_X(\mathbf{x} - \mathbf{x}_0) + O_3(\mathbf{x} - \mathbf{x}_0).$$

Образом кривой L оказывается кривая L^* , описываемая уравнением

$$\begin{aligned} \mathbf{z}_{L^*} &= \varphi(\mathbf{x}_0) + \Phi_X(\mathbf{s}_1 y_1 + \mathbf{s}_n (\frac{a_2}{2} y_1^2 + O_3(y_1))) + \\ &+ \mathbf{s}_1 y_1 + \mathbf{s}_n (\frac{a_2}{2} y_1^2 + O_3(y_1))^T Q_X(\mathbf{s}_1 y_1 + \mathbf{s}_n (\frac{a_2}{2} y_1^2 + O_3(y_1))) + \\ &+ O_3(\mathbf{s}_1 y_1 + \mathbf{s}_n (\frac{a_2}{2} y_1^2 + O_3(y_1))) = \varphi(\mathbf{x}_0) + y_1 \Phi_X \mathbf{s}_1 + y_1^2 (\frac{a_2}{2} \Phi_X \mathbf{s}_n + \mathbf{s}_1^T Q_X \mathbf{s}_1) + O_3(y_1). \end{aligned}$$

Поскольку векторы $\mathbf{s}_1, \dots, \mathbf{s}_{n-1}$ задают касательную гиперплоскость K к поверхности Γ в точке X , то их образы $\Phi(\mathbf{s}_1), \dots, \Phi(\mathbf{s}_{n-1})$ задают касательную гиперплоскость K^* к поверхности Γ^* в точке $\varphi(X)$; а поскольку $\mathbf{s}_n = \mathbf{n}$ является единичной нормалью, то $\Phi_X \mathbf{s}_n = \Pi_\varphi(X) \mathbf{n}^* + \mathbf{k}$, где $\mathbf{n}^*$ — единичная нормаль к поверхности Γ^* в точке $\varphi(X)$, а вектор $\mathbf{k}$ лежит в гиперплоскости K^* .

Оценим величину проекции вектора $\frac{a_2}{2} \Phi_X \mathbf{s}_n + \mathbf{s}_1^T Q_X \mathbf{s}_1$ на нормаль $\mathbf{n}^*$. Столбец $\mathbf{s}_1^T Q_X \mathbf{s}_1$ состоит из значений квадратичных форм вторых дифференциалов $d^2 \varphi_k(\mathbf{s}_1)$ компонент диффеоморфизма φ на единичном векторе $\mathbf{s}_1$, поэтому $|d^2 \varphi_k(\mathbf{s}_1)| \leq |\lambda_k|$ — максимального по модулю собственного числа матрицы $D_k^2 = (\frac{d^2 \varphi_k}{dx_i dx_j})$. Положим $\lambda = (\lambda_1, \dots, \lambda_n)^T$ —

столбец таких собственных чисел, $\Lambda = |\lambda|$. И так как $a_2 = -k(X)$, то $np_n^*(\frac{a_2}{2}\Phi_X \mathbf{s}_n + \mathbf{s}_1^T Q_X \mathbf{s}) < 0$ при выполнении неравенства $k(X)\Pi_\varphi(X) \geq 2\Lambda$. Тем самым доказано

Предложение 2. Пусть $D(\Gamma)$ — выпуклая область, ограниченная поверхностью Γ второго порядка гладкости с линейной кривизной нормальных сечений не менее k , φ — диффеоморфизм, определённый в некоторой окрестности $D(\Gamma)$ и имеющий непрерывные частные производные второго порядка. Тогда для выпуклости образа $D(\Gamma)^* = \varphi(D(\Gamma))$ достаточно, чтобы на поверхности Γ выполнялось неравенство

$$k\Pi_\varphi \geq 2\Lambda,$$

где Π_φ — минимальный поток диффеоморфизма φ на поверхности Γ , а Λ — величина вектора максимальных собственных чисел матриц D_k^2 вторых дифференциалов компонент отображения φ .

Список литературы

- [1] Ван дер Варден Б. Л. Алгебра.- М.: Наука, 1975.
- [2] Воевода А.А., Чехонадских А.В. Об оптимизации системы характеристических корней при бедном множестве параметров// Науч. вестник НГТУ.- Новосибирск: Изд-во НГТУ, 2001.- №1 (10).- С.171–176.
- [3] 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.
- [4] Постников М. М. Аналитическая геометрия // М.: Наука.- 1986.

НАКРЫТИЯ В РЕШЕТКЕ МНОГООБРАЗИЙ m -ГРУПП

О.В. Исаева

Алтайский Государственный университет,
Ленина 61, 656099, Барнаул, РОССИЯ.
e-mail: isaeva@econ.asu.ru

1 Введение

Следуя М. Жираде, И. Рахунеку [1] m -группой называем алгебраическую систему G сигнатуры $m = \{\cdot, e, ^{-1}, \wedge, \vee, \varphi\}$ такую, что $\langle G; \cdot, e, ^{-1}, \vee, \wedge \rangle$ является решеточно упорядоченной группой, а одноместная операция φ является реверсивным автоморфизмом второго порядка группы $\langle G; \cdot, e, ^{-1} \rangle$, т.е. φ является автоморфизмом группы $\langle G; \cdot, e, ^{-1} \rangle$ и антиавтоморфизмом решетки $\langle G; \vee, \wedge \rangle$. Таким образом, φ является взаимнооднозначным отображением G на себя, причем выполнены соотношения

$$\varphi(xy) = \varphi(x)\varphi(y), \quad \varphi(x \vee y) = \varphi(x) \wedge \varphi(y),$$

$$\varphi(x \wedge y) = \varphi(x) \vee \varphi(y), \quad \varphi(\varphi(x)) = x.$$

Теория решеточно упорядоченных групп (ℓ -групп) в настоящее время разработана достаточно широко и основные результаты по ℓ -группам можно найти в [2], [3].

Так же как класс всех ℓ -групп является многообразием сигнатуры $\ell = \{\cdot, e, ^{-1}, \wedge, \vee, \}$, так и класс $\mathcal{M}$ всех m -групп является многообразием сигнатуры m [4].

Через $\mathcal{A}$ будем обозначать многообразие абелевых m -групп, т.е. многообразие, определяемое тождеством $[x, y] = e$. В [1] доказано, что данное многообразие порождается группой $(\mathbf{Z} \times \mathbf{Z}^*, Exch)$, где $\mathbf{Z}$ – линейно упорядоченная относительно естественного порядка группа целых чисел, причем пара $(a, b) > 0$ тогда и только тогда, когда $a > 0$ и $b < 0$ в линейно упорядоченной группе $\mathbf{Z}$; линейно упорядоченная группа $\mathbf{Z}^*$ получается из группы $\mathbf{Z}$ обращением порядка, т.е. $a > 0$ в группе $\mathbf{Z}^*$ тогда и только тогда, когда $a < 0$ в группе $\mathbf{Z}$; $Exch$ – реверсивный автоморфизм

второго порядка ℓ -группы $\mathbf{Z} \times \mathbf{Z}^*$ и $Exch(a, b) = (b, a)$. В отличие от решетки многообразий ℓ -групп, многообразие $\mathcal{A}$ не является наименьшим нетривиальным многообразием в решетке многообразий m -групп. В работе [1] показано, что многообразие $\mathcal{I}$, порожденное m -группой $(\mathbf{Z}, Inv)$, является наименьшим нетривиальным многообразием в решетке многообразий m -групп Λ_m , где $Inv(z) = z^{-1}$ для любого $z \in \mathbf{Z}$.

Говорят, что многообразие m -групп $\mathcal{X}$ покрывает многообразие m -групп $\mathcal{Y}$, если $\mathcal{X} \subseteq \mathcal{Y}$ и для любого многообразия m -групп $\mathcal{Z}$ такого, что $\mathcal{X} \subseteq \mathcal{Z} \subseteq \mathcal{Y}$ следует, что $\mathcal{X} = \mathcal{Z}$ или $\mathcal{Y} = \mathcal{Z}$.

Пусть $(G_\alpha, \varphi_\alpha)$ – произвольные m -группы, где α принадлежит некоторому множеству индексов J . Тогда декартово произведение $\prod_{\alpha \in J} (G_\alpha, \varphi_\alpha)$ этих m -групп является m -группой относительно реверсивного автоморфизма Φ , определенного по правилу:

$$\Phi(D)(\alpha) = \varphi_\alpha(d_\alpha),$$

где $D(\alpha) = d_\alpha$ для любого элемента $D \in \prod_{\alpha \in J} (G_\alpha, \varphi_\alpha)$, т.е. $D(\alpha)$ есть значение элемента D на $\alpha \in G$.

Пусть G – произвольная ℓ -группа и φ – реверсивный автоморфизм второго порядка на G , тогда для любого $x \in G$ выполняется следующее равенство $\varphi(|x|) = |\varphi(x)|^{-1}$ [5]. Из этого факта непосредственно следует справедливость следующего утверждения.

Предложение 1.1. Пусть G – произвольная ℓ -группа и φ – реверсивный автоморфизм второго порядка на группе G , тогда для любого $x \in G$ выполняется следующее равенство

$$\varphi(|x| \vee |\varphi(x)|) = (|x| \vee |\varphi(x)|)^{-1}.$$

Через $\mathcal{L}_p$ будем обозначать многообразие ℓ -групп, определяемое тождеством $[x^p, y^p] = e$. Пусть P – множество неотрицательных чисел $0, 1, \dots, p-1$ и для любой ℓ -группы G и любых элементов $x, y \in G$ положим [6]:

$$\begin{aligned} d_0(x, y) &= x \wedge x^{-1}y^p x \wedge \dots \wedge x^{-(p-1)}y^p x^{p-1}; \\ d_i(x, y) &= x^{-i}d_0(x, y)x^i, \quad (i = 1, 2, \dots, p-1); \\ c_i(x, y) &= \bigvee_{j \in (P \setminus \{i\})} (d_i(x, y) \wedge d_j(x, y)), \quad (i \in P); \\ a_i(x, y) &= d_i(x, y)c_i^{-1}(x, y), \quad (i \in P). \end{aligned}$$

Непосредственно из определения следует, что $a_i(x, y) \geq e$ в G для любых элементов $x, y \in G$ и любого $i \in P$.

Тогда справедливы следующие утверждения.

Лемма 1.2. [6] В любой ℓ -группе $G \in \mathcal{L}_p$ справедливы следующие равенства:

$$\begin{aligned} c_i(x, y) &= c_j(x, y), \quad (i, j \in P); \\ a_i(x, y) \wedge a_j(x, y) &= e, \quad (i, j \in P, i \neq j); \\ x^{-1}a_i(x, y)x &= a_{i+1}(x, y), \quad (i \in P, i \neq p-1); \\ x^{-1}a_{p-1}(x, y)x &= a_0(x, y). \end{aligned}$$

Лемма 1.3. [6] Пусть $G \in \mathcal{L}_p \setminus \mathcal{A}$. Тогда существуют элементы $x, y \in G$ такие, что $a_i(x, y) > e$, для всех $i \in P$.

Пусть (G, φ) – произвольная m -группа и H – ее произвольная ℓ -подгруппа. Тогда H называется m -подгруппой m -группы (G, φ) если для произвольного $x \in H$ следует, что $\varphi(x) \in H$. Таким образом m -подгруппа H является m -группой относительно индуцированных операций и эту m -группу будем обозначать $(H, \varphi|_H)$, где $\varphi|_H$ – ограничение автоморфизма φ на группе H .

Так как любое многообразие m -групп является радикальным классом [7], то в любой m -группе G есть наибольшая выпуклая абелева m -подгруппа, которая называется абелевым радикалом m -группы G и обозначается $\mathcal{A}(G)$.

Гомоморфизм τ отображающий m -группу (G, φ) в m -группу (H, ψ) такой, что выполняются равенства:

$$\begin{aligned} \tau(x \vee y) &= \tau(x) \vee \tau(y), \\ \tau(x \wedge y) &= \tau(x) \wedge \tau(y), \\ \tau(\varphi(x)) &= \psi(\tau(x)) \end{aligned}$$

для всех $x, y \in (G, \varphi)$, называется m -гомоморфизмом (гомоморфизмом m -групп).

Основные факты и определения по теории групп можно найти в [8], по теории алгебраических систем – в [4].

2 Основной результат

Пусть p – простое число, $S_p = gp < a_0, a_1, \dots, a_{p-1}, b \mid b^{-1}a_i b = a_j, i + 1 \equiv j \pmod{p} >$ – группа, порожденная элементами $a_0, a_1, \dots, a_{p-1}, b$ и $x = b^n a_0^{k_0} a_1^{k_1} \dots a_{p-1}^{k_{p-1}} \geq e$ в S_p , тогда и только тогда, когда $n > 0$ или $n = 0$ и $k_0 \geq 0, k_1 \geq 0, \dots, k_{p-1} \geq 0$. Непосредственная проверка показывает,

что S_p является ℓ -группой относительно этого порядка [2] (стр. 212) и обладает следующими свойствами:

- 1) ℓ -группа S_p подпрямой неразложима;
- 2) ℓ -группа S_p конечно определена в сигнатуре ℓ -групп.

В работе М.Жиrade, И.Рахунека [1] на ℓ -группе S_p , где p – простое число, определен реверсивный автоморфизм второго порядка. Напомним это определение. Пусть $p \geq 3$, тогда реверсивный автоморфизм второго порядка φ определим по следующему правилу: $\varphi(b) = b^{-1}$, $\varphi(a_0) = a_0^{-1}$, $\varphi(a_i) = a_{\overline{p-i}}^{-1}$ для всех $i \neq 0$, где число $\overline{p-i}$ – остаток от деления числа $p-i$ на число p . Для $p = 2$ определим реверсивный автоморфизм второго порядка φ на ℓ -группе S_2 по правилу: $\varphi(a_0) = a_1^{-1}$, $\varphi(a_1) = a_0^{-1}$, $\varphi(b) = b^{-1}$. Тогда (S_p, φ) является m -группой для любого простого числа p . Через $\mathcal{S}_p$ обозначим m -многообразие, порожденное m -группой (S_p, φ) .

Теорема 2.1. *Для любого простого числа p многообразие m -групп $\mathcal{S}_p$, порожденное m -группой (S_p, φ) накрывает многообразие абелевых m -групп $\mathcal{A}$ в решетке многообразий m -групп $\mathbf{A}_m$.*

Доказательство. Вначале докажем, что m -многообразие $\mathcal{A}$ содержится в m -многообразии $\mathcal{S}_p$. Для этого достаточно доказать (с учетом результатов М.Жиrade, И.Рахунека [1]), что m -многообразие $\mathcal{S}_p$ содержит m -подгруппу m -изоморфную m -группе $(\mathbf{Z} \times \mathbf{Z}^*, Exch)$. Рассмотрим m -подгруппу (A, φ) , порожденную элементами a_1, a_{p-1} . Тогда произвольный элемент $x \in A$ имеет вид $x = a_1^s a_{p-1}^t$ и $x = a_1^s a_{p-1}^t \geq e$, если $s \geq 0$ и $t \geq 0$, тогда $\varphi(a_1^s a_{p-1}^t) = a_1^{-s} a_{p-1}^{-t} \leq e$. Определим отображение $\alpha : A \rightarrow \mathbf{Z} \times \mathbf{Z}^*$ по правилу: $\alpha(a_1^s a_{p-1}^t) = (s, -t)$. Изоморфизм $\mathbf{Z} \times \mathbf{Z}^*$ и A как групп очевиден. Покажем, что эти группы ℓ -изоморфны. Пусть $a_1^s a_{p-1}^t > e$, т.е. $s > 0$ и $t > 0$ $\alpha(a_1^s a_{p-1}^t) = (s, -t) > 0$, т.к. $s > 0$ и $-t < 0$ в линейно упорядоченной группе $\mathbf{Z}$, т.е. отображение α является порядковым. Покажем, что это отображение сохраняет решеточные операции, т.е. $\alpha(x \vee y) = \alpha(x) \vee \alpha(y)$ и $\alpha(x \wedge y) = \alpha(x) \wedge \alpha(y)$ для любых элементов $x = a_1^s a_{p-1}^t$ и $y = a_1^{s_1} a_{p-1}^{t_1}$ из ℓ -группы A . Действительно, $\alpha(x \vee y) = \alpha(a_1^s a_{p-1}^t \vee a_1^{s_1} a_{p-1}^{t_1}) = \alpha(a_1^{\max(s, s_1)} a_{p-1}^{\max(t, t_1)}) = (\max(s, s_1), -\max(t, t_1))$. Вычислим $\alpha(x) \vee \alpha(y) = \alpha(a_1^s a_{p-1}^t) \vee \alpha(a_1^{s_1} a_{p-1}^{t_1}) = (s, -t) \vee (s_1, -t_1) = (\max(s, s_1), \min(-t, -t_1)) = (\max(s, s_1), -\max(t, t_1))$. Аналогично доказывается равенство $\alpha(x \wedge y) = \alpha(x) \wedge \alpha(y)$.

Докажем, что α является m -изоморфизмом. Для этого достаточно показать, что выполняется равенство $\alpha(\varphi(x)) = Exch(\alpha(x))$ для произвольного элемента $x \in (A, \varphi)$. Пусть $a_1^s a_{p-1}^t \in (A, \varphi)$, тогда $\varphi(x) = \varphi(a_1^s a_{p-1}^t) = a_1^{-s} a_{p-1}^{-t}$. Рассмотрим элемент $\alpha(\varphi(x)) = \alpha(\varphi(a_1^s a_{p-1}^t)) = \alpha(a_1^{-s} a_{p-1}^{-t}) = (-s, t)$ и элемент $Exch(\alpha(x)) = Exch(\alpha(a_1^s a_{p-1}^t)) = Exch(s,$

$-t) = (-t, s)$. Тем самым доказан m -изоморфизм m -групп (A, φ) и $(\mathbf{Z} \times \mathbf{Z}^*, Exch)$.

Поскольку m -группа (S_p, φ) неабелева, то m -многообразие $\mathcal{S}_p$ строго содержит m -многообразие $\mathcal{A}$. Покажем, что m -многообразие $\mathcal{S}_p$ покрывает $\mathcal{A}$ в решетке m -многообразий Λ_m . Для этого достаточно установить, что всякая некоммутативная m -группа из $\mathcal{S}_p$ содержит m -подгруппу, m -изоморфную m -группе (S_p, φ) . Пусть $P = \{0, 1, \dots, p-1\}$ и K – произвольная неабелева m -группа из многообразия $\mathcal{S}_p$. По леммам 1.2 – 1.3 в K существуют элементы x, y такие, что $x > e$ и слова $x^{-1}a_i(x, y)x = a_{i+1}(x, y)$ попарно ортогональные и положительные в ℓ -группе K .

Рассмотрим случай когда простое число $p \geq 3$. По теореме Биркгофа [4] $\mathcal{S}_p = var_m(S_p, \varphi) = HS \overline{\prod_{\alpha \in J} (S_p, \varphi)_\alpha}$. Тогда K является гомоморфным образом некоторой m -группы G , являющейся m -подгруппой декартова произведения $\overline{\prod_{\alpha \in J} (S_p, \varphi)_\alpha}$. Обозначим этот гомоморфизм m -группы G на m -группу K через χ . Пусть X, Y прообразы элементов $x, y \in K$ соответственно, то тогда $X \vee e$ и Y также прообразы этих элементов соответственно и (с учетом лемм 1.2 – 1.3) имеем $a_i(X \vee e, Y) > e$ в группе G , а $\chi(X \vee e) = \chi(X) = x > e$. Поэтому можно считать, что $X > e$. Пусть $A_i = a_i(X, Y)$. Тогда ℓ -группа $gp(X, A_i)$, порожденная элементами X и A_i изоморфна ℓ -группе S_p , где $i \in P$.

Элементы m -группы G являются элементами декартова произведения $\overline{\prod_{\alpha \in J} (S_p, \varphi)_\alpha}$ и пусть значения $X(\alpha)$ и $A_i(\alpha)$ элементов X и A_i принадлежат m -группе (S_p, φ) . Так как элементы A_i ($i \in P$) попарно ортогональны и сопряжены, то значения $A_i(\alpha)$ данных элементов лежат в абелевом радикале $\mathcal{A}(S_p)$ m -группы (S_p, φ) и $A_i(\alpha)$ равно e или $a_k^{t(k)}$, где $t(k)$ – произвольное натуральное число, $k \in P$. Если $A_0(\alpha) = e$, то элемент $X(\alpha) \in S_p$ имеет вид, т.е. $X(\alpha) = b^{s(\alpha)} a_0^{k_0(\alpha)} \dots a_{p-1}^{k_{p-1}(\alpha)} \geq e$. Если же $A_0(\alpha) = a_k^{t(k)}$, то $X(\alpha) = b^{s(\alpha)} a_0^{k_0(\alpha)} \dots a_{p-1}^{k_{p-1}(\alpha)}$, где $s(\alpha)$ и p взаимно простые числа. Тогда множество индексов J разбивается в объединение двух непересекающихся множеств J_1 и J_2 , где множество индексов J_1 состоит из тех элементов α таких, что $A_i(\alpha) = e$, множество индексов J_2 состоит из тех элементов α , что $A_i(\alpha) = a_k^{t(k)}$, $t(k) > 0$.

Пусть $Z = |X| \vee |\Phi(X)|$. Тогда непосредственные вычисления показывают, что ℓ -группа $gp(Z, A_i)$, порожденная элементами Z и A_i ($i \in P$), изоморфна ℓ -группе S_p . Используя определение реверсивного автоморфизма Φ , имеем если $\alpha \in J_1$, то $A_i(\alpha) = e$ для всех индексов $i \in P$ и в этом случае $(|A_i| \wedge |\Phi(A_i)|)(\alpha) = e$, если $\alpha \in J_2$, то

$$(|A_i| \wedge |\Phi(A_i)|)(\alpha) = \begin{cases} a_0^{t(k)}, & \text{если } A_i(\alpha) = a_0^{t(k)}; \\ e, & \text{если } A_i(\alpha) = a_s^{t(s)} s \in P, s \neq 0. \end{cases}$$

Положим $C = \bigvee_{i \in P} (|A_i| \vee |\Phi(A_i)|)$. Тогда значение $C(\alpha)$ элемента $C = \bigvee_{i \in P} (|A_i| \vee |\Phi(A_i)|)$ имеет вид:

$$C(\alpha) = \begin{cases} a_0^{t(k)} \quad (t(k) > 0), & \text{если } \alpha \in J_2; \\ e, & \text{если } \alpha \in J_1. \end{cases}$$

Действительно, пусть $\alpha \in J_2$ и $A_i(\alpha) = a_k^{t(k)}$, где $t(k) > 0$. Тогда среди индексов $0, 1, 2, \dots, p-1$ найдется такой i_0 , что $A_{i_0}(\alpha) = a_0^{t(k)}$, так как все A_i ($i \in P$) попарно ортогональны и сопряжены, то для произвольного индекса $i \in P$, $i \neq i_0$ имеем $A_i(\alpha) \neq a_0^{t(k)}$. Поэтому, используя определение реверсивного автоморфизма Φ , получаем $(|A_i| \wedge |\Phi(A_i)|)(\alpha) = e$ для всех $i \in P$ и $i \neq i_0$.

Покажем, что ℓ -группа $B(p) = \ell\text{-gp}(Z, C)$, порожденная элементами Z и C , является m -группой и, более того, m -группа $(B(p), \Phi|_{B(p)})$ является m -изоморфной m -группе (S_p, φ) . Действительно, так как Φ является автоморфизмом декартова произведения $\prod_{\alpha \in J} (S_p, \varphi)_\alpha$, то

$$\Phi(Z^m C^{k_0} (C^Z)^{k_1} \dots (C^{Z^{p-1}})^{k_{p-1}}) = \Phi(Z^m) \Phi(C^{k_0}) \Phi((C^Z)^{k_1}) \dots \Phi((C^{Z^{p-1}})^{k_{p-1}}).$$

По выбору элемента Z и по предложению 1.1 имеем:

$$\Phi(Z) = Z^{-1}.$$

Далее,

$$\begin{aligned} \Phi(C) &= \Phi\left(\bigvee_{i \in P} (|A_i| \vee |\Phi(A_i)|)\right) = \bigwedge_{i \in P} \Phi(|A_i| \vee |\Phi(A_i)|) = \\ &= \bigwedge_{i \in P} (|A_i| \vee |\Phi(A_i)|)^{-1} = \left(\bigvee_{i \in P} (|A_i| \vee |\Phi(A_i)|)\right)^{-1} = C^{-1}, \end{aligned}$$

т.е.

$$\Phi(C^Z) = C^{-1}.$$

В силу соотношений $C^{Z^p} = C$, $C^{Z^{p-i}} = C^{Z^{-i}}$ для $i = 1, 2, \dots, p-1$ получаем

$$\Phi(C^{Z^{p-i}}) = \Phi(C^{Z^{-i}}) = (C^{-1})^{Z^i} = (C^{Z^i})^{-1}.$$

Из этих соотношений получаем:

$$\Phi(Z^m C^{k_0} (C^Z)^{k_1} \dots (C^{Z^{p-1}})^{k_{p-1}}) = Z^{-m} C^{-k_0} (C^Z)^{-k_{p-1}} \dots (C^{Z^{p-1}})^{-k_1}.$$

Последнее равенство доказывает изоморфизм m -групп $(B(p), \Phi|_{B(p)})$ и (S_p, φ) .

Применим m -гомоморфизм χ к элементам Z и C и покажем, что $\chi(C) \neq e$. Рассмотрим значение элемента $C \vee C^Z \vee C^{Z^2} \vee \dots \vee C^{Z^{p-1}}$ на $\alpha \in J_2$, т.е.

$$(C \vee C^Z \vee C^{Z^2} \vee \dots \vee C^{Z^{p-1}})(\alpha) = a_0^{t(k)} \vee a^{t(k)} \vee \dots a_{p-1}^{t(k)},$$

Очевидно, что

$$(C \vee C^Z \vee C^{Z^2} \vee \dots \vee C^{Z^{p-1}})(\alpha) \geq A_0(\alpha) \neq e$$

для любого индекса $\alpha \in J = J_1 \cup J_2$. Следовательно

$$C \vee C^Z \vee C^{Z^2} \vee \dots \vee C^{Z^{p-1}} \geq A_0 = a_0(x, y).$$

Поэтому

$$\chi(C \vee C^Z \vee C^{Z^2} \vee \dots \vee C^{Z^{p-1}}) \geq \chi(A_0) = \chi(a_0(x, y)) > e$$

в m -группе K . Таким образом, $\chi(C) > e$ и, следовательно, $\chi(C) \neq e$. Так как элементы $\chi(C)$ и $\chi(C^Z)$ ортогональны, то группа $\chi(B(p), \Phi|_{B(p)})$ является неабелевой. Используя изоморфизм m -групп $(B(p), \Phi|_{B(p)})$ и (S_p, φ) и подпрямую неразложимость ℓ -группы S_p , получаем, что m -группа $\chi(B(p), \Phi|_{B(p)})$ изоморфна m -группе (S_p, φ) , что и доказывает теорему для любого простого числа $p \geq 3$.

Рассмотрим теперь случай $p = 2$. По теореме Биркгофа [4] $\mathcal{S}_2 = \text{var}_m(S_2, \varphi) = HS \overline{\prod}_{\alpha \in J} (S_2, \varphi)_\alpha$. Тогда произвольная неабелева m -группа K из m -многообразия $\mathcal{S}_p$ является гомоморфным образом некоторой m -группы G , являющейся m -подгруппой декартова произведения $\overline{\prod}_{\alpha \in J} (S_2, \varphi)_\alpha$.

Обозначим гомоморфизм m -группы G на m -группу K через χ . Пусть X и Y прообразы элементов x и y соответственно относительно гомоморфизма χ . Без ограничения общности можно считать, что $X > e$. Тогда (с учетом лемм 1.2 – 1.3) имеем $a_0(X, Y) > e$ и $a_1(X, Y) > e$ в группе G . Пусть $A_i = a_i(X, Y)$. Тогда ℓ -группа $\ell\text{-gp}(X, A_0, A_1)$, порожденная элементами X, A_0 и A_1 , изоморфна ℓ -группе S_2 .

Элементы m -группы G являются элементами декартова произведения $\overline{\prod}_{\alpha \in J} (S_2, \varphi)_\alpha$ и пусть значения $X(\alpha), A_0(\alpha)$ и $A_1(\alpha)$ элементов X, A_0, A_1

соответственно принадлежат m -группе (S_2, φ) . Так как элементы A_0 и A_1 ортогональны и сопряжены, то значения $A_i(\alpha)$ данных элементов лежат в абелевом радикале $\mathcal{A}(S_2)$ m -группы (S_2, φ) и $A_i(\alpha)$ равно либо e , либо $a_k^{t(k)}$, где $t(k)$ – произвольное натуральное число для $i = 0, 1$ и $k = 0, 1$. Если $A_0(\alpha) = e$, то элемент $X(\alpha)$ из m -группы (S_2, φ) имеет вид: $X(\alpha) = b^{s(\alpha)} a_0^{k_0(\alpha)} a_1^{k_1(\alpha)}$. Если же $A_0(\alpha) = a_k^{t(k)}$, то $X(\alpha) = b^{s(\alpha)} a_0^{k_0(\alpha)} a_1^{k_1(\alpha)}$, где $s(\alpha)$ нечетное число. Пусть множество индексов $J = J_1 \cup J_2$, где множество индексов J_1 состоит из тех элементов α таких, что $A_i(\alpha) = e$, множество индексов J_2 состоит из тех элементов α , что $A_i(\alpha) = a_k^{t(k)}$ для $i = 0, 1$.

Пусть $Z = |X| \vee |\Phi(X)|$. Тогда непосредственные вычисления показывают, что ℓ -группа $B(2) = \ell\text{-gp}(Z, A_0, A_1)$, порожденная элементами Z, A_0 и A_1 , изоморфна ℓ -группе S_2 , при этом $A_0^X = A_0^Z$. Покажем, что ℓ -группа $B(2)$ является m -группой и, более того, m -группа $(B(2), \Phi|_{B(2)})$ является m -изоморфной m -группе (S_2, φ) . Действительно, так как Φ является автоморфизмом декартова произведения $\prod_{\alpha \in J} (S_2, \varphi)_\alpha$, то

$$\Phi(Z^m A_0^{k_0} (A_0^Z)^{k_1}) = \Phi(Z^m) \Phi(A_0^{k_0}) \Phi((A_0^Z)^{k_1}).$$

По выбору элементов Z и A_0 , и по предложению 1.1 имеем: $\Phi(Z) = Z^{-1}$, $\Phi(A_0) = A_1^{-1}$. Далее, $\Phi(A_0^Z) = \Phi(A_0^X) = A_0^{-1}$. Из этих соотношений получаем:

$$\Phi(Z^m A_0^{k_0} (A_0^Z)^{k_1}) = Z^{-m} A_0^{-k_1} (A_0^Z)^{-k_0}.$$

Последнее равенство доказывает изоморфизм m -групп $(B(2), \varphi|_{B(2)})$ и (S_2, φ) . Далее, применяя рассуждения аналогичные выше рассмотренному случаю, получаем справедливость теоремы для простого числа $p = 2$. $\square$

Список литературы

- [1] *M. Giraudet, J. Rachunek* Varieties of half lattice-ordered groups of monotonic permutations of chains, Czechoslovak Math.J., **49**, (1999), 743-766.
- [2] *В.М. Копытов* Решеточно упорядоченные группы. М.: Наука, 1984.
- [3] *V.M. Kopytov, N.Ya. Medvedev* The theory of lattice-ordered groups, Kluwer Academic Publ., Dordrecht-Boston-London, 1994.

- [4] *А.И. Мальцев* Алгебраические системы. М.: Наука, 1970.
- [5] *Н.В. Баянова, О.В. Никонова* Реверсивные автоморфизмы упорядоченных групп, Сиб. мат. ж., **36**, №4, (1995), 763-768.
- [6] *E.B. Scrimger* A large class of small varieties of lattices-ordered groups.— Proc. Amer. Math.Soc., **51**, №2, (1975) p. 301 – 306.
- [7] *О.В. Исеева* Многообразия и классы кручения m -групп, Алгебра и логика, **42**, №5, (2003).
- [8] *М.И. Каргаполов, Ю.И. Мерзляков* Основы теории групп. М.: Наука, 1972.

О РАЦИОНАЛЬНОСТИ ЗНАЧЕНИЙ КОМПЛЕКСНЫХ ХАРАКТЕРОВ СИЛОВСКИХ 2-ПОДГРУПП СИММЕТРИЧЕСКИХ ГРУПП S_{2^n} .

Колесников С.Г.

Красноярский государственный технический университет,
кафедра прикладной математики
e-mail: sklsnkv@mail.ru, sklsnkv@e-mail.ru

Следуя [1] силовскую 2-подгруппу группы S_{2^n} можно определить по индукции следующим образом: $P_1 = \langle \sigma \mid \sigma^2 = 1 \rangle$; если подгруппа P_{n-1} уже определена, то группа P_n порождается инволюцией σ и подгруппой P_{n-1} , причем выполняются условия: $P_{n-1} \cap P_{n-1}^\sigma = 1$ и $ab^\sigma = b^\sigma a$ для любых $a, b \in P_{n-1}$. Отсюда, в частности, следует, что любой элемент группы P_n представим либо в виде ab , либо в виде σab , где $a \in P_{n-1}, b \in P_{n-1}^\sigma$. В Коуровской тетради Берковичем поставлен следующий вопрос: рациональны ли силовские 2-подгруппы симметрических групп S_{2^n} (группа G называется рациональной, если каждый ее неприводимый комплексный характер принимает только рациональные значения). Справедлива

Теорема. Все неприводимые комплексные характеры силовской 2-подгруппы симметрической группы S_{2^n} принимают рациональные значения.

Доказательство. Подгруппа P_1 , очевидно, рациональна. Пусть уже доказана рациональность подгрупп P_k для $k = 1, \dots, n-1$. Докажем рациональность P_n .

Заметим (см., например, [2]), что для произвольной конечной группы G условие рациональности всех комплексных характеров на элементе $g \in G$ эквивалентно следующему условию: для любого натурального числа i такого, что $(i, |g|) = 1$ элементы g и g^i сопряжены в G . Так как P_n — 2-группа, то нам необходимо и достаточно показать, что любой ее элемент сопряжен с любой своей нечетной степенью.

Случай 1. $g = g_1 g_2$, где $g_1 \in P_{n-1}, g_2 \in P_{n-1}^\sigma$.

Так как $g_1g_2 = g_2g_1$, то $g^{2k+1} = g_1^{2k+1}g_2^{2k+1}$. По предположению индукции существуют такие элементы $a \in P_{n-1}$ и $b \in P_{n-1}^\sigma$, что $ag_1a^{-1} = g_1^{2k+1}$ и $bg_2b^{-1} = g_2^{2k+1}$. Отсюда

$$(ab)g(ab)^{-1} = (ab)g_1g_2(b^{-1}a^{-1}) = (ag_1a^{-1})(bg_2b^{-1}) = g_1^{2k+1}g_2^{2k+1} = g^{2k+1}.$$

Случай 2. $g = \sigma g_1g_2$, где $g_1 \in P_{n-1}$, $g_2 \in P_{n-1}^\sigma$.
Докажем индукцией по k , что

$$g^{2k+1} = \sigma(g_1g_2^\sigma)^k g_1(g_2g_1^\sigma)^k g_2 \quad (2.1)$$

При $k = 0$ равенство (2.1), очевидно, выполняется. Далее

$$\begin{aligned} g^{2k+3} &= \sigma(g_1g_2^\sigma)^k g_1(g_2g_1^\sigma)^k g_2(\sigma g_1g_2)(\sigma g_1g_2) \\ &= \sigma(g_1g_2^\sigma)^k g_1(g_2g_1^\sigma)^k g_2g_1^\sigma g_2^\sigma g_1g_2 \\ &= \sigma(g_1g_2^\sigma)^k g_1g_2^\sigma g_1(g_2g_1^\sigma)^k g_2g_1^\sigma g_2 \\ &= \sigma(g_1g_2^\sigma)^{k+1} g_1(g_2g_1^\sigma)^{k+1} g_2. \end{aligned}$$

Таким образом равенство (2.1) доказано.

Элемент $g_1g_2^\sigma$ лежит в P_{n-1} . Поэтому по индукционному предположению в P_{n-1} найдется такой элемент x , что

$$xg_1g_2^\sigma x^{-1} = (g_1g_2^\sigma)^{2k+1} \quad (2.2)$$

Положим

$$a = (g_2^\sigma g_1)^k g_2^\sigma x (g_2^\sigma)^{-1} \quad (2.3)$$

Тогда

$$\begin{aligned} a^{-1} &= g_2^\sigma x^{-1} (g_2^\sigma)^{-1} (g_2^\sigma g_1)^{-k} \\ &= g_1^{-1} x^{-1} x g_1 g_2^\sigma x^{-1} (g_2^\sigma)^{-1} (g_2^\sigma g_1)^{-k} \\ &= g_1^{-1} x^{-1} (g_1 g_2^\sigma)^{2k+1} (g_2^\sigma)^{-1} (g_2^\sigma g_1)^{-k} \\ &= g_1^{-1} x^{-1} (g_1 g_2^\sigma)^k g_1. \end{aligned}$$

последний переход осуществляем следующим образом: расписываем $(g_1 g_2^\sigma)^{2k+1} = g_1 g_2^\sigma \dots g_1 g_2^\sigma$ и $(g_2^\sigma g_1)^{-k} = g_1^{-1} (g_2^\sigma)^{-1} \dots g_1^{-1} (g_2^\sigma)^{-1}$, а затем производим очевидные сокращения. Таким образом

$$a^{-1} = g_1^{-1} x^{-1} (g_1 g_2^\sigma)^k g_1. \quad (2.4)$$

Из равенств (2.3) и (2.4) следует, что

$$a g_2^\sigma x^{-1} = (g_2^\sigma g_1)^k g_2^\sigma, \quad (2.5)$$

$$xg_1a^{-1} = (g_1g_2^\sigma)^k g_1. \quad (2.6)$$

Из (2.5), сопрягая элементом σ , получим

$$a^\sigma g_2(x^{-1})^\sigma = (g_2g_1^\sigma)^k g_2. \quad (2.7)$$

Положим $b = x^\sigma$. Тогда и $b^\sigma = x$ равенства (2.6),(2.7) перепишутся в виде

$$\begin{aligned} b^\sigma g_1a^{-1} &= (g_1g_2^\sigma)^k g_1, \\ a^\sigma g_2b^{-1} &= (g_2g_1^\sigma)^k g_2. \end{aligned}$$

Отсюда

$$\begin{aligned} (ab)g(ab)^{-1} &= abga^{-1}b^{-1} \\ &= ab\sigma g_1g_2a^{-1}b^{-1} \\ &= \sigma a^\sigma b^\sigma g_1g_2a^{-1}b^{-1} \\ &= \sigma(b^\sigma g_1a^{-1})(a^\sigma g_2b^{-1}) \\ &= \sigma(g_1g_2^\sigma)^k g_1(g_2g_1^\sigma)^k g_2 = g^{2k+1}. \end{aligned}$$

Теорема доказана.

Из доказанной теоремы вытекает положительное решение вопроса 15.25 (Беркович) из Коуровской тетради.

Список литературы

- [1] Холл М. Теория групп. // J. London Math. Soc.1937. V. 12. P. 201-204.
- [2] Серр Ж.-П. Группы Галуа над $\mathbb{Q}$. // В кн.: Труды семинара Бурбаки за 1988г., М.: Мир, 1990.

О ПОВЕДЕНИИ ОДНОМЕСТНЫХ ФУНКЦИЙ В СЛАБО О-МИНИМАЛЬНЫХ ТЕОРИЯХ

Б.Ш. Кулпешов

Институт проблем информатики и управления,
Министерство образования и науки,
ул. Пушкина 125,
Алматы 480100, Казахстан
e-mail: kulpesh@usa.net

Пусть L — счетный язык первого порядка. Повсюду в этой статье мы рассматриваем L -структуры и предполагаем что L содержит символ бинарного отношения $<$, который интерпретируется в этих структурах как линейный порядок. Для произвольных подмножеств A, B структуры M мы пишем $A < B$, если $a < b$ всякий раз когда $a \in A$ и $b \in B$. Если $A \subset M$ и $x \in M$, то мы пишем $A < x$, если $A < \{x\}$. Для произвольного полного 1-типа p мы обозначаем через $p(M)$ множество реализаций типа p в M .

Открытый интервал I в структуре M есть параметрически определенное подмножество структуры M вида $I = \{c \in M : M \models a < c < b\}$ для некоторых $a, b \in M \cup \{-\infty, \infty\}$, где $a < b$. Аналогично, мы можем определить *замкнутые*, *полуоткрытые-полузамкнутые* и т.п. интервалы в M , так что например произвольная точка структуры M является сама (тривиальным) замкнутым интервалом. Подмножество A структуры M называется *выпуклым*, если для любых $a, b \in A$ и $c \in M$ всякий раз когда $a < c < b$ мы имеем $c \in A$.

Данная статья касается понятия *слабой о-минимальности*, впервые введенного М. Дикманном в [1]. *Слабо о-минимальная структура* есть линейно упорядоченная структура $M = \langle M, =, <, \dots \rangle$ такая, что любое определенное (с параметрами) подмножество структуры M является объединением конечного числа выпуклых множеств в M . Вспомним что такая структура M называется *о-минимальной*, если каждое определенное (с параметрами) подмножество структуры M является объединением конечного числа интервалов в M . Понятие о-минимальности было введено А. Пиллэем и Ч. Стейнхорном в [2]. Ранг выпуклости формулы с одной свободной переменной введен в [3]. В частности, теория имеет

ранг выпуклости 1, если не существует определимого (с параметрами) отношения эквивалентности с бесконечным числом выпуклых бесконечных классов. Очевидно что о-минимальная теория имеет ранг выпуклости 1. В настоящей работе мы классифицируем поведение одноместной функции во множестве реализаций неалгебраического 1-типа слабо о-минимальной теории в терминах глубины функции (Теорема 19), а также доказываем некоторые свойства неортогональности неалгебраических 1-типов в слабо о-минимальной теории ранга выпуклости 1 (Теорема 24).

Определение 1. [3] Пусть M — линейно упорядоченная структура, $\phi(x)$ — M -определимая формула с одной свободной переменной.

Ранг выпуклости формулы $\phi(x)$ ($RC(\phi(x))$) определяется следующим образом:

- 1) $RC(\phi(x)) = -1$, если $M \models \neg \exists x \phi(x)$
- 2) $RC(\phi(x)) \geq 0$, если $M \models \exists x \phi(x)$
- 3) $RC(\phi(x)) \geq 1$, если $\phi(M)$ бесконечно
- 4) $RC(\phi(x)) \geq \alpha + 1$, если существует параметрически определимое отношение эквивалентности $E(x, y)$, такое что существуют $b_i, i \in \omega$, которые удовлетворяют следующим условиям:

- Для любых $i, j \in \omega$, всякий раз когда $i \neq j$, тогда $M \models \neg E(b_i, b_j)$
- Для любого $i \in \omega$ $RC(E(x, b_i)) \geq \alpha$
- Для любого $i \in \omega$ $E(M, b_i)$ является выпуклым подмножеством множества $\phi(M)$

5) $RC(\phi(x)) \geq \delta$, если $RC(\phi(x)) \geq \alpha$ для всех $\alpha \leq \delta$ (δ предельный ординал)

Если $RC(\phi(x)) = \alpha$ для некоторого α , мы говорим что $RC(\phi(x))$ определяется. В противном случае (т.е. если $RC(\phi(x)) \geq \alpha$ для всех α) мы полагаем $RC(\phi(x)) = \infty$.

В следующих определениях M — слабо о-минимальная структура, $A, B \subseteq M$, M — $|A|^+$ -насыщенна, $p, q \in S_1(A)$ — неалгебраические.

Определение 2. (Байжанов Б.С., [4]) Будем говорить что тип p не является слабо ортогональным типу q ($p \not\perp^w q$), если существуют A -определимая формула $H(x, y)$, $\alpha \in p(M)$ и $\beta_1, \beta_2 \in q(M)$ такие что $\beta_1 \in H(M, \alpha)$ и $\beta_2 \notin H(M, \alpha)$.

Лемма 3. [4], Следствие 34 (iii)) $\not\perp^w$ является отношением эквивалентности на $S_1(A)$.

Определение 4. (Байжанов Б.С., [5]) Будем говорить что тип p не является *почти ортогональным* типу q ($p \not\perp^a q$), если существуют A -определимая формула $H(x, y)$, $\alpha \in p(M)$ и $\beta_1, \beta_2 \in q(M)$ такие что $H(M, \alpha) \neq \emptyset$ и $\beta_1 < H(M, \alpha) < \beta_2$.

Факт 5. $p \not\perp^a q \Rightarrow p \not\perp^w q$.

Определение 6. (Байжанов Б.С., [5]) Будем говорить что слабо о-минимальная теория T является *почти о-минимальной*, если для любой модели $M \models T$ для любого $A \subseteq M$ для любых неалгебраических типов $p, q \in S_1(A)$ имеет место следующее: $p \perp^a q \Leftrightarrow p \perp^w q$.

Факт 7. Любая о-минимальная теория является почти о-минимальной.

Пример 8. Пусть $M = \langle M, <, =, U_1^1, U_2^1, R^2 \rangle$, где $\langle M, < \rangle$ имеет порядковый тип Q . Универсум M есть непересекающееся объединение U_1 и U_2 с условием $a < b$ всякий раз когда $a \in U_1, b \in U_2$, и каждый предикат U_i не имеет конечных точек в M . Чтобы определить R , отождествим U_i с Q для каждого $i \leq 2$, и для любых $a \in U_1$ и $b \in U_2$ мы имеем $R(a, b) \Leftrightarrow b < a + \sqrt{2}$.

Очевидно что $Th(M)$ допускает элиминацию кванторов. Можно доказать что $Th(M)$ — слабо о-минимальная теория. Пусть $p = \{U_1\}$, $q = \{U_2\}$. Очевидно что $p, q \in S_1(\emptyset)$, $p \perp^a q$, но $p \not\perp^w q$, т.е. $Th(M)$ не является почти о-минимальной.

Лемма 9. ([3], Следствие 5.5) Пусть T — слабо о-минимальная теория ранга выпуклости 1. Тогда T имеет Принцип Замены для алгебраического замыкания.

Пусть $Y \subset M^{n+1}$ — $\emptyset$ -определимо, $\pi : M^{n+1} \rightarrow M^n$ — проекция, отбрасывающая последнюю координату, $Z := \pi(Y)$, и для $\bar{a} \in Z$ $Y_{\bar{a}} := \{y : (\bar{a}, y) \in Y\}$. Предположим, что для каждого $\bar{a} \in Z$ множество $Y_{\bar{a}}$ ограничено сверху, но не имеет супремума в M . Определим отношение эквивалентности $\sim$ на M^n следующим образом: множество $M^n \setminus Z$ является одним $\sim$ -классом, и для $\bar{a}, \bar{b} \in Z$ $\bar{a} \sim \bar{b}$ тогда и только тогда, когда $\sup Y_{\bar{a}} = \sup Y_{\bar{b}}$. Пусть $\bar{Z} := Z / \sim$, и для каждого $\bar{x}$ пусть $[\bar{x}]$ обозначает $\sim$ -класс кортежа $\bar{x}$. Существует естественный $\emptyset$ -определимый линейный порядок на $M \cup \bar{Z}$, определенный следующим образом: если $\bar{a} \notin Z$, тогда $[\bar{a}] < x$ для всех $x \in M$; если $\bar{a} \in Z$ и $x \in M$, тогда $[\bar{a}] < x$ тогда и только тогда, когда $w < x$ для любого $w \in Y_{\bar{a}}$. Ясно что если $\bar{a} \not\sim \bar{b}$, тогда существует $x \in M$, такой что $[\bar{a}] < x < [\bar{b}]$ или $[\bar{b}] < x < [\bar{a}]$, поэтому мы получаем линейный порядок на $M \cup \bar{Z}$. Мы называем такое

множество $\overline{Z}$ сортом в $\overline{M}$ (в данном случае, $\emptyset$ -определимым сортом). Аналогично мы можем получить сорт в $\overline{M}$, рассматривая инфимумы вместо супремумов.

Определение 10. [6] Пусть M — линейно упорядоченная структура, $D \subseteq M$ — бесконечно, $K \subseteq \overline{M}$, $f : D \rightarrow K$ — функция. Будем говорить, что f является *опрятной*, если выполняется одно из следующих свойств:

1. Для любого $x \in D$ существует бесконечный интервал $J \subseteq D$, содержащий x , так что f является строго монотонно возрастающей на J (будем говорить, что f *локально возрастающая* на D)
2. Для любого $x \in D$ существует бесконечный интервал $J \subseteq D$, содержащий x , так что f является строго монотонно убывающей на J (будем говорить, что f *локально убывающая* на D)
3. Для любого $x \in D$ существует бесконечный интервал $J \subseteq D$, содержащий x , так что f является константой на J (будем говорить, что f *локально константа* на D)

Определение 11. [6] Если M — линейно упорядоченная структура, $B \subseteq M$, тогда будем говорить, что M *имеет монотонность*, если всякий раз когда $A \subseteq \overline{M}$ — B -определимый сорт и $f : M \rightarrow A$ — B -определимая частичная функция, мы имеем что существует $m \in \omega$ и разбиение $\text{dom}(f)$ на B -определимые множества $X, I_1, \dots, I_m$ так что X конечно, каждое I_i выпукло и бесконечно, и на каждом I_i функция f является опрятной.

Теорема 12. (Арефьев Р.Д., [7]) *Любая слабо о-минимальная структура имеет монотонность.*

Будем говорить, что функция f является *локально монотонной* на множестве $D \subseteq M$, если f не является строго монотонной на D и f является либо локально возрастающей, либо локально убывающей, либо локально константой на D .

Лемма 13. Пусть M — слабо о-минимальная структура, $B, D \subseteq M$, $A \subseteq \overline{M}$ — B -определимый сорт и $f : D \rightarrow A$ — B -определимая функция. Предположим что функция f является локально монотонной на D . Тогда существует B -определимое отношение эквивалентности $E_f(x, y)$, разбивающее D на бесконечное число выпуклых открытых классов.

Доказательство Леммы 13.

Рассмотрим случай локально возрастающей функции. Тогда следующее отношение является искомым:

$$E_f(x, y) := [x < y \rightarrow \forall t[x < t < y \rightarrow f(x) < f(t) < f(y)]] \wedge \\ \wedge (x > y \rightarrow \forall t[x > t > y \rightarrow f(x) > f(t) > f(y)])$$

□

Следствие 14. Пусть T — слабо о-минимальная теория ранга выпуклости 1, $M \models T$, $B \subseteq M$. Тогда всякий раз когда $A \subseteq \overline{M}$ является B -определимым сортом и $f : M \rightarrow A$ есть B -определимая частичная функция, существует $m \in \omega$ и разбиение $\text{dom}(f)$ на B -определимые множества $X, I_1, \dots, I_m$ так что X конечно, каждое I_i бесконечно и выпукло, и на каждом множестве I_i функция f является строго монотонной или константой.

Следствие 15. Пусть T — слабо о-минимальная теория ранга выпуклости 1, $M \models T$, $A \subseteq M$, $p \in S_1(A)$ — неалгебраический. Тогда любая функция в определимый сорт, область определения которой содержит $p(M)$, является монотонной или константой на $p(M)$.

Лемма 16. Пусть T — слабо о-минимальная теория, $M \models T$, $A \subseteq M$, $U(x), U'(x)$ изолируют полные неалгебраические 1-типы над A , $U(M) \cap U'(M) = \emptyset$. Предположим что существует $b \in U(M)$ такой что $\text{dcl}(A \cup \{b\}) \cap U'(M) \neq \emptyset$. Тогда имеет место следующее:

1. Если в любой модели теории T имеет место Принцип Замены для алгебраического замыкания, то существует A -определимая биекция $f : U(M) \rightarrow U'(M)$, являющаяся одной из следующих: монотонная, локально возрастающая или локально убывающая.
2. Если T имеет ранг выпуклости 1, то существует A -определимая монотонная биекция $f : U(M) \rightarrow U'(M)$
3. Если к пункту 1 или 2 добавить условие $\aleph_0$ -категоричности T , то данная биекция единственна.

Определение 17. (Вербовский В.В., [8]) Пусть M — слабо о-минимальная структура, $B, D \subseteq M$, $A \subseteq \overline{M}$ — B -определимый сорт и $f : D \rightarrow A$ — B -определимая функция, являющаяся локально возрастающей (убывающей) на D . Будем говорить, что функция f имеет глубину n на множестве D , если существуют отношения эквивалентности $E_1(x, y), \dots, E_n(x, y)$,

разбивающие D на бесконечное число бесконечных выпуклых классов так что для любого $2 \leq i \leq n$ каждый E_i -класс разбивается на бесконечное число бесконечных выпуклых E_{i-1} -подклассов и выполняется следующее:

- $f|_{E_k}$ является локально убывающей (возрастающей) для любого нечетного $k \leq n$
- $f|_{E_k}$ является локально возрастающей (убывающей) для любого четного $k \leq n$
- $f|_{E_n}$ является строго монотонной.

В этом случае функцию f будем называть *локально возрастающей (убывающей) глубины n* .

Строго монотонно возрастающую (убывающую) функцию назовем *локально возрастающей (убывающей) глубины 0*.

Теорема 18. (Вербовский В.В., [8]) Пусть — слабо o -минимальная теория. Тогда любая функция в определимый сорт имеет конечную глубину.

Теорема 19. Пусть T — слабо o -минимальная теория, $M \models T$, $A \subseteq M$, $p \in S_1(A)$ — неалгебраический. Предположим что существуют $a, b \in p(M)$ и формула $\Phi(x, y)$ такие что $\Phi(M, b) \subseteq p(M)$ и $\Phi(M, b) < a$. Тогда функция $f(y) := \sup \Phi(M, y)$ имеет только одно из следующих поведений на $p(M)$:

1. f — локально возрастающая четной глубины.
2. f — локально убывающая нечетной глубины.
3. f — локально константа, причем $f|_{E_f}$ является строго монотонно возрастающей на $p(M)$.

Доказательство Теоремы 19.

1. Допустим противное: f — локально возрастающая нечетной глубины n . Тогда из Определения 17 следует существование отношения эквивалентности E_n такого, что $f|_{E_n}$ — строго монотонно убывающая на $p(M)$. Рассмотрим следующие формулы:

$$\theta^+(x) := f(x) \geq x, \quad \theta^-(x) := f(x) < x$$

Очевидно что $\theta^+(M) \cap \theta^-(M) = \emptyset$. Поймем что $\theta^+(M) \cap p(M) \neq \emptyset$, $\theta^-(M) \cap p(M) \neq \emptyset$. Предположим что $\theta^+(M) \cap p(M) = \emptyset$ и рассмотрим $a_1, a_2 \in$

$p(M)$ такие что $a_1 < a_2$ и $\neg E_n(a_1, a_2)$. Так как $f|_{E_n}$ строго монотонно убывающая, то $f(a_1) > f(a_2)$. Так как $\theta^+(M) \cap p(M) = \emptyset$, то $f(a_2) < f(a_1) < a_1 < a_2$. Очевидно что $\neg E_n(f(a_2), a_2)$, поэтому $f^2(a_2) > f(a_2)$. С другой стороны, так как $\theta^+(M) \cap p(M) = \emptyset$, то $f(a_2) > f^2(a_2)$. Противоречие. Следовательно, $\theta^+(M) \cap p(M) \neq \emptyset$. Аналогично можно показать что $\theta^-(M) \cap p(M) \neq \emptyset$. Тогда получаем что как $p(x) \cup \{\theta^+(x)\}$, так и $p(x) \cup \{\theta^-(x)\}$ оба совместны, противоречия тому что p является полным типом над A . Аналогично рассматриваются остальные случаи. $\square$

Следствие 20. Пусть T — слабо о-минимальная теория, $M \models T$, $A \subseteq M$, $p \in S_1(A)$ — неалгебраический. Предположим что существуют $a, b \in p(M)$ такие что $a \neq b$ и $a \in \text{dcl}(A \cup \{b\})$. Тогда имеет место следующее:

1. Если в любой модели теории T имеет место Принцип Замены для алгебраического замыкания, то существует A -определимая биекция $f : p(M) \rightarrow p(M)$, являющаяся либо локально возрастающей четной глубины, либо локально убывающей нечетной глубины.
2. Если T имеет ранг выпуклости 1, то существует A -определимая строго монотонно возрастающая биекция $f : p(M) \rightarrow p(M)$.
3. T не является $\aleph_0$ -категоричной.

Определение 21. (Байжанов Б.С., [5]) Пусть M — слабо о-минимальная структура, $A \subseteq M$, M — $|A|^+$ -насыщенна, $p \in S_1(A)$ — неалгебраический. Будем говорить что тип p является *неодиночным*, если существуют A -определимая формула $H(x, y)$ и $\alpha, \gamma_1, \gamma_2 \in p(M)$ такие что $H(M, \alpha) \setminus \{\alpha\} \neq \emptyset$ и $\gamma_1 < H(M, \alpha) < \gamma_2$.

Лемма 22. Пусть T — слабо о-минимальная теория ранга выпуклости 1, $M \models T$, $A \subseteq M$, $p_1, p_2 \in S_1(A)$ — неалгебраические, p_2 — одиночный. Предположим что существует $b \in p_1(M)$ такой что $\text{dcl}(A, b) \cap p_2(M) \neq \emptyset$. Тогда существует единственная A -определимая биекция $f : p_1(M) \rightarrow p_2(M)$ так что f является монотонной.

Доказательство Леммы 22.

Учитывая Лемму 16, осталось показать единственность такой биекции. Допустим противное: существует другая A -определимая биекция $g : p_1(M) \rightarrow p_2(M)$. Так как $f \neq g$, то существует $b \in p_1(M)$ такой что $f(b) \neq g(b)$. Пусть $f(b) = c_1$, $g(b) = c_2$ и пусть для определенности $c_1 < c_2$. Тогда $gf^{-1} : p_2(M) \rightarrow p_2(M)$ — биекция (определимая над A), причем $gf^{-1}(c_1) = c_2$. Рассмотрим следующую формулу: $H(x, y) :=$

$x \leq y \leq gf^{-1}(x)$. Очевидно что $H(x, y)$ — A -определимая формула и $c_1 \leq H(c_1, M) \leq c_2$, противоречия одиночности типа p_2 . $\square$

Лемма 23. Пусть T — слабо o -минимальная теория ранга выпуклости 1, $M \models T$, $A \subseteq M$, $p_1, p_2 \in S_1(A)$ — неалгебраические, p_2 — одиночный. Предположим что существует $b \in p_1(M)$ такой что $dcl(A, b) \cap p_2(M) = \emptyset$. Тогда не существует A -определимой формулы $\Theta(x, y)$ такой, что $\Theta(M, b)$ выпукло и для некоторых $c_1, c_2 \in p_2(M)$ имеет место следующее: $c_1 < \Theta(M, b) < c_2$.

Доказательство Леммы 23.

Допустим противное: предположим что существует A -определимая формула $\Theta(x, y)$ такая, что $\Theta(M, b)$ выпукло и существуют $c_1, c_2 \in p_2(M)$ с условием $c_1 < \Theta(M, b) < c_2$. Так как $dcl(A, b) \cap p_2(M) = \emptyset$, то $\Theta(M, b)$ бесконечно. Рассмотрим произвольный элемент $c \in \Theta(M, b)$ и $g \in \text{Aut}_A(M)$ такой, что $g(c_1) = c_2$. Тогда мы имеем

$$\Theta(M, g^{-1}(b)) < g^{-1}(c_2) = c_1 < \Theta(M, b) < c_2 = g(c_1) < \Theta(M, g(b))$$

Так как $c \in \Theta(M, b)$, то мы имеем $\Theta(M, g^{-1}(b)) < c < \Theta(M, g(b))$, т.е. $g^{-1}(b), g(b) \notin \Theta(c, M)$. Предположим что $g(b) < b$. Тогда мы имеем $b < g^{-1}(b)$ и следовательно $g(b) < \Theta(c, M) < g^{-1}(b)$. Рассмотрим следующую формулу:

$$H(x, c) := \exists y[\Theta(c, y) \wedge \Theta(x, y)]$$

Ясно что $H(M, c) \subseteq p_2(M)$. Покажем что существуют $\gamma_1, \gamma_2 \in p_2(M)$ с условием $\gamma_1 < H(M, c) < \gamma_2$. Пусть $D(x) := \exists y\Theta(y, x)$, $B := D(M)$. Определим отношение эквивалентности $\sim$ на M следующим образом: для любых $a_1, a_2 \in B$, $a_1 \sim a_2$ тогда и только тогда, когда $\sup \Theta(M, a_1) = \sup \Theta(M, a_2)$. Пусть $\bar{B} := B / \sim$.

Определим функцию $f : M \rightarrow \bar{B}$ следующим образом: $f(x) := \sup \Theta(M, x)$.

В силу Следствия 15 f должна быть монотонной или константой на $p_1(M)$. Так как существуют $c_1, c_2 \in p_2(M)$ такие что $c_1 < f(b) < c_2$, то f не может быть константой. Если f является строго монотонно возрастающей, то $f(g^{-1}(b)) > f(d)$ для любого $d \in \Theta(c, M)$. Если f является строго монотонно убывающей, то $f(g(b)) > f(d)$ для любого $d \in \Theta(c, M)$. Таким образом, в любом случае существует $\gamma_2 \in p_2(M)$ такой что $H(M, c) < \gamma_2$. Аналогично рассматривая $\mu(x) := \inf \Theta(M, x)$, можно показать что существует $\gamma_1 \in p_2(M)$ такой что $\gamma_1 < H(M, c)$. Получаем противоречие одиночности типа p_2 . $\square$

Теорема 24. Пусть T — слабо o -минимальная теория ранга выпуклости 1, $M \models T$, $A \subseteq M$, $p_1, p_2 \in S_1(A)$ — неалгебраические, p_2 — одиночный. Предположим что $p_1 \not\perp^w p_2$. Тогда либо $p_1 \perp^a p_2$, либо существует единственная A -определимая монотонная биекция $f : p_1(M) \rightarrow p_2(M)$.

Доказательство Теоремы 24 следует из Лемм 22 и 23.

Следствие 25. Пусть T — почти o -минимальная теория ранга выпуклости 1, $M \models T$, $A \subseteq M$, $p_1, p_2 \in S_1(A)$ — неалгебраические, p_2 — одиночный. Тогда либо $p_1 \perp^w p_2$, либо существует единственная A -определимая монотонная биекция $f : p_1(M) \rightarrow p_2(M)$.

Список литературы

- [1] M.A. Dickmann, *Elimination of quantifiers for ordered valuation rings*, **Proceedings of the 3rd Easter Model Theory Conference at Gross Koris**, Berlin, 1985.
- [2] A. Pillay, Ch. Steinhorn, *Definable sets in ordered structures I*, **Transactions of the American Mathematical Society**, 295 (1986), pp. 565–592.
- [3] B.Sh. Kulpeshov, *Weakly o -minimal structures and some of their properties*, **The Journal of Symbolic Logic**, 63 (1998), pp. 1511–1528.
- [4] B.S. Baizhanov, *Expansion of a model of a weakly o -minimal theory by a family of unary predicates*, **The Journal of Symbolic Logic**, 66 (2001), pp. 1382–1414.
- [5] B.S. Baizhanov, *Orthogonality of one-types in weakly o -minimal theories*, **Algebra and Model Theory II**, (A.G. Pinus and K.N. Ponomaryov, editors), Novosibirsk State Technical University, 1999, pp. 3–28.
- [6] H.D. Macpherson, D. Marker, and Ch. Steinhorn, *“Weakly o -minimal structures and real closed fields”*, **Transactions of The American Mathematical Society**, 352 (2000), pp. 5435–5483.
- [7] Р.Д. Арефьев, *О свойстве монотонности слабо o -минимальных моделей*, **Algebra and Model Theory**, (A.G. Pinus and K.N. Ponomaryov, editors), Novosibirsk, 1997, pp. 8–15.
- [8] V.V. Verbovskiy, *On formula depth of weakly o -minimal structures*, **Algebra and Model Theory**, (A.G. Pinus and K.N. Ponomaryov, editors), Novosibirsk, 1997, pp. 209–223.

О СЛАБО ФАКТОРИЗУЕМЫХ ГРУППАХ ЛИЕВА ТИПА МАЛЫХ РАНГОВ И СПОРАДИЧЕСКИХ ГРУППАХ

А.Г. Лихарев*

Красноярский госуниверситет
кафедра алгебры и математической логики,
пр. Свободный, 79, Красноярск 660041
e-mail: levchuk@lan.krasu.ru

Введение. Подгруппу группы G назовем *слабо дополняемой* в G , если она дополняема в некоторой большей подгруппе группы G или совпадает с G . Напомним, что подгруппу M называют *дополняемой* в группе G , если в G существует *дополнение* к ней, т.е. подгруппа K такая, что $M \cap K = 1$ и $MK = G$. Группы с дополняемыми подгруппами (вполне факторизуемые группы) изучены в работах Ф. Холла [1], С. Н. Черникова [2] и Н. В. Баевой (Черниковой) [3], [4]. В "Коуровской тетради" [5] записан вопрос 8.31 об описании конечных слабо факторизуемых групп, т.е. групп у которых каждая подгруппа слабо дополняема. В работе В. М. Левчука [6] рассматриваются некоторые свойства слабо факторизуемых групп и выявляется склонность к слабой факторизуемости силовских подгрупп конечных классических групп. Там же высказывается гипотеза о том, что простые неабелевы конечные группы со свойством слабой факторизуемости исчерпываются единственной группой — $PSL_2(7) (\cong PSL_3(2))$.

Справедливость гипотезы для групп $PSL_2(q)$ над конечным полем порядка q по существу вытекает из работы Н. Ито [7], описывающей факторизации этих групп. В данной работе гипотеза подтверждается для некоторых спорадических групп (теорема 2), для групп лиева типа ранга 1 и групп $PSL_3(q)$, за несколькими исключениями (теоремы 1).

*Работа выполнена при поддержке Российского фонда фундаментальных исследований (код проекта 03-01-00905).

§ 1. В этом параграфе доказывается следующая теорема.

Теорема 1 Пусть $G(q)$ простая группа Шевалле лиева ранга 1 над конечным полем порядка q или $G(q) = PSL_3(q)$. Если $G(q)$ слабо факторизуемая группа, то $G(q) \cong PSL_3(q)$, $q = 2, 3, 4$.

В группах Шевалле мономиальная подгруппа N и подгруппа Бореля (см. [8], [9]), как правило, являются максимальными подгруппами. Отметим, что условие слабой дополняемости максимальных подгрупп равносильно условию их дополняемости во всей группе (см. лемма 3 [6]). Поэтому для доказательства теоремы достаточно установить не дополняемость подгруппы Бореля или мономиальной подгруппы во всей группе.

Следующая лемма устанавливает не дополняемость подгруппы Бореля в некоторых группах.

Лемма 1. В группах $Sz(q)$, $q = 2^{2k+1}$, $k \geq 1$ и $Re(q)$, $q = 3^{2k+1}$, $k \geq 1$ подгруппа Бореля не дополняема.

Доказательство. В группе $G(q)$ подгруппа Бореля совпадает с нормализатором силовой p -подгруппы группы $G(q)$, где p — характеристика основного поля.

Рассмотрим группу $Sz(q)$, $q = 2^{2k+1}$, $k \geq 1$ (при $k = 1$ группа $Sz(q)$ так же как и $Re(q)$ не является простой). Как установлено в [10], максимальная подгруппа группы $Sz(q)$, $q = 2^{2k+1}$, $k \geq 1$ сопряжена в ней с одной из следующих подгрупп:

- а) $Sz(m)$, где $m^p = q$, p -простое число, делящее $2k + 1$, порядка $m^2(m - 1)(m^2 - 1)$;
- б) группа Фробениуса порядка $4(q + r + 1)$, $r^2 = 2q$;
- в) нормализатор в группе $Sz(q)$ подгруппы всех ее диагональных матриц, изоморфный диэдральной группе порядка $2(q - 1)$;
- г) группа Бореля порядка $q^2(q - 1)$.

Пусть существует неединичное дополнение K к подгруппе Бореля в $Sz(q)$. В силу того, что $|Sz(q)| = q^2(q - 1)(q^2 + 1)$, порядок группы K равен $(q^2 + 1)$. Воспользовавшись описанием максимальных подгрупп легко увидеть, что $Sz(q)$ не содержит подгрупп такого порядка.

Аналогичные рассуждения применимы и для групп $Re(q)$. Как установлено в [11], максимальная подгруппа группы $Re(q)$, $q = 3^{2k+1}$, $k \geq 1$ сопряжена в ней с одной из следующих подгрупп:

- а) $C(\eta)$ — централизатор инволюции η порядка $q(q^2 - 1)$;
- б) $Re(m)$, где $m^p = q$, p -простое число, делящее $2k + 1$, порядка $m^3(m - 1)(m^3 - 1)$;

в) $N(A_i)$ - нормализатор подгруппы A_i , $i = 1, 2, 3$, где A_i - циклические холловы подгруппы порядка $q + 1/4$, $q + 1 - 3^{n+1}$, $q + 1 + 3^{n+1}$ соответственно;

г) группа Бореля порядка $q^3(q - 1)$.

Пусть $k \geq 1$ и K — неединичное дополнение к подгруппе Бореля в $Re(q)$. Порядок группы $Re(q)$ равен $q^3(q - 1)(q^3 + 1)$, отсюда $|K| = q^3 + 1$. Воспользовавшись описанием максимальных подгрупп легко увидеть, что группа $Re(q)$ не содержит подгрупп такого порядка. Лемма доказана.

Далее, лемма 2 устанавливает не дополняемость мономиальных подгрупп в некоторых группах.

Лемма 2. В группах $Sz(q)$ ($q \neq 2$), $Re(q)$ ($q \neq 3$), $PSL_3(q)$ ($q \geq 5$), $PSU_3(q^2)$ мономиальная подгруппа N не дополняема.

Доказательство. Для групп $Sz(q)$ и $Re(q)$ справедливость утверждения вытекает из описания максимальных подгрупп в лемме 1. Мономиальные подгруппы в данных группах имеют порядок $2(q - 1)$ и, следовательно, дополнения к ним должны иметь порядки $q^2(q^2 + 1)/2$ и $q^3(q^3 + 1)/2$, соответственно. Однако подгрупп таких порядков группы $Sz(q)$ и $Re(q)$ не содержат.

Рассмотрим группы $PSL_3(q)$; их подгруппы $PSL_3(q)$ описаны (см. [12], [13], а так же [14]). Порядок мономиальной подгруппы N в $PSL_3(q)$ равен $6(q - 1)^2/d$, $d = (3, q - 1)$. Предположим, что существует дополнение K к N . Тогда $|K| = q^3(q + 1)(q^2 + q + 1)/6d$. Однако группа $PSL_3(q)$ не имеет подгрупп такого порядка. Действительно, подгруппа H группы $SL_3(q)$, $q = p^n$ (p - простое число), с точностью до сопряженности совпадает с одной из следующих подгрупп (см. [13]):

- а) подгруппа группы $M_i = \{ \|a_{kj}\| \in SL_3(q) : a_{ij} = 0 \text{ при } j \neq i \}$, $i = 1$;
- б) подгруппа группы $M_{i'}$, полученной транспонированием матриц из M_i , $i = 1$;
- в) подгруппа нормализатора $N(D)$ в $SL_3(q)$ подгруппы D всех диагональных матриц из $SL_3(q)$;
- г) $\langle SL_3(m), \|a, a, a^{-2}\| \rangle$, где $m^k = q$, число $|a^3|$ делит $m - 1$;
- д) $\langle SU_3(m^2), \|b, b, b^{-2}\| \rangle$, где $m^{2k} = q$, число $|b^3|$ делит $m + 1$;
- е) $p > 2$, $m^k = q$, $m > 3$: образ $G_{0m} \cong PSL_2(m)$ группы $SL_2(m)$ или образ $G_{1m} \cong PGL_2(m)$ группы $GL_2(m)$ при гомоморфизме группы $GL_2(q)$;
- ж) H имеет циклический нормальный делитель порядка, делящего $q^2 + q + 1$, индекс которого равен 1 или 3;
- з) $H \cong A_6(mod E)$, если $q = 2^{2k}$, либо $q \equiv 1$ или $19(mod 30)$;

и) $q = 5^{2k}$: $H' \supset E$ и H/E изоморфна A_6 , A_7 или группе, содержащей A_6 с индексом 2;

к) $p > 2$: $H \cong A_5$ при $q^2 - 1$ кратном 10 или $H \cong PSL_2(7)$ при $q^3 - 1$ кратном 7;

л) $p > 2$, $q \equiv 1 \pmod{3}$: H содержит, как нормальный делитель, группу T , порожденную матрицами $\|1, e, e^2\|$, $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, где $e \neq 1$ —

кубический корень из единицы в поле $GF(q)$.

Наконец рассмотрим группу $PSU_3(q^2)$. Ее порядок равен $q^3(q^2 - 1)(q^3 + 1)/d$, $d = (3, q - 1)$, а порядок мономиальной подгруппы равен $|N| = 2(q + 1)$. Пусть существует неединичное дополнение K к N . Соответственно порядок подгруппы K равен $q^3(q - 1)(q^3 + 1)/2d$. K содержит подгруппу Бореля группы $PSU_3(q^2)$, следовательно K удовлетворяет условию теоремы 3 из [14] из которой следует, что подгруппы с таким условием на порядок в $PSU_3(q^2)$ нет. Лемма доказана.

Теперь докажем теорему 1.

Доказательство теоремы 1. Как уже отмечалось, в работе Н. Ито [7] рассмотрены все факторизации групп $PSL_2(q)$ над конечными полями порядка q откуда легко следует, что среди групп $PSL_2(q)$, только группа $PSL_2(7)$ является слабо факторизуемой.

Справедливость теоремы 1 следует из леммы 1 и леммы 2, достаточно заметить, что в группах $Sz(q)$, $q = 2^{2k+1}$ и $Re(q)$, $q = 3^{2k+1}$ при $k \geq 1$ подгруппы Бореля являются максимальными, а для групп $PSL_3(q)$ и $PSU_3(q^2)$ при $q \geq 5$, максимальными являются мономиальные подгруппы. Теорема доказана.

§ 2. Далее рассмотрим некоторые спорадические группы

Теорема 2. Группы M_{11} , M_{12} , J_2 , J_3 не являются слабо факторизуемыми

Доказательство. Максимальные подгруппы большинства спорадических групп описаны в [17]. Группа M_{11} имеет порядок равный $7920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11$, она обладает максимальной подгруппой $GL_2(3)$ порядка $48 = 2^4 \cdot 3$. Пусть существует дополнение K к $GL_2(3)$ в M_{11} тогда ввиду максимальной $GL_2(3)$ порядок K равен $3 \cdot 5 \cdot 11$. Как видно из описания максимальных подгрупп группы M_{11} , такая подгруппа может содержаться только в $PSL_2(11)$ и должна содержать подгруппу Бореля группы $PSL_2(11)$ порядка $5 \cdot 11$, а это противоречит максимальной подгруппы Бореля в $PSL_2(11)$.

Аналогичные рассуждения применимы и для группы M_{12} . Порядок группы M_{12} равен $95040 = 2^6 \cdot 3^3 \cdot 5 \cdot 11$, в ней содержится в качестве максимальной подгруппы нормализатор нормальной четверной подгруппы из G_2 , имеющий порядок $2^6 \cdot 3$. Пусть существует дополнение K к данной подгруппе, тогда его порядок равен $3^2 \cdot 5 \cdot 11$. Как видно из [17] такую подгруппу может содержать в M_{12} только максимальная подгруппа M_{11} . Так же как и для M_{11} получаем, что подгрупп такого порядка в M_{12} нет.

В группах J_2 и J_3 максимальная подгруппа L — нормализатор нормальной четвертной подгруппы из силовской 2-подгруппы группы J_2 имеет порядок $2^7 \cdot 3^2$. Если существуют неединичные дополнения к L в J_2 и J_3 , то их порядки равны $3 \cdot 5^2 \cdot 7$ и $3^3 \cdot 5 \cdot 17 \cdot 19$ соответственно. Как следует из описания максимальных подгрупп J_2 и J_3 , подгрупп таких порядков в J_2 и J_3 нет. Теорема доказана.

ЛИТЕРАТУРА

1. Hall Ph. Complemented groups. // J. London Math. Soc. 1937. V. 12. P. 201-204.
2. Черников С.Н. Группы с системами дополняемых подгрупп // Матем. сб. 1954. Т. 35(77). №1. С. 93-128.
3. Баева Н.В. Вполне факторизуемые группы. // Докл. АН СССР. 1953. Т. 92. №5. С. 877-880.
4. Черникова Н.В. Группы с дополняемыми подгруппами // Матем. сб. 1956. Т. 39(81). №3. С. 273-292.
5. Коуровская тетрадь (Нерешенные вопросы теории групп). 14-е изд. Новосибирск: ИМ СО РАН. 1999.
6. Левчук В.М. О слабо факторизуемых группах. // Мат. заметки. 2003. Т. 73, №4. С. 565-572.
7. Ito N. On the factorizations of the linear fractional group $LF(2, p^n)$. // Acta Sci. Math. 1953. V. 15. №1. P. 79-84.
8. Стейнберг Р. Лекции о группах Шевалле. М.: Мир, 1975.
9. Carter R. Simple groups of Lie type. New York: Wiley and Sons, 1972.
10. Suzuki M. On a class of doubly transitive groups. // Ann. Math. 1962. V. 75. №1. P. 105-145.

11. Левчук В.М. Нужин Я.Н. О строении групп Ри. //Алгебра и логика. 1985. Т. 24. №1. С. 26-41.
12. Hartley R.W. Determination of the ternary collineation groups whose coefficients lie in the $GF(2^n)$. //Ann. Math. 1925. V. 27. P. 140-158.
13. Mitchell H.H. Determination of the ordinary and modular ternary linear group // Trans. Amer. Math. Soc. 1911. V. 19. №2. P. 207-242.
14. Bloom D. The subgroups of $PSL(3, q)$ for odd q . // Trans. Amer. Math. Soc. 1967. V. 127. №1. P. 150-176.
15. Левчук В.М. Об аппроксимируемости свободных групп группами $PSL(3, q)$ при нечетном q // Сб. Алгебра. Вложение групп. Алгоритмические вопросы. Красноярск: ИФ СО АН СССР. 1970 С. 71-93.
16. Нужин Я. Н. О строении групп лиева типа ранга 1 // Мат. заметки. 1984. Т. 36, №2. С. 149-158.
17. Сыскин С. А. Абстрактные свойства простых спорадических групп. // Успехи матем.наук. 1980. Т. 35. №5(215). С. 181-212.
18. Холл М. Теория групп. М.: ИЛ,1962.
19. Каргаполов М. И., Мерзляков Ю. И. Основы теории групп.4-е изд.. М.: Наука,1996.
20. Key J. D. Some maximal subgroups of $PSL(n, q)$, $n \geq 3$, $q = 2^r$. // Geom. de dic . 1975. V. 4. №2-4. P. 377-386; Erratum.-ibid. 1977. V.6, №3. P. 389.

ПАРАМЕТРЫ ВЛОЖЕНИЯ ИНВОЛЮЦИЙ ЗНАКОПЕРЕМЕННЫХ ГРУПП

Листова О.В.*

Институт вычислительного моделирования СО РАН,
Россия, 660036, Красноярск, Академгородок
e-mail: listova@ksc.krasn.ru

§ 1. По известной теореме Р. Брауэра *существует только конечное число конечных простых групп с данным централизатором инволюции*. К обобщению приводит введенное В. П. Шунковым понятие параметра вложения инволюции. Как обычно, централизатор элемента i в группе G обозначаем через $C_G(i)$, класс сопряженных элементов группы G с представителем i — через i^G .

Определение (В. П. Шунков [2]). *Параметром вложения инволюции i в группе G назовем число*

$$t(G, i) = \max_{g \in G} |gC_G(i) \cap i^G i^G|.$$

Параметр вложения $t(G, i)$ инволюции i бесконечной группы G очевидно может быть и бесконечным. В. П. Шунковым доказана

Теорема (В. П. Шунков [5]). *Существует только конечное число периодических простых групп с инволюцией, имеющей конечный параметр вложения, причем все такие группы конечны.*

Условие конечности параметра вложения инволюции i является более слабым, чем конечность централизатора $C_G(i)$, и поэтому теорема В. П. Шункова обобщает теорему Р. Брауэра. В связи с теоремой В. П. Шункова естественно возникает задача вычисления и оценки параметров вложения инволюций в простых конечных группах.

Сопряженные в группе инволюции имеют одинаковые параметры вложения, так что параметр вложения инволюции в группе требуется вычислять лишь для представителей из каждого класса сопряженных инволюций. В настоящей статье вычисляются явно параметры вложения класса сопряженных инволюций знакопеременных групп A_n с представителем $(1\ 2)(3\ 4)$. Доказана

*Работа выполнена при финансовой поддержке РФФИ (грант №02-01-00078)

Теорема 1. В знакопеременной группе A_n , $n \geq 4$, параметр вложения инволюции $(1\ 2)(3\ 4)$ равен числу

$$\frac{1}{384}n^8 - \frac{11}{96}n^7 + \frac{1283}{576}n^6 - \frac{5977}{240}n^5 + \frac{201667}{1152}n^4 - \frac{76087}{96}n^3 + \frac{650797}{288}n^2 - \frac{445849}{120}n + 2705.$$

Ранее задача вычисления и оценки параметров вложения инволюций исследовалась автором [1] с использованием системы компьютерной алгебры GAP для некоторых спорадических групп, а также для знакопеременных групп A_n , $n \leq 11$. См. также § 5.

§ 2. Нам потребуется описание классов сопряженных инволюций в A_n . В [3, глава 5] описаны классы сопряженных элементов симметрической группы подстановок S_n .

Лемма 1 [3]. *Если*

$$T = (a_{11} \dots a_{1r})(a_{21} \dots a_{2s}) \dots (a_{m1} \dots a_{mt})$$

и

$$S = \begin{pmatrix} a_{11} & \dots & a_{1r} & a_{21} & \dots & a_{2s} & \dots & a_{m1} & \dots & a_{mt} \\ b_{11} & \dots & b_{1r} & b_{21} & \dots & b_{2s} & \dots & b_{m1} & \dots & b_{mt} \end{pmatrix},$$

то

$$S^{-1}TS = (b_{11} \dots b_{1r})(b_{21} \dots b_{2s}) \dots (b_{m1} \dots b_{mt}).$$

Доказательство. Для произвольного элемента $b_{j, k}$ имеем

$$S^{-1}TS : b_{j, k} \longrightarrow a_{j, k} \longrightarrow a_{j, k+1} \longrightarrow b_{j, k+1},$$

т.е. подстановка $S^{-1}TS$ переводит элемент $b_{j, k}$ в элемент $b_{j, k+1}$. Лемма доказана.

Из леммы 1 почти непосредственно вытекает следующий критерий сопряженности в симметрической группе S_n (см. [3, теорема 5.1.3])

Следствие 1. *Две подстановки сопряжены в симметрической группе тогда и только тогда, когда они имеют одинаковое число циклов каждой длины.*

Классы сопряженных инволюций знакопеременных групп описывает

Лемма 2. *Знакопеременная группа A_n ($n \geq 4$) имеет, в точности, $\left[\frac{n}{4}\right]$ классов сопряженных инволюций, представителями которых можно выбрать следующие инволюции*

$$\tau_k = (1\ 2)(3\ 4)(5\ 6)(7\ 8) \dots (4k-3\ 4k-2)(4k-1\ 4k), \quad 1 \leq k \leq \left[\frac{n}{4}\right].$$

Доказательство. Подстановки τ_k не сопряжены в S_n , в силу следствия 1. Отсюда вытекает, что S_n и, тем более, A_n имеет не менее, чем $\lfloor \frac{n}{4} \rfloor$ классов сопряженных инволюций. Произвольная инволюция из A_n есть произведение четного числа $2k$ независимых циклов длины 2. Она имеет вид $(a_1 a_2)(a_3 a_4) \dots (a_{4k-1} a_{4k})$ и поэтому сопряжена подходящим элементом $S \in S_n$, как и в лемме 1, с элементом τ_k . Тот же результат получим, если в нижней строке подстановки S поменяем местами первые два элемента. Следовательно, S можно выбрать в A_n . Лемма доказана.

Из определения параметра $t(G, i)$ вытекают неравенства

$$t(G, i) \leq |C_G(i)|, \quad t(G, i) \leq |i^G i^G|,$$

определяющие верхние границы параметра вложения инволюции. Для инволюции $\sigma = (1\ 2)(3\ 4) (= \tau_1)$ получаем оценку $t(A_n, \sigma) \leq 4 \cdot (n-4)!$ как показывает

Лемма 3. Порядок централизатора подстановки $\sigma = (1\ 2)(3\ 4)$ в знакопеременной группе A_n , $n \geq 4$, равен

$$|C_{A_n}(\sigma)| = 4 \cdot (n-4)!$$

Доказательство. Если

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ j_1 & j_2 & j_3 & j_4 & \dots & j_n \end{pmatrix},$$

то $\pi^{-1}\sigma\pi = (j_1 j_2)(j_3 j_4)$, по лемме 1. При $\pi \in C_{A_n}(\sigma)$ получаем равенство множеств $\{j_5, \dots, j_n\} = \{5, \dots, n\}$, так что упорядоченный набор $j_5, \dots, j_n$ можно выбрать $(n-4)!$ различными способами. Кроме того,

$$\text{либо } \{j_1, j_2\} = \{1, 2\}, \quad \{j_3, j_4\} = \{3, 4\},$$

$$\text{либо } \{j_1, j_2\} = \{3, 4\}, \quad \{j_3, j_4\} = \{1, 2\}.$$

Поэтому для выбора символов j_1, j_2, j_3, j_4 в подстановке π из S_n имеется всего 8 возможностей; очевидно, лишь в половине этих случаев выполняется включение $\pi \in A_n$. Таким образом, централизатор $C_{A_n}(\sigma)$ состоит из $4 \cdot (n-4)!$ подстановок. Лемма доказана.

§ 3. Следующая лемма и ее доказательство описывают произведение $\sigma^{A_n} \sigma^{A_n}$.

Лемма 4. Для инволюции $\sigma = (1\ 2)(3\ 4)$ знакопеременной группы A_n , $n \geq 5$, имеем

$$\begin{aligned} |\sigma^{A_n} \sigma^{A_n}| &= \frac{1}{384}n^8 - \frac{1}{32}n^7 + \frac{83}{576}n^6 - \frac{77}{240}n^5 + \frac{547}{1152}n^4 - \frac{55}{96}n^3 + \frac{109}{288}n^2 - \frac{3}{40}n + 1 = \\ &= 4!C_n^5 + 3!C_n^2 C_{n-2}^4 + 2!C_n^3 + 2!C_n^3 C_{n-3}^3 + C_n^2 C_{n-2}^2 C_{n-4}^3 + \frac{1}{4!}C_n^2 C_{n-2}^2 C_{n-4}^2 C_{n-6}^2 + \end{aligned}$$

$$+\frac{1}{2!}C_n^2C_{n-2}^2+1.$$

Доказательство. Рассмотрим произведение подстановок

$$\sigma_1 = (i_1 i_2)(i_3 i_4) \in \sigma^{A_n}, \quad \sigma_2 = (j_1 j_2)(j_3 j_4) \in \sigma^{A_n}$$

в зависимости от пересечения множеств $I(\sigma_1) = \{i_1, i_2, i_3, i_4\}$ и $I(\sigma_2) = \{j_1, j_2, j_3, j_4\}$.

Допустим, что $I(\sigma_1) \cap I(\sigma_2) = \emptyset$. Тогда $\sigma_1\sigma_2$ очевидно равно произведению

$$(i_1 i_2)(i_3 i_4)(j_1 j_2)(j_3 j_4) = \pi_0$$

четырех независимых циклов длины 2. При этом первый цикл подстановки π_0 можно выбрать C_n^2 способами, второй цикл — C_{n-2}^2 способами, третий цикл — C_{n-4}^2 способами и четвертый — C_{n-6}^2 способами. Так как эти четыре цикла можно переставить $4!$ способами, то получаем $\frac{1}{4!}C_n^2C_{n-2}^2C_{n-4}^2C_{n-6}^2$ подстановок вида π_0 .

Если $I(\sigma_1) \cap I(\sigma_2) = \{k\}$, то с точностью до перестановки сомножителей в подстановках σ_1 и σ_2 , общий символ k находится во вторых их сомножителях, и даже является последним символом в них, с точностью до перестановки символов в циклах. В этом случае произведение $\sigma_1\sigma_2$ равно

$$(i_1 i_2)(i_3 k)(j_1 j_2)(j_3 k) = (i_1 i_2)(j_1 j_2)(i_3 j_3 k) = \pi_1$$

и количество подстановок вида π_1 равно $C_n^2C_{n-2}^2C_{n-4}^3$.

Пусть $I(\sigma_1) \cap I(\sigma_2) = \{k, m\}$. Тогда произведение $\sigma_1\sigma_2$ равно одной из подстановок

$$(i_1 i_2)(k m)(j_1 j_2)(k m) = (i_1 i_2)(j_1 j_2) = \pi_2,$$

$$(i_1 k)(i_3 m)(j_1 k)(j_3 m) = (i_1 j_1 k)(i_3 j_3 m) = \pi_{2'},$$

$$(i_1 i_2)(k m)(j_1 k)(j_3 m) = (i_1 i_2)(j_1 k j_3 m) = \pi_{2''}.$$

Число подстановок вида π_2 в $\sigma^{A_n}\sigma^{A_n}$ равно $\frac{1}{2!}C_n^2C_{n-2}^2$, вида $\pi_{2'}$ — $2!C_n^3C_{n-3}^3$, наконец, вида $\pi_{2''}$ — $3!C_n^2C_{n-2}^4$.

Рассмотрим случай, когда $I(\sigma_1) \cap I(\sigma_2) = \{k, m, q\}$. В этом случае произведение $\sigma_1\sigma_2$ имеет вид либо

$$(i_1 k)(m q)(j_1 k)(m q) = (i_1 j_1 k) = \pi_3,$$

либо

$$(i_1 k)(m q)(j_1 m)(k q) = (i_1 q j_1 m k) = \pi_{3'}.$$

Количество подстановок вида π_3 равно $2!C_n^3$, вида $\pi_{3'}$ — $4!C_n^5$.

В оставшемся случае, когда $I(\sigma_1) \cap I(\sigma_2) = \{k, m, q, r\}$, имеем либо

$$\sigma_1 \sigma_2 = (k \ m)(q \ r)(k \ q)(m \ r) = (k \ r)(m \ q) = \pi_2,$$

либо $\sigma_1 = \sigma_2$ и $\sigma_1 \sigma_2$ — тождественная подстановка.

Суммируя количество найденных подстановок, получаем искомую формулу для $|\sigma^{A_n} \sigma^{A_n}|$. Лемма доказана.

§ 4. Доказательство теоремы 1. Исследуем пересечение $C_{A_n}(\sigma) \cap \sigma^{A_n} \sigma^{A_n}$ и его мощность. Неединичные подстановки из произведения $\sigma^{A_n} \sigma^{A_n}$ представлены в доказательстве леммы 4 как подстановки вида π_i , $i = 0, 1, 2, 3, 2', 2'', 3'$. Перечислим подстановки π_i , лежащие в централизаторе $C_{A_n}(\sigma)$. Пусть k, l, m, q, o, p, r, s — попарно различные элементы множества $\{5, 6, \dots, n\}$. Тогда подстановки вида π_0 , лежащие в централизаторе, исчерпываются следующими:

$\frac{3}{2!} C_{n-4}^2 C_{n-6}^2$ подстановок вида

$$(1 \ 2)(3 \ 4)(k \ l)(m \ q), \quad (1 \ 3)(2 \ 4)(k \ l)(m \ q), \quad (1 \ 4)(2 \ 3)(k \ l)(m \ q);$$

$\frac{2}{3!} C_{n-4}^2 C_{n-6}^2 C_{n-8}^2$ подстановок $(1 \ 2)(k \ l)(m \ q)(o \ p), (3 \ 4)(k \ l)(m \ q)(o \ p);$

$\frac{1}{4!} C_{n-4}^2 C_{n-6}^2 C_{n-8}^2 C_{n-10}^2$ подстановок $(k \ l)(m \ q)(o \ p)(r \ s).$

Подстановкам вида π_1 соответствуют следующие подстановки централизатора:

$3 \cdot 2! C_{n-4}^3$ подстановок вида $(1 \ 2)(3 \ 4)(k \ l \ m), (1 \ 3)(2 \ 4)(k \ l \ m), (1 \ 4)(2 \ 3)(k \ l \ m);$

$2 \cdot 2! C_{n-4}^2 C_{n-6}^3$ подстановок $(1 \ 2)(k \ l)(m \ q \ o), (3 \ 4)(k \ l)(m \ q \ o);$

$C_{n-4}^2 C_{n-6}^2 C_{n-8}^3$ подстановок $(k \ l)(m \ q)(o \ p \ r).$

Подстановкам вида π_2 соответствуют следующие подстановки централизатора:

$2 C_{n-4}^2$ подстановок вида $(1 \ 2)(k \ l), (3 \ 4)(k \ l);$

$\frac{1}{2!} C_{n-4}^2 C_{n-6}^2$ подстановок $(k \ l)(m \ q);$

а также 3 подстановки $(1 \ 2)(3 \ 4), (1 \ 3)(2 \ 4), (1 \ 4)(2 \ 3).$

Подстановкам вида $\pi_{2'}$ соответствуют следующие подстановки централизатора:

$2! C_{n-4}^3 C_{n-7}^3$ подстановок вида $(k \ l \ m)(q \ o \ p).$

Подстановкам вида $\pi_{2''}$ соответствуют следующие подстановки централизатора:

$2 C_{n-4}^2$ подстановок вида $(1 \ 3 \ 2 \ 4)(k \ l), (1 \ 4 \ 2 \ 3)(k \ l);$

$2 \cdot 3! C_{n-4}^4$ подстановок $(1 \ 2)(k \ l \ m \ q), (3 \ 4)(k \ l \ m \ q);$

$3!C_{n-4}^2C_{n-6}^4$ подстановок $(kl)(mqor)$.

$2!C_{n-4}^3$ подстановок (klm) централизатора соответствуют подстановкам вида π_3 .

$4!C_{n-4}^5$ подстановок $(klmqo)$ централизатора соответствуют подстановкам вида $\pi_{3'}$.

Таким образом, количество подстановок, лежащих в пересечении $C_{A_n}(\sigma) \cap \sigma^{A_n}\sigma^{A_n}$, равно

$$\begin{aligned} & \frac{1}{4!}C_{n-4}^2C_{n-6}^2C_{n-8}^2C_{n-10}^2 + \frac{2}{3!}C_{n-4}^2C_{n-6}^2C_{n-8}^2 + 2 \cdot 2!C_{n-4}^2C_{n-6}^3 + 2C_{n-4}^2C_{n-6}^2 + 4 \cdot 2!C_{n-4}^3 + \\ & + C_{n-4}^2C_{n-6}^2C_{n-8}^3 + 2!C_{n-4}^3C_{n-7}^3 + 3!C_{n-4}^2C_{n-6}^4 + 2 \cdot 3!C_{n-4}^4 + 4!C_{n-4}^5 + 4C_{n-4}^2 + 4 = \\ & \frac{1}{384}n^8 - \frac{11}{96}n^7 + \frac{1283}{576}n^6 - \frac{5977}{240}n^5 + \frac{201667}{1152}n^4 - \frac{76087}{96}n^3 + \frac{650797}{288}n^2 - \frac{445849}{120}n + 2705. \end{aligned}$$

Далее исследуем мощность пересечения квадрата $\sigma^{A_n}\sigma^{A_n}$ с произвольным смежным классом H по централизатору $C_{A_n}(\sigma)$, $H \neq C_{A_n}(\sigma)$. Любой элемент $g \in H \cap (\sigma^{A_n}\sigma^{A_n})$ имеет вид π_j . Он содержит хотя-бы один цикл $\omega \notin C_{S_n}(\sigma)$ с символом из множества $\{1, 2, 3, 4\}$, причем длина цикла ω , как и у циклов π_i , не больше 5. Используя описание элементов пересечения $C_{A_n}(\sigma) \cap (\sigma^{A_n}\sigma^{A_n})$, сейчас нетрудно проверить, что

$$|H \cap (\sigma^{A_n}\sigma^{A_n})| \leq |C_{A_n}(\sigma) \cap (\sigma^{A_n}\sigma^{A_n})|.$$

Отсюда вытекает равенство $t(A_n, \sigma) = |C_{A_n}(\sigma) \cap (\sigma^{A_n}\sigma^{A_n})|$. Теорема доказана.

§ 5. Укажем два следствия теоремы 1.

Следствие 2. Параметр вложения инволюции $\sigma = (12)(34)$ локально конечной группы $G = \bigcup_{n=1}^{\infty} A_n$ бесконечен.

В связи с теоремой Р. Брауэра отметим, что число $|C_{A_n}(i)|$ растет вместе с n быстрее, чем параметр $t(A_n, i)$. Более точно, справедливо

Следствие 3. При $n \rightarrow \infty$ разность $|C_{A_n}(i)| - t(A_n, i)$ растет быстрее любой показательной функции.

Доказательство. Число $t(A_n, i)$ по теореме 1 является многочленом восьмой степени от n . Учитывая лемму 3, получаем требуемое утверждение. Следствие доказано.

Замечание. Некоторые элементарные свойства параметра вложения инволюции вытекают из работы [2]. Там же показано, что если числа t и m фиксированы, то среди групп G с инволюцией i , параметр вложения которой в G не превосходит t , строго i -вещественную подгруппу порядка $> m$ содержат те группы, для которых порядок $|i^G|$ достаточно велик. Подгруппа H группы G с инволюцией i называется строго i -вещественной, если каждый элемент из H инвертируется инволюцией i .

Список литературы

- [1] *Листова О.В.* Параметры вложения инволюций в некоторых простых конечных группах // Материалы Конференции молодых ученых Института вычислительного моделирования СО РАН. - Красноярск: ИВМ СО РАН. — 2002. — С. 21-23.
- [2] *Рябинина Н.А., Сучков Н.М., Шунков В.П.* Об особых подгруппах конечных групп с инволюциями // Алгебраические системы (сборник научных трудов). Красноярск: Препринт ВЦ СО РАН (1995), N 10, С.3-11.
- [3] *Холл М.* Теория групп. Под ред. Л.А. Калужнина. — М.: издательство иностранной литературы. — 1962.
- [4] *Шунков В.П.* Группы с конечно вложенной инволюцией // Алгебра и логика. — 1990. — Т. 29, N 1. — С. 102-123.
- [5] *Шунков В.П.* Группы с инволюциями // Международный семинар по теории групп, посвященный 70-летию А.И.Старостина и 80-летию Н.Ф.Сесекина, Екатеринбург, 17-21 декабря 2001г.: Тез.Докл. - Екатеринбург: Ин-т мат. и мех. УрО РАН, изд-во Урал.ун-та, 2001, с.245-246.

КОНСТРУКЦИЯ САМБИНА И НЕГАТИВНЫЕ ОПЕРАТОРЫ

С.И. Мардаев*

Институт математики СО РАН
Россия, 630090,
Новосибирск, пр. Коптюга 4
e-mail: mardaev@math.nsc.ru

В теории модальных логик имеется очень известная теорема о неподвижной точке, значение которой выходит за рамки неклассических логик. В этой теореме рассматриваются модализованные формулы (операторы) и логика Геделя-Леба GL , связанная с арифметической доказуемостью. Логика GL характеризуется классом всех строго частично упорядоченных шкал с обрывом возрастающих цепей. Для построения формулы, определяющей неподвижную точку в этой теореме, имеется элегантная конструкция Дж. Самбина. В статье указывается новое применение этой конструкции. Доказано, что конструкция дает формулу, определяющую неподвижную точку негативного оператора в классе транзитивных и антисимметричных моделей Крипке с условием обрыва возрастающих цепей. Этот класс шире, чем упомянутый класс всех строго частично упорядоченных шкал с обрывом возрастающих цепей.

Таким образом, конструкция Самбина построения определяющей формулы работает в следующих случаях:

- 1) в строго частично упорядоченных моделях с обрывом возрастающих цепей для модализованных операторов,
- 2) в транзитивных и антисимметричных моделях с условием обрыва возрастающих цепей для негативных операторов.

О негативных операторах имеется еще работа [4]. В ней указан класс формул такой, что если соответствующий оператор имеет неподвижную точку в транзитивной модели, то эта точка единственна и определима.

Модальные пропозициональные формулы состояются из пропозициональной константы $\perp$ (ложь) и пропозициональных переменных $p, q, r, \dots$ с помощью бинарных логических связок $\wedge, \vee$, унарных связок $\neg$ и $\Box$. Будем использовать стандартные обозначения $\top = \neg\perp$, $\Box\alpha = \alpha \wedge \Box\alpha$, $\Diamond\alpha = \neg\Box\neg\alpha$, $\alpha \rightarrow \beta = \neg\alpha \vee \beta$, $\alpha \leftrightarrow \beta = (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha)$. *Шкала Крипке* $\langle W, R \rangle$ состоит из непустого множества W и бинарного отношения R на W . *Модель*

*Работа выполнена при финансовой поддержке Российского Фонда Фундаментальных Исследований, проект №03-06-80178

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 . Это подмножество $v(q)$ называется *значением* переменной q . Считаем, что переменная истинна на элементах своего значения. Значение переменной q_i обозначим соответствующей прописной буквой Q_i . Функция v естественным образом продолжается на формулы: константе $\perp$ всегда соответствует пустое множество, связкам $\neg, \wedge, \vee, \Box$ соответствуют дополнение, пересечение, объединение множеств и следующая операция на множествах: $\Box A = \{x \mid \forall y (xRy \Rightarrow y \in A)\}$. Таким образом, значение формулы всегда является подмножеством множества W . Говорим, что формула *истинна* на элементе модели, если элемент принадлежит значению этой формулы. Значение формулы $\alpha(q_1, \dots, q_n)$ обозначим через $\alpha(Q_1, \dots, Q_n)$. Формула α *истинна* в модели $\langle W, R, v \rangle$, если α истинна на каждом элементе модели. Формула α *общезначима* на шкале $\langle W, R \rangle$ если α истинна в каждой модели $\langle W, R, v \rangle$, основанной на этой шкале. Обозначение $\alpha \sim \beta$ означает, что формулы α и β принимают одно и то же значение на некотором классе моделей, который в каждом конкретном случае будет ясен из контекста.

Вхождение переменной или константы в формулу называется

- 1) *модализованным*, если это вхождение находится под действием $\Box$,
- 2) *позитивным*, если это вхождение находится под действием четного числа отрицаний (это число может быть равно нулю),
- 3) *негативным*, если это вхождение находится под действием нечетного числа отрицаний.

Пусть дана формула $\varphi(p, q_1, \dots, q_n)$ от переменных $p, q_1, \dots, q_n$. Рассмотрим модель $\langle W, R, v \rangle$, в которой заданы значения $Q_1, \dots, Q_n$ переменных $q_1, \dots, q_n$, а значение переменной p не задано. Формула $\varphi(p, q_1, \dots, q_n)$ определяет на модели $\langle W, R, v \rangle$ оператор $F_\varphi(P) = \varphi(P, Q_1, \dots, Q_n)$, который каждому множеству P сопоставляет множество $\varphi(P, Q_1, \dots, Q_n)$. Т.е. переменной p придается значение P и рассматривается значение формулы φ при этом означивании. Операторы такого вида назовем *формульными*.

Если каждое вхождение переменной p в формулу $\varphi(p, q_1, \dots, q_n)$ модализованное, то назовем эту формулу *модализованной* по переменной p , а оператор F_φ назовем *модализованным*. Если каждое вхождение переменной p в формулу $\varphi(p, q_1, \dots, q_n)$ негативное, то назовем эту формулу *негативной* по p , а оператор F_φ назовем *негативным*.

Пусть дана шкала $\langle W, R \rangle$. Рассмотрим оператор F , не обязательно формульный, который каждому подмножеству A множества W сопоставляет некоторое подмножество $F(A)$ множества W . Множество P называется *неподвижной точкой* оператора F , если выполняется $P = F(P)$. Таким образом, неподвижная точка формульного оператора F_φ является решением уравнения $P = \varphi(P, Q_1, \dots, Q_n)$. Если неподвижная точка P совпадает в модели со значением некоторой формулы $\omega(q_1, \dots, q_n)$, то эта формула ω *определяет* неподвижную точку P в данной модели. Назовем эту формулу *определяющей*. Она дает яв-

ный вид решения.

Нормальная модальная логика **L** характеризуется классом S шкал Крипке, если **L** совпадает с множеством формул, общезначимых на всех шкалах из класса S .

Следующая теорема принадлежит К. Бернарди, Д. де Йонгу, К. Смориному и Дж. Самбину и широко известна [1, 11, 8]. Она говорит о логике $\mathbf{GL} = \mathbf{K4} \oplus \Box(\Box p \rightarrow p) \rightarrow \Box p$. Известно [10, 2, 7], что эта логика характеризуется классом всех строго частично упорядоченных шкал с обрывом возрастающих цепей (кроме того, она характеризуется классом всех конечных строго частично упорядоченных шкал). В терминах этой статьи ее можно сформулировать так:

Теорема 1 (о неподвижной точке) Для любого модализованного оператора F_φ его неподвижная точка в любой строго частично упорядоченной модели Крипке с обрывом возрастающих цепей существует и единственна и, кроме того, существует формула ω , определяющая эту точку во всех таких моделях.

Есть разные конструкции определяющей формулы, одна из конструкций принадлежит Дж. Самбину [9]. Она позволяет дать короткое доказательство этой теоремы [6].

Мы исследуем не модализованный случай, а негативный. Негативный случай в некотором смысле сводится к модализованному. Рассмотрим негативный оператор F_φ . В формуле φ заменим на $\perp$ все вхождения p , не находящиеся под действием $\Box$. Полученную формулу обозначим ζ . Оператор F_ζ — тоже негативный.

Предложение 1 В любой модели Крипке $\langle W, R, v \rangle$ любая неподвижная точка оператора F_φ является неподвижной точкой оператора F_ζ .

Доказательство Пусть P — неподвижная точка оператора F_φ . При замене значение формулы в модели может при этом измениться только внутри P . Так как p входит негативно, то значение может только увеличиться. Поэтому значение не изменится и P будет неподвижной точкой оператора F_ζ . Предложение доказано.

Обычной является ситуация, когда негативный оператор на одних моделях имеет неподвижные точки, а на других — не имеет. Более того, он может иметь более чем одну неподвижную точку (пример см. в [4]). Рассмотрим случай, когда неподвижная точка единственна.

Следующее понятие введено в [5]. Шкала $\langle W, R \rangle$ удовлетворяет *сильному условию обрыва возрастающих цепей*, если в ней не существует бесконечной последовательности элементов $x_1, x_2, \dots$ такой, что для всех i выполняется $x_i \neq x_{i+1}$ и $x_i R x_{i+1}$. В [5] доказано, что если в модели Крипке с сильным условием обрыва возрастающих цепей неподвижная точка негативного оператора существует, то неподвижная точка единственна. Но, как показывают примеры, даже в этом случае точка может быть не определимой. Для определимости нужно накладывать дополнительные условия. Естественным явля-

ется наложить условие транзитивности.

Если взять транзитивное замыкание отношения R , удовлетворяющего сильному условию обрыва возрастающих цепей, то полученная шкала также будет удовлетворять сильному условию обрыва возрастающих цепей. Если отношение R транзитивно, то сильное условие эквивалентно выполнению двух условий: антисимметричности и условию обрыва возрастающих цепей. Например, на частично упорядоченных и строго частично упорядоченных шкалах это условие эквивалентно условию обрыва возрастающих цепей. Можно сказать, что шкала с транзитивным отношением и сильным условием обрыва возрастающих цепей получается следующим образом: берется строго частично упорядоченная шкала с обрывом возрастающих цепей и некоторые элементы делаются рефлексивными. Т.е. этот класс шире класса строго частично упорядоченных шкал с обрывом возрастающих цепей.

Теорема 2 Для любого негативного оператора F_φ существует формула ω , определяющая неподвижную точку этого оператора во всех транзитивных моделях Крипке с сильным условием обрыва возрастающих цепей, в которых неподвижная точка существует.

Доказательство Как упоминалось выше, доказано, что в моделях Крипке с сильным условием обрыва возрастающих цепей неподвижная точка единственна (если существует). Теорема 1 из работы Л.Л.Максимовой [3] утверждает, что любая нормальная модальная логика $\mathbf{L}$, содержащая $\mathbf{K4}$, обладает свойством Бета. Можно воспользоваться этим свойством и доказать существование определяющей формулы (подробности см. в [5]). Однако, теорема 1 [3] доказывается в [3] без построения в явном виде определяющей формулы, поэтому представляет интерес в нашем случае привести алгоритм построения определяющей формулы. Это сделано в [5], однако приведенная там конструкция более сложна, чем конструкция Самбина.

Докажем, что конструкция Дж. Самбина дает определяющую формулу. Пусть в транзитивной модели $\langle W, R, v \rangle$ с сильным условием обрыва возрастающих цепей неподвижная точка P существует. Заменим в формуле φ на $\perp$ все вхождения p , не находящиеся под действием $\Box$. В силу предложения 1 определяющая формула для нового оператора будет определять неподвижную точку для исходного оператора. Наш оператор стал модализованным и негативным.

Представим φ в виде

$$\alpha(\Box\beta_1(p, q_1, \dots, q_n), \dots, \Box\beta_m(p, q_1, \dots, q_n), q_1, \dots, q_n).$$

Здесь модальная формула $\alpha(s_1, \dots, s_m, q_1, \dots, q_n)$ содержит переменные $q_1, \dots, q_n$ и новые переменные $s_1, \dots, s_m$, а формулы $\beta_i(p, q_1, \dots, q_n)$ содержат только $p, q_1, \dots, q_n$. Вместо $\beta_i(p, q_1, \dots, q_n)$ будем писать просто β_i . Будем считать, что все $\Box\beta_i$ содержат p (это единственное отличие от конструкции Дж. Самбина, там этого условия нет). Такое представление, вообще говоря, не единственно. Индукцией по m строим формулу

и доказываем, что она – определяющая.

Базис $m = 0$. Тогда φ не содержит p , поэтому неподвижная точка определена формулой $\varphi = \omega$.

Шаг индукции $m \rightarrow m + 1$. Пусть $\varphi = \alpha(\Box\beta_1, \dots, \Box\beta_{m+1}, q_1, \dots, q_n)$. Для каждого $1 \leq i \leq m + 1$ введем формулу

$$\varphi_i = \alpha(\Box\beta_1, \dots, \Box\beta_{i-1}, \top, \Box\beta_{i+1}, \dots, \Box\beta_{m+1}, q_1, \dots, q_n).$$

По индукционному предположению построены формулы $\omega_i(q_1, \dots, q_n)$, определяющие неподвижные точки операторов F_{φ_i} . Докажем, что формула

$$\omega = \alpha(\Box\beta_1(\omega_1, q_1, \dots, q_n), \dots, \Box\beta_{m+1}(\omega_{m+1}, q_1, \dots, q_n), q_1, \dots, q_n)$$

определяет неподвижную точку оператора F_φ .

Возьмем в качестве значения переменной p неподвижную точку P . Докажем, что для любого i формулы $\Box\beta_i$ и $\Box\beta_i(\omega_i, q_1, \dots, q_n)$ эквивалентны на данной модели. Отсюда получим, что ω определяет неподвижную точку, так как после замены в φ подформулы $\Box\beta_i$ на $\Box\beta_i(\omega_i, q_1, \dots, q_n)$ получим ω .

Пусть $x \not\models \Box\beta_i$. Среди всех y таких, что xRy и $y \not\models \beta_i$, выберем максимальный (такой существует в силу обрыва возрастающих цепей). На модели введем естественные отношения $\geq$ и $>$ и рассмотрим подмодель, основанную на $\{z \mid z \geq y\}$. Если y иррефлексивный, то в этой подмодели формула $\Box\beta_i$ эквивалентна $\top$, поэтому $P \cap \{z \mid z \geq y\}$ является неподвижной точкой оператора F_{φ_i} . Эта точка по индукционному предположению определяется формулой ω_i . Поэтому, замена p на ω_i не изменяет истинность формулы на элементах подмодели, в том числе и на y . Получаем $y \not\models \beta_i(\omega_i, q_1, \dots, q_n)$ и значит $x \not\models \Box\beta_i(\omega_i, q_1, \dots, q_n)$.

Пусть y рефлексивный. Заметим, что в подмодели, основанной на $\{z \mid z > y\}$, формула $\Box\beta_i$ эквивалентна $\top$, поэтому φ эквивалентна φ_i . Неподвижные точки операторов F_φ и F_{φ_i} совпадают и p эквивалентна ω_i .

1) Пусть $\Box\beta_i$ входит в φ позитивно. Заметим, что так как $\Box\beta_i$ содержит p , то $\Box\beta_i$ не может входить и позитивно, и негативно, иначе φ не была бы негативной по p .

Теперь рассмотрим элемент y и допустим, что $y \models p$. Тогда $y \models \varphi$. Так как $\Box\beta_i$ входит только позитивно, то замена $\Box\beta_i$ на $\top$ не уменьшает значение формулы φ , поэтому $y \models \varphi_i$. Получаем, что φ эквивалентна φ_i на всех элементах подмодели, основанной на $\{z \mid z \geq y\}$. Неподвижные точки операторов F_φ и F_{φ_i} совпадают и p эквивалентна ω_i . Получаем $y \models \omega_i$.

Итак, независимо от значения p на y имеем, что в подмодели, основанной на $\{z \mid z \geq y\}$, значение p содержится в значении ω_i . Так как p входит в $\Box\beta_i$ только негативно, то в этой подмодели значение $\beta_i(\omega_i, q_1, \dots, q_n)$ содержится в значении β_i . А так как $y \not\models \beta_i$, то $y \not\models \beta_i(\omega_i, q_1, \dots, q_n)$.

2) Пусть $\Box\beta_i$ входит в φ негативно. Допустим, что $y \not\models p$. Тогда $y \not\models \varphi$. Так как $\Box\beta_i$ входит только негативно, то замена $\Box\beta_i$ на $\top$ не увеличивает значение

формулы φ , поэтому $y \not\models \varphi_i$. Получаем, что φ эквивалентна φ_i на всех элементах подмодели, основанной на $\{z \mid z \geq y\}$. Неподвижные точки операторов F_φ и F_{φ_i} совпадают и p эквивалентна ω_i . Получаем $y \not\models \omega_i$.

Итак, независимо от значения p на y имеем, что в подмодели, основанной на $\{z \mid z \geq y\}$, значение ω_i содержится в значении p . Так как p входит в $\Box\beta_i$ только позитивно, то в этой подмодели значение $\beta_i(\omega_i, q_1, \dots, q_n)$ содержится в значении β_i . А так как $y \not\models \beta_i$, то $y \not\models \beta_i(\omega_i, q_1, \dots, q_n)$.

Итак, в обоих случаях $y \not\models \beta_i(\omega_i, q_1, \dots, q_n)$, поэтому $x \not\models \Box\beta_i(\omega_i, q_1, \dots, q_n)$.

Пусть $x \models \Box\beta_i$. В подмодели, основанной на $\{z \mid z \geq x\}$, формула $\Box\beta_i$ эквивалентна $\top$, поэтому φ эквивалентна φ_i . Неподвижные точки операторов F_φ и F_{φ_i} совпадают и p эквивалентна ω_i . Значит $x \models \Box\beta_i(\omega_i, q_1, \dots, q_n)$. Теорема доказана.

Пример Рассмотрим формулу $\varphi = (q \vee \Box(\neg p \vee \neg q)) \wedge (\neg q \vee \Box(\neg p \vee q))$. Пусть $\alpha(s_1, s_2, q) = (q \vee s_1) \wedge (\neg q \vee s_2)$, $\Box\beta_1 = \Box(\neg p \vee \neg q)$, $\Box\beta_2 = \Box(\neg p \vee q)$. Тогда $\varphi_1 = (q \vee \top) \wedge (\neg q \vee \Box(\neg p \vee q)) \sim \neg q \vee \Box(\neg p \vee q)$. Аналогично $\varphi_2 \sim q \vee \Box(\neg p \vee \neg q)$.

Отсюда $(\varphi_1)_1 = \neg q \vee \top \sim \top$. Тогда $\omega_1 \sim \neg q \vee \Box(\neg(\varphi_1)_1 \vee q) \sim \neg q \vee \Box q$. Аналогично $\omega_2 \sim q \vee \Box\neg q$. Тогда

$$\begin{aligned} \omega &= (q \vee \Box\beta_1(\omega_1, q)) \wedge (\neg q \vee \Box\beta_2(\omega_2, q)) \sim \\ &= (q \vee \Box(\neg(\neg q \vee \Box q) \vee \neg q)) \wedge (\neg q \vee \Box(\neg(q \vee \Box\neg q) \vee q)) \sim \\ &= (q \vee \Box(\neg\Box q \vee \neg q)) \wedge (\neg q \vee \Box(\neg\Box\neg q \vee q)) \sim (q \vee \Box(\Diamond\neg q \vee \neg q)) \wedge (\neg q \vee \Box(\Diamond q \vee q)). \end{aligned}$$

На рефлексивных моделях $\omega \sim (q \vee \Box\Diamond\neg q) \wedge (\neg q \vee \Box\Diamond q)$. Пример закончен.

Напомним обозначения формулы и логики

$$\begin{aligned} \mathbf{grz}_1 &: \Box(\Box(p \rightarrow \Box p) \rightarrow p) \rightarrow \Box p, \\ \mathbf{Grz}_1 &= \mathbf{K4} \oplus \mathbf{grz}_1. \end{aligned}$$

Формула $\mathbf{grz}_1$ упоминается в [10]. С помощью стандартной техники канонических моделей [10] нетрудно доказать

Предложение 2 Логика $\mathbf{Grz}_1$ характеризуется классом всех конечных транзитивных и антисимметричных шкал. Кроме того, эта логика характеризуется классом всех транзитивных шкал с сильным условием обрыва возрастающих цепей.

Собственно теоремой о неподвижной точке можно назвать следующее

Следствие Для любой негативной по p формулы $\varphi(p, q_1, \dots, q_n)$ существует формула $\omega(q_1, \dots, q_n)$ такая, что логика $\mathbf{Grz}_1$ содержит формулу

$$\Box(p \leftrightarrow \varphi) \rightarrow (p \leftrightarrow \omega).$$

Список литературы

- [1] C. Bernardi, *The fixed-point theorem for diagonalizable algebras*, *Studia Logica* **34** (1975), №3, 239–251.
- [2] A. Chagrov and M. Zakharyashev, *Modal Logic*, Oxford Logic Guides, vol. 35, Clarendon Press, 1997.
- [3] Л. Л. Максимова, *Аналог теоремы Бета в нормальных расширениях модальной логики K4*, *Сибирский математический журнал* **33** (1992), №6, 118–130.
- [4] S. I. Mardaev, *Fixed points of modal negative operators*, *Bulletin of the Section of Logic* **26** (1997), №3, 135–138.
- [5] С. И. Мардаев, *Негативные модальные схемы*, *Алгебра и логика* **37** (1998), №3, 329–337.
- [6] L. Reidhaar-Olson, *A new proof of the fixed-point theorem of provability logic*, *Notre Dame Journal of Formal Logic* **31** (1990), №1, 37–43.
- [7] V. V. Rybakov, *Admissibility of Logical Inference Rules*, *Studies in Logic and the Foundations of Mathematics*, vol. 136, Elsevier Science Publishers B.V., 1997.
- [8] G. Sambin, *An effective fixed-point theorem in intuitionistic diagonalizable algebras*, *Studia Logica* **35** (1976), №4, 345–361.
- [9] G. Sambin and S. Valentini, *The modal logic of provability: The sequential approach*, *Journal of Philosophical Logic* **11** (1982), №3, 311–342.
- [10] K. Segerberg, *An Essay in Classical Modal Logic*, *Filosofiska Studier*, № 13, Uppsala Universitet, Uppsala, 1971.
- [11] C. Smoryński, *Consistency and related metamathematical properties*, Univ. of Amsterdam, Mathematics Institute Technical Report 75-02, 1975.

IDEALS IN VECTOR LATTICE OF PIECEWISE POLYNOMIAL FUNCTIONS

N.Ya. Medvedev*

Altai State University,
Dimitrova 66,
656099 Barnaul, Russia.
e-mail: medvedev@math.dcn-asu.ru

1 Introduction and Background

Let $\mathbb{R}, \mathbb{Z}, \mathbb{N}$ denote the sets of real numbers, integer numbers and positive integer numbers, respectively. We will write $C(\mathbb{R}, \mathbb{R})$ for the additive group of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$ with the pointwise ordering: $f \leq g$ iff $f(x) \leq g(x)$ for all $x \in \mathbb{R}$.

A real vector space V which is also a lattice under some partial ordering is called a *vector lattice* if $u+(v \vee w) = (u+v) \vee (u+w)$ and $u+(v \wedge w) = (u+v) \wedge (u+w)$ for all $u, v, w \in V$ and $\lambda u \geq 0$ for any non-negative real number λ and any $v \in V, v \geq 0$ [1].

Let X be a partially ordered set and $Y \subseteq X$. Then Y is said to be *convex* (in X) if $x \in Y$ iff $y_1, y_2 \in Y$ with $y_1 \leq x \leq y_2$.

The convex sublattice subspaces of a real vector lattice are called *ideals*. An ideal P is called *prime* if for any ideals I, J equality $P = I \cap J$ implies that $P = I$ or $P = J$. Any I ideal is an intersection of prime ideals over I , and an ideal P of a vector lattice G is prime iff the quotient G/P is totally ordered for the induced ordering ($P + g \leq P + h$ iff $g \leq p + h$ for some $p \in P$). For further background, see [2], [4].

2 Main result

It is clear that the additive group of all continuous functions $C(\mathbb{R}, \mathbb{R})$ from $\mathbb{R}$ to $\mathbb{R}$ with the pointwise ordering is a vector lattice.

A function $f \in C(\mathbb{R}, \mathbb{R})$ is said to be a *continuous piecewise polynomial of bounded support* if there are $x_1 < \dots < x_m$ in $\mathbb{R}$ such that the restriction of f on

*This work was funded by a London Mathematical Society Scheme 5 Grant and a grant DAAD A/02/06270.

each interval $[x_j, x_{j+1}]$ is a polynomial function ($j = 1, \dots, m-1$), and $f(x) = 0$ if $x < x_1$ or $x > x_m$. Let $V = BP(\mathbb{R})$ denote this vector sublattice of $C(\mathbb{R}, \mathbb{R})$. As usual, by $f'_+(r)(f'_-(r))$ we denote the right (left) derivative of the function f in the point r . The symbol $f_+^{(n)}(r)(f_-^{(n)}(r))$ denotes the n -right (left) derivative of the function f in the point r .

For each $n \in \mathbb{N}$, let

$$V_{r,+}^{(n)} = \{f \in V : f(r) = f'_+(r) = \dots f_+^{(n)}(r) = 0\}$$

and

$$V_{r,-}^{(n)} = \{f \in V : f(r) = f'_-(r) = \dots f_-^{(n)}(r) = 0\}.$$

Clearly,

$$\bigcap_{n \in \mathbb{Z}_+} V_{r,+}^{(n)} = V_{r,+} \quad \text{and} \quad \bigcap_{n \in \mathbb{Z}_+} V_{r,-}^{(n)} = V_{r,-},$$

where

$$V_{r,+} = \{g \in V_r : (\exists \varepsilon = \varepsilon(g) > 0)(g = 0 \text{ on } [r, r + \varepsilon])\}$$

and

$$V_{r,-} = \{g \in V_r : (\exists \varepsilon = \varepsilon(g) > 0)(g = 0 \text{ on } [r - \varepsilon, r])\}.$$

Moreover,

$$V_r \supseteq V_{r,+}^{(1)} \supseteq V_{r,+}^{(2)} \supseteq \dots \supseteq V_{r,+} \quad \text{and} \quad V_r \supseteq V_{r,-}^{(1)} \supseteq V_{r,-}^{(2)} \supseteq \dots \supseteq V_{r,-}.$$

The direct verification shows the validity of the following statement.

Lemma 2.1. *Every ideal from the list*

$$V_r, V_{r,+}^{(1)}, V_{r,+}^{(2)}, \dots, V_{r,+}, V_{r,-}^{(1)}, V_{r,-}^{(2)}, \dots, V_{r,-}, V_{r,-}$$

is the prime ideal of the free vector lattice $V = BP(\mathbb{R})$.

Lemma 2.2. *Every proper ideal of $V = BP(\mathbb{R})$ is contained in some V_r . Hence, any prime ideal lies in the unique V_r .*

Proof: Let C be an ideal of V and $f \in V_+$. If, for all $r \in \mathbb{R}$, $C \not\subseteq V_r$, then for each r in the closure K of the support of f , there is $g_r \in C_+ \setminus V_r$. By replacing g_r by some suitable multiple (dependent on r) we may further assume that $g_r(r) > f(r)$, and hence obtain an open interval J_r containing r on which $g_r > f$. Since K is compact, there are $r_1, \dots, r_p$ such that $K \subseteq J_{r_1} \cup \dots \cup J_{r_p}$. Then $f \leq g = \bigvee_{j=1}^{j=p} g_{r_j} \in C$. Hence, $C = V$.

Now the prime ideals containing a given prime ideal form a chain for inclusion relation ([4], Theorem 2); this proves the lemma. //

Lemma 2.3. *Let P be a proper prime ideal of $V = BP(\mathbb{R})$ with $P \subseteq V_r$. Then either $P \subseteq V_{r,+}^{(1)}$ or $P \subseteq V_{r,-}^{(1)}$.*

Proof: Let P be a prime ideal of V and $P \not\subseteq V_{r,+}^{(1)}$ and $P \not\subseteq V_{r,-}^{(1)}$ but $P \subseteq V_r$. Let $0 < h_1 \in P \setminus V_{r,+}^{(1)}$ and $0 < h_2 \in P \setminus V_{r,-}^{(1)}$. Let g be any positive function from V_r and $M = \sup\{g(x) | x \in \mathbb{R}\}$. Since $0 < h_1 \in P \subseteq V_r$ and $h_1 \notin V_{r,+}^{(1)}$ there must be $\varepsilon_1 > 0$ such that on the interval $[r, r + \varepsilon_1]$ the following equality holds:

$$h_1(x) = c_1(x - r) + c_2(x - r)^2 + \cdots + c_n(x - r)^n$$

where $c_1 > 0$ and $N \cdot h_1 \geq g(x)$ for every $x \in [r, r + \varepsilon_1]$ and for some positive integer N . Similarly there is a positive real number $\varepsilon_2 > 0$ such that $N \cdot h_2 \geq g(x)$ on the interval $[r - \varepsilon_2, r]$. Now let K_0 be a closure of the set $\text{supp}(g) \setminus (r - \varepsilon_2, r + \varepsilon_1)$. The set K_0 is compact and $r \notin K_0$. Since P is prime, from Lemma 6.2 it follows that if $s \in K_0$, then $P \not\subseteq V_s$. As in the proof of Lemma 6.2 we can find $f \in P$ with $f > 0$ and $f(x) \geq g(x)$ for all $x \in K_0$. Then $0 \leq g \leq f \vee N(h_1 \vee h_2)$ with $f \vee N(h_1 \vee h_2) \in P$. So $g \in P$ and $V_r = P$, the desired contradiction. //

Lemma 2.4. *The set $S(V) = \{V_r, V_{r,+}^{(n)}, V_{r,-}^{(n)}, V_{r,+}, V_{r,-} : r \in \mathbb{R}, n \in \mathbb{Z}_+\}$ is the set of all prime ideals of $V = BP(\mathbb{R})$. Moreover, the list has no repetitions.*

Proof: We need only to prove that any prime ideal $P \subseteq V_r$ of V is from the above.

Firstly, suppose that $P \subset V_{r,+}$. Then there is $g \in V_{r,+} \setminus P$ with $g > 0$. So there is $\varepsilon > 0$ such that $g(x) = 0$ for all $x \in [r, r + \varepsilon]$. Let $f \in V$ be defined so that it has support $(r, r + \varepsilon)$, is $x - r$ on $[r, r + \varepsilon/2]$ and is $r + \varepsilon - x$ on $[r + \varepsilon/2, r + \varepsilon]$. Then $f \in P \subset V_{r,+}$ since $g \perp f$ and $g \notin P$, a contradiction. Therefore, $V_{r,+}, V_{r,-}$ are minimal prime ideals of V .

Secondly, suppose now that P is a prime ideal with $P \subseteq V_{r,+}^{(1)}$ but $P \not\subseteq V_{r,+}^{(2)}$. Let $0 < h_1 \in P \setminus V_{r,+}^{(2)}$ and $0 < h_2 \in P \setminus V_{r,-}^{(1)}$ (an element h_2 does exist since the prime ideals $V_{r,+}^{(1)}$ and $V_{r,-}^{(1)}$ are incomparable). Now arguments similar to the proof of Lemma 2.3 show that for any $g \in V_{r,+}^{(1)}, g > 0$ there are $\varepsilon_1, \varepsilon_2, N$ such that $N \cdot h_1(x) \geq g(x)$ on the interval $[r, r + \varepsilon_1]$ and $N \cdot h_2(x) \geq g(x)$ on the interval $[r - \varepsilon_2, r]$. Now let K_0 be a closure of the set $\text{supp}(g) \setminus (r - \varepsilon_2, r + \varepsilon_1)$. The set K_0 is compact and $r \notin K_0$ and arguments identical to the used in the proof of Lemma 2.3 imply $P = V_{r,+}^{(1)}$. The same arguments show that if P is a prime ideal with $P \subseteq V_{r,+}^{(n)}$ but $P \not\subseteq V_{r,+}^{(n+1)}$ then $P = V_{r,+}^{(n)}$. From this it follows that if $P \neq V_{r,+}^{(n)}$ for all $n \in \mathbb{N}$ then $P \subseteq V_{r,+}$. Clearly, all statements are valid if we replace all occurrences of $r+$ by $r-$. //

Let $S, S(+, 1), S(-, 1), \dots, S(+, n), S(-, n), \dots, S(+, \infty), S(-, \infty)$ be subsets of real numbers such that:

- 1) S is a closed subset of $\mathbb{R}$.
- 2) $S \supseteq S(+, 1) \supseteq \dots \supseteq S(+, n) \supseteq \dots S(+, \infty)$
and $S \supseteq S(-, 1) \supseteq \dots \supseteq S(-, n) \supseteq \dots S(-, \infty)$.
- 3) for each sequence $\{s_n \mid n \in \mathbb{N}\}$ in S with $\lim s_n = s$ we have that if the sequence $\{s_n \mid n \in \mathbb{N}\}$ is strictly decreasing, then $s \in S(-, \infty)$, whereas if $\{s_n \mid n \in \mathbb{N}\}$ is strictly increasing, then $s \in S(+, \infty)$.
- 4) $s \in S(+, n)$ for all $n \in \mathbb{N}$ if and only if $s \in S(+, \infty)$ and $s \in S(-, n)$ for all $n \in \mathbb{N}$ if and only if $s \in S(-, \infty)$.

Let us denote the set of all infinite tuples

$$(S, S(+, 1), S(-, 1), \dots, S(+, \infty), S(-, \infty))$$

with properties 1) – 4) by $\mathfrak{S}$. Let us order $\mathfrak{S}$ by setting

$$(S, S(+, 1), S(-, 1), \dots, S(+, \infty), S(-, \infty)) \leq \\ \leq (T, T(+, 1), T(-, 1), \dots, T(+, \infty), T(-, \infty))$$

if $S \supseteq T$, $S(+, 1) \supseteq T(+, 1)$, $S(-, 1) \supseteq T(-, 1)$, $\dots$, $S(+, \infty) \supseteq T(+, \infty)$, $S(-, \infty) \supseteq T(-, \infty)$. It is clear that this order is a lattice order on $\mathfrak{S}$.

Theorem A. *There is a lattice isomorphism between $\mathfrak{S}$ and the lattice of all ideals of $BP(\mathbb{R})$.*

Proof: Let C be any ideal of $V = BP(\mathbb{R})$.

Let $S(C) = \{r \in \mathbb{R} : C \subseteq V_r\}$,

$$S(C, +, n) = \{r \in \mathbb{R} : C \subseteq V_{r,+}^{(n)}\}, \quad S(C, -, n) = \{r \in \mathbb{R} : C \subseteq V_{r,-}^{(n)}\},$$

$$S(C, +) = \{r \in \mathbb{R} : C \subseteq V_{r,+}\}, \quad \text{and} \quad S(C, -) = \{r \in \mathbb{R} : C \subseteq V_{r,-}\}.$$

Obviously, this gives an element of $\mathfrak{S}$ which we denote by $\Psi(C)$. Since $C = D$ iff C and D are contained in the same prime ideals, Ψ is injective. Further, for any prime ideal P and ideals C, D , we have $C \cap D \subseteq P$ iff $C \subseteq P$ or $D \subseteq P$. Hence, $\Psi(C) \vee \Psi(D) = \Psi(C \cap D)$. Therefore, Ψ is a lattice embedding.

So it remains to prove that Ψ is surjective.

Let $\bar{S} = (S, S(+, 1), \dots, S(-, \infty)) \in \mathfrak{S}$ and let $C =$

$$\bigcap_{r \in S} V_r \quad \bigcap_{n \in \mathbb{N}, r \in S(+, n)} V_{r,+}^{(n)} \quad \bigcap_{n \in \mathbb{N}, r \in S(-, n)} V_{r,-}^{(n)} \quad \bigcap_{r \in S(+, \infty)} V_{r,+} \quad \bigcap_{r \in S(-, \infty)} V_{r,-}.$$

Then C is an ideal of V and $\Psi(C) \leq \bar{S}$. We claim that $S = S(C)$, $S(+, n) = S(C, +, n)$,

$S(-, n) = S(C, -, n)$ for every $n \in \mathbb{N}$ and $S(+, \infty) = S(C, +, \infty)$, $S(-, \infty) = S(C, -, \infty)$. Assume that $S \neq S(C)$. Then there is $r \in S(C) \setminus S$. Since the set S is closed, there exists a positive real number $\varepsilon > 0$ such that the interval $[r - 2\varepsilon, r + 2\varepsilon]$ does not contain points from S . Now define $f \in V$ to have support $(r - \varepsilon, r + \varepsilon)$,

and be linear on each of $[r - \varepsilon, r]$ and $[r, r + \varepsilon]$ with $f(r) > 0$. Since $(r - \varepsilon, r + \varepsilon)$ is disjoint from S , we get $C \not\subseteq V_r$, a contradiction. Thus, $S(C) = S$. Suppose now that $S(+, 1) \neq S(C, +, 1)$. Then there is $s \in S(C, +, 1) \setminus S(+, 1)$. By property 4) there is a positive real number $\varepsilon > 0$ such that the interval $[r, r + 2\varepsilon]$ does not contain any point from S except r . Again define $f \in V$ to have a support in $[r, r + \varepsilon]$ and to be linear on $[r, r + \frac{\varepsilon}{2}]$ and $[r + \frac{\varepsilon}{2}, r + \varepsilon]$ with $f(r + \frac{\varepsilon}{2}) > 0$. By definition, $f \in C$ but $f \notin V_{r,+}^{(1)}$, a contradiction.

Using similar tricks (using polynomials $(x - r)^n$ on $(r, r + \varepsilon/2)$ or $(r - \varepsilon/2, r)$, etc.), we deduce that $\bar{S} = \Psi(C)$. This completes the proof. //

For each $m \in \mathbb{N}$, let $BP_m(\mathbb{R})$ denote the vector lattice of all piecewise polynomial functions from $\mathbb{R}$ to $\mathbb{R}$ of bounded support with each polynomial piece having degree at most m .

We truncate the sets in $\mathfrak{S}$ by only considering the sets $S, S(\pm, j), S(\pm\infty)$ with $j \leq m$. Let the result be denoted by $\mathfrak{S}_m$. Then the above proof shows

Corollary 2.5. $\mathfrak{S}_m$ is isomorphic to the lattice of ideals of $BP_m(\mathbb{R})$.

Corollary 2.6. [3] $\mathfrak{S}_1$ is isomorphic to the lattice of ideals of $BP_1(\mathbb{R})$ of piecewise linear functions of bounded support of the real line $\mathbb{R}$.

The above conclusions are valid if we merely regard $BP(\mathbb{R}), BP_m(\mathbb{R})$ as Abelian ℓ -groups.

It is well-known that vector lattices $BP(\mathbb{R}), BP_m(\mathbb{R})$ ($m \in \mathbb{N}$) are rings under usual operation of multiplication of functions. Direct verification shows that every ideal C of vector lattices $BP(\mathbb{R}), BP_m(\mathbb{R})$ is an ideal of ring $BP(\mathbb{R}), BP_m(\mathbb{R})$, respectively.

Corollary 2.7. 1) $\mathfrak{S}$ is isomorphic to the lattice of ideals of the ring of continuous piecewise polynomial functions $BP(\mathbb{R})$. $\mathfrak{S}_m$ is isomorphic to the lattice of ideals of the ring $BP_m(\mathbb{R})$ of continuous piecewise polynomial functions.

References

- [1] G. Birkhoff, *Lattice theory*, Third Edition, Amer. Math. Soc. Coll. Publ., 25, 1984.
- [2] A. M. W. Glass, *Partially ordered groups*, World Sci. Pub. Co., Singapore, 1999.
- [3] D. Kenoyer, *Recognizability in the lattice of convex subgroups of a lattice-ordered group*, Czech. Math. J., **34** (1984), 411–416.
- [4] V.M. Kopytov, N.Ya. Medvedev, *The theory of lattice-ordered groups*, Kluwer Academic Publ., Dordrecht-Boston-London, 1994.

ПОРОЖДЕННОСТЬ КОНЕЧНЫХ АЛГЕБР, БАЗИРУЕМОСТЬ ИХ УСЛОВНО ЭКВАЦИОНАЛЬНЫХ ТЕОРИЙ И ШКАЛА ПОТЕНЦИАЛОВ ВЫЧИСЛИМОСТИ n -ЭЛЕМЕНТНЫХ АЛГЕБР

А.Г. Пинус*

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

Стандартными вопросами при изучении универсальных алгебр и их многообразий являются вопросы о порождающих алгебр и о базирруемости их эквациональных теорий. Естественным является рассмотрение подобных вопросов в контексте изучения потенциалов вычислимости конечных алгебр и условно эквациональных теорий этих алгебр. Все определения и основные результаты, связанные с условными термами, условными тождествами, потенциалами вычислимости универсальных алгебр и шкалами этих потенциалов n -элементных алгебр можно найти в работах [1] — [2]. Всюду, далее, все n -элементные универсальные алгебры будем считать заданными на основном множестве $n = \{0, 1, \dots, n-1\}$.

Прежде всего заметим, что вопрос о порождающих алгебры $\mathcal{A} = \langle n; \sigma \rangle$ целиком зависит лишь от совокупности $Sub \mathcal{A}$. Кроме того, вопрос о том, является ли данная совокупность $\{i_1, \dots, i_k\} \subseteq n$ элементов алгебры $\mathcal{A}$ порождающими этой алгебры, зависит от совокупности ее термальных функций $T(\mathcal{A})$ не глобально, а локально, т. е. сводится к следующему: для $r \in n$ существует ли термальная функция $t(x_1, \dots, x_k) \in T(\mathcal{A})$ такая, что $t(i_1, \dots, i_k) = r$. Таким образом, этот вопрос может ставиться не относительно совокупности $T(\mathcal{A})$, а относительно совокупности $CT(\mathcal{A})$ условно термальных функций этой алгебры. Тем самым, если на совокупности n -элементных ввести в рассмотрение функцию, задающую минимальное число порождающих соответствующей

*Работа выполнена при финансовой поддержке РФФИ (грант №02-01-00258)

алгебры, то эта функция зависит от потенциала вычислимости соответствующей алгебры, а не от нее самой. И при этом, если для алгебр $\mathcal{A}_1 = \langle n; \sigma_1 \rangle$ и $\mathcal{A}_2 = \langle n; \sigma_2 \rangle$ имеет место включение $CT(\mathcal{A}_1) \subseteq CT(\mathcal{A}_2)$ (т. е. для потенциалов вычислимости $\overline{\mathcal{A}}_1, \overline{\mathcal{A}}_2$ алгебр $\mathcal{A}_1, \mathcal{A}_2$ имеет место неравенство $\overline{\mathcal{A}}_1 \leq \overline{\mathcal{A}}_2$ в шкале $\langle CT_n; \leq \rangle$ потенциалов вычислимости n -элементных алгебр), то минимальное число порождающих алгебры $\mathcal{A}_2$ не меньше такового же числа для алгебры $\mathcal{A}_1$.

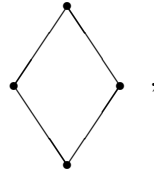
Итак, если опеределить на совокупности CT_n функцию $G_n(x)$ следующим образом: для $\overline{\mathcal{A}} \in CT_n$ положим $G_n(\overline{\mathcal{A}})$ равным минимальному числу порождающих алгебры $\mathcal{A}$, то, в силу отмеченного выше, имеет место следующее

УТВЕРЖДЕНИЕ 1. Функция G_n является антимонотонным отображением шкалы $\langle CT_n; \leq \rangle$ на интервал $[1, n]$.

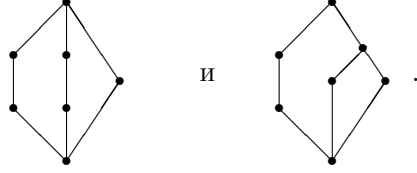
Представляет интерес более детальное изучение строения функции G_n и, в частности, следующая

ПРОБЛЕМА. Для любого натурального n найти точное значение, либо достаточно хорошие оценки, числа $|G_n^{-1}(k)|$ потенциалов вычислимости k -порожденных n -элементных алгебр при $1 \leq k \leq n$.

Выше уже замечалось, что значение функции $G_n(\overline{\mathcal{A}})$ целиком зависит от совокупности $Sub \mathcal{A}$. Столь же очевидным образом $G_n(\overline{\mathcal{A}})$ не определяется абстрактной решеткой $Sub \mathcal{A}$: пусть алгебры $\mathcal{A}_1 = \langle \{0, 1, 2\}; \sigma_1 \rangle$ и $\mathcal{A}_2 = \langle \{0, 1, 2\}; \sigma_2 \rangle$ таковы, что $Sub \mathcal{A}_1 = \{\emptyset, \{0\}, \{1\}, \{0, 1, 2\}\}$ и $Sub \mathcal{A}_2 = \{\emptyset, \{0\}, \{1, 2\}, \{0, 1, 2\}\}$. Тогда решетки $Sub \mathcal{A}_1$ и $Sub \mathcal{A}_2$ изоморфны решетке



но, в то же время, $G_3(\overline{\mathcal{A}}_1) = 1$ и $G_3(\overline{\mathcal{A}}_2) = 2$. В связи с этим, наряду с решеткой $Sub \mathcal{A}$, введем в рассмотрение следующую решетку $Sub' \mathcal{A}$, получаемую из решетки $Sub \mathcal{A}$ добавлением в качестве ее атомов новых элементов $0, 1, \dots, n-1$ таких, что $\emptyset < i$ и для любой подалгебры $B \subseteq n$ алгебры $\mathcal{A}$ неравенство $i < B$ равносильно включению $i \in B$. Таким образом, в частности, для любой одноэлементной подалгебры $\{i\}$ алгебры $\mathcal{A}$ справедливы неравенства $\emptyset < i < \{i\}$. Для указанных выше алгебр $\mathcal{A}_1$ и $\mathcal{A}_2$ их решетки $Sub' \mathcal{A}_1$ и $Sub' \mathcal{A}_2$ изоморфны, соответственно, решеткам



Очевидно, что значение функции $G_n(\overline{\mathcal{A}})$ определено абстрактной решеткой $Sub'\mathcal{A}$. А именно, имеет место

УТВЕРЖДЕНИЕ 2. $G_n(\overline{\mathcal{A}}) = 1$ тогда и только тогда, когда единица решетки $Sub'\mathcal{A}$ (множество n) является верхним покрытием некоторого ее атома и, в противном случае, $G_n(\mathcal{A}) = k$ ($2 \leq k \leq n$), где k -минимальное число атомов решетки $Sub'\mathcal{A}$ супремумом которых является ее единица.

Обратимся теперь к вопросу базлируемости условно эквациональных теорий n -элементных алгебр и связи этого вопроса со строением шкалы $\langle CT_n; \leq \rangle$.

Обозначим условно эквациональную теорию алгебры $\mathcal{A}$ (т. е. совокупность условных тождеств истинных на $\mathcal{A}$) как $CEq(\mathcal{A})$. В работе [3] (см., так же [1] — [2]) построено исчисление условных тождеств и доказана теорема полноты этого исчисления: для любой совокупности условных тождеств T и любого условного тождества $t_1 = t_2$ отношения $T \models t_1 = t_2$ и $T \vdash t_1 = t_2$ равносильны. Здесь $T \models t_1 = t_2$ означает, что для любой алгебры $\mathcal{A}$ на которой истинны условные тождества из T истинно и условное тождество $t_1 = t_2$, а $T \vdash t_1 = t_2$ — существование вывода условного тождества $t_1 = t_2$ из совокупности T в исчислении условных тождеств. По аналогии с эквациональными теориями $CEq(\mathcal{A})$ назовем однобазлируемой, если существует условное тождество $t_1 = t_2$, входящее в $CEq(\mathcal{A})$ такое, что для любого условного тождества $t' = t''$ из $CEq(\mathcal{A})$ имеет место $\{t_1 = t_2\} \vdash t' = t''$.

Покажем, что имеет место следующее

УТВЕРЖДЕНИЕ 3. Для любой конечной алгебры $\mathcal{A}$ ее условно эквациональная теория $CEq(\mathcal{A})$ однобазлируема.

Доказательство. Для любой конечной алгебры $\mathcal{A} = \langle n; \sigma \rangle$ через $\mathcal{A}^d$ обозначим ее обращение путем добавления в ее сигнатуру трехместной функции $d(x, y, z)$, интерпретируемой на $\mathcal{A}^d$ как дискриминатор. Таким образом, на $\mathcal{A}^d$ истинно условное тождество

$$\begin{cases} x \neq y \rightarrow x \\ x = y \rightarrow z \end{cases} = d(x, y, z).$$

Через $Eq(\mathcal{B})$ обозначим эквационную теорию алгебры $\mathcal{B}$. В силу известного результата Р.Падманабхана и Р.В. Квакенбуша [4] эквациональная теория $Eq(\mathcal{A}^d)$ однобазлируема. Пусть тождество $t_1 = t_2$ является базисом теории $Eq(\mathcal{A}^d)$ и $\mathcal{M}(\mathcal{A}^d)$ — многообразие алгебр порожденное алгеброй $\mathcal{A}^d$. По лемме

Йонссона [5] о подпрямо неразложимых алгебрах конгруэнц-дистрибутивных многообразий, подпрямо неразложимые (или, что то же самое в данном случае, дискриминаторные) алгебры многообразия $\mathcal{M}(\mathcal{A}^d)$ суть алгебры изоморфные алгебре $\mathcal{A}^d$ и ее подалгебрам. Заменяем каждое вхождение терма $d(t', t'', t''')$ в тождество $t_1 = t_2$ на условный терм

$$\begin{cases} t' \neq t'' \rightarrow t' \\ t' = t'' \rightarrow t''' \end{cases}.$$

Полученное условное тождество обозначим как $t'_1 = t'_2$. В силу отмеченного выше, любая алгебра $\mathcal{B}$ на которой истинно это условное тождество будет изоморфна некоторой подалгебре алгебры $\mathcal{A}$ (напомним, что для любых алгебр $\mathcal{B}_1$ и $\mathcal{B}_2$ изоморфизм алгебр $\mathcal{B}_1^d$ и $\mathcal{B}_2^d$ равносильен изоморфизму алгебр $\mathcal{B}_1$ и $\mathcal{B}_2$). Тем самым, действительно, базисом условно эквациональной теории $Seq(\mathcal{A})$ является условное тождество $t'_1 = t'_2$ и справедливость утверждения 3 доказана.

Условное тождество $t_1 = t_2$ сигнатуры σ будем рассматривать как слабое условное тождество верное на алгебре $\mathcal{A}$, если при некоторой подстановке условных термов алгебры $\mathcal{A}$ вместо функциональных символов сигнатуры σ в тождество $t_1 = t_2$ соответствующее тождество истинно на алгебре $\mathcal{A}$.

Обозначим условное тождество $t'_1 = t'_2$ из доказательства утверждения 3 как $t'_{\mathcal{A}} = t''_{\mathcal{A}}$. В силу доказательства утверждения 3 и равносильности для любых n -элементных алгебр $\mathcal{A}, \mathcal{B}$ условий:

- 1) $\overline{\mathcal{A}} \leq \overline{\mathcal{B}}$,
- 2) для некоторой перестановки π множества n имеет место $CT(\mathcal{A}) \subseteq CT(\pi(\mathcal{B}))$

УТВЕРЖДЕНИЕ 4. Для любого натурального n , для любых n -элементных алгебр $\mathcal{A}, \mathcal{B}$ следующие условия равносильны:

- 1) $\overline{\mathcal{A}} \leq \overline{\mathcal{B}}$ в шкале $\langle CT_n \leq \rangle$,
- 2) на алгебре $\mathcal{B}$ истинно слабое условное тождество $t'_{\mathcal{A}} = t''_{\mathcal{A}}$.
- 3) любое слабо условное тождество истинное на алгебре $\mathcal{A}$ будет слабо условным тождеством истинным на алгебре $\mathcal{B}$.

Список литературы

- [1] А.Г. Пинус. Условные термы и их применение в алгебре и теории вычислений // Успехи матем. наук, т. 56, №4, 2001, с. 35 — 72.
- [2] А.Г. Пинус. Условные термы и их применение в алгебре и теории вычислений // Из-во НГТУ, Новосибирск, 2002, 238 с.
- [3] А.Г. Пинус. Исчисление условных тождеств и условно рациональная эквивалентность // Алгебра и логика, т. 37, №4, 1998, с. 432 — 459.

- [4] R. Padmanabhan, P.W. Quackenbush. Equational theories of agebras with distributive congruences // Proc.Amer. Math. Soc. — v. 41, №2, 1973, p. 373 — 377.
- [5] B. Jonsson. Algebras whose congruence lattices are distributive // Math. Scand. — v.21, №1, 1967,p.110 — 121.

ОБ УТВЕРЖДЕНИЯХ ТИПА ТЕОРЕМЫ ЛОВАША

А.Г. Пинус*

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

В 60-е годы среди известных проблем универсальной алгебры была и следующая проблема Тарского: обязаны ли быть изоморфными конечные универсальные алгебры, декартовы квадраты которых изоморфны. Положительный ответ был дан Л. Ловашем в работе [1]. Известно также, что ограничение на конечность алгебр является существенным (см., к примеру, результат Дж. Кетонена [2] о вложимости произвольной счетной коммутативной полугруппы в декартов счетный скелет многообразия булевых алгебр). Помимо отношений изоморфности, важную роль в универсальной алгебре играет отношение рациональной (термальной) эквивалентности. В работах автора (обзор результатов см. [3]) в качестве отношения, соответствующего совпадению программно вычислительных возможностей алгебр введено отношение условной рациональной эквивалентности. В работах [4] — [6], как естественное обобщение последнего, определены отношения позитивно условной, $\exists^+$ -условной и элементарно условной рациональной эквивалентности алгебр и их классов. Цель настоящей работы — рассмотрение вопроса о возможности переноса утверждения теоремы Ловаша на перечисленные отношения между универсальными алгебрами. Необходимые определения условных, позитивно условных, $\exists^+$ -условных, элементарно условных термов и соответствующих отношений рациональной эквивалентности можно найти в указанных выше работах автора [3] — [6].

ТЕОРЕМА 1. Для любых конечных алгебр $\mathcal{A}$ и $\mathcal{B}$, если алгебра $\mathcal{A}^2$ рационально эквивалентна алгебре $\mathcal{B}^2$, то и алгебра $\mathcal{A}$ рационально эквивалентна алгебре $\mathcal{B}$.

Доказательство. Через $\mathcal{A}^*$ обозначим полное термальное обогащение алгебры $\mathcal{A}$. Если π — некоторая перестановка сигнатурных символов алгебры $\mathcal{A}$, то $\pi(\mathcal{A})$ будет обозначать алгебру, получаемую из $\mathcal{A}$ перестановкой, согласно π , соответствующих сигнатурных функций алгебры $\mathcal{A}$. Таким образом, для любых алгебр $\mathcal{A}_1, \mathcal{A}_2$ их рациональная эквивалентность равносильна существованию перестановки π сигнатурных символов алгебры $\mathcal{A}_1^*$ такой, что

*Работа выполнена при финансовой поддержке РФФИ (грант №02-01-00258)

алгебры $\pi(\mathcal{A}_1^*)$ и $\mathcal{A}_2^*$ изоморфны. Заметим так же, что $(\mathcal{A}^2)^* = (\mathcal{A}^*)^2$ и для любой перестановки π сигнатурных символов алгебры $\mathcal{A}$ имеет место равенство $\pi((\mathcal{A}^2)^2) = (\pi(\mathcal{A}))^2$. Тем самым, если алгебра $\mathcal{A}^2$ и $\mathcal{B}^2$ рационально эквивалентны, то существует перестановка π сигнатурных символов алгебры $\mathcal{A}^*$ такая, что $\pi((\mathcal{A}^2)^*) \cong (\mathcal{A}^2)^*$. Но тогда $\pi((\mathcal{A}^2)^*) = \pi((\mathcal{A}^*)^2) = (\pi(\mathcal{A}^*))^2$, $(\mathcal{B}^2)^* = (\mathcal{B}^*)^2$, т. е. $(\pi(\mathcal{A}^*))^2 \cong (\mathcal{B}^*)^2$. По теореме Ловаша, алгебры $\pi(\mathcal{A}^*)$ и $\mathcal{B}^*$ будут изоморфными и, тем самым, алгебры $\mathcal{A}$ и $\mathcal{B}$ — рационально эквивалентны. Теорема доказана.

ТЕОРЕМА 2. Для любых конечных алгебр $\mathcal{A}$ и $\mathcal{B}$, если алгебра $\mathcal{A}^2$ $\exists^+$ -условно рационально эквивалентна алгебре $\mathcal{B}^2$, то и алгебра $\mathcal{A}$ $\exists^+$ -условно рационально эквивалентна алгебре $\mathcal{B}$.

Доказательство. По следствию 3 из [6] $\exists^+$ -условная рациональная эквивалентность алгебр $\mathcal{A}_1$ и $\mathcal{A}_2$ равносильна существованию биекции φ основного множества алгебры $\mathcal{A}_1$ на основное множество алгебры $\mathcal{A}_2$ такой, что $\varphi(\text{Sub } \mathcal{A}_1) = \text{Sub } \mathcal{A}_2$ и φ сопрягает совокупности эндоморфизмов алгебр $\mathcal{A}_1$ и $\mathcal{A}_2$. Пусть π_1 и π_2 — эндоморфизмы алгебры $\mathcal{A}^2$, соответствующие проецированию алгебры $\mathcal{A}^2$ на ее сомножители, рассматриваемые как диагональная подалгебра $\Delta_{\mathcal{A}}$ алгебры $\mathcal{A}^2$ (т. е. $\pi_1(\langle a, b \rangle) = \langle a, a \rangle$, $\pi_2(\langle a, b \rangle) = \langle b, b \rangle$). Тогда, если φ — биекция $\mathcal{A}^2$ на $\mathcal{B}^2$, соответствующая $\exists^+$ -условной рациональной эквивалентности алгебр $\mathcal{A}^2$ и $\mathcal{B}^2$, то $\varphi\pi_1\varphi^{-1}$ и $\varphi\pi_2\varphi^{-1}$ так же образуют пару эндоморфизмов алгебры $\mathcal{B}^2$, соответствующих проецированиям алгебры $\mathcal{B}^2$ при некотором изоморфном представлении последней как декартова квадрата $\mathcal{L} \times \mathcal{L}$ ($\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$, $\theta_1 \vee \theta_2 = \nabla_{\mathcal{B}^2}$, $\theta_1 \wedge \theta_2 = \Delta_{\mathcal{B}^2}$, где $\theta_i = \ker \varphi\pi_i\varphi^{-1}$) для $\mathcal{L} = \varphi\pi_1\varphi^{-1}(\mathcal{B}^2) = \varphi\pi_2\varphi^{-1}(\mathcal{B}^2)$. При этом $\varphi(\Delta_{\mathcal{A}}) = \mathcal{L}$, $\varphi(\text{Sub } \Delta_{\mathcal{A}}) = \text{Sub } \mathcal{L}$ и φ сопрягает эндоморфизмы алгебр $\Delta_{\mathcal{A}}$ и $\mathcal{L}$. Последнее, по следствию 3 из [6], в силу изоморфизма алгебр $\Delta_{\mathcal{A}}$ и $\mathcal{A}$, влечет $\exists^+$ -условную рациональную эквивалентность алгебр $\mathcal{A}$ и $\mathcal{L}$. В силу же теоремы Ловаша, изоморфизм алгебр $\mathcal{B}^2$ и $\mathcal{L}^2$ влечет изоморфизм алгебр $\mathcal{L}$ и $\mathcal{B}$. Теорема доказана.

Точно также, на основе следствия 1 из [5] (критерия позитивной условной рациональной эквивалентности алгебр $\mathcal{A}_1$ и $\mathcal{A}_2$: алгебры $\mathcal{A}_1$ и $\mathcal{A}_2$ позитивно условно рационально эквивалентны тогда и только тогда, когда существует биекция φ алгебры $\mathcal{A}_1$ на $\mathcal{A}_2$ такая, что $\varphi(\text{Sub } \mathcal{A}_1) = \text{Sub } \mathcal{A}_2$ и φ сопрягает совокупности внутренних гомоморфизмов, т. е. гомоморфизмов между подалгебрами алгебр $\mathcal{A}_1$ и $\mathcal{A}_2$, соответственно) доказывается следующее утверждение.

ТЕОРЕМА 3. Для любых конечных алгебр $\mathcal{A}$ и $\mathcal{B}$, если алгебра $\mathcal{A}^2$ позитивно условно рационально эквивалентна алгебре $\mathcal{B}^2$, то и алгебры $\mathcal{A}$ и $\mathcal{B}$ позитивно условно рационально эквивалентны.

Остановимся на вопросе переноса утверждений теорем 1 — 3 на бесконеч-

ные алгебры.

ЛЕММА 1. Для любых булевых алгебр $\mathcal{B}_1$ и $\mathcal{B}_2$ следующие условия равносильны:

- 1) $\mathcal{B}_1$ и $\mathcal{B}_2$ изоморфны,
- 2) $\mathcal{B}_1$ и $\mathcal{B}_2$ рационально эквивалентны,
- 3) $\mathcal{B}_1$ и $\mathcal{B}_2$ позитивно условно рационально эквивалентны,
- 4) $\mathcal{B}_1$ и $\mathcal{B}_2$ $\exists^+$ -условно рационально эквивалентны,
- 5) $\mathcal{B}_1$ и $\mathcal{B}_2$ условно рационально эквивалентны,
- 6) $\mathcal{B}_1$ и $\mathcal{B}_2$ элементарно условно рационально эквивалентны.

Доказательство. Импликации 1) $\rightarrow$ 2), 2) $\rightarrow$ 3), 3) $\rightarrow$ 4), 3) $\rightarrow$ 5), 4) $\rightarrow$ 6), 5) $\rightarrow$ 6) очевидны. С другой стороны, так же очевидно, что если $\mathcal{B}_1$ и $\mathcal{B}_2$ элементарно условно рационально эквивалентны, то существует биекция π основного множества алгебры $\mathcal{B}_1$ на основное множество алгебры $\mathcal{B}_2$ такая, что $\pi(\text{Sub } \mathcal{B}_1) = \text{Sub } \mathcal{B}_2$. В то же время, как хорошо известно ([9]), изоморфизм решеток подалгебр булевых алгебр $\mathcal{B}_1$ и $\mathcal{B}_2$ влечет изоморфизм самих булевых алгебр $\mathcal{B}_1$ и $\mathcal{B}_2$, т. е. импликация 6) $\rightarrow$ 1) так же имеет место.

Заметим теперь, что утверждения теорем 1 — 3 перестают быть верными для бесконечных алгебр. К примеру, как хорошо известно ([2]) существуют неизоморфные бесконечные булевы алгебры $\mathcal{B}_1$ и $\mathcal{B}_2$ такие, что их квадраты $\mathcal{B}_1^2$ и $\mathcal{B}_2^2$ изоморфны. В силу утверждения леммы, эти алгебры являются контрпримерами для утверждений теорем 1 — 3 и аналогов этих теорем для отношений условной и элементарно условной рациональной эквивалентностей, распространенных на бесконечные алгебры.

Вопрос о справедливости аналогов утверждений теорем 1 — 3 для отношений условной и элементарно условной рациональной эквивалентности на конечных алгебрах остается открытым.

В силу известных критериев условной и элементарно условной эквивалентности алгебр ([7],[4]) этот вопрос может быть сформулирован в следующем виде:

ПРОБЛЕМА. Пусть для некоторых конечных алгебр $\mathcal{A} = \langle A; \sigma_1 \rangle$, $\mathcal{B} = \langle B; \sigma \rangle$ существует биекция φ множества A^2 на множество B^2 такая, что $\varphi(\text{Sub } \mathcal{A}^2) = \text{Sub } \mathcal{B}^2$ и φ сопрягает совокупности $\text{Iso } \mathcal{A}^2$ и $\text{Iso } \mathcal{B}^2$ (φ сопрягает совокупности $\text{Aut } \mathcal{A}^2$ и $\text{Aut } \mathcal{B}^2$) обязана ли в этом случае существовать биекция ψ множества A на множество B такая, что $\psi(\text{Sub } \mathcal{A}) = \text{Sub } \mathcal{B}$ и ψ сопрягает совокупности $\text{Iso } \mathcal{A}$ и $\text{Iso } \mathcal{B}$ (φ сопрягает совокупности $\text{Aut } \mathcal{A}$ и $\text{Aut } \mathcal{B}$)?

Здесь $\text{Iso } \mathcal{L}$ — совокупность изоморфизмов между подалгебрами алгебры $\mathcal{L}$.

Для отношения условной рациональной эквивалентности между алгебрами мы можем привести лишь следующие результаты

УТВЕРЖДЕНИЕ. Для любых конечных неодноэлементных алгебр $\mathcal{A}$ и $\mathcal{B}$, если алгебра $\mathcal{A}^2$ условно рационально эквивалентна алгебре $\mathcal{B}^2$, то найдутся такие неодноэлементные подалгебры $\mathcal{A}' \subseteq \mathcal{A}$, $\mathcal{B}' \subseteq \mathcal{B}$, что $\mathcal{A}'$ и $\mathcal{B}'$ условно рационально эквивалентны.

Доказательство. По следствию 1 из [7] условно рациональная эквивалентность алгебр $\mathcal{L}_1$ и $\mathcal{L}_2$ равносильна существованию биекции φ основного множества алгебры $\mathcal{L}_1$ на основное множество алгебры $\mathcal{L}_2$ такой, что $\varphi(\text{Sub } \mathcal{L}_1) = \text{Sub } \mathcal{L}_2$ и φ сопрягает совокупности внутренних изоморфизмов (изоморфизмов между подалгебрами) алгебр $\mathcal{L}_1$ и $\mathcal{L}_2$. Пусть π_i (при $i = 1, 2$) эпиморфизмы алгебры $\mathcal{L}^2$ на сомножители $\mathcal{L}$ (т.е. $\pi_1(\langle a, b \rangle) = a$, $\pi_2(\langle a, b \rangle) = b$).

Пусть $\mathcal{A}'$ — минимальная по мощности неодноэлементная подалгебра алгебры $\mathcal{A}$ и пусть $|\mathcal{A}| = k$. Тогда в $\mathcal{A}^2$ тоже нет неодноэлементных подалгебр, мощности меньшей, чем k . Это же, в силу существования биекции φ , будет верно и для алгебры $\mathcal{B}^2$. Но тогда, для некоторого $i \in \{1, 2\}$ $\pi_i \varphi$ будет биекцией алгебры $\Delta_{(\mathcal{A}')^2}$ на некоторую подалгебру $\mathcal{B}'$ алгебры $\mathcal{B}$. При этом, т.к. $\mathcal{A}' \cong \Delta_{(\mathcal{A}')}$, то композиция этого изоморфизма и биекции $\pi_i \varphi$ сохраняет подалгебры алгебры $\mathcal{A}'$ и ее внутренние изоморфизмы, т.е. $\mathcal{A}'$ и $\mathcal{B}'$ условно термально эквивалентны, что и требовалось доказать.

В заключении остановимся на вопросе сохранимости рассмотренных выше отношений между алгебрами, относительно операции декартова квадрата. Очевидным образом, этим свойством обладает отношение рациональной эквивалентности, т.е., если алгебры $\mathcal{A}$ и $\mathcal{B}$ рационально эквивалентны, то таковыми будут и их квадраты $\mathcal{A}^2$ и $\mathcal{B}^2$. Для отношения условной рациональной эквивалентности это уже не так. К примеру, если $\mathcal{A}$ двухэлементная решетка, а $\mathcal{B}$ — обогащение $\mathcal{A}$ путем добавления в сигнатуру трехместного дискриминатора, то $\mathcal{A}$ и $\mathcal{B}$ условно рационально эквивалентны. В то же время $\mathcal{A}^2$ содержит трехэлементную подалгебру, а в $\mathcal{B}^2$ трехэлементных подалгебр нет и, значит, в силу следствия 1 из [7], алгебры $\mathcal{A}^2$ и $\mathcal{B}^2$ не являются условно рационально эквивалентными. Этот же пример доказывает, что элементарно условная рациональная, позитивная условная и $\exists^+$ -условная эквивалентности не сохраняются при возведении в квадрат: $\mathcal{A}$ и $\mathcal{B}$ эквивалентны относительно всех перечисленных эквивалентностей ($\text{Sub } \mathcal{A} = \text{Sub } \mathcal{B}$, $\text{Aut } \mathcal{A} = \text{Aut } \mathcal{B}$, $\text{End } \mathcal{A} = \text{End } \mathcal{B}$, $\text{Ihm } \mathcal{A} = \text{Ihm } \mathcal{B}$), а $\mathcal{A}^2$ и $\mathcal{B}^2$ нет ($|\text{Sub } \mathcal{A}^2| \neq |\text{Sub } \mathcal{B}^2|$).

Наконец, укажем на результат Г. Такаша [8], представляющий интерес в связи с затронутыми в этой работе вопросами: для любых конечных решеток L и K , изоморфизм решеток $\text{Sub } K^2$ и $\text{Sub } L^2$ влечет изоморфизм решеток K и L , либо K и L^* . Здесь L^* — решетка двойственная к решетке L .

Таким образом, в частности, позитивно условно, $\exists^+$ -условно, условно и элементарно условно рациональная эквивалентности квадратов двух конечных

решеток влекут соответствующую эквивалентность самих этих решеток.

Список литературы

- [1] L.Lovasz. Operations with structures // Acta Math. Acad. Sci. Hungar., 1967, v.18, №3–4, p.321–328.
- [2] J. Ketonen. The structure of countable boolean algebras // Ann. of Math., 1978, v.108, №1, p.41–89.
- [3] А.Г. Пинус. Условные термы и их применение в алгебре и теории вычислений // Успехи матем. наук, 2001, т. 56, №2, с. 37–72.
- [4] А.Г. Пинус. N-элементарные вложения и n-условные термы // Известия вузов. Математика, 1999, №4, с. 39–43.
- [5] А.Г. Пинус. Внутренние гомоморфизмы и позитивно условные термы // Алгебра и логика, 2001, т. 40, №2, с. 158–173.
- [6] А.Г. Пинус. О функциях коммутирующих с преобразованиями алгебр // Сиб. мат. журнал, 2000, т. 41, №6, с.1409–1418.
- [7] А.Г. Пинус. Исчисление условных тождеств и условно рациональная эквивалентность // Алгебра и логика, 1998, т. 37, №4, с. 432–459.
- [8] G. Takach. Notes on sublattice - lattices //Periodica Math.Hungar., 1997, v. 35, №3, p. 215–224.
- [9] D.Sachs. The lattice of subalgebras of a Boolean algebra // Canad. J. Math., 1962, v. XIV, №3, p. 451–460.

ГРУППЫ ЕДИНИЦ ЦЕЛОЧИСЛЕННЫХ ГРУППОВЫХ КОЛЕЦ КОНЕЧНЫХ ГРУПП

Попова А. М., Порошенко Е. Н.*

Кафедра алгебры и математической логики
Новосибирский государственный технический университет
проспект К. Маркса, 20
Новосибирск, 2003, Россия
e-mail: algebra@nstu.ru

Введение

В данной работе мы продолжаем исследование алгоритма, подробно описанного в [1], для конкретных групп, а именно, реализуем этот алгоритм для S_3 , A_4 . При этом уточняется результат для S_3 , полученный ”вручную“ и опубликованный в [2].

1 Описание алгоритма и формулировки результатов

Поскольку для выше перечисленных групп известны таблицы характеров, реализация алгоритма начинается с шага 4 (см. [1]). Напомним его. Пусть $G = \{g_1 = e, g_2, \dots, g_N\}$ — конечная группа; $H_1, H_2, \dots, H_s$ — классы сопряженности элементов группы G ; $Z_1(G), Z_2(G), \dots, Z_s(G)$ — все неприводимые неэквивалентные представления группы G ; $z_1, z_2, \dots, z_s$ — их порядки; χ_i^j — значение характера χ_i на классе H_j , $i, j = 1, 2, \dots, s$; $R(G)$ —регулярное (правое или левое) представление группы G . Образует матрицы

$$A_j = \frac{z_j}{N} \sum_{g \in G} \chi_j(g) R(g). \quad (2.1)$$

Находим базисы подпространств собственных векторов этих матриц, относящихся к собственному значению $\lambda = 1$. Эти подпространства инвариантны

*Работа выполнена при поддержке РФФИ (проекты 01-01-0062 и 02-01-00258).

относительно $R(G)$ (см. [3]), поэтому в базисе, составленном из этих векторов, $R(G)$ приводится к клеточно-диагональному виду

$$R(G) \simeq T(G) = \begin{pmatrix} \boxed{T_1(G)} & & 0 \\ & \ddots & \\ 0 & & \boxed{T_s(G)} \end{pmatrix}. \quad (2.2)$$

Следует заметить, что в клеточно-диагональном виде (2.2) клетки $T_i(G)$ являются неэквивалентными представлениями группы G . Если при этом $T_i(G)$ и $T_j(G)$ ($i \neq j$) неизоморфны, то они *расклеиваются*, то есть кольцо $QT(G)$ содержит матрицы вида

$$\text{diag}(0, \dots, 0, T_i(G), 0, \dots, 0) \text{ и} \\ \text{diag}(0, \dots, 0, T_j(G), 0, \dots, 0).$$

Если же $T_i(G)$ и $T_j(G)$ изоморфны, то они не расклеиваются (см. [4]). Понятно, что если они расклеиваются, то порождающие группы единиц можно искать отдельно для клеток $T_i(G)$ и $T_j(G)$. В противном случае порождающие можно искать только для клетки $T_i(G)$, так как $T_i(G) \simeq T_j(G)$. Таким образом, в обоих случаях задача сводится к рассмотрению одной клетки. Вопрос о расклейке легко решается определением совместности систем линейных уравнений вида (2.3) над полем рациональных чисел:

$$x_1 T(e) + x_2 T(g_2) + \dots + x_s T(g_s) = \\ = \text{diag}(0, \dots, 0, T_i(e), 0, \dots, 0), \quad i = 1, 2, \dots, s. \quad (2.3)$$

В свою очередь, каждая клетка $T_i(G)$ приводится к клеточно-диагональному виду

$$T_i(G) \simeq D_i(G) = \begin{pmatrix} \boxed{Z_i(G)} & & 0 \\ & \ddots & \\ 0 & & \boxed{Z_i(G)} \end{pmatrix},$$

где $Z_i(G)$ — i -е неприводимое представление группы G , причем в $T_i(G)$ содержится в точности z_i клеток, они изоморфны, поэтому не расклеиваются (см. [5]). Поскольку $Z_i(G)$ — абсолютно неприводимое представление, то в кольце $\mathbb{Z}Z_i(G)$ лежат матрицы $m_{i,j}e_{i,j}$ для некоторых ненулевых натуральных $m_{i,j}$. Поэтому очевидно, что любая матрица из $\mathbb{Z}T_i(G)$ имеет ранг kz_i , где $k = 0, 1, \dots, z_i$. Это следует из того, что линейная оболочка неприводимой группы совпадает с полной матричной алгеброй над некоторым телом (см. [6]). Для приведения $T_i(G)$ к клеточно-диагональному виду достаточно в $\mathbb{Z}T_i(G)$ найти матрицу ранга z_i и породить ею правый идеал, найти в этом идеале минимальный базис из z_i элементов и представить в этом базисе каждое

$T_i(g)$ ($g \in G$), как линейный оператор, действующий на этом идеале правыми умножениями. Под минимальным базисом мы понимаем такой аддитивный базис идеала, по которому все элементы идеала раскладываются с целыми коэффициентами. Отыскание такого базиса описано в [4].

Итак, мы получаем представление

$$D(G) = \begin{pmatrix} \boxed{Z_1(G)} & & & & & \\ & \ddots & & & & 0 \\ & & \boxed{Z_1(G)} & & & \\ \underbrace{\hspace{10em}}_{z_1} & & & \ddots & & \\ & & 0 & & \boxed{Z_s(G)} & \\ & & & & & \ddots \\ & & & & \underbrace{\hspace{10em}}_{z_s} \boxed{Z_s(G)} & \end{pmatrix},$$

которое, очевидно, изоморфно такому:

$$\tilde{D}(G) = \begin{pmatrix} \boxed{Z_1(G)} & & 0 \\ & \ddots & \\ 0 & & \boxed{Z_s(G)} \end{pmatrix}.$$

Теперь уже для каждой клетки $Z_i(G)$ находим ее *расклеивающее число*, то есть наименьшее ненулевое натуральное число m_i , для которого $\text{diag}(0, \dots, 0, m_i Z_i(G), 0, \dots, 0) \subseteq \mathbb{Z}\tilde{D}(G)$. Если клетки $Z_i(G)$ и $Z_j(G)$ не расклеиваются, то находим m_i такое, что

$$\text{diag}(0, \dots, 0, m_i Z_i(G), 0, \dots, 0, m_i Z_j(G), 0, \dots, 0) \subseteq \mathbb{Z}\tilde{D}(G).$$

Понятно, что m_i есть наименьшее общее кратное знаменателей решения системы

$$x_1 \tilde{D}(g_{i_1}) + \dots + x_k \tilde{D}(g_{i_k}) = \text{diag}(0, \dots, 0, E_{z_i}, 0, \dots, 0). \quad (2.4)$$

Здесь $\tilde{D}(g_{i_1}), \tilde{D}(g_{i_2}), \dots, \tilde{D}(g_{i_k})$ — аддитивный базис кольца $\mathbb{Z}\tilde{D}(G)$, который находим аналогично [4], E_{z_i} — единичная матрица порядка z_i .

Обозначим для краткости $\mathbb{Z}\tilde{D}(G) = \vartheta$, $\mathbb{Z}Z_i(G) = \vartheta_i$, $i = 1, 2, \dots, s$ и введем обозначения аналогично [4]. Пусть m_i — расклеивающее число для ϑ_i .

$$\begin{aligned} \gamma_{m_i} : \mathbb{Z} &\longrightarrow \mathbb{Z}/(m_i) = \overline{\mathbb{Z}}, \\ \psi_{m_i} : \mathbb{Z}_{z_i} &\longrightarrow \overline{\mathbb{Z}}_{z_i}, \\ \varphi_{m_i} : \text{GL}_{z_i}(\mathbb{Z}) &\longrightarrow \text{GL}_{z_i}(\overline{\mathbb{Z}}), \\ U_0(\vartheta_i) &= U(\vartheta_i) \cap \text{Ker} \varphi_{m_i} \end{aligned}$$

Здесь $U(\vartheta_i)$ — группа единиц кольца ϑ_i . Пусть

$$\begin{aligned}\psi_m(\vartheta) &= \text{diag}(\psi_{m_1}(\vartheta_1), \psi_{m_2}(\vartheta_2), \dots, \psi_{m_s}(\vartheta_s)) = \\ &= \text{diag}(\bar{\vartheta}_1, \bar{\vartheta}_2, \dots, \bar{\vartheta}_s), \\ U_0(\vartheta) &= \text{diag}(U_0(\vartheta_1), U_0(\vartheta_2), \dots, U_0(\vartheta_s)), \\ \overline{U(\vartheta)} &= U(\vartheta)/U_0(\vartheta).\end{aligned}$$

Теперь понятно, что порождающие $U(\vartheta)$ можно искать в два этапа: сначала порождающие $\overline{U(\vartheta)}$, затем — порождающие $U_0(\vartheta)$.

Остановимся на порождающих $\overline{U(\vartheta)}$. Понятно, что можно найти порождающие $\overline{U(\vartheta_i)}$ для каждого $i = 1, 2, \dots, s$, как целочисленные линейные комбинации базисов колец ϑ_i (см. [4]). Заметим, что, в силу абсолютной неприводимости представлений $Z_i(G)$, элементы этих базисов можно выбрать из элементов $Z_i(G)$. Тогда всякая целочисленная линейная комбинация элементов $\bar{\vartheta}_i$ однозначно определяет элемент из $\bar{\vartheta}$. Поэтому в качестве порождающих $\overline{U(\vartheta)}$ достаточно взять пересечение множеств линейных комбинаций всех $\overline{U(\vartheta_i)}$. Именно в этом месте реализации алгоритма и возникает перебор. Действительно, пусть $\vartheta_i = \{t_1, t_2, \dots, t_{z_i}\}_{\mathbb{Z}}$, где $t_j \in Z_i(G)$. Тогда $\bar{\vartheta}_i = \{\sum_{j=1}^{z_i} n_j t_j, 0 \leq n_j \leq m_i - 1\}$, $\overline{U(\vartheta_i)} = \{\sum_{j=1}^{z_i} u_j t_j \mid \sum_{j=1}^{z_i} u_j = 1, \det(\sum_{j=1}^{z_i} n_j t_j) = \pm 1\}$. Таким образом, для нахождения элементов $\overline{U(\vartheta_i)}$ нужно перебрать $m_i^{z_i-1}$ линейных комбинаций и выбрать из них те, которые удовлетворяют равенству $\det(\sum_{j=1}^{z_i} n_j t_j) = \pm 1$. Чтобы выбрать порождающие $\overline{U(\vartheta_i)}$, нужно из полученного множества матриц выбросить те, которые являются произведениями других, и те, которые равны между собой по модулю m_i .

Теперь о порождающих $\text{Ker } \varphi_{m_i}$. Если $z_i \geq 3$, то, как следует из [7], $\text{Ker } \varphi_{m_i} = (\tau_{kj}(m_i), k \neq j, k, j = 1, 2, \dots, z_i)$, здесь $\tau_{kj}(\lambda) = E_{z_i} + \lambda e_{kj}$, где e_{kj} — матричная единица порядка z_i .

Отдельного рассмотрения требует случай $z_i = 2$. Пусть $0 \in m \in \mathbb{N}$, $\varphi_m : \text{GL}_2(\mathbb{Z}) \rightarrow \text{GL}_2(\overline{\mathbb{Z}})$, $a = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $H = (a, b^m, b^{-1}ab, \dots, b^{-m+1}ab^{m-1})$.

Лемма 1. $\text{Ker } \varphi_m = H$.

Доказательство. Очевидно, $H \subseteq \text{Ker } \varphi_m$. Докажем, что $\text{Ker } \varphi_m \subseteq H$. Пусть $g \in \text{Ker } \varphi_m$, тогда первая строчка g получается как элемент орбиты группы $G = (a, b)$ элемента $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ (см. [7]). Теперь легко вычислить, что $g = a^l(a^{\alpha_1}b^{\beta_1}a^{\alpha_2}b^{\beta_2} \dots a^{\alpha_r}b^{\beta_r})^\top$, отсюда следует, что $\tilde{g} = a^{\alpha_1}b^{\beta_1}a^{\alpha_2}b^{\beta_2} \dots a^{\alpha_r}b^{\beta_r} \in \text{Ker } \varphi_m$. Применяем собирательный процесс: $ba = abb^{-1}a^{-1}ba = abh$, $h \in H$.

После применения собирательного процесса получаем $\tilde{g} = hb^\beta h'$, где $h, h' \in H$. Так как $\tilde{g}, h, h' \in \text{Ker } \varphi_m$, получаем $b^\beta \in \text{Ker } \varphi_m$, то есть $\beta \equiv 0 \pmod{m}$, отсюда следует, что $\sum_{i=1}^r \beta_i \equiv 0 \pmod{m}$, а тогда имеем $a^{\alpha_1}b^{\beta_1}a^{\alpha_2}b^{\beta_2} \dots a^{\alpha_r}b^{\beta_r} =$

$a^{\alpha_1} b^{\beta_1} a^{\alpha_2} b^{-\beta_1} b^{\beta_1 + \beta_2} \dots a^{\alpha_r} b^{\beta_1 + \dots + \beta_r} \in H$. Откуда $g^\top \in H$, а поскольку $(\text{Кер } \varphi_m)^\top = \text{Кер } \varphi_m$, то и $g \in H$. Что и требовалось доказать.

Итак, вопрос о порождающих группы $\text{Кер } \varphi_m$ решен для любых $z_i \geq 2$.

Для $z_i = 1$ вопрос о порождающих $U(\vartheta_i)$ сводится к вопросу о порождающих группы единиц кольца целых чисел над алгебраическими расширениями поля рациональных чисел. Этот вопрос подробно изложен в [8]. У нас он возник при реализации алгоритма для A_4 . Здесь поле $\mathbb{Q}(\sqrt[3]{1})$. Но так как $|\mathbb{Q}(\sqrt[3]{1}) : \mathbb{Q}| = 2$, $s = 0$, $t = 1$, имеем $r = s + t - 1 = 0$, то есть в любом порядке этого поля группа единиц тривиальна (Систему обозначений см. в [8]).

Как было замечено в начале, мы реализовали алгоритм для S_3 и A_4 . Поскольку $\mathbb{Z}R(G) \simeq \mathbb{Z}\tilde{D}(G) \simeq \mathbb{Z}G$, то, найдя порождающие для $U(\mathbb{Z}\tilde{D}(G))$, можно вернуться в $U(\mathbb{Z}G)$ и записать порождающие в виде целочисленных линейных комбинаций элементов соответствующих групп.

Дадим запись результатов в матричной форме. Предварительно заметим, что для S_3 $z_1 = z_2 = 1$, $z_3 = 2$, а расклеивающее число для $T_3(S_3)$ $m = 3$.

$$\tilde{D}((12)) = \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & 1 & 0 \\ & & -1 & -1 \end{pmatrix}, \tilde{D}((13)) = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & -1 & -1 \\ & & 0 & 1 \end{pmatrix},$$

$$\begin{aligned} a &= \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}, & b &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \\ b^{-1}ab &= \begin{pmatrix} -2 & -3 \\ 3 & 4 \end{pmatrix}, & b^{-2}ab^2 &= \begin{pmatrix} -5 & -12 \\ 3 & 7 \end{pmatrix}. \end{aligned}$$

$$U(\mathbb{Z}S_3) \simeq \{\pm 1\} \times \left(\begin{pmatrix} 1 & & & \\ & -1 & & \\ & & 1 & 0 \\ & & -1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & -1 & -1 \\ & & 0 & 1 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & 0 \\ & & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & 3 \\ & & 0 & 1 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & -2 & -3 \\ & & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & -5 & -12 \\ & & 3 & 7 \end{pmatrix} \right).$$

Теорема 1.

Из теоремы 1 следует, что группа единиц кольца $\mathbb{Z}S_3$ порождается, естественно, самой группой S_3 и группой изоморфной $\text{Кер } \varphi_3$ порядка 2.

Аналогичный результат получен для $\mathbb{Z}A_4$. Здесь $z_1 = z_2 = z_3 = 1$, $z_4 = 3$, расклеивающее число для $Z_4(A_4)$ $m = 4$:

$$\tilde{D}((123)) = \begin{pmatrix} 1 & & & & & \\ & -\frac{1}{2} - i\frac{\sqrt{3}}{2} & & & & \\ & & -\frac{1}{2} + i\frac{\sqrt{3}}{2} & & & \\ & & & 0 & 1 & 0 \\ & & & 1 & 0 & -1 \\ & & & -1 & 1 & 0 \end{pmatrix},$$

$$\tilde{D}((12)(34)) = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & -1 & -1 & 1 \\ & & 0 & 0 & 1 \\ & & 0 & 1 & 0 \end{pmatrix}.$$

Теорема 2. $U(\mathbb{Z}A_4) \simeq \{\pm 1\} \times (\tilde{D}((123)), \tilde{D}((12)(34)), \text{diag}(1, 1, 1, \tau_{kl}(4)) | k \neq l; k, l = 1, 2, 3; \tau_{kl} = E_3 + 4e_{kl})$.

2 Реализация алгоритма

В предыдущем разделе был описан алгоритм поиска порождающих группы единиц целочисленных групповых колец. К сожалению, этот алгоритм очень трудоемок, поэтому, даже в случае небольших групп (например, A_4), обойтись без компьютерных вычислений невозможно. Причем трудоемкость этого алгоритма возникает не только ввиду большого перебора, осуществляемого для нахождения порождающих $\overline{U}(\vartheta)$, фактически все расчеты, осуществляемые в процессе реализации алгоритма, достаточно громоздки. По этой причине мы по возможности полностью исключили вычисления вручную, начиная с построения левого регулярного представления. Для компьютерных вычислений использовались система Maple V и GAP, а также язык программирования Borland Pascal.

Перейдем к описанию реализации алгоритма. Опишем эту реализацию применительно к группе A_4 , так как для случая S_3 фактически все, кроме перебора довольно несложно проделать вручную. После того, как мы произвольным образом упорядочили все элементы группы, строим регулярное левое представление этой группы. В результате получаем 12 матриц по количеству элементов в группе. По формулам (2.1) получаем четыре матрицы (по количеству характеров). Для каждой из них находим собственные векторы, соответствующие собственному значению $\lambda = 1$. Как и следовало из алгоритма, в первых трех случаях (соответствующих характерам одномерных представлений), получим по одному собственному вектору, причем во втором и третьем

случаях, так как коэффициенты таблице характеров комплексные, получим комплексную матрицу и, соответственно, комплексный собственный вектор. В последнем случае, относящемся к трехмерному представлению, собственных векторов будет 9. Теперь составим матрицу B из 12 найденных собственных векторов (записывая их координаты по столбцам), тогда все 12 матриц $BR(g)B^{-1}$ будут иметь клеточно диагональный вид (ср. с (2.2)):

$$R(g) \simeq T(g) = \begin{pmatrix} \boxed{T_1(g)} & & 0 \\ & \ddots & \\ 0 & & \boxed{T_4(g)} \end{pmatrix},$$

где $T_1(g)$, $T_2(g)$ и $T_3(g)$ — это клетки 1×1 , причем в $T_2(g)$ и $T_3(g)$ могут быть комплексные числа, а $T_4(g)$ — клетка 9×9 .

Для разбиения клетки $T_4(g)$ на 3 клетки третьего порядка $Z_4(g)$, нам необходимо в $\mathbb{Z}T_4(G)$ рассмотреть главный правый идеал, порожденный матрицей ранга 3. Это один из немногих моментов, который не удалось алгоритмизировать. Было замечено, что матрица $C = T_4((123)) - T_4((124))$ имеет целые собственные числа: $-1, 0, 1$, поэтому матрица $C + E = C + T_4(e)$ имеет те же собственные векторы, только их собственные значения будут равны соответственно $0, 1, 2$. Поэтому в качестве матрицы, порождающей идеал, можно взять $H_1 = C(C + E)$. После этого находим еще две матрицы ранга 3: H_2 и H_3 , чтобы эти три матрицы образовывали базис полученного идеала. Оказалось, что можно взять $H_2 = H_1 T_4((123))$ и $H_3 = H_1 T_4((134))$. Рассмотрим каждое $T_4(g)$ как оператор, действующий правым умножением на элементы идеала и распишем это действие в базисе $\{H_1, H_2, H_3\}$. Полученные матрицы третьего порядка и будут соответствующими $Z_4(g)$.

Для того, чтобы найти расклеивающие числа для каждой клетки, необходимо построить матрицы $\tilde{D}(G)$ и найти решения системы (2.4). Получаем, что $m_1 = 12$, $m_4 = 4$, а клетки $Z_2(G)$ и $Z_3(G)$ соответствуют изоморфным представлениям, которые можно расклеить только при помощи $m_i \in \mathbb{C}$, $i = 2, 3$. Поэтому делаем попытку "отклеить" эти две клетки от остальных. Получаем "расклеивающее" число $m_{2,3} = 12$.

Теперь рассмотрим клетки $Z_4(g)$, $g \in G$ по модулю $m_4 = 4$. Выбираем из этих матриц 9 линейно независимых и перебираем все возможные линейные комбинации из этих линейно независимых матриц (опять же, по модулю 4) и отбираем те из них, определитель которых равен ± 1 . В итоге получили $2^{15} \cdot 3$ матриц (вопрос о природе этого числа, пока еще остается открытым). Однако, так как $\mathbb{Z}_4$, в котором мы работаем, не является полем, среди этих матриц есть равные. После того, как мы оставили каждую матрицу в одном экземпляре, их осталось $2^9 \cdot 3$. Теперь осталось выбрать из этих матриц порождающее множество, для этого необходимо исключить из них матрицы таким образом, чтобы любую исключенную можно было выразить через оставшиеся матрицы. Это самая трудоемкая часть алгоритма, ее сложность — $O(n^3)$,

где n — число матриц. После того, как эта работа была проделана, осталось всего 44 матрицы, с которыми уже можно было работать вручную, а именно осталось по этим матрицам с определителями ± 1 в $\mathbb{Z}_4$ найти матрицы с определителями ± 1 в $\mathbb{Z}$.

Проделанная работа показала, что даже для небольшой группы ($|A_4| = 12$), работа по нахождению порождающих группы единиц целочисленного группового кольца сопряжена с определенными трудностями вычислительного характера. Пока еще есть некоторый "запас прочности", но он очень небольшой, поэтому необходимо модернизировать обработку информации при поиске матриц с определителями ± 1 в $\mathbb{Z}_{m_i}$ и особенно при выборе из них порождающего множества.

Список литературы

- [1] ASYA M. POPOVA, ILYA DM. TCHERNYKH, Units in Integral Group Rings of Finite Groups, Алгебра и теория моделей 3, Новосибирск, 2001, 119–125.
- [2] А. М. ПОПОВА, Порождающие группы единиц целочисленных групповых колец конечных групп, Международная конференция "Алгебра и ее приложения", Красноярск, 2002, 98.
- [3] Ж.-П. СЕРР, Линейные представления конечных групп, Москва, Мир, 1970, 132.
- [4] А. М. ПОПОВА, Группы обратимых элементов матричных колец, Сиб. мат. журнал, 40(1999), 5, 1127–1136.
- [5] К. Р. КЭРТИС, Ж. РАЙНЕР, Теория представлений конечных групп и ассоциативных алгебр, Москва, 1969, 668.
- [6] Д. А. СУПРУНЕНКО, Группы матриц, Москва, Наука, 1972, 351.
- [7] Ч. БАСС, ДЖ. МИЛНОР, Ж.-П. СЕРР Решение конгруэнц-проблемы для SL_n ($n \geq 3$) и Sp_{2n} ($n \geq 2$), Математика, 14(1970), 6, 64–128.
- [8] З. И. БОРЕВИЧ, И. Р. ШАФАРЕВИЧ, Теория чисел, Москва, Наука, 1985, 503.

БАЗИС СВОБОДНОЙ АЛГЕБРЫ ЛЕЙБНИЦА

Е.Н. Порошенко *

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

Определение 1. Алгеброй Лейбница называется алгебра, в которой выполнено тождество:

$$(xy)z = (xz)y + x(yz). \quad (2.1)$$

Легко видеть, что это тождество представляет собой одну из форм записи тождества Якоби. Таким образом, любая алгебра Ли является алгеброй Лейбница. Легко получить, что в алгебре Лейбница выполняется аналог тождества антикоммутативности в ослабленном виде:

$$x(yz) = -x(z y). \quad (2.2)$$

В связи с этим возникает вопрос, как теоремы для алгебр Ли могут быть обобщены для алгебр Лейбница. Данная работа посвящена нахождению базиса свободной алгебры Лейбница.

Для начала напомним некоторые факты из теории алгебр Ли.

Пусть $X = \{x_i | i \in I\}$ это вполне упорядоченный алфавит, а X^* — множество ассоциативных слов, состоящих из элементов X (включая пустое слово 1). На множестве X^* введем лексикографический порядок.

Определение 2. Ассоциативное слово u называется *ассоциативным словом Линдона — Ширшова*, если для любых непустых v и w таких, что $u = vw$ выполнено $vw > wv$.

Определение 3. Неассоциативное слово $[u]$ называется *словом Линдона — Ширшова* если

- (1) u — правильное ассоциативное слово,
- (2) если $[u] = [[u_1][u_2]]$, то $[u_1]$ и $[u_2]$ — слова Линдона — Ширшова,
- (3) если $[u] = [[[u_{11}][u_{12}]]u_2]$, то $u_2 \geq u_{12}$.

*Работа выполнена при поддержке РФФИ (проекты 01-01-0062 и 02-01-00258).

Как было доказано в [1], на любом ассоциативном слове Линдона — Ширшова можно единственным способом расставить скобки, чтобы получилось неассоциативное слово Линдона — Ширшова. Именно неассоциативное слово Линдона — Ширшова, полученное из ассоциативного слова Линдона — Ширшова u мы и будем обозначать в дальнейшем $[u]$. Из [2] следует, что множество всех неассоциативных слов Линдона — Ширшова образует базис свободной алгебры, с множеством порождающих X .

Пусть k — поле характеристики $\neq 2$. Рассмотрим свободную алгебру Лейбница с множеством порождающих X (обозначим ее $\text{Leib}_k(X)$).

Конечную последовательность $x_{i_1}, x_{i_2}, \dots, x_{i_n}$ назовем *набором* длины n и будем обозначать ее $\bar{x} = (x_{i_1}, x_{i_2}, \dots, x_{i_n})$ (в наборе любой элемент множества X может повторяться любое число раз, два набора, различающиеся порядком элементов считаем различными). Рассмотрим множество $X \cup \{y\}$, полагая $y > x_i$ для любого i .

Каждому набору $(x_{i_1}, x_{i_2}, \dots, x_{i_n})$ поставим в соответствие элемент алгебры $\text{Leib}_k(X)$ (будем обозначать его $l(x_{i_1}, x_{i_2}, \dots, x_{i_n}) = l(\bar{x})$) по следующему правилу: рассмотрим правильное ассоциативное слово Линдона — Ширшова $u = yx_{i_2} \dots x_{i_n}$, расставим на нем скобки, чтобы получить неассоциативное слово Линдона — Ширшова (обозначим его $[u]$). Тогда $l(\bar{x})$ получается из $[u]$ заменой y на x_{i_1} .

Теорема. *Линейным базисом $\text{Leib}_k(X)$ является множество слов $l(\bar{x})$, где $\bar{x}$ пробегает множество всех наборов из элементов множества X .*

Доказательство. Пусть $\bar{x} = (x_{i_1}, x_{i_2}, \dots, x_{i_n})$ — произвольный набор. Рассмотрим неассоциативное слово $br(\bar{x})$, где br обозначает произвольную расстановку скобок на элементах набора. Рассмотрим слово $br(yx_{i_2} \dots x_{i_n})$. Как следует из [2], применяя тождества (2.1) и антикоммутативности, можно получить разложение

$$br(yx_{i_2} \dots x_{i_n}) = \sum_s \alpha_s [u_s]. \quad (2.3)$$

где $\alpha_s \in k$, а $[u_s]$ — неассоциативные слова Линдона — Ширшова. Легко заметить, что, так как y является наибольшей из букв, при преобразовании слова $br(yx_{i_2} \dots x_{i_n})$ на всех шагах мы будем получать слова, начинающиеся с y , следовательно, если мы преобразуем слово при помощи тождества антикоммутативности, то преобразуемое подслово не может содержать первой буквы слова, а значит это преобразование можно провести с помощью тождества (2.2). Как было отмечено, любое слово $[u_s]$ начинается с y . Заменяя эту букву в каждом слове $[u_s]$ на x_{i_1} , получим представление $br(x_{i_1}x_{i_2} \dots x_{i_n})$ в виде линейной комбинации слов требуемого вида.

Осталось доказать, что эти слова действительно образуют базис, то есть, что искомое разложение единственно. Пусть для некоторого слова $br(x_{i_1}x_{i_2} \dots x_{i_n})$ существуют хотя бы два таких разложения. В этом случае, как было доказано выше, все слова каждого из этих разложений начинаются на x_{i_1} .

Заменяя в каждом из слагаемых в разложениях x_{i_1} на y , получим, что слово $br(yx_{i_2} \dots x_{i_n})$ можно представить в виде линейной комбинации слов Линдона — Ширшова двумя различными способами, полученное противоречие доказывает теорему.

Напомним, что *составом слова* называется множество букв, входящих в это слово с указанием, сколько раз та или иная буква входит в слово. Аналогично введем понятие *состава набора*. Фактически, состав набора — это состав неассоциативного слова, полученного из данного набора.

Следствие. *Множество всех неассоциативных слов в алфавите X с левонормированной расстановкой скобок образует базис алгебры $\text{Leib}_k(X)$.*

Доказательство. Очевидно, любое слово представимо в виде линейной комбинации левонормированных слов. Осталось доказать, что все левонормированные слова линейно независимы.

Рассмотрим множество всех слов одного состава. Это множество образует конечномерное векторное пространство. В силу теоремы, размерность этого пространства равна количеству различных наборов данного состава. С другой стороны, количество левонормированных неассоциативных слов данного состава равно этому же числу. Для завершения доказательства осталось отметить, что в силу полилинейности свойства (2.1) при преобразованиях слова данного состава получаем слова того же состава.

Список литературы

- [1] А. И. Ширшов, О свободных кольцах Ли, Мат. сборник, 45(87), 2 (1958), 113–122.
- [2] А. И. Ширшов, О базах свободной алгебры Ли, Алгебра и логика, 1962, 1(1), 14–19.

ПЕРЕЧИСЛЕНИЕ КВАДРИК ПРОЕКТИВНЫХ ПЛОСКОСТЕЙ И ПРОСТРАНСТВ НАД ЛОКАЛЬНЫМИ КОЛЬЦАМИ ГЛАВНЫХ ИДЕАЛОВ

Старикова О.А.

Северный международный университет,
кафедра алгебры и геометрии,
Россия, 685000 Магадан, ул. Портовая 13
e-mail: star-olga@yandex.ru

§ 1. Квадрикой проективного пространства RP_{n-1} над R называется множество (проективное многообразие) его точек v , определяемых уравнением $vAv^T = 0$ с ненулевой симметричной $n \times n$ -матрицей A над R . К одной из основных в теории квадрик относится задача их классификации и перечисления с точностью до проективных конгруэнтностей, то есть преобразований $v \mapsto vU$ ($v \in RP_{n-1}$) для $U \in PGL_n(R)$, и с точностью до проективностей; близкой является задача классификации симметрических форм модулей над R . Эти взаимосвязанные задачи достаточно хорошо изучены, когда R — поле, [1, гл. 3], [6, 41.1]. Интерес к переходу от полей к более общим кольцам коэффициентов возрастал вместе с развитием K -теории и [8] перенесением основной теоремы проективной геометрии. В [7, § 3] доказана диагонализированность или существование ортогонального базиса "сильно невырожденной" симметрической формы на модуле над локальным кольцом с обратимым элементом 2. С другой стороны, как показывают примеры, в описаниях симметрических форм при переходе от полей к локальным кольцам коэффициентов определяющая роль форм с обратимой матрицей утрачивается.

Целью данной работы является перечисление квадрик над локальным кольцом R с главным максимальным идеалом J и обратимым элементом 2. Теорема 1 из § 2 устанавливает конгруэнтность диагональной матрице любой симметрической $n \times n$ -матрицы над R . Через R^* обозначается мультипликативная группа обратимых элементов кольца R . При $|R^* : R^{*2}| = 2$ нормальный диагональный вид симметрической матрицы указывает теорема 2, когда в $1 + R^2$ существует обратимый неквадрат, а в случае $1 + R^{*2} \subset R^{*2}$ — теорема 3, распространяющая закон инерции вещественных квадратичных форм. При указанных ограничениях и нильпотентном идеале J теорема 4 указывает

число классов проективно конгруэнтных квадрик проективного пространства RP_{n-1} .

В условиях теорем 2 и 3 на R теорема 4 и доказанная в § 3 теорема 5 завершают перечисление классов проективно эквивалентных квадрик проективной плоскости RP_2 ; такое перечисление при более специальном выборе R устанавливалось ранее, см. [9], [10]. Теоремы 1 – 4 приводятся в § 2 без доказательства; они установлены в нераздельном соавторстве с В.М.Левчуком и с полными доказательствами публикуются в другой статье.

§ 2. Следующая теорема устанавливает диагонализированность симметрических $n \times n$ -матриц над локальным кольцом R главных идеалов с $2 \in R^*$. Через M_{R^*} обозначаем фиксированную систему представителей смежных классов группы R^* по подгруппе R^{*2} , содержащую единицу кольца R .

Теорема 1. Пусть R есть локальное кольцо с главным максимальным идеалом $\langle \varepsilon \rangle$ и обратимым элементом 2. Тогда всякая симметрическая $n \times n$ -матрица A над R конгруэнтна диагональной матрице вида

$$\text{diag} (k_1 \varepsilon^{t_1}, k_2 \varepsilon^{t_2}, \dots, k_r \varepsilon^{t_r}, 0, \dots, 0), \quad 0 \leq t_1 \leq t_2 \leq \dots \leq t_r, \quad \varepsilon^{t_r} \neq 0, \quad (2.1)$$

где $k_i \in M_{R^*}$ и для линейно упорядоченной системы M_{R^*} при $t_{i-1} = t_i$ предполагаем также $k_{i-1} \leq k_i$. Набор показателей $t_1, t_2, \dots, t_r$ определен для A однозначно, в частности, при $R^{*2} = R^*$ матрица A конгруэнтна единственной матрице (2.1).

При дополнительных ограничениях на R следующие две теоремы указывают нормальный диагональный вид симметрической матрицы. Ограничение $1 + J \subset R^{*2}$ в них не является жестким; несложно показывается, что если J — ниль-идеал в R или J есть собственный идеал кольца R формальных степенных рядов над полем, то $1 + J \subset R^{*2}$.

Теорема 2. Пусть R есть локальное кольцо с обратимым элементом 2 и главным максимальным идеалом $J = \langle \varepsilon \rangle$, причем $1 + J \subset R^{*2}$, $|R^* : R^{*2}| = 2$ и существует обратимый неквадрат $k \in 1 + R^2$. Тогда всякая ненулевая симметрическая матрица над R конгруэнтна единственной диагональной матрице вида

$$\text{diag}(\delta_i \varepsilon^i, \varepsilon^i, \dots, \varepsilon^i, \dots, \delta_m \varepsilon^m, \varepsilon^m, \dots, \varepsilon^m, 0, \dots, 0), \quad 0 \leq i < \dots < m, \quad (2.2)$$

где $\varepsilon^m \neq 0$ и каждый элемент $\delta_i, \dots, \delta_m$ равен 1 или k .

Заметим, что теорема 1 устанавливает диагонализированность и квадратичных форм над R . Следующая теорема распространяет закон инерции вещественных квадратичных форм на случай определенных локальных колец коэффициентов. Выделим формы вида

$$[-(x_1^2 + \dots + x_{s_1}^2) + (x_{s_1+1}^2 + \dots + x_{r_1}^2)]\varepsilon^{i_1} + \dots + [-(x_{r_1+\dots+r_{q-1}+1}^2 + \dots + x_{r_1+\dots+r_{q-1}+s_q}^2) + (x_{r_1+\dots+r_{q-1}+s_q+1}^2 + \dots + x_{r_1+\dots+r_{q-1}+r_q}^2)]\varepsilon^{i_q}, \quad (2.3)$$

где $q > 0$, $0 \leq i_1 < \dots < i_q$, $\varepsilon^{i_q} \neq 0$, $r_1, \dots, r_q$ — целые положительные числа, $r_1 + \dots + r_q \leq n$, $s_1, \dots, s_q$ — целые числа, $0 \leq s_1 \leq r_1, \dots, 0 \leq s_q \leq r_q$.

Теорема 3. Пусть R есть локальное кольцо с главным максимальным идеалом $J = \langle \varepsilon \rangle$, причем $1 + J \subset R^{*2}$, $|R^* : R^{*2}| = 2$ и $1 + R^{*2} \subset R^{*2}$. Тогда всякая ненулевая квадратичная форма над R приводится обратимым R -линейным преобразованием неизвестных к диагональному виду (2.3), в котором показатели $i_1, \dots, i_q$ и целые числа $r_1, \dots, r_q$, $s_1, \dots, s_q$ не зависят от способа приведения.

Для ненулевой симметричной $n \times n$ -матрицы A над R уравнение $v(\lambda A)v^T = 0$ при всех $\lambda \in R^*$, очевидно, определяет одну и ту же квадрику. Если одна квадрика получается из другой проективным линейным преобразованием $v \mapsto vU$ ($v \in RP_{n-1}$) для $U \in PGL_n(R)$ (аналогично, проективностью), то квадрики называем проективно конгруэнтными (соответственно, проективно эквивалентными).

Следующая теорема устанавливает число $N(n, s)$ классов проективно конгруэнтных квадрик пространства RP_{n-1} в условиях теорем 2 и 3. Пусть $\Omega_q(m)$ — совокупность всех упорядоченных наборов $(n_1, \dots, n_q)$ целых чисел $n_j > 0$ с суммой m . Число $\binom{p}{q}'$ считаем равным $\binom{p}{q}$ для целых чисел $p \geq q \geq 0$ и равным 0 в других случаях.

Теорема 4. Пусть R — локальное кольцо с нильпотентным ступени s главным максимальным идеалом, $2 \in R^*$ и $|R^* : R^{*2}| = 2$. Тогда соответственно случаям $1 + R^{*2} \subset R^{*2}$ и $R^* \cap (1 + R^2) \not\subset R^{*2}$ число $N(n, s)$ классов проективно конгруэнтных квадрик пространства RP_{n-1} равно $([\dots])$ — целая часть числа

$$N(n, s) = \sum_{m=1}^n \sum_{q=1}^{\min\{m, s\}} \binom{s}{q} \left\{ \binom{m/2-1}{q-1}' + \sum_{(n_1, \dots, n_q) \in \Omega_q(m)} \left[\frac{1}{2} \prod_{j=1}^q (n_j + 1) \right] \right\}, \quad (2.4)$$

$$N(n, s) = \sum_{m=1}^n \sum_{q=1}^{\min\{m, s\}} \binom{s}{q} 2^{q-1} \left\{ \binom{m/2-1}{q-1}' + \binom{m-1}{q-1} \right\}. \quad (2.5)$$

§ 3. Отметим, что матрица (2.1) представляется в виде

$$\Phi = \text{diag}(\varepsilon^{t_1} A_1, \varepsilon^{t_2} A_2, \dots, \varepsilon^{t_q} A_q, O), \quad 0 \leq t_1 < t_2 < \dots < t_q, \quad \varepsilon^{t_q} \neq 0, \quad (2.6)$$

с обратимыми диагональными клетками $A_1, \dots, A_q$, сумма размерностей которых и размерности нулевой клетки O равна n .

По основной теореме проективной геометрии [8] всякая проективность есть произведение проективного линейного преобразования пространства RP_{n-1} и его кольцевого автоморфизма, индуцированного автоморфизмом основного кольца. Легко видеть, что в условиях теорем 3 и 4 и неавтоморфных элементов ε и $k\varepsilon$ кольца R число классов проективно эквивалентных квадрик совпадает с числом $N(n, s)$. Следующая теорема указывает число классов проективно эквивалентных квадрик для проективной плоскости в оставшемся случае, когда элементы ε и $k\varepsilon$ автоморфны.

Теорема 5. *Если максимальный идеал $J = \langle \varepsilon \rangle$ локального кольца R нильпотентен степени s , $|R^* : R^{*2}| = 2$ и элементы ε и $k\varepsilon$ для неквадрата k в кольце R автоморфны, то число N классов проективно эквивалентных квадрик проективной плоскости RP_2 , в соответствии с тем, четно или нечетно число s , равно*

$$N = (s(5s^2 + 15s + 28))/12 \quad \text{или} \quad N = (5s^3 + 15s^2 + 31s - 3)/12,$$

при $R^* \cap (1 + R^2) \not\subseteq R^{*2}$, а при $1 + R^{*2} \subset R^{*2}$ —

$$N = (s(5s^2 + 21s + 28))/12 \quad \text{или} \quad N = (5s^3 + 21s^2 + 31s + 3)/12.$$

Доказательство. В соответствии с теоремой 1 классы проективно эквивалентных квадрик можно представлять матрицами $D = \text{diag}(k_1\varepsilon^{t_1}, k_2\varepsilon^{t_2}, k_3\varepsilon^{t_3})$, где $0 \leq t_1 \leq t_2 \leq t_3 \leq s$, $t_1 < s$ и $k_i \in \{1, k\}$ для обратимого неквадрата k , фиксированного как и в теореме. Ясно, что матрицы D и kD представляют один класс квадрик и поэтому, например, при $\varepsilon^{t_3} \neq 0$ можем полагать $k_3 = 1$.

Допустим, что $t_1 = t_2 = t_3 = m$. В силу теорем 2, 3 и предыдущего замечания, при любом m , $0 \leq m < s$, класс квадрик представляется одной из матриц

$$D_1 = \varepsilon^m \text{diag}(1, 1, 1), \quad D_2 = \varepsilon^m \text{diag}(k, 1, 1), \quad D_3 = \varepsilon^m \text{diag}(k, k, 1).$$

Замечаем, что классы квадрик с матрицами D_3 и kD_3 совпадают, а матрицы D_2 и kD_3 конгруэнтны. Если $R^* \cap (1 + R^2) \not\subseteq R^{*2}$, то по лемме 3 матрицы D_2 и kD_1 конгруэнтны и, в силу произвола в выборе m , получаем всего s классов. С другой стороны, при $1 + R^{*2} \subset R^{*2}$ классы квадрик с матрицами D_1 и D_2 не совпадают и поэтому получаем $2s$ классов квадрик.

Найдем число классов квадрик с $t_3 = s$. Случай $0 \leq t_1 < t_2 = t_3 = s$ дает в точности s классов. В остальных случаях каждый класс представляется матрицей $\text{diag}(k_1\varepsilon^{t_1}, \varepsilon^{t_2}, 0)$, $0 \leq t_1 \leq t_2 < s$. При $t_1 = t_2$ получаем $2s$ различных классов. Если t_1, t_2 — одной четности и различны, то получаем $2C_{[s+1/2]}^2$ или $2C_{[s/2]}^2$ классов, в соответствии с тем, четны или нечетны числа t_1, t_2 ; здесь $[\dots]$

— целая часть числа. В случае, когда числа t_1, t_2 имеют различную четность, легко убедиться, что квадратики с матрицами $\text{diag}(k\varepsilon^{t_1}, \varepsilon^{t_2}, 0)$ и $\text{diag}(\varepsilon^{t_1}, \varepsilon^{t_2}, 0)$ автоморфны и поэтому число классов здесь равно произведению $C_{[s+1/2]}^1 C_{[s/2]}^1$.

Пусть $t_3 < s$. Допустим, что среди чисел t_1, t_2, t_3 есть как четные, так и нечетные. Зафиксируем четный показатель t_i и нечетный показатель t_j . Как и выше, можем полагать $k_i = 1$. С помощью кольцевого автоморфизма добиваемся также равенства $k_j = 1$, не изменяя коэффициента k_i , в силу четности t_i . Тогда различные значения оставшегося третьего коэффициента, независимо от третьего показателя в D , приводят к различным классам проективно эквивалентных квадратов. Таким образом, получаем $2C_{[s+1/2]}^2 C_{[s/2]}^1 + 2C_{[s+1/2]}^1 C_{[s/2]}^2$ классов, когда все три показателя различны, и $2C_{[s+1/2]}^1 C_{[s/2]}^1$ классов в каждом из случаев $t_1 = t_2 < t_3$ и $t_1 < t_2 = t_3$.

В случае, когда числа t_1, t_2, t_3 — одной четности и различны, то в соответствии с тем, четны они или нечетны, получаем $4C_{[s+1/2]}^3$ или $4C_{[s/2]}^3$ классов. Рассмотрим оставшийся случай, когда числа t_1, t_3 — одной четности и различны, а число t_2 совпадает с одним из них. Допустим вначале, что $t_1 = t_2$. Тогда каждый класс квадратиков представляется матрицей $\text{diag}(\varepsilon^{t_1} D_i, \varepsilon^{t_3})$, где $D_1 = \text{diag}(1, 1)$, $D_2 = \text{diag}(k, 1)$, $D_3 = \text{diag}(k, k)$. Для фиксированных t_1, t_3 все три возможности очевидно приводят к различным классам при $1 + R^{*2} \subset R^{*2}$ и всего получаем $3M$ классов, где $M = C_{[s+1/2]}^2 + C_{[s/2]}^2$; при $R^* \cap (1 + R^2) \not\subset R^{*2}$ должны иметь $2M$ классов, так как матрицы D_1 и D_3 конгруэнтны. Резюмируя, получаем утверждение теоремы.

ЛИТЕРАТУРА

1. Артин Э. Геометрическая алгебра. М.: Наука. 1969. 284 с.
2. Benz W. Vorlesungen über Geometrie der Algebren. Berlin – Heidelberg – New York. Springer – Verlag. 1973. 365 p.
3. Brown W. Matrices over commutative rings. New York. 1993. 282 p.
4. Вишневский В.В., Широков А.П., Шурыгин В.В. Пространства над алгебрами. Казань: Изд. Казанского университета. 1985. 263 с.
5. Касселс Дж. Рациональные квадратичные формы. М: Мир, 1982. 440 с.
6. Мерзляков Ю.И. Рациональные группы. М: Наука. 1980. 464 с.
7. Милнор Дж., Хьюзмоллер Д. Симметрические билинейные формы. М: Наука. 1986. 176 с.
8. Ojanguren M., Sridharan R. // Comm. Math. Helv. 1969. 44. no. 3. p. 310 - 315.

9. Старикова О.А. // Материалы VIII науч. конф. асп. и молодых исследователей СМУ. Магадан: Сев. Межд. Ун-т. 2001. с. 16-18.
10. Старикова О.А. // Сборник статей "II Всесибирский конгресс женщин-математиков". Красноярск: КГУ. 2002. с. 138-144.
11. Старикова О.А. // В сб. Международ. конф. "Алгебра и ее приложения". Красноярск: КГУ. 2002. с. 113-114.
12. Холл М. Комбинаторика. М: Мир. 1970. 424 с.

ВНУТРЕННЯЯ Σ -ОПРЕДЕЛИМОСТЬ В НАСЛЕДСТВЕННО КОНЕЧНЫХ НАДСТРОЙКАХ

А.И. Стукачев*

Институт математики СО РАН
Новосибирск, Россия
e-mail: aistu@math.nsc.ru

1 Об универсальной Σ -функции

В данной главе рассматривается следующая задача: найти теоретико-модельные условия существования универсальной Σ -функции в наследственно конечной надстройке над моделью. В.А. Руднев в [4] показал, что в наследственно конечных надстройках над моделями s -простых теорий существует универсальная Σ -функция. Впоследствии Ю.Л. Ершов в [1], используя понятие квазирезольвентности, установил, что универсальная Σ -функция существует в наследственно конечных надстройках над моделями регулярных теорий.

В данной работе приводится еще одно достаточное условие существования универсальной Σ -функции в $HF(\mathfrak{M})$, которое определяется в терминах 1-разрешимости. Данное условие с точки зрения обобщенной вычислимости над моделями представляется более естественным, чем условие, сформулированное в терминах квазирезольвентности наследственно конечной надстройки. Кроме того, класс моделей, удовлетворяющих данному условию, также содержит все модели регулярных теорий. Для моделей ω -категоричных и разрешимых теорий найдено необходимое и достаточное условие существования универсальной Σ -функции.

Все рассматриваемые в дальнейшем модели имеют вычислимую сигнатуру, с которой связывается некоторая вычислимая геделевская нумерация формул этой сигнатуры. Для формулы φ через $[\varphi]$ обозначается ее геделевский номер.

*Работа выполнена при финансовой поддержке РФФИ, проект N02-0100540, Совета по грантам Президента РФ и государственной поддержке ведущих научных школ, проект НШ-2069.2003.1, программы "Университеты России", проект УР.04.01.019.

Определение 1. Модель $\mathfrak{M}$ сигнатуры σ называется **разрешимой в $HF(\mathfrak{M})$** , если множество

$$\{\langle \bar{m}, [\varphi] \rangle \mid \bar{m} \in M^{<\omega}, \varphi(\bar{x}) - \text{формула сигнатуры } \sigma, \mathfrak{M} \models \varphi(\bar{m})\}$$

является Σ -подмножеством в $HF(\mathfrak{M})$.

Данное понятие допускает эквивалентное определение в терминах Σ -определимости алгебраических систем [1]: модель $\mathfrak{M}$ является разрешимой в $HF(\mathfrak{M})$ тогда и только тогда, когда морлиевское обогащение модели $\mathfrak{M}$ Σ -определимо в $HF(\mathfrak{M})$. Отметим, что для модели $\mathfrak{M}$ регулярной теории в $HF(\mathfrak{M})$ справедлива теорема о равномерной униформизации тогда и только тогда, когда некоторое скулемовское обогащение модели $\mathfrak{M}$ Σ -определимо в $HF(\mathfrak{M})$ (см. [5]).

Рассмотрим более слабую версию этого понятия, с помощью которого и формулируем достаточное условие существования универсальной Σ -функции.

Определение 2. Модель $\mathfrak{M}$ сигнатуры σ называется **n -разрешимой в $HF(\mathfrak{M})$** ($n > 0$), если множество

$$\begin{aligned} \{\langle \bar{m}, [\varphi] \rangle \mid \bar{m} \in M^{<\omega}, \varphi(\bar{x}) - \text{формула сигнатуры } \sigma \\ \text{с меньшим, чем } n, \text{ числом перемен кванторов} \\ \text{в пренексной нормальной форме, } \mathfrak{M} \models \varphi(\bar{m})\} \end{aligned}$$

является Σ -подмножеством в $HF(\mathfrak{M})$.

Очевидно, что $\mathfrak{M}$ разрешима в $HF(\mathfrak{M})$ тогда и только тогда, когда $\mathfrak{M}$ n -разрешима в $HF(\mathfrak{M})$ для всех $n > 0$ (если под 0-разрешимостью понимать равномерную Σ -определимость истинности бескванторных формул, то, очевидно, всякая модель будет 0-разрешимой в HF -надстройке). Очевидным также является следующее утверждение (напомним, что теория называется регулярной [1], если она модельно полна и разрешима):

Предложение 1. Если $Th(\mathfrak{M})$ регулярна, то $\mathfrak{M}$ является разрешимой в $HF(\mathfrak{M})$.

Поэтому, в частности, всякая модель регулярной теории является 1-разрешимой в наследственно конечной надстройке. Покажем, что условие 1-разрешимости является достаточным для существования в наследственно конечной надстройке универсальной Σ -функции. В случае 1-разрешимых моделей в предыдущем определении вместо произвольных формулы без перемен кванторов в пренексной нормальной форме можно ограничиться только $\forall$ -формулами. Действительно, вследствие существования универсального Σ -предиката в допустимых множествах, для всякой модели проверка истинности $\exists$ -формул тривиально определяется Σ -предикатом в наследственно конечной надстройке.

Теорема 1. Если $\mathfrak{M}$ является 1-разрешимой в $HF(\mathfrak{M})$, то в $HF(\mathfrak{M})$ существует универсальная Σ -функция.

Доказательство. Пусть $\mathfrak{M}$ — модель сигнатуры σ . Рассмотрим произвольную Σ -функцию $f : HF(\mathfrak{M}) \rightarrow HF(\mathfrak{M})$. Для нее существует функция $h : HF(\omega) \rightarrow HF(\omega)$, такая, что, в обозначениях [1], для любых $\varkappa \in HF(\omega)$ и $\bar{m} \in M^{<\omega}$

$$f(t_{\varkappa}(\bar{m})) = t_{h(\varkappa)}(g_{\varkappa}(\bar{m})),$$

причем h — A -вычислимая функция для некоторого A вида $Th_{\exists}(\mathfrak{M}, \bar{m})$, $\bar{m} \in M^{<\omega}$, а $g_{\varkappa} : M^{<\omega} \rightarrow M^{<\omega}$ — Σ -определимая в $HF(\mathfrak{M})$ частичная функция. Вследствие этого, существование универсальной Σ -функции в $HF(\mathfrak{M})$ эквивалентно существованию в $HF(\mathfrak{M})$ вычислимой нумерации Σ -функций вида $g : M^{<\omega} \rightarrow M^{<\omega}$.

Пусть $g : M^{<\omega} \rightarrow M^{<\omega}$ — Σ -функция в $HF(\mathfrak{M})$. Тогда существует вычислимая последовательность

$$\Phi = \{\varphi_n(\bar{x}_n, \bar{y}_n, \bar{z}) \mid n \in \omega\}$$

$\exists$ -формулы сигнатуры σ такая, что для некоторого $\bar{m}_0 \in M^{<\omega}$

$$g = \{\langle \bar{m}, \bar{m}' \rangle \mid \bar{m}, \bar{m}' \in M^{<\omega}, \exists n \in \omega \mathfrak{M} \models \varphi_n(\bar{m}, \bar{m}', \bar{m}_0)\}.$$

Здесь и всюду далее считается, что для формул вычислимой последовательности, определяющей функцию такого вида, существует эффективная процедура "сотировки" переменных: набор переменных $\bar{x}_n$ соответствует аргументу, а набор переменных $\bar{y}_n$ — значению функции.

Назовем $\exists$ -формулу $\varphi(\bar{x}, \bar{y}, \bar{z})$ сигнатуры σ *функциональной для набора* $\bar{m}_0 \in M^{<\omega}$, если $\mathfrak{M} \models \forall \bar{x} \exists^{\leq 1} \bar{y} \varphi(\bar{x}, \bar{y}, \bar{m}_0)$. Аналогично, (вычислимую) последовательность $\exists$ -формул $\{\varphi_n(\bar{x}_n, \bar{y}_n, \bar{z}) \mid n \in \omega\}$ сигнатуры σ назовем *функциональной для набора* $\bar{m}_0 \in M^{<\omega}$, если

$$\mathfrak{M} \models \forall \bar{x} \exists^{\leq 1} \bar{y} \bigvee_{n \in \omega} \varphi_n(\bar{x}_n, \bar{y}_n, \bar{m}_0).$$

Из определения очевидно, что элементами функциональной последовательности являются функциональные формулы. Отметим, что условие функциональности для $\exists$ -формулы записывается $\forall$ -формулой. Действительно, если $\varphi(\bar{x}, \bar{y}, \bar{z})$ — $\exists$ -формула, то формула

$$\forall \bar{x} \forall \bar{y} \forall \bar{y}' (\varphi(\bar{x}, \bar{y}, \bar{z}) \wedge \varphi(\bar{x}, \bar{y}', \bar{z}) \rightarrow \bar{y} = \bar{y}'),$$

очевидно, является $\forall$ -формулой. Аналогично, условие функциональности для (вычисляемых) последовательностей $\exists$ -формул записывается (вычислимой) бесконечной Π_1 -формулой.

Существенным является следующее замечание: если $\mathfrak{M}$ — 1-разрешимая в $HF(\mathfrak{M})$ модель, то в $HF(\mathfrak{M})$ существует вычислимая нумерация всех вычислимых последовательностей функциональных $\exists$ -формул. Действительно, для каждого $\bar{m}_0 \in M^{<\omega}$ эффективно определяется Σ -функция $f : \omega \rightarrow \omega$, такая, что, с оракулом $A = Th_{\forall}(\mathfrak{M}, \bar{m}_0)$, $\{W_{f(n)}^A | n \in \omega\}$ — искомая нумерация вычислимых последовательностей (геделевских номеров) функциональных $\exists$ -формул для $\bar{m}_0$. Здесь $\{W_n | n \in \omega\}$ — универсальная нумерация всех вычислимо перечислимых множеств натуральных чисел, а значение $f(n)$ определяется для каждого $n \in \omega$ из условия: $k \in W_{f(n)}^A$ тогда и только тогда, когда $k \in W_n$, k — геделевский номер $\exists$ -формулы $\varphi(\bar{x}, \bar{y}, \bar{z})$ сигнатуры σ , и формула $\forall \bar{x} \exists^{\leq 1} \bar{y} \varphi(\bar{x}, \bar{y}, \bar{m}_0)$ выполняется в модели $\mathfrak{M}$, то есть принадлежит теории $Th_{\forall}(\mathfrak{M}, \bar{m}_0)$.

Наконец, по нумерации всех вычислимых последовательностей функциональных $\exists$ -формул эффективно (в случае 1-разрешимых моделей) находится нумерация всех Σ -функций из $M^{<\omega}$ в $^{<\omega}$. Действительно, если $\bar{m}_0 \in M^{<\omega}$ и $n_0 \in \omega$, то по вычислимой последовательности $W_{f(n_0)}^A = \{[\varphi_k(\bar{x}_k, \bar{y}_k, \bar{z})] | k \in \omega\}$, $A = Th_{\forall}(\mathfrak{M}, \bar{m}_0)$, определим Σ -функцию $g : M^{<\omega} \rightarrow M^{<\omega}$ так: $g(\bar{m}_1) = \bar{m}_2$ тогда и только тогда, когда $\exists k_0((\mathfrak{M} \models \varphi_{k_0}(\bar{m}_1, \bar{m}_2, \bar{m}_0)) \wedge \forall k \leq k_0(\mathfrak{M} \models \forall \bar{y} \neg \varphi_k(\bar{m}_1, \bar{y}, \bar{m}_0)))$ (последняя формула является $\forall$ -формулой). $\square$

На самом деле, по аналогии с условием предыдущей теоремы можно сформулировать условие, которое будет уже необходимым и достаточным для существования универсальной Σ -функции в наследственно конечной надстройке. А именно, для произвольной модели $\mathfrak{M}$ сигнатуры σ семейство $\mathcal{F}$ функциональных последовательностей назовем *базисным*, если для всякой функциональной последовательности $\Phi(\bar{m})$ существует функциональная последовательность $\Psi(\bar{m}')$ из $\mathcal{F}$, такая, что

$$HF(\mathfrak{M}) \models \forall \bar{x} \forall \bar{y} \left(\bigvee_{\varphi \in \Phi(\bar{x}, \bar{y}, \bar{m})} \varphi(\bar{x}, \bar{y}, \bar{m}) \leftrightarrow \bigvee_{\psi \in \Psi(\bar{x}, \bar{y}, \bar{m}')} \psi(\bar{x}, \bar{y}, \bar{m}') \right).$$

Теорема 2. Пусть $\mathfrak{M}$ — модель сигнатуры σ . В наследственно конечной надстройке $HF(\mathfrak{M})$ существует универсальная Σ -функция тогда и только тогда, когда в $HF(\mathfrak{M})$ существует вычислимая нумерация некоторого семейства базисных функциональных последовательностей.

Доказательство этого утверждения аналогично доказательству предыдущей теоремы. Проверка условия этого критерия представляется довольно трудной задачей, поэтому он едва ли может иметь большую практическую ценность. Однако полезным следствием данной теоремы является критерий существования универсальной Σ -функции в надстройках над моделями ω -категоричных и разрешимых теорий. А именно, под $\forall \exists^{\leq 1} \exists$ -теорией модели $\mathfrak{M}$ сигнатуры σ (обозначение $Th_{\forall \exists^{\leq 1} \exists}(\mathfrak{M})$) будем понимать множество истинных в $\mathfrak{M}$ предложений вида

$$\forall \bar{x} \exists^{\leq 1} \bar{y} \varphi(\bar{x}, \bar{y}),$$

где $\varphi(\bar{x}, \bar{y})$ — $\exists$ -формула сигнатуры σ . Очевидно, что всякая $\forall\exists^{\leq 1}$ -формула эквивалентна $\forall$ -формуле, поэтому можно считать, что $Th_{\forall\exists^{\leq 1}\exists}(\mathfrak{M}) \subseteq Th_{\forall}(\mathfrak{M})$.

Теорема 3. Пусть модель $\mathfrak{M}$ такова, что $Th(\mathfrak{M})$ ω -категорична и разрешима. Тогда в $HF(\mathfrak{M})$ существует универсальная Σ -функция в том и только том случае, когда множество

$$\{\langle \bar{m}, [\varphi] \rangle \mid \bar{m} \in M^{<\omega}, \varphi \in Th_{\forall\exists^{\leq 1}\exists}(\mathfrak{M}, \bar{m})\}$$

является Σ -подмножеством в $HF(\mathfrak{M})$.

Доказательство. Действительно, вследствие ω -категоричности всякая бесконечная формула эквивалентна конечной, поэтому базисным множеством функциональных последовательностей будет множество всех (вследствие разрешимости) функциональных $\exists$ -формул. $\square$

Следствие 1. Пусть $\mathfrak{M}$ — модель ω -категоричной и разрешимой теории. Пусть в $HF(\mathfrak{M})$ существует универсальная Σ -функция, и пусть $\bar{m}_0 \in M^{<\omega}$ — набор праэлементов, входящих в параметры определения этой функции. Тогда для любых наборов $\bar{m}_1, \bar{m}_2 \in M^{<\omega}$ из включения

$$Th_{\exists}(\mathfrak{M}, \bar{m}_0, \bar{m}_1) \subseteq Th_{\exists}(\mathfrak{M}, \bar{m}_0, \bar{m}_2)$$

следует включение

$$Th_{\forall\exists^{\leq 1}\exists}(\mathfrak{M}, \bar{m}_0, \bar{m}_1) \subseteq Th_{\forall\exists^{\leq 1}\exists}(\mathfrak{M}, \bar{m}_0, \bar{m}_2).$$

Используя необходимое условие из этого следствия, легко убедиться, что в наследственно конечной надстройке над моделью, построенной В.А.Рудневым в [4], не существует универсальной Σ -функции. Действительно, предположим, что это не так. Любые два элемента из этой модели либо имеют одинаковую $\exists$ -теорию, либо $\exists$ -теория одного элемента является собственным подмножеством $\exists$ -теории другого. Однако в этом случае соответствующее вложение для $\exists^{\leq 1}$ -теорий этих элементов, как легко убедиться, места не имеет.

2 Внутренняя определимость наследственно конечных надстроек и кардинальные нумерации

Пусть $\mathbb{A}$ — допустимое множество, $B \subseteq A$ — Σ -подмножество. Назовем допустимое множество $\mathbb{A}$ **конструктивизируемым внутри B** , если существуют Σ -формулы $\Phi(x_0, y)$, $\Phi_=(x_0, x_1, y)$, $\Psi_=(x_0, x_1, y)$, $\Phi_{\in}(x_0, x_1, y)$, $\Psi_{\in}(x_0, x_1, y)$,

$\Phi_U(x_0, y)$, $\Psi_U(x_0, y)$ и параметр $b \in B$ такие, что $\Phi(x, b)^{\mathbb{A}} \subseteq B$ и система релятивизованных формул $\langle \Phi^B, (\Phi_{=})^B, (\Psi_{=})^B, (\Phi_{\in})^B, (\Psi_{\in})^B, (\Phi_U)^B, (\Psi_U)^B \rangle$ с параметром a определяют допустимое множество $\mathbb{A}$ в $\mathbb{A}$.

Пусть $rank(B) = \sup\{rank(b) | b \in B\}$. Для допустимого множества $\mathbb{A}$ рассмотрим ординал

$$dr(\mathbb{A}) = \inf\{rank(B) | \mathbb{A} \text{ конструктивизируемо внутри } B\}.$$

Теорема 4. Пусть $\mathfrak{M}$ — модель вычислимой сигнатуры. Тогда

- 1) если $\mathfrak{M}$ конечна, то $dr(HF(\mathfrak{M})) = \omega$,
- 2) если $\mathfrak{M}$ бесконечна, то $dr(HF(\mathfrak{M})) \leq 2$.

Пусть, как обычно, $HF_n(\mathfrak{M})$ — множество элементов из $HF(\mathfrak{M})$ ранга не больше n . Очевидно, что если $\mathfrak{M}$ конечна, то $HF(\mathfrak{M})$ не является конструктивизируемым внутри $HF_n(\mathfrak{M})$ для любого $n \in \omega$, откуда следует справедливость пункта 1. Справедливость пункта 2 вытекает из следующего замечания: имеет место

Теорема 5. Если $\mathfrak{M}$ бесконечна, то наследственно конечная надстройка $HF(\mathfrak{M})$ является конструктивизируемой внутри $HF_2(\mathfrak{M})$.

Доказательство. Построим $HF_2(\mathfrak{M})$ -конструктивизацию ν стандартной модели арифметики $\langle \omega, \leq, +, \cdot, s, 0, 1 \rangle$. Воспользуемся для этого кардинальным представлением натуральных чисел в модели $\mathfrak{M}$: каждому $n \in \omega$ сопоставим семейство всех множеств из n элементов:

$$M_n \Leftarrow \{a \subseteq M \mid |a| = n\}.$$

Два множества лежат в одном семействе (то есть представляют одно и то же натуральное число), если существует биекция из одного множества на другое. Заметим, что для представления функций на $\mathfrak{M}$ с конечной областью определения в $HF(\mathfrak{M})$ достаточно элементов ранга 2. Действительно, всякая функция вида $f = \{\langle u_1, v_1 \rangle, \dots, \langle u_n, v_n \rangle\}$ однозначно определяется элементом

$$a_f = \{\{u_1, v_1\}, \dots, \{u_n, v_n\}, u_1, \dots, u_n\}$$

ранга 2. Вследствие этого нумерационная эквивалентность для кардинальной нумерации ν является Σ -определимой в $HF_2(\mathfrak{M})$:

$$\nu(a) = \nu(b) \iff HF_2(\mathfrak{M}) \models \exists f (Fun(f) \wedge Dom(f) = a \wedge Ran(f) = b).$$

Аналогично, для отношения порядка $\leq$ имеем

$$\nu(a) \leq \nu(b) \iff HF_2(\mathfrak{M}) \models \exists a' ((\nu(a') = \nu(a)) \wedge (a' \subseteq b)),$$

$$\nu(a) < \nu(b) \iff HF_2(\mathfrak{M}) \models \exists a' \exists b' ((\nu(a') = \nu(a)) \wedge (a' \subseteq b) \wedge (b' \subseteq b) \wedge (b = a' \cup b') \wedge (b' \neq \emptyset)),$$

откуда, так как $\nu(a) \neq \nu(b) \iff ((\nu(a) < \nu(b)) \vee (\nu(b) < \nu(a)))$, получаем, что нумерационная эквивалентность и отношение порядка являются Δ -определимыми в $HF_2(\mathfrak{M})$.

Для операций сложения и умножения имеем

$$\nu(a) + \nu(b) = \nu(c) \iff HF_2(\mathfrak{M}) \models \exists a' \exists b' ((\nu(a') = \nu(a)) \wedge (\nu(b') = \nu(b)) \wedge (a' \subseteq c) \wedge (b' \subseteq c) \wedge (c = a' \cup b')),$$

$$\nu(a) \cdot \nu(b) = \nu(c) \iff HF_2(\mathfrak{M}) \models \exists c' ((\cap c' = c) \wedge ("c' = \{a'_1, \dots, a'_{\nu(b)}\}" \wedge ("a'_i \cap a'_j = \emptyset \text{ при } i \neq j") \wedge (" \nu(a'_i) = \nu(a) \text{ для всех } i"))),$$

где, например, запись $"c' = \{a'_1, \dots, a'_{\nu(b)}\}"$ есть сокращение для формулы

$$\exists c'' ((\nu(c'') = \nu(b)) \wedge \forall a' \in c' \exists! x \in a' (x \in c'')).$$

Таким образом, операции сложения и умножения $HF_2(\mathfrak{M})$ -конструктивизируемы с помощью кардинальной нумерации ν .

По данной $HF_2(\mathfrak{M})$ -конструктивизации системы $\langle \omega, \leq, +, \cdot, s, 0, 1 \rangle$ и произвольной конструктивизации $\gamma : \omega \rightarrow HF(\omega)$ построим $HF_2(\mathfrak{M})$ -конструктивизацию ν_* для $HF(\mathfrak{M})$ следующим образом: для всякого $a \in HF(\mathfrak{M})$, такого, что $a = t_{\mathfrak{x}}(m_1, \dots, m_k)$ положим $\nu_*^{-1}(a)$ равным множеству всех элементов вида

$$\{a_{\mathfrak{x}}, \{m_1, u_1\}, \dots, \{m_k, u_1, \dots, u_k\}, u_1, \dots, u_k\},$$

где множество $a_{\mathfrak{x}} \subseteq M$ таково, что $\nu(a_{\mathfrak{x}}) = \gamma^{-1}(\mathfrak{x})$, а элементы $u_1, \dots, u_k$ из M различны и удовлетворяют условиям $\{u_1, \dots, u_k\} \cap \{m_1, \dots, m_k\} = \{u_1, \dots, u_k\} \cap a_{\mathfrak{x}} = \{m_1, \dots, m_k\} \cap a_{\mathfrak{x}} = \emptyset$.

Построенная таким образом $HF_2(\mathfrak{M})$ -конструктивизация ν_* , является, очевидно, конструктивизацией $HF(\mathfrak{M})$ внутри $HF_2(\mathfrak{M})$. $\square$

Из теоремы 5, в частности, следуют некоторые результаты из [6] об определимости в многосортных языках, в которых переменные могут принимать значения только определенного типа.

В [3] рассматривалось понятие приемлемой (acceptable) структуры. Имеет место следующее

Предложение 2. $dr(HF(\mathfrak{M})) = 0$ тогда и только тогда, когда $\mathfrak{M}$ — приемлемая (acceptable) структура.

Список литературы

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

- [2] *Ю.Л. Ершов*, Проблемы разрешимости и конструктивные модели, М., Наука, 1980.
- [3] *J. Barwise*, Admissible sets and structures, Berlin, 1975.
- [4] *В.А. Руднев*, Об универсальной рекурсивной функции на допустимых множествах, Алгебра и логика, **25**, N 4 (1986), 425 – 435.
- [5] *А.И. Стукачев*, Теорема об униформизации в наследственно конечных надстройках, в сб. "Обобщенная определимость и вычислимость", (Вычислительные системы, 161), Новосибирск, Ин-т Математики СО РАН, 1998, 3 – 14.
- [6] *R. Montague*, Recursion theory as a branch of model theory, Proceedings of the Third International Congress for Logic, Methodology and Philosophy of Science, Amsterdam, 1967, 63 – 86.

FUZZY POLYGONOMETRIES

S. Sudoplatov*

Novosibirsk State Technical University,
K.Marksa 20, Novosibirsk, 630092, Russia
e-mail: sudoplat@ngs.ru

The notion of polygonometry has a long history. It is a natural generalization of the notion of trigonometry when ratios of parameters in polygons are considered instead of ratios of parameters in triangles. Thus the class of polygonometries includes both the classical trigonometry on the Euclidian plane and the spherical trigonometry [1].

Polygonometries were investigated by A. I. Lexell [2], [3], N. I. Fuss [4], T. Banachiewicz and others. Both triangulation method and polygonometrical method play an important role in astronomy and geodesy [5]. From the other hand polygonometries can be considered as algebraic and combinatorial objects [6], [7], [8]. As shown in [9], [10], [11] polygonometries are useful for realizations of many structural properties of *Ehrenfeucht theories* (i.e. complete first order theories having a finite (> 1) number of pairwise non-isomorphic countable models).

The author introduced the notion of generalized polygonometry in [12]. At present article we propose a fuzzy interpretations of generalized polygonometries.

We shall use the terminology of [6]. Remember the notions from [12] of side-angle matrices and of generalized polygonometry.

Let G_1 and G_2 be some groups. By *side-angle matrix* or *SA-matrix* (over the pair (G_1, G_2)) we mean any matrix $\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}$, where $a_i \in G_1 \cup \{\infty\}$, $\alpha_i \in G_2 \cup \{\infty\}$, $i = 1, \dots, n$, $n \geq 3$. The set $\mathbf{S}$ of some SA-matrices is said to be *closed*, if the following conditions are satisfied:

- 1) $\Delta_e(G_1, G_2) \subseteq \mathbf{S}$ (see [6]);
- 2) if some element of first row of a matrix from $\mathbf{S}$ is equal to ∞ , then $\mathbf{S}$ contains $\begin{pmatrix} \infty & \infty & \infty \\ e & e & e \end{pmatrix}$ and all matrices of form $\begin{pmatrix} \infty & g_1 & \infty \\ e & e & e \end{pmatrix}$, $g_1 \in G_1$;
- 3) if some element of second row of a matrix from $\mathbf{S}$ is equal to ∞ , then $\mathbf{S}$ contains $\begin{pmatrix} e & e & e \\ \infty & \infty & \infty \end{pmatrix}$ and all matrices of form $\begin{pmatrix} e & e & e \\ \infty & g_2 & \infty \end{pmatrix}$, $g_2 \in G_2$;
- 4) for any $S \in \mathbf{S}$ the set $\mathbf{S}$ contains cyclic permutations and turns of S , and it is closed under joinings of matrices where values of $\alpha \cdot \infty$ and $\infty \cdot \alpha$ are equal to ∞ , $\infty^{-1} = \infty$ and values of $\infty \cdot \infty$ can be arbitrary from $G_1 \cup G_2 \cup \{\infty\}$.

*The author was supported in part by the Russian Foundation for Basic Researches (the code of project 02-01-00258).

By a *generalized polygonometry* $\text{gpm}(G_1, G_2, \mathcal{P})$ of group pair (G_1, G_2) on a system $\mathcal{P} = \langle P, L, \in \rangle$ containing the *set of points* P and the *set of lines* L (where any line is a subset of P) we mean an algebraic system

$$\mathcal{M} = \langle P, \langle Q_{g_1}^{(2)} \mid g_1 \in G_1 \rangle, \langle R_{g_2}^{(3)} \mid g_2 \in G_2 \rangle \rangle,$$

containing nonempty relations Q_{g_1} , $g_1 \in G_1$, and R_{g_2} , $g_2 \in G_2$, and satisfying the following conditions:

- a) $\mathcal{M} \models \forall x R_e(x, x, x)$ and $(\mathcal{M} \models R_e(a, b, c) \Leftrightarrow \text{elements } a, b \text{ and } c \text{ are collinear})$;
- b) if $\mathcal{M} \models Q_{g_1}(a, b)$, then elements a and b belong to a common line;
- c) if $\mathcal{M} \models R_{g_2}(a, b, c)$, then there is a line l_1 , containing elements a and b , and there is a line l_2 , containing elements b and c ;
- d) $\mathcal{M} \models (R_e(a, b, c) \wedge Q_{g_1}(a, b) \wedge Q_{g'_1}(b, c)) \rightarrow (Q_{g_1 \cdot g'_1}(a, c) \wedge Q_{g_1^{-1}}(b, a))$;
- e) $\mathcal{M} \models (R_{g_2}(a, b, c) \wedge R_{g'_2}(c, b, d)) \rightarrow (R_{g_2 \cdot g'_2}(a, b, d) \wedge R_{g_2^{-1}}(c, b, a))$;
- f) if p_1 and p_2 are points belonging to lines l_1 and l_2 accordingly, then there exists an automorphism $f \in \text{Aut } \mathcal{M}$ such that $f(p_1) = p_2$ and $f(l_1) = l_2$.

Let $S = (p_1, p_2, \dots, p_n)$ be a *polygon* of generalized polygonometry $\text{gpm} = \text{gpm}(G_1, G_2, \mathcal{P})$, i.e. a sequence of points, for which there are lines $l(p_i, p_{i+1}) \ni p_i, p_{i+1}$, $i = 1, \dots, n-1$, and $l(p_n, p_1) \ni p_n, p_1$. Define parameters of *sides* $p_i \hat{p}_{i+1}$ and $p_n \hat{p}_1$ of polygon S as elements a_i of *side group* G_1 such that $\models Q_{a_i}(p_i, p_{i+1})$, $i = 1, \dots, n-1$, and $\models Q_{a_n}(p_n, p_1)$. Here if the pair (p_i, p_{i+1}) (or (p_n, p_1)) doesn't belong to the relation $\bigcup_{g_1 \in G_1} Q_{g_1}$, we set $a_i = \infty$ ($a_n = \infty$). Accordingly we define

parameters of *angles* $l(p_{i-1}, p_i) \hat{l}(p_i, p_{i+1})$, $i = 2, \dots, n-1$, $l(p_{n-1}, p_n) \hat{l}(p_n, p_1)$ and $l(p_n, p_1) \hat{l}(p_1, p_2)$ in S as elements α_i of *angle group* G_2 such that $\models R_{\alpha_{i-1}}(p_{i-1}, p_i, p_{i+1})$, $i = 2, \dots, n-1$, $\models R_{\alpha_{n-1}}(p_{n-1}, p_n, p_1)$ and $\models R_{\alpha_n}(p_n, p_1, p_2)$. Here if a sequential 3-tuple of points doesn't belong to the relation $\bigcup_{g_2 \in G_2} R_{g_2}$, then according

element α_i is equal to ∞ . Thus the parameters of polygon S are defined by SA-matrices of form $\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}$.

Denote by $\mathbf{S}(\text{gpm})$ the set of all SA-matrices correspondent to polygons from gpm .

Obviously any set $\mathbf{S}(\text{gpm})$ is closed. From the other hand any closed set of SA-matrices corresponds to some generalized polygonometry.

Theorem 1. [12] *For any closed set of SA-matrices $\mathbf{S}$ over group pair (G_1, G_2) there exists a generalized polygonometry $\text{gpm} = \text{gpm}(G_1, G_2, \mathcal{P})$ such that $\mathbf{S}(\text{gpm}) = \mathbf{S}$.*

Let $\mathbf{S}$ be a closed set of SA-matrices over (G_1, G_2) . Taking parameters $(a_1, \alpha_1, \dots, \dots, a_{n-2}, \alpha_{n-2}, a_{n-1})$ and $\alpha_1, a_2, \dots, \alpha_{n-2}, a_{n-1}, \alpha_{n-1}$ of a matrices $\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix} \in \mathbf{S}$ we get many-valued $(2n-3)$ -ary partial functions f_{ra}^{2n-3} , f_{ms}^{2n-3} , f_{la}^{2n-3} , f_{rs}^{2n-3} ,

$f_{ma}^{2n-3}, f_{ls}^{2n-3}$ satisfying the following conditions:

$$\begin{aligned} f_{ra}^{2n-3}(a_1, \alpha_1, \dots, a_{n-2}, \alpha_{n-2}, a_{n-1}) &= \left\{ \alpha_{n-1} \mid \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix} \in \mathbf{S} \right\}, \\ f_{ms}^{2n-3}(a_1, \alpha_1, \dots, a_{n-2}, \alpha_{n-2}, a_{n-1}) &= \left\{ a_n \mid \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix} \in \mathbf{S} \right\}, \\ f_{la}^{2n-3}(a_1, \alpha_1, \dots, a_{n-2}, \alpha_{n-2}, a_{n-1}) &= \left\{ \alpha_n \mid \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix} \in \mathbf{S} \right\}, \\ f_{rs}^{2n-3}(\alpha_1, a_2, \dots, \alpha_{n-2}, a_{n-1}, \alpha_{n-1}) &= \left\{ a_n \mid \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix} \in \mathbf{S} \right\}, \\ f_{ma}^{2n-3}(\alpha_1, a_2, \dots, \alpha_{n-2}, a_{n-1}, \alpha_{n-1}) &= \left\{ \alpha_n \mid \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix} \in \mathbf{S} \right\}, \\ f_{ls}^{2n-3}(\alpha_1, a_2, \dots, \alpha_{n-2}, a_{n-1}, \alpha_{n-1}) &= \left\{ a_1 \mid \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix} \in \mathbf{S} \right\}. \end{aligned}$$

Let $f : X \rightarrow Y$ be a function. By R_f we shall denote the plot $\{(x, y) \mid y = f(x)\}$ of function f .

For any partial many-valued function f_τ^{2n-3} consider characteristic real-valued function $\mu_\tau^{2n-3} : R_{f_\tau^{2n-3}} \rightarrow [0, 1]$, $\tau \in \{ra, ms, la, rs, ma, ls\}$. Thus any function μ_τ^{2n-3} defines the probability $p = \mu_\tau^{2n-3}(\xi_1, \xi_2, \dots, \xi_{2n-2})$ of equality $f_\tau^{2n-3}(\xi_1, \xi_2, \dots, \xi_{2n-3}) = \xi_{2n-2}$, $\xi_i \in G_1 \cup G_2 \cup \{\infty\}$. We shall denote this equality with its probability by $(f_\tau^{2n-3}(\xi_1, \xi_2, \dots, \xi_{2n-3}) = \xi_{2n-2} \mid p)$.

Let $\text{gpm} = \text{gpm}(G_1, G_2, \mathcal{P})$ be a generalized polygonometry such that $\mathbf{S}(\text{gpm}) = \mathbf{S}$. The system $\text{fgpm} = \langle \text{gpm}, \mu_\tau^{2n-3} \rangle_{\substack{n \in \omega \setminus \{0, 1, 2\}, \\ \tau \in \{ra, ms, la, rs, ma, ls\}}}$ is said to be a *fuzzy*

generalized polygonometry if it satisfies the following conditions for any SA-matrix

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix} \in \mathbf{S}(\text{gpm}):$$

$$\begin{aligned} \mu_{ra}^{2n-3}(a_1, \alpha_1, \dots, a_{n-2}, \alpha_{n-2}, a_{n-1}, \alpha_{n-1}) &> 0, \\ \mu_{ms}^{2n-3}(a_1, \alpha_1, \dots, a_{n-2}, \alpha_{n-2}, a_{n-1}, a_n) &> 0, \\ \mu_{la}^{2n-3}(a_1, \alpha_1, \dots, a_{n-2}, \alpha_{n-2}, a_{n-1}, \alpha_n) &> 0, \\ \mu_{rs}^{2n-3}(\alpha_1, a_2, \dots, \alpha_{n-2}, a_{n-1}, \alpha_{n-1}, a_n) &> 0, \\ \mu_{ma}^{2n-3}(\alpha_1, a_2, \dots, \alpha_{n-2}, a_{n-1}, \alpha_{n-1}, \alpha_n) &> 0, \\ \mu_{ls}^{2n-3}(\alpha_1, a_2, \dots, \alpha_{n-2}, a_{n-1}, \alpha_{n-1}, a_1) &> 0. \end{aligned} \tag{2.1}$$

Taking in a fuzzy polygonometry fgpm any $2n - 3$ sequential parameters of sides and angles of n -gon we get some number of possibilities for remaining three parameters and probabilities for each variant of these parameters.

Let $\mathbf{S}$ be a closed set of SA-matrices, μ_τ^{2n-3} , $\tau \in \{ra, ms, la, rs, ma, ls\}$, be characteristic real-valued function satisfying conditions (1) for any SA-matrix

$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix} \in \mathbf{S}$. Then the system $\langle \mathbf{S}, \mu_\tau^{2n-3} \rangle_{\substack{n \in \omega \setminus \{0,1,2\}, \\ \tau \in \{ra, ms, la, rs, ma, ls\}}}$ is said to be *f-closed*.

Obviously for any fuzzy polygonometry

$$\text{fgpm} = \langle \text{gpm}, \mu_\tau^{2n-3} \rangle_{\substack{n \in \omega \setminus \{0,1,2\}, \\ \tau \in \{ra, ms, la, rs, ma, ls\}}}$$

the system $\langle \mathbf{S}(\text{gpm}), \mu_\tau^{2n-3} \rangle_{\substack{n \in \omega \setminus \{0,1,2\}, \\ \tau \in \{ra, ms, la, rs, ma, ls\}}}$ is *f-closed*. Using theorem 1 we get its fuzzy analogue.

Theorem 2. *For any f-closed system $\langle \mathbf{S}, \mu_\tau^{2n-3} \rangle_{\substack{n \in \omega \setminus \{0,1,2\}, \\ \tau \in \{ra, ms, la, rs, ma, ls\}}}$ over group pair (G_1, G_2) there exists a fuzzy generalized polygonometry*

$$\text{fgpm} = \langle \text{gpm}, \mu_\tau^{2n-3} \rangle_{\substack{n \in \omega \setminus \{0,1,2\}, \\ \tau \in \{ra, ms, la, rs, ma, ls\}}},$$

$\text{gpm} = \text{gpm}(G_1, G_2, \mathcal{P})$, such that

$$\langle \mathbf{S}(\text{gpm}), \mu_\tau^{2n-3} \rangle_{\substack{n \in \omega \setminus \{0,1,2\}, \\ \tau \in \{ra, ms, la, rs, ma, ls\}}} = \langle \mathbf{S}, \mu_\tau^{2n-3} \rangle_{\substack{n \in \omega \setminus \{0,1,2\}, \\ \tau \in \{ra, ms, la, rs, ma, ls\}}}.$$

As proved in [13] the class of partial algebras correspondent to group pair polygonometries is axiomatizable. Analogously one can show that the class of fuzzy polygonometries is axiomatizable in a two-sorted first order logic.

References

- [1] *Stepanov N. N.* Spherical trigonometry (Russian). Moscow, Leningrad: ONTI NKTP USSR, 1948.
- [2] *Lysenko V. I.* Polygonometric work in Russia in the 18th century (Russian) // *Istor.-Mat. Issled.* 1959. V. 12. P. 161-178.
- [3] *Lysenko V. I.* On the mathematical works of A. I. Lexell (Russian) // *History and methodology of the natural sciences*, XXV. Moscow. 1980. P. 104-112.
- [4] *Lysenko V. I.* Nikolai Ivanovich Fuss (1755-1826) (Russian). M.: Nauka, 1975.
- [5] *Danilov V. V.* Exact polygonometry. Moscow, 1953.
- [6] *Sudoplatov S. V.* Group polygonometries and related algebraic systems // *Contributions to General Algebra 11 / Proc. of the Olomouc Workshop '98 on General Algebra*. Klagenfurt: Verlag Johannes Heyn, 1999. P. 191-210.

- [7] *Sudoplatov S. V.* Group polygonometries with symmetrical conditions // Algebra and Model Theory 2 (Edited by A. G. Pinus and K. N. Ponomaryov). Novosibirsk: Novosibirsk State Technical University, 1999. P. 140–159.
- [8] *Antippa A. F.* The combinatorial structure of trigonometry // International J. of Mathematics and Math. Sciences. V. 2003, N 8. P. 475–500.
- [9] *Sudoplatov S. V.* On trigonometries of groups on a projective plane // Siberian Math. J. 1995. V. 36, N 2. P. 419–431.
- [10] *Sudoplatov S. V.* ω -Stable trigonometries on a projective plane // Siberian Advances in Math. 2002. V. 12, N 4. P. 97–124.
- [11] *Sudoplatov S. V.* Powerful digraphs // Siberian Math. J. (Submitted in 2003).
- [12] *Sudoplatov S. V.* Closed sets of side-angle matriëes and correspondent geometrical structures // Algebra and Model Theory 3 (Edited by A. G. Pinus and K. N. Ponomaryov). Novosibirsk: Novosibirsk State Technical University, 2001. P. 131–135.
- [13] *Sudoplatov S. V.* Partial algebras associated with group pair polygonometries // Algebra and Logic. 1997. V. 36, N 4. P. 454–476.

О МЕРАХ БЛИЗОСТИ И ОПРОВЕРЖИМОСТИ ЛОГИЧЕСКИХ ФОРМУЛ С ВЕРОЯТНОСТЯМИ НА КОНЕЧНЫХ КЛАССАХ МЕТРИЧЕСКИХ МОДЕЛЕЙ

А.А. Викентьев, Р.А. Викентьев*

Институт математики СО РАН
Россия, 630090, Новосибирск, пр. Коптюга, 4
phone: (3832) 363008
e-mail: vikent@math.nsc.ru

Введение

К настоящему времени достаточно хорошо развиты теория и методы построения решающих функций распознавания образов на основе анализа эмпирической информации, представленной в виде таблиц данных. Наряду с этим проявляется все больший интерес к анализу экспертной информации, заданной в виде вероятностных логических высказываний нескольких экспертов. С помощью подходящей процедуры высказывания экспертов можно записать в виде формул исчисления высказываний или формул языка первого порядка с вероятностями. Ясно, что различные высказывания экспертов (и соответствующие им формулы) несут в себе, вообще говоря, разное количество информации.

В работе [1] Г.С. Лбовым и В.Я. Блющицыным поставлена задача о введении меры информативности I на множестве классов эквивалентных формул языка первого порядка, и сформулированы естественные требования, которым должна удовлетворять эта функция, выражаемая через некоторую метрику ρ на множестве классов эквивалентных формул, значения которой принадлежат интервалу $[0, 1]$. Все желаемые свойства меры информативности [1] мы сформулируем на формулах — представителях классов, где эти формулы лежат:

*Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 01-01-00839).

- 1) Если $\varphi \equiv 1$, то $I(\varphi) = 0$ (информативность тождественно истинной формулы равна нулю).
- 2) Если $\varphi \equiv \psi$, то $I(\varphi \wedge \psi) = I(\varphi)$.
- 3) Если $\rho(\varphi, \psi) = 1$, то $I(\varphi \wedge \psi) = I(\varphi) + I(\psi)$.
- 4) В случае $\rho(\varphi, \psi) \in (0, 1)$, $I(\varphi \wedge \psi) = f(I(\varphi), I(\psi), \rho(\varphi, \psi))$, где $f(x, y, z)$ некоторая функция от переменных x, y, z удовлетворяющая следующим свойствам:
 - а) $f(x, y, 1) = x + y$; б) $f(x, x, 0) = x$;
 - в) $f(x, y, z_1) \leq f(x, y, z_2)$, если $z_1 \leq z_2$.
- 5) $I(\varphi) = 1 - I(\neg\varphi)$.

Таким образом, для решения поставленной задачи (для применения в приложениях) необходимо решить две подзадачи:

- 1) ввести достаточно адекватную метрику (с точки зрения экспертов) на классах формул с учетом метрики в модели (если она есть);
- 2) найти такую функцию $f(x, y, z)$, которая обладает требуемыми свойствами.

В работах [2, 4] эта задача решена для формул исчисления высказываний. Мера информативности определена как мера опровержимости формулы на моделях. В случае непротиворечивости формулы (если для нее существует хотя бы одна модель, на которой она истинна) эта мера отражает интуитивное представление о количестве информации, содержащейся в высказывании эксперта, и ее ценности с точки зрения эксперта. В [5] задача решена для формул языка первого порядка с использованием конечного класса моделей.

В настоящей работе предлагается некоторый общий подход с использованием конечного класса моделей и его модификаций для вычисления естественных расстояний, мер информативности и установления свойств, удовлетворяющих требованиям 1) – 5). В дальнейшем вместо понятия мера информативности будем использовать слова мера опровержимости, поскольку это более соответствует сути вводимой меры. Рассматривается также задача введения расстояний на множестве вероятностных формул. Для предложенных расстояний также справедливы хорошие свойства метрики (как в предыдущих случаях) и меры опровержимости.

Предложенные метрики и меры опровержимости апробированы на отдельных примерах и на задаче по интеграционному проекту СО РАН “Компьютерная система для анализа антропологической информации” (рук. д.т.н., профессор Г.С. Лбов), которые кратко приводятся в работе.

Отметим, что проблемой введения расстояний в классе специальных формул и предикатов занимается Н.Г. Загоруйко [6, 7]. Его подход более проработан с точки зрения практических применений. Наш подход отличается некоторой общностью (произвольные предикаты и формулы) и детальной теоретической проработкой исследований как свойств предлагаемых метрик, так и решением задачи о введении информативности (как меры опровержимости).

В решении поставленных задач важную роль играет конечное число моделей и используется логическая теория моделей, что позволяет изучать вопрос

не только с точки зрения высказываний экспертов, но и "знаний" экспертов (гипотез), выраженных в виде интерпретаций сигнатурных предикатов (возможно и многоместных).

Исследование позволит решать вопросы связанные с согласованием экспертных высказываний, построением решающих функций, распознавания образов, а также при создании логических баз знаний, их кластеризации и разработки экспертных систем [2, 5].

1. Расстояния между формулами языка первого порядка

Пусть $\Omega = \{P_1^{m_1}, \dots, P_t^{m_t}\}$ — фиксированная сигнатура, состоящая из конечного числа предикатных символов, которые выбираются для записи и изучения имеющихся связей между переменными в конкретной прикладной области. Случай исчисления высказываний описан в [2, 4]. Пусть задано некоторое исходное множество переменных $X = \{x_1, \dots, x_p\}$. Обозначим через D_{x_j} непустое множество с конечной мерой возможных значений переменной x_j . Пусть $A_n = \bigcup_{j=1}^p D_{x_j}$ — непустое множество мощности n , являющееся объединением всех значений рассматриваемых переменных, включенных в предикаты.

В сигнатуру Ω для каждой переменной x_j дополнительно включен одноместный предикат P_{x_j} , выделяющий область значений переменной x_j в A_n , то есть предикат $P_{x_j}(a)$ истинен в модели A_n на элементах $a \in A_n$ тогда и только тогда, когда $a \in D_{x_j}$.

Определение 1 [7]. Под интерпретацией будем понимать отображение γ , ставящее в соответствие каждому m_i -местному предикатному символу $P_i^{m_i}$ из сигнатуры Ω m_i -местный предикат (отношение) $P_i^{A_n} \subseteq A_n^{m_i}$, заданный на множестве A_n . Это позволяет говорить о модели $\langle A_n, \Omega \rangle$ сигнатуры Ω . В модели $\langle A_n, \Omega \rangle$ предикат $P_i(x_1, \dots, x_{m_i})$ истинен на элементах $a_1, \dots, a_{m_i}$ из A_n (записывается $\langle A_n, \Omega \rangle \models P_i(a_1, \dots, a_{m_i})$) тогда и только тогда, когда $\langle a_1, \dots, a_{m_i} \rangle \in P_i^{A_n}$ и $a_j \in D_{x_j}$. Будем рассматривать модели только конечной сигнатуры.

Пусть имеется конечное число s экспертов и области возможных значений всех переменных. Модели (в смысле теории моделей) задаются специалистами согласно утверждениям экспертов. С каждым экспертом связывается модель, согласно его знаниям интерпретируются сигнатурные предикаты. Каждый эксперт "задает" свою интерпретацию каждого предикатного символа $P_i^{m_i}$ сигнатуры Ω соответствующим отношением (предикатом) на множестве A_n . В результате имеем множество моделей $\{M_j\}_{j=1}^s$ (исходный класс моделей).

"Знания" экспертов можно записать в виде формул (возможно с кванторами) в некоторой сигнатуре первого порядка (возможно и предложениями, то есть формулами с кванторами без свободных переменных). Предложения либо истинны, либо ложны на модели, а формулы с переменными определя-

ют формульные предикаты (подмножества) в каждой модели M_j по заданной интерпретации сигнатурных символов предикатов j -го эксперта [2].

Пусть $F = \bigcup_k F_k$ — множество формул сигнатуры Ω , содержащее формулы, отвечающие "знаниям" экспертов, и замкнутое относительно подформул, логических операций $\neg$, $\wedge$, $\vee$ (возможно бесконечных) и кванторов $\forall$ и $\exists$ по переменным, где через F_k обозначено множество формул из F от фиксированных k переменных.

Мы хотим задать вероятностную меру на множестве формул F , которая удовлетворяла следующему определению.

Определение 2 [9]. Вероятностной мерой ν на множестве F называется отображение $\nu : F \rightarrow [0, 1]$, удовлетворяющее для φ и $\psi \in F$ условиям:

- 1) если $\vdash \varphi \equiv \psi$, то $\nu(\varphi) = \nu(\psi)$, ($\vdash \varphi$ означает, что на всех моделях φ истинна);
- 2) если $\vdash \neg(\varphi \wedge \psi)$, то $\nu(\varphi \vee \psi) = \nu(\varphi) + \nu(\psi)$;
- 3) если $\vdash \varphi$, то $\nu(\varphi) = 1$;
- 4) если $\vdash \neg\varphi$, то $\nu(\varphi) = 0$;
- 5) $\nu(\neg\varphi) = 1 - \nu(\varphi)$.

Пусть B_k — система μ -измеримых подмножеств множества A_n^k , образующая σ -алгебру, где $\mu : B_k \rightarrow [0, 1]$ обладает свойствами функции вероятности Колмогорова, а $A_n^k = \underbrace{A_n \times \dots \times A_n}_k$.

В дальнейшем мы предполагаем, что при фиксированной интерпретации сигнатурных символов сигнатуры Ω (задании экспертом модели M_i) для любого k каждой формуле $\psi_j \in F_k$ соответствует (формульное) подмножество $S_j \in B_k$, где S_j — это множество кортежей из A_n^k , на которых истинна формула ψ_j в модели M_i .

Таким образом, фиксируя модель M_i и отождествляя формулы, имеющие одинаковые интерпретации (эквивалентные в модели M_i формулы), получаем взаимно-однозначное отображение алгебры попарно неэквивалентных формул $F_k / \equiv$ на некоторую σ -подалгебру алгебры B_k , сохраняющее булевы операции. Заметим, что $F_k / \equiv$ является булевой алгеброй и замкнуто относительно бесконечного числа конъюнкций и дизъюнкций.

Тем самым зададим вероятностную меру μ_i (по модели M_i) для каждой k и формулы $\psi_j \in F_k$ $\mu_i(\psi_j) = \mu(\psi_j^{M_i})$, которая обладает всеми свойствами определения 2.

По заданным "знаниям" экспертов мы построили класс моделей (исходный класс). Чтобы более полно использовать информацию экспертов расширим исходный класс моделей. Учитывая одновременно информацию нескольких экспертов, можно уточнить каждую модель (тем самым получить еще одну или более новых моделей) и эти новые модели добавить в исходный класс. Уточнять модели будем следующим образом. Вместо "знания", заданного экспертом в виде предиката P_i в модели M_j , далее будем рассматривать его уточнение — предикат $\tilde{P}_i$.

Под уточнением $\tilde{P}_i$ предиката P_i понимаем уточнение интерпретации этого предиката в модели M_j одним из способов:

- 1) оставить предикат P_i без изменений;
- 2) исключить из P_i те элементы, в истинности которых j -ый эксперт не совсем уверен;
- 3) в предикат P_i добавить новые элементы и исключить некоторые старые, например, с учетом "знаний" других экспертов;
- 4) выполнить пункты 2) и 3) одновременно.

Обозначим произвольный модифицированный класс моделей через $\text{Mod}_n(\Omega)$. Введем расстояние на множестве "знаний" экспертов с помощью этого класса моделей $\text{Mod}_n(\Omega)$. Модели различаются интерпретациями сигнатурных предикатов, входящих в "знания" экспертов.

Определим расстояние между формульными подмножествами (предикатами) от одних и тех же переменных в каждой модели $M_i \in \text{Mod}_n(\Omega)$, как нормированную меру их модифицированной симметрической разности как в [3]. Предикат $P_i^{M_j}$ в новой добавленной к исходному классу модели M_j это предикат $\tilde{P}_i^{M_j}$.

Определение 3. Расстоянием между предикатами (формульными подмножествами) $P_k^{M_i}$ и $P_j^{M_i}$ от одних и тех же переменных, определенными в модели M_i , назовем величину

$$\rho_{M_i}(P_k^{M_i}, P_j^{M_i}) = \mu(P_k^{M_i} \triangle P_j^{M_i}).$$

Замечание 1. Это определение можно расширить на формулы с различными наборами свободных переменных. В этом случае, если рассматриваемые предикаты имеют разную местность или разный набор переменных, и эксперт считает отсутствующую в одной из формул переменную x_i несущественной, полагаем, что она принимает любое из возможных значений и добавляем конъюнктивно к нужной формуле предикат P_{x_i} , выделяющий область значений этой переменной. В противном случае (если она существенна) доопределяем эту переменную, добавив конъюнктивно к нужной формуле предикат P'_{x_i} , уточняющий значения этой переменной после повторного обращения к эксперту [2]. Если расстояние измеряется между формулами, у которых наборы переменных различаются, например, по переменной x_i , причем в одной из формул переменная x_i находится под действием квантора, а в другую формулу x_i не входит, тогда относительно переменной x_i в таких формулах никаких изменений делать не надо. Если же расстояние измеряется между формулами, у которых наборы переменных различаются по переменной x_i , и в одной из формул переменная x_i находится под действием квантора, а в другой формуле x_i является свободной переменной, тогда доопределяем эту переменную, добавив конъюнктивно к нужной формуле предикат P_{x_i} или P'_{x_i} , уточняющий значения этой переменной, в зависимости от способа доопределения переменной. Например, заменяем формулу $\psi(x_j) = \exists x_i \varphi(x_i, x_j)$

на формулу $\psi(x_i, x_j) = \exists x_i(\varphi(x_i, x_j) \wedge P'_{x_i}) \wedge P'_{x_i}$. Аналогично рассматривается случай с квантором $\forall$.

В дальнейшем, с учетом выше сказанного, будем изучать расстояния между формулами от одних и тех же переменных (одной ариности).

Расстояние между формулами, определенными на множестве моделей $\text{Mod}_n(\Omega)$, определим как среднее (возможно с весами) на множестве расстояний в моделях.

Определение 4. Расстоянием между формулами P_k и P_j от одних и тех же переменных, определенными на множестве $\text{Mod}_n(\Omega)$, назовем величину

$$\rho_1(P_k, P_j) = \frac{\sum_{M_i \in \text{Mod}_n(\Omega)} \rho_{M_i}(P_k^{M_i}, P_j^{M_i})}{|\text{Mod}_n(\Omega)|}.$$

Теперь рассмотрим способ определения расстояния между предложениями (замкнутыми формулами). Обозначим через $\text{Mod}(\varphi)$ множество моделей из $\text{Mod}_n(\Omega)$, на которых истинно предложение φ , т.е. $\text{Mod}(\varphi) = \{M_i \in \text{Mod}_n(\Omega) \mid M_i \models \varphi\}$.

Очевидно, существуют такие модели, на которых предложение (эксперта) истинно, и такие, на которых оно ложно. Естественно с семантической точки зрения измерять различие информации, содержащейся в предложениях, количеством моделей, на которых предложения принимают разные значения истинности.

Определение 5. Расстоянием между предложениями φ и ψ от одних и тех же переменных назовем величину

$$\rho_2(\varphi, \psi) = \frac{|\text{Mod}((\neg\varphi \wedge \psi) \vee (\varphi \wedge \neg\psi))|}{|\text{Mod}_n(\Omega)|}.$$

Рассмотрим еще один способ определения расстояния между формулами. Дополним сигнатуру Ω константами из множества A_n . Для этого множества рассмотрим произвольные кортежи $\bar{a}$ длины местности формул, равной $\ell(\bar{a})$. При подстановке кортежей в формулы, в предположении, что формулы имеют одинаковую местность (как этого добиться было показано выше), формулы становятся предложениями.

Под эквивалентностью двух формул $\varphi(\bar{x})$ и $\psi(\bar{x})$ ($\varphi(\bar{x}) \equiv \psi(\bar{x})$) будем понимать эквивалентность их в классе моделей $\text{Mod}_n(\Omega)$, то есть в каждой модели $M_i \in \text{Mod}_n(\Omega)$ соответствующие $\varphi(\bar{x})$ и $\psi(\bar{x})$ формульные подмножества (множество реализаций формул) совпадают.

Тогда расстояние между неэквивалентными формулами φ и ψ определим как минимум расстояний, определенных по всем кортежам, которые реализуют формулу φ , но не реализуют формулу ψ и наоборот, используя определенное выше расстояние для предложений. Расстояние между эквивалентными формулами равно нулю.

Определение 6. Расстоянием между формулами φ и ψ от одних и тех же переменных назовем величину

$$\rho_3(\varphi(\bar{x}), \psi(\bar{x})) = \begin{cases} \min_{\bar{a} \in \chi(A_n^{\ell(\bar{a})})} \rho_2(\varphi(\bar{a}), \psi(\bar{a})), & \varphi(\bar{x}) \not\equiv \psi(\bar{x}) \\ 0, & \varphi(\bar{x}) \equiv \psi(\bar{x}), \end{cases}$$

где $\chi(\bar{x}) = (\neg\varphi(\bar{x}) \wedge \psi(\bar{x})) \vee (\varphi(\bar{x}) \wedge \neg\psi(\bar{x}))$ и $\chi(A_n^{\ell(\bar{a})}) = \{\bar{b} \in A_n^{\ell(\bar{a})} \mid \exists M_i \in \text{Mod}_n(\Omega) : M_i \models \chi(\bar{b})\}$

Ранее доказана теорема [3-6], из которой следует, что предложенные расстояния действительно являются метриками. В теореме 1 обобщается этот результат и приведены некоторые специальные свойства введенных для формул расстояний.

Далее вместо $\varphi(\bar{x})$, $\psi(\bar{x})$, $\chi(\bar{x})$ для краткости будем писать φ , ψ , χ .

Теорема 1. Для любых формул φ , ψ , χ от одних и тех же переменных и любой конечной модификации исходного класса моделей для любого ρ_i ($i = 1, 2, 3$) выполняются следующие свойства:

1. $0 \leq \rho_i(\varphi, \psi) \leq 1$.
2. $\rho_i(\varphi, \psi) = \rho_i(\psi, \varphi)$ (симметричность).
3. Если $\rho_i(\varphi, \psi) = \rho_i(\varphi_1, \psi_1)$ и $\rho_i(\varphi_1, \psi_1) = \rho_i(\varphi_2, \psi_2)$, то $\rho_i(\varphi, \psi) = \rho_i(\varphi_2, \psi_2)$.
4. $\rho_i(\varphi, \psi) \leq \rho_i(\varphi, \chi) + \rho_i(\chi, \psi)$.
5. $\varphi \equiv \psi \iff \rho_i(\varphi, \psi) = 0$.
6. $\varphi \equiv \neg\psi \iff \rho_i(\varphi, \psi) = 1$.
7. $\rho_i(\varphi, \psi) = 1 - \rho_i(\varphi, \neg\psi) = \rho_i(\neg\varphi, \neg\psi)$.
8. $\rho_i(\varphi, \psi) = \rho_i(\varphi \wedge \psi, \varphi \vee \psi)$.
9. $\rho_i(\varphi, \neg\varphi) = \rho_i(\varphi, \psi) + \rho_i(\psi, \neg\varphi)$.

Доказательство теоремы следует из определений, свойств вероятностной меры, теоретико-модельных вычислений и аналогично доказательству из [3,4]. Для наглядности приведем доказательство пункта 4.

Для $i = 1$ достаточно показать, что $\mu(\varphi^{M_i} \triangle \psi^{M_i}) \leq \mu(\varphi^{M_i} \triangle \chi^{M_i}) + \mu(\chi^{M_i} \triangle \psi^{M_i})$ для каждой модели M_i . Рассмотрим $\mu(\varphi^{M_i} \triangle \psi^{M_i}) = \mu(\varphi^{M_i} \setminus \psi^{M_i}) + \mu(\psi^{M_i} \setminus \varphi^{M_i}) = \mu(\varphi^{M_i} \wedge \neg\psi^{M_i}) + \mu(\psi^{M_i} \wedge \neg\varphi^{M_i}) = \mu(\varphi^{M_i} \wedge \chi^{M_i} \wedge \neg\psi^{M_i}) + \mu(\varphi^{M_i} \wedge \neg\chi^{M_i} \wedge \neg\psi^{M_i}) + \mu(\psi^{M_i} \wedge \neg\varphi^{M_i} \wedge \chi^{M_i}) + \mu(\psi^{M_i} \wedge \neg\varphi^{M_i} \wedge \neg\chi^{M_i}) \leq \mu(\chi^{M_i} \wedge \neg\psi^{M_i}) + \mu(\varphi^{M_i} \wedge \neg\chi^{M_i}) + \mu(\neg\varphi^{M_i} \wedge \chi^{M_i}) + \mu(\psi^{M_i} \wedge \neg\chi^{M_i}) = \mu(\varphi^{M_i} \triangle \chi^{M_i}) + \mu(\chi^{M_i} \triangle \psi^{M_i})$, что и требовалось получить.

Докажем свойство 4 для $i = 2$. Обозначим через $S_1 = \text{Mod}((\neg\varphi \wedge \psi) \vee (\varphi \wedge \neg\psi))$, $S_2 = \text{Mod}((\neg\varphi \wedge \chi) \vee (\varphi \wedge \neg\chi))$, $S_3 = \text{Mod}((\neg\chi \wedge \psi) \vee (\chi \wedge \neg\psi))$. Докажем, что $|S_1| \leq |S_2| + |S_3|$. Достаточно доказать, что $S_1 \subset S_2 \cup S_3$. Возьмем произвольно $M_j \in S_1$, тогда $(M_j \models (\neg\varphi \wedge \psi)) \vee (M_j \models (\varphi \wedge \neg\psi))$. Без ограничения общности (используя симметричность) будем считать, что $M_j \models (\neg\varphi \wedge \psi)$. Значит, $M_j \models \neg\varphi$ и $M_j \models \psi$. Для произвольного χ ясно, что $(M_j \models \chi) \vee (M_j \models \neg\chi)$. Если $M_j \models \chi$, то $M_j \models (\neg\varphi \wedge \chi)$, т. е. $M_j \in S_2$. Если $M_j \models \neg\chi$, то $M_j \models (\neg\chi \wedge \psi)$, т. е. $M_j \in S_3$. Получили, что $(M_j \in S_2) \vee (M_j \in S_3)$, т. е. $M_j \in S_2 \cup S_3$. В силу произвольности M_j имеем $S_1 \subset S_2 \cup S_3$. Поэтому,

$|S_1| \leq |S_2 \cup S_3| = |S_2| + |S_3| - |S_2 \cap S_3| \leq |S_2| + |S_3|$, что и требовалось. Для $i = 3$ свойство 4 доказывается аналогично.

2. Меры опровержимости и вероятности формул

С точки зрения важности информации, сообщенной экспертом, которому мы доверяем, естественно считать, что опровержимость непустой формулы тем выше, чем меньше число удовлетворяющих ей элементов для конечного случая, и чем меньше мера задаваемого предикатной формулой подмножества в общем случае. Поэтому введем меру опровержимости следующим образом.

Определение 7. Мерой опровержимости формулы $\varphi(\bar{x})$ назовем величину

$$I_i(\varphi(\bar{x})) = \rho_i(\varphi(\bar{x}), 1),$$

где 1 — тождественно истинный предикат (например, $\bar{x} = \bar{x}$).

Для введенных расстояний ρ_i ($i = 1, 2, 3$) получаем соответственно следующие меры опровержимости:

$$I_1(\varphi) = \frac{\sum_{M_i \in \text{Mod}_n(\Omega)} \mu(\neg\varphi^{M_i})}{|\text{Mod}_n(\Omega)|}, \quad I_2(\varphi) = \frac{|\text{Mod}(\neg\varphi)|}{|\text{Mod}_n(\Omega)|}, \quad I_3(\varphi) = \frac{\min_{\bar{a} \in \chi(A_n^{\ell(\bar{a})})} |\text{Mod}(\neg\varphi(\bar{a}))|}{|\text{Mod}_n(\Omega)|}.$$

Для мер опровержимости справедлива следующая

Теорема 2. Для любых формул исчисления предикатов φ и ψ от одних и тех же переменных и любой модификации исходного класса моделей справедливы для любого ρ_i ($i = 1, 2, 3$) следующие свойства:

1. $0 \leq I_i(\varphi) \leq 1$.
2. $I_i(1) = 0$.
3. $I_i(0) = 1$.
4. $I_i(\varphi) = 1 - I_i(\neg\varphi)$.
5. $I_i(\varphi) \leq I_i(\varphi \wedge \psi)$.
6. $I_i(\varphi) \geq I_i(\varphi \vee \psi)$.
7. $I_i(\varphi \wedge \psi) = \rho_i(\varphi, \psi) + I_i(\varphi \vee \psi)$.
8. Если $\varphi \equiv \psi$, то $I_i(\varphi) = I_i(\psi)$.
9. Если $\rho_i(\varphi, \psi) = 0$, то $I_i(\varphi \vee \psi) = I_i(\varphi \wedge \psi) = I_i(\varphi)$.
10. $I_i(\varphi \wedge \psi) = (I_i(\varphi) + I_i(\psi) + \rho_i(\varphi, \psi))/2$.
11. $I_i(\varphi \vee \psi) = (I_i(\varphi) + I_i(\psi) - \rho_i(\varphi, \psi))/2$.

Для доказательства теоремы используются введенные определения, свойства метрики из теоремы 1 и теоретико-модельные вычисления аналогичные доказательству из [4]. Приведем доказательство пункта 10.

Докажем для $i = 1$. $I_1(\varphi \wedge \psi) = 1 - I_1(\neg(\varphi \wedge \psi)) = 1 - I_1(\neg\varphi \vee \neg\psi) =$
 $= 1 - \frac{\sum_{M_i \in \text{Mod}_n(\Omega)} \mu(\varphi^{M_i} \wedge \psi^{M_i})}{|\text{Mod}_n(\Omega)|} = 1 + \frac{\sum_{M_i \in \text{Mod}_n(\Omega)} (\mu(\varphi^{M_i}) + \mu(\psi^{M_i}) - 2\mu(\varphi^{M_i} \wedge \psi^{M_i}))}{2|\text{Mod}_n(\Omega)|} -$
 $- \frac{\sum_{M_i \in \text{Mod}_n(\Omega)} (\mu(\varphi^{M_i}) + \mu(\psi^{M_i}))}{2|\text{Mod}_n(\Omega)|} = 1 + \frac{\sum_{M_i \in \text{Mod}_n(\Omega)} \mu(\varphi^{M_i} \Delta \psi^{M_i})}{2|\text{Mod}_n(\Omega)|} - \frac{I_1(\neg\varphi) + I_1(\neg\psi)}{2} = 1 +$
 $+ \frac{1}{2}\rho_1(\varphi, \psi) - \frac{1}{2}(1 - I_1(\varphi) + 1 - I_1(\psi)) = \frac{1}{2}(I_1(\varphi) + I_1(\psi) + \rho_1(\varphi, \psi)).$ Что и требовалось доказать. Для $i = 2, 3$ аналогично.

На практике же эксперт обычно задает высказывание с его "вероятностью". А вопрос состоит в изучении и согласовании таких высказываний, введении некоторой метрики на таких высказываниях. Первоочередной задачей, на наш взгляд, является определение вероятностей для формул с помощью модельного подхода.

Определение 8. Вероятностью формулы $\varphi(\bar{x})$ назовем величину

$$P_i(\varphi(\bar{x})) = \rho_i(\varphi(\bar{x}), 0).$$

В следующей лемме содержатся некоторые дополнительные свойства введенной вероятности.

Лемма 3. Для любого конечной модификации исходного класса моделей P_i ($i = 1, 2, 3$) является вероятностной мерой на множестве формул F и для любых формул исчисления предикатов φ и ψ от одних и тех же переменных и для любого ρ_i ($i = 1, 2, 3$) справедливы следующие утверждения:

1. $0 \leq P_i(\varphi) \leq 1$.
2. $P_i(1) = 1$.
3. $P_i(0) = 0$.
4. $P_i(\varphi) = 1 - P_i(\neg\varphi)$.
5. $P_i(\varphi) \geq P_i(\varphi \wedge \psi)$.
6. $P_i(\varphi) \leq P_i(\varphi \vee \psi)$.
7. $P_i(\varphi \wedge \psi) = P_i(\varphi \vee \psi) - \rho_i(\varphi, \psi)$.
8. Если $\varphi \equiv \psi$, то $P_i(\varphi) = P_i(\psi)$.
9. Если $\rho_i(\varphi, \psi) = 0$, то $P_i(\varphi \vee \psi) = P_i(\varphi \wedge \psi) = P_i(\varphi)$.
10. $P_i(\varphi \wedge \psi) = (P_i(\varphi) + P_i(\psi) - \rho_i(\varphi, \psi))/2$.
11. $P_i(\varphi \vee \psi) = (P_i(\varphi) + P_i(\psi) + \rho_i(\varphi, \psi))/2$.

Ясно, что так введенная функция P_i удовлетворяет всем свойствам определения 2. Для доказательства теоремы 3 последовательно используются результаты теорем 1 и 2 и то, что $P_i(\varphi(\bar{x})) = I_i(\neg\varphi(\bar{x}))$.

Так вычисленные с использованием модельного подхода вероятности позволяют уточнять "вероятности" экспертов и будут применяться в дальнейшем.

Разработан и реализован алгоритм для вычисления расстояний между формулами и мер опровержимости формул. Приведем один из тестовых примеров.

Пример 1. Пусть три эксперта высказываются о возрасте человека и его профессии, предсказывая наличие у него того или иного заболевания, например, радикулита и ухудшения зрения. То есть

$$X = \{x_1(), x_2()\};$$

$$D_{x_1} = \{, , , \};$$

$$D_{x_2} = \{41, 42, 43, 44, 45\};$$

$$\Omega = \{P_1 -, P_2 - \}.$$

Для краткости формулу $(x = a_1 \vee x = a_2 \vee x = a_3)$ будем записывать как $(x = a_1 \vee a_2 \vee a_3)$ и через $P(x, y) =$ обозначать, что предикат истинен.

1-ый эксперт:

$$P_1^1(x_1, x_2) = \iff [(x_1 = \vee \vee) \wedge (x_2 = 42 \vee 43 \vee 44 \vee 45)]$$

$$P_2^1(x_1, x_2) = \iff [(x_1 = \vee \vee) \wedge (x_2 = 41 \vee 42 \vee 43 \vee 44)]$$

2-ой эксперт:

$$P_1^2(x_1, x_2) = \iff [(x_1 =) \wedge (x_2 = 44 \vee 45)]$$

$$P_2^2(x_1, x_2) = \iff [(x_1 = \vee \vee) \wedge (x_2 = 43 \vee 44 \vee 45)]$$

3-ий эксперт:

$$P_1^3(x_1, x_2) = \iff [(x_1 = \vee)]$$

$$P_2^3(x_1, x_2) = \iff [(x_1 = \vee) \wedge (x_2 = 41 \vee 43 \vee 45)]$$

Вычислим расстояние между предикатами P_1 и P_2 и меры их опровержимости.

В модели M_1 первого эксперта имеем:

$$\rho_{M_1}(P_1^1, P_2^1) = 0, 6; I_{M_1}(P_1^1) = 0, 4; I_{M_1}(P_2^1) = 0, 4.$$

В модели M_2 второго эксперта имеем:

$$\rho_{M_2}(P_1^2, P_2^2) = 0, 35; I_{M_2}(P_1^2) = 0, 9; I_{M_2}(P_2^2) = 0, 55.$$

В модели M_3 третьего эксперта имеем:

$$\rho_{M_3}(P_1^3, P_2^3) = 0, 5; I_{M_3}(P_1^3) = 0, 5; I_{M_3}(P_2^3) = 0, 7.$$

Тогда результирующее расстояние между предикатами P_1 и P_2 равно $\rho(P_1, P_2) = 0, 4833$; а меры опровержимости предикатов соответственно равны $I(P_1) = 0, 6$; $I(P_2) = 0, 55$.

Можно вычислить расстояния между "знаниями" экспертов относительно одного и того же заболевания:

$$\rho(P_1^1, P_1^2) = 0, 5; \rho(P_1^1, P_1^3) = 0, 3; \rho(P_1^2, P_1^3) = 0, 4;$$

$$\rho(P_2^1, P_2^2) = 0, 65; \rho(P_2^1, P_2^3) = 0, 7; \rho(P_2^2, P_2^3) = 0, 35.$$

Приведем еще один пример.

Пример 2 ([6]). Два эксперта высказываются о влажности (X_1), которая измеряется четырьмя значениями, то есть $D_{X_1} = \{\text{нулевая, низкая, средняя, высокая}\}$, о количестве азотных удобрений (X_2), диапазон изменений которого от 0 до 320 кг/га, то есть $D_{X_2} = (0, 320)$ (X_2 - непрерывная переменная), о типе почвы (X_3), число которых 4, и видах культур-предшественников (X_4), число которых 8.

На вопрос, каковы условия для получения хорошего урожая пшеницы, эксперты дали такие ответы:

$$1: (X_1 =) \wedge (X_2 \in (160 - 200)) \wedge (X_3 =),$$

$$2: (X_1 = \vee) \wedge (X_2 \in (200 - 280)) \wedge (X_4 = \vee).$$

Тогда расстояние между высказываниями экспертов и мера опровержимости высказываний, вычисленные по введенным формулам с учетом замечания 1 следующие:

$$\rho_1(1, 2) = 0, 039, I_1(1) = 0, 992, I_1(2) = 0, 969.$$

Если не учитывать замечание 1, а вычислять расстояние только по общим переменным, то результат получается такой: $\rho'_1(1, 2) = 0, 156$.

Если вычислять расстояние между этими мнениями экспертов по формуле, предложенной Н.Г. Загоруйко в работах [5, 6], то получается $R = 0, 18$.

3. Расстояние между вероятностными высказываниями экспертов

Как уже отмечалось, на практике эксперт обычно задает высказывание с его "вероятностью". В этом случае вопрос состоит в изучении и согласовании таких высказываний, введении некоторой метрики на таких высказываниях. Рассмотрим "знания" экспертов, представленные формулами исчисления высказываний с вероятностями (вероятностные высказывания), т. е. высказывания вида: " φ с вероятностью p_φ ", где φ — формула исчисления высказываний. Используем следующую запись для таких высказываний: $B_i = \langle \varphi, p_\varphi \rangle$, $B_j = \langle \psi, p_\psi \rangle$.

Заметим, что для этого случая используется другая σ -алгебра [2, 3], но идейно подходы похожи.

Пусть Σ — база знаний, состоящая из формул исчисления высказываний (в Σ содержатся все те формулы, которые дали эксперты), $S(\varphi)$ — носитель формулы φ , т.е. множество элементарных высказываний, используемых при написании формулы φ , и $S(\Sigma) = \bigcup_{\varphi \in \Sigma} S(\varphi)$ — носитель совокупности знаний.

Рассмотрим множество $P(S(\Sigma)) = 2^{S(\Sigma)}$ — множество всех подмножеств множества $S(\Sigma)$. Элементы множества $P(S(\Sigma))$ назовем моделями. Известно, что мощность множества $P(S(\Sigma))$ равна $2^{|S(\Sigma)|} = n$ (обозначим для простоты).

Предположим, что эксперты говорят о вероятностях формул на множестве всех моделей, и каждое высказывание присутствует только с одной вероятностью (случай, когда у высказывания не одна вероятность будет рассмотрен ниже).

Тогда интерпретируем вероятность, данную экспертом, следующим образом:

$B = \langle \varphi, p_\varphi \rangle$ означает, что высказывание φ истинно на $n_\varphi = \lfloor n \cdot p_\varphi \rfloor$ моделях, где $n = 2^{|S(\Sigma)|}$ — всего моделей.

Пусть даны два вероятностных логических высказывания $B_i = \langle \varphi, p_\varphi \rangle$ и $B_j = \langle \psi, p_\psi \rangle$, и требуется вычислить расстояние $\rho(B_i, B_j)$ между такими высказываниями.

Тогда, интерпретируя данные экспертами вероятности описанным выше способом, получаем, что высказывание φ истинно на $n_\varphi = \lfloor n \cdot p_\varphi \rfloor$ моделях, а высказывание ψ истинно на $n_\psi = \lfloor n \cdot p_\psi \rfloor$ моделях.

Отметим, однако, что неизвестно на каких именно моделях каждое высказывание истинно, а также число моделей, на которых эти высказывания истинны одновременно.

Рассмотрим следующую подзадачу. Пусть высказывание φ истинно на n_φ моделях, высказывание ψ истинно на n_ψ моделях и k — число моделей, на которых эти высказывания одновременно истинны. Требуется вычислить расстояние между высказываниями $B_i = \langle \varphi, p_\varphi \rangle$ и $B_j = \langle \psi, p_\psi \rangle$.

Возникающие в дальнейшем расстояния обозначим через $\rho_k(B_i, B_j)$, где $k = t, t+1, \dots, \min(n_\varphi, n_\psi)$, здесь и далее $t = \max(0, n_\varphi + n_\psi - n)$. Заметим, что значение k для каждой пары высказываний свое.

Как и раньше [3–4], расстояние $\rho_k(B_i, B_j)$ определим как симметрическую разность, то есть

$$\rho_k(B_i, B_j) = \frac{1}{n}(n_\varphi - k + n_\psi - k) = \frac{1}{n}(n_\varphi + n_\psi - 2k), \quad (2.1)$$

для каждого $k = t, t + 1, \dots, \min(n_\varphi, n_\psi)$.

Для расстояний $\rho_k(B_i, B_j)$ справедливы все утверждения теоремы 1. (Здесь $B_i \equiv B_j \iff \varphi \equiv \psi$ и $p_\varphi = p_\psi$, это означает, что формулы φ и ψ истинны на одних и тех же моделях.)

Предложим несколько способов вычисления расстояния $\rho(B_i, B_j)$ между вероятностными высказываниями $B_i = \langle \varphi, p_\varphi \rangle$ и $B_j = \langle \psi, p_\psi \rangle$.

Так как нам не известно число k (число моделей, на которых высказывания φ и ψ одновременно истинны), и если нет никаких предпочтений для значения k (предпочтение может быть высказано экспертами), то можем поступить следующим образом.

Предположим, что для нас все значения для числа k равновероятны. Тогда расстояние между вероятностными высказываниями $B_i = \langle \varphi, p_\varphi \rangle$ и $B_j = \langle \psi, p_\psi \rangle$ определим как усреднение расстояний $\rho_k(B_i, B_j)$ по всем значениям k , то есть

$$\rho(B_i, B_j) = \frac{\sum_{k=t}^{\min(n_\varphi, n_\psi)} \rho_k(B_i, B_j)}{\min(n_\varphi, n_\psi) + 1 - t}. \quad (2.2)$$

Для этого расстояния также справедлива теорема 1.

Если экспертами высказано, какое значение для k для пары B_i и B_j предпочтительнее, то в качестве $\rho(B_i, B_j)$ берется это $\rho_k(B_i, B_j)$, то есть

$$\rho(B_i, B_j) = \rho_k(B_i, B_j). \quad (2.3)$$

Подойдем к этому вопросу с вероятностной точки зрения: для каждого k построим вероятностную модель и вычислим вероятность того, что ровно на k моделях высказывания φ и ψ одновременно истинны.

Рассмотрим следующую задачу. Найти вероятность p_k того, что в выбранных n_φ и n_ψ моделях (выбираются из n моделей) будет ровно k моделей, на которых высказывания φ и ψ одновременно истинны, где $k = t, t + 1, \dots, \min(n_\varphi, n_\psi)$.

Сначала определим вероятностное пространство $\langle \Omega, A, p \rangle$, где Ω — пространство элементарных исходов, $\Omega = \{t, t + 1, \dots, \min(n_\varphi, n_\psi)\}$ — множество всевозможных совпадений моделей в наборах из n_φ и n_ψ моделей, A — система подмножеств множества Ω , образующая σ -алгебру событий, и p — вероятность на $\langle \Omega, A \rangle$. Определим на Ω такую случайную величину ξ что $\xi(k) = \rho_k(B_i, B_j)$.

Вероятность того, что ровно k моделей совпало в наборах из n_φ и n_ψ моделей вычисляется следующим образом:

$$p_k = \binom{n}{k} \binom{n-k}{n_\varphi-k} \binom{n-n_\varphi}{n_\psi-k} / \left\{ \binom{n}{n_\varphi} \binom{n}{n_\psi} \right\}.$$

В результате имеем $\rho_k(B_i, B_j)$ с вероятностями p_k , где $k = t, t+1, \dots, \min(n_\varphi, n_\psi)$.

Зная вероятности p_k для каждого расстояния $\rho_k(B_i, B_j)$, в качестве расстояния между вероятностными высказываниями $B_i = \langle \varphi, p_\varphi \rangle$ и $B_j = \langle \psi, p_\psi \rangle$ можно взять расстояние $\rho_k(B_i, B_j)$ с наибольшей вероятностью, то есть

$$\rho_{\max p}(B_i, B_j) = \rho_m(B_i, B_j), \quad p_m = \max_k p_k. \quad (2.4)$$

Очевидно, что для расстояния $\rho_{\max p}(B_i, B_j)$ справедливы утверждения теоремы 1.

Можно в качестве расстояния между вероятностными высказываниями $B_i = \langle \varphi, p_\varphi \rangle$ и $B_j = \langle \psi, p_\psi \rangle$ взять величину, равную математическому ожиданию или среднему значению случайной величины ξ , то есть

$$\rho(B_i, B_j) = M\xi = \sum_{k=t}^{\min(n_\varphi, n_\psi)} \rho_k(B_i, B_j) \cdot p_k. \quad (2.5)$$

Для этого расстояния $\rho(B_i, B_j)$ справедливы все утверждения теоремы 1.

В предложенных формулах (1)–(5) расстояний не учитывается вид формул, между которыми вычисляется расстояние. Поэтому естественно предложить расстояние, которое учитывает и сами формулы.

Применяя модельный подход [3–4] к элементам множества $P(S(\Sigma))$ (моделям), найдем вероятности $P(\varphi)$ и $P(\psi)$ и расстояние $\rho(\varphi, \psi)$ (модельные вероятности и расстояние). Затем по свойству, аналогичному свойству 10 теоремы 3, справедливому и для формул исчисления высказываний, вычислим $P(\varphi \wedge \psi) = \frac{1}{2}(P(\varphi) + P(\psi) - \rho(\varphi, \psi))$. Тогда можно найти число $k_0 = \lfloor n \cdot P(\varphi \wedge \psi) \rfloor$ — число моделей, на которых высказывания φ и ψ одновременно истинны.

Имея число k_0 (вычисленное по моделям), можно уменьшить число возможных значений для k . Здесь возможны 3 случая:

- 1) если $t < k_0 < \min(n_\varphi, n_\psi)$, то $k = k_0 - 1, k_0, k_0 + 1$;
- 2) если $k_0 = t$ или $k_0 = \min(n_\varphi, n_\psi)$, то, например, $k = k_0, k_0 + 1$ или $k = k_0 - 1, k_0$ соответственно;
- 3) если $k_0 > \min(n_\varphi, n_\psi)$ или $k_0 < t$, то $k = \min(n_\varphi, n_\psi)$ или $k = t$ соответственно.

И уже к этим значениям для числа k применять предложенные выше формулы (1)–(5). По необходимости возможно некоторое расширение числа значений для k .

Теперь рассмотрим случай, когда одно и то же высказывание присутствует с разными вероятностями. В этом случае предлагаем два варианта введения расстояния:

1) Пусть имеется s экспертов, которые указали вероятности $p_1, p_2, \dots, p_s$ высказывания φ . Тогда в качестве вероятности p_φ можно взять $p_\varphi = \frac{1}{s} \sum_{i=1}^s p_i$.

Проделав такую процедуру для каждого высказывания, получим, что каждое высказывание присутствует только с одной вероятностью. Далее следует уменьшить число возможных значений для k и применять формулы (1)–(5).

2) Рассмотрим r -того эксперта. Имеем высказывание φ с вероятностью p_r и высказывание ψ с вероятностью q_r , данные r -тым экспертом. Тогда вычислим расстояние $\rho(B_i, B_j)$ для r -ого эксперта как в случае высказываний с одной вероятностью. Это расстояние обозначим через $\rho^r(B_i, B_j)$. Такую процедуру проделаем с каждым из имеющихся s экспертов, а за $\rho(B_i, B_j)$ примем $\rho(B_i, B_j) = \frac{1}{s} \sum_{r=1}^s \rho^r(B_i, B_j)$.

Замечание 2. Предложенными способами можно также вычислять расстояние между следующими высказываниями: $B_i = \langle \varphi, p_{\varphi_i} \rangle$ — информация, полученная от i -го эксперта, и $B_j = \langle \varphi, p_{\varphi_j} \rangle$ — информация, полученная от j -го эксперта.

Результаты предыдущих рассуждений переносятся на формулы исчисления предикатов с вероятностями и произвольного конечного класса конечных моделей фиксированной сигнатуры. Остановимся на существенных моментах, отличающих этот случай от предыдущего.

Рассмотрим "знания" экспертов, представленные формулами исчисления предикатов с вероятностями, т. е. высказывания вида: " $\varphi(\bar{x})$ с вероятностью p_φ ", где $\varphi(\bar{x})$ — формула исчисления предикатов. Используем следующую запись для таких высказываний: $B_i = \langle \varphi(\bar{x}), p_\varphi \rangle$, $B_j = \langle \psi(\bar{x}), p_\psi \rangle$.

Напомним, что $\Omega = \{P_1^{m_1}, \dots, P_t^{m_t}\}$ — сигнатура, $X = \{x_1, \dots, x_p\}$ — множество переменных, $D_{x_1}, \dots, D_{x_p}$ — конечные множества возможных значений переменных, s — число экспертов. Каждый эксперт "задает" свою интерпретацию каждого предикатного символа сигнатуры Ω соответствующим отношением с приписанной ему вероятностью, т. е. "знания" i -го эксперта могут быть записаны в виде: $\langle P_1^i(\bar{x}), p_1^i \rangle, \dots, \langle P_t^i(\bar{x}), p_t^i \rangle$. $\{M_i\}_{i=1}^s$ — исходное множество моделей. Высказывания экспертов могут быть представлены и формулами исчисления предикатов данной сигнатуры.

Зададим для простоты расстояние между предикатами P_l и P_j . Для этого сначала вычислим расстояние между вероятностными интерпретациями $B_l^i = \langle P_l^i(\bar{x}), p_l^i \rangle$ и $B_j^i = \langle P_j^i(\bar{x}), p_j^i \rangle$ предикатов в каждой модели M_i . Расстояния вычисляются между предикатами одинаковой местности и от одних и тех же переменных (см. замечание 1).

"Знание" $B_l^i = \langle P_l^i(x_1, \dots, x_p), p_l^i \rangle$ означает, что предикат $P_l^i(x_1, \dots, x_p)$ ис-

истинен на $n_{P_l^i} = \lfloor n \cdot p_l^i \rfloor$ кортежах длины p в модели M_i , где $n = \prod_{j=1}^p |D_{x_j}|$.

Аналогично случаю исчисления высказываний пусть предикат $P_l^i(\bar{x})$ истинен на $n_{P_l^i}$ кортежах в модели M_i , предикат $P_j^i(\bar{x})$ истинен на $n_{P_j^i}$ кортежах в модели M_i и k^i — число кортежей, на которых эти предикаты одновременно истинны, где $k^i = t, t+1, \dots, \min(n_{P_l^i}, n_{P_j^i})$, $t = \max(0, n_{P_l^i} + n_{P_j^i} - n)$. Значение k^i для каждой пары предикатов свое. Тогда для каждого k^i расстояние $\rho_{k^i}(B_l^i, B_j^i)$ зададим формулой

$$\rho_{k^i}(B_l^i, B_j^i) = \frac{1}{n}(n_{P_l^i} + n_{P_j^i} - 2k^i).$$

Для расстояний $\rho_{k^i}(B_l^i, B_j^i)$ справедливы все утверждения теоремы 1.

Применяя модельный подход [3–4] и теорему 3, вычислим вероятности $P_{M_i}(P_l^i)$, $P_{M_i}(P_j^i)$ и расстояние $\rho_{M_i}(P_l^i, P_j^i)$ в модели M_i , затем вычислим вероятность $P_{M_i}(P_l^i \wedge P_j^i)$ и найдем число $k_0^i = \lfloor P_{M_i}(P_l^i \wedge P_j^i) \cdot n \rfloor$ — число кортежей, на которых предикаты одновременно истинны, вычисленное по моделям.

Далее поступаем как в случае исчисления высказываний: в каждой модели M_i вычислим расстояния $\rho^i(B_l^i, B_j^i)$ с учетом вероятностей и уменьшенного числа значений для k^i , и в качестве $\rho(P_l, P_j)$ возьмем величину

$$\rho(P_l, P_j) = \frac{1}{s} \sum_{i=1}^s \rho^i(B_l^i, B_j^i). \quad (2.6)$$

Для расстояния $\rho(P_l, P_j)$ также справедлив аналог теоремы 1.

Таким же образом вводится расстояние между двумя формулами языка первого порядка с вероятностями.

Мера опровержимости формул с вероятностями (в случае исчисления высказываний и в случае языка первого порядка) вводится так же, как в пункте 2, то есть

$$I(\varphi) = \rho(\varphi, 1),$$

где 1 — тождественно истинная формула, а ρ — одно из введенных по формулам (2)–(6) расстояний на вероятностных высказываниях.

Для так введенных мер опровержимости справедливы все свойства теоремы 2, доказанные нами для формул исчисления высказываний и формул исчисления предикатов с использованием исходного конечного класса моделей.

Приведем один из тестовых примеров для формул исчисления предикатов.

Пример 3. Рассмотрим высказывания экспертов, приведенные в примере 1, но с приписанной экспертами вероятностью (вероятностные высказывания).

1-ый эксперт:

$$\begin{aligned} P_1^1(x_1, x_2) &= \iff [(x_1 = \vee \vee) \wedge (x_2 = 42 \vee 43 \vee 44 \vee 45)], \text{ вероятность } p_1^1 = 0,5. \\ P_2^1(x_1, x_2) &= \iff [(x_1 = \vee \vee) \wedge (x_2 = 41 \vee 42 \vee 43 \vee 44)], \text{ вероятность } p_2^1 = 0,7. \end{aligned}$$

2-ой эксперт:

$$P_1^2(x_1, x_2) = \iff [(x_1 =) \wedge (x_2 = 44 \vee 45)], \text{ вероятность } p_1^2 = 0, 8.$$

$$P_2^2(x_1, x_2) = \iff [(x_1 = \vee \vee) \wedge (x_2 = 43 \vee 44 \vee 45)], \text{ вероятность } p_2^2 = 0, 6.$$

3-ий эксперт:

$$P_1^3(x_1, x_2) = \iff [(x_1 = \vee)], \text{ вероятность } p_1^3 = 0, 6.$$

$$P_2^3(x_1, x_2) = \iff [(x_1 = \vee) \wedge (x_2 = 41 \vee 43 \vee 45)], \text{ вероятность } p_2^3 = 0, 7.$$

Вычислим расстояние между вероятностными высказываниями экспертов, выраженными предикатами P_1 и P_2 , и меры их опровержимости.

В модели M_1 первого эксперта имеем:

$n_{P_1^1} = 10$; $n_{P_2^1} = 14$; $k^1 = 4, \dots, 10$; $P^1(P_1^1 \wedge P_2^1) = 0, 3$; тогда $k_0^1 = 6$ и, следовательно, $k^1 = 5, 6, 7$; $\rho_5^1(P_1^1, P_2^1) = 0, 7$; $\rho_6^1(P_1^1, P_2^1) = 0, 6$; $\rho_7^1(P_1^1, P_2^1) = 0, 5$; тогда расстояние $\rho^1(P_1^1, P_2^1) = 0, 6$ и меры опровержимости $I^1(P_1^1) = 0, 5$ и $I^1(P_2^1) = 0, 3$.

В модели M_2 второго эксперта имеем:

$n_{P_1^2} = 16$; $n_{P_2^2} = 12$; $k^2 = 8, \dots, 12$; $P^2(P_1^2 \wedge P_2^2) = 0, 1$; тогда $k_0^2 = 2$ и, следовательно, $k^2 = 8$; $\rho_8^2(P_1^2, P_2^2) = 0, 6$; тогда расстояние $\rho^2(P_1^2, P_2^2) = 0, 6$ и меры опровержимости $I^2(P_1^2) = 0, 2$ и $I^2(P_2^2) = 0, 4$.

В модели M_3 третьего эксперта имеем:

$n_{P_1^3} = 12$; $n_{P_2^3} = 14$; $k^3 = 6, \dots, 12$; $P^3(P_1^3 \wedge P_2^3) = 0, 15$; тогда $k_0^3 = 3$ и, следовательно, $k^3 = 6$; $\rho_6^3(P_1^3, P_2^3) = 0, 7$; тогда расстояние $\rho^3(P_1^3, P_2^3) = 0, 7$ и меры опровержимости $I^3(P_1^3) = 0, 4$ и $I^3(P_2^3) = 0, 3$.

Усредняя, получаем расстояние $\rho(P_1, P_2) = 0, 6333$ и меры опровержимости $I(P_1) = 0, 3667$ и $I(P_2) = 0, 3333$.

Пример 4. Под руководством Г.С. Лбова решалась задача из области археологии в рамках интеграционного проекта "Компьютерная система для анализа антропологической информации". В.Б. Бериковым и Т.И. Лучшевой независимо были получены закономерности, характеризующие антропологические промеры черепов той или иной определенной эпохи. В анализируемый антропометрический комплекс входили 21 непрерывных переменных, представляющие собой важнейшие метрики, дифференцирующие основные расы и их локальные варианты. Множество рассматриваемых объектов (черепов) было разбито на 24 образа, отвечающих той или иной культуре.

Для хорошей кластеризации (таксономии) множества объектов и хорошего распознавания образов желательно, чтобы расстояние между своими представителями каждого кластера были малыми, а расстояния до представителей других кластеров по возможности большими.

Для примера рассмотрим полученные закономерности для двух кластеров.

Закономерности для 1-го образа (кластера):

1. (X1 [165; 188.50]) (X3 [123.50; 134.05]) (X4 [93.50; 103.25])
(X8 [68.94; 86]) (X11 [24.95; 32]) (X14 [19.95; 25.20])
(X15 [2.04; 3.84]) (X20 [83.80; 89.15]).
2. (X3 [123.50; 134.05]) (X8 [68.94; 86]) (X10 [28.75; 36.25])

(X11 [24.95; 32]) (X15 [2.04; 3.84]) (X16 [5.14; 9.14])
 (X18 [140.89; 150.44]) (X20 [83.80; 89.15]).
 3. (X3 [123.50; 134.05]) (X8 [68.94; 86]) (X11 [24.95; 32])
 (X13 [8.94; 12.14]) (X15 [2.04; 3.84]) (X16 [5.14; 9.14])
 (X19 [124.84; 143.14]) (X20 [83.80; 89.15]).

Закономерности для 2-го кластера:

4. (X1 [174.50; 188.50]) (X3 [125.50; 139.50]) (X12 [53.90; 58.09])
 (X14 [19.45; 23.34]) (X17 [78.75; 92.50]) (X20 [84.90; 90.15])
 (X21 [20.89; 34]).
 5. (X9 [40.84; 46.04]) (X12 [53.90; 58.09]) (X14 [19.45; 23.34])
 (X17 [78.75; 92.50]) (X18 [137.10; 153.85]) (X19 [127.90; 146.39])
 (X20 [84.90; 90.15]) (X21 [20.89; 34]).
 6. (X7 [125.50; 148.50]) (X8 [69.90; 82.34]) (X9 [40.84; 46.04])
 (X12 [53.90; 58.09]) (X14 [19.45; 23.34]) (X17 [78.75; 92.50])
 (X20 [84.90; 90.15]) (X21 [20.89; 34]).

Расстояния между закономерностями 1-го кластера, вычисленные по предложенным нами формулам следующие:

$$\rho(1, 2) = 0,0006643; \rho(1, 3) = 0,0007205; \rho(2, 3) = 0,0006942.$$

Расстояния между закономерностями 2-го кластера соответственно следующие:

$$\rho(4, 5) = 0,0006458; \rho(4, 6) = 0,0006411; \rho(5, 6) = 0,0007238.$$

И расстояния между закономерностями из разных кластеров:

$$\begin{aligned} \rho(1, 4) &= 0,0095527; \rho(1, 5) = 0,0381027; \rho(1, 6) = 0,0270584; \\ \rho(2, 4) &= 0,0644439; \rho(2, 5) = 0,0810485; \rho(2, 6) = 0,0825482; \\ \rho(3, 4) &= 0,0645001; \rho(3, 5) = 0,0971838; \rho(3, 6) = 0,0826044. \end{aligned}$$

Если вычислить меру информативности (опровержимости) каждой закономерности, то получаем следующие результаты:

$$I(1) = 0,999655; I(2) = 0,999681; I(3) = 0,999625; I(4) = 0,999718; I(5) = 0,999636; I(6) = 0,99964.$$

Оценим диаметр каждого кластера через среднее расстояние между всеми парами представителей одного кластера. Получаем, что $diam_1 = 0,007207$ и $diam_2 = 0,007239$. И оценим расстояние между кластерами (разнесенность кластеров) через среднее расстояние между всеми парами представителей из разных кластеров. Получаем, что $\rho_{1,2} = 0,0606527$.

Аналогичные результаты характерны и для всех остальных кластеров и закономерностей.

Таким образом, введенное в работе расстояние позволяет посмотреть на закономерности с точки зрения близости. Результаты говорят о том, что эти закономерности обладают высокой информативностью, и полученные кластеры образуют "компактные" сгустки [5], что говорит о хорошей кластеризации закономерностей.

Заключение

Рассмотрены логические высказывания экспертов, представленные формулами исчисления высказываний и формулами языка первого порядка. Предложен некоторый общий подход с использованием конечного класса моделей с метрикой и его модификаций для вычисления естественных расстояний с учетом "удаленности" формул друг от друга в моделях с метрикой, мер информативности, вероятностей формул и установления свойств, которым должны удовлетворять расстояния и мера информативности. Рассмотрена также задача введения хороших расстояний на множестве вероятностных формул. Для предложенных расстояний справедливы важные свойства метрики и ее связи с мерой опровержимости.

Авторы благодарят Г.С. Лбова за постоянное внимание к работе и Л.Н. Кореневу за активное участие в этой работе и проверке приведенных примеров.

Литература

1. Блощицын В.Я., Лбов Г.С. О мерах информативности логических высказываний. // Доклады Республиканской Школы-Семинара "Технология разработки экспертных систем". Кишинев, 1978. С.12-14.
2. Лбов Г.С., Старцева Н.Г. Логические решающие функции и вопросы статистической устойчивости решений. Новосибирск: Изд-во Института математики, 1999.
3. Викентьев А.А., Викентев Р.А. Метрика и информативность на знаниях экспертов на классе конечных моделей // Математические и информационные технологии в энергетике, экономике, экологии ч.2, Иркутск-2003, с.194-199
4. Vikent'ev A.A., Lbov G.S. Setting the metric and informativeness on statements of experts // Pattern Recognition and Image Analysis. 1997. V. 7, N. 2. P. 175–189.
5. Vikent'ev A.A., Koreneva L.N. Setting the metric and measures of informativity in predicate formulas corresponding to the statements of experts about hierarchical objects// Pattern Recognition and Image Analysis. 2000. V. 10, N. 3. P.303–308.
6. Загоруйко Н.Г. Прикладные методы анализа данных и знаний. Новосибирск: Изд-во Института математики, 1999.
7. Загоруйко Н.Г., Бушуев М.В. Меры расстояния в пространстве знаний.// Анализ данных в экспертных системах. Новосибирск, 1986. Вып. 117: Вычислительные системы. С. 24-35.

8. Ершов Ю.Л., Палютин Е.А. Математическая логика. М.: Наука, 1991.
9. Gaifman H. Concerning measures in the first order calculi. // Israel Math. 1964. V. 2, N. 1. P. 1 -18.

АЛГОРИТМ ТОЧНОЙ МИНИМИЗАЦИИ БУЛЕВЫХ ФУНКЦИЙ В КЛАССЕ КРОНЕКЕРОВЫХ ФОРМ

Винокуров С.Ф.

Рябец Л.В.

Иркутский
Государственный
Педагогический
Университет

e-mail: vin@math.isu.ru

Иркутский
Государственный
Университет

e-mail: lev_lv@mailru.com

1. Обозначения и определения

Изложение результатов удобно вести на операторном языке. В этом случае кронекерovy формы являются частным случаем операторных форм булевых функций.

В работе используются следующие обозначения:

- $\oplus, \sum$ — сложение по модулю 2;
- через $\tilde{x}$ обозначается набор переменных $(x_1, \dots, x_n)$, $\tilde{\alpha}$ — набор констант $(\alpha_1, \dots, \alpha_n)$, длины наборов n определяются по контексту;
- $f_{x_i}^\alpha(\tilde{x}) = f(x_1, \dots, x_{i-1}, \alpha, x_{i+1}, \dots, x_n)$ — остаточная функция от функции $f(\tilde{x})$ по переменной x_i ;
- $f'_{x_i}(\tilde{x}) = f_{x_i}^0(\tilde{x}) \oplus f_{x_i}^1(\tilde{x})$ — производная функции $f(\tilde{x})$ по переменной x_i ;
- $x^\alpha = \begin{cases} \bar{x}, & \alpha = 0; \\ x, & \alpha = 1. \end{cases}$
- символ f означает тоже самое, что и $f(x_1, \dots, x_n)$;
- конец доказательства — символ $\square$.

Оператор $\mathbf{t}$ представляется как последовательность $\mathbf{t}_1 \dots \mathbf{t}_n$, где $\mathbf{t}_i \in \{\mathbf{d}, \mathbf{e}, \mathbf{p}\}$, n — размерность оператора. Действие оператора $\mathbf{t}$ на функцию $g(\tilde{x})$ определяется по правилу $\mathbf{t}g(\tilde{x}) = g_n(\tilde{x})$, где $g_0(\tilde{x}) = g(\tilde{x})$ и

$$g_i(\tilde{x}) = \begin{cases} g_{i-1}(\tilde{x}) & , \text{ если } \mathbf{t}_i = \mathbf{e}; \\ g_{i-1}(x_1, \dots, x_{i-1}, \bar{x}_i, x_{i+1}, \dots, x_n) & , \text{ если } \mathbf{t}_i = \mathbf{p}; \\ (g_{i-1}(\tilde{x}))'_{x_i} & , \text{ если } \mathbf{t}_i = \mathbf{d}. \end{cases}$$

Упорядоченный набор $(\mathbf{t}^{\bar{0}}, \dots, \mathbf{t}^{\bar{\tau}}, \dots, \mathbf{t}^{\bar{1}})$, состоящий из 2^n операторов, действующих по переменным $(x_1, \dots, x_n)$, называется *пучком операторов* или

операторным пучком. В пучке все операторы имеют одну размерность, длина или количество операторов пучка всегда связана с этой размерностью. А именно, длина пучка операторов размерности n всегда равна 2^n .

Пучок $(\mathbf{b}_{\tilde{x}}^{\bar{0}}, \dots, \mathbf{b}_{\tilde{x}}^{\tilde{\tau}}, \dots, \mathbf{b}_{\tilde{x}}^{\bar{1}})$ операторов размерности n будет называться базисным, если существует функция $g(\tilde{x})$ такая, что ее операторные образы $\{\mathbf{b}_{\tilde{x}}^{\bar{0}}g(\tilde{x}), \dots, \mathbf{b}_{\tilde{x}}^{\bar{1}}g(\tilde{x})\}$ образуют базис линейного пространства всех булевых функций от n переменных. Соответственно, функция $g(\tilde{x})$ будет называться базисной.

Свойства таких операторов и операторных пучков подробно рассмотрены в [1].

Пучок операторов $\mathbf{A} = (\mathbf{a}^{\bar{0}}, \dots, \mathbf{a}^{\tilde{\tau}}, \dots, \mathbf{a}^{\bar{1}})$ будем называть двупорожденным, если существуют такие операторы $\mathbf{b} = \mathbf{b}_0 \dots \mathbf{b}_n$ и $\mathbf{c} = \mathbf{c}_0 \dots \mathbf{c}_n$, $\mathbf{b}_i \neq \mathbf{c}_i$ для любого i , что оператор $\mathbf{a}^{\tilde{\tau}} = \mathbf{t}_1 \dots \mathbf{t}_n$ пучка A определяется следующим образом:

$$\mathbf{t}_i = \begin{cases} \mathbf{b}_i, & \text{если } \tau_i = 0, \\ \mathbf{c}_i, & \text{если } \tau_i = 1. \end{cases}$$

Непосредственно на операторах можно ввести частичную операцию "сложение". Для этой операции также будет использоваться символ " $\oplus$ ":

$\mathbf{c} = \mathbf{a} \oplus \mathbf{b}$ тогда и только тогда, когда для любой функции $f(\tilde{x})$ имеет место равенство:

$$\mathbf{c}f(\tilde{x}) = \mathbf{a}f(\tilde{x}) \oplus \mathbf{b}f(\tilde{x}).$$

Операция определена на парах операторов, отличающихся только по одной компоненте. Пусть $\mathbf{a} = \mathbf{a}_1 \dots \mathbf{a}_n$ и $\mathbf{b} = \mathbf{b}_1 \dots \mathbf{b}_n$ — два оператора, отличающиеся в позиции с номером s . Результат такой операции выглядит так:

$$\mathbf{a}_1 \dots \mathbf{a}_n \oplus \mathbf{b}_1 \dots \mathbf{b}_n = \mathbf{c}_1 \dots \mathbf{c}_n,$$

где $\mathbf{c}_i = \mathbf{a}_i$ для $i \neq s$; $\mathbf{c}_i \neq \mathbf{a}_i$ и $\mathbf{c}_i \neq \mathbf{b}_i$ для $i = s$.

Для изложения результатов нам необходима следующая теорема из [2].

Теорема 1 [2]. Для любого оператора $\mathbf{b}$ существует единственный (с точностью до перенумерации операторов) двупорожденный пучок операторов $\mathbf{A} = (\mathbf{a}^{\bar{0}}, \dots, \mathbf{a}^{\tilde{\tau}}, \dots, \mathbf{a}^{\bar{1}})$, такой что имеет место равенство:

$$\mathbf{b} = \sum_{\tilde{\tau}} \mathbf{a}^{\tilde{\tau}},$$

размерности оператора $\mathbf{b}$ и операторов из пучка $\mathbf{A}$ совпадают.

Эта теорема позволяет ввести новое операторное представление.

Пусть $(\mathbf{b}^1, \dots, \mathbf{b}^t)$ — набор операторов размерности n . Выражение

$$f(x_1, \dots, x_n) = \sum_{i=1}^t \mathbf{b}^i g(x_1, \dots, x_n) \quad (1)$$

будет называться операторной формой (OF) функции $f(x_1, \dots, x_n)$ по функции $g(x_1, \dots, x_n)$. Операторная форма называется редуцированной, если в ней нет одинаковых слагаемых. Очевидно, что любую операторную форму можно редуцировать, проведя сокращение пар совпадающих слагаемых. Заметим, что если операторы $\mathbf{b}^1, \dots, \mathbf{b}^t$ — из базисного пучка $\mathbf{B}$, то для любой функции существует единственная операторная форма, которую будем называть операторной формой функции f по пучку $\mathbf{B}$.

Пусть $R(OF)$ обозначает операцию приведения операторной формы OF к редуцированной форме.

По теореме 1 для любого оператора $\mathbf{b}^i$ из (1) найдется двупорожденный пучок операторов $\mathbf{A}_i = (\mathbf{a}^{\bar{0},i}, \dots, \mathbf{a}^{\bar{1},i})$, что имеет место равенство:

$$\mathbf{b}^i = \sum_{\bar{\tau}} \mathbf{a}^{\bar{\tau},i}.$$

В равенстве (1) каждый оператор можно заменить на соответствующую сумму и полученное выражение редуцировать. После редуцирования для функции $f(x_1, \dots, x_n)$ получается выражение:

$$f(x_1, \dots, x_n) = R \left(\sum_{i=1}^t \sum_{\bar{\tau}} \mathbf{a}^{\bar{\tau},i} (g(x_1, \dots, x_n)) \right). \quad (2)$$

Это представление функции $f(x_1, \dots, x_n)$ будет называться специальной операторной формой этой функции по функции $g(x_1, \dots, x_n)$ и обозначаться $SOF_g f(x_1, \dots, x_n)$.

Определение. $SOF_g f(x_1, \dots, x_n)$ представима в классе $\mathbf{K}$ двупорожденных операторных пучков, если существуют $\mathbf{A}_1, \dots, \mathbf{A}_s \in \mathbf{K}$, $\mathbf{A}_i = (\mathbf{a}^{\bar{0},i}, \dots, \mathbf{a}^{\bar{1},i})$ что имеет место равенство

$$SOF_g f(x_1, \dots, x_n) = R \left(\sum_{i=1}^s \sum_{\bar{\tau}} \mathbf{a}^{\bar{\tau},i} g(x_1, \dots, x_n) \right). \quad (3)$$

Определение. Минимальное s , для которого выполняется (3), будем называть сложностью специальной операторной формы $SOF_g f(x_1, \dots, x_n)$ в классе $\mathbf{K}$ и обозначать $|SOF_g(f)|^K$.

Определение. Под сложностью представления $L_g^{OF}(f)$ функции $f(x_1, \dots, x_n)$ операторной формой OF по функции $g(x_1, \dots, x_n)$ понимается число слагаемых в OF .

Если операторная форма построена по пучку $\mathbf{B}$, то сложность представления будет обозначаться $L_g^{\mathbf{B}}(f)$.

Определение. Пусть $\mathbf{K}$ класс операторных пучков. Тогда $L_g^K(f) = \min_{\mathbf{B} \in \mathbf{K}} |L_g^{\mathbf{B}}(f)|$ называют сложностью функции $f(x_1, \dots, x_n)$ в классе операторных форм $\mathbf{K}$ по функции $g(x_1, \dots, x_n)$.

Пусть $\mathbf{b}$ оператор и $K_{\mathbf{b}} = \{\mathbf{A}_1, \dots, \mathbf{A}_N\}$ класс всех двупорожденных операторных пучков

$$\mathbf{A}_i = (\mathbf{a}^{\tilde{0},i}, \dots, \mathbf{a}^{\tilde{1},i})$$

таких что операторы $\mathbf{a}^{\tilde{0},i}$ равняются $\mathbf{b}$.

Среди классов $K_{\mathbf{b}}$ находится класс всех поляризованных полиномов Жегалкина. Этот класс получается при $\mathbf{b} = \mathbf{ddd}$ и все составляющие его пучки представлены в списке:

- 1) (ddd, dde, ded, dee, edd, ede, eed, eee);
- 2) (ddd, ddp, ded, dep, edd, edp, eed, eep);
- 3) (ddd, dde, dpd, dpe, edd, ede, epd, epe);
- 4) (ddd, ddp, dpd, dpp, edd, edp, epd, epp);
- 5) (ddd, dde, ded, dee, pdd, pde, ped, pee);
- 6) (ddd, ddp, ded, dep, pdd, pdp, ped, pep);
- 7) (ddd, dde, dpd, dpe, pdd, pde, ppd, ppe);
- 8) (ddd, ddp, dpd, dpp, pdd, pdp, ped, ppp).

В этом списке первый пучок порождает полином Жегалкина при $g(x_1, x_2, x_3) = x_1 \cdot x_2 \cdot x_3$.

2. Свойства SOF

Свойства специальной операторной формы, необходимые для построения алгоритма, изложены в следующих трех теоремах.

Теорема 2. Сложность представления $SOF_g(f)$ в классе $K_{\mathbf{b}}$ равняется мощности множества $\{SOF_g(f)\} \cap \{\mathbf{a}^{\tilde{1},1}, \dots, \mathbf{a}^{\tilde{1},N}\}$, где $\{SOF_g(f)\}$ множество слагаемых в $SOF_g(f)$

$$|SOF_g(f)|^{K_{\mathbf{b}}} = \text{card}(\{SOF_g(f)\} \cap \{\mathbf{a}^{\tilde{1},1}, \dots, \mathbf{a}^{\tilde{1},N}\}).$$

Доказательство. Рассмотрим операторы $\mathbf{a} = \mathbf{a}_1 \dots \mathbf{a}_n$, $\mathbf{b} = \mathbf{b}_1 \dots \mathbf{b}_n$, $\mathbf{c} = \mathbf{c}_1 \dots \mathbf{c}_n$ такие что $\mathbf{a}_i \neq \mathbf{b}_i$, $\mathbf{a}_i \neq \mathbf{c}_i$, $\mathbf{b}_i \neq \mathbf{c}_i$ для любого i . За $\mathbf{q}^{\tilde{\tau}}$ обозначим оператор $\mathbf{q}_1 \dots \mathbf{q}_n$ такой что

$$\mathbf{q}_i = \begin{cases} \mathbf{a}_i & \text{if } \tau_i = 0 \\ \mathbf{b}_i & \text{if } \tau_i = 1 \end{cases}$$

Согласно определению положим

$$\mathbf{Q} = (\mathbf{q}^{\tilde{0}}, \dots, \mathbf{q}^{\tilde{\tau}}, \dots, \mathbf{q}^{\tilde{1}}).$$

По построению $\mathbf{Q}$ — двупорожденный операторный пучок. Из этого следует, что существует операторная форма

$$f(\tilde{x}) = \sum_{\tilde{\tau}} \alpha_{\tilde{\tau}} \cdot \mathbf{q}^{\tilde{\tau}}(g(\tilde{x})). \quad (4)$$

За $\mathbf{A}_{\tilde{\tau}}$ обозначим двупорожденный операторный пучок $(\mathbf{a}^{\tilde{0}}, \dots, \mathbf{a}^{\tilde{1}})$, где $\mathbf{a}^{\tilde{0}} = \mathbf{b}$ и $\mathbf{a}^{\tilde{1}} = \mathbf{q}^{\tilde{\tau}}$. Согласно Теореме 1, имеем следующее представление:

$$\mathbf{q}^{\tilde{\tau}} = \sum_{\tilde{\sigma}} \mathbf{a}^{\tilde{\sigma}}, \quad (5)$$

где $(\mathbf{a}^{\tilde{0}}, \dots, \mathbf{a}^{\tilde{\sigma}}, \dots, \mathbf{a}^{\tilde{1}}) = \mathbf{A}_{\tilde{\tau}}$.

Пусть множество $\{\mathbf{A}_1, \dots, \mathbf{A}_k\}$ является множеством всех пучков $\mathbf{A}_{\tilde{\tau}}$ таких, что $\alpha_{\tilde{\tau}} = 1$ в (4). Обозначим за $(\mathbf{a}^{\tilde{0},i}, \dots, \mathbf{a}^{\tilde{\tau},i}, \dots, \mathbf{a}^{\tilde{1},i})$ операторы из $\mathbf{A}_i$.

Подставив (5) для $\mathbf{q}^{\tilde{\tau}}$ в (4), получим

$$f(\tilde{x}) = \sum_{i=1}^k \sum_{\tilde{\tau}} \mathbf{a}^{\tilde{\tau},i}(g(\tilde{x})). \quad (6)$$

Итак,

$$SOF_g(f) = R \left(\sum_{i=1}^k \sum_{\tilde{\tau}} \mathbf{c}^{\tilde{\tau},i}(g) \right).$$

По построению, $\mathbf{a}^{\tilde{1},i} \neq \mathbf{a}^{\tilde{\tau},i}$ если $\tilde{\tau} \neq \tilde{1}$ и $i \neq j$. Отсюда следует, что $\mathbf{a}^{\tilde{1},i}$ входят слагаемыми в $SOF_g(f)$.

Окончательно, $\mathbf{a}^{\tilde{1},i}$ присутствуют в $SOF_g(f)$ тогда и только тогда, когда соответствующее $\alpha_{\tilde{\tau}}$ равняется 1 в (4) для соответствующего $\tilde{\tau}$.

□

Определение. На операторах $\mathbf{a} = \mathbf{a}_1 \dots \mathbf{a}_n$ и $\mathbf{b} = \mathbf{b}_1 \dots \mathbf{b}_n$ можно определить функционал "о" следующим образом:

$$\mathbf{a} \circ \mathbf{b} = \begin{cases} 1, & \text{если } \mathbf{a}_i \neq \mathbf{b}_i \text{ для любого } i \in \{1, \dots, n\}; \\ 0, & \text{иначе.} \end{cases}$$

В дальнейшем такой функционал будем называть произведением операторов.

Следующая несложная теорема позволяет упростить вычисления, связанные с нахождением пересечения в Теореме 2.

Теорема 3. Если $\mathbf{a} \in (\{SOF_g(f)\} \cap \{a^{\tilde{1},1}, \dots, a^{\tilde{1},N}\})$, тогда $\mathbf{a} \circ \mathbf{b} = 1$.

Доказательство. Если $\mathbf{a} \in (\{SOF_g(f)\} \cap \{a^{\tilde{1},1}, \dots, a^{\tilde{1},N}\})$, то $\mathbf{a} \in \mathbf{a}^{\tilde{1},i}$ для некоторого i . Тогда в классе $K_{\mathbf{b}}$ имеется пучок $\mathbf{B}^i = (\mathbf{b}^{\tilde{0}}, \dots, \mathbf{b}^{\tilde{1}})$, что $\mathbf{b}^{\tilde{0}} = \mathbf{b}$, $\mathbf{b}^{\tilde{1}} = \mathbf{a}$. тсюда следует, что $\mathbf{a} \circ \mathbf{b} = 1$.

□

Следующая теорема позволяет связать сложность представления SOF в классе со сложностью самой функции.

Теорема 4. Пусть $\mathbf{H}$ класс всех двупорожденных операторных пучков. Тогда для любой булевой функции найдется оператор $\mathbf{b}$ такой, что

$$L_g^H(f) = |SOF_g|^K \mathbf{b}.$$

Доказательство. Положим $L(f) = s$. Пусть

$$\mathbf{A} = (\mathbf{a}^{\tilde{0}}, \dots, \mathbf{a}^{\tilde{\sigma}}, \dots, \mathbf{a}^{\tilde{1}})$$

двупорожденный операторный пучок такой, что функция $f(x_1, \dots, x_n)$ имеет минимальное представление:

$$f(x_1, \dots, x_n) = \bigoplus_{i=1}^s \mathbf{a}^i g(x_1, \dots, x_n) \quad (7)$$

Рассмотрим класс $K_{\mathbf{b}}$, где оператор $\mathbf{b} = \mathbf{b}_1 \dots \mathbf{b}_n$ построен следующим образом

$$\mathbf{b}_i \neq (\mathbf{a}^{\tilde{0}})_i, \mathbf{b}_i \neq (\mathbf{a}^{\tilde{1}})_i,$$

где $(\mathbf{a}^{\tilde{0}})_i$ — i -я компонента оператора $\mathbf{a}^{\tilde{0}}$, $(\mathbf{a}^{\tilde{1}})_i$ — i -я компонента оператора $\mathbf{a}^{\tilde{1}}$. Для двупорожденных пучков такое построение всегда возможно.

По Теореме 1 для каждого оператора $\mathbf{a}^i$ из (7) существует двупорожденный пучок $\mathbf{B}^i = (\mathbf{b}^{\tilde{0},i}, \dots, \mathbf{b}^{\tilde{1},i})$ такой что имеется представление $\mathbf{a}^i = \bigoplus_{\tilde{\tau}} \mathbf{b}^{\tilde{\tau},i}$ и $SOF(f)$ имеет вид

$$SOF_g(f) = R \left(\bigoplus_{i=1}^s \bigoplus_{\tilde{\tau}} \mathbf{b}^{\tilde{\tau},i}(g) \right).$$

Нетрудно заметить, что оператор $\mathbf{b}$ входит в каждый пучок $\mathbf{B}^i$.

Пусть $\mathbf{b} = \mathbf{b}^{\tilde{\tau},i}$. По пучку $\mathbf{B}^i$ строим пучок $\mathbf{C} = (\mathbf{c}^{\tilde{0}}, \dots, \mathbf{c}^{\tilde{\sigma}}, \dots, \mathbf{c}^{\tilde{1}})$ являющийся перестановкой операторов пучка $\mathbf{B}^i$ по правилу:

$$\mathbf{c}^{\sigma \oplus \tau} = \mathbf{b}^{\tau}.$$

Легко видеть, что $\mathbf{C} \in K_{\mathbf{b}}$, причем

$$R \left(\bigoplus_{i=1}^s \bigoplus_{\tilde{\tau}} \mathbf{c}^{\tilde{\tau},i}(g) \right) = R \left(\bigoplus_{i=1}^s \bigoplus_{\tilde{\tau}} \mathbf{b}^{\tilde{\tau},i}(g) \right) = SOF_g(f).$$

Это равенство показывает, что $SOF_g(f)$ имеет представление в классе $K_{\mathbf{b}}$ и, следовательно,

$$L_g^H(f) = |SOF_g|^K \mathbf{b}$$

□

3. Алгоритм получения сложности SOF_g в классах $K_{\mathbf{b}}$

Алгоритм нахождения $|SOF(f)_g|^{K_{\mathbf{b}}}$ непосредственно дает Теорема 2. Для этого необходимо построить $SOF(f)_g$ и все пучки, входящие в $K_{\mathbf{b}}$. Далее достаточно найти пересечение множества всех операторов, входящих в $SOF(f)_g$ и множества, состоящего из операторов, имеющих в самый большой номер — $\tilde{1}$ в некотором пучке их класса $K_{\mathbf{b}}$. Считается, что оператор $\mathbf{b}$ имеет самый маленький номер — $\tilde{0}$.

Теорема 3 позволяет нахождение $|SOF_g(f)|^{K_{\mathbf{b}}}$ свести к формуле

$$|SOF_g(f)|^{K_{\mathbf{b}}} = \sum_{\mathbf{a} \in \{SOF_g(f)\}} \mathbf{a} \circ \mathbf{b}.$$

Алгоритм нахождения $|SOF_g(f)|^{K_{\mathbf{b}}}$ предыдущего пункта позволяет работать с любой базисной функцией $g(x_1, \dots, x_n)$. Однако можно заметить, что $|SOF_g(f)|^{K_{\mathbf{b}}}$ зависит от базисной функции $g(x_1, \dots, x_n)$ только в той мере, в какой зависит вхождение того или иного слагаемого в $SOF_g(f)$. Более того, в задаче нахождения минимального представления используются не сами слагаемые, а только операторы, их порождающие. Поэтому, если символ базисной функции g в записи отсутствует, считается, что $g(x_1, \dots, x_n) = x_1 \cdot \dots \cdot x_n$.

Формально алгоритм можно записать следующим образом.

Алгоритм 1. Вычисление сложности $|SOF_g(f)|^{K_{\mathbf{b}}}$

```
Function Complexity (sof, b) {
  vars
  i: integer;
  comp: integer;
  a: operator;
  sofsz: //Количество слагаемых в SOF
  comp ← 0;
  for i ← 1 to sofsz do
  {
    return_next(sof, a);
    comp ← comp+a*b;
  }
  return comp;
}
```

Замечание. Таким образом, например, вычисление сложности булевой функции f в классе поляризованных полиномов Жегалкина линейно относительно длины специальной операторной формы этой функции.

4. Алгоритм нахождения минимальной сложности функций в кронекеровских формах

Необходимо заметить, что при базисной функции $g(x_1, \dots, x_n) = x_1 \cdots x_n$ класс H всех двупорожденных пучков операторов порождает класс широко известных кронекеровых форм.

В этом разделе примеры рассматриваются при $g(x_1, \dots, x_n) = x_1 \cdots x_n$, в обозначениях символ g опущен.

Обычно кронекеровы формы записывают в виде кронекерова произведения трех видов базисов $[\bar{x}, x]$, $[1, x]$, $[1, \bar{x}]$. Теорема 4 позволяет свести нахождение минимальной сложности функций в кронекеровских формах к вычислению минимальной сложности $SOF(f)$ в классах $K_{\mathbf{b}}$. То есть фактически нам нужно найти такой класс, в котором сложность $SOF(f)$ будет минимальной.

Суть алгоритма заключается в следующем. Пусть нам требуется минимизировать функцию $f(x_1, \dots, x_n)$. Для этого находим $SOF(f)$ и строим матрицу принадлежности, строки и столбцы которой составляют все возможные операторы от n переменных. Матрица принадлежности на основании Теоремы 3 показывает, может ли оператор, стоящий в столбце, принадлежать пучку, порожденному оператором из строки матрицы. Элементами этой матрицы являются произведения соответствующих операторов. Затем из множества столбцов операторов выбираем те, которые принадлежат $SOF(f)$. Тогда каждая строка будет иметь свой вес, являющийся суммой выбранных элементов этой строки. Минимальный из всех этих весов и будет минимумом сложности f в данном классе, порожденным соответствующим оператором.

Пример. Переобозначим символы: $\mathbf{p} = 0, \mathbf{e} = 1, \mathbf{d} = 2$. Теперь оператор, как последовательность трех цифр, можно представить числом в троичной системе счисления. Все операторы естественным образом упорядочиваются.

Матрица принадлежности для $n = 3$ представлена на таблице 1.

Составим для функции (10111111) $SOF(f)$ и выберем входящие в нее столбцы (В таблице они отмечены знаком "+"). Столбец W представляет собой вектор весов во всех классах.

Таблица 1

	000	001	002	010	011	012	020	021	022	100	101	102	110	111	112	120	121	122	200	201	202	210	211	212	220	221	222	W
000	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	1	0	0	0	1	1	0	1	1	5
001	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	1	0	0	0	1	0	1	0	1	7
002	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	0	0	0	1	1	0	1	0	4	
010	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	1	1	0	1	0	1	0	0	1	1	1	3	
011	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	1	0	1	1	0	1	0	0	1	0	1	5	
012	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	0	1	1	0	0	0	1	1	0	4	
020	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	0	0	0	0	1	1	0	1	0	0	0	4	
021	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	0	0	0	1	0	1	1	0	1	0	0	4	
022	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	0	0	0	1	1	0	1	1	0	0	0	4	
100	0	0	0	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	3	
101	0	0	0	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	5	
102	0	0	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	4	
110	0	1	1	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	2	
111	1	0	1	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	1	0	1	3	
112	1	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	3	
120	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	0	3	
121	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	0	0	4	
122	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	0	0	5	
200	0	0	0	0	1	1	0	1	1	0	0	0	1	1	0	1	1	1	0	0	0	0	0	0	0	0	4	
201	0	0	0	1	0	1	1	0	1	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	4	
202	0	0	0	1	1	0	1	1	0	0	0	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	4	
210	0	1	1	0	0	0	0	1	1	0	1	1	0	0	0	1	1	0	1	0	0	0	0	0	0	0	3	
211	1	0	1	0	0	0	1	0	1	1	0	1	0	0	0	1	0	1	0	0	0	0	0	0	0	0	4	
212	1	1	0	0	0	0	1	1	0	1	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	5	
220	0	1	1	0	1	1	0	0	0	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	5	
221	1	0	1	1	0	1	0	0	0	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	4	
222	1	1	0	1	1	0	0	0	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	7	
	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	

Из таблицы видно, что минимум функции равен 2 в классе $K_{\text{сеп}}$. Формально алгоритм можно записать следующим образом.

Алгоритм 2. Вычисление минимальной сложности функции

```

Function Minimization (sof) {
  vars
  i, j: integer;
  min, sum: integer;
  a, b, min_class: operator;
  sofsizе: //Количество слагаемых в SOF
  for i ← 0 to  $3^n$  do
  {
    convert_operator(a ← i);
    sum ← 0;
    for j ← 1 to sofsizе do
    {
      return_next(sof, b);
      sum ← sum+a*b;
    }
    if (sum<min){min ← sum; min_class ← a;}
  }
  return min, min_class;
}

```

Алгоритм 2 может быть значительно улучшен, если воспользоваться одним из свойств матрицы принадлежности. Если, сохраняя новые обозначения, составить столбцы и строки матрицы в естественном порядке, то в ней обнаружится четко выраженная структура.

Матрица принадлежности

Рисунок представляет собой полную матрицу принадлежности, на котором черными квадратиками обозначены произведения операторов, равные 1. На нем видно, что полная матрица для функций n переменных является одной девятой матрицы для функций $n + 1$ переменных. Тогда представляется возможность хранить полную матрицу для функции k переменных и в процессе работы программы разворачивать ее до требуемого размера (возвращаться к ней) для получения произведения операторов функции n переменных при $n > k$.

Алгоритм 3. Вычисление минимальной сложности функции с использованием матрицы принадлежности

```
Function Minimization_Save (sof) {
  vars
  i, j: integer;
  min, sum: integer;
  a, b, min_class: operator; // Операторы размерности  $n$ 
  c, d: operator; // Операторы размерности  $k$ 
  e, f: operator; // Операторы размерности  $n - k$ 
  sofsize; // Количество слагаемых в SOF
  matrix: array; // Матрица принадлежности для функций  $k$  переменных
  for i ← 0 to  $3^n$  do
  {
    convert_operator(a ← i);
    sum ← 0;
    for j ← 1 to sofsize do
    {
      return_next(sof, b);
      c, e ← a;
      d, f ← b;
      if (e*f=1)
      {sum ← sum+matrix[c,d]; }
    }
    if (sum<min){min ← sum; min_class ← a;}
  }
  return min, min_class;
}
```

На основании предложенного алгоритма была написана программа на языке программирования C++. Она позволяет находить минимум сложности функции от 16 переменных в кронекеровском базисе.

Литература

1. Избранные вопросы теории булевых функций // Под ред. Винокурова С.Ф. и Перязева Н.А.– М.: ФИЗМАТЛИТ, 2001.–192с.– ISBN 5-9221-0085-8.
2. Steinbach, B., Mishchenko, A.: SNF: A Special Normal Form for ESOPs. Proceedings of the 5th International Workshop on Application of the Reed-Muller Expansion in Circuit Design (RM 2001), August 10 - 11, 2001. Mississippi State University, Starkville (Mississippi) USA, pp. 66–81.

ВЕРХНЯЯ ОЦЕНКА СЛОЖНОСТИ БУЛЕВЫХ ФУНКЦИЙ В КЛАССЕ ПНФ

Винокуров С.Ф.

Казимиров А.С.

Иркутский
Государственный
Педагогический
Университет

e-mail: vin@math.isu.ru

Иркутский
Государственный
Университет

e-mail: cybrid@rambler.ru

В работе рассматривается сложность $L(n)$ представления булевых функций в классе полиномиальных нормальных форм. Показано, что для любой функции 7 переменных минимальная ПНФ содержит не более 28 слагаемых. Из этого результата следует, что $L(n) \leq \frac{7}{32}2^n$ при $n \geq 7$.

Полиномиальной нормальной формой (ПНФ) функции f называется ее представление в виде суммы по модулю 2:

$$f(x_1, \dots, x_n) = K_1 \oplus \dots \oplus K_s, \quad (1)$$

в которое в качестве слагаемых входят произведения $K_i = z_1 \cdot \dots \cdot z_{k_i}$, где $z_j = x_t$ или $z_j = \bar{x}_t$ для некоторой переменной x_t , причем переменная может входить в произведение не более одного раза. В сумму может входить K_i , не содержащее ни одной переменной. Такое K_i считается равным 1.

Для функции f представление (1) не единственно. Поэтому естественно рассмотреть сложность представления (1) функции $f(x_1, \dots, x_n)$ как s — число слагаемых.

Сложность $L(f)$ функции $f(x_1, \dots, x_n)$ определяется как сложность минимального представления этой функции.

Сложность $L(n)$ класса F_n всех булевых функций от n -переменных определяется так:

$$L(n) = \max_{f \in F_n} L(f)$$

ПНФ удобно рассматривать как частный случай операторной формы.

Для дальнейшего изложения нам потребуются следующие обозначения:

$$\tilde{x} = x_1, \dots, x_n; \tilde{\alpha} = \alpha_1, \dots, \alpha_n;$$

$$x^\alpha = \begin{cases} x & , \text{ если } \alpha = 1, \\ \bar{x} & , \text{ если } \alpha = 0; \end{cases}$$

$$\begin{aligned} f_{x_i}^0 &= f(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n); \\ f_{x_i}^1 &= f(x_1, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n); \\ f_{x_i}' &= f_{x_i}^0 \oplus f_{x_i}^1. \end{aligned}$$

Если в записи функции отсутствуют переменные, то предполагается, что ее переменными являются $x_1, \dots, x_n$.

Оператор $\mathbf{t}$ представляется последовательностью $\mathbf{t}_1 \dots \mathbf{t}_n$, где $\mathbf{t}_i \in \{\mathbf{d}, \mathbf{e}, \mathbf{p}\}$, n — размерность оператора. Действие оператора $\mathbf{t}$ на функцию $g(\tilde{x})$ определяется по правилу $\mathbf{t}g(\tilde{x}) = g_n(\tilde{x})$, где $g_0(\tilde{x}) = g(\tilde{x})$ и

$$g_i(\tilde{x}) = \begin{cases} g_{i-1}(\tilde{x}) & , \text{ если } \mathbf{t}_i = \mathbf{e} \\ g_{i-1}(x_1, \dots, x_{i-1}, \bar{x}_i, x_{i+1}, \dots, x_n) & , \text{ если } \mathbf{t}_i = \mathbf{p} \\ (g_{i-1}(\tilde{x}))'_{x_i} & , \text{ если } \mathbf{t}_i = \mathbf{d}. \end{cases}$$

Пример.

$$\begin{aligned} \mathbf{drep}(x_1 \vee x_2 \vee x_3 \vee x_4) &= (x_1 \vee \bar{x}_2 \vee x_3 \vee \bar{x}_4)'_{x_1} = \overline{\bar{x}_2 \vee x_3 \vee \bar{x}_4} \\ \mathbf{drep}(x_1 \cdot x_2 \cdot x_3 \cdot x_4) &= \bar{x}_2 \cdot x_3 \cdot \bar{x}_4 \\ f(x_1, x_2, x_3) &= 1 \oplus \bar{x}_1 \bar{x}_2 \oplus x_1 x_2 x_3 = \mathbf{ddd}(x_1 \cdot x_2 \cdot x_3) \oplus \mathbf{dpp}(x_1 \cdot x_2 \cdot x_3) \oplus \\ &\mathbf{eee}(x_1 \cdot x_2 \cdot x_3) \end{aligned}$$

Теперь представление (1) может быть записано в виде

$$f(x_1, \dots, x_n) = \sum_{i=1}^s \mathbf{a}^i(x_1 \cdot \dots \cdot x_n),$$

где $\mathbf{a}^i$ — соответствующие операторы.

На множестве операторов размерности n определим отображение φ следующим образом.

Пусть P — группа подстановок на множестве $\{\mathbf{d}, \mathbf{e}, \mathbf{p}\}$:

$$P = \left\{ \begin{pmatrix} \mathbf{dep} \\ \mathbf{dep} \end{pmatrix}, \begin{pmatrix} \mathbf{dep} \\ \mathbf{dpe} \end{pmatrix}, \begin{pmatrix} \mathbf{dep} \\ \mathbf{edp} \end{pmatrix}, \begin{pmatrix} \mathbf{dep} \\ \mathbf{epd} \end{pmatrix}, \begin{pmatrix} \mathbf{dep} \\ \mathbf{pde} \end{pmatrix}, \begin{pmatrix} \mathbf{dep} \\ \mathbf{ped} \end{pmatrix} \right\}.$$

Пусть φ — последовательность $\varphi_1 \varphi_2 \dots \varphi_n$, где $\varphi_i \in P$. Тогда отображение φ действует на оператор $\mathbf{a}_1 \dots \mathbf{a}_n$ так:

$$\varphi(\mathbf{a}_1 \dots \mathbf{a}_n) = \varphi_1(\mathbf{a}_1) \dots \varphi_n(\mathbf{a}_n).$$

Отображение φ операторов продолжается на множество функций. Если имеется операторное представление $f(x_1, \dots, x_n) = \sum_{i=1}^s \mathbf{a}^i(x_1 \cdot \dots \cdot x_n)$, то

$$\varphi(f) = \sum_{i=1}^s \varphi(\mathbf{a}^i)(x_1 \cdot \dots \cdot x_n) \quad (2)$$

Отображение (2) функций называется ОР-отображением. Очевидно, что ОР-отображения обратимы.

Пример.

$$\begin{aligned}
 \varphi &= \varphi_1 \varphi_2 \varphi_3 = \begin{pmatrix} \mathbf{dep} \\ \mathbf{dep} \end{pmatrix} \begin{pmatrix} \mathbf{dep} \\ \mathbf{dpe} \end{pmatrix} \begin{pmatrix} \mathbf{dep} \\ \mathbf{dep} \end{pmatrix}. \\
 f(x_1, x_2, x_3) &= 1 \oplus \bar{x}_1 \bar{x}_2 \oplus x_1 x_2 x_3 \\
 \varphi(f) &= \varphi(1) \oplus \varphi(\bar{x}_1 \bar{x}_2) \oplus \varphi(x_1 x_2 x_3) = \\
 &= \varphi(\mathbf{ddd}(x_1 \cdot x_2 \cdot x_3)) \oplus \varphi(\mathbf{dpp}(x_1 \cdot x_2 \cdot x_3)) \oplus \varphi(\mathbf{eee}(x_1 \cdot x_2 \cdot x_3)) = \\
 &= \varphi_1(\mathbf{d}) \varphi_2(\mathbf{d}) \varphi_3(\mathbf{d}) x_1 \cdot x_2 \cdot x_3 \oplus \varphi_1(\mathbf{d}) \varphi_2(\mathbf{p}) \varphi_3(\mathbf{p}) x_1 \cdot x_2 \cdot x_3 \oplus \varphi_1(\mathbf{e}) \varphi_2(\mathbf{e}) \varphi_3(\mathbf{e}) x_1 \cdot \\
 &x_2 \cdot x_3 = \\
 &= \mathbf{ddd}(x_1 \cdot x_2 \cdot x_3) \oplus \mathbf{dep}(x_1 \cdot x_2 \cdot x_3) \oplus \mathbf{epe}(x_1 \cdot x_2 \cdot x_3) = 1 \oplus x_2 \bar{x}_3 \oplus x_1 \bar{x}_2 x_3
 \end{aligned}$$

Определение. Функции f и g называются ОР-эквивалентными, если существует ОР-отображение φ , что $g = \varphi(f)$, и N-эквивалентными, если $\varphi = \varphi_1 \dots \varphi_n$, $\varphi_i \in P_1$, где $P_1 \subset P$:

$$P_1 = \left\{ \begin{pmatrix} \mathbf{dep} \\ \mathbf{dep} \end{pmatrix}, \begin{pmatrix} \mathbf{dep} \\ \mathbf{dpe} \end{pmatrix} \right\}.$$

Можно заметить, что N-эквивалентность соответствует расстановке отрицаний над переменными, т.е. N-эквивалентные функции выглядят так:

$$g(x_1, \dots, x_n) = f(x_1^{\alpha_1}, \dots, x_n^{\alpha_n}), \quad \alpha_i \in \{0, 1\}.$$

Теорема 1. Если $f(x_1, \dots, x_n)$ и $g(x_1, \dots, x_n)$ — ОР-эквивалентны, то $L(f) = L(g)$.

Доказательство. Пусть $f(x_1, \dots, x_n)$ и $g(x_1, \dots, x_n)$ — ОР-эквивалентны и

$$f(x_1, \dots, x_n) = \bigvee_{i=1}^t \mathbf{b}^i(x_1 \cdot \dots \cdot x_n)$$

является минимальной операторной формой функции f .

Тогда $g(x_1, \dots, x_n)$ имеет представление

$$g(x_1, \dots, x_n) = \bigvee_{i=1}^t \varphi(\mathbf{b}^i)(x_1 \cdot \dots \cdot x_n). \quad (3)$$

Откуда следует, что $L(g) \leq L(f)$. Предположим, что функция g имеет операторную форму:

$$g(x_1, \dots, x_n) = \bigvee_{j=1}^s \mathbf{a}^j(x_1 \cdot \dots \cdot x_n), \quad (4)$$

в которой $s < t$.

Поскольку (3) и (4) — операторные формы одной функции, имеем:

$$\sum_{i=1}^t \varphi(\mathbf{b}_i)(x_1 \cdots x_n) = \sum_{j=1}^s \mathbf{a}^j(x_1 \cdots x_n).$$

Обозначим через ψ обратное отображение к φ . Имеет место следующая цепочка равенств:

$$\begin{aligned} \psi\left(\sum_{i=1}^t \varphi(\mathbf{b}^i)(x_1 \cdots x_n)\right) &= \psi\left(\sum_{j=1}^s \mathbf{a}^j(x_1 \cdots x_n)\right) = \psi(g) = \\ &= \sum_{i=1}^t \psi(\varphi(\mathbf{b}^i))(x_1 \cdots x_n) = \sum_{i=1}^t \mathbf{b}^i(x_1 \cdots x_n) = f = \sum_{i=1}^s \psi(\mathbf{a}^i)(x_1 \cdots x_n). \end{aligned}$$

Откуда следует, что $L(f) \leq s < t$. Значит, $L(f) = L(g)$.

□

Компьютерными вычислениями [2,3] получены следующие результаты (которые проверены и дополнены в п.5) авторами):

1. $L(5) = 9$.
2. $L(6) = 15$.
3. Если $L(f(x_1, \dots, x_6)) = 15$, тогда f является N-эквивалентной функции $s_1 = hex(7EE9E997E997977E)$ или N-эквивалентной функции $s_2 = hex(E997977E977E7EE9)$, где функции записаны в виде шестнадцатеричного вектора: 7=0111, E=1101, 9=1001.
4. s_1 и s_2 — симметрические функции.
5. Функции s_1 и s_2 — ОР-эквивалентны.

Теорема 2. $L(7) \leq 28$.

Доказательство. Для любой функции n переменных имеется представление через функции $n - 1$ переменной:

$$f(x_1, \dots, x_n, x_{n+1}) = \bar{x}_{n+1}f_{x_{n+1}}^0 \oplus x_{n+1}f_{x_{n+1}}^1 \quad (5)$$

Из этого представления следует:

$$L(n) \leq 2L(n - 1).$$

Для $n = 7$ получаем $L(7) \leq 2L(6) = 2 \cdot 15 = 30$.

I. Пусть $L(7) = 30$. Заметим, что это возможно только в случае (с точностью до N-эквивалентности), когда функция f имеет вид:

$$f(x_1, \dots, x_7) = \bar{x}_7 s_k(x_1, \dots, x_6) \oplus x_7 s_l(x_1^{\alpha_1}, \dots, x_6^{\alpha_6}); k, l \in \{1, 2\}.$$

Очевидно, что в наборе $(\alpha_1, \dots, \alpha_6)$ найдутся две одинаковые компоненты. Пусть $\alpha_1 = \alpha_2$. Поскольку функция s_l — симметрическая, то функция $s_l(x_1^{\alpha_1}, \dots, x_6^{\alpha_6})$ — симметрична по переменным x_1 и x_2 . Откуда следует, что функция $f(x_1, \dots, x_7)$ также симметрична по x_1, x_2 . Тогда для функции f имеется представление

$$f(x_1, \dots, x_7) = \bar{x}_1 \bar{x}_2 (f_{x_1 x_2}^{00} \oplus f_{x_1 x_2}^{01}) \oplus x_1 x_2 (f_{x_1 x_2}^{10} \oplus f_{x_1 x_2}^{11}) \oplus f_{x_1 x_2}^{01}.$$

Из этого разложения следует, что

$$L(f) \leq 3 \cdot L(5) = 27.$$

II. Пусть $L(7) = 29$. В этом случае для разложения (5) можно считать, что $L(f_{x_7}^0) = 14$ и $L(f_{x_7}^1) = 15$.

Рассмотрим $f'_{x_7}(x_1, \dots, x_7)$. Возможны два случая:

1. $L(f'_{x_7}) = 15$. Построим функцию $g(x_1, \dots, x_7) = \bar{x}_7 f'_{x_7} \oplus x_7 f_{x_7}^1$. Для этой функции верно предыдущее рассуждение из п. I, согласно которому $L(g) \leq 27$. Функции f и g — ОР-эквивалентны, так как:

$$f = \bar{x}_7 f_{x_7}^0 \oplus x_7 f_{x_7}^1, g = \bar{x}_7 f'_{x_7} \oplus x_7 f_{x_7}^1 = \bar{x}_7 f_{x_7}^0 \oplus 1 \cdot f_{x_7}^1;$$

$$\varphi(f) = g, \quad \varphi = \varphi_1 \dots \varphi_7$$

$$\varphi_i = \begin{pmatrix} \text{dep} \\ \text{dep} \end{pmatrix}, i = \overline{1, 6}; \varphi_7 = \begin{pmatrix} \text{dep} \\ \text{edp} \end{pmatrix}.$$

По теореме 1 получаем:

$$L(f) = L(g) \leq 27.$$

2. $L(f'_{x_7}) \leq 14$. В этом случае функция $g(x_1, \dots, x_7) = \bar{x}_7 f_{x_7}^0 \oplus x_7 f'_{x_7}$, также ОР-эквивалентна f . Сложность функции g удовлетворяет неравенству:

$$L(g) \leq L(f_{x_7}^0) \oplus L(f'_{x_7}) \leq 14 + 14 = 28.$$

Окончательно получаем $L(7) \leq 28$.

□

Следствие. $L(n) \leq \frac{7}{32} 2^n, n \geq 7$.

Замечание. В [4] получена верхняя оценка на $L(n)$, которая имеет вид:

$$L(n) \leq 2^{\frac{\log_2 n + 1}{n}} \cdot 2^n.$$

Можно заметить, что неравенство:

$$2^{\frac{\log_2 n + 1}{n}} \cdot 2^n < \frac{7}{32}$$

выполняется при $n \geq 65$. Тогда следствие можно переформулировать так:
 $L(n) \leq \frac{7}{32}2^n, 7 \leq n \leq 64$.

Литература

1. Избранные вопросы теории булевых функций // Под ред. Винокурова С.Ф. и Перязева Н.А. – М.: ФИЗМАТЛИТ, 2001. – 192 с.
2. Gaidukov A. Algorithm to derive minimum ESOP for 6-variable function // 5th International Workshop on Boolean Problems. Freiberg, Germany, 2002. – P.141–148.
3. Koda N., Sasao T. An Upper Bound on the Number of Products in Minimum ESOPs // Workshop in Application of the Reed-Muller Expansion Application in Curcuit Design, Japan, 1995. – P.94–101.
4. Кириченко К.Д. Верхняя оценка функции Шеннона сложности полиномиальных форм булевых функций. // Методы оптимизации и их приложения. Труды XII Байкальской международной конференции. – Иркутск, 2001 – Том 5. Дискретная математика. – С. 66–70.

ОПИСАНИЕ СИЛЬНО СУБМИНИМАЛЬНЫХ АЛГЕБРАИЧЕСКИХ СИСТЕМ

Д. Ю. Власов

Институт математики СО РАН

Россия, 630090,

Новосибирск, пр. Коптюга 4

1 Введение

Данная работа является продолжением работ [3] и [4]. В статье [3] описываются алгебраические системы конечной предикатной сигнатуры с единственной полной теорией бесконечных подсистем. Было доказано, что все предикаты в таких системы выражаются бескванторными формулами либо через равенство, либо через линейный порядок по типу ω на носителе системы (ясно, что в этом случае система должна быть счётной). В [4], кроме основного результата данной работы, также анонсирован результат о строении алгебраических систем с конечным множеством теорий бесконечных подсистем. В соответствии с этим результатом, все алгебраические системы конечной предикативной сигнатуры с конечным множеством теорий бесконечных подсистем также описываются в терминах бескванторной выразимости через равенство или некоторый линейный порядок некоторого простого типа и конечное множество констант.

В данной работе получены результаты, позволяющие описать класс систем, очень близкий к классу систем с конечным множеством типов бесконечных подсистем в терминах суббранга и субстепени - ординалов, характеризующих сложность предложений в алгебраической системе по их выполнимости на некоторых подсистемах в данной системе. Оказалось, что класс сильно субминимальных алгебраических систем конечной предикатной сигнатуры (то есть минимально возможного суббранга и субстепени для данного класса) совпадает с классом мономорфных систем с конечным множеством теорий бесконечных подсистем. Таким образом, открывается возможность продолжить описание подобных систем для некоторых фиксированных значений суббранга и субстепени.

2 Определение субранга и субстепени

Определение. Пусть $\mathfrak{A}$ - некоторая алгебраическая система сигнатуры Σ , $\phi \in S(\Sigma)$ - некоторое предложение сигнатуры Σ . Обозначим через $\mathfrak{A}(\phi)$ множество всех подсистем $\mathfrak{B}$, на которых истинно предложение ϕ : $\mathfrak{A}(\phi) = \{\mathfrak{B} \subseteq \mathfrak{A} \mid \mathfrak{B} \models \phi\}$.

Если для некоторого предложения ϕ множество $\mathfrak{A}(\phi)$ непусто, то предложение ϕ называется субвыполнимым (субсовместным) в системе $\mathfrak{A}$.

Заметим, что если мы рассмотрим множество $\{\mathfrak{A}(\phi) \mid \phi \in S(\Sigma(\mathfrak{A}))\}$, то оно очевидно будет замкнуто относительно теоретико-множественных булевых операций, то есть по отношению к ним оно будет образовывать булеву алгебру:

$$SB(\mathfrak{A}) = \langle \{\mathfrak{A}(\phi) \mid \phi \in S(\Sigma(\mathfrak{A}))\}, \cup, \cap, -, \emptyset, \mathfrak{A} \rangle$$

Для некоторой заданной алгебраической системы $\mathfrak{A}$ сигнатуры Σ на множестве предложений сигнатуры Σ определим следующую эквивалентность: если $\phi, \psi \in S(\Sigma)$, то $\phi \equiv_{\mathfrak{A}}^{sub} \psi$ тогда и только тогда, когда $\mathfrak{A}(\phi) = \mathfrak{A}(\psi)$, $[\phi]_{\mathfrak{A}}^{sub}$ будет обозначать класс эквивалентности предложения ϕ .

Очевидно, что тогда

$$SB(\mathfrak{A}) \cong \langle S(\Sigma) / \equiv_{\mathfrak{A}}^{sub}, \vee, \wedge, \neg, 0, 1 \rangle.$$

Определение. Пусть $\mathfrak{A}$ - некоторая алгебраическая система сигнатуры Σ , $\phi \in S(\Sigma)$ - некоторое предложение сигнатуры Σ . Определим субранг $sr_{\mathfrak{A}}(\phi) \in On \cup \{\infty, -1\}$ этого предложения в системе $\mathfrak{A}$ следующим образом:

- если предложение ϕ не субвыполнимо в системе $\mathfrak{A}$, то положим $sr_{\mathfrak{A}}(\phi) = -1$.
- если предложение ϕ субвыполнимо в системе $\mathfrak{A}$, то $sr_{\mathfrak{A}}(\phi) \geq 0$.
- если $\alpha = \beta + 1$ (непределельный ординал), то $sr_{\mathfrak{A}}(\phi) \geq \alpha$ тогда и только тогда, когда существует счётное множество попарно субнесовместных в $\mathfrak{A}$ предложений $\psi_i, i < \omega$ таких, что $sr_{\mathfrak{A}}(\phi \wedge \psi_i) \geq \beta$ для всех $i < \omega$.
- если α - предельный ординал, то $sr_{\mathfrak{A}}(\phi) \geq \alpha$ тогда и только тогда, когда $sr_{\mathfrak{A}}(\phi) \geq \beta$ для всех ординалов $\beta < \alpha$.

Положим $sr_{\mathfrak{A}}(\phi) = \alpha$ если $sr_{\mathfrak{A}}(\phi) \geq \alpha$, но $sr_{\mathfrak{A}}(\phi) \not\geq \alpha + 1$.

Если же $sr_{\mathfrak{A}}(\phi) \geq \alpha$ для всех ординалов, то $sr_{\mathfrak{A}}(\phi) = \infty$. Будем считать, что $\infty > \alpha$ для всех ординалов $\alpha \in On$.

В дальнейшем, если понятно, о какой системе идёт речь, индекс $\mathfrak{A}$ в обозначении для ранга будет опускаться.

Лемма 1. Зафиксируем некоторую алгебраическую систему $\mathfrak{A}$ сигнатуры Σ и два предложения $\phi, \psi \in S(\Sigma)$. Тогда:

- если $\mathfrak{A}(\phi) \subseteq \mathfrak{A}(\psi)$, то $sr(\phi) \leq sr(\psi)$. В частности, для любого предложения χ , $sr(\phi \wedge \chi) \leq \min\{sr(\phi), sr(\chi)\}$.
- если $sr(\phi) \geq \alpha$ и $\alpha \geq \beta$, то $sr(\phi) \geq \beta$.
- $sr(\phi \vee \psi) = \max\{sr(\phi), sr(\psi)\}$

Доказательство. Доказательство ведётся трансфинитной индукцией по определению суббранга.

Докажем первое утверждение. Для этого достаточно показать, что если $\mathfrak{A}(\phi) \subseteq \mathfrak{A}(\psi)$, то для любого ординала α , если $sr(\phi) \geq \alpha$, то $sr(\psi) \geq \alpha$.

- Если $\alpha = 0$, то $sr(\phi) \geq \alpha$ означает субвыполнимость ϕ на некоторой подсистеме $\mathfrak{B} \in \mathfrak{A}(\phi) \subseteq \mathfrak{A}(\psi)$, то есть ψ тоже субвыполнима, а значит $sr(\psi) \geq \alpha$.
- Пусть $\alpha = \beta + 1$ - неопредельный ординал. Тогда $sr(\phi) \geq \alpha$ означает, что существует бесконечное множество попарно субнесовместных предложений $\psi_i, i < \omega$ таких, что $sr(\phi \wedge \psi_i) \geq \beta$ для всех $i < \omega$. Заметим, что $\mathfrak{A}(\phi \wedge \psi_i) \subseteq \mathfrak{A}(\psi \wedge \psi_i)$ для всех $i < \omega$. Но тогда, по индукционному предположению, $sr(\psi \wedge \psi_i) \geq \beta$ для всех $i < \omega$, а значит $sr(\psi) \geq \alpha$.
- Если α - предельный ординал и $sr(\phi) \geq \alpha$, то $sr(\phi) \geq \beta$ для всех $\beta < \alpha$, тогда по индукционной гипотезе сразу $sr(\psi) \geq \beta$ для всех $\beta < \alpha$, а значит $sr(\psi) \geq \alpha$.

Докажем второе утверждение.

- Для $\alpha = 0$ утверждение тривиально.
- Если α - предельный ординал, то по определению суббранга сразу получаем, что $sr(\phi) \geq \beta$.
- Если же $\alpha = \gamma + 1$ (неопредельный ординал), то существует бесконечное множество попарно субнесовместных предложений $\psi_i, i < \omega$ таких, что $sr(\phi \wedge \psi_i) \geq \gamma$ для всех $i < \omega$. Но тогда, по индукционному предположению, $sr(\phi \wedge \psi_i) \geq \delta$ для всех $i < \omega$, и $\delta \leq \gamma$. Если ординал γ - предельный, то по первому пункту $\delta \leq sr(\phi \wedge \psi_i) \leq sr(\phi)$, то есть $sr(\phi) \geq \gamma$. Если же $\gamma = \delta + 1$, то поскольку $sr(\psi \wedge \psi_i) \geq \delta$ для всех $i < \omega$, то опять же $sr(\phi) \geq \gamma$.

Поскольку можно считать $\beta < \alpha$, то $\beta \leq \gamma$, и поскольку $sr(\phi) \geq \gamma, \gamma \geq \beta$, то по индукционной гипотезе $sr(\phi) \geq \beta$.

Теперь докажем третье утверждение. Из первого пункта ясно, что $sr(\phi \vee \psi) \geq \max\{sr(\phi), sr(\psi)\}$. Требуется показать обратное неравенство. Предположим противное, то есть что для некоторого ординала α_0 выполнено $sr(\phi \vee \psi) \geq$

α_0 , но $sr(\phi) \not\geq \alpha_0$ и $sr(\psi) \not\geq \alpha_0$. Пусть α_0 - наименьший такой ординал для всех пар ϕ и ψ .

Заметим, что $\alpha_0 \neq 0$, поскольку из субвыполнимости $\phi \vee \psi$ очевидно следует субвыполнимость либо ϕ либо ψ .

Если α_0 - предельный ординал, то по определению суббранга, $sr(\phi \vee \psi) \geq \beta$ для всех $\beta < \alpha_0$. В силу минимальности α_0 для каждого ординала $\beta < \alpha_0$ одно из предложений $\theta_\beta \in \{\phi, \psi\}$ будет иметь суббранг не менее β : $sr(\theta_\beta) \geq \beta$. Разложим ординал α на две части: $\alpha_0 = X \cup Y$

$$X = \{\beta < \alpha_0 \mid \theta_\beta = \phi\} \text{ и}$$

$$Y = \{\beta < \alpha_0 \mid \theta_\beta = \psi\}.$$

Тогда одно из множеств - X или Y будет конфинально в α_0 . Для определённости пусть X - конфинально в α_0 . Но тогда для каждого ординала $\beta < \alpha_0$ найдётся такой $\alpha_0 > \beta' \geq \beta$, что $\beta' \in X$, то есть $sr(\phi) \geq \beta'$. Тогда по второму утверждению $sr(\phi) \geq \beta$. По определению суббранга на предельных ординалах, в этом случае $sr(\phi) \geq \alpha_0$ - противоречие с исходным предположением.

Рассмотрим теперь случай, когда ординал $\alpha_0 = \beta + 1$ - не предельный. Тогда существует такая счётная последовательность попарно субнесовместных предложений $\psi_i, i < \omega$, что $sr((\phi \wedge \psi_i) \vee (\psi \wedge \psi_i)) \geq \beta$ для всех $i < \omega$. В силу минимальности α_0 , тогда для каждого $i < \omega$ либо $sr(\phi \wedge \psi_i) \geq \beta$ либо $sr(\psi \wedge \psi_i) \geq \beta$. Ясно, что тогда одно из множеств

$$X = \{i < \omega \mid sr(\phi \wedge \psi_i) \geq \beta\} \text{ и}$$

$$Y = \{i < \omega \mid sr(\psi \wedge \psi_i) \geq \beta\} - \text{бесконечно.}$$

Пусть, для определённости, бесконечно множество X . Но тогда $sr(\phi) \geq \beta + 1 = \alpha_0$ - опять противоречие с выбором α_0 $\square$

Предложение. Пусть задана некоторая система $\mathfrak{A}$ сигнатуры Σ и дано предложение $\phi \in S(\Sigma)$. Тогда если $sr(\phi) = \alpha < \infty$, то существует такое число $d \in \omega$, что для любой последовательности попарно субнесовместных предложений $\psi_i, i < \omega$, существует число $i \leq d + 1$, для которого $sr(\phi \wedge \psi_i) < \alpha$.

Наименьшее такое число назовём субстепенью предложения ϕ и будем обозначать через $sd_{\mathfrak{A}}(\phi)$ (или просто $sd(\phi)$, когда ясно, о какой системе идёт речь).

Доказательство. Предположим, что это не так, и для некоторого предложения ϕ такого числа не существует, то есть для любого k существует такая последовательность предложений $\psi_j^k, 0 < i \leq k$, что $sr(\phi \wedge \psi_j^k) \geq \alpha$ для всех $k < \omega, 0 < j \leq k$.

Во-первых мы можем считать, что $\psi_j^k \wedge \phi \equiv \psi_j^k$. Во-вторых, добавив при необходимости в качестве ψ_0^k предложение $\phi \wedge \neg \left(\bigvee_{0 < j \leq k} \psi_j^k \right)$, мы для каждого k получим разбиение исходного предложения ϕ . Стоит отметить, что на $sr(\psi_0^k)$ налагаемое условие (равенство α) автоматически не распространяется.

Покажем, что для любого $m < \omega$ существует такой индекс $i^* \leq m$, что для предложения $\psi_{i^*}^m$ данное предложение не выполняется. Зафиксируем некоторый индекс m .

Заметим, что для любого индекса $k < \omega$ и любого $0 < j \leq k$ существует такое число $i_j^k \leq m$, что $sr(\psi_j^k \wedge \psi_{i_j^k}^m) \geq \alpha$. Действительно, очевидно, что $\psi_j^k \equiv \bigvee_{i \leq m} \psi_j^k \wedge \psi_i^m$. Поскольку $sr(\psi_j^k) = \alpha$ то по свойствам субранга (лемма 1) $sr(\psi_j^k) = \max\{sr(\psi_j^k \wedge \psi_i^m) | i \leq m\}$, а значит найдётся такое число $i_j^k \leq m$, что $sr(\psi_j^k \wedge \psi_{i_j^k}^m) = \alpha$.

Заметим, что для любого $k \geq m$ существует такой индекс $i_k \leq m$, что $|\{j | i_j^k = i_k\}| \geq \lfloor \frac{k}{m} \rfloor$. Тогда для некоторого $i^* \leq m$ найдётся бесконечное множество индексов $V \subseteq \omega$ такое, что для всех индексов $k \in V$ выполнено $|\{j | i_j^k = i^*\}| \geq \lfloor \frac{k}{m} \rfloor$. Предложение $\psi_{i^*}^m$ и будет искомым, для которого не выполняется данное предположение. В частности, при $m = 2$ (либо $m = 1$, если для полноты разбиения при $m = 1$ добавлялось дополнительное предложение) получим, что для одной из двух компонент разбиения ϕ предложение не выполняется, и её ранг равен α .

Далее построим следующую последовательность предложений $\phi_i, i < \omega$, для которой не выполнено предположение:

- $\phi_0 = \phi$
- в качестве ϕ_{i+1} возьмём ту компоненту разбиения ϕ_i на две части, для которой предложение не выполнено.

Тем самым построена последовательность попарно субнесовместных предложений $\phi_i, i < \omega$ ранга α , которые лежат под ϕ , что противоречит тому, что $sr(\phi) = \alpha$. $\square$

Определение. Субранг (субстепень) алгебраической системы $\mathfrak{A}$ определим как субранг (субстепень соответственно) предложения $\exists x = x$, то есть максимальный субранг (субстепень) предложения в этой системе, и будем обозначать как $sr(\mathfrak{A})(sd(\mathfrak{A}))$ соответственно).

Алгебраические системы субранга 1 и субстепеней 1 будем называть сильно субминимальными.

Лемма 2. Пусть $\mathfrak{A}$ и $\mathfrak{B}$ - две произвольные алгебраические системы. Тогда если существует эпиморфизм (сюръективный гомоморфизм) булевых алгебр $h : SB(\mathfrak{A}) \rightarrow SB(\mathfrak{B})$, то $sr(\mathfrak{B}) \leq sr(\mathfrak{A})$, и если $sr(\mathfrak{B}) = sr(\mathfrak{A})$, то $sd(\mathfrak{B}) \leq sd(\mathfrak{A})$.

Доказательство. Докажем, что если $h(\mathfrak{A}(\phi)) = \mathfrak{B}(\psi)$, то $sr_{\mathfrak{B}}(\psi) \leq sr_{\mathfrak{A}}(\phi)$.

Предположим противное. Пусть ϕ - предложение с наименьшим субрангом α такое, что $sr_{\mathfrak{B}}(\psi) > sr_{\mathfrak{A}}(\phi)$. В этом случае очевидно, что $sr_{\mathfrak{B}}(\psi) \geq \alpha + 1$. По определению субранга, это означает, что найдётся последовательность предложений $\psi_i, i < \omega$, таких, что

- $sr_{\mathfrak{B}}(\psi_i) \geq \alpha$

- $\psi_i \wedge \psi \equiv_{\mathfrak{B}}^{sub} \psi_i$
- $\psi_i \wedge \psi_j \equiv_{\mathfrak{B}}^{sub} 0$

Рассмотрим последовательность формул из прообразов, то есть таких предложений ϕ_i , что $\phi_i \in h^{-1}([\psi_i]_{\mathfrak{B}}^{sub})$, $i < \omega$. Поскольку h - гомоморфизм, для них будет выполнено:

- $\phi_i \wedge \phi \equiv_{\mathfrak{A}}^{sub} \phi_i$
- $\phi_i \wedge \phi_j \equiv_{\mathfrak{A}}^{sub} 0$

Кроме того, $sr_{\mathfrak{B}}(\phi_i) \geq \alpha$ для всех $i < \omega$, поскольку иначе, $sr_{\mathfrak{B}}(\phi_i) < \alpha \leq sr_{\mathfrak{B}}(\psi_i)$ и $h(\mathfrak{A}(\phi_i)) = \mathfrak{B}(\psi_i)$ - противоречие с минимальностью α .

Это означает, что $sr_{\mathfrak{A}}(\phi) \geq \alpha + 1$ - противоречие.

Пусть теперь $sr(\mathfrak{B}) = sr(\mathfrak{A}) = \alpha$. Предположим, что $sd(\mathfrak{B}) > sd(\mathfrak{A})$. Тогда если $d = sd(\mathfrak{B})$, то в $\mathfrak{B}$ существует набор из d попарно субнесовместных в $\mathfrak{B}$ предложений ψ_i , $1 \leq i \leq d$ ранга $sr(\mathfrak{B}) = \alpha$. Рассмотрим последовательность предложений ϕ_i таких, что $\phi_i \in h^{-1}([\psi_i]_{\mathfrak{B}}^{sub})$, $1 \leq i \leq d$. Заметим, что $\alpha = sr_{\mathfrak{A}}(\phi_i) \geq sr_{\mathfrak{B}}(\psi_i) = \alpha$ для всех $1 \leq i \leq d$, то есть $sr_{\mathfrak{A}}(\phi_i) = \alpha$. Кроме того, все ψ_i , $1 \leq i \leq d$ попарно субнесовместны в $\mathfrak{A}$ (в силу гомоморфности отображения h), что противоречит тому, что $sd(\mathfrak{A}) < d$. $\square$

Лемма 3. Пусть $\mathfrak{A}$ и $\mathfrak{B}$ - две произвольные алгебраические системы. Тогда если существует вложение булевых алгебр $f : SB(\mathfrak{B}) \rightarrow SB(\mathfrak{A})$, то $sr(\mathfrak{B}) \leq sr(\mathfrak{A})$, и если $sr(\mathfrak{B}) = sr(\mathfrak{A})$, то $sd(\mathfrak{B}) \leq sd(\mathfrak{A})$.

Доказательство. Докажем, что если $f(\mathfrak{B}(\psi)) = \mathfrak{A}(\phi)$, то $sr_{\mathfrak{B}}(\psi) \leq sr_{\mathfrak{A}}(\phi)$.

Предположим противное. Пусть ϕ - предложение с наименьшим субрангом α такое, что $sr_{\mathfrak{B}}(\psi) > sr_{\mathfrak{A}}(\phi)$. В этом случае очевидно, что $sr_{\mathfrak{B}}(\psi) \geq \alpha + 1$. По определению субранга, это означает, что найдётся последовательность предложений ψ_i , $i < \omega$, таких, что

- $sr_{\mathfrak{B}}(\psi_i) \geq \alpha$
- $\psi_i \wedge \psi \equiv_{\mathfrak{B}}^{sub} \psi_i$
- $\psi_i \wedge \psi_j \equiv_{\mathfrak{B}}^{sub} 0$

Рассмотрим последовательность представителей образов формул ϕ_i под действием f : $\phi_i \in f([\psi_i]_{\mathfrak{B}}^{sub})$, $i < \omega$. Поскольку f - вложение, для них будет выполнено:

- $\phi_i \wedge \phi \equiv_{\mathfrak{A}}^{sub} \phi_i$
- $\phi_i \wedge \phi_j \equiv_{\mathfrak{A}}^{sub} 0$

Кроме того, $sr_{\mathfrak{B}}(\phi_i) \geq \alpha$ для всех $i < \omega$, поскольку иначе, $sr_{\mathfrak{B}}(\phi_i) < \alpha \leq sr_{\mathfrak{B}}(\psi_i)$ и $f(\mathfrak{A}(\phi_i)) = \mathfrak{B}(\psi_i)$ - противоречие с минимальностью α .

Это означает, что $sr_{\mathfrak{A}}(\phi) \geq \alpha + 1$ - противоречие.

Пусть теперь $sr(\mathfrak{B}) = sr(\mathfrak{A}) = \alpha$. Предположим, что $sd(\mathfrak{B}) > sd(\mathfrak{A})$. Тогда если $d = sd(\mathfrak{B})$, то в $\mathfrak{B}$ существует набор из d попарно субнесовместных в $\mathfrak{B}$ предложений ψ_i , $1 \leq i \leq d$ ранга $sr(\mathfrak{B}) = \alpha$. Рассмотрим последовательность предложений ϕ_i таких, что $\phi_i \in f([\psi_i]_{\mathfrak{B}}^{sub})$, $1 \leq i \leq d$. Заметим, что $\alpha = sr_{\mathfrak{A}}(\phi_i) \geq sr_{\mathfrak{B}}(\psi_i) = \alpha$ для всех $1 \leq i \leq d$, то есть $sr_{\mathfrak{A}}(\phi_i) = \alpha$. Кроме того, все ψ_i , $1 \leq i \leq d$ попарно субнесовместны в $\mathfrak{A}$, что противоречит тому, что $sd(\mathfrak{A}) < d$. $\square$

Замечание. Поскольку последовательность предложений $\exists^n x$ попарно несовместна и все её члены субвыполнимы в любой алгебраической системе предикатной сигнатуры, субранг предложения $\exists x = x$ в такой системе не может быть меньше 1. Таким образом сильно субминимальные алгебраические системы предикатной сигнатуры - это системы предикатной сигнатуры с минимально возможным субрангом и субстепеню.

Определение. Пусть $\mathfrak{A}, \mathfrak{B}$ - две алгебраические системы и Γ - некоторый класс (свойство) формул.

1. система $\mathfrak{B}$ интерпретируется в системе $\mathfrak{A}$ формулами из Γ , если существует биекция $f : B \rightarrow A$ и отображение $\theta : \Sigma_{\mathfrak{B}} \rightarrow F(\Sigma_{\mathfrak{A}}) \cap \Gamma$ такие, что для любого предиката $P \in \Sigma_{\mathfrak{B}}$ выполнено $\mathfrak{B} \models P(\bar{b}) \Leftrightarrow \mathfrak{A} \models \theta(P)(f(\bar{b}))$
2. системы $\mathfrak{A}$ и $\mathfrak{B}$ взаимно интерпретируются формулами из Γ , если существует биекция $f : B \rightarrow A$ и два отображения $\theta_1 : \Sigma_{\mathfrak{B}} \rightarrow F(\Sigma_{\mathfrak{A}}) \cap \Gamma$ и $\theta_2 : \Sigma_{\mathfrak{A}} \rightarrow F(\Sigma_{\mathfrak{B}}) \cap \Gamma$ такие, что для любого предиката $P \in \Sigma_{\mathfrak{B}}$ выполнено $\mathfrak{B} \models P(\bar{b}) \Leftrightarrow \mathfrak{A} \models \theta_1(P)(f(\bar{b}))$ и для любого предиката $Q \in \Sigma_{\mathfrak{A}}$ выполнено $\mathfrak{A} \models Q(\bar{a}) \Leftrightarrow \mathfrak{B} \models \theta_2(Q)(f^{-1}(\bar{a}))$

Обозначение. Символьно интерпретируемость $\mathfrak{B}$ в $\mathfrak{A}$ формулами Γ записывается следующим образом: $\mathfrak{A} \Rightarrow_{\Gamma} \mathfrak{B}$. Взаимная интерпретируемость $\mathfrak{B}$ в $\mathfrak{A}$ формулами Γ записывается следующим образом: $\mathfrak{A} \Leftrightarrow_{\Gamma} \mathfrak{B}$.

Если носитель у систем $\mathfrak{A}$ и $\mathfrak{B}$ один, а различаются они только множествами предикатов (сигнатурами) Σ_1 и Σ_2 соответственно, то записи $\Sigma_1 \Rightarrow_{\Gamma} \Sigma_2$ и $\Sigma_1 \Leftrightarrow_{\Gamma} \Sigma_2$ обозначают то же, что $\mathfrak{A} \Rightarrow_{\Gamma} \mathfrak{B}$ и $\mathfrak{A} \Leftrightarrow_{\Gamma} \mathfrak{B}$ соответственно.

Определение. Определим для каждой формулы ϕ глубину её кванторной приставки $qd(\phi)$ по индукции следующим образом:

- если ϕ - бескванторная формула, то $qd(\phi) = 0$
- если $\phi = (\phi_1 \wedge \phi_2)$ либо $(\phi_1 \vee \phi_2)$ то $qd(\phi) = \max\{qd(\phi_1), qd(\phi_2)\}$
- если $\phi = \neg(\phi_1)$ то $qd(\phi) = qd(\phi_1)$

- если $\phi = \forall x(\phi_1)$ либо $\exists x(\phi_1)$ то $qd(\phi) = qd(\phi_1) + 1$

Обозначение. Введём следующие обозначения отношения интерпретируемости для классов формул с глубиной кванторной приставки не превосходящей некоторого числа: (взаимную) интерпретируемость $\mathfrak{B}$ в $\mathfrak{A}$ формулами с глубиной кванторной приставки не превышающей n будем обозначать через $\mathfrak{A}(\Leftrightarrow_n) \Rightarrow_n \mathfrak{B}$.

Интерпретируемость произвольными формулами (без ограничений) будем обозначать тройной стрелкой без индекса: $\mathfrak{A}(\Leftrightarrow) \Rightarrow \mathfrak{B}$ означает, что $\mathfrak{B}$ (взаимно) интерпретируется в $\mathfrak{A}$ произвольными формулами первого порядка.

Замечание. Если система $\mathfrak{B}$ интерпретируется в системе $\mathfrak{A}$, то соответствующее отображение $\theta : \Sigma(\mathfrak{B}) \rightarrow F(\Sigma(\mathfrak{A}))$ индуцирует отображение $\theta^* : F(\Sigma(\mathfrak{B})) \rightarrow F(\Sigma(\mathfrak{A}))$.

При этом для любой формулы $\phi(\bar{x}) \in F(\Sigma(\mathfrak{B}))$ и любого кортежа $\bar{a} \in B$ соответствующей длины, $\mathfrak{B} \models \phi(\bar{a})$ выполнено тогда и только тогда, когда $\mathfrak{A} \models \theta^*(\phi)(f(\bar{a}))$.

Кроме того, если $\phi \in S(\Sigma(\mathfrak{B}))$ - некоторое предложение и $\mathfrak{B}_0 \subseteq \mathfrak{B}$ - подсистема в $\mathfrak{B}$, то $\mathfrak{B}_0 \models \phi$ тогда и только тогда, когда $f(\mathfrak{B}) \models \theta^*(\phi)$.

Здесь f - это биекция носителей систем $\mathfrak{A}$ и $\mathfrak{B}$ из определения интерпретируемости.

Доказательство. Отображение θ^* строится очевидным образом индукцией по построению формулы:

- для $P \in \Sigma(\mathfrak{B})$ определим $\theta^*(P)$ как: $\theta^*(P) \equiv \theta(P)$.
- $\theta^*(\neg\phi) \equiv \neg\theta^*(\phi)$
- $\theta^*(\phi_1 \vee \phi_2) \equiv \theta^*(\phi_1) \vee \theta^*(\phi_2)$
- $\theta^*(\phi_1 \wedge \phi_2) \equiv \theta^*(\phi_1) \wedge \theta^*(\phi_2)$
- $\theta^*(\exists x\phi) \equiv \exists x\theta^*(\phi)$
- $\theta^*(\forall x\phi) \equiv \forall x\theta^*(\phi)$

Проверка первого утверждения проводится индукцией по построению формулы. Проверка второго утверждения также тривиальна. $\square$

Лемма 4. Пусть $\mathfrak{A}$ и $\mathfrak{B}$ - две алгебраические системы, и выполнено одно из двух условий:

- $\mathfrak{B} \subseteq \mathfrak{A}$
- $\mathfrak{A} \Rightarrow \mathfrak{B}$

Тогда $sr(\mathfrak{A}) \geq sr(\mathfrak{B})$, и если $sr(\mathfrak{A}) = sr(\mathfrak{B})$, то $sd(\mathfrak{A}) \geq sd(\mathfrak{B})$.

Доказательство. В первом случае, в силу леммы 2, достаточно построить гомоморфизм $h : SB(\mathfrak{A}) \rightarrow SB(\mathfrak{B})$. Искомый гомоморфизм будет индуцироваться тождественным отображением на факторе $S(\Sigma(\mathfrak{A}))/\equiv_{\mathfrak{A}}^{sub}$:

$$h([\phi]_{\mathfrak{A}}^{sub}) = [\phi]_{\mathfrak{B}}^{sub}.$$

Во втором случае, в силу леммы 3, достаточно построить вложение $f : SB(\mathfrak{B}) \rightarrow SB(\mathfrak{A})$. Это вложение строится на основе отображения θ^* :

$$f([\phi]_{\mathfrak{B}}^{sub}) = [\theta^*(\phi)]_{\mathfrak{A}}^{sub}.$$

□

3 Строение шкалы интерпретируемости для систем, бескванторно выражающихся через заданный линейный порядок

Определение. Пусть A - некоторое множество. Обозначим через $Str(A)$ множество всех конечных множеств отношений на множестве A :

$$Str(A) = P_{\omega}(\bigcup_{n < \omega} P(A^n)) \text{ (здесь } P_{\kappa}(M) = \{N \subseteq M \mid |N| < \kappa\}).$$

Если $\Sigma_0 \in Str(A)$ - некоторое конечное множество отношений на множестве A , то введём следующее обозначение для множества структур, интерпретирующихся в Σ_0 формулами с глубиной кванторной приставки не превосходящей n :

$$Str_{\Sigma_0}^n(A) = \{\Sigma \in Str(A) \mid \Sigma_0 \Rightarrow_n \Sigma\}.$$

Кроме того, для любого конечного множества отношений $\Sigma_0 \in Str(A)$ определим класс взаимно интерпретирующихся с ним формулами с глубиной кванторной приставки не превосходящей n конечных множеств отношений $[\Sigma_0]^n = \{\Sigma \in Str(A) \mid \Sigma_0 \Leftrightarrow_n \Sigma\}$

Поскольку отношения $\Rightarrow_0$ и $\Rightarrow_{\omega}$ транзитивны, то на классах $[\Sigma]^0$ и $[\Sigma]_{\omega}$ определён частичный порядок, индуцированный отношением интерпретируемости. Этот частичный порядок будем называть шкалой интерпретируемости.

В дальнейшем будет установлено строение шкалы интерпретируемости на множестве структур выражающихся бескванторно через некоторый фиксированный линейный порядок.

В этом параграфе будет использоваться терминология и некоторые факты из [3]. В частности, будут использоваться специальные обозначения для индикативных групп, критерий интерпретируемости бескванторными формулами для мономорфных систем через группы автоморфизмов и следующее из него отождествление сторого m - местных предикатов с их группами автоморфизмов. Ознакомиться с индикативными группами можно в главе 11 в [1].

Лемма 5. Пусть P - некоторый строго n -местный индикативный предикат на бесконечном линейно упорядоченном множестве $\langle A, < \rangle$ типа I_n, J_n, T_n, D_n или S_n . Тогда формула

$$\phi(x_1, \dots, x_{n-1}) \equiv \exists y (\bigvee_{i < n} P(x_1, \dots, x_i, y, x_{i+1}, \dots, x_{n-1}))$$

определяет $n - 1$ местный индикативный предикат того же типа, что и исходный предикат P .

Доказательство. Переберём все типы предиката P .

$$P = I_n$$

Если $A \models \phi(a_1, \dots, a_{n-1})$, то для некоторого b выполнено $a_1 < \dots < a_i < b < a_{i+1} < \dots < a_{n-1}$, но тогда очевидно, что $a_1 < \dots < a_i < a_{i+1} < \dots < a_{n-1}$, то есть $A \models I_{n-1}(a_1, \dots, a_{n-1})$. Обратно, если $A \models I_{n-1}(a_1, \dots, a_{n-1})$, то поскольку носитель системы бесконечен, то найдётся элемент b отличный от $a_1, \dots, a_{n-1}$. Поскольку порядок $<$ линейный, то для некоторого $i < n$ будет выполнено $a_1 < \dots < a_i < b < a_{i+1} < \dots < a_{n-1}$, то есть $A \models \phi(a_1, \dots, a_{n-1})$.

$$P = J_n$$

Если $A \models \phi(a_1, \dots, a_{n-1})$, то для некоторого b выполнено либо $a_1 < \dots < a_i < b < a_{i+1} < \dots < a_{n-1}$, либо $a_1 > \dots > a_i > b > a_{i+1} > \dots > a_{n-1}$, но тогда выполнено либо $a_1 < \dots < a_i < a_{i+1} < \dots < a_{n-1}$, либо $a_1 > \dots > a_i > a_{i+1} > \dots > a_{n-1}$, то есть $A \models J_{n-1}(a_1, \dots, a_{n-1})$. Обратно, если $A \models J_{n-1}(a_1, \dots, a_{n-1})$, то найдётся элемент b отличный от $a_1, \dots, a_{n-1}$. Поскольку порядок $<$ линейный, то для некоторого $i < n$ будет выполнено либо $a_1 < \dots < a_i < b < a_{i+1} < \dots < a_{n-1}$, либо $a_1 > \dots > a_i > b > a_{i+1} > \dots > a_{n-1}$, то есть $A \models J_n(a_1, \dots, a_i, b, a_{i+1}, \dots, a_{n-1})$ и соответственно $A \models \phi(a_1, \dots, a_{n-1})$.

$$P = T_n$$

Если $A \models \phi(a_1, \dots, a_{n-1})$, то для некоторого b выполнено

$$T_n(a_1, \dots, a_i, b, a_{i+1}, \dots, a_{n-1}).$$

Из строения предиката T_n ясно, что $A \models T_{n-1}(a_1, \dots, a_{n-1})$.

Обратно, пусть $A \models T_{n-1}(a_1, \dots, a_{n-1})$. Это означает, что для некоторого $j < n$ выполнено $a_j < \dots < a_{n-1} < a_1 < \dots < a_{j-1}$. Как уже замечалось, всегда существует элемент b отличный от $a_1, \dots, a_{n-1}$, и для некоторого $i < n$ будет выполнено $a_j < \dots < a_i < b < a_{i+1} < \dots < a_{n-1} < a_1 < \dots < a_{j-1}$ либо $a_j < \dots < a_{n-1} < a_1 < \dots < a_i < b < a_{i+1} < \dots < a_{j-1}$, то есть $A \models T_n(a_1, \dots, a_i, b, a_{i+1}, \dots, a_{n-1})$, а значит и $A \models \phi(a_1, \dots, a_{n-1})$.

$$P = D_n$$

Если $A \models \phi(a_1, \dots, a_{n-1})$, то для некоторого b выполнено

$$D_n(a_1, \dots, a_i, b, a_{i+1}, \dots, a_{n-1}).$$

Из строения предиката D_n ясно, что $A \models D_{n-1}(a_1, \dots, a_{n-1})$.

Обратно, пусть $A \models D_{n-1}(a_1, \dots, a_{n-1})$. Это означает, что для некоторого $\sigma \in S_{n-1}$ выполнено $a_{\sigma(1)} < \dots < a_{\sigma(n-1)}$. Если $\sigma \in T_{n-1}$ или $\sigma \in J_{n-1}$, то $A \models \phi(a_1, \dots, a_{n-1})$ по двум предыдущим случаям. Иначе для некоторого $j < n$ возможны два случая: $a_1 < a_2 < \dots < a_j < a_{n-1} < a_{n-2} < \dots < a_{j+1}$ либо $a_j < a_{j-1} < \dots < a_1 < a_{j+1} < a_{j+2} < \dots < a_{n-1}$. Как уже замечалось, всегда существует элемент b отличный от $a_1, \dots, a_{n-1}$. Разберём случай, когда $a_1 < a_2 < \dots < a_j < a_{n-1} < a_{n-2} < \dots < a_{j+1}$ (второй разбирается аналогично). В этом случае возможно два подслучая: $b < a_{n-1}$ и $b > a_{n-1}$. Если $b < a_{n-1}$, то для некоторого $i < j + 1$ будет выполнено $a_1 < a_2 < \dots < a_i < b < a_{i+1} < \dots < a_j < a_{n-1} < a_{n-2} < \dots < a_{j+1}$, то есть $A \models D(a_1, \dots, a_i, b, a_{i+1}, \dots, a_{n-1})$. Если же $b > a_{n-1}$, то для некоторого $j < i < n$ выполнено $a_1 < a_2 < \dots < a_j < a_{n-1} < a_{n-2} < \dots < a_{i+1} < b < a_i < \dots < a_{j+1}$, то есть опять $A \models D(a_1, \dots, a_i, b, a_{i+1}, \dots, a_{n-1})$, а значит и $A \models \phi(a_1, \dots, a_{n-1})$.

$P = S_n$ Тривиальный случай.

□

Лемма 6. Рассмотрим формулу

$$\begin{aligned} & \phi(x_1, \dots, x_{n-1}) \Leftrightarrow \exists y \\ & \left[\bigvee_{i < p} I_n^{p,q}(y, x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_i, x_p, x_{p+1}, \dots, x_{n-1}) \right] \vee \\ & \left[\bigvee_{p \leq i < n-q} I_n^{p,q}(x_1, \dots, x_i, y, x_{i+1}, \dots, x_{n-1}) \right] \vee \\ & \left[\bigvee_{i \geq n-q} I_n^{p,q}(x_1, \dots, x_{n-q-1}, x_i, \dots, x_{i-1}, x_{i+1}, \dots, x_{n-1}, y) \right] \end{aligned}$$

на бесконечном линейно упорядоченном множестве $\langle A, < \rangle$.

Если $p + q \geq n - 1$, то верна следующая эквивалентность формул:

$$I_{n-1}^{p,q}(x_1, \dots, x_{n-1}) \equiv \phi(x_1, \dots, x_{n-1})$$

Доказательство. Пусть $A \models \phi(a_1, \dots, a_{n-1})$. В этом случае для некоторого $b \in A$ истинен один из трёх членов дизъюнкции в формуле ϕ . Пусть истинен первый член дизъюнкции. Тогда для некоторого $i < p$ имеет место $A \models I_n^{p,q}(b, a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_i, a_p, a_{p+1}, \dots, a_{n-1})$, то есть

- $b, a_1, \dots, a_{p-1} < a_p$
- $a_p < a_{p+1} < \dots < a_{n-q-1}$
- $a_{n-q-1} < a_{n-q}, \dots, a_{n-1}$

Но тогда в частности

- $a_1, \dots, a_p < a_{p+1}$
- $a_{p+1} < \dots < a_{n-q-1}$
- $a_{n-q-1} < a_{n-q}, \dots, a_{n-1}$

то есть $A \models I_{n-1}^{p,q}(a_1, \dots, a_{n-1})$.

Если истинен второй член дизъюнкции, то для некоторого $p \leq i < n - q$ $A \models I_n^{p,q}(a_1, \dots, a_i, b, a_{i+1}, \dots, a_{n-1})$, то есть $a_{p+1} < \dots < a_i < b < a_{i+1} < \dots < a_{n-q-1}$, а значит $A \models I_{n-1}^{p,q}(a_1, \dots, a_{n-1})$.

Третий вариант - когда истинен третий член дизъюнкции - рассматривается аналогично первому.

Обратно, пусть теперь $A \models I_{n-1}^{p,q}(a_1, \dots, a_{n-1})$. Выберем любой элемент $b \notin \{a_1, \dots, a_{n-1}\}$.

Рассмотрим три варианта расположения элемента b по отношению к элементам $a_1, \dots, a_{n-1}$.

Вариант 1 Если $a_1, \dots, a_p < b < a_{n-q}, \dots, a_{n-1}$, то в этом случае существует такое $p < i < n - q - 1$ что $A \models I_n^{p,q}(a_1, \dots, a_i, b, a_{i+1}, \dots, a_{n-1})$, то есть $A \models \phi(a_1, \dots, a_{n-1})$.

Вариант 2 Существует такой индекс $i \leq p$ что $b < a_i$. Выберем из множества $a_1, \dots, a_p$ максимальный элемент a_j . Тогда ясно, что

- $b, a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_p < a_j$
- $a_j < a_{p+1} < \dots < a_{n-q-1}$
- $a_{n-q-1} < a_{n-q}, \dots, a_{n-1}$

то есть $A \models I_n^{p,q}(b, a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_p, a_j, a_{p+1}, \dots, a_{n-1})$, а значит $A \models \phi(a_1, \dots, a_{n-1})$.

Вариант 3 Существует такой индекс $i \geq n - q$ что $b > a_i$. Рассматривается аналогично второму варианту. $\square$

Лемма 7. Рассмотрим формулу

$$\begin{aligned} & \psi(x_1, \dots, x_{n-1}) \Leftrightarrow \exists y \\ & \left[\bigvee_{i < r} J_n^r(y, x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_i, x_r, x_{r+1}, \dots, x_{n-1}) \right] \vee \\ & \left[\bigvee_{r \leq i < n-r} J_n^r(x_1, \dots, x_{i-1}, y, x_{i+1}, \dots, x_{n-1}) \right] \vee \\ & \left[\bigvee_{i \geq n-r} J_n^r(x_1, \dots, x_{n-r-1}, x_i, \dots, x_{i-1}, x_{i+1}, \dots, x_{n-1}, y) \right] \\ & \text{на бесконечном линейно упорядоченном множестве } \langle A, < \rangle. \end{aligned}$$

Если $p + q \geq n - 1$, то верна следующая эквивалентность формул:

$$J_{n-1}^r(x_1, \dots, x_{n-1}) \equiv \psi(x_1, \dots, x_{n-1})$$

Доказательство. Пусть $A \models \psi(a_1, \dots, a_{n-1})$. В этом случае для некоторого $b \in A$ истинен один из трёх членов дизъюнкции в формуле ϕ . Пусть истинен первый член дизъюнкции. Тогда для некоторого $i < r$ имеет место $A \models J_n^r(b, a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_i, a_p, a_{p+1}, \dots, a_{n-1})$. В силу строения группы J_n^r возможны два варианта.

Вариант 1

- $b, a_1, \dots, a_{p-1} < a_p$

Рис. 1: Диаграмма включения индикативных групп

- $a_p < a_{p+1} < \dots < a_{n-q-1}$
- $a_{n-q-1} < a_{n-q}, \dots, a_{n-1}$

Этот вариант в точности соответствует разобранному в лемме 6.

Вариант 2

- $b, a_1, \dots, a_{p-1} > a_p$
- $a_p > a_{p+1} > \dots > a_{n-q-1}$
- $a_{n-q-1} > a_{n-q}, \dots, a_{n-1}$

Этот вариант аналогичен предыдущему с точностью до замены порядка на обратный. В обоих случаях получаем, что $A \models J_{n-1}^r(a_1, \dots, a_{n-1})$. Случаи, когда истинны остальные члены дизъюнкции тоже распадаются на два подслучая и рассматриваются аналогично.

Обратно, пусть теперь $A \models J_{n-1}^r(a_1, \dots, a_{n-1})$. Опять возможны два варианта упорядочения кортежа $a_1, \dots, a_{n-1}$ - прямой (как в лемме 6) и обратный. В случае прямого упорядочения рассуждения в точности повторяют рассуждения из леммы 6, а в случае обратного - проводятся аналогично, но с учётом замены порядка на обратный, и в результате получается, что $A \models \psi(a_1, \dots, a_{n-1})$. $\square$

Лемма 8. Пусть p, q - n -арные индикативные группы, $n < m$ и выполнено $p^m \leq q^m$ (здесь через p^m обозначается m -арное расширение группы p . Определение можно найти в [1], глава 11). Тогда $p \leq q$.

Доказательство. Для каждой арности m индикативных предикатов, диаграмму их включения друг в друга как подгрупп (а значит и бескванторной интерпретируемости) можно изобразить диаграммой 1.

При малых m некоторые вершины могут склеиваться (например $D_3 = S_3$), но эта диаграмма обладает следующей монотонностью: если вершины a и b

несмежны в диаграмме для некоторого m , то они будут несмежны и во всех диаграммах при больших $m' > m$. Это легко устанавливается из строения индикативных групп.

Кроме того, k -арное расширение индикативной группы одного из типов будет такого же типа, то есть k -арные расширения сохраняют тип индикативной группы.

По условию $p^m \leq q^m$, то есть группы p^m и q^m представляют собой смежные вершины на диаграмме. Поскольку k -арные расширения для индикативных групп не выводят за тип индикативности, несмежность p и q влекла бы несмежность p^m и q^m . $\square$

Теорема 1. Пусть $\langle A, < \rangle$ - бесконечный линейный порядок. Тогда шкала интерпретируемости для множества систем $Str_{<}^0(A)$ определяемых через этот порядок бескванторными формулами полностью покрывается следующими классами:

$$Str_{<}^0(A) = [<_2] \cup [T_3] \cup [J_3] \cup [D_4] \cup \{[I_{p+q}^{p,q}] | p, q > 0\} \cup \{[J_{2r}^r] | r > 0\} \cup [=]$$

среди которых 5 дискретных классов и две бесконечные серии.

Доказательство. Пусть $< \Rightarrow_0 \Sigma$ - некоторое конечное множество предикатов, выражающихся бескванторными формулами через порядок $<$, $\Sigma = \{p_1, \dots, p_n\}$. Без ограничения общности можно считать, что все предикаты p_i - строго k_i -местные, причём являются группами. Пусть также $q_i \leq p_i$ - максимальные индикативные подгруппы в исходных предикатах.

Заметим, что $Aut_{\Sigma}(m) = \bigcap_{i \leq n} Aut_{p_i}(m)$. Кроме того, по теореме 4.6 из главы 11 в [1], для каждого $i \leq n$ существует достаточно большое число m_i такое, что $Aut_{p_i}(m_i) = Aut_{q_i}(m_i)$. Пусть $m_0 = \max\{m_i | i \leq n\}$. Тогда $Aut_{\Sigma}(m_0) = \bigcap_{i \leq n} Aut_{p_i}(m_0) = \bigcap_{i \leq n} Aut_{q_i}(m_0) = q_0$ - некоторая индикативная группа. Ясно, что $\Sigma \Rightarrow_0 q_0$.

Из лемм 5, 6 и 7 следует, что $q_0 \Rightarrow p_0$, где $p_0 \in \{<, T_3, J_3, D_4, =\} \cup \{I_{p+q}^{p,q} | p, q > 0\} \cup \{J_{2r}^r | r > 0\}$ - индикативный предикат того же типа, что и q_0 . В силу транзитивности определимости $\Sigma \Rightarrow p_0$.

Остаётся заметить, что $p_0 \Rightarrow p_i$ для всех $0 < i \leq n$. Для этого достаточно показать, что $p_0^{m_i} \leq q_i$, поскольку $q_i \leq p_i$. Заметим, что $p_0^{m_0} = q_0 \leq q_i^{m_0}$, но тогда по лемме 8 получаем искомое: $p_0^{m_i} \leq q_i$. $\square$

4 Строение сильно субминимальных систем

Лемма 9. Любые два конечных линейных порядка, мощности не меньшей 2^n , неразличимы предложениями сигнатуры $<$ не более чем с n кванторами, то есть n -эквивалентны.

Доказательство. Доказательство проводится индукцией по n . Для $n = 1$ утверждение тривиально. Пусть утверждение леммы верно для $n - 1$. Для

доказательства утверждения для n достаточно показать, что если x, y - два конечных линейных порядка, $|x| \geq 2^n$ и $|y| = |x| + 1$, то $y \equiv_n x$. Чтобы показать это, докажем существование беспроигрышной стратегии в игре Эренфойхта за n шагов между x и y .

Разметим два частично предопределённых сценария ведения игры:

Заметим, что:

- эти сценарии пересекаются в единственной выделенной точке A
- любая точка каждого из обоих исходных множеств попадает в один из сценариев

Соответственно если в игре Эренфойхта выбирается некоторая точка на одном из этих множеств, то возможны два варианта:

- если эта точка отлична от точки A , то она попадает ровно в один из сценариев, и её образ выбирается в соответствии с этим сценарием.
- если требуется найти образ точки A , то выбирается любой из сценариев, и по нему определяется образ.

Выбранный сценарий фиксируется. В дальнейшем в игре Эренфойхта образы точек, которые покрываются этим сценарием, будут выбираться в соответствии с ним. Заметим, что поскольку оба сценария определяют изоморфизм линейных порядков, непродолжаемость строимого частичного изоморфизма может возникнуть только при определении образа точки, не покрываемой выбранным сценарием. Но если мы рассмотрим множества точек, не покрываемых одним из сценариев, то это будут два линейно упорядоченных множества, мощность которых различается на единицу и не меньше, чем 2^{n-1} . По индукционной гипотезе, между этими множествами существует беспроигрышная стратегия для игры Эренфойхта за $n - 1$ шагов. Применяя эту стратегию к тем точкам, которые не покрываются фиксированным сценарием построения частичного изоморфизма, мы получим полную беспроигрышную стратегию на всех точках. $\square$

Обозначение. Если фиксирован некоторый линейный порядок $\langle A, < \rangle$, и $a \in A$ - некоторый элемент основного множества, то через a^+ мы будем обозначать непосредственного последователя a в порядке $<$ (если он существует), а через a^- - непосредственного предшественника этого элемента.

Также введём следующее индуктивное определение:

- $a^{+/-0} \equiv a$

- $a^{+/-n} \Rightarrow (a^{+/(n-1)})^{+/-}$, если этот последователь существует

Таким образом, запись a^{+n} (a^{-n}) обозначает элемент, отстоящий ровно на n элементов дальше (соответственно ближе) в порядке $<$, чем элемент a . Этот элемент будем называть n -последователем (n -предшественником) элемента a .

$\exists a^{+n}$ ($\exists a^{-n}$) будет обозначать сокращённую запись утверждения того, что у элемента a существует n -последователь (n -предшественник соответственно) в исходном порядке.

Лемма 10. Пусть $\langle A, < \rangle$ - некоторый дискретный линейный порядок. Определим формулу $\phi_D^{\min, \max}(x, t) \Rightarrow \forall y \forall z (D_4(x, y, z, t) \vee D_4(x, z, y, t))$.

Если в порядке $\langle A, < \rangle$ есть наибольший и наименьший элементы, то формула $\phi_D^{\min, \max}(x, t)$ выделяет в этом порядке в точности два кортежа: $(a_{\min}, a_{\max})$ и $(a_{\max}, a_{\min})$. Если же в исходном порядке нет наибольшего или наименьшего элемента, то формула $\phi_D^{\min, \max}(x, t)$ не удовлетворяется ни одним кортежом.

Доказательство. Если в порядке $\langle A, < \rangle$ есть наибольший и наименьший элементы $a_{\max}$ и $a_{\min}$, то нетрудно проверить, что

$$\langle A, < \rangle \models \phi_D^{\min, \max}(a_{\min}, a_{\max}) \wedge \phi_D^{\min, \max}(a_{\max}, a_{\min}).$$

Для сокращения записей в дальнейшем будем отождествлять символы переменных x, y, z, t с соответствующими им значениями.

Обратно, пусть $\langle A, < \rangle \models \phi_D^{\min, \max}(x, t)$. Покажем, что тогда либо $x = a_{\min}$ и $t = a_{\max}$, либо $x = a_{\max}$ и $t = a_{\min}$. Предположим противное, например что $x \neq a_{\min}$ и $x \neq a_{\max}$. Возьмём в качестве y и z в формуле $\phi_D^{\min, \max}(x, t)$ элементы a^- и a^+ соответственно. Тогда для упорядочения элемента t относительно элементов x, y, z останется два варианта: $t < y < x < z$ и $y < x < z < t$. Остаётся убедиться, что $\langle A, < \rangle \not\models D_4(t, y, x, z)$ и $\langle A, < \rangle \not\models D_4(y, x, z, t)$. Для этого достаточно расписать дизъюнкцию $D_4(x, y, z, t) \vee D_4(x, z, y, t)$ в явном виде:

$$\begin{aligned} & D_4(x, y, z, t) \vee D_4(x, z, y, t) = \\ & (x < y < z < t) \vee (y < z < t < x) \vee (z < t < x < y) \vee (t < x < y < z) \vee \\ & (y < x < t < z) \vee (x < t < z < y) \vee (z < y < x < t) \vee (t < z < y < x) \vee \\ & (x < z < y < t) \vee (z < y < t < x) \vee (y < t < x < z) \vee (t < x < z < y) \vee \\ & (z < x < t < y) \vee (x < t < y < z) \vee (y < z < x < t) \vee (t < y < z < x) \quad \square \end{aligned}$$

Лемма 11. Определим следующую формулу:

$$\phi_D(x) \Rightarrow \exists y (x \neq y) \wedge \forall z ((y \neq z) \wedge (z \neq x) \rightarrow \exists t D_4(x, y, z, t))$$

Тогда для любого линейного порядка $\mathfrak{A} = \langle A, < \rangle$, определяющего D_4 , верно следующее:

- I Если в порядке $<$ есть наименьший элемент $a_{\min}$ и наибольший элемент $a_{\max}$, то $\phi_D(\mathfrak{A}) = \{x \in A \mid \neg \exists x^+ \vee \neg \exists x^-, x \notin \{a_{\min}, a_{\max}\}\}$
- II Если в порядке $<$ нет наибольшего или наименьшего элемента, то $\phi_D(\mathfrak{A}) = \{x \in A \mid \neg \exists x^+ \vee \neg \exists x^-\}$

Доказательство. Вначале запишем определение предиката D_4 в исходном порядке $<$ в явном виде:

$$D_4(x, y, z, t) = \\ (x < y < z < t) \vee (y < z < t < x) \vee (z < t < x < y) \vee (t < x < y < z) \vee \\ (y < x < t < z) \vee (x < t < z < y) \vee (z < y < x < t) \vee (t < z < y < x)$$

Пусть $\mathfrak{A} \models \phi_D(x)$. Предположим, что $\exists x^+$ и $\exists x^-$ в порядке $<$. Рассмотрим два возможных случая:

Случай 1

y - не предшественник x , то есть в наших обозначениях $y \neq x^-$. Возьмём в качестве z предшественника x : $z = x^-$. Рассмотрим два возможных подслучая:

1. $y < z$. Тогда для выбора t остаётся три варианта: $t < y < z < x$, $y < t < z < x$ и $y < z < x < t$. Ни на одном из этих вариантов предикат D_4 не может быть истинен.
2. $y > z$. Для выбора t опять остаётся три варианта: $t < z < x < y$, $z < x < t < y$ и $z < x < y < t$. Как и в предыдущем случае ни на одном из этих наборов предикат D_4 не может быть истинен.

Случай 2

y - предшественник x , то есть $y = x^-$. В качестве z возьмём последователя x : $z = x^+$. В этом случае для выбора t остаётся всего два варианта: $t < y < x < z$ и $y < x < z < t$. На обоих из этих вариантов предикат D_4 не может быть истинен.

Значит действительно $\neg \exists x^+ \vee \neg \exists x^-$.

Пусть в порядке $<$ есть наибольший и наименьший элементы $a_{\max}$ и $a_{\min}$. Покажем, что тогда $x \neq a_{\max}$ и $x \neq a_{\min}$. Предположим, что $x = a_{\min}$. Рассмотрим два возможных случая:

Случай 1

y - последователь x ($y = x^+$). Тогда в качестве z возьмём наибольший элемент $a_{\max}$. Для расположения t в порядке $<$ относительно x, y и z остаётся единственная возможность: $x < y < t < z$. Но предикат D_4 не истинен на такой перестановке переменных.

Случай 2

y - не последователь x . Тогда в качестве z возьмём последователя x : $z = x^+$. Для выбора t остаётся два варианта: $x < z < t < y$ и $x < z < y < t$, на которых предикат D_4 не истинен.

Случай, когда $x = a_{\max}$ рассматривается аналогично.

Покажем теперь включение в обратную сторону. Пусть у элемента x нет предшественника справа или слева, и если в исходном порядке есть наибольший и наименьший элементы $a_{\max}$ и $a_{\min}$, то $x \notin \{a_{\min}, a_{\max}\}$.

Вначале рассмотрим случай, когда x - не наибольший и не наименьший элемент. Тогда x - предельный элемент. Для определённости будем считать,

что x - предельный слева элемент. Случай, когда x - предельный справа (то есть у x нет последователя) рассматривается аналогично.

Разберём два возможных варианта:

Вариант 1 у элемента x есть последователь. Возьмём его в качестве y . Тогда для любого $z \neq x, y$ есть всего два варианта расположения по отношению к x и y :

1. $z < x < y$. Поскольку x - предельный слева элемент, то найдётся элемент $z < t < x$. Остаётся заметить, что $\mathfrak{A} \models D_4(z, t, x, y)$.
2. $x < y < z$. Поскольку x - не наименьший элемент по условию, то найдётся элемент $t < x$. Тогда $\mathfrak{A} \models D_4(t, x, y, z)$.

Вариант 2 у элемента x нет ни предшественника, ни последователя. Этот вариант распадается на два возможных случая:

Случай 1 в порядке $<$ есть наименьший элемент $a_{\min}$. Возьмём его в качестве y . Тогда для любого $z \neq x, y$ есть два варианта расположения по отношению к x и y :

1. $y < z < x$. Поскольку x - предельный слева элемент в порядке $<$, то найдётся элемент $z < t < x$. Тогда $\mathfrak{A} \models D_4(y < z < t < x)$.
2. $y < x < z$. Поскольку x - предельный справа элемент в порядке $<$, то найдётся элемент $x < t < z$ и $\mathfrak{A} \models D_4(y < x < t < z)$.

Случай 2 в порядке $<$ нет наименьшего элемента. Возьмём в качестве y любой элемент меньший x . Тогда для любого $z \neq x, y$ есть три варианта расположения по отношению к x и y :

1. $z < y < x$. Поскольку в исходном порядке нет наименьшего элемента, то найдётся элемент $t < z$. Тогда $\mathfrak{A} \models D_4(t < z < y < x)$.
2. $y < z < x$. Поскольку x - предельный слева элемент, то найдётся элемент $z < t < x$ и $\mathfrak{A} \models D_4(y < z < t < x)$.
3. $y < x < z$. Поскольку x - предельный справа элемент, то найдётся элемент $x < t < z$ и $\mathfrak{A} \models D_4(y < x < t < z)$.

Теперь рассмотрим случай, когда x - наименьший элемент (случай, когда x - наибольший элемент рассматривается аналогично). Заметим, что по условию тогда наибольшего элемента в порядке $<$ нет. Рассмотрим два возможных варианта:

Вариант 1 у элемента x есть последователь. Тогда возьмём его в качестве y . Тогда для расположения z по отношению к x, y в порядке $<$ остаётся единственная возможность: $x < y < z$. Поскольку наибольшего элемента не существует, то найдётся элемент $z < t$. Ясно, что $\mathfrak{A} \models D_4(x, y, z, t)$.

Вариант 2 у элемента x нет последователя. Тогда в качестве y возьмём любой элемент $y > x$. Тогда есть два варианта расположения z по отношению к x и y :

1. $x < y < z$. В этом случае поскольку в исходном порядке не существует наибольшего элемента, то найдётся элемент $z < t$ и тогда $\mathfrak{A} \models D_4(x, y, z, t)$.
2. $x < z < y$. Поскольку x - предельный справа элемент, то найдётся элемент $x < t < z$. Но в этом случае $\mathfrak{A} \models D_4(x, t, z, y)$.

□

Обозначение. Зафиксируем некоторый линейный порядок $\langle A, < \rangle$. Введём следующие обозначения:

- если $a \in A$ - некоторый элемент, то $O^p(a) \Rightarrow \{b \in A \mid \text{между } b \text{ и } a \text{ в порядке } < \text{ менее } p \text{ элементов}\}$
- $M_-^p(A) \Rightarrow \begin{cases} O^p(a_{\min}), & \text{если в } \langle A, < \rangle \text{ есть наименьший элемент } a_{\min} \\ \emptyset, & \text{иначе} \end{cases}$
- $M_+^q(A) \Rightarrow \begin{cases} O^q(a_{\max}), & \text{если в } \langle A, < \rangle \text{ есть наибольший элемент } a_{\max} \\ \emptyset, & \text{иначе} \end{cases}$
- $M^{p,q}(A) \Rightarrow M_+^p(A) \cup M_-^q(A)$

Определение. Определим несколько предикатов следующими формулами:

- $I'_2(x_1, x_2) \Rightarrow \exists y_1 \dots \exists y_p \exists z_1 \dots \exists z_q I_{p+q+2}^{p,q}(y_1, \dots, y_p, x_1, x_2, z_1, \dots, z_q)$
Нетрудно заметить, что $\mathfrak{A} \models I'_2(a, b)$ тогда и только тогда, когда $\mathfrak{A} \models a < b$ и $a, b \notin M^{p,q}(A)$.
- $J'_4(x_1, x_2, x_3, x_4) \Rightarrow \exists y_1 \dots \exists y_r \exists z_1 \dots \exists z_r J_{2r+4}^r(y_1, \dots, y_r, x_1, x_2, x_3, x_4, z_1, \dots, z_r)$
Отметим, что $\mathfrak{A} \models J'_4(a, b, c, d)$ тогда и только тогда, когда $\mathfrak{A} \models J_4(a, b, c, d)$ (то есть либо $a < b < c < d$, либо $d < c < b < a$) и $a, b, c, d \notin M^{r,r}(A)$.
- $D'_4(x_1, x_2, x_3, x_4) \Rightarrow \bigvee_{\sigma \in D_4} J'_4(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)})$
Для этого формульного предиката также заметим, что $\mathfrak{A} \models D'_4(a, b, c, d)$ тогда и только тогда, когда $\mathfrak{A} \models D_4(a, b, c, d)$ и $a, b, c, d \notin M^{r,r}(A)$.

Замечание. Множество $A \setminus M^{r,r}(A)$ определимо через предикат J_{2r+4}^r следующей формулой:

$$\chi(x_1) \Rightarrow \exists x_2 \exists x_3 \exists x_4 \bigvee_{\sigma \in S_4} J'_4(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)})$$

Лемма 12. Последовательно определим несколько формул через предикат $I_{p+q+2}^{p,q}$:

- $\phi_I^+(x) \equiv \forall y(I_2'(y, x) \rightarrow \exists z(I_2'(y, z) \wedge I_2'(z, x))) \wedge \exists y I_2'(y, x)$
- $\phi_I^-(x) \equiv \forall y(I_2'(x, y) \rightarrow \exists z(I_2'(x, z) \wedge I_2'(z, y))) \wedge \exists y I_2'(x, y)$
- $\phi_I(x) \equiv \phi_I^+(x) \vee \phi_I^-(x)$

Тогда для любого линейного порядка $\mathfrak{A} = \langle A, < \rangle$, определяющего $I_{p+q+2}^{p,q}$ формула $\phi_I(x)$ выделяет в точности все предельные элементы исходного линейного порядка, не лежащие в множестве $M^{p,q}(A)$.

Доказательство. Очевидно в силу определения предиката $I_2'(x, y)$. $\square$

Лемма 13. Определим следующую формулу через предикат J_{2r+4}^r :

$$\phi_J(x) \equiv \chi(x) \wedge \exists y(\chi(y) \wedge (x \neq y) \wedge \forall z(\chi(z) \wedge (y \neq z) \wedge (z \neq x) \rightarrow \exists t \chi(t) \wedge D_4'(x, y, z, t)))$$

Тогда для любого линейного порядка $\mathfrak{A} = \langle A, < \rangle$, определяющего J_{2r+4}^r , верно следующее:

- I** Если в порядке $<$ существует элемент $a_{\min}^{+r}$ (то есть элемент, отстоящий ровно на r элементов вправо от наименьшего элемента $a_{\min}$) и элемент $a_{\max}^{-r}$, то
- $$\phi_D(\mathfrak{A}) = \{x \in A \mid \neg \exists x^+ \vee \neg \exists x^-, x \notin \{a_{\min}^{+r}, a_{\max}^{-r}\}\} \setminus M^{r,r}(A)$$
- II** Если в порядке $<$ не существует элемента $a_{\min}^{+r}$ или $a_{\max}^{-r}$, то
- $$\phi_D(\mathfrak{A}) = \{x \in A \mid \neg \exists x^+ \vee \neg \exists x^-\} \cup \{a_{\min}^{+r}, a_{\max}^{-r}\} \setminus M^{r,r}(A)$$

Доказательство. Поскольку предикат D_4' совпадает с предикатом D_4 на множестве $A \setminus M^{r,r}(A)$, то доказательство аналогично доказательству леммы 11. $\square$

Лемма 14. Определим следующую формулу через предикат $J_2^r r + 4$:

$$\phi_J^{\min, \max}(x, t) \equiv \forall y \forall z (\chi(y) \wedge \chi(z) \rightarrow D_4'(x, y, z, t) \vee D_4'(x, z, y, t)).$$

Пусть $\langle A, < \rangle$ - линейный порядок, причём все элементы из множества $A \setminus M^{r,r}(A)$ неопредельные. Если в этом порядке существуют элементы $a_{\min}^{+r}$ и $a_{\max}^{-r}$, то формула $\phi_J^{\min, \max}(x, t)$ выделяет в этом порядке в точности два кортежа: $(a_{\min}^{+r}, a_{\max}^{-r})$ и $(a_{\max}^{-r}, a_{\min}^{+r})$. Если же в исходном порядке нет одного из элементов $a_{\min}^{+r}$ и $a_{\max}^{-r}$, то формула $\phi_J^{\min, \max}(x, t)$ не выделяет ни одного кортежа.

Доказательство. Поскольку предикат D_4' совпадает с предикатом D_4 на множестве $A \setminus M^{r,r}(A)$, то доказательство аналогично доказательству леммы 10. $\square$

Обозначение. Если $\mathfrak{A}$ - некоторая алгебраическая система, то через $ST_{\mathfrak{A}}(\infty)$ будем обозначать множество всех элементарных теорий бесконечных подсистем в $\mathfrak{A}$:

$$ST_{\mathfrak{A}}(\infty) \equiv \{Th(\mathfrak{B}) \mid \mathfrak{B} \subseteq \mathfrak{A}, |B| \geq \omega\}$$

Теорема 2. Пусть $\mathfrak{A}$ - алгебраическая система конечной предикатной сигнатуры Σ . Тогда следующие условия эквивалентны:

1. $\mathfrak{A}$ - сильно субминимальна
2. $|ST_{\mathfrak{A}}(\infty)| < \omega$ и $\mathfrak{A}$ - мономорфна.

Доказательство. Покажем, что из 1 следует 2.

Предположим, что $\mathfrak{A}$ не мономорфна. В любом случае в $\mathfrak{A}$ существует бесконечная мономорфная подсистема $\mathfrak{A}_0 \subset \mathfrak{A}$. Пусть x_0 - некоторая конечная подсистема, которая неизоморфна равномошной ей подсистеме в $\mathfrak{A}_0$. Ясно, что можно записать предложением ϕ утверждение о существовании конечной подсистемы, изоморфной x_0 . Заметим, что существуют сколь угодно большие конечные подсистемы, содержащие x_0 (а значит удовлетворяющие ϕ), причём все они выделяются предложениями, фиксирующими мощность подсистемы. Значит $sr(\phi) \geq 1$. С другой стороны под $\neg\phi$ лежат все предложения, фиксирующие типы изоморфизма конечных подсистем из $\mathfrak{A}_0$, этих предложений бесконечно много, и поэтому $sr(\neg\phi) \geq 1$, что противоречит сильной субминимальности $\mathfrak{A}$.

Таким образом $\mathfrak{A}$ мономорфна, а значит все предикаты из Σ выражаются бескванторными формулами через некоторый линейный порядок $<$ на A . Остаётся показать, что $|ST_{\mathfrak{A}}(\infty)| < \omega$.

По теореме 1 о строении шкалы интерпретируемости мономорфных систем конечной сигнатуры, $\mathfrak{A}$ взаимно интерпретируется с системой $\langle A, P \rangle$, где $P \in \{<, =, T_3, J_3, D_4\} \cup \{I_{p+q}^{p,q} \mid p, q > 0\} \cup \{J_{2r}^r \mid r > 0\}$. Поэтому можно сразу считать, что система $\mathfrak{A}$ такого типа. Случай, когда все предикаты исходной сигнатуры взаимно интерпретируются с равенством тривиален. Рассмотрим четыре оставшихся варианта в соответствии с тем, какой индикативный предикат взаимно интерпретируется с исходной системой, и в каждом из этих вариантов определим такое предложение ϕ , что оно выделяет из всех линейных порядков в точности дискретные линейные порядки с наибольшим и наименьшим элементами.

$P = <$ В этом случае последовательно определим несколько формул:

- $\phi_{<}^+(x) \equiv \forall y((y < x) \rightarrow \exists z(y < z < x)) \wedge \exists y(y < x)$
Эта формула выделяет предельные слева элементы.
- $\phi_{<}^-(x) \equiv \forall y((x < y) \rightarrow \exists z(x < z < y)) \wedge \exists y(x < y)$
Эта формула выделяет предельные справа элементы.

- $\phi_{<}(x) \equiv \phi_{<}^+(x) \vee \phi_{<}^-(x)$

Эта формула все предельные элементы.

Окончательно положим

$$\phi \equiv \forall x \neg \phi_{<}(x) \wedge \exists x \forall y \neg (x < y) \wedge \exists x \forall y \neg (y < x),$$

то есть предложению ϕ удовлетворяют в точности все дискретные линейные порядки с наибольшим и наименьшим элементами, в частности все конечные линейные порядки.

$P \in \{J_3, T_3, D_4\}$ Поскольку предикат D_4 выражается бескванторными формулами через предикаты J_3 и T_3 , то можно считать, что P - это предикат D_4 .

В этом случае положим

$$\phi \equiv \forall x \neg \phi_D(x) \wedge \exists y \exists z \phi_D^{\min, \max}(y, z).$$

Заметим, что по лемме 11, если $\langle A, < \rangle \models \phi$, то порядок $\langle A, < \rangle$ является дискретным. Но тогда применима лемма 10, и поскольку $\langle A, < \rangle \models \exists y \exists z \phi_D^{\min, \max}(y, z)$, то в исходном порядке есть наибольший и наименьший элементы. Это значит, что формуле ϕ удовлетворяют в точности все конечные линейные порядки и порядки типа $\omega + (\omega^* + \omega)\alpha + \omega^*$, где α - произвольный линейный порядок (то есть все дискретные линейные порядки с наибольшим и наименьшим элементами).

$P = I_{p+q}^{p,q}$ В этом случае положим

$$\phi \equiv \forall x \neg \phi_I(x) \wedge \exists x (\forall y \neg I'_2(x, y) \wedge \exists z I'_2(z, x)) \wedge \exists x (\forall y \neg I'_2(y, x) \wedge \exists z I'_2(x, z))$$

Тогда по лемме 12, формуле ϕ удовлетворяют в точности все конечные линейные порядки, а также порядки типа $\omega + (\omega^* + \omega)\alpha + \omega^*$, где α - произвольный линейный порядок (то есть ϕ удовлетворяют все дискретные линейные порядки с наибольшим и наименьшим элементом).

Действительно, формула $\forall \neg \phi_I(x)$ утверждает, что не существует предельных элементов далее, чем на расстоянии p элементов от наименьшего элемента и на расстоянии q элементов от наибольшего элемента. Но на самом деле, если истинна формула ϕ , то в исходном порядке нет предельных элементов вообще. Предположим, что это не так, и a - предельный справа элемент, расположенный на расстоянии не более p элементов от наименьшего элемента $a_{\min}$, а элемент b - это такой элемент, что $\forall y \neg I'_2(y, b) \wedge \exists z I'_2(b, z)$. Поскольку выполнено $\exists z I'_2(b, z)$, элемент b не лежит в множестве $M^{p,q}(A)$, то есть $a < b$. Поскольку a - предельный справа элемент, то выберем между a и b $p+1$ элемент: $a < c_p < c_{p-1} < \dots < c_0 < b$. Тогда элемент c_0 не лежит в множестве $M^{p,q}(A)$ и, кроме того, $c_0 < b$. Значит верно $I'_2(c_0, b)$, что противоречит

$\forall y \neg I'_2(y, b)$. Случай, когда a - предельный слева элемент из множества $M^{p,q}(A)$ рассматривается аналогично.

$P = J_{2r}^r$. В этом случае положим

$$\phi \equiv \forall x \neg \phi_J(x) \wedge \exists y \exists z \phi_J^{\min, \max}(y, z)$$

Заметим, что по лемме 13, если $\langle A, < \rangle \models \phi$, то все элементы из множества $A \setminus M^{r,r}(A)$ неопредельные, то есть удовлетворяются условия леммы 14. В таком случае, поскольку $\langle A, < \rangle \models \exists y \exists z \phi_J^{\min, \max}(y, z)$, то в исходном порядке существуют элементы $a_{\min}^{+r}$ и $a_{\max}^{-r}$, а значит в множестве $M^{r,r}(A)$ нет предельных элементов, то есть линейный порядок $\langle A, < \rangle$ - это дискретный линейный порядок с наибольшим и наименьшим элементами.

Таким образом формуле ϕ удовлетворяют в точности все конечные линейные порядки и порядки типа $\omega + (\omega^* + \omega)\alpha + \omega^*$. Здесь α - произвольный линейный порядок.

Заметим, что поскольку все бесконечные дискретные линейные порядки с наибольшим и наименьшим элементами элементарно эквивалентны в сигнатуре $<$ (см. [2]), то они элементарно эквивалентны и в исходной сигнатуре системы $\mathfrak{A}$. Таким образом, ϕ - это полная формула в теории бесконечного линейного порядка.

Поскольку все попарно неизоморфные конечные линейные порядки отделяются друг от друга попарно несовместными предложениями $\phi_n \equiv \exists^{=n} x$, и все ϕ_n лежат под предложением ϕ , то $sr(\phi) \geq 1$.

Предположим, что $|ST_{\mathfrak{A}}(\infty)| \geq \omega$. Но поскольку формула ϕ полна в теории бесконечного линейного порядка, то она может лежать только в одной теории из $ST_{\mathfrak{A}}(\infty)$. Поэтому множество теорий $X \equiv \{T \in ST_{\mathfrak{A}}(\infty) \mid \neg \phi \in T\}$ бесконечно. Выделим счётную последовательность различных теорий из X : $\{T_i \mid i < \omega\} \subseteq X$ и счётное множество индексированных формул: $\{\phi^{j,k} \in T_i \setminus T_j \mid i, j < \omega\}$.

По условию $\mathfrak{A}$ сильно субминимальна, то есть поскольку $sr(\phi) \geq 1$, то $sr(\neg \phi) = 0$. Пусть $d = sd(\neg \phi)$ - субстепень предложения $\neg \phi$. Рассмотрим $d+1$ предложение $\psi_j \equiv \left(\bigwedge_{k \leq d+1} \phi^{j,k} \right) \wedge \left(\bigwedge_{k \leq d+1} \neg \phi^{k,j} \right)$, $j \leq d+1$.

Заметим, что тогда

- все формулы $\psi_j \wedge \neg \phi$, $j \leq d+1$ субвыполнимы ($\psi_j, \neg \phi \in T_j$)
- все формулы ψ_j , $j \leq d+1$ попарно несовместны по построению

то есть $sd(\neg \phi) \geq d+1$. Противоречие.

Теперь докажем обратную импликацию из 2 в 1.

Пусть $|ST_{\mathfrak{A}}(\infty)| < \omega$ и система $\mathfrak{A}$ - мономорфна. По теореме о строении систем с конечным множеством элементарных типов бесконечных подсистем, анонсированной в [4], $\mathfrak{A}$ интерпретируется либо в некотором линейном порядке

простого типа, либо в системе $\langle A, T_3 \rangle$, где трансляция T_3 опять же определена через некоторый простой линейный порядок на A , либо через равенство. В силу леммы 4 достаточно доказать сильную субминимальность системы, в которой интерпретируется исходная система.

Заметим, что поскольку $\mathfrak{A}$ - мономорфна, то атомарными предложениями на конечных подсистемах во всех случаях будут предложения $\phi_n \equiv \exists^n x$, $n \in \omega$. Кроме того, по лемме 9, для каждого предложения ϕ существует такое число k , что для любых двух конечных подсистем $\mathfrak{B}_1, \mathfrak{B}_2 \subset \mathfrak{A}$ мощности не менее k , $\mathfrak{B}_1 \models \phi \Leftrightarrow \mathfrak{B}_2 \models \phi$.

$\langle A, = \rangle \Rightarrow_0 \mathfrak{A}$ В этом случае любое предложение ψ эквивалентно:

- если ψ не имеет бесконечных моделей, то $\psi \equiv \bigvee_{i \leq m} \phi_{n_i}$, где $\{n_1, \dots, n_m\} = \{n \mid \exists \mathfrak{B} \subset \mathfrak{A}, \mathfrak{B} \models \psi, n = |B|\}$ - некоторый набор натуральных чисел. Ясно, что в этом случае $sr(\psi) = 0$, $sd(\psi) = m$.
- если ψ имеет бесконечные модели, то $\psi \equiv \left(\bigvee_{i \leq m} \phi_{n_i} \right) \vee (\exists^{\geq k} x)$, где $\{n_1, \dots, n_m\} = \{n \mid \exists \mathfrak{B} \subset \mathfrak{A}, \mathfrak{B} \models \psi, n = |B|\}$ и k - такое натуральное число, что для всех $k' \geq k$, если $\mathfrak{B} \subset \mathfrak{A}$ и $|B| = k'$, то $\mathfrak{B} \models \psi$. Тогда $sr(\psi) = 1$, но и $sd(\psi) = 1$, поскольку конъюнкция любых двух таких предложений субсовместна.

Поскольку $\exists x = x \equiv \exists^{\geq 1} x$, то система субминимальна.

$\langle \omega N, T_3 \rangle \Rightarrow_0 \mathfrak{A}$ Рассмотрим формулу $\phi_{-lim}^T(x) \equiv \forall y \exists z T_3(x, y, z)$. Пусть $\langle A, < \rangle$ - некоторый произвольный линейный порядок. Тогда:

- В случае, если в этом порядке есть наибольший элемент, то формула $\phi_{-lim}^T(x)$ выделяет в точности предельные элементы.
- Если же в порядке $\langle A, < \rangle$ нет наибольшего элемента, то формула $\phi_{-lim}^T(x)$ выделяет в точности элементы не имеющие предшественника (то есть предельные и элемент и наименьший, если он есть).

Для установления этого запишем предикат $T_3(x, y, z)$ в явном виде: $T_3(x, y, z) = (x < y < z) \vee (y < z < x) \vee (z < x < y)$.

Действительно, если $\langle A, < \rangle \models \phi_{-lim}^T(x)$ для некоторого линейного порядка $\langle A, < \rangle$, и у элемента x есть предшественник, который мы возьмём в качестве y , то для выбора элемента z остаётся две возможности: либо $z < y < x$, либо $y < x < z$. Но по определению T_3 , в обоих случаях $\langle A, < \rangle \not\models T_3(x, y, z)$, что противоречит условию $\langle A, < \rangle \models \phi_{-lim}^T(x)$. Таким образом формула $\phi_{-lim}^T(x)$ выделяет элементы, не имеющие предшественника.

Для проверки в обратную сторону требуется рассмотреть два варианта: исходный порядок имеет наибольший элемент или нет.

- Пусть исходный порядок $\langle A, < \rangle$ имеет наибольший элемент, и x - элемент, не имеющий предшественника, но не наименьший. Покажем, что тогда $\langle A, < \rangle \models \phi_{\lim}^T(x)$. Выберем произвольный элемент y в исходном порядке. Возможны два случая:

- $y < x$. Тогда элемент x не является наименьшим, а значит он является предельным слева. В качестве z возьмём любой элемент $y < z < x$.
- $x < y$, в этом случае найдётся некоторый элемент $z < x$, поскольку x - не наименьший элемент.

ясно, что в обоих случаях выполнено $T_3(x, y, z)$.

- Пусть исходный порядок $\langle A, < \rangle$ не имеет наибольшего элемента, и x - элемент, не имеющий предшественника (в том числе и наименьший). Покажем, что тогда $\langle A, < \rangle \models \phi_{\lim}^T(x)$. Выберем произвольный элемент y в исходном порядке. Возможны два случая:

- $y < x$. Этот случай полностью аналогичен рассмотренному выше случаю порядка с наибольшим элементом.
- $x < y$, в этом случае найдётся некоторый элемент $y < z$, поскольку в исходном порядке нет наибольшего элемента. Получаем, что $x < y < z$, а значит выполнено $T_3(x, y, z)$.

Заметим, что тогда предложения $\phi_{\omega n} \Leftrightarrow \exists^n x \phi_{\lim}^T(x)$ будут атомарными предложениями, выделяющими бесконечные подсистемы, поскольку эти предложения выделяют подсистемы изоморфные $\langle \omega n, T_3 \rangle$ (только внутри исходной системы!), а значит и её полный элементарный тип (опять же только внутри исходной системы!).

Пусть ϕ - произвольное предложение. Возможны два случая:

- существует такое число k , что ϕ не истинно на всех конечных подсистемах мощности больше k . В этом случае

$$\phi \equiv \left(\bigvee_{i \leq r} \phi_{n_i} \right) \vee \left(\bigvee_{j \leq s} \phi_{\omega m_j} \right), \text{ где}$$

$$\{n_1, \dots, n_r\} = \{n \mid \exists \mathfrak{B} \subset \mathfrak{A}, \mathfrak{B} \models \phi, n = |B|\} \text{ и}$$

$$\{m_1, \dots, m_s\} = \{n \mid \exists \mathfrak{B} \subset \mathfrak{A}, \mathfrak{B} \models \phi, \mathfrak{B} \cong \langle \omega n, T_3 \rangle\}.$$

Ясно, что поскольку под таким предложением лежит конечное число атомов, то $sr(\phi) = 0$ и $sd(\phi) = r + s$.

- существуют сколь угодно большие конечные подсистемы в исходной системе, удовлетворяющие ϕ . В этом случае

$$\phi \equiv \left(\bigvee_{i \leq r} \phi_{n_i} \right) \vee \left(\bigvee_{j \leq s} \phi_{\omega m_j} \right) \vee (\forall x \neg \phi_{\lim}^T(x) \wedge \exists^{\geq k} x), \text{ где}$$

$$\{n_1, \dots, n_r\} = \{n \mid \exists \mathfrak{B} \subset \mathfrak{A}, \mathfrak{B} \models \phi, n = |B|\},$$

$\{m_1, \dots, m_s\} = \{n | \exists \mathfrak{B} \subset \mathfrak{A}, \mathfrak{B} \models \phi, \mathfrak{B} \cong \langle \omega n, T_3 \rangle\}$ и k - такое натуральное число, что для всех $k' \geq k$, если $\mathfrak{B} \subset \mathfrak{A}$ и $|B| = k'$, то $\mathfrak{B} \models \phi$.

Ясно, что поскольку под таким предложением лежит бесконечно много атомов, то $sr(\phi) = 1$ но так как конъюнкция любых двух таких предложений субсовместна, то $sd(\phi) = 1$.

В частности и для предложения $\exists x = x$ его субранг и субстепень равны 1, то есть система сильно субминимальна.

$\langle \omega + N, < \rangle \Rightarrow_0 \mathfrak{A}$ Поскольку система $\langle \omega + N, < \rangle$ антиизоморфна подсистеме системы $\langle N + \omega^* + \omega, < \rangle$, по лемме 4 достаточно доказать сильную субминимальность второй системы.

$\langle N + \omega^* + \omega, < \rangle \Rightarrow_0 \mathfrak{A}$ Определим следующие формулы:

- $\alpha \equiv \forall x \exists y (x < y)$
- $\beta \equiv \forall x \exists y (y < x)$
- $\gamma^{n+\omega^*} \equiv \exists x_1 \dots \exists x_n \forall y ((x_1 < y) \rightarrow \exists z (x_1 < z < y)) \wedge (\bigwedge_{1 \leq i \leq n} (x_i < x_1))$
- $\phi_{+\lim}^<(x) \equiv \forall y (x < y) \rightarrow \exists z (x < z < y)$

Заметим, что атомами в этом случае будут следующие предложения:

- $\phi_n \equiv \exists^{=n} x$ - атомы, выделяющие конечные подсистемы
- $\phi_\omega \equiv \alpha \wedge \neg \beta$ - системы типа ω
- $\phi_{\omega^*} \equiv \neg \alpha \wedge \beta$ - системы типа ω^*
- $\phi_{\omega^*+\omega} \equiv \alpha \wedge \beta$ - системы типа $\omega^* + \omega$
- $\phi_{m+\omega^*} \equiv \gamma^{m+\omega^*} \wedge \neg \alpha$ - системы типа $m + \omega^*$
- $\phi_{m+\omega^*+\omega} \equiv \gamma^{m+\omega^*} \wedge \alpha$ - системы типа $m + \omega^* + \omega$

Обозначим через At множество атомов, которые выделяют бесконечные подсистемы:

$$At \equiv \{\phi_\omega, \phi_{\omega^*}, \phi_{\omega^*+\omega}\} \cup \{\phi_{m+\omega^*}, \phi_{m+\omega^*+\omega} | 1 \leq m \leq N\}.$$

Заметим, что атомы из множества At выделяют все типы изоморфизма бесконечных подсистем в исходной системе (их конечное множество).

Пусть ϕ - произвольное предложение. Как и при рассмотрении предыдущих случаев, возможны следующие два варианта:

- существует такое число k , что ϕ не истинно на всех конечных подсистемах мощности больше k . В этом случае

$$\phi \equiv \left(\bigvee_{i \leq r} \phi_{n_i} \right) \vee \left(\bigvee_{t \in T(\phi)} \phi_t \right), \text{ где}$$

$$\{n_1, \dots, n_r\} = \{n \mid \exists \mathfrak{B} \subset \mathfrak{A}, \mathfrak{B} \models \phi, n = |B|\} \text{ и}$$

$$T(\phi) = \{t \in At \mid t \models \phi\} \text{ (здесь истинность на индексе формулы понимается как истинность на линейном порядке соответствующего типа). Ясно, что поскольку под таким предложением лежит конечное число атомов, то } sr(\phi) = 0 \text{ и } sd(\phi) = r + s.$$
- существуют сколь угодно большие конечные подсистемы в исходной системе, удовлетворяющие ϕ . В этом случае

$$\phi \equiv \left(\bigvee_{i \leq r} \phi_{n_i} \right) \vee \left(\bigvee_{t \in T(\phi)} \phi_t \right) \vee (\neg \alpha \wedge \forall x \neg \phi_{+\lim}^<(x) \wedge \exists^{\geq k} x), \text{ где}$$

$$\{n_1, \dots, n_r\} = \{n \mid \exists \mathfrak{B} \subset \mathfrak{A}, \mathfrak{B} \models \phi, n = |B|\},$$

$$T(\phi) = \{t \in At \mid t \models \phi\} \text{ и } k - \text{такое натуральное число, что для всех } k' \geq k, \text{ если } \mathfrak{B} \subset \mathfrak{A} \text{ и } |B| = k', \text{ то } \mathfrak{B} \models \phi. \text{ Ясно, что поскольку под таким предложением лежит бесконечно много атомов, то } sr(\phi) = 1 \text{ но, так как конъюнкция любых двух таких предложений субсовместна, то } sd(\phi) = 1.$$

В частности и для предложения $\exists x = x$ его субранг и субстепень равны 1, то есть система сильно субминимальна.

□

Список литературы

- [1] *Roland Fraisse*, Theory of relations. Amsterdam a.o.: North-Holland, 1986.
- [2] *Ершов Ю.Л., Лавров И.А., Тайманов А.Д., Тайцлин М.А.* Элементарные теории. УМН, 1965, 20, №4
- [3] *Дмитрий Власов*, Строение алгебраических систем с полной теорией бесконечных подсистем. Сиб. мат. журнал, Март-апрель 2003, том 44, №2.
- [4] *Дмитрий Власов*, Исследование структурных свойств алгебраических систем с условиями минимальности субранга и субстепени, определяемых по выполнимости предложений на подсистемах. Проблемы теоретической и прикладной математики: труды 33-й региональной молодёжной конференции, Екатеринбург: УрО РАН, 2002.

Abstracts

B. Baizhanov, V. Verbovskiy, G. Turekhanova. *Non-Orthogonality Of 1-Types In Weakly O-Minimal Structures Of A Finite Depth.*

In this paper authors generalize and simplify Theorem 33 of Baizhanov's paper "Expansion of a model of a weakly o-minimal theory by a family of unary predicates" (JSL, 66, Number 3 (2001), 1382–1414) on existence of monotonic formula, which acts between two non-orthogonal 1-types over a subset of a model of weakly o-minimal theory.

In the new theorem the condition of weak o-minimality of a theory is replaced by weak o-minimality of a structure, which has a finite depth.

O.V. Bryuhanov. *Matrix Representability And Structure Of Groups.*

Matrix representability of nilpotent products $A(n)B$, $n \geq 2$ for linear groups A , B and structure of abstract infinite groups that has matrix representations over fields of arbitrary characteristics are studied.

In theorem 1.1 the criteria of matrix representability of nilpotent products $A(n)B$, $n \geq 2$ for finitely generated linear groups A , B is presented.

In theorem 1.2 the problem on matrix representability of nilpotent product $A(n)B$ is reduced to the question of matrix representability of nilpotent factor group $\bar{A}(n)\bar{B}$. Theorem 1.2 implies that if $F(X)$, $F(Y)$ are free groups then nilpotent products $F(X)(n)F(Y)$, $n \geq 2$ are matrix representable over fields of null characteristic and not represented by matrix over fields of prime characteristics.

In theorem 2.4 is it proved that group G without free subgroups F_2 has matrix representations over fields of different characteristics p and q if and only if G is virtual abelian and $\tau_p(A)$, $\tau_q(A)$, $rank(\tau A)$ are finite for some abelian subgroup A of finite index in the group G .

A.V. Chekhonadskih, A.A. Voevoda. *On Correctness Of Optimization Problems On Sets Of Characteristic Roots.*

In the paper we investigate the conditions for a set of characteristic polynomial roots, that will be sufficient for a corresponding polynomial coefficients set to be convex. In more general form, let $\varphi : G \rightarrow H$ be a diffeomorphism of the 2nd order of smoothness, where G is a convex set with minimal linear flexion κ of the border surface $D(G)$, Π — minimal flow of φ on $D(G)$, and Λ — a module of a spectral maximums vector of quadratic forms $d^2\varphi_\kappa$. If condition $\kappa\Pi < 2\Lambda$ holds on $D(G)$, then the image set H will be convex.

O.V. Isaeva. *Covers In The Lattice Of Varieties Of m -Groups.*

In this article an infinity series of varieties of m -groups, which covers the varieties of all abelian m -groups A_m in the lattice of varieties of m -groups has been constructed.

S.G. Kolesnikov. *About Rationality Of Complex Character Of Sylow 2-Subgroups Of Symmetric Groups S_{2^n} .*

Let χ be a complex character of sylow 2-subgroup of symmetric group S_{2^n} . Then any value is rational.

B. Sh. Kulpeshov. *On Behavior Of Unary Functions In Weakly O-Minimal Theories.*

Here we classify a behaviour of a unary function in the set of realizations of a non-algebraic 1-type of a weakly o-minimal theory in terms of function depth, and also we prove some properties of non-orthogonality of non-algebraic 1-types in a weakly o-minimal theory of convexity rank 1.

A.G. Likharev. *On Weakly Factorizable Groups Of Lie Type Little Ranks And Sporadic Groups.*

We call a group to be weakly factorizable one, if each its proper subgroup is complementable in some larger subgroup. V. M. Levchuk advanced the following hypothesis : *all simply finite not abelian groups is not weakly factorizable, except $PSL_2(7)$.* The Theorem 1 and Theorem 2 establishes right of this hypothesis for groups of Lie type little ranks and some sporadic groups.

O.V. Listova. *Parameters Of Embedding Involutions Of Alternating Groups.*

In this paper the parameters of embedding involutions of alternating groups is calculated.

S.I. Mardaev. *Sambin's Construction And Negative Operators.*

We investigate definability of fixed points of negative operators in modal logic. There is the well-known Fixed Point Theorem for modalized operators. Very elegant Sambin's construction gives defining formula. We have found new application of this construction. We have proved that Sambin's construction gives defining formula for fixed point of negative operator in some class of models.

N.Ya. Medvedev. *Ideals In Vector Lattice Of Piecewise Polynomial Functions.*

In this article a classification of the ideals of the additive group of all continuous piecewise polynomial functions with pointwise ordering has been done.

A.G. Pinus. *Generation Of Finite Algebras, Baseness Of Their Conditionally Equational Theories And Scale Of Potentials Of Computability Of n -Element Algebras.*

A connection of relation of order between potentials of computability of n -element algebras with the question on the number of generators of these algebras and with the question on their conditionally equational theories are investigated.

A.G. Pinus. *Assertions Of Type Of Lovash Theorem.*

For relation that are not equal to isomorphism relation (relations of rational equivalence, of conditional rational equivalence and others) it is considered an analogue of Lovash theorem (two finite universal algebras with isomorphic cartesian squares are isomorphic).

A.M. Popova, E.N. Poroshenko. *Group Of Units In Integral Group Rings Of Finite Groups.*

In present work, we continue the investigation of algorithm described in details in [1] for concrete finite groups, namely we apply this algorithm for S_3 , A_4 . Doing that we specify the result for S_3 , which was got and published in [2].

E.N. Poroshenko. *On Basis Of Leibnitz Algebra.*

In this work we construct a linear basis for the free Leibnitz algebra.

O.A. Starikova. *Enumeration Of Quadrics Of Projective Planes And Spaces Over Local Principal Ideal Ring.*

In this report the normal diagonal view of symmetric matrix over local principal ideal ring is established. It is obtained number of classes of projective congruous quadrics of space RP_{n-1} and number of classes of projective equivalent quadrics of plane RP_2 .

A.I. Stukachev. *Intrinsic Σ -Definability In Hereditary Finite Superstructures.*

We introduce the notion of n -decidability of a structure in hereditary finite superstructure and prove that if M is 1-decidable in $HF(M)$ then there exists universal Σ -function in $HF(M)$.

S. Sudoplatov. *Fuzzy Polygonometries.*

We present an interpretation of generalized polygonometries as fuzzy polygonometries i.e. polygonometries with probabilistic many-valued functions of parameters of polygons. Some historical aspects of polygonometries are considered.

A.A. Vikent'ev, R.A. Vikentiev. *About Measure Of Proximity And Refutable Of The Logical Formulas With Probabilities On Finite Class Of Metric Models.*

The paper discusses a logical expert statements represented as the formulas of the first order language with probabilities. Methods for setting metrics on

such formulas in the finite class models, measures of refutation and probabilities of formulas are offered. Entered metric's properties and corresponding to it's measures are investigated. A number of natural metric on probabilistic knowledge of experts is offered with use of suitable class of models and modification symmetric difference. The research can be applied to solving the problems of the reconciliation of expert statements, to constructing the decision functions in pattern recognition and development of expert systems.

S.F. Vinokurov, L.V. Ryabets. *Algorithm Of Exact Minimization Of Boolean Functions In The Class Of Kronecker Forms.*

This paper presents an algorithm to derive minimal special ESOP called Kronecker forms. The algorithm is based on the properties of special operator form, which is a generalization of special normal form first introduced in [1].

S.F. Vinokurov, A.S. Kazimirov. *An Upper Bound On The Complexity Of Minimum ESOPs.*

This paper considers the complexity $L(n)$ of exclusive-or sum-of-products expressions of Boolean functions. It is showed, that an arbitrary 7-variable functions can be realized by minimum ESOP with at most 28 products. By this result, we showed that $L(n) \leq \frac{7}{32}2^n$ for $n \geq 7$.

D. Yu. Vlasov. *The Description Of Strongly Subminimal Structures.*

Notions of subrank and subdegree of a sentence in a structure are defined as well as a notion of subrank and subdegree of the whole structure.

Strongly subminimal in this sence (of subrank 1 and subdegree 1) structures of finite predicate language are described.

Contents

Introduction	3
School Programme	4
B. Baizhanov, V. Verbovskiy, G. Turekhanova, <i>Non-Orthogonality Of 1-Types In Weakly O-Minimal Structures Of A Finite Depth</i>	7
O.V. Bryuhanov, <i>Matrix Representability And Structure Of Groups</i>	15
A.V. Chekhonadskih, A.A. Voevoda, <i>On Correctness Of Optimization Problems On Sets Of Characteristic Roots</i>	30
O.V. Isaeva, <i>Covers In The Lattice Of Varieties Of m-Groups</i>	35
S.G. Kolesnikov, <i>About Rationality Of Complex Character Of Sylow 2-Subgroups Of Symmetric Groups S_{2^n}</i>	44
B. Sh. Kulpeshov, <i>On Behavior Of Unary Functions In Weakly O-Minimal Theories</i>	47
A.G. Likharev, <i>On Weakly Factorizable Groups Of Lie Type Little Ranks And Sporadic Groups</i>	56
O.V. Listova, <i>Parameters Of Embedding Involutions Of Alternating Groups</i>	62
S.I. Mardaev, <i>Sambin's Construction And Negative Operators</i>	69
N.Ya. Medvedev, <i>Ideals In Vector Lattice Of Piecewise Polynomial Functions</i>	76
A.G. Pinus, <i>Generation Of Finite Algebras, Baseness Of Their Conditionally Equational Theories And Scale Of Potentials Of Computability Of n-Element Algebras</i>	81
A.G. Pinus, <i>Assertions Of Type Of Lovash Theorem</i>	86
A.M. Popova, E.N. Poroshenko, <i>Group Of Units In Integral Group Rings Of Finite Groups</i>	91
E.N. Poroshenko, <i>On Basis Of Leibnitz Algebra</i>	99
O.A. Starikova, <i>Enumeration Of Quadrics Of Projective Planes And Spaces Over Local Principal Ideal Ring</i>	102
A.I. Stukachev, <i>Intrinsic Σ-Definability In Hereditary Finite Superstructures</i>	108
S. Sudoplatov, <i>Fuzzy Polygonometries</i>	116
A.A. Vikent'ev, R.A. Vikentiev, <i>About Measure Of Proximity And Refutable Of The Logical Formulas With Probabilities On Finite Class Of Metric Models</i>	121
S.F. Vinokurov, L.V. Ryabets, <i>Algorithm Of Exact Minimization Of Boolean Functions In The Class Of Kronecker Forms</i>	140
S.F. Vinokurov, A.S. Kazimirov, <i>An Upper Bound On The Complexity Of Minimum ESOPs</i>	152
D. Yu. Vlasov, <i>The Description Of Strongly Subminimal Structures</i>	158
Abstracts	185