

МАТЕМАТИКА И ТЕОРЕТИЧЕСКИЕ КОМПЬЮТЕРНЫЕ НАУКИ

Издается с 2023 года
Выходит 4 раза в год
ISSN 2949-3919

Том 2
Выпуск 4



Казань
2024

МАТЕМАТИКА И ТЕОРЕТИЧЕСКИЕ КОМПЬЮТЕРНЫЕ НАУКИ

Издается с 2023 года

Выходит 4 раза в год

ISSN 2949-3919

Том 2
Выпуск 4

Казань
2024

Учредитель: ФГАОУ ВО КИФУ
Адрес редакции: 420008, Республика Татарстан,
г. Казань, Казанский федеральный университет,
Институт математики и механики, ул. Кремлевская,
д. 35, комн. 501.
Тел. +7 843 233-70-60
E-mail: mathematics.tcs@gmail.com
URL: <https://mathtcs.ru/>

Издается с 2023 года.
Выходит 4 раза в год.
ISSN 2949-3919
Регистрационный номер СМИ: Эл № ФС77-84704

Сетевое издание «Математика и теоретические компьютерные науки» основано в 2023 году Научно-образовательным математическим центром Приволжского федерального округа (НОМЦ ПФО). Его учредителем является ФГАОУ ВО «Казанский (Приволжский) федеральный университет». Издание ориентировано на публикацию научных статей по следующим направлениям фундаментальной и прикладной

математики, теоретической информатики и компьютерных наук:

- вещественный, комплексный и функциональный анализ;
- дифференциальные уравнения, динамические системы и оптимальное управление;
- математическая физика;
- геометрия и топология;
- теория вероятностей и математическая статистика;
- математическая логика, алгебра и теория чисел;
- вычислительная математика;
- теория вычислимости и сложности вычислений;
- дискретная математика и математическая кибернетика;
- теоретическая информатика;
- математические методы в искусственном интеллекте.

Также принимаются к печати обзоры, научно-популярные статьи, статьи о математической жизни. Все статьи проходят процедуру рецензирования. Все опубликованные статьи находятся в открытом доступе. Языки журнала – русский и английский.

Главный редактор

Арсланов М.М. (Россия, г. Казань)

Заместители главного редактора

Бикчентаев А.М. (Россия, г. Казань)

Файзрахманов М.Х. (Россия, г. Казань)

Ответственный секретарь

Тапкин Д.Т. (Россия, г. Казань)

Редакционная коллегия

Абызов А.Н. (Россия, г. Казань)

Авхадиев Ф.Г. (Россия, г. Казань)

Амосов Г.Г. (Россия, г. Москва)

Асташкин С.В. (Россия, г. Самара)

Баженов Н.А. (Россия, г. Новосибирск)

Герман О.Н. (Россия, г. Москва)

Данчев П.В. (Болгария, г. София)

Демиденко Г.В. (Россия, г. Новосибирск)

Ефремова Л.С. (Россия, г. Нижний Новгород)

Касымов Н.Х. (Узбекистан, г. Ташкент)

Каюмов И.Р. (Россия, г. Казань)

Морозов А.С. (Россия, г. Новосибирск)

Мусин И.Х. (Россия, г. Уфа)

Насыров С.Р. (Россия, г. Казань)

Попов А.А. (Россия, г. Казань)

Семенов А.Л. (Россия, г. Москва)

Туганбаев А.А. (Россия, г. Москва)

Турилова Е.А. (Россия, г. Казань)

Фоменко А.Т. (Россия, г. Москва)

Швидефски М.В. (Россия, г. Новосибирск)

СОДЕРЖАНИЕ

Баженов Н.А., Марчук М.И., Фьори-Каронес М. Элементарная вложимость относительно сводимости по Вайрауху	4
Вечтомов Е.М. О мультипликативно идемпотентных полукольцах с уравнительными свойствами	24
Галатенко А.В., Галатенко В.В., Панкратьев А.Е. Некоторые свойства почти всех n -квазигрупп	35
Дудаков С.М. О степени неразрешимости теории фигур в линейных пространствах	51
Касымов Н.Х. Отделимые нумерации универсальных алгебр	66
Молчанов В.А., Фарахутдинов Р.А. Относительно элементарная определимость класса универсальных частичных графовых полуавтоматов в классе полугрупп	103

МАТЕМАТИЧЕСКАЯ ЖИЗНЬ

Конкурс 2025 года на соискание медали и премии имени Н.И. Лобачевского	124
--	-----

Элементарная вложимость относительно сводимости по Вайрауху

Н.А. Баженов, М.И. Марчук, М. Фьори-Каронес

Аннотация. Изучается сложность по Вайрауху для проблем нахождения элементарных вложений в контексте классической теории моделей. Доказано, что проблема нахождения элементарного вложения из простой модели $\mathcal{M}$ в произвольную модель $\mathcal{N}$ (элементарно эквивалентную $\mathcal{M}$) является сильно эквивалентной по Вайрауху известной проблеме lim , которая находит предел последовательности в пространстве Бэра. Установлено, что проблема нахождения элементарного вложения из произвольной модели $\mathcal{M}$ в счетно-насыщенную модель $\mathcal{N}$ также сильно эквивалентна по Вайрауху проблеме lim .

Ключевые слова: сводимость по Вайрауху, элементарное вложение, простая модель, счетно-насыщенная модель.

DOI: 10.26907/2949-3919.2024.4.4-23

Введение

Данная работа посвящена исследованию различных теорем в теории моделей с точки зрения сводимости по Вайрауху. Обратная математика (reverse mathematics) и сводимость по Вайрауху дают два различных метода сравнения теорем из разных областей математики.

Обратная математика – это область математической логики, направленная на нахождение точной аксиоматической силы математических теорем. В обратной математике утверждения о счетных (или счетно представимых) структурах формулируются в формальной системе арифметики второго порядка Z_2 . Основные подсистемы в Z_2 получаются при помощи ограничения аксиом индукции и аксиом выделения на специальные подклассы формул. В частности, в слабой базовой системе RCA_0 есть выделение для Δ_1^0 -определимых множеств и индукция для Σ_1^0 -формул. Система ACA_0 есть расширение RCA_0 , позволяющее задавать множества с помощью арифметического выделения (в частности, отсюда вытекает и индукция для Σ_n^0 -формул). Дальнейшие сведения по обратной математике можно найти в монографиях [1, 2].

Благодарности. Работа Н.А. Баженова и М.И. Марчук выполнена в рамках государственного задания ИМ СО РАН (проект № FWNF-2022-0011).

© 2024 Н.А. Баженов, М.И. Марчук, М. Фьори-Каронес

Поступила: 30.09.2024. Принята: 10.12.2024. Опубликовано: 26.12.2024.

Существует достаточно много работ, посвященных обратной математике для теории моделей (см., например, [3–7]). В частности, известны следующие результаты (над системой RCA_0), связанные с элементарными вложениями для моделей произвольной полной теории T .

- (А) Утверждение о том, что любая счетная атомная модель теории T является простой (т.е. элементарно вкладывается в любую модель теории T), эквивалентно ACA_0 (теорема 2.3 в [3]).
- (В) Утверждение о том, что любая счетная модель теории T элементарно вкладывается в счетно-насыщенную модель теории T , эквивалентно ACA_0 [8].

Следуя [9], одной из основных целей изучения сводимости по Вайрауху является классификация теоретико-вычислительной силы математических теорем вида

$$(\forall x \in X)(x \in D \rightarrow (\exists y \in Y)P(x, y)).$$

Такой теореме можно сопоставить (частичную) многозначную функцию $F : \subseteq X \rightrightarrows Y$, такую что $\text{dom}(F) = D$ и $F : x \mapsto \{y \in Y : P(x, y)\}$. Сводимость по Вайрауху $\leq_W$ и сильная сводимость по Вайрауху $\leq_{sW}$ позволяют сравнивать сложность подобных многозначных функций (формальные детали приведены в подразделе 1.2). Подробные сведения о сводимости по Вайрауху можно найти, например, в обзорах [9, 10].

Заметим, что сводимость по Вайрауху для теорем из теории моделей до сих пор особо не изучалась (при этом отметим, что в [7, § 7.3] получены результаты о $\leq_W$ -степенях для некоторых теорем существования для моделей полной теории T). В данной работе изучаются следующие математические проблемы, соответствующие результатам (А) и (В), приведенным выше.

(i) $\text{ElEm}(\text{prime}, \text{any})$:

- Пример проблемы (instance) или входные данные (input): полные диаграммы счетных моделей $\mathcal{M}$ и $\mathcal{N}$ такие, что $\mathcal{M}$ и $\mathcal{N}$ элементарно эквивалентны и при этом модель $\mathcal{M}$ является атомной.
- Решение (solution): элементарное вложение $\theta : \mathcal{M} \rightarrow \mathcal{N}$.

(ii) $\text{ElEm}(\text{any}, \text{sat})$:

- Пример проблемы: полные диаграммы счетных моделей $\mathcal{M}$ и $\mathcal{N}$ такие, что $\mathcal{M}$ и $\mathcal{N}$ элементарно эквивалентны и при этом модель $\mathcal{N}$ является счетно-насыщенной.
- Решение: элементарное вложение $\theta : \mathcal{M} \rightarrow \mathcal{N}$.

Известно, что для данной теоремы Γ , эквивалентной ACA_0 в обратной математике, соответствующую степень Вайрауха для Γ зачастую можно описать при помощи проблемы $\lim$ или ее конечных скачков $\lim^{(n)}$, $n \geq 1$ (см., например, [9, § 3] и [10, § 11.9.3]). Говоря неформально, проблема $\lim : \subseteq \omega^\omega \rightarrow \omega^\omega$ есть взятие предела в пространстве Бэра (формальное определение $\lim$ приведено в подразделе 1.2). В связи с этим внимание в данной работе сосредоточено на степени $\deg_{sW}(\lim)$.

Работа построена следующим образом. В разделе 1 приводятся необходимые предварительные сведения. В разделе 2 доказывается, что проблема $\text{ElEm}(\text{prime}, \text{any})$ сильно эквивалентна по Вайрауху проблеме lim (теорема 5). В разделе 3 доказывается, что проблема $\text{ElEm}(\text{any}, \text{sat})$ также сильно эквивалентна по Вайрауху проблеме lim (теорема 11).

1. Предварительные сведения

Все рассматриваемые сигнатуры σ являются вычислимыми. Будем отождествлять формулы $\psi(\bar{x})$ сигнатуры σ с их гёделевыми номерами.

Для $A \subseteq \omega$ через χ_A обозначаем характеристическую функцию множества A . Говорят, что $\mathcal{A} = (A, E)$ является *структурой эквивалентности* (equivalence structure), если бинарный предикат E есть отношение эквивалентности на множестве A .

Как обычно, запись $\mathcal{M} \equiv \mathcal{N}$ означает, что модели $\mathcal{M}$ и $\mathcal{N}$ элементарно эквивалентны.

1.1. ПРОСТЫЕ И СЧЕТНО-НАСЫЩЕННЫЕ МОДЕЛИ. Если $\mathcal{M}$ – модель сигнатуры σ , то через $\text{Th}(\mathcal{M})$ обозначается элементарная теория модели $\mathcal{M}$. Модель $\mathcal{M}$ называется *простой*, если $\mathcal{M}$ элементарно вкладывается в любую модель теории $\text{Th}(\mathcal{M})$.

Модель $\mathcal{M}$ сигнатуры σ называется *атомной*, если для любого набора $\bar{a} = a_0, \dots, a_n$ из $\mathcal{M}$ существует формула $\varphi(x_0, \dots, x_n)$ сигнатуры σ такая, что $\mathcal{M} \models \varphi(\bar{a})$ и для любой формулы $\psi(x_0, \dots, x_n)$ выполнено: если $\mathcal{M} \models \psi(\bar{a})$, то

$$\mathcal{M} \models \forall \bar{x} (\varphi(\bar{x}) \rightarrow \psi(\bar{x})).$$

Формулу φ , удовлетворяющую таким условиям, называют *полной формулой* теории $\text{Th}(\mathcal{M})$. Известен следующий критерий (см. [11, теорема 2.3.4]).

Теорема 1 (Р.Л. Воот). *Пусть $\mathcal{M}$ – модель счетной сигнатуры σ . Тогда $\mathcal{M}$ является простой в том и только том случае, когда модель $\mathcal{M}$ счетная атомная.*

Пусть κ – бесконечный кардинал. Модель $\mathcal{M}$ сигнатуры σ называется *κ -насыщенной*, если она реализует все 1-типы над каждым подмножеством $|M|$, мощность которого меньше чем κ .

Модель $\mathcal{M}$ называют *счетно-насыщенной*, если $\mathcal{M}$ счетна и ω -насыщенна. Модель $\mathcal{M}$ называется *счетно-универсальной*, если она счетна и для любой счетной модели $\mathcal{N}$ такой, что $\mathcal{N} \equiv \mathcal{M}$, верно, что $\mathcal{N}$ элементарно вкладывается в $\mathcal{M}$.

Счетная модель $\mathcal{M}$ является *однородной*, если для любых конечных наборов $\bar{a}$ и $\bar{b}$ из модели $\mathcal{M}$, таких что $(\mathcal{M}, \bar{a}) \equiv (\mathcal{M}, \bar{b})$, и любого элемента $c \in \mathcal{M}$ найдется элемент $d \in \mathcal{M}$ с условием $(\mathcal{M}, \bar{a}, c) \equiv (\mathcal{M}, \bar{b}, d)$. Известен следующий результат (см., например, [11, теорема 5.1.14]).

Теорема 2. *Пусть $\mathcal{M}$ – модель счетной сигнатуры σ . Тогда $\mathcal{M}$ является счетно-насыщенной в том и только том случае, когда $\mathcal{M}$ счетно-универсальна и однородна.*

Как принято в обратной математике (см., например, [7]), будем отождествлять счетную модель $\mathcal{M}$ с ее *полной диаграммой* $FD(\mathcal{M})$. Интуитивно говоря, это означает, что можно считать, что все рассматриваемые счетные модели являются X -разрешимыми относительно некоторого подходящего оракула $X \subseteq \omega$. Кроме того, без ограничения общности можно считать, что счетная модель $\mathcal{M}$ имеет носитель ω .

1.2. Сводимость по ВАЙРАУХУ. В рамках данного подхода [10] математические проблемы задаются как многозначные функции $F : \subseteq X \rightrightarrows Y$ (которые фактически являются бинарными отношениями $F \subseteq X \times Y$). Элемент $p \in \text{dom}(F)$ называют *примером* (instance) проблемы F . Произвольный элемент $q \in F(p)$ называют *решением* (solution) проблемы F на примере p .

Дадим здесь определение *сводимости по Вайрауху*, которое не эквивалентно общему определению сводимости по Вайрауху на проблемах F , заданных на произвольных представленных пространствах X, Y . Тем не менее, это определение эквивалентно общему определению в случае, когда X и Y являются подпространствами пространства Бэра ω^ω . Отметим, что в этой работе рассматриваются только такие пространства: в частности, данная счетная модель $\mathcal{M}$ (имеющая носитель ω) отождествляется с характеристической функцией $\chi_{FD(\mathcal{M})} \in 2^\omega$ для ее полной диаграммы.

Приведенное ниже определение следует определению 1.5 из приложения А в работе [12].

Определение 3. Пусть $F, G : \subseteq \omega^\omega \rightrightarrows \omega^\omega$ – многозначные функции.

(а) Говорят, что F *сводится по Вайрауху* к G (обозначается через $F \leq_W G$), если существуют тьюринговы функционалы $\Phi, \Psi : \subseteq \omega^\omega \rightarrow \omega^\omega$ такие, что:

- $\Phi(p) \in \text{dom}(G)$ для любого $p \in \text{dom}(F)$,
- $\Psi(p \oplus q) \in F(p)$ для любых $p \in \text{dom}(F)$ и $q \in G(\Phi(p))$.

Говоря неформально, оператор «предобработки» Φ преобразует данный пример p проблемы F в пример p_G проблемы G . Зная произвольное решение q для проблемы G на примере p_G , оператор «постобработки» Ψ выдает элемент $\Psi(p \oplus q)$, являющийся решением исходной проблемы F на примере p .

(б) Говорят, что F *сильно сводится по Вайрауху* к G (обозначается через $F \leq_{sW} G$), если существуют тьюринговы функционалы $\Phi, \Psi : \subseteq \omega^\omega \rightarrow \omega^\omega$ такие, что:

- $\Phi(p) \in \text{dom}(G)$ для любого $p \in \text{dom}(F)$,
- $\Psi(q) \in F(p)$ для любых $p \in \text{dom}(F)$ и $q \in G(\Phi(p))$.

Говоря неформально, сильная сводимость $\leq_{sW}$ отличается от $\leq_W$ тем, что оператору постобработки Ψ не нужно знать исходный пример $p \in \text{dom}(F)$.

Для $p \in \omega^\omega$ и $i \in \omega$ через $p^{[i]}$ обозначаем i -й столбец для p , т.е. $p^{[i]}(x) = p(\langle i, x \rangle)$.

Определим две математические проблемы.

(1) *Предельным отображением* (limit map) называется функция $\lim : \subseteq \omega^\omega \rightarrow \omega^\omega$ такая, что:

- $\lim(p) = \lim_{i \rightarrow \infty} p^{[i]}$, если существует предел $\lim_{i \rightarrow \infty} p^{[i]}$,
 - $\lim(p)$ не определено в противном случае.
- (2) *Тьюринговым скачком* называют функцию $J: \omega^\omega \rightarrow \omega^\omega$ такую, что

$$J(p)(i) = \begin{cases} 1, & \text{если } \varphi_i^p(\emptyset) \downarrow, \\ 0, & \text{иначе,} \end{cases}$$

для всех $p \in \omega^\omega$ и $i \in \omega$.

Известен следующий результат о связи между проблемами $\lim$ и J :

Теорема 4 (см. [10, теорема 11.6.7]). $\lim \equiv_{sW} J$.

2. Простые модели

Основным результатом данного раздела является следующая

Теорема 5. $\text{ElEm}(\text{prime}, \text{any}) \equiv_{sW} \lim$.

Для доказательства теоремы построим две сильные сводимости по Вайрауху (в предложениях 6 и 7).

Предложение 6. $\text{ElEm}(\text{prime}, \text{any}) \leq_{sW} \lim$.

Доказательство. Пусть $\mathcal{M}$ и $\mathcal{N}$ – счетные модели некоторой полной теории T (в сигнатуре σ) такие, что $\mathcal{M}$ является простой моделью. Построим элемент $p_{(\mathcal{M}, \mathcal{N})} \in \omega^\omega$ такой, что используя $\lim p_{(\mathcal{M}, \mathcal{N})}$, можно равномерно вычислимым образом построить элементарное вложение θ из $\mathcal{M}$ в $\mathcal{N}$. Рассмотрим следующее множество формул:

$$\text{AtForm}_s = \{\varphi(\bar{x}) : T \vdash \exists \bar{x} \varphi(\bar{x}) \text{ и для любой } \psi(\bar{x}) \text{ с гёделевым номером } \leq s \\ \text{верно: } T \vdash \varphi(\bar{x}) \rightarrow \psi(\bar{x}) \text{ или } T \vdash \varphi(\bar{x}) \rightarrow \neg \psi(\bar{x})\}.$$

Заметим, что множество $\text{AtForm} = \lim_{s \rightarrow \infty} \text{AtForm}_s$ является в точности множеством всех полных формул теории T . Зададим $p = p_{(\mathcal{M}, \mathcal{N})}$ по следующим правилам:

- $p(\langle 3e, s \rangle) = \chi_{\text{AtForm}_s}(e)$ для формулы $\varphi(\bar{x})$ сигнатуры σ , имеющей номер e ;
- $p(\langle 3e + 1, s \rangle) = \chi_{FD(\mathcal{M})}(e)$ для каждого $s \in \omega$;
- $p(\langle 3e + 2, s \rangle) = \chi_{FD(\mathcal{N})}(e)$ для каждого $s \in \omega$.

Рассмотрим элемент $p^* = \lim(p)$. Заметим, что $p^* = \chi_{\text{AtForm}} \oplus \chi_{FD(\mathcal{M})} \oplus \chi_{FD(\mathcal{N})}$. В частности, получаем, что p^* «кодирует» полные диаграммы моделей $\mathcal{M}$ и $\mathcal{N}$.

Используя элемент p^* в качестве оракула, можно с помощью стандартного «одностороннего» применения челночной конструкции построить (равномерно по p^*) элементарное вложение из $\mathcal{M}$ в $\mathcal{N}$. Конструкция подробно описана, например, в [11, теорема 2.3.4] (см. также теорему 2.3 в [3], обсуждающую доказательство в аксиоматической системе ACA_0). $\square$

Предложение 7. $\lim \leq_{sW} \text{ElEm}(\text{prime}, \text{any})$.

Доказательство. Зафиксируем $p \in \omega^\omega$, по данному p построим неориентированный граф $\mathcal{M}_p = (|\mathcal{M}_p|, E)$. Пусть A, B, C – попарно непересекающиеся бесконечные вычислимые множества такие, что $A \cup B \cup C = \omega$. Определим множество B как объединение равномерно вычислимых, попарно непересекающихся, бесконечных множеств: $B = \bigcup_{k \in \omega} B^k$. Считаем, что $B^k = \{b_m^k : m \in \omega\}$.

Приведем краткое неформальное описание графа $\mathcal{M}_p$. Для каждого $i \in \omega$ граф $\mathcal{M}_p$ содержит бесконечно много циклов длины $i+3$. Цепью длины $n \geq 1$ будем называть последовательность попарно различных элементов $x_0, \dots, x_n$ такую, что $\mathcal{M}_p \models \bigwedge_{0 \leq i < n} E(x_i, x_{i+1})$. Если $\varphi_i^p(\emptyset) \uparrow$, тогда к каждому циклу длины $i+3$ прикреплен одна бесконечная цепь элементов. Если $\varphi_i^p(\emptyset) \downarrow$, тогда существует бесконечно много циклов длины $i+3$, к которым прикреплен цепь длины L_i , и бесконечно много циклов длины $i+3$, к которым прикреплен цепь длины L_i+1 , для некоторого $L_i \geq 1$.

Продолжим формальное описание графа $\mathcal{M}_p$. Зафиксируем частично вычислимую биекцию α , действующую из ω^3 на ω такую, что $\text{dom}(\alpha) = \{(i, j, k) : j \leq i+2\}$ и $\text{ran}(\alpha) = A$. Если $j \leq i+2$, тогда через $a_i^{k,j}$ будем обозначать элемент $\alpha(i, j, k)$. Пусть γ – вычислимая биекция, действующая из ω^3 на C . Для $i, j, k \in \omega$ через $c_i^{k,j}$ обозначим элемент $\gamma(i, j, k)$.

Далее опишем построение графа $\mathcal{M}_p$ по шагам. Также будем строить частично p -вычислимую функцию $\lambda(x)$ такую, что $\text{dom}(\lambda) = \{e : \varphi_e^p(\emptyset) \downarrow\}$, и на каждом шаге $s > 0$ будем строить вспомогательное множество D_s^* . Если на шаге s в D_s^* добавляем формулу $E(a, b)$, то будем полагать, что $E(b, a)$ также добавляется в D_s^* .

Шаг 0. $D_0 = \emptyset$, $|\mathcal{M}_p^0| = \emptyset$ и $t'(0) = 0$.

Шаг $s+1$. Предположим, что $s = \langle e, t \rangle$. Если $t = 0$, тогда полагаем следующее:

$$D_{s+1}^* = D_s \cup \{E(a_e^{k,j}, a_e^{k,j+1}) : k \in \omega, j \leq e+1\} \cup \{E(a_e^{k,e+2}, a_e^{k,0}) : k \in \omega\} \\ \cup \{E(a_e^{k,0}, c_e^{k,0}) : k \in \omega\}.$$

Пусть $|\mathcal{M}_p^{s+1}| = |\mathcal{M}_p^s| \cup \{a_e^{k,j}, c_e^{k,0} : k \in \omega, j \leq e+1\}$ и $t'(s+1) = t'(s) + 1$.

Определим D_{s+1}^* как множество D_{s+1}^* , в которое дополнительно добавили все соответствующие отрицания формул для новых элементов. Под соответствующими отрицаниями будем понимать следующее: если $E(u, v) \notin D_{s+1}^*$ для $u \in |\mathcal{M}_p^{s+1}| \setminus |\mathcal{M}_p^s|$, $v \in |\mathcal{M}_p^{s+1}|$, тогда $\neg E(u, v) \in D_{s+1}^*$. Также соответствующие отрицания будут включать в себя формулы, устанавливающие, что все новые элементы попарно различны.

Если $t > 0$, тогда выполнен один из следующих двух случаев.

Случай 1. Пусть t – наименьший шаг такой, что $\varphi_{e,t}^p(\emptyset) \downarrow$. Пусть m – наименьший элемент такой, что $b_m^k \notin \mathcal{M}_p^s$. Полагаем

$$D_{s+1}^* = D_s \cup \{E(c_e^{k,j}, c_e^{k,j+1}) : t-1 \leq j < t'(s), k \in \omega\} \\ \cup \{E(b_j^k, b_{j+1}^k) : m \leq j \leq m+e+1, k \in \omega\} \cup \{E(b_m^k, b_{m+e+2}^k) : k \in \omega\}$$

$$\cup \{E(b_j^k, b_{j+1}^k) : m + e + 2 \leq j \leq m + e + t'(s) + 3, k \in \omega\}.$$

Пусть $|\mathcal{M}_p^{s+1}| = |\mathcal{M}_p^s| \cup \{c_e^{k,j} : k \in \omega, t \leq j \leq t'(s)\} \cup \{b_j^k : k \in \omega, m \leq j \leq m + e + t'(s) + 4\}$ и $t'(s+1) = t'(s) + 2$.

Определим D_{s+1} как множество D_{s+1}^* , к которому добавили все соответствующие отрицания формул. Полагаем $\lambda(e) = t'(s)$.

Случай 2. Если $\varphi_{e,t}^p(\emptyset) \uparrow$, тогда $D_{t+1}^* = D_t \cup \{E(c_e^{k,t-1}, c_e^{k,t}) : k \in \omega\}$.

Пусть $|\mathcal{M}_p^{s+1}| = |\mathcal{M}_p^s| \cup \{c_e^{k,t} : k \in \omega\}$ и $t'(s+1) = t'(s) + 1$.

Определим D_{s+1} как множество D_{s+1}^* , к которому добавили все соответствующие отрицания формул.

Описание конструкции завершено. Полагаем $|\mathcal{M}_p| = \bigcup_{s \in \omega} |\mathcal{M}_p^s|$ и $D(\mathcal{M}_p) = \bigcup_{s \in \omega} D_s$. Заметим, что $a \in \mathcal{M}_p$ тогда и только тогда, когда выполнено одно из условий:

- 1) $a \in A \cup B$;
- 2) $a = c_e^{k,t}$ и $a \in M_{\langle e,t \rangle + 1}$ для некоторых $e, k, t \in \omega$.

Следовательно, множество $|\mathcal{M}_p|$ p -вычислимо и $\mathcal{M}_p$ является p -вычислимым графом.

Лемма 8. *Граф $\mathcal{M}_p$ разрешим относительно оракула p .*

Доказательство леммы следует схеме доказательства леммы 3.1 работы [13]. Покажем, что полная диаграмма $FD(\mathcal{M}_p)$ есть p -рекурсивно аксиоматизируемая полная теория. Будем полагать, без потери общности, что $|\mathcal{M}_p| = \omega$. Определим следующие вспомогательные формулы для $n \geq 3$:

$$\psi_C^n(x_1, \dots, x_n) := \bigwedge_{1 \leq i < j \leq n} (x_i \neq x_j) \ \& \ \bigwedge_{1 \leq i < n} E(x_i, x_{i+1}) \ \& \ E(x_n, x_1).$$

Формула $\psi_C^n(\bar{x})$ говорит, что элементы из набора $\bar{x}$ образуют в графе цикл длины n . Для $n \in \omega$ определим формулу $\psi_{deg,n}(x)$, говорящую о том, что вершина x имеет степень n :

$$\begin{aligned} \psi_{deg,0}(x) &:= \neg \exists y E(x, y), \\ \psi_{deg,n+1}(x) &:= \exists y_0 \dots \exists y_n \left(\bigwedge_{i \leq n} E(x, y_i) \ \& \ \bigwedge_{i < j \leq n} y_i \neq y_j \right) \ \& \ \forall z_0 \dots \forall z_{n+1} \left(\bigwedge_{i \leq n+1} E(x, z_i) \rightarrow \right. \\ &\quad \left. \bigvee_{i < j \leq n+1} z_i = z_j \right). \end{aligned}$$

Зададим p -вычислимо перечислимый список аксиом в сигнатуре $\{E^2\} \cup \{c_k : k \in \omega\}$, включающий в себя следующие предложения:

- (1) Все формулы из атомной диаграммы графа $\mathcal{M}_p$.
- (2) Предложение, говорящее о том, что отношение E симметрично и иррефлексивно.
- (3) $\forall x [\psi_{deg,1}(x) \vee \psi_{deg,2}(x) \vee \psi_{deg,3}(x)]$.

(4) Для всех $n \in \omega$:

$$\forall x \forall y_0 \dots \forall y_n \left[\left(\psi_{deg,3}(x) \ \& \ E(x, y_0) \ \& \ \bigwedge_{i < n} E(y_i, y_{i+1}) \right) \rightarrow (y_n = x \vee \neg \psi_{deg,3}(y_n)) \right].$$

Эта серия предложений говорит о том, что каждая компонента связности графа содержит не более одной вершины степени 3.

(5) Для всех $n \in \omega$:

$$\forall x \forall y_0 \dots \forall y_n \left[\left(\psi_{deg,1}(x) \ \& \ E(x, y_0) \ \& \ \bigwedge_{i < n} E(y_i, y_{i+1}) \right) \rightarrow (y_n = x \vee \neg \psi_{deg,1}(y_n)) \right].$$

Другими словами, каждая компонента связности графа содержит не более одной вершины степени 1.

(6) Для всех $n \geq 3$ и $m \geq 1$:

$$\exists x_1^1 \dots \exists x_n^1 \dots \exists x_1^m \dots \exists x_n^m \left[\bigwedge_{1 \leq i \leq m} \psi_C^n(\bar{x}^i) \ \& \ \bigwedge_{1 \leq l \neq p \leq m} \left[\bigwedge_{1 \leq i, j \leq n} (x_i^l \neq x_j^p) \right] \right].$$

Это предложение говорит о том, что существует m циклов длины n .

(7) Для ненулевого натурального числа N выберем s – наименьший шаг конструкции, для которого существует $e \leq s$, такое что $\lambda(e)[s]$ определено и не меньше, чем N . Рассмотрим следующие два случая:

(7a) Пусть существует $e' \leq s$, для которого $\lambda(e')[s] \downarrow \in \{N-1, N\}$. Тогда добавим в список следующее предложение:

$$\forall x_0 \dots \forall x_N \forall y \left[\left(\psi_{deg,1}(x_0) \ \& \ \bigwedge_{i < N} E(x_i, x_{i+1}) \ \& \ \bigwedge_{1 \leq i < j \leq N} (x_i \neq x_j) \ \& \ \bigwedge_{1 \leq i \leq N} \psi_{deg,2}(x_i) \right. \right. \\ \left. \left. \ \& \ E(x_N, y) \ \& \ \psi_{deg,3}(y) \right) \rightarrow \exists z_2 \dots \exists z_{e'+3} \psi_C^{e'+3}(y, \bar{z}) \right].$$

(7b) Если e' из предыдущего случая не существует, то добавляем формулу

$$\forall x_0 \dots \forall x_N \forall y \left[\left(\psi_{deg,1}(x_0) \ \& \ \bigwedge_{i < N} E(x_i, x_{i+1}) \ \& \ \bigwedge_{1 \leq i < j \leq N} (x_i \neq x_j) \ \& \ \bigwedge_{1 \leq i \leq N} \psi_{deg,2}(x_i) \right. \right. \\ \left. \left. \ \& \ E(x_N, y) \right) \rightarrow \neg \psi_{deg,3}(y) \right].$$

Положим, что T – теория, аксиоматизируемая списком аксиом, приведенным выше. Учитывая свойства конструкции, можно установить, что $T \subseteq FD(\mathcal{M}_p)$. Покажем, что теория T полна. Чтобы установить полноту теории T , достаточно показать, что любые две насыщенные модели T , имеющие мощность ω_1 , изоморфны.

Пусть $\mathcal{M}^*$ и $\mathcal{M}^{**}$ – насыщенные модели теории T мощности ω_1 . Построим изоморфизм F из $\mathcal{M}^*$ на $\mathcal{M}^{**}$. Стандартные элементы отображаются естественным образом.

Говоря неформально, образ стандартного элемента a относительно F определяется следующими условиями:

- 1) видом компоненты связности $\mathcal{C}$, в которой лежит a (т.е. длиной цикла $\mathcal{R}$, входящего в $\mathcal{C}$, и количеством элементов $\mathcal{C}$, не принадлежащих $\mathcal{R}$);
- 2) расстоянием от a до единственной вершины степени 3 из $\mathcal{C}$;
- 3) принадлежит ли a циклу $\mathcal{R}$ или нет.

ζ -цепью в модели $\mathcal{N}$ теории T будем называть последовательность $\{x_i : i \in \mathbb{Z}\}$ попарно различных элементов модели $\mathcal{N}$ такую, что $\mathcal{N} \models \psi_{deg,2}(x_i)$ и $\mathcal{N} \models E(x_i, x_{i+1})$ для каждого $i \in \mathbb{Z}$. ω -цепью в модели $\mathcal{N}$ называем последовательность $\{x_i : i < \omega\}$ попарно различных элементов $\mathcal{N}$ такую, что $\mathcal{N} \models \psi_{deg,1}(x_0)$, $\mathcal{N} \models \psi_{deg,2}(x_{i+1})$ и $\mathcal{N} \models E(x_i, x_{i+1})$ для каждого $i < \omega$.

Приведем краткое описание отображения нестандартных элементов модели $\mathcal{M}^*$ в нестандартные элементы модели $\mathcal{M}^{**}$. Нестандартные элементы могут быть трех типов.

Нестандартный элемент *первого типа* входит в некоторую ζ -цепь. Элемент *второго типа* лежит в ω -цепи. Заметим, что ζ -цепей и ω -цепей содержится по ω_1 штук в каждой из моделей $\mathcal{M}^*$ и $\mathcal{M}^{**}$. При построении изоморфизма между $\mathcal{M}^*$ и $\mathcal{M}^{**}$ элементы из ω -цепей отображаем в соответствии с их местоположением относительно вершины степени 1. Элементы из ζ -цепей можно челночным методом отобразить друг в друга.

Нестандартный элемент *третьего типа* лежит в компоненте связности $\mathcal{C}$, не содержащей циклов и при этом имеющей в точности один элемент степени 3. В силу схемы аксиом (7) все остальные элементы $\mathcal{C}$ имеют степень 2. В каждой из моделей $\mathcal{M}^*$ и $\mathcal{M}^{**}$ содержится ω_1 попарно различных таких компонент. Элементы третьего типа отображаем друг в друга в соответствии с их местоположением относительно вершины степени 3.

Следовательно, $\mathcal{M}^*$ и $\mathcal{M}^{**}$ изоморфны, таким образом, теория T является полной. В силу того, что T полна, выполнено $FD(\mathcal{M}_p) = T$. Отсюда вытекает, что полная диаграмма $FD(\mathcal{M}_p)$ p -вычислима. Лемма 8 доказана. $\square$

Отметим, что в доказательстве леммы 8 полная диаграмма $FD(\mathcal{M}_p)$ строится равномерно по p : действительно, по данному $p \in \omega^\omega$ можно равномерно построить список аксиом для $FD(\mathcal{M}_p)$.

Лемма 9. *Модель $\mathcal{M}_p$ является простой.*

Доказательство. В силу теоремы 1 достаточно показать, что любой конечный набор $\bar{d}$ из графа $\mathcal{M}_p$ удовлетворяет некоторой полной формуле $\theta(\bar{x})$. Приведем здесь набросок доказательства (использующий вспомогательные формулы из леммы 8).

Проверка полноты построенной формулы $\theta(\bar{x})$ осуществляется следующим образом. Необходимо установить следующий факт: если два кортежа $\bar{d}$ и $\bar{d}'$ удовлетворяют формуле $\theta(\bar{x})$ в модели $\mathcal{M}_p$, то эти кортежи автоморфны (а следовательно, верно и $(\mathcal{M}_p, \bar{d}) \equiv (\mathcal{M}_p, \bar{d}')$).

- (1) Для данного элемента d из $\mathcal{M}_p$ полную формулу $\theta(x)$ можно построить следующим образом.

Если $\varphi_e^p(\emptyset) \uparrow$, то элемент $a_e^{k,0}$ удовлетворяет полной формуле

$$\theta_{e,A}^1(x) = \psi_{deg,3}(x) \ \& \ \exists \bar{y} \psi_C^{e+3}(x, \bar{y}).$$

Если $\varphi_e^p(\emptyset) \downarrow$, то выполнено следующее:

- элемент $a_e^{k,0}$ удовлетворяет полной формуле $\theta_{e,A}^2(x)$, являющейся конъюнкцией $\theta_{e,A}^1(x)$ и утверждения о том, что к x присоединена цепь длины $\lambda(e)$, оканчивающаяся элементом y степени 1;
- элемент b_{m+e+2}^k из конструкции теоремы удовлетворяет полной формуле $\theta_{e,B}(x)$, утверждающей следующее: выполнено $\theta_{e,A}^1(x)$ и при этом к x присоединена цепь длины $\lambda(e) + 1$, оканчивающаяся элементом степени 1.

Если элемент $d \neq a_e^{k,0}$ лежит в компоненте связности элемента $a_e^{k,0}$, то он соединен с $a_e^{k,0}$ цепью некоторой длины ℓ и при этом d либо лежит в цикле длины $e+3$ (т. е. выполнено $\exists \bar{y} \psi_C^{e+3}(d, \bar{y})$), либо лежит в присоединенной к этому циклу цепи. Опираясь на формулы $\theta_{e,A}^1$ и $\theta_{e,A}^2$, нетрудно восстановить и полную формулу для d . Аналогично рассматривается случай, когда d лежит в компоненте связности элемента b_{m+e+2}^k .

(2) Рассмотрим набор $\bar{d} = d_1, \dots, d_n$, где $n \geq 2$. Полная формула $\theta(x_1, \dots, x_n)$ для $\bar{d}$ задается как конъюнкция следующих формул:

- полные формулы $\theta_i(x_i)$ для каждого элемента d_i ;
- формулы вида $x_i = x_j$ для $d_i = d_j$;
- если элементы $d_i \neq d_j$ лежат в одной компоненте связности, то нужно записать, что x_i и x_j связаны цепью подходящей длины $\ell_{i,j}$;
- если d_i и d_j лежат в разных компонентах связности, то добавляем следующую формулу: существуют вершины z_i и z_j степени 3, такие что $z_i \neq z_j$ и при этом для $m \in \{i, j\}$ элемент x_m связан с z_m цепью подходящей длины ℓ_m .

Нетрудно проверить, что из условия $\mathcal{M}_p \models \theta(\bar{d}) \& \theta(\bar{d}')$ вытекает, что наборы $\bar{d}$ и $\bar{d}'$ автоморфны. Лемма 9 доказана. $\square$

Наконец, установим следующий факт:

Лемма 10. *Существует p -разрешимая изоморфная копия $\mathcal{M}'_p$ графа $\mathcal{M}_p$ такая, что если F – произвольное элементарное вложение из $\mathcal{M}'_p$ в $\mathcal{M}_p$, то F вычисляет $J(p)$ (равномерно по p).*

Доказательство. Построение графа $\mathcal{M}'_p$ проводится аналогично конструкции графа $\mathcal{M}_p$ со следующими основными изменениями: на шаге $s+1$ в случае 1 полагаем:

$$\begin{aligned} D_{s+1}^* = & D_s \cup \{E(c_e^{k,j}, c_e^{k,j+1}) : t-1 \leq j < t'(s)+1, k \in \omega\} \\ & \cup \{E(b_j^k, b_{j+1}^k) : m \leq j \leq m+e+1, k \in \omega\} \cup \{E(b_m^k, b_{m+e+2}^k) : k \in \omega\} \\ & \cup \{E(b_j^k, b_{j+1}^k) : m+e+2 \leq j \leq m+e+t'(s)+2, k \in \omega\}. \end{aligned}$$

Пусть F – элементарное вложение из $\mathcal{M}_p$ в $\mathcal{M}'_p$, и пусть $k \in \omega$. Тогда выполнено:

- (a) $J(p)(e) = 0 \Leftrightarrow F(a_e^{k,0}) \in A$;
- (b) $J(p)(e) = 1 \Leftrightarrow F(a_e^{k,0}) \in B$.

Действительно, если $\varphi_e^p(\emptyset) \uparrow$, то как в графе $\mathcal{M}_p$, так и в графе $\mathcal{M}'_p$, элементы любого цикла длины $e + 3$ лежат в A . Если же $\varphi_e^p(\emptyset) \downarrow$, то в графе $\mathcal{M}_p$ элемент $a_e^{k,0}$ лежит в цикле длины $e + 3$, имеющем присоединенную цепь длины $\lambda(e)$. При этом в $\mathcal{M}'_p$ все такие циклы состоят из элементов множества B . Лемма 10 доказана. $\square$

Построение полных диаграмм для модели $\mathcal{M}_p$ и модели $\mathcal{M}'_p$ из леммы 10 осуществляется равномерно по $p \in \omega^\omega$. Применяя теорему 4, заключаем, что предложение 7 и теорема 5 доказаны. $\square$

3. Счетно-насыщенные модели

Основным результатом данного раздела является следующая

Теорема 11. $\text{ElEm}(\text{any}, \text{sat}) \equiv_{sW} \text{lim}$.

Для доказательства теоремы построим две сильных сводимости по Вайрауху (в предложении 12 и подразделе 3.2).

Предложение 12. $\text{ElEm}(\text{any}, \text{sat}) \leq_{sW} \text{lim}$.

Доказательство. Пусть $\mathcal{M}$ и $\mathcal{N}$ – счетные модели полной теории T такие, что модель $\mathcal{N}$ счетно-насыщенная. Зададим всюду определенную функцию $q: \omega^2 \rightarrow \{0, 1\}$ по следующему правилу: $q(\langle k, l \rangle, s) = 1$ в том и только том случае, когда k есть номер некоторого кортежа $\bar{a}$ из $\mathcal{M}$, l есть номер некоторого кортежа $\bar{b}$ из $\mathcal{N}$, длины наборов $\bar{a}$ и $\bar{b}$ равны, и при этом для каждой формулы $\psi(\bar{x})$, имеющей гёделев номер $\leq s$, верно:

$$\mathcal{M} \models \psi(\bar{a}) \Leftrightarrow \mathcal{N} \models \psi(\bar{b}).$$

Заметим, что $\lim_s q(\langle k, l \rangle, s) = 1$ в том и только том случае, когда типы соответствующих кортежей $\bar{a}$ и $\bar{b}$ совпадают. Полагаем $q^* = \lim(q)$.

Аналогично доказательству предложения 6, можно задать элемент $p = p_{\mathcal{M}, \mathcal{N}}$ такой, что для $p^* = \lim(p)$ верно $p^* = q^* \oplus \chi_{FD(\mathcal{M})} \oplus \chi_{FD(\mathcal{N})}$.

Следуя стандартному доказательству (см., например, [14, лемма 4.3.17]), построим элементарное вложение θ из $\mathcal{M}$ в $\mathcal{N}$. Полагаем $\theta^0 = \emptyset$. Пусть θ^s уже построено, при этом $\text{dom}(\theta^s) = \{a_0, a_1, \dots, a_{s-1}\}$, $b_i = \theta^s(a_i)$, и типы кортежей $a_0, \dots, a_{s-1}$ и $b_0, \dots, b_{s-1}$ совпадают. Выберем наименьший элемент $a_s \in \mathcal{M} \setminus \text{dom}(\theta^s)$. В силу того, что модель $\mathcal{N}$ является ω -насыщенной, в модели $\mathcal{N}$ найдется элемент b такой, что типы кортежей $a_0, \dots, a_{s-1}, a_s$ и $b_0, \dots, b_{s-1}, b$ одинаковы. Используя оракул p^* , находим (равномерно по p^* и θ^s) наименьший такой элемент $b \in \mathcal{N}$. Полагаем $\theta^{s+1} = \theta^s \cup \{(a_s, b)\}$.

Построенное (равномерно по p^*) отображение $\theta = \bigcup_{s \in \omega} \theta^s$ есть элементарное вложение из $\mathcal{M}$ в $\mathcal{N}$. Заключаем, что $\text{ElEm}(\text{any}, \text{sat}) \leq_{sW} \text{lim}$. $\square$

Прежде чем устанавливать существование оставшейся сильной сводимости $\leq_{sW}$, в подразделе 3.1 приведем необходимые предварительные сведения.

3.1. Игры ЭРЕНФОЙХТА–ФРАЙССЕ И СТРУКТУРЫ ЭКВИВАЛЕНТНОСТИ. Следуя [15, 16], кратко опишем игры Эренфойхта–Фрайссе для структур конечной предикатной сигнатуры σ .

Пусть $\mathcal{A}$ и $\mathcal{B}$ – структуры сигнатуры σ с непересекающимися носителями. Пусть n – ненулевое натуральное число. *Раунд* (play) игры $EF_n(\mathcal{A}, \mathcal{B})$ – это упорядоченная последовательность из n повторений следующих действий:

- игрок $\forall$ выбирает элемент из одной из структур $\mathcal{A}$ или $\mathcal{B}$,
- игрок $\exists$ выбирает элемент из другой структуры.

Элемент из структуры $\mathcal{A}$, выбранный во время хода t , обозначается через a_t . Элемент из $\mathcal{B}$, выбранный на ходе t , обозначаем через b_t .

Говорим, что игрок $\exists$ *выиграл* раунд игры, если отображение $\psi: a_t \mapsto b_t$ есть изоморфизм конечных структур $\mathcal{A} \upharpoonright \{a_1, a_2, \dots, a_n\}$ и $\mathcal{B} \upharpoonright \{b_1, b_2, \dots, b_n\}$. В противном случае считаем, что выиграл игрок $\forall$.

Пусть $A = \text{dom}(\mathcal{A})$ и $B = \text{dom}(\mathcal{B})$. Говорят, что игрок $\exists$ имеет *выигрышную стратегию* в игре $EF_n(\mathcal{A}, \mathcal{B})$, если существуют функции $f_1, f_2, \dots, f_n$, удовлетворяющие следующим условиям:

- (a) Область определения f_t есть множество всех упорядоченных t -кортежей элементов из $A \cup B$.
- (b) Если $c_1, \dots, c_t \in A \cup B$ (этот кортеж представляет выборы игрока $\forall$ за первые t ходов), то

$$f_t(c_1, \dots, c_t) \in \begin{cases} A, & \text{если } c_t \in B, \\ B, & \text{если } c_t \in A. \end{cases}$$

- (c) Пусть $c_1, \dots, c_n \in A \cup B$. Для ненулевого $t \leq n$ зададим

$$a_t = \begin{cases} c_t, & \text{если } c_t \in A, \\ f_t(c_1, \dots, c_t), & \text{если } c_t \in B; \end{cases} \quad b_t = \begin{cases} c_t, & \text{если } c_t \in B, \\ f_t(c_1, \dots, c_t), & \text{если } c_t \in A. \end{cases}$$

Тогда отображение $\psi: a_t \mapsto b_t$ является изоморфизмом конечных структур $\mathcal{A} \upharpoonright \{a_1, a_2, \dots, a_n\}$ и $\mathcal{B} \upharpoonright \{b_1, b_2, \dots, b_n\}$.

Если у игрока $\exists$ нет выигрышной стратегии, то говорим, что игрок $\forall$ имеет выигрышную стратегию. Будем писать $\mathcal{A} \sim_n \mathcal{B}$, если игрок $\exists$ имеет выигрышную стратегию в игре $EF_n(\mathcal{A}, \mathcal{B})$.

Теорема 13 (см., например, [15, следствие 3.3.3]). *Структуры $\mathcal{A}$ и $\mathcal{B}$ элементарно эквивалентны в том и только том случае, когда $\mathcal{A} \sim_n \mathcal{B}$ для всех $n \geq 1$.*

Приведем теперь необходимые сведения о структурах эквивалентности.

Пусть $\mathcal{A} = (A, E)$ – структура эквивалентности. Для $a \in A$ через $[a]_{\mathcal{A}}$ обозначаем класс эквивалентности элемента a в структуре $\mathcal{A}$. *Характером* структуры $\mathcal{A}$ называют множество

$$\chi(\mathcal{A}) = \{(n, k) : 1 \leq n, k < \omega, \text{ и } \mathcal{A} \text{ имеет не менее } k \text{ классов размера } n\}.$$

Говорят, что $\mathcal{A}$ имеет *неограниченный характер*, если для любого $n \in \omega$ структура $\mathcal{A}$ имеет класс конечного размера N , такого что $N > n$.

Установим следующий общий факт о структурах эквивалентности:

Предложение 14. Пусть $\mathcal{A}$ и $\mathcal{B}$ – это (не обязательно счетные) структуры эквивалентности, имеющие неограниченный характер.

- a) $\mathcal{A} \equiv \mathcal{B}$ в том и только том случае, когда $\chi(\mathcal{A}) = \chi(\mathcal{B})$.
- b) Пусть $\bar{c} = c_1, \dots, c_m$ – набор элементов из $\mathcal{A}$, $\bar{d} = d_1, \dots, d_m$ – набор элементов из $\mathcal{B}$. Тогда $(\mathcal{A}, \bar{c}) \equiv (\mathcal{B}, \bar{d})$ в том и только том случае, когда выполнены следующие условия:
 - $\chi(\mathcal{A}) = \chi(\mathcal{B})$;
 - наборы $\bar{c}$ и $\bar{d}$ удовлетворяют одним и тем же атомарным формулам;
 - для каждого $i \leq m$ либо размеры классов эквивалентности $[c_i]_{\mathcal{A}}$ и $[d_i]_{\mathcal{B}}$ конечны и равны, либо эти размеры бесконечны.

Доказательство. а) Ясно, что если структуры $\mathcal{A}$ и $\mathcal{B}$ элементарно эквивалентны, то их характеры совпадают. Действительно, для $n \geq 1$ зададим следующие вспомогательные формулы:

- $\psi_{\geq n}(x) = \exists y_1 \exists y_2 \dots \exists y_n [y_i \text{ попарно различны и } (y_i E x)]$,
- формула $\psi_{=n}(x) = \psi_{\geq n}(x) \ \& \ \neg \psi_{\geq n+1}(x)$ говорит о том, что класс эквивалентности $[x]_E$ имеет размер n .

Тогда условие $(n, k) \in \chi(\mathcal{A})$ выполнено в том и только том случае, когда в $\mathcal{A}$ существуют попарно не эквивалентные $x_1, \dots, x_k$, удовлетворяющие $\psi_{=n}(x_i)$, $i \leq k$.

Пусть теперь $\chi(\mathcal{A}) = \chi(\mathcal{B})$. Опишем выигрышную стратегию для игрока $\exists$ в игре Эренфойхта–Фраиссе $EF_n(\mathcal{A}, \mathcal{B})$ для $n \geq 1$.

Пусть игроками $\forall$ и $\exists$ на первых $(t-1)$ ходах уже были выбраны элементы $a_1, \dots, a_{t-1} \in \mathcal{A}$ и $b_1, \dots, b_{t-1} \in \mathcal{B}$ со следующими свойствами:

- (i) наборы $a_1, \dots, a_{t-1}$ и $b_1, \dots, b_{t-1}$ удовлетворяют одним и тем же атомарным формулам,
- (ii) либо $\text{card}([a_i]_{\mathcal{A}}) = \text{card}([b_i]_{\mathcal{B}}) \leq n$, либо $(\text{card}([a_i]_{\mathcal{A}}) > n \text{ и } \text{card}([b_i]_{\mathcal{B}}) > n)$.

Если на t -ом ходе игрок $\forall$ выбирает элемент $a_t \in \mathcal{A}$ такой, что $\text{card}([a_t]_{\mathcal{A}}) \leq n$, то игрок $\exists$ должен выбрать $b_t \in \mathcal{B}$ такой, что $\text{card}([b_t]_{\mathcal{B}}) = \text{card}([a_t]_{\mathcal{A}})$ и при этом наборы $a_1, \dots, a_{t-1}, a_t$ и $b_1, \dots, b_{t-1}, b_t$ удовлетворяют одним и тем же атомарным формулам. Такой выбор возможен в силу того, что для каждого $n' \leq n$ структуры $\mathcal{A}$ и $\mathcal{B}$ имеют одинаковое число классов размера n' .

Пусть теперь игрок $\forall$ выбирает элемент $a_t \in \mathcal{A}$ такой, что $\text{card}([a_t]_{\mathcal{A}}) > n$ (при этом, возможно, эта мощность бесконечна). Если $a_t = a_i$ для некоторого $i < t$, то полагаем $b_t = b_i$. Если $a_t \notin \{a_j : j < t\}$ и при этом $a_t \in [a_i]_{\mathcal{A}}$ для (наименьшего) $i < t$, то можно выбрать $b_t \in [b_i]_{\mathcal{B}}$ такой, что $b_t \notin \{b_j : j < t\}$. Действительно, такой выбор возможен в силу того, что

$$\text{card}([b_i]_{\mathcal{B}} \cap \{b_j : j < t\}) > n - (t - 1) > 0.$$

Если же a_t не эквивалентен ни одному из a_j , $j < t$, то игрок $\exists$ выбирает в качестве b_t такой элемент из $\mathcal{B}$, что $\text{card}([b_t]_{\mathcal{B}}) > n$ и при этом b_t не эквивалентен ни одному из b_j , $j < t$. Этот выбор возможен в силу того, что характер $\chi(\mathcal{B})$ неограничен.

Случай, когда игрок $\forall$ выбирает элемент $b_t \in \mathcal{B}$, рассматривается аналогично: в этом случае игрок $\exists$ может найти подходящий элемент $a_t \in \mathcal{A}$. Индукцией по $t \leq n$ нетрудно показать, что отображение $\psi: a_t \mapsto b_t$ есть изоморфизм конечных структур эквивалентности $\mathcal{A} \upharpoonright \{a_1, \dots, a_n\}$ и $\mathcal{B} \upharpoonright \{b_1, \dots, b_n\}$.

Закключаем, что для каждого $n \geq 1$ выполнено $\mathcal{A} \sim_n \mathcal{B}$. Следовательно, по теореме 13, структуры $\mathcal{A}$ и $\mathcal{B}$ элементарно эквивалентны.

б) Доказательство проводится аналогично доказательству пункта а). При этом в стратегию для игры $EF_n((\mathcal{A}, \bar{c}), (\mathcal{B}, \bar{d}))$ необходимо добавить следующее условие:

(iii) для любых $k \leq m$ и $i < t$ выполнено: $a_i \in [c_k]_{\mathcal{A}} \Leftrightarrow b_i \in [d_k]_{\mathcal{B}}$.

Предложение 14 доказано. $\square$

Следствие 15. Пусть $\mathcal{A}$ – это счетная структура эквивалентности, имеющая неограниченный характер и бесконечное число бесконечных классов эквивалентности. Тогда $\mathcal{A}$ является счетно-насыщенной моделью.

Доказательство. Пусть $\mathcal{S}$ – это счетная структура, элементарно эквивалентная структуре $\mathcal{A}$. По предложению 14 п. а) характер $\chi(\mathcal{S})$ равен $\chi(\mathcal{A})$. Отсюда получаем, что нетрудно построить изоморфное вложение θ из $\mathcal{S}$ в $\mathcal{A}$, такое что для любого $b \in \mathcal{S}$ выполнено $\text{card}([\theta(b)]_{\mathcal{A}}) = \text{card}([b]_{\mathcal{S}})$. По предложению 14 п. б) получаем, что $(\mathcal{S}, \bar{b}) \equiv (\mathcal{A}, \theta(\bar{b}))$ для любого конечного кортежа $\bar{b}$ из $\mathcal{S}$. Закключаем, что θ есть элементарное вложение из $\mathcal{S}$ в $\mathcal{A}$. Следовательно, модель $\mathcal{A}$ счетно-универсальна.

В силу теоремы 2 осталось показать, что модель $\mathcal{A}$ является однородной. Пусть $(\mathcal{A}, \bar{a}) \equiv (\mathcal{A}, \bar{b})$ и $c \in \mathcal{A}$. Из предложения 14 п. б) вытекает, что существует автоморфизм g структуры $\mathcal{A}$ такой, что $\bar{b} = g(\bar{a})$. Получаем, что $(\mathcal{A}, \bar{a}, c) \equiv (\mathcal{A}, \bar{b}, g(c))$. Следовательно, модель $\mathcal{A}$ однородна. Следствие 15 доказано. $\square$

Также нам понадобится следующий известный факт:

Теорема 16 (следует, например, из [17, § 5]). Пусть $\mathcal{A}$ – вычислимая структура эквивалентности. Структура $\mathcal{A}$ является разрешимой в том и только том случае, когда вычислимы следующие два множества:

- характер $\chi(\mathcal{A})$;
- множество $K(\mathcal{A}) = \{(a, k) \in \text{dom}(\mathcal{A}) \times \omega : \text{card}([a]_{\mathcal{A}}) \geq k\}$.

3.2. ПРОДОЛЖЕНИЕ ДОКАЗАТЕЛЬСТВА ТЕОРЕМЫ 11

Предложение 17. $\lim \leq_{sW} \text{ElEm}(\text{any}, \text{sat})$.

Доказательство. Зафиксируем разрешимую структуру эквивалентности $\mathcal{U}$ со следующими свойствами:

- для каждого $\beta \in (\omega \setminus \{0\}) \cup \{\omega\}$ структура $\mathcal{U}$ имеет бесконечно много классов размера β ;
- функция $c_{\mathcal{U}}: a \mapsto \text{card}([a]_{\mathcal{U}})$ вычислима.

В силу того, что характер $\chi(\mathcal{U})$ неограничен и $\mathcal{U}$ имеет бесконечно много бесконечных классов эквивалентности, по следствию 15, $\mathcal{U}$ есть счетно-насыщенная модель.

Для данного $p \in \omega^\omega$ зададим счетную структуру эквивалентности $\mathcal{E}_p$. Структура $\mathcal{E}_p$ определяется как дизъюнктивное объединение структуры $\mathcal{U}$ и структуры $\mathcal{A}$, которую построим по шагам.

Носитель структуры $\mathcal{A}$ будет равен $\{a_e : e \in \omega\} \cup \{b_i : i \in \omega\}$. В конструкции будем придерживаться следующего правила: $[a_i]_{\mathcal{A}} \neq [a_j]_{\mathcal{A}}$ при $i \neq j$.

На шаге 0 задаем $\mathcal{A}_0 = \emptyset$.

Шаг $s + 1$. Пусть конечная структура $\mathcal{A}_s$ уже построена. Добавляем элемент a_s в структуру $\mathcal{A}_{s+1}$. Для каждого $e \leq s$ осуществляем следующие действия. Если $\varphi_{e,s}^p(\emptyset) \uparrow$, то добавляем в класс $[a_e]_{\mathcal{A}_{s+1}}$ элемент b_m с наименьшим индексом m такой, что этот b_m ранее не был добавлен в $\mathcal{A}_{s+1}$.

Конструкция описана. Полагаем $\mathcal{A} = \bigcup_{s \in \omega} \mathcal{A}_s$. В силу того, что для каждого $\beta \in (\omega \setminus \{0\}) \cup \{\omega\}$ структура $\mathcal{E}_p = \mathcal{U} \sqcup \mathcal{A}$ имеет бесконечно много классов размера β , получаем, что $\mathcal{E}_p \cong \mathcal{U}$. Нетрудно понять, что структура $\mathcal{E}_p$ вычислима относительно оракула p .

Заметим, что для всех $e \in \omega$ и $m \geq 1$ выполнено: $\text{card}([a_e]_{\mathcal{A}}) \geq m$ тогда и только тогда, когда $\text{card}([a_e]_{\mathcal{A}_{e+m}}) \geq m$. Кроме того, для данного b_i можно p -вычислимо найти такой индекс e , что $b_i \in [a_e]_{\mathcal{A}}$. Отсюда следует, что множество

$$K(\mathcal{E}_p) = \{(c, m) : \text{card}([c]_{\mathcal{E}_p}) \geq m\}$$

вычислимо относительно оракула p . Применяя релятивизованную версию теоремы 16, получаем, что структура $\mathcal{E}_p$ p -разрешима (равномерно относительно p).

Пусть теперь θ — это произвольное элементарное вложение из $\mathcal{E}_p$ в $\mathcal{U}$. По предложению 14 п. б) получаем, что для любого $c \in \mathcal{E}_p$ верно $\text{card}([c]_{\mathcal{E}_p}) = \text{card}([\theta(c)]_{\mathcal{U}})$. Отсюда вытекает следующее:

- если $\varphi_e^p(\emptyset) \downarrow$, то мощность $\text{card}([\theta(a_e)]_{\mathcal{U}})$ конечна;
- если $\varphi_e^p(\emptyset) \uparrow$, то $\text{card}([\theta(a_e)]_{\mathcal{U}}) = \omega$.

Получаем, что зная θ , можно (равномерно по θ) вычислить скачок $J(p)$. Выводим (применяя теорему 4), что $\lim \equiv_{sW} J \leq_{sW} \text{ElEm}(\text{any}, \text{sat})$. Предложение 17 и теорема 11 доказаны. $\square$

Список литературы

- [1] S.G. Simpson, *Subsystems of second order arithmetic. Second edition.* Cambridge Univ. Press, Cambridge, 2009.
DOI: <https://doi.org/10.1017/CBO9780511581007>
- [2] D.R. Hirschfeldt, *Slicing the truth: On the computable and reverse mathematics of combinatorial principles.* World Scientific Publishing Co., Hackensack, NJ, 2015.
DOI: <https://doi.org/10.1142/9208>
- [3] D.R. Hirschfeldt, R.A. Shore, T.A. Slaman, *The atomic model theorem and type omitting*, Trans. Amer. Math. Soc. **361** (11), 5805–5837 (2009).
DOI: <https://doi.org/10.1090/S0002-9947-09-04847-8>
- [4] D.R. Belanger, *Reverse mathematics of first-order theories with finitely many models*, J. Symb. Log. **79** (3), 955–984 (2014).
DOI: <https://doi.org/10.1017/jsl.2014.32>
- [5] D.R. Belanger, *WK_L and induction principles in model theory*, Ann. Pure Appl. Logic **166** (7–8), 767–799 (2015).
DOI: <https://doi.org/10.1016/j.apal.2015.04.001>
- [6] P. Cholak, C. McCoy, *Effective prime uniqueness*, Proc. Amer. Math. Soc. **145** (12), 5363–5379 (2017).
DOI: <https://doi.org/10.1090/proc/13675>
- [7] D.R. Hirschfeldt, K. Lange, R.A. Shore, *Induction, bounding, weak combinatorial principles, and the homogeneous model theorem*, Mem. Amer. Math. Soc. **249** (1187), 2017.
DOI: <https://doi.org/10.1090/memo/1187>
- [8] K. Harris, *The reverse mathematics of saturated models*, preprint (2006).
- [9] V. Brattka, *Weihrauch complexity and the Hagen school of computable analysis*, arXiv:2203.06166 (2022).
DOI: <https://doi.org/10.48550/arXiv.2203.06166>
- [10] V. Brattka, G. Gherardi, A. Pauly, *Weihrauch complexity in computable analysis*, in: Handbook of Computability and Complexity in Analysis, Springer, Cham, 367–417 (2021).
DOI: https://doi.org/10.1007/978-3-030-59234-9_11
- [11] Г. Кейслер, Ч.Ч. Чэн, *Теория моделей*, Мир, М., 1977.
- [12] F.G. Dorais, D.D. Dzhafarov, J.L. Hirst, J.R. Mileti, P. Shafer, *On uniform relationships between combinatorial problems*, Trans. Amer. Math. Soc. **368** (2), 1321–1359 (2016).
DOI: <https://doi.org/10.1090/tran/6465>

- [13] Н.А. Баженов, М.И. Марчук, *Степени автоустойчивости относительно сильных конструктивизаций графов*, Сиб. матем. журн. **59** (4), 719–735 (2018).
DOI: <https://doi.org/10.17377/smzh.2018.59.401>
- [14] D. Marker, *Model theory: An introduction*, Springer, New York, 2002.
DOI: <https://doi.org/10.1007/b98860>
- [15] W. Hodges, *Model theory*, Cambridge Univ. Press, Cambridge, 1993.
DOI: <https://doi.org/10.1017/CBO9780511551574>
- [16] J.G. Rosenstein, *Linear orderings*, Academic Press, New York, 1982.
URL: <https://www.sciencedirect.com/bookseries/pure-and-applied-mathematics/vol/98>
- [17] D. Cenzer, V. Harizanov, J.B. Remmel, Σ_1^0 and Π_1^0 equivalence structures, Ann. Pure Appl. Logic **162** (7), 490–503 (2011).
DOI: <https://doi.org/10.1016/j.apal.2011.01.002>

Николай Алексеевич Баженов

Институт математики им. С.Л. Соболева СО РАН,
пр. Акад. Коптюга, д. 4, г. Новосибирск, 630090, Россия,
e-mail: bazhenov@math.nsc.ru

Маргарита Игоревна Марчук

Институт математики им. С.Л. Соболева СО РАН,
пр. Акад. Коптюга, д. 4, г. Новосибирск, 630090, Россия,
e-mail: margaretmarchuk@gmail.com

Марта Фьори-Каронес

Институт математики им. С.Л. Соболева СО РАН,
пр. Акад. Коптюга, д. 4, г. Новосибирск, 630090, Россия,
e-mail: marta.floricarones@outlook.it

Elementary embeddability with respect to Weihrauch reducibility

N.A. Bazhenov, M.I. Marchuk, M. Fiori-Carones

Abstract. We study the Weihrauch complexity for problems of finding an elementary embedding (within the framework of the classical model theory). We prove that the problem of finding an elementary embedding from a prime model $\mathcal{M}$ into an arbitrary model $\mathcal{N}$ (which is elementarily equivalent to $\mathcal{M}$) is strongly Weihrauch equivalent to the familiar problem lim (i.e., the problem of finding the limit of a sequence in Baire space). We show that the problem of finding an elementary embedding from an arbitrary model $\mathcal{M}$ into a countable saturated model $\mathcal{N}$ is also strongly Weihrauch equivalent to lim .

Keywords: Weihrauch reducibility, elementary embedding, prime model, countable saturated model.

DOI: 10.26907/2949-3919.2024.4.4-23

References

- [1] S.G. Simpson, *Subsystems of second order arithmetic. Second edition.* Cambridge Univ. Press, Cambridge, 2009.
DOI: <https://doi.org/10.1017/CBO9780511581007>
- [2] D.R. Hirschfeldt, *Slicing the truth: On the computable and reverse mathematics of combinatorial principles.* World Scientific Publishing Co., Hackensack, NJ, 2015.
DOI: <https://doi.org/10.1142/9208>
- [3] D.R. Hirschfeldt, R.A. Shore, T.A. Slaman, *The atomic model theorem and type omitting*, Trans. Amer. Math. Soc. **361** (11), 5805–5837 (2009).
DOI: <https://doi.org/10.1090/S0002-9947-09-04847-8>
- [4] D.R. Belanger, *Reverse mathematics of first-order theories with finitely many models*, J. Symb. Log. **79** (3), 955–984 (2014).
DOI: <https://doi.org/10.1017/jsl.2014.32>
- [5] D.R. Belanger, *WKL_0 and induction principles in model theory*, Ann. Pure Appl. Logic **166** (7–8), 767–799 (2015).
DOI: <https://doi.org/10.1016/j.apal.2015.04.001>

Acknowledgements. The work of N.A. Bazhenov and M.I. Marchuk was carried out within the framework of the state contract of the Sobolev Institute of Mathematics (project no. FWNF-2022-0011).

-
- [6] P. Cholak, C. McCoy, *Effective prime uniqueness*, Proc. Amer. Math. Soc. **145** (12), 5363–5379 (2017).
DOI: <https://doi.org/10.1090/proc/13675>
- [7] D.R. Hirschfeldt, K. Lange, R.A. Shore, *Induction, bounding, weak combinatorial principles, and the homogeneous model theorem*, Mem. Amer. Math. Soc. **249** (1187), 2017.
DOI: <https://doi.org/10.1090/memo/1187>
- [8] K. Harris, *The reverse mathematics of saturated models*, preprint (2006).
- [9] V. Brattka, *Weihrauch complexity and the Hagen school of computable analysis*, arXiv:2203.06166 (2022).
DOI: <https://doi.org/10.48550/arXiv.2203.06166>
- [10] V. Brattka, G. Gherardi, A. Pauly, *Weihrauch complexity in computable analysis*, in: Handbook of Computability and Complexity in Analysis, Springer, Cham, 367–417 (2021).
DOI: https://doi.org/10.1007/978-3-030-59234-9_11
- [11] C.C. Chang, H.J. Keisler, *Model theory*, North-Holland, Amsterdam, 1973.
URL: <https://www.sciencedirect.com/bookseries/studies-in-logic-and-the-foundations-of-mathematics/vol/73/>
- [12] F.G. Dorais, D.D. Dzhabarov, J.L. Hirst, J.R. Mileti, P. Shafer, *On uniform relationships between combinatorial problems*, Trans. Amer. Math. Soc. **368** (2), 1321–1359 (2016).
DOI: <https://doi.org/10.1090/tran/6465>
- [13] N.A. Bazhenov, M.I. Marchuk, *Degrees of autostability relative to strong constructivizations of graphs*, Siberian Math. J. **59** (4), 565–577 (2018).
DOI: <https://doi.org/10.1134/S0037446618040018>
- [14] D. Marker, *Model theory: An introduction*, Springer, New York, 2002.
DOI: <https://doi.org/10.1007/b98860>
- [15] W. Hodges, *Model theory*, Cambridge Univ. Press, Cambridge, 1993.
DOI: <https://doi.org/10.1017/CBO9780511551574>
- [16] J.G. Rosenstein, *Linear orderings*, Academic Press, New York, 1982.
URL: <https://www.sciencedirect.com/bookseries/pure-and-applied-mathematics/vol/98>
- [17] D. Cenzer, V. Harizanov, J.B. Remmel, Σ_1^0 and Π_1^0 equivalence structures, Ann. Pure Appl. Logic **162** (7), 490–503 (2011).
DOI: <https://doi.org/10.1016/j.apal.2011.01.002>

Nikolay Alekseyevich Bazhenov

Sobolev Institute of Mathematics,
4 Acad. Koptug Ave., Novosibirsk 630090, Russia,
e-mail: bazhenov@math.nsc.ru

Margarita Igorevna Marchuk

Sobolev Institute of Mathematics,
4 Acad. Koptug Ave., Novosibirsk 630090, Russia,
e-mail: margaretmarchuk@gmail.com

Marta Fiori-Carones

Sobolev Institute of Mathematics,
4 Acad. Koptug Ave., Novosibirsk 630090, Russia,
e-mail: marta.fioricarones@outlook.it

О мультипликативно идемпотентных полукольцах с уравнительными свойствами

Е.М. Вечтомов

Аннотация. Изучается один класс полуколец, близких к дистрибутивным решеткам, именно: полукольца с коммутативным идемпотентным умножением, удовлетворяющие тождеству $x + 2xy = x$. Для таких полуколец исследуются уравнительные свойства (теоремы 7, 8, 10, предложение 12). Полученные результаты применены к дистрибутивным решеткам (предложения 15, 16, 17). Приведены примеры и поясняющие замечания.

Ключевые слова: мультипликативно идемпотентное полукольцо, дистрибутивная решетка, уравнительное условие, аннуляторное условие, уравнительное свойство.

DOI: 10.26907/2949-3919.2024.4.24-34

1. Предварительные сведения

Статья посвящена теории полуколец с дополнительными условиями; в ней продолжается изучение мультипликативно идемпотентных полуколец и дистрибутивных решеток, обладающих различными уравнительными свойствами [1–3].

Полукольцом называется алгебраическая структура $\langle S, +, \cdot \rangle$ с двумя бинарными операциями: коммутативно-ассоциативной операцией сложения $+$ и ассоциативной операцией умножения $\cdot$, дистрибутивной относительно сложения с обеих сторон. Полукольцо с коммутативным умножением называется *коммутативным*. Если полукольцо S имеет элемент, нейтральный по сложению и поглощающий по умножению, то такой элемент называется *нулем* полукольца S и обозначается 0 , а S называется *полукольцом с нулем*. Если S имеет нейтральный по умножению элемент, называемый *единицей* полукольца S и обозначаемый 1 , то S называется *полукольцом с единицей*. Полукольцо с тождеством идемпотентности $xx = x$ ($x + x = x$) называется *мультипликативно идемпотентным* (соответственно, *аддитивно идемпотентным*). Полукольцо называется *идемпотентным*, если оно мультипликативно идемпотентно и аддитивно идемпотентно. Мультипликативно идемпотентные кольца называются *булевыми*; они коммутативны и удовлетворяют тождеству $x + x = 0$.

Благодарности. Работа выполнена при поддержке Российского научного фонда, проект №24-21-00117.

Для полуколец естественным образом определяются понятия подполукольца, идеала, конгруэнции, фактор-полукольца, прямого произведения полуколец (см. [4]). Теории мультипликативно идемпотентных полуколец посвящена книга [2].

Базовые сведения о решетках можно найти в монографиях [5, 6].

Хорошо известны два эквивалентных определения *решетки* – порядковое и алгебраическое [6, теорема 1, с. 20–21]. При порядковом подходе решетка определяется как упорядоченное множество $\langle L, \leq \rangle$, любые элементы a, b которого имеют точную верхнюю грань $\sup\{a, b\}$ и точную нижнюю грань $\inf\{a, b\}$. В алгебраическом смысле решеткой называется алгебраическая структура $\langle L, +, \cdot \rangle$ с двумя идемпотентными коммутативными ассоциативными операциями $+$ и $\cdot$, связанными законами *поглощения* $x + xy = x$ и $x(x + y) = x$. При этом для любых элементов a, b решетки L выполняются соотношения: $a + b = \sup\{a, b\}$, $ab = \inf\{a, b\}$ и $a \leq b \Leftrightarrow a + b = b$, равносильно, $ab = a$. Решетки L удобно рассматривать как алгебраические системы $\langle L, +, \cdot, \leq \rangle$.

Решетка с тождеством $x(y + z) = xy + xz$, равносильно, с тождеством $x + yz = (x + y)(x + z)$, называется *дистрибутивной*. Легко видеть, что дистрибутивные решетки суть в точности коммутативные мультипликативно идемпотентные полукольца, удовлетворяющие тождеству поглощения $x + xy = x$.

Дистрибутивные решетки и булевы кольца принадлежат классу коммутативных мультипликативно идемпотентных полуколец, удовлетворяющих тождеству $x + 2xy = x$.

Замечание 1. Коммутативные мультипликативно идемпотентные полукольца с тождеством $x + 2xy = x$ рассматривались в работах [7, р. 119], [2, с. 160–161]. Они образуют многообразие полуколец, порожденное двухэлементной цепью и двухэлементным полем. Такие полукольца являются подпрямыми произведениями булева кольца и дистрибутивной решетки.

Непустое подмножество F полукольца S назовем *коидеалом* в S , если $ab \in F$ и $a + x \in F$ для любых элементов $a, b \in F$ и $x \in S$. Ясно, что идеалы и коидеалы любого полукольца являются его подполукольцами.

Пусть L – произвольная решетка. Непустое подмножество F решетки L называется ее *фильтром*, если соотношения $a, b \in F$ и $a \leq x \in L$ влекут $ab \in F$ и $x \in F$ (заметим, что $a \leq x \Leftrightarrow a + x = x$). Коидеалы и фильтры решетки L совпадают. Подрешетка A решетки L называется *выпуклой*, если для любых элементов $a \leq b$ из A весь интервал $[a, b] = \{x \in L : a \leq x \leq b\}$ лежит в A . Выпуклые подрешетки решетки L – это в точности непустые пересечения некоторых идеала и фильтра в L [6, лемма 6, с. 38]. Решетка с нулем 0 и ненулевой единицей 1 называется *ограниченной*.

Неодноэлементная ограниченная дистрибутивная решетка L называется *булевой*, если каждый ее элемент a имеет дополнение $a' \in L$ (оно единственно): $a + a' = 1$ и $aa' = 0$. Дистрибутивная решетка с нулем называется *обобщенной булевой решеткой*, если она обладает относительными дополнениями. Напомним, что *относительным дополнением* элемента b до элемента a в решетке L с нулем 0 называется такой элемент $a \setminus b \in L$, что

$(a \setminus b)b = 0$ и $(a \setminus b) + b = a + b$. В дистрибутивных решетках с нулем имеющиеся относительные дополнения единственны. Легко видеть, что обобщенные булевы решетки – это в точности дистрибутивные решетки L с нулем, ненулевые главные идеалы aL которых являются булевыми решетками с единицами a . С другой стороны, любая булева решетка L будет неоднородной обобщенной булевой решеткой, в которой $a \setminus b = ab'$ для любых $a, b \in L$.

Для произвольных элементов a, c полукольца S обозначим через $\text{Eq}(a, c)$ их (левый) *уравнитель* $\{x \in S : xa = xc\}$, а через $\text{Seq}(a, c)$ – их *коуравнитель* $\{x \in S : x + a = x + c\}$. Скажем, что полукольцо S удовлетворяет *уравнительному условию*, соответственно, *коуравнительному условию*, если

$$\forall a, b, c \in S \quad (\text{Eq}(a, c) = \text{Eq}(b, c) \Rightarrow a = b),$$

соответственно, $\forall a, b, c \in S \quad (\text{Seq}(a, c) = \text{Seq}(b, c) \Rightarrow a = b)$.

Для элемента a полукольца S с нулем 0 (с единицей 1) определим (левый) *аннулятор* $\text{Ann } a = \{x \in S : xa = 0\}$ (соответственно, *коаннулятор* $\text{Can } a = \{x \in S : x + a = 1\}$). Полукольцо S с 0 (с единицей 1) называется полукольцом с *аннуляторным условием* (соответственно, с *коаннуляторным условием*), если различные его элементы имеют различные аннуляторы (различные коаннуляторы).

Отметим, что мультипликативно идемпотентные полукольца и дистрибутивные решетки, удовлетворяющие аннуляторному условию, рассматривались в статьях [1, 3].

Замечание 2. Если S – полукольцо с нулем 0 , то $\text{Eq}(a, 0) = \text{Ann } a$ для любого $a \in S$. Пусть теперь S – полукольцо с единицей 1 . Тогда равенство $\text{Seq}(a, 1) = \text{Can } a$ при фиксированном элементе $a \in S$ эквивалентно формуле

$$\forall x \in S \quad (x + a = x + 1 \Leftrightarrow x + a = 1),$$

которая, в свою очередь, эквивалентна формуле

$$\forall x \in S \quad (x + a = 1 \Rightarrow x + 1 = 1).$$

Отметим, что коммутативные мультипликативно идемпотентные полукольца с тождеством $x + 1 = 1$ (влекущим закон поглощения $xy + y = y$) и коммутативные идемпотентные полукольца с тождеством $x + 2xy = x$ будут дистрибутивными решетками.

Для произвольного полукольца $\langle S, +, \cdot \rangle$ обозначим через $L(S)$ алгебраическую структуру $\langle S, \vee, \cdot \rangle$, где $a \vee b = a + ab + b$ для любых $a, b \in S$.

Нам понадобятся следующие утверждения.

Лемма 3 ([3, свойства 1 и 2 предложения 3]). *Мультипликативно идемпотентные полукольца с аннуляторным условием коммутативны и удовлетворяют тождеству $x + 2xy = x$.*

Лемма 4. Для того чтобы коммутативное мультипликативно идемпотентное полукольцо S удовлетворяло тождеству $x + 2xy = x$, необходимо и достаточно, чтобы алгебраическая структура $L(S)$ была дистрибутивной решеткой.

Доказательство. Необходимость. Пусть дано коммутативное мультипликативно идемпотентное полукольцо S , удовлетворяющее тождеству $x + 2xy = x$. Его мультипликативная полугруппа – полурешетка $\langle S, \cdot \rangle$ – определяет порядок $\leq$ на S по правилу: $a \leq b \Leftrightarrow ab = a$ для любых $a, b \in S$, причем, $ab = \inf\{a, b\}$. Покажем, что $a \vee b = \sup\{a, b\}$ для любых элементов a, b упорядоченного множества $\langle S, \leq \rangle$. Поскольку $a(a \vee b) = a(a + ab + b) = a + 2ab = a$, то $a \leq a \vee b$. Аналогично, $b \leq a \vee b$. Значит, $a \vee b$ – верхняя грань множества $\{a, b\}$. Возьмем произвольную верхнюю грань $c \in S$ множества $\{a, b\}$, т. е. $ac = a$ и $bc = b$. Тогда

$$(a \vee b)c = (a + ab + b)c = ac + abc + bc = a + ab + b = a \vee b,$$

т. е. $a \vee b \leq c$. Следовательно, $a \vee b = \sup\{a, b\}$. Получаем решетку $\langle S, \leq \rangle$ в порядковом смысле или, равносильно, решетку $\langle S, \vee, \cdot \rangle$ как алгебраическую структуру. Для любых $a, b, c \in S$ имеем $(a \vee b)c = (a + ab + b)c = ac + (ac)(bc) + bc = (ac) \vee (bc)$, что доказывает дистрибутивность решетки $L(S) = \langle S, \vee, \cdot \rangle$.

Достаточность. Если $L(S)$ – дистрибутивная решетка, то для любых элементов $a, b \in S$ имеем $a = a(a \vee b) = a(a + ab + b) = a + ab + ab = a + 2ab$. $\square$

Замечание 5. Для произвольного булева кольца S дистрибутивная решетка $L(S)$ является обобщенной булевой решеткой, в которой $a \setminus b = a + ab$ для всех $a, b \in S$. Обратно, если $L = \langle L, \vee, \cdot \rangle$ – обобщенная булева решетка, то $S = \langle L, +, \cdot \rangle$ будет булевым кольцом при $a + b = (a \setminus b) \vee (b \setminus a)$ для всех $a, b \in L$; при этом $L(S) = L$. Получаем естественное взаимно однозначное соответствие между классом булевых колец (булевых колец с ненулевой единицей) и классом обобщенных булевых решеток (булевых решеток). Подробности в [6, с. 109, теорема 9].

Пример 6. Всякий коидеал F полукольца S является фильтром решетки $L(S)$. Действительно, пусть F – коидеал полукольца S . Если $a \in F$, $x \in L(S) = S$ и $a \leq x$, то $x = a \vee x = a + (ax + x) \in F$. Значит, F – фильтр решетки $L(S)$.

Обратное утверждение неверно. Возьмем булево кольцо S с $1 \neq 0$. Тогда $L(S)$ будет булевой решеткой. Пусть F – собственный фильтр решетки $L(S)$, например, $F = \{1\}$. Если $a \in F$, то $a + a = 0 \notin F$, стало быть, F не является коидеалом полукольца S .

2. Полукольца с уравнительным условием

Докажем несколько утверждений о свойствах мультипликативно идемпотентных полуколец с уравнительным условием.

Теорема 7. Для того чтобы мультипликативно идемпотентное полукольцо S с нулем 0 удовлетворяло уравнительному условию, необходимо и достаточно, чтобы S удовлетворяло аннуляторному условию.

Доказательство. Необходимость. Возьмем мультипликативно идемпотентное полукольцо S с нулем 0 , обладающее уравнительным свойством. Имеем $\text{Eq}(a, 0) = \text{Ann } a$ для любого элемента $a \in S$. Поэтому уравнительное свойство полукольца S при $c = 0$ влечет аннуляторное условие.

Достаточность. Рассмотрим мультипликативно идемпотентное полукольцо S с аннуляторным условием. Полукольцо S коммутативно по лемме 3. Пусть $\text{Eq}(a, c) = \text{Eq}(b, c)$ для некоторых элементов $a, b, c \in S$. Имеем $ac \in \text{Eq}(a, c)$ и $bc \in \text{Eq}(b, c)$. Поэтому $ac = abc = bc$. Предположим от противного, что $a \neq b$. Тогда по условию $\text{Ann } a \neq \text{Ann } b$, скажем, $ax = 0$, но $bx \neq 0$. Для элемента $ac + bx$ получаем

$$a(ac + bx) = ac + bax = ac = ac + axc = ac + bxc = c(ac + bx),$$

т.е. $ac + bx \in \text{Eq}(a, c)$. Но $b(ac + bx) = ac + bx \neq ac$, поскольку равенство $ac + bx = ac$ влечет $acx + bx = acx$ и $bx = 0$, что невозможно. Поэтому $ac + bx \notin \text{Eq}(b, c)$. Следовательно, $\text{Eq}(a, c) \neq \text{Eq}(b, c)$. Получили противоречие. $\square$

В теореме 7 вместо (левого) уравнительного условия можно взять правое или двустороннее уравнительное условие.

Теорема 8. *Любой идеал коммутативного мультипликативно идемпотентного полукольца S с тождеством $x + 2xu = x$, удовлетворяющего уравнительному условию, является полукольцом с уравнительным условием.*

Доказательство. Пусть полукольцо S удовлетворяет условиям теоремы и J – идеал в S . Возьмем элементы $a, b, c \in J$, для которых $\text{Eq}(a, c) = \text{Eq}(b, c)$ в полукольце J . Покажем, что $\text{Eq}(a, c) = \text{Eq}(b, c)$ в полукольце S . Тогда получим $a = b$, что и требуется доказать. Допустим, что $xa = xc$ для некоторого элемента $x \in S$. Рассмотрим элемент $a \vee b \vee c$, принадлежащий – по леммам 3 и 4 – идеалу J . Имеем $x(a \vee b \vee c) \in J$ и $(a \vee b \vee c)a = a$, $(a \vee b \vee c)b = b$, $(a \vee b \vee c)c = c$. Поэтому $x(a \vee b \vee c) \in \text{Eq}(a, c)$, значит, $x(a \vee b \vee c) \in \text{Eq}(b, c)$ в J . Откуда $xb = x(a \vee b \vee c)b = x(a \vee b \vee c)c = xc$. Стало быть, $\text{Eq}(a, c) \subseteq \text{Eq}(b, c)$ в полукольце S . В силу равноправности элементов a и b получаем также включение $\text{Eq}(b, c) \subseteq \text{Eq}(a, c)$ в S . Тем самым, $\text{Eq}(a, c) = \text{Eq}(b, c)$ в S , и теорема доказана. $\square$

Из теорем 7 и 8 вытекает

Следствие 9 ([3, свойство 6 предложения 3]). *Все идеалы мультипликативно идемпотентного полукольца с аннуляторным условием будут полукольцами с аннуляторным условием.*

Теорема 10. *Для произвольного коммутативного мультипликативно идемпотентного полукольца S с тождеством $x + 2xu = x$ равносильны следующие утверждения:*

- 1) полукольцо S удовлетворяет уравнительному условию;
- 2) все идеалы полукольца S удовлетворяют уравнительному условию;

- 3) любой коидеал с нулем полукольца S является полукольцом с аннуляторным условием;
- 4) если пересечение идеала и коидеала с нулем в полукольце S не пусто, то оно будет полукольцом с аннуляторным условием.

Доказательство. 1) $\Rightarrow$ 2) по теореме 8.

2) $\Rightarrow$ 3). Предположим, что полукольцо S удовлетворяет уравнительному условию и F – его коидеал с нулем θ . Возьмем такие элементы $a, b \in F$, что $\text{Ann } a = \text{Eq}(a, \theta) = \text{Eq}(b, \theta) = \text{Ann } b$ в полукольце F . Покажем, что $\text{Eq}(a, \theta) = \text{Eq}(b, \theta)$ в самом полукольце S . Тогда по условию $a = b$. Значит, F будет полукольцом с аннуляторным условием. Пусть $x \in S$ и $xa = x\theta$. Имеем $x + \theta \in F$ и $(x + \theta)a = xa + \theta a = x\theta + \theta = (x + \theta)\theta$. Поэтому $(x + \theta)b = (x + \theta)\theta$. Откуда $xb + \theta = \theta$ и $xb + xb\theta = xb\theta = x\theta$. Так как $\theta + \theta = \theta$, то $xb\theta = 2xb\theta$. Значит, $xb = xb + 2xb\theta = xb + xb\theta = x\theta$. В полукольце S имеем $\text{Eq}(a, \theta) \subseteq \text{Eq}(b, \theta)$. Аналогично, $\text{Eq}(a, \theta) \supseteq \text{Eq}(b, \theta)$. Тем самым, $\text{Eq}(a, \theta) = \text{Eq}(b, \theta)$ в самом полукольце S .

3) $\Rightarrow$ 4) по теореме 8.

4) $\Rightarrow$ 1). В силу 4) в полукольце S каждый коидеал с нулем является полукольцом с аннуляторным условием. Возьмем в S произвольные элементы a, b, c , для которых $\text{Eq}(a, c) = \text{Eq}(b, c)$. Требуется доказать, что $a = b$. Положим $\theta = 2abc$ и рассмотрим множество $F = \{x \in S : x\theta = \theta\}$. Имеем $a, b, c \in F$ и $\theta + \theta = 4abc = 2abc = \theta$. Пусть $x, y \in F$ и $z \in S$. Тогда $(xy)\theta = \theta$ и $(x + z)\theta = x\theta + z\theta = \theta + 2z\theta = \theta$. Значит, F – коидеал полукольца S . Кроме того, $x\theta = \theta$ и $x + \theta = x + 2x\theta = x$, т.е. θ служит нулем полукольца F . По условию F будет полукольцом с аннуляторным условием. Равенство $\text{Eq}(a, c) = \text{Eq}(b, c)$ выполняется и в F . Тогда $a = b$ в силу теоремы 7. $\square$

Замечание 11. Для краткости, рассматриваемые уравнительное, коуравнительное, аннуляторное и коаннуляторное условия будем называть просто *уравнительными свойствами*.

Легко видеть, что имеет место

Предложение 12. *Справедливы следующие утверждения:*

- 1) *прямое произведение любого непустого семейства полуколец с данным уравнительным свойством удовлетворяет этому уравнительному свойству;*
- 2) *если прямое произведение непустого семейства полуколец с нулем удовлетворяет некоторому уравнительному свойству, то все сомножители также удовлетворяют этому уравнительному свойству;*
- 3) *прямая сумма непустого семейства полуколец с нулем будет полукольцом с уравнительным свойством тогда и только тогда, когда все ее слагаемые являются полукольцами с этим же уравнительным свойством.*

Пример 13. Произвольное кольцо R удовлетворяет коуравнительному условию. В самом деле, если $\text{Seq}(a, c) = \text{Seq}(b, c)$ для некоторых элементов $a, b, c \in R$, то выполнение равенств $x + a = x + c$ и $x + b = x + c$ в кольце R влечет $a = c = b$. В кольцах с единицей выполняется и коаннуляторное условие. Однако, кольца с аннуляторным условием

суть в точности булевы кольца [1, теорема 1]. Поэтому любое небулево кольцо, будучи полукольцом с коуравнительным условием, не удовлетворяет уравнительному условию по теореме 7. Булевы же кольца с единицей обладают всеми четырьмя рассматриваемыми уравнительными свойствами, т. е. удовлетворяют уравнительному, коуравнительному, аннуляторному и коаннуляторному условиям.

3. Случай дистрибутивных решеток

Рассмотрим применения теорем 7, 8, 10 к дистрибутивным решеткам L , для которых условия этих теорем очевидным образом справедливы.

Замечание 14. Дистрибутивная решетка L обладает некоторым уравнительным свойством тогда и только тогда, когда двойственная ей дистрибутивная решетка L' обладает двойственным уравнительным свойством.

Поэтому из теоремы 7 вытекает

Предложение 15. *Дистрибутивная решетка с единицей удовлетворяет коуравнительному условию тогда и только тогда, когда она удовлетворяет коаннуляторному условию.*

Из теоремы 8 в силу замечания 14 следует

Предложение 16. *Любой фильтр дистрибутивной решетки с коуравнительным условием (с коаннуляторным условием) является дистрибутивной решеткой с коуравнительным условием (соответственно, с коаннуляторным условием).*

Из теоремы 10 и замечания 14 вытекает

Предложение 17. *Для произвольной дистрибутивной решетки L эквивалентны следующие утверждения:*

- 1) L удовлетворяет коуравнительному условию;
- 2) все фильтры в L удовлетворяют коуравнительному условию;
- 3) любой главный идеал решетки L удовлетворяет коаннуляторному условию;
- 4) любая выпуклая подрешетка решетки L , обладающая наибольшим элементом, удовлетворяет коаннуляторному условию.

Приведем ряд примеров дистрибутивных решеток с теми или иными уравнительными свойствами.

Пример 18. Всякая обобщенная булева решетка L удовлетворяет уравнительному и коуравнительному условиям. Возьмем в L элементы $a \neq b$. Тогда $a \setminus b \neq 0$ или $b \setminus a \neq 0$, ибо иначе $b = (a \setminus b) + b = a + b = (b \setminus a) + a = a$. Скажем, $a \setminus b \neq 0$. Имеем $a \setminus b \in \text{Ann } b$, но $a \setminus b \notin \text{Ann } a$, так как

$$(a \setminus b)a = (a \setminus b)a + (a \setminus b)b = (a \setminus b)(a + b) = (a \setminus b)(a \setminus b + b) = a \setminus b \neq 0.$$

Значит, L удовлетворяет аннуляторному условию. По теореме 7 L удовлетворяет и уравнительному условию. Каждый главный идеал J решетки L является булевой решеткой (как подрешетка в L), которая самодвойственна (взятие дополнения устанавливает изоморфизм между булевой решеткой J и двойственной к ней булевой решеткой J'). По уже доказанному булева решетка J' удовлетворяет уравнительному условию, стало быть, решетка $J = (J')'$ удовлетворяет коуравнительному условию. По предложению 17 сама решетка L также удовлетворяет коуравнительному условию.

Пример 19. Зафиксируем бесконечное множество A и возьмем в нем бесконечное подмножество B так, чтобы множество $A \setminus B$ было бесконечным. Образует решетку множеств

$$L = \{X \subseteq A : X \text{ конечно или } A \setminus X \text{ конечно или } X = (B \setminus Y) \cup Z \text{ для конечных } Y, Z \subseteq A\}.$$

Очевидно, L замкнуто относительно бинарных операций $\cup$ и $\cap$ множеств. Как легко видеть, получаем небулеву ограниченную дистрибутивную решетку L с аннуляторным и коаннуляторным условиями. По теореме 7 и предложению 15 решетка L удовлетворяет уравнительному и коуравнительному условиям.

Пример 20. Возьмем бесконечное множество A . И пусть L есть решетка множеств, состоящая из конечных подмножеств в A и самого множества A . Получаем ограниченную дистрибутивную решетку L с аннуляторным условием, не удовлетворяющую коаннуляторному условию. По теореме 7 решетка L удовлетворяет уравнительному условию. По предложению 15 решетка L не удовлетворяет коуравнительному условию. Отметим, что ее подрешетка (наибольший идеал) $L \setminus \{A\}$ является обобщенной булевой решеткой. Двойственная решетка L' удовлетворяет коаннуляторному и коуравнительному условиям, но не удовлетворяет ни аннуляторному, ни уравнительному условию.

Пример 21. Всякая неодноэлементная конечная небулева дистрибутивная решетка L не удовлетворяют ни аннуляторному, ни коаннуляторному условию. Действительно, любая неодноэлементная конечная дистрибутивная решетка с аннуляторным условием булева [1, замечание 2]. Поэтому в силу замечания 14 любая неодноэлементная конечная дистрибутивная решетка с коаннуляторным условием также будет булевой. Следовательно, по предложениям 15 и 17 решетка L не удовлетворяет ни уравнительному условию, ни коуравнительному условию.

Замечание 22. Руководствуясь предложением 12 и примерами 13, 18, 19, 20 и 21 мы можем получить примеры коммутативных мультипликативно идемпотентных полуколец S с тождеством $x + 2xy = x$, не являющихся дистрибутивными решетками, обладающих наперед заданными уравнительными свойствами. Пусть R – неодноэлементное булево кольцо с единицей, L – ограниченная дистрибутивная решетка из примеров 18, 19, 20 или 21, и пусть $S = R \times L$ – их прямое произведение. В силу предложения 12 и примера 13 полукольцо S обладает некоторым уравнительным свойством тогда и только тогда, когда этим свойством обладает дистрибутивная решетка L .

Список литературы

- [1] Е.М. Вечтомов, *Аннуляторные характеристики булевых колец и булевых решеток*, Матем. заметки **53** (2), 15–24 (1993).
URL: <https://www.mathnet.ru/rus/mzm3943>
- [2] Е.М. Вечтомов, А.А. Петров, *Функциональная алгебра и полукольца. Полукольца с идемпотентным умножением*, Лань, Санкт-Петербург, 2023.
URL: <https://e.lanbook.com/book/302885>
- [3] Е.М. Вечтомов, А.А. Петров, *Мультипликативно идемпотентные полукольца с аннуляторным условием*, Изв. вузов. Матем. (3), 29–40 (2023).
DOI: <https://doi.org/10.26907/0021-3446-2023-3-29-40>
- [4] J.S. Golan, *Semirings and their applications*, Kluwer Academic Publ., Dordrecht-Boston-London, 1999.
DOI: <https://doi.org/10.1007/978-94-015-9333-5>
- [5] Г. Биркгоф, *Теория решеток*, Наука, М., 1984.
- [6] Г. Гретцер, *Общая теория решеток*, Мир, М., 1982.
- [7] S. Ghosh, *A characterization of semirings which are subdirect products of a distributive lattice and a ring*, Semigroup Forum **59** (1), 106–120 (1999).
DOI: <https://doi.org/10.1007/PL00005999>

Евгений Михайлович Вечтомов

Вятский государственный университет,
ул. Московская, д. 36, г. Киров, 610000, Россия,
e-mail: vecht@mail.ru

About multiplicatively idempotent semirings with annihilator properties

E.M. Vechtomov

Abstract. We study one class of semirings close to distributive lattices, namely: semirings with commutative idempotent multiplication, satisfying the identity $x+2xy = x$. For such semirings, the equalizing properties are investigated (Theorems 7, 8, 10, Proposition 12). The results obtained can be applied to distributive lattices (Propositions 15, 16, 17). The work provides examples and explanatory notes.

Keywords: multiplicatively idempotent semiring, distributive lattice, equalizing condition, annihilator condition, equalizing property.

DOI: 10.26907/2949-3919.2024.4.24-34

References

- [1] E.M. Vechtomov, *Annihilator characterizations of boolean rings and boolean lattices*, Math. Notes **53** (2), 124–129 (1993).
DOI: <https://doi.org/10.1007/BF01208314>
- [2] E.M. Vechtomov, A.A. Petrov, *Functional algebra and semirings. Semirings with idempotent multiplication*, Lan, Saint Petersburg, 2023 [in Russian].
URL: [URL:https://e.lanbook.com/book/302885](https://e.lanbook.com/book/302885)
- [3] E.M. Vechtomov, A.A. Petrov, *Multiplicatively idempotent semirings with annihilator condition*, Russ. Math. **67** (3), 23–31 (2023).
DOI: <https://doi.org/10.3103/S1066369X23030064>
- [4] J.S. Golan, *Semirings and their applications*, Kluwer Academic Publ., Dordrecht-Boston-London, 1999.
DOI: <https://doi.org/10.1007/978-94-015-9333-5>
- [5] G. Birkhoff, *Lattice theory*, AMS Colloq. Publ., Providence, RI, 1979.
- [6] G. Grätzer, *General lattice theory*, Birkhäuser Verlag, Basel, 2003.

Acknowledgements. The work is supported by the Russian Science Foundation (grant no. 24-21-00117).

Received: 22 July 2024. Accepted: 02 September 2024. Published: 26 December 2024.

- [7] S. Ghosh, *A characterization of semirings which are subdirect products of a distributive lattice and a ring*, Semigroup Forum **59** (1), 106–120 (1999).
DOI: <https://doi.org/10.1007/PL00005999>

Evgenii Mikhailovich Vechtomov

Vyatka State University,

36 Moskovskay str., Kirov 610000, Russia,

e-mail: vecht@mail.ru

Некоторые свойства почти всех n -квазигрупп

А.В. Галатенко, В.В. Галатенко, А.Е. Панкратьев

Аннотация. Изучается “типичность” свойств простоты, неаффинности и полиномиальной полноты конечных n -квазигрупп. Показано, что при фиксированном n почти все n -квазигруппы сильно неаффинны, т. е. не изотопны аффинным. Найдено точное значение числа простых, аффинных и одновременно простых и аффинных n -квазигрупп порядка 4. Как следствие, показано, что почти все n -квазигруппы порядка 4 полиномиально полны и сильно неаффинны.

Ключевые слова: квазигруппа, n -квазигруппа, простота, аффинность, полиномиальная полнота.

DOI: 10.26907/2949-3919.2024.4.35-50

Введение

Конечные квазигруппы и их n -арные обобщения – конечные n -квазигруппы – становятся перспективной платформой для реализации различных криптографических примитивов (см., например, квазигрупповые обзоры [1, 2]). Для обеспечения высокой стойкости к используемым объектам предъявляются дополнительные требования, такие как бесформенность [3] и нефрактальность [4]. В.А. Артамоновым с соавторами было предложено использовать полиномиально полные квазигруппы (см., например, [5]), так как задача проверки разрешимости уравнений над полиномиально полными алгебрами NP-полна [6]. Известно, что полиномиальная полнота конечных n -квазигрупп эквивалентна одновременной простоте и неаффинности. Для случая квазигрупп порядка 4 в работе [7] были найдены мощности классов, определенных наличием и/или отсутствием свойств простоты и/или аффинности, однако некоторые из указанных в работе [7] значений требуют корректировки. Имеется ряд результатов о “типичности” свойства полиномиальной полноты. В.Л. Мурским было установлено, что при фиксированной значности логики почти все алгебры полиномиально полны [8]. Кэмерон доказал, что почти любая квазигрупповая операция и множество всех констант порождают знакопеременную группу [9], откуда по теореме Саломеа [10] следует, что почти все квазигруппы полиномиально полны. В работе [11] этот результат был усилен: оказалось, что почти все квазигруппы не изотопны квазигруппам, не являющимся полиномиально полными.

В нашей работе сперва изучается задача “типа Кэмерона”, когда арность n является фиксированной, а значность логики растет. В этом случае удастся показать, что почти все n -квазигруппы являются сильно неаффинными, т.е. не изотопны аффинным n -квазигруппам. Отметим, что с точки зрения криптографических приложений именно неаффинность является ключевым аспектом полиномиальной полноты, так как разрешимость систем уравнений над аффинными квазигруппами полиномиальна, а над неаффинными NP-полна [12]; кроме того, в ряде случаев (например, для n -квазигрупп простого порядка) свойство простоты заведомо выполнено. Затем исследуется задача “типа Мурского”, когда значность логики k фиксируется, а арность операции растет. В случае $k = 2$ задача тривиальна: для любого n имеется ровно две n -квазигруппы, являющиеся простыми и аффинными; при $k = 3$ ситуация аналогична: число n -квазигрупп равно $3 \cdot 2^n$ и все они простые и аффинные. Первый нетривиальный случай возникает при $k = 4$. Здесь удалось найти точные значения для чисел простых, аффинных и одновременно простых и аффинных квазигрупп, откуда следуют утверждения о полиномиальной полноте и сильной неаффинности почти всех n -квазигрупп порядка 4, а также исправленные значения мощностей классов квазигрупп, обладающих или не обладающих соответствующими свойствами. Отметим, для случая n -квазигрупп порядка 4 в работе [13] было доказано, что такие квазигруппы либо изотопны n -квазигруппам, не являющимся простыми, либо разложимы в неповторную суперпозицию n -квазигрупп меньшей арности.

Дальнейшее изложение имеет следующую структуру. В разделе 1 вводятся основные определения. В разделе 2 устанавливается сильная неаффинность почти всех n -квазигрупп при фиксированном n . В разделе 3 изучается случай n -квазигрупп порядка 4. Раздел 4 является заключением.

1. Основные определения и обозначения

Пусть $k, n \in \mathbb{N}$, $k, n \geq 2$.

Определение 1. n -квазигруппой порядка k называется пара (Q, f) , где $|Q| = k$, а $f: Q^n \rightarrow Q$ обратима по каждому аргументу.

В дальнейшем для краткости мы будем использовать термин “ n -квазигруппа”, а при $n = 2$ – термин “квазигруппа”. Без ограничения общности можно считать, что $Q = E_k = \{0, 1, \dots, k-1\}$, а f – функция k -значной логики арности n .

Пусть $x \oplus y$ обозначает сложение по модулю 2. Легко увидеть, что имеется ровно две n -квазигруппы порядка 2, для которых операция $f(x_1, \dots, x_n)$ имеет вид $x_1 \oplus x_2 \oplus \dots \oplus x_n \oplus c$, $c \in E_2$.

Для n -квазигрупп порядка 3 верен аналогичный результат: число n -квазигрупп равно $3 \cdot 2^n$, а операция $f(x_1, \dots, x_n)$ задается соотношением $c_0 + c_1 x_1 + c_2 x_2 + \dots + c_n x_n \pmod{3}$, где $c_0, c_1, \dots, c_n \in E_3$, $c_1, \dots, c_n \neq 0$ (см., например, [14]).

В работе [15] показано, что мощность Q_4 множества всех n -квазигрупп порядка 4 удовлетворяет соотношению

$$Q_4 = 4 \cdot 3^{n+1} \cdot 2^{2^{n+1}}(1 + o(1)), \quad n \rightarrow \infty. \quad (1)$$

В общем случае известные оценки существенно менее точные. В работе [16] получена следующая нижняя оценка на число $Q(n, k)$ n -квазигрупп порядка $k > 3$:

$$Q(n, k) \geq \begin{cases} 2^{(k/2)^n} & \text{при четных } k, \\ 2^{n(k/3)^n} & \text{при } k \text{ кратных } 3, \\ 2^{3^{n/3-c}} & \text{при } k = 5, \text{ где } c < 0.072 \text{ зависит от } n \bmod 3, \\ 2^{1.5[k/3]^n} & \text{в остальных случаях.} \end{cases} \quad (2)$$

Для случая нечетных $k \geq 5$ эта оценка была уточнена в [17] следующим образом:

$$\log_2 Q(n, k) > \left(\frac{k-3}{2} \right)^{\frac{n}{2}} \left(\frac{k-1}{2} \right)^{\frac{n}{2}}. \quad (3)$$

В той же работе [17] была получена верхняя оценка

$$Q(n, k) \leq 2^{c_k(k-2)^n}, \quad \text{где } c_k = \frac{\log_2 k!}{k-2} + \frac{k}{k-4}.$$

В статье [18] была доказана асимптотическая оценка

$$Q(n, k) \lesssim \left((1 + o(1)) \frac{k}{e^n} \right)^{k^n},$$

при фиксированном n и $k \rightarrow \infty$, а в статье [19] была приведена нижняя оценка, из которой следует, что $\log Q(n, k) = \Theta(k^n \log k)$ при тех же предположениях.

Определение 2. Две n -квазигруппы (E_k, f_1) и (E_k, f_2) назовем изотопными, если существуют перестановки $\sigma_0, \sigma_1, \dots, \sigma_n$ на множестве E_k такие, что

$$f_1(x_1, \dots, x_n) \equiv \sigma_0^{-1}(f_2(\sigma_1(x_1), \dots, \sigma_n(x_n))).$$

Пусть $m \in \mathbb{N} \cup \{0\}$. Множество всех функций из E_k^m в E_k обозначим через P_k^m (в частности, P_k^0 – множество всех констант), $\bigcup_{m=0}^{\infty} P_k^m$ обозначим через P_k .

Определение 3. Пусть $f \in P_k^m$, а $\sim$ – отношение эквивалентности на множестве E_k . Функция f сохраняет отношение $\sim$, если для любых двух наборов $\alpha = (a_1, \dots, a_m)$, $\beta = (b_1, \dots, b_m) \in E_k^m$ таких, что $a_i \sim b_i$ для $i = 1, \dots, m$, выполнено $f(\alpha) \sim f(\beta)$.

Определение естественным образом обобщается на произвольное множество функций $F \subseteq P_k$.

Определение 4. n -квазигруппа (E_k, f) называется простой, если не существует нетривиального отношения эквивалентности, сохраняемого f . В противном случае n -квазигруппа называется непростой.

Несложно показать, что в случае n -квазигрупп сохраняться могут только отношения эквивалентности, все классы которых равноможны. В дальнейшем мы будем рассматривать только отношения эквивалентности с равноможными классами без явного указания на это предположение. Кроме того, известно (см. [20]), что n -квазигруппа (E_k, f) сохраняет нетривиальное отношение эквивалентности тогда и только тогда, когда это отношение сохраняется всеми унарными функциями, полученными из f произвольной подстановкой констант вместо всех переменных, кроме одной.

Определение 5. n -квазигруппа (E_k, f) называется аффинной, если существует абелева группа $(E_k, +)$, автоморфизмы $\alpha_1, \dots, \alpha_n$ этой группы и элемент $c \in E_k$ такие, что

$$f(x_1, x_2, \dots, x_n) \equiv \alpha_1(x_1) + \alpha_2(x_2) + \dots + \alpha_n(x_n) + c. \quad (4)$$

В противном случае n -квазигруппа называется неаффинной.

В работе [20] показано, что без ограничения общности можно считать, что нейтральным элементом группы $(E_k, +)$ является 0.

Определение 6. n -квазигруппа (E_k, f) называется сильно неаффинной, если она не изотопна n -квазигруппам, являющимся аффинными.

На множестве P_k стандартным образом введем операцию суперпозиции, порожденную удалением и добавлением фиктивных переменных, переименованием переменных без отождествления, отождествлением пары переменных и подстановкой одной функции в другую. Суперпозиция естественным образом индуцирует операцию замыкания множества функций: замыкание представляет собой множество всех функций, которые могут быть получены конечными цепочками суперпозиций из функций замыкаемого множества. Замыкание множества $F \subseteq P_k$ обозначим через $[F]$. Более подробное описание операций суперпозиции и замыкания можно найти, например, в монографии [21].

Определение 7. n -квазигруппа (E_k, f) называется полиномиально полной, если $[\{f\} \cup P_k^0] = P_k$. В случае, если (E_k, f) не изотопна n -квазигруппам, не являющимся полиномиально полными, она называется сильно полиномиально полной.

Из теоремы Розенберга (см., например, [21]) следует, что n -квазигруппа полиномиально полна тогда и только тогда, когда она одновременно проста и неаффинна.

2. Сильная неаффинность почти всех n -квазигрупп

Теорема 8. Для любого фиксированного $n \in \mathbb{N}$, $n \geq 2$, доля сильно неаффинных n -квазигрупп порядка k стремится к 1 при $k \rightarrow \infty$.

Доказательство. Для доказательства теоремы скомбинируем несколько достаточно грубых оценок. Число автоморфизмов абелевой группы порядка k заведомо не превосходит $k!$, причем в представлении (4) требуется выбрать n автоморфизмов; число абелевых групп порядка k , изоморфных данной, также не превосходит $k!$; число способов выбора константы равно k . Число n -квазигрупп, изотопных данной, оценивается сверху величиной $(k!)^{n+1}$. Таким образом, число n -квазигрупп, не являющихся сильно неаффинными (т. е., изотопных аффинным), оценивается сверху величиной

$$S(k) = a(k) \cdot k \cdot (k!)^{2n+2},$$

где $a(k)$ – число различных (с точностью до изоморфизма) абелевых групп порядка k . Заметим, что при достаточно больших k выполняется неравенство

$$a(k) \leq k^4$$

(оно следует из асимптотической формулы Харди и Рамануждана [22] на значение $p(x)$ числа разбиений x). Таким образом,

$$S(k) \lesssim k^5 \cdot (k!)^{2n+2} < k^{k(2n+7)}.$$

При логарифмировании получаем верхнюю оценку $(2n+7)k \log_2 k$. С другой стороны, из нижних оценок на число n -квазигрупп (2), (3) следует, что логарифм числа n -квазигрупп порядка k по порядку больше или равен k^n , откуда с учетом неравенства $n \geq 2$ следует утверждение теоремы. $\square$

Замечание 9. Полностью аналогичным образом можно показать, что доля сильно неаффинных n -квазигрупп порядка k стремится к 1 при фиксированном $k \geq 5$ и $n \rightarrow \infty$. Так как все n -квазигруппы простого порядка являются простыми, отсюда следует, что почти все n -квазигруппы простого порядка $k \geq 5$ сильно полиномиально полны.

3. Свойства n -квазигрупп порядка 4

В этом разделе сперва доказываются вспомогательные, а затем основные утверждения о свойствах n -квазигрупп порядка 4.

3.1. ВСПОМОГАТЕЛЬНЫЕ УТВЕРЖДЕНИЯ

Лемма 10. Пусть перестановка $\sigma \in S_4$ сохраняет два из трех отношений эквивалентности $0 \sim 1, 2 \sim 3; 0 \sim 2, 1 \sim 3; 0 \sim 3, 1 \sim 2$. Тогда σ сохраняет все три отношения эквивалентности, причем $\sigma(x) = x \oplus c$ для некоторой константы $c \in E_4$, где $\oplus$ – операция сложения в группе $\mathbb{Z}_2^2$.

Доказательство. Без ограничения общности рассмотрим случай, когда сохраняются первые два отношения эквивалентности. Пусть $\sigma(0) = c$ для некоторого элемента $c \in E_4$. Тогда из сохранения первого отношения эквивалентности следует, что $\sigma(1) = c \oplus 1$, из условия сохранения второго отношения эквивалентности – что $\sigma(2) = c \oplus 2$. Таким образом, $\sigma(3) = c \oplus 3$, и третье отношение эквивалентности также сохраняется. $\square$

Следствие 11. *Непростая n -квазигруппа порядка 4 сохраняет либо ровно одно нетривиальное отношение эквивалентности, либо все три нетривиальных отношения эквивалентности. Существует ровно четыре n -квазигруппы (E_4, f) порядка 4, сохраняющие все три отношения эквивалентности, причем f имеет вид $c \oplus x_1 \oplus \dots \oplus x_n$.*

Лемма 12. *Пусть $(E_4, +_i)$, $i = 1, 2, 3$, – абелевы группы с операциями, заданными следующими таблицами Кэли:*

$+_1$	0	1	2	3	$+_2$	0	1	2	3	$+_3$	0	1	2	3
0	0	1	2	3	0	0	1	2	3	0	0	1	2	3
1	1	2	3	0	1	1	0	3	2	1	1	3	0	2
2	2	3	0	1	2	2	3	1	0	2	2	0	3	1
3	3	0	1	2	3	3	2	0	1	3	3	2	1	0

Пусть $1 \leq i, j \leq 3$, $i \neq j$. Тогда если квазигруппа (E_4, f) аффинна относительно $(E_4, +_i)$, она не аффинна относительно $(E_4, +_j)$.

Заметим, что группы из условия леммы получены из группы $\mathbb{Z}_4$ переобозначением элемента порядка 2 и элемента порядка 4.

Доказательство. Рассмотрим случай $i = 1$, $j = 2$. Остальные случаи рассматриваются полностью аналогично. Заметим, что операция $+_1$, все константы и любой автоморфизм группы $(E_4, +_1)$ сохраняют предикат p арности 4, обращающийся в истину на всех наборах (x, y, z, w) , удовлетворяющих соотношению $x +_1 y = z +_1 w$, и только на них. Понятие сохранения предиката подробно описано, например, в монографии [21]. Содержательно сохранение предиката функцией арности t означает, что если рассмотреть произвольные t наборов, на которых предикат обращается в истину, записать их в виде столбцов матрицы и применить функцию к каждой строке, на выходе получится набор, также обращающий предикат в истину. Известно, что множество всех функций, сохраняющих заданный предикат, является замкнутым классом относительно операции суперпозиции. В случае предиката p этот класс отличен от множества всех функций. Примером функции, не сохраняющей предикат, является $g(x, y) = x +_2 y$. Действительно, рассмотрим набор $(2, 2, 0, 0)$. Так как $2 +_1 2 = 0$, он обращает p в истину, однако покомпонентное применение функции g к двум копиям этого набора дает $(1, 1, 0, 0)$, обращающий p в ложь.

Предположим, что квазигруппа (E_4, f) аффинна относительно групп $(E_4, +_1)$ и $(E_4, +_2)$. Из аффинности относительно $(E_4, +_1)$ следует, что f и все функции, полученные суперпозициями из f , констант и операции $+_1$, сохраняют предикат p . Из аффинности f

относительно группы $(E_4, +_2)$ следует, что $f(x, y) = \alpha_1(x) +_2 \alpha_2(y) +_2 c$, где α_1, α_2 – автоморфизмы $(E_4, +_2)$. Пусть $a = \alpha_2^{-1}(\alpha_1^{-1}(-_2\alpha_1(c) -_2 \alpha_2(c) -_2 c))$. Рассмотрим функцию $h(x, y) = f(f(x, a), f(0, y))$. Покажем, что $h(x, y) = x +_2 y$. Действительно, с учетом того, что для любого автоморфизма α группы $\mathbb{Z}_4$ верно, что α^2 – тождественное отображение, получаем следующую цепочку равенств:

$$\begin{aligned} h(x, y) &= \alpha_1(\alpha_1(x) +_2 \alpha_2(\alpha_2^{-1}(\alpha_1^{-1}(-_2\alpha_1(c) -_2 \alpha_2(c) -_2 c))) +_2 c) \\ &+ _2 \alpha_2(\alpha_1(0) +_2 \alpha_2(y) +_2 c) +_2 c = x +_2 -_2\alpha_1(c) -_2 \alpha_2(c) -_2 c +_2 \alpha_1(c) +_2 y +_2 \alpha_2(c) +_2 c = x +_2 y. \end{aligned}$$

Таким образом, суперпозиции функции f и констант породили функцию, не сохраняющую предикат p . Полученное противоречие завершает доказательство леммы. $\square$

3.2. ОСНОВНЫЕ УТВЕРЖДЕНИЯ

Теорема 13. Для любого фиксированного $n \in \mathbb{N}$, $n \geq 2$, число n -квазигрупп порядка 4, не являющихся простыми, равно $3 \cdot 2^{2^n+1} - 8$.

Доказательство. Есть три способа выбрать сохраняемое отношение эквивалентности, выбрав элемент $c \in E_4$, $c \neq 0$, и положив $0 \sim c$. Пусть (E_4, f) – n -квазигруппа, сохраняющая выбранное отношение. Тогда это отношение порождает разбиение множества входных наборов f на 2^n классов $C = \{(a_1, \dots, a_n)\}$ таких, что для любого i , $1 \leq i \leq n$, из условия $\alpha, \beta \in C$ вытекает эквивалентность i -х компонент наборов α и β , причем на любой паре аргументов из одного класса f принимает эквивалентные значения. Таким образом, есть 2 варианта выбора класса эквивалентности для значений на классе C , содержащем нулевой набор (классы значений на оставшихся C будут определены однозначно), и 2 варианта выбора значений на наборах внутри каждого класса C . Значит, при фиксированном отношении эквивалентности имеется ровно $2 \cdot 2^{2^n} = 2^{2^n+1}$ непростых n -квазигрупп, сохраняющих это отношение. Для доказательства теоремы осталось применить следствие 11 и учесть, что четыре n -квазигруппы, сохраняющие все три отношения, были посчитаны трижды. $\square$

Из теоремы 13 с учетом оценки (1) на мощность множества всех n -квазигрупп порядка 4 непосредственно вытекает следующий факт.

Следствие 14. Доля простых n -квазигрупп порядка 4 стремится к 1 при $n \rightarrow \infty$.

Теорема 15. Для любого фиксированного $n \in \mathbb{N}$, $n \geq 2$, число n -квазигрупп порядка 4, являющихся аффинными, равно $3 \cdot 2^{n+2} (3^{n-1} + 1)$.

Доказательство. Сперва заметим, что с точностью до изоморфизма абелева группа $(E_4, +)$ может быть выбрана двумя способами: $\mathbb{Z}_4$ и $\mathbb{Z}_2^2$. Также заметим, что из аффинности n -квазигруппы (E_k, f) следует аффинность квазигруппы (E_k, f') , где f' получена из f произвольной подстановкой констант вместо переменных $x_3, \dots, x_n$. Известно (см.,

например, [20]), что если квазигруппа аффинна относительно абелевой группы, то эти квазигруппа и группа изотопны. Так как группы $\mathbb{Z}_4$ и $\mathbb{Z}_2^2$ не являются изотопными, аффинность относительно первой означает неаффинность относительно второй, и наоборот.

Рассмотрим случай n -квазигрупп, аффинных относительно групп, изоморфных $\mathbb{Z}_2^2$. Как отмечалось выше, без ограничения общности можно считать, что нейтральным элементом группы является 0. Таким образом, имеется шесть вариантов абелевой группы, полученных из $\mathbb{Z}_2^2$ перестановкой элементов, сохраняющей 0. Легко увидеть, что любая такая перестановка σ является автоморфизмом группы $\mathbb{Z}_2^2$. Обозначим через $\oplus$ сложение в группе $\mathbb{Z}_2^2$, через $+$ сложение в изоморфном образе. Предположим, что n -квазигруппа (E_4, f) аффинна относительно $(E_4, +)$, т.е. $f(x_1, \dots, x_n) = \alpha_1(x_1) + \dots + \alpha_n(x_n) + c$, где $\alpha_1, \dots, \alpha_n$ – автоморфизмы $(E_4, +)$. Тогда верна следующая цепочка равенств:

$$\begin{aligned} f(x_1, \dots, x_n) &= \sigma(\alpha_1(\sigma^{-1}(x_1)) \oplus \dots \oplus \alpha_n(\sigma^{-1}(x_n)) \oplus \sigma^{-1}(c)) = \\ &= \sigma(\alpha_1(\sigma^{-1}(x_1))) \oplus \dots \oplus \sigma(\alpha_n(\sigma^{-1}(x_n))) \oplus c, \end{aligned}$$

причем $\sigma \circ \alpha_i \circ \sigma^{-1}$ являются автоморфизмами группы $\mathbb{Z}_2^2$. Таким образом, без ограничения общности можно считать, что в рассматриваемом случае все n -квазигруппы аффинны относительно $\mathbb{Z}_2^2$. Легко увидеть, что разным автоморфизмам и константам в представлении (4) соответствуют разные n -квазигруппы. Значит, число n -квазигрупп, аффинных относительно групп, изоморфных $\mathbb{Z}_2^2$, равно $4 \cdot 6^n$ (четыре способа выбора константы и шесть способов выбора каждого из n автоморфизмов).

Рассмотрим случай n -квазигрупп, аффинных относительно групп, изоморфных $\mathbb{Z}_4$. Заметим, что если изоморфизм между двумя такими группами переставляет элементы порядка 4, то, аналогично предыдущему случаю, легко показать, что множества n -квазигрупп, аффинных относительно этих групп, совпадают. Таким образом, с учетом леммы 12 имеется ровно три непересекающихся множества n -квазигрупп, аффинных относительно групп $(E_4, +_1)$, $(E_4, +_2)$ и $(E_4, +_3)$. Значит, число n -квазигрупп, аффинных относительно групп, изоморфных $\mathbb{Z}_4$, равно $3 \cdot 4 \cdot 2^n$ (три способа выбора операции абелевой группы, четыре способа выбора константы и два способа выбора каждого из n автоморфизмов).

Для завершения доказательства остается сложить оценки из первого и второго случаев:

$$3 \cdot 4 \cdot 2^n + 4 \cdot 6^n = 3 \cdot 2^{n+2} (3^{n-1} + 1). \quad \square$$

Заметим, что число n -квазигрупп, получаемых из некоторой n -квазигруппы (E_4, f) с помощью изотопий, очевидным образом оценивается сверху величиной $(4!)^{n+1}$. Таким образом, из теоремы 15 и оценки (1) вытекает следующий факт.

Следствие 16. *Доля сильно неаффинных n -квазигрупп порядка 4 стремится к 1 при $n \rightarrow \infty$.*

Следующее утверждение напрямую выводится из теорем 13, 15 и критерия полиномиальной полноты.

Следствие 17. *Доля полиномиально полных n -квазигрупп порядка 4 стремится к 1 при $n \rightarrow \infty$.*

Теорема 18. *Для любого фиксированного $n \in \mathbb{N}$, $n \geq 2$, число n -квазигрупп порядка 4, являющихся одновременно непростыми и аффинными, равно $24 \cdot 2^n - 8$.*

Доказательство. Выше мы показали, что множество аффинных n -квазигрупп порядка 4 разбивается в объединение двух непересекающихся подмножеств: n -квазигрупп, аффинных относительно групп, изоморфных $\mathbb{Z}_4$, и n -квазигрупп, аффинных относительно групп, изоморфных $\mathbb{Z}_2^2$. Покажем, что в первом случае все аффинные n -квазигруппы не являются простыми. Рассмотрим подслучай группы $(E_4, +_1)$, остальные подслучаи рассматриваются полностью аналогично. Зафиксируем отношение эквивалентности $0 \sim 2$, $1 \sim 3$. Заметим, что множество функций, сохраняющих это отношение, является замкнутым классом, т. е. любая суперпозиция таких функций сохраняет отношение $\sim$. Также заметим, что все константы, все автоморфизмы абелевой группы и операция $+_1$ сохраняет отношение $\sim$. Значит, в силу представления (4), любая n -квазигруппа, аффинная относительно $(E_4, +_1)$, также сохраняет искомое отношение эквивалентности, т. е. не является простой.

Перейдем к случаю n -квазигрупп (E_4, f) , аффинных относительно групп, изоморфных $\mathbb{Z}_2^2$. Выше было показано, что без ограничения общности можно считать, что группа совпадает с $\mathbb{Z}_2^2$. Проанализируем, каким критериям должны удовлетворять автоморфизмы α_i в представлении (4), чтобы получающаяся n -квазигруппа не была простой. Для этого необходимо и достаточно, чтобы все унарные функции, полученные из f всевозможными подстановками констант, сохраняли какое-то нетривиальное фиксированное отношение эквивалентности (см. [20]). В следствии 11 было показано, что если все автоморфизмы тривиальны, получающиеся n -квазигруппы сохраняют все три возможных отношения эквивалентности.

Пусть некоторый автоморфизм является транспозицией (i, j) , $1 \leq i < j \leq 3$. Обозначим через s ненулевой элемент E_4 , отличный от i и j . Автоморфизм (i, j) сохраняет отношение эквивалентности $i \sim j$, $0 \sim s$. Так как все константы и сложение в группе $\mathbb{Z}_2^2$ также сохраняют это отношение эквивалентности, все n -квазигруппы, аффинные относительно $\mathbb{Z}_2^2$ и такие, что каждый автоморфизм в представлении (4) либо тривиален, либо представляет собой транспозицию (i, j) , не являются простыми. С другой стороны, транспозиция (i, j) не сохраняет нетривиальное отношение эквивалентности такое, что $0 \sim i$ или $0 \sim j$. Действительно, в этом случае эквивалентные аргументы $0 \sim i$ ($0 \sim j$, соответственно) переходят в неэквивалентные $0 \not\sim j$ ($0 \not\sim i$, соответственно). Из этого наблюдения следует, что n -квазигруппа, аффинная относительно группы $\mathbb{Z}_2^2$ и имеющая по крайней мере два различных автоморфизма-транспозиции в представлении (4), проста. Действительно, пусть для определенности $\alpha_u = (i, j)$, $\alpha_v = (i, s)$. Из определения n -квазигруппы следует, что можно так зафиксировать значения всех переменных, кроме

x_u (x_v , соответственно), что получившаяся функция одной переменной будет совпадать с транспозицией (i, j) ((i, s) , соответственно). Так как первая унарная функция сохраняет только отношение эквивалентности, включающее пару $0 \sim s$, а вторая – только отношение эквивалентности, включающее пару $0 \sim j$, $j \neq s$, множество унарных функций, порожденных подстановкой констант в f , не сохраняет никакое нетривиальное отношение эквивалентности, т. е. n -квазигруппа проста.

Наконец, пусть некоторый автоморфизм α является циклом длины 3. Тогда он не сохраняет никакое нетривиальное отношение эквивалентности. Действительно, если предположить, что сохраняется отношение, для которого $0 \sim i$, то $\alpha(0) = 0$, $j = \alpha(i) \neq i$, т. е. отношение не сохраняется.

Таким образом, доказано, что n -квазигруппа, аффинная относительно группы $\mathbb{Z}_2^2$, не является простой тогда и только тогда, когда каждый автоморфизм в представлении (4) либо тривиален, либо представляет собой транспозицию (i, j) . Отсюда общее число таких n -квазигрупп равно $4 \cdot (3 \cdot 2^n - 2)$ (четыре варианта выбора константы, три варианта выбора транспозиции, два варианта выбора автоморфизма для каждой из n позиций, при этом случай, когда все автоморфизмы тривиальны, посчитан трижды).

Для завершения доказательства осталось сложить оценки для двух случаев:

$$3 \cdot 4 \cdot 2^n + 4 \cdot (3 \cdot 2^n - 2) = 24 \cdot 2^n - 8.$$

□

В заключение раздела приведем сводную таблицу числа n -квазигрупп порядка 4 различных типов для наиболее интересных для практике случаев $n = 2$ (таблица 1) и $n = 3$ (таблица 2). Значения для числа простых и непростых аффинных n -квазигрупп получены с помощью теорем 15 и 18, число неаффинных непростых n -квазигрупп получено с помощью теорем 13 и 18, оставшиеся значения были найдены с использованием информации о числе n -квазигрупп порядка 4 (576 для $n = 2$, 55296 для $n = 3$; см., например, [17]). Дополнительная валидация результатов была проведена с помощью программных реализаций алгоритмов проверки простоты и неаффинности из работы [20].

простые \ аффинные	да	нет
	104	384
да	104	384
нет	88	0

Таблица 1. Число квазигрупп различных типов порядка 4.

простые \ аффинные	да	нет
	776	52992
да	776	52992
нет	184	1344

Таблица 2. Число 3-квазигрупп различных типов порядка 4.

4. Заключение

В работе изучается “типичность” свойств простоты, неаффинности и полиномиальной полноты n -квазигрупп. Установлено, что при фиксированном n почти все n -квазигруппы сильно неаффинны, т. е. не изотопны аффинным. Найдено точное значение числа простых, аффинных и одновременно простых и аффинных n -квазигрупп порядка 4. Как следствие, показано, что почти все n -квазигруппы порядка 4 полиномиально полны и сильно неаффинны.

В дальнейшем планируется установить сильную простоту и сильную полиномиальную полноту почти всех n -квазигрупп при фиксированном значении n , а также при $k = 4$ и $n \rightarrow \infty$.

Авторы благодарят М.В. Волкова за привлечение внимания к задаче, Р.Б. Халитову за ряд интересных наблюдений, на основе которых удалось получить приведенные в работе оценки, рецензента за ценные и конструктивные замечания и предоставленные ссылки.

Материалы данной работы являются продолжением исследований, проводившихся авторами в рамках проекта под руководством В.А. Артамонова.

Список литературы

- [1] V.A. Shcherbacov, *Quasigroups in cryptology*, Comput. Sci. J. Mold. **17** (2), 193–228 (2009).
- [2] D. Chauhan, I. Gupta, R. Verma, *Quasigroups and their applications in cryptography*, Cryptologia **45** (3), 227–265 (2021).
DOI: <https://doi.org/10.1080/01611194.2020.1721615>
- [3] A. Mileva, S. Markovski, *Shapeless quasigroups qerived by Feistel orthomorphisms*, Glas. Mat. Ser. III **47** (2), 333–349 (2012).
DOI: <http://dx.doi.org/10.3336/gm.47.2.09>
- [4] V. Dimitrova, S. Markovski, *Classification of quasigroups by image patterns*, Proceedings of the Fifth International Conference for Informatics and Information Technology, 152–160 (2007).
- [5] V.A. Artamonov, S. Chakrabarti, S. Gangopadhyay, S.K. Pal, *On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts*, Quasigroups Relat. Syst. **21** (2), 117–130 (2013).
- [6] G. Horváth, C.L. Nehaniv, Cs. Szabó, *An assertion concerning functionally complete algebras and NP-completeness*, Theoret. Comput. Sci. **407** (1–3), 591–595 (2008).
DOI: <https://doi.org/10.1016/j.tcs.2008.08.028>

- [7] V.A. Artamonov, S. Chakrabarti, S.K. Pal, *Characterization of polynomially complete quasigroups based on Latin squares for cryptographic transformations*, Discrete Appl. Math. **200**, 5–17 (2016).
DOI: <https://doi.org/10.1016/j.dam.2015.06.033>
- [8] В.Л. Мурский, *Конечная базируемость тождеств и другие свойства “почти всех” алгебр*, Проблемы кибернетики **30**, 43–56 (1975).
- [9] P.J. Cameron, *Almost all quasigroups have rank 2*, Discrete Math. **106–107**, 111–115 (1992).
DOI: [https://doi.org/10.1016/0012-365X\(92\)90537-P](https://doi.org/10.1016/0012-365X(92)90537-P)
- [10] A. Salomaa, *Some completeness criteria for sets of functions over a finite domain II*, Annales Universitatis Turkuensis. Series AI **63**, 19 pp. (1963).
- [11] А.В. Галатенко, В.В. Галатенко, А.Е. Панкратьев, *О сильной полиномиальной полноте почти всех квазигрупп*, Матем. заметки **111** (1), 8–14 (2022).
DOI: <https://doi.org/10.4213/mzm13229>
- [12] B. Larose, L. Zádori, *Taylor terms, constraint satisfaction and the complexity of polynomial equations over finite algebras*, Int. J. Algebra Comput. **16** (3), 563–581 (2006).
DOI: <https://doi.org/10.1142/S0218196706003116>
- [13] D.S. Krotov, V.N. Potapov, *n -ary quasigroups of order 4*, SIAM J. Discrete Math. **23** (2), 561–570 (2009).
DOI: <https://doi.org/10.1137/070697331>
- [14] C.F. Laywine, G.L. Mullen, *Discrete mathematics using Latin squares*, Wiley, New York, 1998.
- [15] В.Н. Потапов, Д.С. Кротов, *Асимптотика числа n -квазигрупп порядка 4*, Сиб. матем. журн. **47** (4), 873–887 (2006).
URL: <https://www.mathnet.ru/rus/smj902>
- [16] D.S. Krotov, V.N. Potapov, P.V. Sokolova, *On reconstructing reducible n -ary quasigroups and switching subquasigroups*, Quasigr. Relat. Syst. **16** (1), 55–67 (2008).
- [17] В.Н. Потапов, Д.С. Кротов, *О числе n -арных квазигрупп конечного порядка*, Дискрет. матем. **24** (1), 60–69 (2012).
DOI: <https://doi.org/10.4213/dm1172>
- [18] N. Linial, Z. Luria, *An upper bound on the number of high-dimensional permutations*, Combinatorica **34** (4), 471–486 (2014).
DOI: <https://doi.org/10.1007/s00493-011-2842-8>
- [19] V.N. Potapov, *On the number of SQSs, latin hypercubes and MDS codes*, J. Combin. Des. **26** (5), 237–248 (2018).
DOI: <https://doi.org/10.1002/jcd.21603>

- [20] А.В. Галатенко, А.Е. Панкратьев, В.М. Староверов, *Алгоритмы проверки некоторых свойств n -квазигрупп*, Программирование (1), 40–53 (2022).
DOI: <https://doi.org/10.31857/s0132347422010046>
- [21] D. Lau, *Function algebras on finite sets: a basic course on many-valued logic and clone theory*, Springer-Verlag, Berlin, 2006.
DOI: <https://doi.org/10.1007/3-540-36023-9>
- [22] G.H. Hardy, S. Ramanujan, *Asymptotic formulae in combinatory analysis*, Proc. London Math. Soc. **17**, 75–115 (1918).
DOI: <https://doi.org/10.1112/plms/s2-17.1.75>

Алексей Владимирович Галатенко

МГУ имени М.В. Ломоносова,
механико-математический факультет,
Ленинские горы, д. 1, г. Москва, 119991, Россия,
e-mail: agalat@msu.ru

Владимир Владимирович Галатенко

МГУ имени М.В. Ломоносова,
механико-математический факультет,
Ленинские горы, д. 1, г. Москва, 119991, Россия,
e-mail: vgalat@msu.ru

Антон Евгеньевич Панкратьев

МГУ имени М.В. Ломоносова,
механико-математический факультет,
Ленинские горы, д. 1, г. Москва, 119991, Россия,
e-mail: apankrat@intsys.msu.ru

Some properties of almost all n -quasigroups

A.V. Galatenko, V.V. Galatenko, A.E. Pankratiev

Abstract. We study the generic nature of simplicity, non-affinity and polynomial completeness of finite n -quasigroups. It is shown that for fixed n almost all n -quasigroups are strongly non-affine, i.e., not isotopic to affine n -quasigroups. Exact number of simple, affine and simultaneously simple and affine n -quasigroups of the order 4 is established. As a corollary, it is proven that almost all n -quasigroups of the order 4 are polynomially complete and strongly non-affine.

Keywords: quasigroup, n -quasigroup, simplicity, affinity, polynomial completeness.

DOI: 10.26907/2949-3919.2024.4.35-50

References

- [1] V.A. Shcherbacov, *Quasigroups in cryptology*, Comput. Sci. J. Mold. **17** (2), 193–228 (2009).
- [2] D. Chauhan, I. Gupta, R. Verma, *Quasigroups and their applications in cryptography*, Cryptologia **45** (3), 227–265 (2021).
DOI: <https://doi.org/10.1080/01611194.2020.1721615>
- [3] A. Mileva, S. Markovski, *Shapeless quasigroups qerived by Feistel orthomorphisms*, Glas. Mat. Ser. III **47** (2), 333–349 (2012).
DOI: <http://dx.doi.org/10.3336/gm.47.2.09>
- [4] V. Dimitrova, S. Markovski, *Classification of quasigroups by image patterns*, Proceedings of the Fifth International Conference for Informatics and Information Technology, 152–160 (2007).
- [5] V.A. Artamonov, S. Chakrabarti, S. Gangopadhyay, S.K. Pal, *On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts*, Quasigroups Relat. Syst. **21** (2), 117–130 (2013).
- [6] G. Horváth, C.L. Nehaniv, Cs. Szabó, *An assertion concerning functionally complete algebras and NP-completeness*, Theoret. Comput. Sci. **407** (1–3), 591–595 (2008).
DOI: <https://doi.org/10.1016/j.tcs.2008.08.028>

-
- [7] V.A. Artamonov, S. Chakrabarti, S.K. Pal, *Characterization of polynomially complete quasigroups based on Latin squares for cryptographic transformations*, Discrete Appl. Math. **200**, 5–17 (2016).
DOI: <https://doi.org/10.1016/j.dam.2015.06.033>
- [8] V.L. Murskiy, *Finite basis of identities and other properties of “almost all” algebras*, Problemy kibernetiki **30**, 43–56 (1975) [in Russian].
- [9] P.J. Cameron, *Almost all quasigroups have rank 2*, Discrete Math. **106–107**, 111–115 (1992).
DOI: [https://doi.org/10.1016/0012-365X\(92\)90537-P](https://doi.org/10.1016/0012-365X(92)90537-P)
- [10] A. Salomaa, *Some completeness criteria for sets of functions over a finite domain II*, Annales Universitatis Turkuensis. Series AI **63**, 19 pp. (1963).
- [11] A.V. Galatenko, V.V. Galatenko, A.E. Pankrat'ev, *Strong polynomial completeness of almost all quasigroups*, Math. Notes **111** (1), 7–12 (2022).
DOI: <https://doi.org/10.1134/S0001434622010023>
- [12] B. Larose, L. Zádori, *Taylor terms, constraint satisfaction and the complexity of polynomial equations over finite algebras*, Int. J. Algebra Comput. **16** (3), 563–581 (2006).
DOI: <https://doi.org/10.1142/S0218196706003116>
- [13] D.S. Krotov, V.N. Potapov, *n -ary quasigroups of order 4*, SIAM J. Discrete Math. **23** (2), 561–570 (2009).
DOI: <https://doi.org/10.1137/070697331>
- [14] C.F. Laywine, G.L. Mullen, *Discrete mathematics using Latin squares*, Wiley, New York, 1998.
- [15] V.N. Potapov, D.S. Krotov, *Asymptotics for the number of n -quasigroups of order 4*, Siberian Math. J. **47** (4), 720–731 (2006).
DOI: <https://doi.org/10.1007/s11202-006-0083-9>
- [16] D.S. Krotov, V.N. Potapov, P.V. Sokolova, *On reconstructing reducible n -ary quasigroups and switching subquasigroups*, Quasigr. Relat. Syst. **16** (1), 55–67 (2008).
- [17] V. N. Potapov, D. S. Krotov, *On the number of n -ary quasigroups of finite order*, Discrete Math. Appl. **21** (5–6), 575–585 (2011).
DOI: <https://doi.org/10.1515/dma.2011.035>
- [18] N. Linial, Z. Luria, *An upper bound on the number of high-dimensional permutations*, Combinatorica **34** (4), 471–486 (2014).
DOI: <https://doi.org/10.1007/s00493-011-2842-8>
- [19] V.N. Potapov, *On the number of SQSs, latin hypercubes and MDS codes*, J. Combin. Des. **26** (5), 237–248 (2018).
DOI: <https://doi.org/10.1002/jcd.21603>

- [20] A.V. Galatenko, A.E. Pankratiev, V.M. Staroverov, *Algorithms for checking some properties of n -quasigroups*, Program. Comput. Softw. **48** (1), 36–48 (2022).
DOI: <http://doi.org/10.1134/s0361768822010042>
- [21] D. Lau, *Function algebras on finite sets: a basic course on many-valued logic and clone theory*, Springer-Verlag, Berlin, 2006.
DOI: <https://doi.org/10.1007/3-540-36023-9>
- [22] G.H. Hardy, S. Ramanujan, *Asymptotic formulae in combinatory analysis*, Proc. London Math. Soc. **17**, 75–115 (1918).
DOI: <https://doi.org/10.1112/plms/s2-17.1.75>

Alexei Vladimirovich Galatenko

Moscow State University,
Faculty of Mechanics and Mathematics,
1 Leninskie Gory, Moscow 119991, Russia,
e-mail: agalat@msu.ru

Vladimir Vladimirovich Galatenko

Moscow State University,
Faculty of Mechanics and Mathematics,
1 Leninskie Gory, Moscow 119991, Russia,
e-mail: vgalat@msu.ru

Anton Evgevievich Pankratiev

Moscow State University,
Faculty of Mechanics and Mathematics,
1 Leninskie Gory, Moscow 119991, Russia,
e-mail: apankrat@intsys.msu.ru

О степени неразрешимости теории фигур в линейных пространствах

С.М. Дудаков

Аннотация. Мы изучаем аддитивную теорию произвольных фигур в линейных пространствах, т. е. теорию множеств точек/векторов, на которые естественным образом распространена операция сложения. Наш основной результат: если линейное пространство бесконечно, то аддитивная теория фигур в нем позволяет интерпретировать арифметику второго порядка и, следовательно, имеет не меньшую степень неразрешимости. Для счетно бесконечных пространств мы доказываем обратный результат: теория фигур в них может быть проинтерпретирована в арифметике второго порядка, следовательно, две такие теории алгоритмически эквивалентны. Для несчетных пространств последний вопрос остается открытым; мы показываем, что для пространств разных мощностей аддитивные теории фигур в них могут не быть элементарно эквивалентны.

Ключевые слова: линейное пространство, алгебра подмножеств, алгоритмическая неразрешимость, арифметика второго порядка.

DOI: 10.26907/2949-3919.2024.4.51-65

Введение

Построение новых алгебр из уже существующих, и изучение их свойств и свойств их теорий является одним из важнейших разделов математической логики. Набор таких операций весьма широк: прямые и фильтрованные произведения, степени, подсистемы, гомоморфные образы и т. д.

В этой работе мы рассматриваем переход от исходной алгебры $\mathfrak{A}$ к алгебре всех ее непустых подмножеств $\text{exr } \mathfrak{A}$, в которой операции определяются естественным образом, как множество всевозможных поточечных результатов:

$$f(A_1, \dots, A_n) = \{f(a_1, \dots, a_n) : a_i \in A_i, i = 1, \dots, n\}.$$

Во многих случаях такая операция является естественной. Например, если исходной алгеброй $\mathfrak{A}$ является алгебра слов с операцией конкатенации, то $\text{exr } \mathfrak{A}$ будет алгеброй непустых

языков с конкатенацией (см. [1]). Такой метод находит применение и при описании программных конструкций (см. [2]), исследованиях по модальной логике (см. [3]) и в ряде других случаев. В этих же терминах можно сформулировать и некоторые конкретные математические задачи, скажем, бинарная проблема Гольдбаха – это утверждение $P + P = E$, где P – множество простых чисел, начиная с 3, а E – множество четных чисел, начиная с 6.

Свойства новой алгебры существенно зависят от свойств исходной, но могут при этом сильно от них отличаться (см. [4]). Например, при переходе от $\mathfrak{A}$ к $\text{exr } \mathfrak{A}$ сохраняются свойства ассоциативности и коммутативности операций. Поэтому, если $\mathfrak{A}$ было (коммутативной) полугруппой, то и $\text{exr } \mathfrak{A}$ будет такой полугруппой. Собственно говоря, именно изучению таких структур и была посвящена одна из первых работ (см. [5]), в которой подробно изучался вопрос о переходе от $\mathfrak{A}$ к $\text{exr } \mathfrak{A}$. Другие сохраняющиеся свойства – это те, которые описываются экзистенциальными формулами: так как одноэлементные подмножества вида $\{a\}$ образуют в $\text{exr } \mathfrak{A}$ алгебру, изоморфную исходной, то переход от $\mathfrak{A}$ к $\text{exr } \mathfrak{A}$ является расширением, поэтому сохраняет истинность всех экзистенциальных формул.

С другой стороны, теория алгебры $\text{exr } \mathfrak{A}$ может быть как более, так и менее выразительной, чем теория исходной системы. Бывает, что теория новой системы совпадает с исходной (см. [6]). Нетрудно построить и примеры, когда теория алгебры $\mathfrak{A}$ будет сколь угодно высокой степени неразрешимости, а теория $\text{exr } \mathfrak{A}$ – разрешимой. Они получаются рассмотрением совокупности конечных пунктированных множеств (C, a_C) и унарной функции, для которой $f(b) = a_c$ для всех $b \in C$. Комбинируя множества C разных мощностей, легко добиться указанного результата.

Но все же с интуитивной точки зрения обычно должно быть наоборот: теория системы $\text{exr } \mathfrak{A}$ должна быть сложнее, чем теория $\mathfrak{A}$. Для ряда случаев, когда система $\mathfrak{A}$ является полугруппой (моноидом), нами такой ответ получен. Например, в работе [7] мы показали, что уже для аддитивной арифметики натуральных чисел $\Omega = (\omega, +)$ алгебра конечных множеств алгоритмически эквивалентна элементарной арифметике, а алгебра всех множеств – арифметике второго порядка. В [8] аналогичный результат о конечных подмножествах получен для более общего типа коммутативных моноидов: имеющих элемент бесконечного порядка и при этом допускающих сокращение. В [9] это доказано для групп кручения бесконечной экспоненты.

В настоящей работе изучается теория подмножеств для линейных пространств. Линейные пространства над полями являются одним из фундаментальных объектов алгебры и математики вообще, поскольку огромное число математических понятий оказываются частными их случаями. Очевидно, что если пространство $\mathfrak{L}$ конечно, то и $\text{exr } \mathfrak{L}$ будет конечным, поэтому теория $\text{exr } \mathfrak{L}$ разрешима. Поэтому мы будем исследовать случай, когда $\mathfrak{L}$ является бесконечным.

Мы отдельно рассматриваем случаи пространств над полями характеристики нуль и над полями конечной характеристики. Это связано с тем, что бесконечное пространство

над конечным полем необходимо является бесконечномерным, в то время как для пространств над полями характеристики нуль это не так. Отсюда возникает необходимость в различных методах интерпретации.

В обоих случаях мы показываем, что для бесконечного пространства $\mathfrak{L}$ в алгебре $\text{exr } \mathfrak{A}$ всех его подмножеств можно интерпретировать арифметику второго порядка. Для счетных пространств эта оценка степени неразрешимости будет точной: если пространство $\mathfrak{L}$ счетно, то теория алгебры $\text{exr } \mathfrak{L}$ тоже может быть проинтерпретирована в арифметике второго порядка. Для несчетных пространств ситуация более сложна; мы показываем, что для пространств $\mathfrak{L}$ разной мощности теории систем $\text{exr } \mathfrak{L}$ могут быть различны, и их существует, по крайней мере, столько же, сколько теорий ординалов, как упорядоченных множеств.

1. Алгебры подмножеств

Если $\mathfrak{A}$ является алгебраической системой функциональной сигнатуры, алгеброй, то мы естественным образом можем обобщить все определенные в ней операции на произвольные подмножества $\mathfrak{A}$:

$$f(X_1, \dots, X_n) = \{f(a_1, \dots, a_n) : a_1 \in X_1, \dots, a_n \in X_n\}.$$

Таким образом, образуется алгебра всех подмножеств $\text{exr}_\varnothing \mathfrak{A}$, включая пустое множество. Однако, если хотя бы один из аргументов функции f в алгебре $\text{exr}_\varnothing \mathfrak{A}$ будет пустым множеством, то, очевидно, и результат будет пустым. Обратное тоже верно: если все аргументы непусты, то и результат непуст. Таким образом, непустые подмножества образуют в $\text{exr}_\varnothing \mathfrak{A}$ подалгебру $\text{exr } \mathfrak{A}$. Если среди операций есть хоть одна f , имеющая местность два или больше, то пустое множество в $\text{exr}_\varnothing \mathfrak{A}$ определимо:

$$X = \varnothing \equiv (\forall Y) f(X, Y, \dots, Y) = X.$$

Следовательно, определима и подалгебра $\text{exr } \mathfrak{A}$. При этом, в силу однозначной определенности операций над пустым множеством, выразительная сила и алгоритмические свойства алгебр $\text{exr}_\varnothing \mathfrak{A}$ и $\text{exr } \mathfrak{A}$ будут совпадать. Поэтому в дальнейшем будем рассматривать только алгебру непустых подмножеств $\text{exr } \mathfrak{A}$.

В настоящей работе мы будем изучать ситуацию, когда алгебра $\mathfrak{A}$ представляет собой линейное пространство над некоторым полем $\mathbb{F}^*$. При этом это пространство можно рассматривать и как линейное пространство над простым полем $\mathbb{F} \subseteq \mathbb{F}^*$. В последнем случае операции умножения векторов x пространства на элементы α поля можно описать при помощи одного только сложения: $\alpha x = y \equiv y = \underbrace{x + \dots + x}_{\alpha \text{ раз}}$ для α из поля вычетов

$\mathbb{F} = \mathbb{Z}_p$ или натурального α из поля рациональных чисел $\mathbb{Q}$, $\alpha x = y \equiv y + (-\alpha)x = 0$ для отрицательного α из $\mathbb{Q}$ или $\alpha x = y \equiv nx = ty$ для дробного $\alpha = n/m$ из $\mathbb{Q}$. Поэтому

мы считаем, что линейное пространство $\mathfrak{L}$ – это абелева группа, снабженная только одной двухместной операцией – сложением.

Отметим некоторые свойства алгебры $\text{exr } \mathfrak{L}$, которые не зависят от основного поля.

Лемма 1. *В системе $\text{exr } \mathfrak{L}$ определимо нулевое подпространство $\{0\}$ и совокупность одноэлементных множеств вида $\{a\}$.*

Доказательство. Нулевое подпространство является (единственным) нейтральным в $\text{exr } \mathfrak{L}$ элементом:

$$X = \{0\} \equiv (\forall Y)X + Y = Y.$$

Одноэлементные множества – это в точности обратимые в $\text{exr } \mathfrak{L}$ элементы:

$$\text{One}(X) \equiv (\exists Y)X + Y = \{0\}.$$

В самом деле, $Y + \{0\} = Y$ для любого Y . Если же X содержит как минимум два элемента, то и $X + Y$ будет содержать как минимум два элемента, т. е. $X + Y \neq \{0\}$. $\square$

В дальнейшем для краткости будем при помощи строчных букв обозначать множества вида $\{a\}$ и называть их векторами, как и элементы самого пространства $\mathfrak{L}$. При этом в силу обратимости таких элементов мы можем для них использовать не только сложение, но и вычитание:

$$X - y = Z \equiv Z + y = X.$$

2. Пространства над полем рациональных чисел

В данном разделе мы изучаем только пространства над полями характеристики нуль, о чем не всегда будем упоминать специально. Для доказательства возможности интерпретации в алгебре $\text{exr } \mathfrak{L}$ арифметики второго порядка, когда основное поле имеет характеристику нуль, используем наш ранний результат:

Теорема 2 ([7, теорема 6]). *Для аддитивного моноида натуральных чисел $\Omega = (\omega, +)$ теория алгебры $\text{exr}_0 \Omega$ подмножеств, содержащих нуль, алгоритмически эквивалентна арифметике второго порядка.*

Таким образом, нашей задачей будет выделить в алгебре $\text{exr } \mathfrak{L}$ подалгебру, изоморфную $\text{exr}_0 \Omega$. Сначала покажем, как выделить в $\text{exr } \mathfrak{L}$ множества, являющиеся циклическими подгруппами $\mathfrak{L}$.

Лемма 3. *Формула*

$$I_{\mathbb{Z}}(X) \equiv X + X = X \wedge (\exists y)[y \neq \{0\} \wedge X + y = X \wedge X - y = X \\ \wedge (\forall Z)(X + Z = X \wedge Z + y = Z \wedge Z - y = Z \rightarrow X = Z)]$$

выделяет в $\text{exp } \mathfrak{L}$ множества, которые являются аддитивными подгруппами пространства $\mathfrak{L}$, изоморфными $\mathbb{Z}$.

Доказательство. Если $X \subseteq \mathfrak{L}$ является подгруппой, порожденной одним элементом a , то равенство $X + X = X$ очевидно, а в качестве y возьмем $\{a\}$, получим $X \pm y = X$. Так как $0 \in X$, то $Z = Z + \{0\} \subseteq Z + X$, поэтому из $Z + X = X$ следует $Z \subseteq X$, а из $Z \pm y = Z$ вытекает, что Z содержит все элементы вида na для целых n , т. е. $Z = X$.

Пусть теперь выполнено $I_{\mathbb{Z}}(X)$ для некоторого $y = \{a\}$. Тогда для любого $b \in X$ получаем $b + na \in X$ для целых n . Возьмем $Z = \{na : n \in \mathbb{Z}\}$. Поскольку $X + Z$ будет состоять из элементов вида $b + na \in X$, то $X + Z \subseteq X$, а с другой стороны из $0 \in Z$ следует $X = X + \{0\} \subseteq X + Z$. Таким образом, $Z = X$. Значит, все элементы X имеют вид na и X изоморфно $\mathbb{Z}$. $\square$

Теперь укажем способ определить, интересующие нас моноиды.

Лемма 4. Формула

$$I_{\Omega}(X) \equiv X + X = X \wedge X \neq \{0\} \wedge \neg I_{\mathbb{Z}}(X) \wedge (\exists Z) [I_{\mathbb{Z}}(Z) \wedge X + Z = Z \wedge X \neq Z \\ \wedge (\forall Y)(Y + Y = Y \wedge Y + Z = Z \wedge X + Y = Y \rightarrow X = Y \vee Y = Z)]$$

выделяет в $\text{exp } \mathfrak{L}$ множества, которые являются аддитивными моноидами, изоморфными Ω .

Доказательство. Если X является моноидом, изоморфным Ω , то берем в качестве Z объединение X и противоположных ему по знаку элементов. Это гарантирует истинность первой строки формулы. Если теперь взять любой Y , удовлетворяющей посылке импликации из второй строки, то из $Y + Z = Z$ следует $Y \subseteq Z$. Далее, из $X + Y = Y$ вытекает, что вместе с любым a множество Y будет содержать и все бóльшие a элементы, если рассматривать их как целые числа, а X как натуральные. Одни только положительные числа Y содержать не может, так как не будет выполнено $Y + Y = Y$. Если Y не содержит отрицательных чисел, то оно содержит 0 и все бóльшие него числа, т. е. должно совпадать с X . Если же Y содержит хотя бы одно отрицательное число, то из $Y + Y = Y$ получаем, что Y содержит сколь угодно малые числа, поэтому оно совпадает со всем Z .

Пусть теперь выполнено $I_{\Omega}(X)$. Зафиксируем Z , существование которого утверждается и снова будем рассматривать элементы Z как целые числа. Из $X + Z = Z$ получаем, что $X \subseteq Z$, поэтому будем считать, что X тоже состоит из целых чисел.

Если X содержит числа разных знаков, то выбрав среди его элементов наименьший по модулю a , мы получим, что X является порожденной a циклической группой, что противоречит $\neg I_{\mathbb{Z}}(X)$.

С другой стороны, X не может содержать одни только положительные или одни только отрицательные числа, так как при этом не будет выполнено $X + X = X$.

Итак, X должно содержать 0 и числа одного знака, например, положительные, т. е. натуральные. Но если бы X не совпало с множеством всех натуральных чисел ω , то взяв ω в качестве Y мы получили бы ложность второй строки. $\square$

Теперь легко получить интересующий нас результат для пространств над полями характеристики нуль.

Теорема 5. *Если $\mathfrak{L}$ – линейное пространство над полем характеристики нуль, то теория аддитивной алгебры $\text{exr } \mathfrak{L}$ позволяет интерпретировать арифметику второго порядка.*

Доказательство. Зафиксируем какое-либо элемент X_0 алгебры $\text{exr } \mathfrak{L}$, для которого истинна формула $I_\Omega(X_0)$.

Теперь если рассматривать только такие подмножества X пространства $\mathfrak{L}$, для которых выполнено $X + X_0 = X_0$, то это будут в точности подмножества X_0 , содержащие 0. Аддитивная теория таких подмножеств позволяет интерпретировать арифметику второго порядка, согласно теореме 2. $\square$

Определим еще одну формулу, которая будет нами использована позднее при изучении алгебр $\text{exr } \mathfrak{L}$ для подпространств $\mathfrak{L}$ различной мощности.

Лемма 6. *Формула*

$$\text{Subspace}(X) \equiv X + X = X \wedge (\forall Y)(\forall Z)(I_\Omega(Y) \wedge I_{\mathbb{Z}}(Z) \wedge X + Y = X \wedge Y + Z = Z \rightarrow X + Z = X) \quad (1)$$

истинна в $\text{exr } \mathfrak{L}$ тогда и только тогда, когда X является подпространством $\mathfrak{L}$.

Доказательство. Если X является подпространством, то истинность всех формул, входящих в $\text{Subspace}(X)$ очевидна.

Пусть теперь выполнено $\text{Subspace}(X)$. Возьмем $a \in X$, тогда из $X + X = X$ получаем $na \in X$ для всех целых положительных n . Рассмотрим $Y = \{na : n \in \omega\}$, тогда, очевидно, $X + Y = X$. Выберем теперь любое целое положительное m и определим $Z = \{na/m : n \in \mathbb{Z}\}$. Тогда истинной будет левая часть импликации во второй строке, следовательно, $X + Z = X$. Это рассуждение доказывает, что X содержит все αa для $\alpha \in \mathbb{Q}$. Иными словами, X замкнуто относительно умножения на все рациональные числа, в частности оно содержит 0 и $-a$. Теперь из $X + X = X$ сразу следует, что X замкнуто относительно сложения и вычитания, т. е. является подпространством над множеством рациональных чисел $\mathbb{Q}$. $\square$

3. Пространства над полями вычетов

В этом разделе рассматриваются только пространства над полями вычетов $\mathbb{Z}_p$. При этом некоторые результаты, которые мы отметим отдельно, от основного поля не зависят,

поэтому их можно будет позже использовать и для пространств над полями характеристики нуль.

Для пространств над полями вычетов $\mathbb{Z}_p$ подпространства определяются в $\text{exp } \mathfrak{L}$ проще, чем в лемме 6.

Лемма 7. Формула

$$\text{Subspace}(X) \equiv X + X = X \quad (2)$$

истинна в $\text{exp } \mathfrak{L}$ тогда и только тогда, когда X является подпространством $\mathfrak{L}$.

Доказательство. Если X – подпространство, то из $0 \in X$ сразу получаем

$$X + X \subseteq X = X + \{0\} \subseteq X + X,$$

т. е. $X + X = X$.

Пусть $X + X = X$, тогда X замкнуто относительно сложения, а вместе с любым a множество содержит $2a$, $3a$ и т. д. Для полей конечной характеристики p сразу получаем $0 = pa \in X$ и $-a = (p-1)a \in X$. $\square$

Заметим, что дальнейшие утверждения, кроме леммы 13 и ее следствий, не используют характеристику основного поля, поэтому они будут справедливы и для полей характеристики нуль (нужно только вместо формулы (2) использовать формулу (1)), что нам потребуется в следующем разделе.

Лемма 8. Формула $X + Y = Y$ истинна в $\text{exp } \mathfrak{L}$ для подпространства Y тогда и только тогда, когда X является подмножеством Y .

Доказательство. Если $X + Y = Y$, то из $0 \in Y$ немедленно получаем

$$X = X + \{0\} \subseteq X + Y = Y.$$

Если $X \subseteq Y$ и $a \in X$, то $X + Y \subseteq Y + Y = Y = Y + \{a\} \subseteq Y + X$, т. е. $X + Y = Y$. $\square$

В частности, для одноэлементных множеств $x = \{a\}$ отношение $x \subseteq Y$ означает $a \in Y$, поэтому далее для наглядности будем писать $x \in Y$. Также в дальнейшем при помощи заглавных букв будем обозначать только подмножества $\mathfrak{L}$, являющиеся подпространствами, что специально не будем отмечать, чтобы не загромождать формулы обозначениями.

В частности, определимость $\subseteq$ для подпространств означает определимость того, что пространства не пересекаются:

$$X \perp Y \equiv (\forall Z)(Z \subseteq X \wedge Z \subseteq Y \rightarrow Z = \{0\}).$$

Лемма 9. Формула

$$\text{Subspace}_1(X) \equiv (\forall Y)(Y \subseteq X \rightarrow X = Y \vee Y = \{0\})$$

истинна в $\text{exp } \mathfrak{L}$ тогда и только тогда, когда X является одномерным подпространством.

Доказательство. В формуле явно сказано, что любое подпространство X будет или нулевым, или совпадающим с X . $\square$

Для непересекающихся изоморфных подпространств X и Y можно определить изоморфизм h между X и Y , указав множество E пар вида $a + h(a)$ для $a \in X$. Это множество, очевидно, снова будет подпространством, так как

$$(a + h(a)) + (b + h(b)) = (a + b) + (h(a) + h(b)) = (a + b) + h(a + b)$$

для $a, b \in X$. Заметим, что по E можно однозначно восстановить h : если предположить, что $h_1 \neq h_2$, но $E_1 = E_2 = E$, то $h_1(a) \neq h_2(a)$ для некоторого $a \in X$. Следовательно, $a + h_1(a) \neq a + h_2(a)$. Но с другой стороны, $a + h_2(a) \in E$, что должно означать $a + h_1(a) = b + h_2(b) \in E$ для некоторого $b \in X$, которое необходимо отличается от a . Тогда $0 = a + h_1(a) - (b + h_2(b)) = (a - b) - (h_2(b) - h_1(a))$, т. е. $a - b = h_2(b) - h_1(a)$, что противоречит тому, что X и Y не пересекаются, потому как $0 \neq a - b \in X$, а $h_2(b) - h_1(a) \in Y$.

Лемма 10. Пусть подпространства X и Y не пересекаются. Формула

$$\begin{aligned} \text{Iso}(X, E, Y) \equiv & (\forall x \in X)(\exists! y \in Y)x + y \in E \\ & \wedge (\forall y \in Y)(\exists! x \in X)x + y \in E \wedge (\forall e \in E)(\exists! x \in X)(\exists! y \in Y)x + y = e \end{aligned}$$

определяет изоморфизм E между X и Y . Здесь сокращение $\exists!$ как обычно означает “существует и единственный”. Формула

$$\text{Value}(E, x, y) \equiv (\exists e)(e \in E \wedge e = x + y)$$

определяет значение $y \in Y$ изоморфизма E на векторе $x \in X$.

Теперь мы в состоянии определить подпространства бесконечной размерности.

Лемма 11. Формула

$$\begin{aligned} \text{Inf}(X) \equiv & (\exists U, V, W \subseteq X)(\neg U \subseteq V \wedge U + V \perp W \\ & \wedge (\exists E_1, E_2)(\text{Iso}(V, E_1, W) \wedge \text{Iso}(U + V, E_2, W))) \end{aligned}$$

истинна в $\text{exp } \mathfrak{L}$ тогда и только тогда, когда X является бесконечномерным.

Доказательство. В бесконечномерном пространстве можно выделить три подпространства U, V, W такие, что $U \not\subseteq V$, $U + V$ и W не пересекаются, а W изоморфно как V , так и большему подпространству $U + V$: V и W счетно-бесконечномерны, U — одномерное не из V . В конечномерном подпространстве такого, очевидно, сделать нельзя. $\square$

Используя два изоморфизма между непересекающимися подпространствами, $h : X \rightarrow Y$ и $g : Y \rightarrow X$, можно определить автоморфизм A подпространства X , который будем задавать четверкой $A = (X, E_h, Y, E_g)$.

Лемма 12. *Формула*

$$\text{Auto}(A) \equiv X \perp Y \wedge \text{Iso}(X, E_h, Y) \wedge \text{Iso}(Y, E_g, X)$$

определяет автоморфизм $A = (X, E_h, Y, E_g)$ подпространства X . Формула

$$A(x) = z \equiv (\exists y)(y \in Y \wedge \text{Value}(E_h, x, y) \wedge \text{Value}(E_g, y, z))$$

определяет значение $z \in X$ автоморфизма $A = (X, E_h, Y, E_g)$ на векторе $x \in X$.

Мы построим интерпретацию арифметики второго порядка в $\text{exp } \mathfrak{L}$, интерпретируя каждое натуральное число n с помощью подпространства размерности n , поэтому областью интерпретации будут подпространства X , удовлетворяющие формуле $\neg \text{Inf}(X)$.

Лемма 13. *Отношение равенства переменных первого порядка $x = y$ интерпретируется формулой*

$$\text{Equ}(X, Y) \equiv (\exists Z, E_1, E_2)(Z \perp X \wedge Z \perp Y \wedge \text{Iso}(X, E_1, Z) \wedge \text{Iso}(Z, E_2, Y)). \quad (3)$$

Доказательство. Переменные первого порядка принимают натуральные значения. Тогда они должны интерпретироваться подпространствами конечной размерности. В силу конечности простого поля, эти подпространства конечны, поэтому в бесконечном пространстве $\mathfrak{L}$ еще одно Z такой же размерности обязательно найдется.

С другой стороны, изоморфные подпространства обязаны иметь одну и ту же размерность. $\square$

Отметим, что предыдущая лемма уже неверна для произвольных пространств над полями характеристики нуль, так как для них из бесконечности пространства не следует его бесконечномерность.

Лемма 14. *Отношение “меньше” переменных первого порядка $x < y$ интерпретируется формулой*

$$\text{Less}(X, Y) \equiv (\exists Z)(Z \subseteq Y \wedge Z \neq Y \wedge \text{Equ}(Z, X)). \quad (4)$$

Доказательство. Если $x < y$, то X можно изоморфно вложить в Y так, что образ не совпадет со всем Y . Если $x \geq y$, то в силу конечномерности X и Y , так сделать невозможно. $\square$

Лемма 15. *Операция сложения переменных первого порядка $x + y = z$ интерпретируется формулой*

$$\text{Add}(X, Y, Z) \equiv (\exists X', Y')(\text{Equ}(X, X') \wedge \text{Equ}(Y, Y') \wedge X' \perp Y' \wedge X' + Y' = Z).$$

Доказательство. Здесь просто записано, что Z является прямой суммой двух своих подпространств, изоморфных X и Y . $\square$

Заметим, что аналогично интерпретируется и прибавление единицы.

Лемма 16. *Прибавление единицы $x + 1 = y$ интерпретируется формулой*

$$\text{Inc}(X, Y) \equiv (\exists U, V)(U \perp V \wedge U + V = Y \wedge \text{Equ}(X, U) \wedge \text{Subspace}_1(V)).$$

Напомним, что любой линейный автоморфизм разлагает линейное пространство, на котором он действует, в прямую сумму максимальных неприводимых инвариантных подпространств (см. [10]). Само такое разложение не единственно, но размерности этих подпространств определяются однозначно, чем мы и воспользуемся.

Лемма 17. *Отношение “ U является ненулевым инвариантным подпространством автоморфизма $A = (X, E_1, Y, E_2)$ ” определяется формулой*

$$\text{Inv}_0(A, U) \equiv U \subseteq X \wedge U \neq \{0\} \wedge (\forall x)(x \in U \rightarrow A(x) \in U).$$

Отношение “ U является неприводимым инвариантным подпространством автоморфизма A ” определяется формулой

$$\text{Inv}_1(A, U) \equiv \text{Inv}_0(A, U) \wedge (\forall V, W) \neg (V + W = U \wedge V \perp W \wedge \text{Inv}_0(V) \wedge \text{Inv}_0(W)).$$

Отношение “ U является максимальным неприводимым инвариантным подпространством автоморфизма A ” определяется формулой

$$\text{Inv}(A, U) \equiv \text{Inv}_1(A, U) \wedge (\forall V)(U \subseteq V \wedge \text{Inv}_1(V) \rightarrow U = V).$$

Теперь укажем метод интерпретации переменных второго порядка. Для элементарной арифметики можно считать, что они обозначают множества, состоящие из натуральных чисел (см. [11]). Множество T натуральных чисел мы будем интерпретировать, как автоморфизм некоторого подпространства, имеющий максимальными неприводимыми инвариантными подпространствами в точности такие, которые имеют размерность $n + 2$ для $n \in T$. Такое преобразование легко построить, взяв некоторое подпространство X и его автоморфизм, матрица которого в каком-нибудь базисе состоит из жордановых клеток размера $n + 2$, $n \in T$.

Лемма 18. *Отношение принадлежности $x \in T$ интерпретируется следующей формулой, в которой $A_T = (X, E_1, Y, E_2)$,*

$$\text{In}(X, A_T) \equiv (\exists Z)(\text{Equ}([X + 2], Z) \wedge \text{Inv}(A_T, Z)).$$

С помощью $[X + 2]$ мы обозначили подпространство, размерность которого на 2 больше размерности X , т. е. оно определяется двукратным применением леммы 16.

Построенных отношений $=$, $\in$ и операции сложения достаточно, чтобы интерпретировать арифметику второго порядка, так как, используя перечисленные отношения можно задать отношение делимости, а через него – умножение (см. [12]).

Теорема 19. *Отношение делимости определимо в арифметике второго порядка следующей формулой:*

$$x \mid y \equiv (\exists T)(0 \in T \wedge x \in T \wedge y \in T \\ \wedge (\forall z)(0 < z \wedge z < x \rightarrow \neg z \in T) \wedge (\forall z)(z \in T \leftrightarrow z + x \in T)).$$

Доказательство. Формула определяет арифметическую прогрессию с разностью x , начинающуюся с нуля, элементом которой является y . $\square$

4. Счетные и несчетные пространства

Покажем, что для счетно-бесконечных линейных пространств $\mathfrak{L}$ полученная оценка степени неразрешимости является точной: теория системы $\text{exp } \mathfrak{L}$ тоже интерпретируется в арифметике второго порядка.

Теорема 20. *Пусть линейное пространство $\mathfrak{L}$ над простым полем является счетно бесконечным. Тогда существует интерпретация теории системы $\text{exp } \mathfrak{L}$ в арифметике второго порядка.*

Доказательство. Прежде всего, отметим, что элементы α простого поля $\mathbb{F}$ (поля вычетов $\mathbb{Z}_p$ или рациональных чисел $\mathbb{Q}$) могут быть представлены в арифметике натуральными числами r_α так, что сложение $\alpha + \beta$ и умножение $\alpha\beta$ элементов поля тоже представляется в арифметике некоторыми формулами. Счетно бесконечное пространство имеет счетно бесконечный или, возможно, конечный для поля $\mathbb{Q}$, базис $\{e_0, e_1, \dots\}$. Тогда каждый вектор a имеет вид $\sum_{i < n} \alpha_i e_i$ и может быть представлен в арифметике конечной последовательностью $(r_{\alpha_0}, \dots, r_{\alpha_{n-1}})$, а с помощью β -функции Геделя ее можно закодировать одним натуральным числом r_a (см. [12]). В этом случае в арифметике для натуральных чисел легко определить операцию $\oplus$, интерпретирующую сложение векторов. Тогда множество X векторов естественным образом интерпретируется в арифметике второго порядка множеством T_X , состоящим из всех r_a , где $a \in X$. Операция сложения $X + Y = Z$ подмножеств $\mathfrak{L}$ интерпретируется формулой

$$T_X + T_Y = T_Z \equiv (\forall z)(z \in T_Z \leftrightarrow (\exists x \in T_X, y \in T_Y)x \oplus y = z).$$

$\square$

Для несчетных и, следовательно, несчетномерных линейных пространств, это утверждение уже не является самоочевидным. Тем более, что для пространств разной размерности элементарные теории алгебр $\text{exp } \mathfrak{L}$ будут различны.

Теорема 21. Пусть α и β – не элементарно эквивалентные как упорядоченные множества ординалы. Тогда для бесконечномерных пространств $\mathfrak{L}_\alpha$ и $\mathfrak{L}_\beta$ размерностей ω_α и ω_β соответственно теории алгебр $\text{exr } \mathfrak{L}_\alpha$ и $\text{exr } \mathfrak{L}_\beta$ различны. Здесь ω_i – это i -й кардинал, начиная со счетно бесконечного $\omega_0 = \omega$.

Доказательство. Зафиксируем в $\mathfrak{L}$ некоторое подпространство X^* , удовлетворяющее следующему условию:

$$(\exists Y, E)(Y \perp X^* \wedge \text{Iso}(X^*, E, Y) \wedge X^* + Y = \mathfrak{L}). \quad (5)$$

Эта формула говорит, что X^* является “половиной” пространства $\mathfrak{L}$. В силу бесконечности $\mathfrak{L}$ размерность X^* будет такой же.

Рассмотрим интерпретацию τ теории некоего ординала в теории алгебры $\text{exr } \mathfrak{L}$. Каждый ординал γ будем интерпретировать как подпространство $X_\gamma \subseteq X^*$ размерности ω_γ (и такой же мощности). Ввиду того, что существует еще одно подпространство как минимум такой же размерности, не пересекающееся с X_γ (оно является подмножеством Y из (5)), мы можем по-прежнему использовать формулы из леммы 13 и далее.

Отношения равенства $x = y$ и порядка $x < y$ тогда интерпретируются формулами (3) и (4) из лемм 13 и 14 соответственно.

В результате, очевидно, любая формула φ будет истинна в теории ординала α тогда и только тогда, когда ее интерпретация $\tau(\varphi)$ будет истинна в теории $\text{exr } \mathfrak{L}$ бесконечного пространства мощности ω_α . $\square$

5. Заключение

В последней части мы доказали, что системы $\text{exr } \mathfrak{L}$ могут иметь разные теории для $\mathfrak{L}$ различной мощности. Поэтому возникает естественный вопрос: возможно ли интерпретировать теорию системы $\text{exr } \mathfrak{L}$ для несчетномерных пространств в арифметике второго порядка?

Второй, связанный с этим же вопрос: сколько существует теорий вида $\text{exr } \mathfrak{L}$, счетно ли их количество?

Список литературы

- [1] S.M. Dudakov, B.N. Karlov, *On decidability of theories of regular languages*, Theory Comput. Syst. **65** (3), 462–478 (2021).
DOI: <https://doi.org/10.1007/s00224-020-09995-4>
- [2] I. Rewitzky, C. Brink, *Predicate transformers as power operations*. Form. Asp. Comput. **7** (2), 169–182 (1995).
DOI: <https://doi.org/10.1007/BF01211604>

- [3] J. van Benthem, N. Bezhanishvili, *Modal structures in groups and vector spaces*, J. Logic Comput. **34** (1), 75–124 (2024).
DOI: <https://doi.org/10.1093/logcom/exac105>
- [4] C. Brink, *Power structures*, Algebra Universalis **30** (2), 177–216 (1993).
DOI: <https://doi.org/10.1007/BF01196091>
- [5] T. Tamura, J. Shafer, *Power semigroups*, Math. Japon. **12**, 25–32 (1967).
- [6] Б. Н. Карлов, *Об элементарной эквивалентности некоторых уноидов и уноидов их подмножеств*, Вестник ТвГУ. Серия: Прикладная математика (3), 18–32 (2021).
DOI: <https://doi.org/10.26456/vtprm620>
- [7] S.M. Dudakov, *On undecidability of concatenation theory for one-symbol languages*, Lobachevskii J. Math. **41** (2), 168–175 (2020).
DOI: <https://doi.org/10.1134/S1995080220020055>
- [8] S.M. Dudakov, *On undecidability of subset theory for some monoids*, J. Phys.: Conf. Ser. **1902**, art. 012060 (2021).
DOI: <https://doi.org/10.1088/1742-6596/1902/1/012060>
- [9] S.M. Dudakov, *On undecidability of finite subsets theory for torsion abelian groups*, Mathematics **10** (3), art. 533 (2022).
DOI: <https://doi.org/10.3390/math10030533>
- [10] А. И. Кострикин, Ю. И. Манин, *Линейная алгебра и геометрия*, Наука, М., 1986.
- [11] Х. Роджерс, *Теория рекурсивных функций и эффективная вычислимость*, Мир, М., 1972.
- [12] G.S. Boolos, J.P. Burgess, R.C. Jeffrey, *Computability and logic*, Cambridge Univ. Press, Cambridge, 2007.
DOI: <https://doi.org/10.1017/CBO9780511804076>

Сергей Михайлович Дудаков

Тверской государственный университет,
ул. Желябова, д. 33, г. Тверь, 170100, Россия,
Университет HSE (Высшая школа экономики),
ул. Усачева, д. 6, г. Москва, 119048, Россия,
e-mail: sergeydudakov@yandex.ru

On undecidability degree of theory of figures in linear spaces

S.M. Dudakov

Abstract. We study the additive theory of arbitrary figures in linear spaces, that is, the theory of addition extended to sets of vectors. Our main result is the following: if a linear space is infinite, then the additive theory of figures allows to interpret second-order arithmetic and, therefore, has this or higher degree of undecidability. For countably infinite spaces, we prove the opposite result, the theory of figures can be interpreted in second-order arithmetic. Therefore, these theories are algorithmically equivalent. For uncountable spaces, the last question remains open. We show that for spaces of different cardinalities, the additive theories of figures can be elementary non-equivalent.

Keywords: linear space, subsets algebra, algorithmic undecidability, second-order arithmetic.

DOI: 10.26907/2949-3919.2024.4.51-65

References

- [1] S.M. Dudakov, B.N. Karlov, *On decidability of theories of regular languages*, Theory Comput. Syst. **65** (3), 462–478 (2021).
DOI: <https://doi.org/10.1007/s00224-020-09995-4>
- [2] I. Rewitzky, C. Brink, *Predicate transformers as power operations*. Form. Asp. Comput. **7** (2), 169–182 (1995).
DOI: <https://doi.org/10.1007/BF01211604>
- [3] J. van Benthem, N. Bezhanishvili, *Modal structures in groups and vector spaces*, J. Logic Comput. **34** (1), 75–124 (2024).
DOI: <https://doi.org/10.1093/logcom/exac105>
- [4] C. Brink, *Power structures*, Algebra Universalis **30** (2), 177–216 (1993).
DOI: <https://doi.org/10.1007/BF01196091>
- [5] T. Tamura, J. Shafer, *Power semigroups*, Math. Japon. **12**, 25–32 (1967).

- [6] B.N.Karlov, *On elementary equivalence of some unoids and unoids of their subsets*, Vestnik TvGU. Seriya: Prikladnaya Matematika [Herald of Tver State University. Series: Applied Mathematics] (3), 18–32 (2021) [in Russian].
DOI: <https://doi.org/10.26456/vtpmk620>
- [7] S.M.Dudakov, *On undecidability of concatenation theory for one-symbol languages*, Lobachevskii J. Math. **41** (2), 168–175 (2020).
DOI: <https://doi.org/10.1134/S1995080220020055>
- [8] S.M.Dudakov, *On undecidability of subset theory for some monoids*, J. Phys.: Conf. Ser. **1902**, art. 012060 (2021).
DOI: <https://doi.org/10.1088/1742-6596/1902/1/012060>
- [9] S.M.Dudakov, *On undecidability of finite subsets theory for torsion abelian groups*, Mathematics **10** (3), art. 533 (2022).
DOI: <https://doi.org/10.3390/math10030533>
- [10] A.I.Kostrikin, Yu.I.Manin, *Linear algebra and geometry*, CRC Press, London, 1997.
DOI: <https://doi.org/10.1201/9781466593480>
- [11] H.Rogers, *Theory of recursive functions and effective computability*, MIT Press, Cambridge, Mass., 1967.
- [12] G.S.Boolos, J.P.Burgess, R.C.Jeffrey, *Computability and logic*, Cambridge Univ. Press, Cambridge, 2007.
DOI: <https://doi.org/10.1017/CBO9780511804076>

Sergey Mikhailovich Dudakov

Tver State University,

33 Zhelyabova str., Tver 170100, Russia,

HSE University,

6 Usacheva str., Moscow 119048, Russia,

e-mail: sergeydudakov@yandex.ru

Отделимые нумерации универсальных алгебр

Н.Х. Касымов

Аннотация. В обзоре излагаются основы теории отделимых нумераций универсальных алгебр.

Ключевые слова: отделимо нумерованная алгебра, эффективно отделимая нумерация, негативная и эффективно отделимая аппроксимируемость, трансляционно полная и предполная алгебра, топологическая нумерованная алгебра, подпрямая неразложимость, артинова решетка конгруэнций, алгебраические и логические спецификации структуры данных.

DOI: 10.26907/2949-3919.2024.4.66-102

Введение

Теория нумерованных алгебр, систематическое изучение которой восходит к обзорной статье А.И. Мальцева [1], является бурно развивающейся областью современной математической логики, имеющей многочисленные пересечения с другими разделами естествознания, в частности – с теоретической информатикой. Ввиду обширности класса всех нумерованных систем представляется целесообразным изучение нумерованных систем при наложении алгоритмических ограничений различных типов на нумерационные эквивалентности (ядра) их нумераций. В рамках этого направления в первую очередь, нужно выделить вычислимые, т. е. алгоритмически разрешимые нумерации (см. [2–4]) с вычислимыми ядрами, которые поддерживаются вычислимыми представляющими функциями и отношениями, а ослабление требований к алгоритмической сложности ядер нумераций (при рассмотрении арифметических и других иерархий в качестве допустимых для сложности ядер нумераций) является общепринятым способом расширения изучаемых классов нумерованных алгебр (см. [5, 6]).

Другой подход заключается в игнорировании сложности нумерационной эквивалентности и ограничении рассматриваемых классов нумераций систем алгоритмическими условиями типа отделимости. Идеи применения отделимости в теории вычислимости, восходящие к В.А. Успенскому [7, 8] и А. Нероуду [9], получили дальнейшее и глубокое развитие в работах А.И. Мальцева [10] и Ю.Л. Ершова [11].

Благодарности. Работа выполнена в рамках реализации Программы развития Научно-образовательного математического центра Приволжского федерального округа (соглашение № 075-02-2024-1438).

Классическим и простейшим алгоритмическим условием отделимости является вычислимая отделимость. Многие естественные и важные типы нумерованных универсальных алгебр оказались вычислимо отделимыми, в том числе негативные алгебры, стандартно нумерованные конечно порожденные и финитно аппроксимируемые алгебры, позитивные алгебры со счетными решетками конгруэнций и т. д. (см. обзор [12]). Различные аспекты негативных нумераций и негативных алгебр исследовались Ю.Л. Ершовым [11], А.И. Мальцевым [13], А.С. Морозовым [14], Н.Г. Хисамиевым [5], С.П. Одинцовым и В.Л. Селивановым [6]. Классические результаты о позитивных универсальных алгебрах со счетными решетками конгруэнций можно найти у А.И. Мальцева [1], Ю.Л. Ершова [2], В. Баура [15, 16]. Проблематика исследования стандартных нумераций конечно порожденных алгебр, заложенная А.И. Мальцевым в [1], обосновывается В.А. Успенским и А.Л. Семеновым в [17], а классические образцы использования финитной аппроксимируемости для решения алгоритмических задач алгебры представлены у А.И. Мальцева в [1] и Д. Мак-Кинси в [18].

На базе и в рамках теории вычислимо отделимо представимых универсальных алгебр решается ряд вопросов, возникших в связи с работами А.И. Мальцева [1], В. Баура [15], Д. Бергстры и Д. Такера [19].

В сложных самоорганизующихся системах, по-видимому, важное значение имеет проблема распознавания. Если система задана своим алгоритмическим представлением, то с математической точки зрения это означает, что любая пара различных элементов отделяется алгоритмически определяемыми окрестностями. Важнейшими типами отделимых нумераций алгебр являются эффективно отделимые, т. е. такие, для которых существуют вычислимые (в смысле [11]) семейства отделяющих вычислимо перечислимых множеств. Основания теории отделимо нумерованных множеств и связи между отделимостью и эффективной отделимостью были введены, развиты и исследованы Ю.Л. Ершовым (см. [11]).

Находясь в рамках парадигмы о существовании у нумерованной алгебры эффективной системы алгоритмически порождаемых окрестностей, достаточных для распознавания отделимости любой пары ее элементов, нужно признать, что именно исследовавшееся Ю.Л. Ершовым в [11] наиболее общее понятие отделимой нумерации в случае нумераций универсальных алгебр можно трактовать как одно из математических уточнений понятия сложной развивающейся системы, интенционально заданной семейством представляющих вычислимых функций вместе с ядрами гомоморфизмов (нумераций) и допускающей эффективное распознавание различия составляющих ее элементов путем отделения их подходящими алгоритмически определяемыми окрестностями.

Результаты настоящего обзора в основном базируются на следующих фактах:

Нумерованная алгебра вычислимо отделима (отделима) если и только если она аппроксимируется негативными (эффективно отделимыми) алгебрами ([12, 20, 21]).

Целью настоящего обзора является изложение основ теории отделимо нумерованных универсальных алгебр и демонстрация некоторых приложений этой теории как в математической логике, так и в теоретической информатике.

Автор выражает глубокую благодарность Ю.Л. Ершову, С.С. Гончарову, А.С. Морозову и Б.М. Хусаинову, многочисленные и плодотворные обсуждения с которыми способствовали синтезу теории отделимых нумераций и универсальной алгебры.

1. Нумерованные алгебры

Определение 1. Алгоритмическим представлением счетной универсальной алгебры $\mathfrak{A} = \langle A; \Sigma \rangle$ эффективной сигнатуры Σ называется всякое такое отображение ν множества натуральных чисел ω на основное множество A алгебры $\mathfrak{A}$, для которого существует эффективное семейство F_Σ вычислимых функций, представляющих Σ -операции алгебры $\mathfrak{A}$ в нумерации ν , т.е. всякая операция $\sigma \in \Sigma$ представляется соответствующей ей такой вычислимой функцией $f_\sigma \in F_\Sigma$, что $\forall \bar{x} (\sigma \nu(\bar{x}) = \nu f_\sigma(\bar{x}))$.

Определение 2. Если ν – алгоритмическое представление алгебры $\mathfrak{A}$, то пара $(\mathfrak{A}, \nu)$ называется нумерованной алгеброй.

Далее под гомоморфизмами нумерованных алгебр мы понимаем их морфизмы, т.е. мы работаем в категории нумерованных алгебр с морфизмами в качестве эффективных на номерах гомоморфизмов.

Определение 3. Гомоморфизм $\varphi : \mathfrak{A} \rightarrow \mathfrak{B}$ называется вычислимым гомоморфизмом нумерованных моделей $(\mathfrak{A}, \mu) \rightarrow (\mathfrak{B}, \nu)$, если существует такая вычислимая функция h , что $\varphi \mu = \nu h$.

Ядром представления ν нумерованной алгебры $(\mathfrak{A}, \nu)$ будем называть эквивалентность $\{\langle x, y \rangle \mid \nu x = \nu y\}$. Если ν – представление, то его ядро будем обозначать через $\ker(\nu)$.

Пусть η – фиксированная эквивалентность на ω и $\mathfrak{A}$ – алгебра (не обязательно эффективной сигнатуры), обладающая представлением с ядром равным η . Тогда алгебру $\mathfrak{A}$ будем называть представимой над η (или η -алгеброй).

Для фиксированной алгебры классической является проблема изучения различных ее алгоритмических представлений и соотношений между ними, в частности, проблема существования хороших представлений (например, вычислимых) и их числа (в том числе единственности, с точностью до вычислимого изоморфизма).

С другой стороны, можно фиксировать ядро представления и изучать общие свойства алгебр, обладающих представлениями с данным ядром. Этот подход представляется целесообразным с точки зрения теории алгоритмических представлений алгебраических систем в рамках теоретической информатики (см. [12, 22]).

Изучению алгоритмических свойств эквивалентностей в настоящее время уделяется большое внимание. Можно отметить работы многих авторов, библиографию по этим вопросам можно найти в списках литературы к работам [23–25].

Представимость универсальной алгебры $\mathfrak{A}$ над эквивалентностью η равносильна существованию такой вычислимой алгебры $\langle \omega; F \rangle$, где F – подходящее семейство вычислимых функций, что η является конгруэнцией алгебры $\langle \omega; F \rangle$ и $\mathfrak{A}$ изоморфна фактор-алгебре

$\langle \omega/\eta; F \rangle$, т. е. фактически нумерация есть гомоморфизм из некоторой вычислимой алгебры на абстрактную.

Определение 4. Характеристической трансверсалью эквивалентности η на ω (обозначаемой через $\text{tr}(\eta)$) называется множество всех натуральных чисел, являющихся наименьшими в содержащих их смежных η -классах, т. е. $\text{tr}(\eta) = \{x \mid \forall y(x = y \pmod{\eta} \Rightarrow x \leq y)\}$. Характеристической трансверсалью нумерации ν называется характеристическая трансверсаль ее ядра, т. е. $\text{tr}(\ker(\nu))$.

Эквивалентность с бесконечным (конечным) числом смежных классов будем называть бесконечной (соответственно, конечной).

Если η – эквивалентность на ω , то множество $\alpha \subseteq \omega$ называется η -замкнутым, если $x \in \alpha \wedge x = y \pmod{\eta} \Rightarrow y \in \alpha$.

2. Вычислимо отделимые и отделимые алгебры

2.1. ХАРАКТЕРИЗАЦИИ ВЫЧИСЛИМО ОТДЕЛИМЫХ И ОТДЕЛИМЫХ АЛГЕБР

Определение 5. Подмножество $A_0 \subseteq A$ основного множества нумерованной алгебры $(\mathfrak{A}, \nu)$ называется ν -вычислимым (ν -перечислимым, ν -негативным и т. д.), если таковым является множество $\nu^{-1}A_0$. Множество $\alpha \subseteq \omega$ называется ν -замкнутым, если оно замкнуто относительно ядра нумерации ν , т. е. эквивалентности $\ker(\nu) = \{\langle x, y \rangle \mid \nu x = \nu y\}$.

Если из контекста будет ясно, о какой нумерации ν идет речь, то соответствующее подмножество будем называть вычислимым (и т. д.) без приставки ν .

Определение 6. Нумерация ν алгебры $\mathfrak{A}$ с основным множеством A называется вычислимо отделимой, если для любых различных $a_0, a_1 \in A$ существует такое ν -вычислимое подмножество $A_0 \subseteq A$, что $a_0 \in A_0 \wedge a_1 \notin A_0$.

Определение 7. Для нумерованного множества (A, ν) семейство $\mathfrak{S}$ ν -перечисливых подмножеств A называется полным разделяющим семейством, если для всяких различных $a_0, a_1 \in A$ найдется такое $\sigma \in \mathfrak{S}$, которое отделяет a_0 и a_1 (т. е. $a_0 \in \sigma \wedge a_1 \notin \sigma$ либо $a_1 \in \sigma \wedge a_0 \notin \sigma$).

Определение 8. Нумерация ν алгебры $\mathfrak{A}$ называется эффективно отделимой, если для нее существует полное разделяющее вычислимое семейство.

Неформально, эффективная отделимость нумерации означает наличие алгоритма, равномерно выдающего эффективные способы перечисления отделяющих базовых окрестностей точек множества.

Определение 9. Пусть $K = \{(\mathfrak{A}_i, \nu_i) \mid i \in I\}$ – семейство нумерованных алгебр. Нумерованная алгебра $(\mathfrak{A}, \nu)$ называется аппроксимируемой K -алгебрами (K -аппроксимируемой), если для любых различных $a_0, a_1 \in A$ существует различающий их морфизм $\varphi_j : (\mathfrak{A}, \nu) \longrightarrow (\mathfrak{A}_j, \nu_j)$ для подходящего $j \in I$ (т. е. $\varphi_j(a_0) \neq \varphi_j(a_1)$).

Теорема 10 ([12,20]). *Нумерованная алгебра вычислимо отделима тогда и только тогда, когда она аппроксимируется негативными алгебрами.*

Теорема 11 ([21]). *Нумерованная алгебра отделима тогда и только тогда, когда она аппроксимируется эффективно отделимыми алгебрами.*

Следствие 12. *Всякая вычислимо отделимая (отделимая) нумерация подпрямо неразложимой алгебры негативна (эффективно отделима).*

Следствие 13. *Всякая вычислимо отделимая (отделимая) нумерация алгебры с артиновой решеткой конгруэнций негативна (эффективно отделима).*

Определение 14. Нумерация бесконечного множества называется эффективно (неэффективно) бесконечной, если существует (не существует) бесконечное вычислимое множество натуральных чисел, попарно различных по модулю нумерационной эквивалентности.

Следствие 15. *Всякая алгебра, обладающая неэффективно бесконечной вычислимо отделимой нумерацией финитно аппроксимируема.*

Следствие 16. *Всякая алгебра, обладающая эффективно бесконечной вычислимо отделимой нумерацией с иммунной характеристической трансверсалью, финитно аппроксимируема.*

Определение 17. Бесконечное подмножество α множества ω называется наследственно высоким, если никакое его бесконечное подмножество (включая само α) не лежит в классе Π_3^0 арифметической иерархии.

Предложение 18 ([21]). *Существует такая отделимая бесконечная эквивалентность η , что*

- 1) $\text{tr}(\eta)$ – наследственно высокая;
- 2) *никакое расширение эквивалентности η не является эффективно T_1 -отделимым;*
- 3) *перечислимо порожденное пространство ω/η T_1 -отделимо, но не хаусдорфово;*
- 4) *всякая η -алгебра локально конечна и финитно аппроксимируема.*

2.2. ТРАНСЛЯЦИОННО ПОЛНЫЕ И ПРЕДПОЛНЫЕ АЛГЕБРЫ

Определение 19. Универсальная алгебра называется трансляционно полной, если всякая пара различных ее элементов переводится в любую другую пару различных элементов подходящей трансляцией.

Теорема 20 ([26]). *Всякая тело – трансляционно полная алгебра.*

Определение 21. Универсальная алгебра называется трансляционно предполной, если существует такая пара ее различных элементов, в которую переводится любая пара различных элементов подходящей трансляцией.

Очевидно, что любая трансляционно простая алгебра конгруэнц-проста, а любая трансляционно предполная алгебра подпрямой неразложима.

Предложение 22 ([26]). *Всякая T_2 -отделимая нумерация трансляционно предполной алгебры является негативной.*

Следствие 23. *Всякая T_2 -отделимая нумерация любого поля негативна.*

Однако, имеет место

Теорема 24 ([27]). *Существует T_1 -отделимая, но не $\Sigma_1^0 \cup \Pi_1^0$ -нумерация трансляционно предполной (а значит, и подпрямой неразложимой) алгебры с артиновой решеткой конгруэнций.*

Таковой будет, например, алгебра предшествования $P = \langle \omega; p \rangle$, $p(n+1) = n$, $p(0) = 0$.

Предложение 25 ([28]). *Над всякой негативной эквивалентностью представима трансляционно полная алгебра.*

Очевидно, что если над позитивной эквивалентностью представима трансляционно полная (даже подпрямой неразложимая) алгебра, то эта эквивалентность вычислима.

2.3. РАВНОМЕРНО ВЫЧИСЛИМО ОТДЕЛИМЫЕ АЛГЕБРЫ

Определение 26. Эквивалентность η равномерно вычислимо отделима, если существует такая частичная вычислимая функция g от трех переменных, что если $x \neq y \pmod{\eta}$, то функция $\lambda z.g(x, y, z)$ является характеристической вычислимой функцией для некоторого η -замкнутого множества, отделяющего x от y .

Неформально, равномерность вычислимо отделимой эквивалентности η означает существование такой эффективной процедуры, которая “выдает” для каждой пары натуральных чисел x, y , различных по модулю η , алгоритм разрешения η -замкнутого множества (характеристический индекс этого множества), отделяющего x от y .

Нумерация называется равномерно вычислимо отделимой, если таково ее ядро.

Рассмотрим следующие эквивалентности:

- 1) $\eta^\alpha = \{ \langle 2x, 2x+1 \rangle \mid x \in \alpha \} \cup \{ \langle 2x+1, 2x \rangle \mid x \in \alpha \} \cup \text{id } \omega$;
- 2) $\eta_\alpha = \alpha^2 \cup \text{id } \omega$;
- 3) $\eta_\alpha^* = \{ \langle x, y \rangle \mid \gamma_x \setminus \alpha = \gamma_y \setminus \alpha \}$, где γ – каноническая нумерация конечных множеств.

Легко проверить, что для всякого $\alpha \subseteq \omega$ все эквивалентности $\eta^\alpha, \eta_\alpha, \eta_\alpha^*$ вычислимо отделимы. При этом, η^α равномерно вычислимо отделима при всяком α , а равномерность η_α зависит от выбора α . Известно, что если $\omega \setminus \alpha$ иммунно, но не гипериммунно, то η_α не является равномерной [29]; если α – гиперпростое с регрессивным дополнением, то η_α равномерно вычислимо отделима [29].

2.3.1. СЧЕТНЫЕ РЕШЕТКИ КОНГРУЭНЦИЙ. А.И. Мальцев в работе [1] показал, что конечно порожденная позитивная алгебра, всякая ненулевая конгруэнция которой имеет конечный индекс, является вычислимой.

Предложение 27 ([30]). Пусть $\mathfrak{A}$ – универсальная алгебра, всякая ненулевая конгруэнция которой имеет конечный индекс и ν – ее неразрешимая позитивная нумерация. Тогда $\mathfrak{A}$ локально конечна, финитно аппроксимируема, локально финитно отделима, имеет неартинову решетку конгруэнций и не является уноидом, а характеристическая трансверсаль $\text{tr}(\nu)$ гипериммунна.

Предложение 27 ничего не говорит о существовании таких алгебр.

Теорема 28 ([30]). Существует такая неразрешимая позитивная и равномерно вычислимо отделимая эквивалентность, над которой представима алгебра, всякая ненулевая конгруэнция которой имеет конечный индекс, а решетка конгруэнций изоморфна $1 + \omega^*$.

Теорема 29 ([31, 32]). Всякая позитивная нумерация алгебры со счетной решеткой конгруэнций (в частности, с нетеровой и, тем более, с ненулевыми конгруэнциями только конечного индекса) вычислимо отделима. Более того, такие алгебры аппроксимируются вычислимыми алгебрами.

Теорема 30 ([31]). Всякая позитивная алгебра, обладающая ненулевыми конгруэнциями только конечного индекса, эффективно вложима в конечно порожденную позитивную алгебру с нетеровой решеткой конгруэнций.

Следствие 31. Существует бесконечная конечно порожденная позитивная алгебра, всякое позитивно представимое обогащение которой финитно аппроксимируемо.

2.3.2. ЭФФЕКТИВНО РАСЩЕПЛЯЕМЫЕ КОНГРУЭНЦИИ

Определение 32. Равномерно вычислимо отделимая нумерованная алгебра называется эффективно расщепляемой, если существует эффективная процедура, сопоставляющая любому вычислимому семейству негативных конгруэнций перечислимый индекс такой негативной конгруэнции, которая находится строго ниже пересечения всех конгруэнций данного семейства.

Теорема 33 ([33]). Нумерованная алгебра эффективно расщепляема тогда и только тогда, когда характеристическая трансверсаль ядра ее нумерации полупродуктивна.

Предложение 34 ([33]). Существует эффективно расщепляемая алгебра, характеристическая трансверсаль ядра которой не продуктивна.

2.3.3. ПОЛУПЕРЕЧИСЛИМОСТЬ. Напомним некоторые классические определения [34, 35].

Множество $\alpha \subseteq \omega$ называется

- *полурекурсивным*, если существует такая вычислимая функция $f(x, y)$, что $f(x, y) \in \{x, y\}$ и $(x \in \alpha \vee y \in \alpha) \Rightarrow f(x, y) \in \alpha$;
- *полуперечислимым*, если существует такая частичная вычислимая функция $\psi(x, y)$, что $(x \in \alpha \vee y \in \alpha) \Rightarrow \psi(x, y) \downarrow \wedge \psi(x, y) \in \{x, y\} \cap \alpha$;
- *слабо полурекурсивным*, если существует такая частичная вычислимая функция $\psi(x, y)$, что $(x \in \alpha \Leftrightarrow y \notin \alpha) \Rightarrow \psi(x, y) \downarrow \wedge \psi(x, y) \in \{x, y\} \cap \alpha$.

Непосредственно из определений следует, что полурекурсивность любого множества равносильна полурекурсивности его дополнения. Ясно также, что эти свойства связаны между собой импликациями *полурекурсивность* $\Rightarrow$ *полуперечислимость* $\Rightarrow$ *слабая полурекурсивность*.

Назовем эквивалентность η *сильно равномерно вычислимо отделимой*, если существует частичная вычислимая функция $g(x, y)$ такая, что если $x \neq y \pmod{\eta}$, то $g(x, y) \downarrow$, и $\gamma_{g(x, y)}$ является η -замкнутым множеством, отделяющим x и y (γ – каноническая нумерация конечных множеств).

По определению, сильно равномерно вычислимая эквивалентность равномерно вычислимо отделима. Обратное неверно: если эквивалентность имеет хотя бы два бесконечных смежных класса, то вопрос о ее сильно равномерной вычислимой отделимости лишен смысла. Заметим, что для всякого $\alpha \subseteq \omega$ эквивалентность η^α сильно равномерно вычислимо отделима.

Теорема 35 ([36]). *Для произвольного $\alpha \subseteq \omega$ следующие условия эквивалентны:*

- 1) η_α – сильно равномерно вычислимо отделима;
- 2) η_α – равномерно вычислимо отделима;
- 3) $\omega \setminus \alpha$ – полуперечислимо.

Эта теорема позволяет доказать следующий факт.

Предложение 36 ([36]). *Существуют две равномерно вычислимо отделимые эквивалентности, пересечение которых таковым не является.*

2.4. УСЛОВИЯ КОНЕЧНОСТИ ДЛЯ ВЫЧИСЛИМО ОТДЕЛИМЫХ АЛГЕБР

2.4.1. ЛОКАЛЬНО ФИНИТНАЯ ОТДЕЛИМОСТЬ. Напомним, что универсальная алгебра называется финитно аппроксимируемой, если для любых двух различных ее элементов существует гомоморфизм на конечную алгебру, в котором образы этих элементов также различны. Аналогично, универсальная алгебра A называется финитно отделимой, если для всякой ее подалгебры A_0 и любого элемента $a \in A \setminus A_0$ найдется такая конгруэнция конечного индекса, по модулю которой элемент a отличен от всех элементов подалгебры A_0 . Другими словами, на языке гомоморфизмов, существует такой гомоморфизм φ из алгебры A на конечную алгебру, что $\varphi(a) \notin \varphi(A_0)$. Аналогично, алгебра называется

локально финитно отделимой, если для всякой ее конечно порожденной подалгебры и любого элемента вне этой подалгебры найдется конгруэнция конечного индекса, различающая данный элемент и подалгебру.

Сформулируем критерий локально финитной отделимости всякой алгебры, представимой над равномерно вычислимо отделимой эквивалентностью.

Теорема 37 ([37]). *Для бесконечной равномерно вычислимо отделимой эквивалентности η следующие условия эквивалентны:*

- 1) *характеристическая трансверсаль $\text{tr}(\eta)$ эквивалентности η иммунна;*
- 2) *всякая η -алгебра локально финитно отделима;*
- 3) *всякая η -алгебра финитно аппроксимируема.*

Предложение 38 ([37]). *Существует такая равномерно вычислимо отделимая позитивная эквивалентность η_α для подходящего α с иммунной характеристической трансверсалью, что некоторая η_α -алгебра не является финитно отделимой.*

Предложение 39 ([37]). *Существует такая вычислимо отделимая эквивалентность вида η_α^* с иммунной характеристической трансверсалью, которая является ядром представления подходящей универсальной алгебры, не являющейся локально финитно отделимой.*

Таким образом, в условиях теоремы 37 нельзя отказаться как от алгебраического свойства локальности для финитной отделимости (предложение 38), так и от алгоритмического свойства равномерности для вычислимой отделимости (предложение 39).

Сужая класс иммунных характеристических трансверсалей до гипериммунных и расширяя класс равномерно вычислимо отделимых эквивалентностей до класса вычислимо отделимых эквивалентностей, получаем

Предложение 40 ([37]). *Пусть η – вычислимо отделимая эквивалентность с гипериммунной характеристической трансверсалью. Тогда всякая η -алгебра конечной сигнатуры локально финитно отделима.*

Приведем одну алгебраическую характеристику вычислимо отделимых эквивалентностей.

Предложение 41 ([37]). *Для бесконечной вычислимо отделимой эквивалентности η следующие условия равносильны:*

- 1) *η имеет бесконечное вычислимое расширение;*
- 2) *существует не финитно аппроксимируемая η -алгебра.*

2.4.2. ФИНИТНАЯ АППРОКСИМИРУЕМОСТЬ

Определение 42. Эквивалентность называется неэлиминируемой, если число ее смежных классов конечно и ровно один смежный класс бесконечен.

Эквивалентность, не являющуюся неэлиминируемой, назовем элиминируемой. Таким образом, любая элиминируемая эквивалентность либо бесконечна, либо содержит по крайней мере два бесконечных смежных класса.

Пусть $\mathbb{W}$ – счетное семейство элиминируемых эквивалентностей.

Теорема 43 ([37]). Пусть α – бесконечное и кобесконечное множество, содержащее число 0. Тогда существует такая эквивалентность η , каждый η -класс которой конечен, что $\text{tr}(\eta) = \alpha$ и для любого $W \in \mathbb{W}$ найдется пара элементов, различных по модулю W , но равных по модулю η .

Следствие 44. Пусть α – бесконечное и кобесконечное множество, содержащее число 0. Тогда существует такая эквивалентность η , каждый η -класс которой конечен, что $\text{tr}(\eta) = \alpha$ и всякая η -алгебра финитно аппроксимируема.

Следствие 45. Существует такая бесконечная вычислимо отделимая эквивалентность η с вычислимой характеристической трансверсалью, что всякая η -алгебра финитно аппроксимируема.

Следствие 46. Существует бесконечная вычислимо отделимая эквивалентность с вычислимой характеристической трансверсалью, всякое негативное расширение которой конечно и имеет ровно один бесконечный класс.

2.4.3. ЛОКАЛЬНАЯ КОНЕЧНОСТЬ

Определение 47. Универсальная алгебра называется конечно порожденной (локально конечной), если некоторое (всякое) ее конечное обеднение является конечно порожденным (локально конечным).

Для конечных сигнатур данное определение совпадает с классическим. Для бесконечных сигнатур понятие порожденности конечным множеством элементов и всеми сигнатурными операциями не совпадает с классическим понятием конечной порожденности. Например, рассмотрим алгебру $\mathfrak{A} = \langle \omega; f_n \rangle$, где ω – множество натуральных чисел и $\forall x \in \omega (f_n(x) = n)$. Тогда алгебра $\mathfrak{A}$ локально конечна, но порождается любым своим элементом.

Пусть A – бесконечное множество. Множество $F_A = \{f \mid f : A \rightarrow A\}$ всех отображений A в себя разделим на две части $F_0, F_1 : F_0 \cup F_1 = A$, $F_0 \cap F_1 = \emptyset$ так, что для каждой операции $f \in F_0$ справедливо следующее условие: для любого конечного $B \subset A$ существует такой элемент $a \in A \setminus B$, что $a \neq f(a) \wedge f(a) \in A \setminus B$. Все функции из F_0 будем называть A -нетривиальными или (если из контекста ясно, о каком A идет речь) нетривиальными (без приставки A -).

Операции из F_1 будем называть A -тривиальными или, аналогично сказанному выше, тривиальными. Таким образом, если f тривиально действует на A , т.е. $f \in F_1$, то существует такое конечное $B \subset A$, что для всякого элемента $a \in A \setminus B$ выполняется $a = f(a) \vee f(a) \in B$.

Пусть $\mathfrak{A} = \langle A; \Sigma \rangle$ – универсальная алгебра сигнатуры Σ и $B \subseteq A$. Подалгебру алгебры $\mathfrak{A}$, порожденную подмножеством B , будем обозначать через $\Sigma(B)$.

Предложение 48 ([38]). Пусть $\mathfrak{A}$ – алгебра конечной сигнатуры $\Sigma \subset F_A$ (т. е. $\mathfrak{A}$ – уноид), B – конечное подмножество A и подалгебра $\Sigma(B)$ бесконечна. Тогда существует хотя бы одна нетривиальная Σ -операция (т. е. из F_0).

В частности, имеет место очевидное

Следствие 49. Всякий уноид с тривиальными операциями локально конечен.

Пусть A – бесконечное счетное множество, θ – отношение эквивалентности на A и f – отображение из A^n в A . Будем говорить, что θ опускает f , если f не согласована с θ , т. е. найдутся такие наборы $\bar{x}, \bar{y}$, которые покомпонентно равны по модулю θ , но $f(\bar{x}) \neq f(\bar{y}) \pmod{\theta}$.

Другими словами, опускаемость операции f эквивалентностью θ означает, что действие f на A нельзя корректно перенести на фактор-множество A/η , образуя естественную фактор-алгебру. Если F – семейство операций на A , то будем говорить, что эквивалентность θ опускает семейство F , если θ опускает каждую операцию из F . Далее, до конца раздела будем рассматривать эквивалентности, опускающие семейства нетривиальных функций, заданных на множестве A .

Теперь, для упрощения обозначений, в качестве A будем рассматривать множество натуральных чисел ω .

Теорема 50 ([38]). Пусть F – счетное подсемейство семейства всех ω -нетривиальных отображений и T – бесконечное кобесконечное подмножество ω , содержащее 0. Тогда существует эквивалентность θ с конечными классами и характеристической трансверсалью T , опускающая семейство F .

Следствие 51. Для любого кобесконечного подмножества α множества натуральных чисел ω существует такая вычислимо отделимая эквивалентность θ с характеристической трансверсалью равной $\alpha \cup \{0\}$, что всякая уноидная алгебра представимая над θ является локально конечной.

Теорема 52 ([38]). Пусть α – подмножество множества натуральных чисел ω . Следующие условия равносильны:

- 1) α – кобесконечное множество;
- 2) существует такая эквивалентность θ с конечными θ -классами и характеристической трансверсалью, равной $\alpha \cup \{0\}$, над которой представимы только локально конечные, финитно аппроксимируемые и локально финитно отделимые унарные алгебры.

Таким образом, даже представимость над вычислимо отделимой эквивалентностью только локально конечных уноидов оказывается очень сильным свойством, обеспечивающим финитную аппроксимируемость и локально финитную отделимость любых (не обязательно унарных) алгебр, представимых над ней. Обратное, вообще говоря, неверно, так

как существуют конечно порожденные финитно аппроксимируемые и локально финитно отделимые алгебры, представимые над вычислимо отделимыми эквивалентностями с иммунными характеристическими трансверсями [12].

Ранее было неизвестно, существуют ли бесконечные эквивалентности с не иммунными характеристическими трансверсями, над которыми представимы только локально конечные уноиды.

Следствие 53. *Существует такая вычислимо отделимая эквивалентность с бесконечной вычислимой характеристической трансверсалью, что всякий представимый над ней уноид является локально конечным, финитно аппроксимируемым и локально финитно отделимым.*

3. Эффективно отделимые алгоритмические представления

Теория вычислимо отделимых алгебр и моделей в настоящий момент представляет собой вполне самостоятельную часть теории нумерованных систем со своей проблематикой, методами и парадигмой. Примерами вычислимо отделимых систем, как отмечалось выше, наряду с негативными алгебрами являются стандартно нумерованные финитно аппроксимируемые и конечно порожденные алгебры, позитивные алгебры со счетными (в частности, нетеровыми) решетками конгруэнций и т. д. [12].

Однако, если мы принимаем тезис об отделимости алгоритмических представлений моделей данных в рамках теоретической информатики, то следует рассматривать именно отделимые (а не просто вычислимо отделимые) нумерации.

3.1. Аксиомы отделимости. В этом подразделе рассмотрим некоторые усиления условия отделимости нумерации, которые во многих естественных случаях оказываются достаточными для ее эффективной отделимости и даже негативности. Выше рассматривались отделимые нумерации, которые естественно назвать T_0 -отделимыми. Попытка усиления понятия отделимости приводит к следующему определению.

Определение 54. Нумерация называется T_1 -отделимой (T_2, T_3, T_4 -отделимой), если для всякой пары натуральных чисел, различных по модулю ее нумерационной эквивалентности, найдутся пересечимая окрестность первого числа, не содержащая второе, и пересечимая окрестность второго, не содержащая первое (найдутся непересекающиеся пересечимые окрестности этих чисел; для всякого элемента и замкнутого в эффективно порожденной топологии множества, не содержащего этот элемент, найдутся их непересекающиеся окрестности; для всякой пары непересекающихся замкнутых множеств найдутся их непересекающиеся окрестности).

Обозначим через K_m ($0 \leq m \leq 4$) класс пространств, гомеоморфных эффективно порожденным пространствам, для которых выполняется аксиома T_m -отделимости.

Предложение 55. $K_m \setminus K_{m+1} \neq \emptyset$ для $m \in \{0, 1\}$, $K_3 = K_4$.

Для $m = 0$ тривиальный пример дается связным двоеточием, так как если α – вычислимо перечислимое невычислимое множество, то двухэлементное множество $\{\alpha, \omega \setminus \alpha\}$ с естественной нумерацией, сопоставляющей каждому числу содержащее его множество, есть эффективно порожденное отделимое и не T_1 -отделимое пространство.

Для $m = 1$ в [12] построен пример эффективно порожденного пространства, гомеоморфного счетно-бесконечному пространству Зарисского, поскольку непустыми вполне перечислимыми подмножествами в этом примере являются все коконечные множества, и только они.

Для $m = 3$ вопрос также тривиален, так как в предположении T_1 -отделимости для счетных топологических пространств регулярность и нормальность равносильны.

Для $m = 2$ вопрос открыт.

В случае вычислимо порожденных пространств ситуацию полностью описывает следующее

Предложение 56 ([39]). *Нумерация вычислимо отделима, если и только если вычислимо порожденное топологическое пространство совершенно нормально и вполне несвязно.*

В частности, в этом случае выполняются все аксиомы T_m -отделимости ($m \in \{0, 1, 2, 3, 4\}$).

Определение 57. Нумерация называется эффективно T_1 -отделимой (T_2 -отделимой), если для нее существует вычислимое семейство T_1 -отделяющих (T_2 -отделяющих) множеств.

Для T_1 -отделимых (T_2 -отделимых) нумераций естественно возникает вопрос о справедливости усиленных аналогов теоремы 11: всякая ли T_1 -отделимая (T_2 -отделимая) нумерованная алгебра аппроксимируется эффективно T_1 -отделимыми (T_2 -отделимыми) алгебрами?

Если (A, ν) – нумерованная алгебра и K – класс нумерованных алгебр, однотипных с A , то назовем A простой относительно класса K (K -простой), если никакая ее неединичная фактор-алгебра не принадлежит K . Через K_1 (K_2) обозначим класс эффективно T_1 -отделимых (T_2 -отделимых) нумерованных алгебр. Для алгебр пустой сигнатуры (т.е. нумерованных множеств) верна

Теорема 58 ([21]). *Существует T_1 -отделимое, но не T_2 -отделимое нумерованное множество, никакое фактор-множество которого не является эффективно T_1 -отделимым.*

Следствие 59. *Существует K_1 -простая T_1 -отделимая нумерованная алгебра, эффективно порожденное топологическое пространство которой является пространством Зарисского.*

Простейшими примерами эффективно T_2 -отделимых нумераций являются позитивные и негативные нумерации. Более того, легко заметить, что в этих случаях имеет место равномерная T_2 -отделимость, т.е. существует эффективная процедура, определенная на каждой паре чисел, различных по модулю нумерационной эквивалентности, значением

которой является пара вычислимо перечислимых индексов непересекающихся множеств, замкнутых относительно нумерационной эквивалентности, отделяющих эту пару чисел.

Усиление аксиомы отделимости с T_1 -отделимости до T_2 -отделимости также не дает возможности описать ситуацию с T_2 -отделимо нумерованными универсальными алгебрами в терминах их гомоморфизмов на эффективно T_2 -отделимо нумерованные алгебры. Более того, T_2 -отделимо нумерованные алгебры не аппроксимируются даже эффективно T_1 -отделимо нумерованными алгебрами, как показывает следующее утверждение.

Предложение 60 ([21]). *Существует T_2 -отделимое нумерованное множество с перечислимыми элементами, никакое фактор-множество которого не является эффективно T_1 -отделимым.*

Из конструкции, используемой в доказательстве этого предложения непосредственно вытекает

Следствие 61. *Существует K_1 -простая T_2 -отделимая нумерованная алгебра, эффективно порожденное пространство которой дискретно.*

Теорема 58 и предложение 60 дополнительно подчеркивают фундаментальную роль теоремы Ю.Л. Ершова о вычислимых нумерациях с точки зрения теории нумерованных алгебр, так как для приведенных выше естественных усилений аксиом отделимости теорема об аппроксимации T_1 -отделимых (T_2 -отделимых) алгебр эффективно T_1 -отделимыми (T_2 -отделимыми) неверна. Заметим, что нумерованные множества, существование которых утверждается в теореме 58 и в предложении 60, тривиально аппроксимируются эффективно отделимыми связными двоеточиями.

Отметим, что в некоторых случаях, для известных типов алгебр, существование T_1 -отделимых (T_2 -отделимых) нумераций может являться достаточным условием их негативности (см. [21]).

3.2. ЭФФЕКТИВНО ВЫРОЖДЕННЫЕ НУМЕРАЦИИ. Если η – эквивалентность на ω , то η -замыканием множества α , обозначаемым через $[\alpha]_\eta$, называется пересечение всех η -замкнутых расширений множества α .

Множество называется η -бесконечным (η -конечным), если его η -замыкание состоит из бесконечного (конечного) числа классов η -эквивалентности. Очевидно, что необходимым (но не достаточным) условием η -бесконечности множества является его бесконечность.

Напомним, что под эффективным (вычислимым) топологическим пространством, заданном на нумерованном множестве (A, ν) , мы понимаем топологическое пространство на A , порожденное ν -перечислимыми (ν -вычислимыми) подмножествами множества A . Для сокращения обозначений в данном подразделе $\tau(\nu)$ -топологией будем называть эффективно порожденную топологию на нумерованном множестве (A, ν) , а $\tau(\nu)_{comp}$ -топологией – вычислимо порожденную.

Определение 62. Нумерация ν универсальной алгебры A называется эффективно невырожденной, если эффективно порожденное пространство $\tau(\nu)$ нетривиально (т. е. $\tau(\nu)$ -топология содержит хотя бы один элемент кроме $\emptyset$ и $\omega/\ker(\nu)$).

Нумерацию не являющуюся эффективно невырожденной будем называть эффективно вырожденной. Иначе говоря, эффективная вырожденность нумерации универсальной алгебры равносильна отсутствию нетривиальных перечислимых окрестностей ее элементов.

Предложение 63 ([26]). *Всякая не более чем счетная универсальная алгебра счетной сигнатуры имеет эффективно вырожденную нумерацию.*

Таким образом, эффективно невырожденные нумерованные алгебры образуют достаточно узкий класс (в категории нумерованных алгебр с морфизмами), в рамках которого мы формулируем наши утверждения.

Следствие 64. *Всякая не более чем счетная универсальная алгебра счетной сигнатуры (любой алгоритмической сложности) имеет нумерацию, т. е. представима над некоторой эквивалентностью.*

Для позитивных алгебр вычислимые и перечислимые топологии могут максимально различаться. Например, пусть η – совершенная позитивная эквивалентность (т. е. бесконечная позитивная эквивалентность, которая не имеет собственных η -замкнутых вычислимых подмножеств, см. книгу Ю.Л. Ершова [11]). Тогда η -пространство является дискретным, а η_{comp} -пространство – тривиальным. Оказывается, что в случае негативных алгебр вычислимые и перечислимые топологии совпадают.

Приведем это утверждение в наиболее общей формулировке.

Теорема 65 ([26]). *Если (A, ν) – негативно нумерованное множество, то $\tau(\nu)$ -топология и $\tau(\nu)_{\text{comp}}$ -топология совпадают.*

3.3. ПЕРЕЧИСЛИМЫЕ ТОПОЛОГИИ И ИХ КОМПАКТНЫЕ РАСШИРЕНИЯ. Компактные пространства появляются в теории вычислимости вполне естественным образом. Например, ядро η нумерации, существование которой утверждается в теореме 58 таково, что дополнение всякого η -замкнутого перечислимого непустого множества является η -конечным и потому соответствующее пространство компактно.

Вышесказанное также подтверждает важность и полезность эквивалентностей вида η_α , в особенности для коиммунных α . В приведенных выше примерах принципиально важна финитная аппроксимируемость всех η_α -алгебр, что обеспечивается алгоритмической почти-конечностью иммунных множеств. Это алгоритмическое понятие оказалось равносильным компактности соответствующего вычислимого пространства.

Теорема 66 ([12]). *Для произвольного $\alpha \subseteq \omega$ следующие условия эквивалентны:*

- 1) α коконечно или коиммунно;

- 2) всякая η_α -алгебра финитно аппроксимируема;
- 3) вычислимое η_α -пространство – компакт.

Заметим, что если α вычислимо перечислимо, то перечислимое η_α -пространство компактным не будет. Более того, в этом случае пространство дискретно, т. е. всякое подмножество будет открытым.

Теорема 67 ([40]). *Всякая бесконечная эквивалентность на ω имеет такое бесконечное расширение, эффективное (вычислимое) фактор-пространство по модулю которого является компактным.*

Заметим, что эффективное пространство, являющееся компактным, может и не быть компактом (например, эффективное пространство Зарисского).

Рассмотрим более подробно эффективные топологические пространства над эквивалентностями вида η_α .

По существу, для множества α топология на ω/α является одноточечной компактификацией Александрова, при этом к множеству $\omega \setminus \alpha$ добавляется “точка” α .

Предложение 68 ([41]). *Для любого множества $\alpha \subseteq \omega$ следующие условия равносильны:*

- 1) эффективное η_α -пространство – компакт;
- 2) всякое перечислимое расширение α коконечно.

Следствие 69. *Для любого косжатого множества α следующие условия равносильны:*

- 1) эффективное η_α -пространство – компакт;
- 2) α не является перечислимым.

Предложение 70 ([41]). *Если α максимально, то вычислимое η_α -пространство – компакт, а эффективное η_α -пространство дискретно.*

Теорема 71 ([41]). *Для всякого множества α с бесконечным не гипериммунным дополнением существует такое его расширение $\beta \supseteq \alpha$ также с бесконечным не гипериммунным дополнением, что η_β -пространство есть компакт.*

4. Отделимые представления классических систем

Фундаментальные алгебраические понятия тела и области целостности являются классическими объектами исследования как в алгебре, так и в математической логике, которая, в частности, занимается описанием алгоритмических свойств колец, заданных теми или иными нумерациями (см. [2, 4], там же есть и библиография по теме). Важнейшими среди нумераций (представлений) этих объектов являются вычислимые, т. е. изоморфные кольцам, носителями которых являются вычислимые подмножества множества натуральных чисел, а операции сложения и умножения представлены подходящими вычислимыми операциями.

4.1. ЛОКАЛЬНО ПОЗИТИВНЫЕ И НЕГАТИВНЫЕ ГРУППЫ

Определение 72. Нумерация алгебры называется локально позитивной (негативной), если хотя бы один смежный класс ядра этой нумерации является перечислимым (коперечислимым).

Предложение 73 ([26]). *Для всякой локально позитивной (локально негативной) группы любой смежный класс ее ядра является перечислимым (коперечислимым).*

Предложение 74 ([26]). *Всякая локально позитивная нумерация любой группы является позитивной.*

Следствие 75. *Всякая локально позитивная нумерация любого кольца является позитивной.*

До сих пор, по умолчанию, мы рассматривали группы в сигнатуре с одной бинарной операцией.

Теорема 76 ([26]). *Всякая локально негативная нумерация любой группы в сигнатуре с бинарной групповой и унарной операцией взятия обратного элемента является негативной.*

Автору неизвестен ответ на вопрос: “всякая ли локально негативная группа в сигнатуре с одной бинарной групповой операцией является негативной?”.

Следствие 77. *Всякая локально позитивная нумерация любого тела является вычислимой.*

4.2. НЕГАТИВНОСТЬ ОТДЕЛИМЫХ НУМЕРАЦИЙ ТЕЛ. Под словом “кольцо”, если не оговорено противное, будем понимать ассоциативное кольцо, а под словосочетанием “область целостности” – ассоциативное кольцо (не обязательно коммутативное или с единицей) без делителей нуля.

Так как любое поле является конгруэнц-простой алгеброй (т. е. в нем отсутствуют собственные идеалы), то всякое позитивное представление поля является вычислимым (см. книгу Ю.Л. Ершова [2, с. 299, следствие 1], согласно которому всякая позитивная конгруэнц-простая универсальная алгебра является вычислимой). С другой стороны, всякое бесконечное вычислимо представимое поле обладает негативными невычислимыми представлениями [42]. Из результатов этой работы легко следует, что негативными невычислимыми представлениями обладают и бесконечные области целостности. Простейшим бесконечным полем характеристики нуль является поле рациональных чисел $\langle \mathbb{Q}; +, \times \rangle$, не имеющее не только собственных идеалов, но и собственных подполей. В связи с вышесказанным возникает разумный вопрос о вычислимости естественных позитивных подколец (с единицей, т. е. областей целостности, расширяющих кольцо целых чисел) поля рациональных чисел $\langle \mathbb{Q}; +, \times \rangle$ в любом его вычислимом представлении.

Пусть $\langle \omega; +, \times \rangle$ – вычислимое представление поля рациональных чисел Q , π – произвольное подмножество множества простых чисел $\Pi \subseteq \omega$, $\mathbf{n} = 1 + \dots + 1$ (n раз) и $R(\pi)$ – подкольцо поля Q , порожденное множеством рациональных дробей $\{1/\mathbf{n} \mid \mathbf{n} \in \pi\}$. Ясно, что всякая подобласть целостности R с единицей поля Q имеет вид $R(\pi)$ для подходящего $\pi \subseteq \Pi$, которое будем называть базисом кольца $R(\pi)$.

В качестве демонстрации описания вычислимых подколец поля рациональных чисел приведем без доказательства следующее, почти очевидное, утверждение ([26]), в котором через $Q = \langle \omega; +, \times \rangle$ обозначается вычислимое представление поля рациональных чисел с основным множеством ω .

Предложение 78. *Для произвольного подкольца R с единицей поля Q следующие условия эквивалентны:*

- 1) *всякое позитивное представление кольца R является вычислимым;*
- 2) *базис π кольца R перечислим в $Q = \langle \omega; +, \times \rangle$;*
- 3) *R – вычислимое подкольцо поля $Q = \langle \omega; +, \times \rangle$.*

Замечание. Отметим, что в отличие от полей, все позитивные представления которых вычислимы, позитивные области целостности не обязаны быть вычислимыми.

Теорема 79 ([26]). *Всякая эффективно невырожденная нумерация любого тела является негативной.*

Предложение 80 ([26]). *Всякая локально негативная нумерация любого тела является негативной.*

Доказательство. Непосредственно вытекает из теоремы 79, так как локальная негативность тела обеспечивает эффективную невырожденность соответствующего ему перечислимо порожденного пространства. $\square$

Следствие 81. *Всякая отделимая нумерация любого конечного тела является вычислимой.*

Следствие 82. *Для всякой эффективно невырожденной нумерации любого тела соответствующее перечислимое пространство совершенно нормально и вполне несвязно.*

Как отмечалось выше, если (A, ν) вычислимо отделимая нумерованная конгруэнц-простая универсальная алгебра и $\nu_{\text{отр}}$ -пространство нетривиально, то ν негативна ([12]). Поскольку всякая простая (т. е. без нетривиальных идеалов) коммутативная область целостности является полем (иначе решетка ее идеалов была бы неартиновой), то, по теореме 79, всякое эффективно невырожденное представление простой области целостности негативно. Однако, принципиальный вопрос о негативности эффективно невырожденного представления всякого простого коммутативного кольца (разумеется, с делителями нуля) на настоящий момент открыт.

4.3. ЭФФЕКТИВНАЯ ВЛОЖИМОСТЬ ОБЛАСТИ ЦЕЛОСТНОСТИ В ПОЛЕ. Академиком А.И. Мальцевым в [43] построен знаменитый пример ассоциативного кольца без делителей нуля, не вложимого в тело. Более того, мультипликативная полугруппа построенного им кольца не вложима в группу. Эти результаты стимулировали автора настоящей статьи к изучению вопросов эффективной вложимости колец в поля. Основная часть рассмотренных в текущем подразделе вопросов примыкает именно к этой проблематике.

По-видимому, в литературе по абстрактной вычислимости не уделялось должного внимания тому факту, что процедура вложения коммутативной области целостности в поле своих частных по существу является эффективной.

Идея конструкции поля частных для нумерованной области целостности, так же, как и в классическом случае, заключается в построении отношения эквивалентности (идеала кольца) на множествах пар номеров, вторые члены которых (“знаменатели” формальных дробей) могут принимать в качестве значений все элементы перечислимого множества, являющегося дополнением нулевого элемента исходного кольца. К этой идее апеллирует и введенное выше понятие локальной негативности кольца.

Теорема 83 ([26]). *Для всякой локально негативной области целостности существует негативное представление поля ее частных, в которое она эффективно вложима.*

Следствие 84. *Всякая локально негативная область целостности негативна.*

Следует из эффективной вложимости локально негативной области целостности в локально негативное (а значит, по теореме 79, и негативное) поле.

Следствие 85. *Нумерованная коммутативная область целостности эффективно вложима в эффективно невырожденное поле тогда и только тогда, когда она негативна.*

Предложение 86. *Существует позитивная область целостности, эффективно не вложимая ни в какое эффективно невырожденное поле.*

5. Приложения в теоретической информатике

Продемонстрируем возможности применения понятия отделимо нумерованной универсальной алгебры к решению некоторых вопросов теоретической информатики и расширению класса моделей данных, допускающих эффективные реализации и адекватные логические описания.

5.1. АЛГЕБРАИЧЕСКИЕ СПЕЦИФИКАЦИИ И ИНИЦИАЛЬНЫЕ МОДЕЛИ КВАЗИМНО-ГООБРАЗИЙ. Под структурой данных (или структурой, или системой, или моделью данных) понимается многосортная алгебра конечной сигнатуры, порожденная значениями сигнатурных констант [19, 44–46]. При этом, подразумевается, что структура данных имеет эффективное, в том или ином смысле, алгоритмическое представление [19, 47, 48], в

частности – позитивное [47]. В силу конечной порожденности можно говорить о позитивности структуры данных, если она позитивно представима, имея в виду ее стандартную нумерацию с учетом вычислимой устойчивости [4].

Определение 87. Структура данных называется эквационально специфицируемой, если существует ее обогащение, являющееся свободной системой некоторого конечно-базируемого многообразия.

Очевидно, что всякая эквационально специфицируемая структура данных позитивно представима. Необходимость рассмотрения обогащений обусловлена тем, что важные и простейшие структуры данных (например, просматриваемый стек М. Майстер [49]) не являются эквационально специфицируемыми [50].

В [19] доказано, что всякая вычислимая структура данных эквационально специфицируема. Ясно, что если структура эквационально специфицируема, то она позитивно представима. Верно ли обратное?

Из существования конечно порожденных вычислимо отделимых алгебр с иммунными характеристическими трансверсями (см. следствие 31, а также работу [51]) следует

Теорема 88. *Существует конечно порожденная позитивно представимая алгебра, никакое обогащение которой не является свободной системой ни в каком конечно базируемом многообразии.*

Таким образом, язык тождеств в обогащениях оказывается неполным с точки зрения его выразительных возможностей для адекватного алгебраического описания даже позитивных структур данных.

5.2. УНИВЕРСАЛЬНЫЕ СПЕЦИФИКАЦИИ. В теории спецификаций программ и эффективной реализуемости одним из достаточно утвердившихся тезисов можно считать тезис о позитивной представимости любой модели данных [47]. Семантика таких моделей должна адекватно определяться их синтаксическими описаниями, которые, очевидно, обязаны иметь однозначно определенную интерпретацию и механизмы генерирования фактов о свойствах моделей. Другими словами, языки описания по определению являются логическими. На сегодняшний день наиболее изученным и обладающим достаточно большой областью применимости является язык исчисления предикатов первого порядка и различные его фрагменты. Особенно часто применяемую на практике часть этого языка образуют универсальные хорновские предложения, на которых основаны языки логического программирования [52]. Этот факт связан с двумя обстоятельствами:

- 1) всякое непротиворечивое эффективное множество универсальных хорновских предложений имеет позитивно представимую модель [47, 48, 53];
- 2) семантика этой модели заключена в устройстве инициальной модели данного множества предложений, которая всегда существует и, более того, существует алгоритм извлечения ее эффективной реализации из синтаксического описания [54, 55].

Эти факты являются классическими в математической логике, поэтому определение границ применимости данного языка, вопросы определимости моделей в классах их гомоморфных образов (инициальная семантика – строение свободной системы соответствующего ранга), а также о числе реализаций (эффективных, поскольку ничто другое нельзя считать реализацией в рамках идеологии теоретической информатики) являются основополагающими в этой парадигме программирования, согласно которой алгоритм должен иметь не императивный, а декларативный характер, и решение задачи должно заключаться не в описании конкретных процедур достижения цели, а в формулировке желаемой цели, при предоставлении поиска реализующей процедуры самой машине (универсальному алгоритму), предпринимающей эти попытки, исходя из синтаксического материала, заключенного в описании модели данных.

Спецификацией модели будем называть любое непротиворечивое вычислимо перечислимое множество предложений логики первого порядка, реализующееся в этой модели. Спецификация называется хорновской (универсальной, экзистенциальной, индуктивной и т. д.), если каждое предложение из нее есть предложение хорновское (соответственно универсальное, экзистенциальное, индуктивное и т. д.).

Пусть $(\mathfrak{M}, \mu)$ – позитивная модель, порожденная сигнатурными константами, и Φ – универсальная хорновская спецификация в сигнатуре модели $\mathfrak{M}$, реализующаяся в $\mathfrak{M}$. В работе [53] установлено, что если Φ не реализуется ни в каком позитивном гомоморфном образе модели $(\mathfrak{M}, \mu)$, то μ – вычислимая нумерация. Другими словами, если $(\mathfrak{M}, \mu)$ – позитивная невычислимая модель и Φ – универсальная хорновская спецификация, реализующаяся в $\mathfrak{M}$, то в классе Φ -моделей содержатся собственные позитивные гомоморфные образы модели $(\mathfrak{M}, \mu)$.

Следовательно, никакую позитивную невычислимую модель $\mathfrak{M}$ нельзя выделить в классе ее собственных позитивных гомоморфных образов никакой универсальной хорновской спецификацией, т. е. если Φ – универсальная хорновская спецификация, реализующаяся в $\mathfrak{M}$, то в классе собственных гомоморфных образов этой модели обязательно присутствуют позитивно представимые. Аналогично, никакую невычислимую позитивную модель нельзя выделить в классе ее собственных гомоморфных образов никакой универсальной спецификацией [53].

Сказанное поставило проблему определения тонкой грани между выразительными возможностями языков универсальных хорновских спецификаций и универсальных спецификаций в рамках проблемы универсальной определимости модели в классе ее эффективных гомоморфных образов (проблема номер 13 из списка вопросов в [12]). Иначе говоря, можно ли в принципе выделить позитивную невычислимую модель в классе ее собственных позитивных гомоморфных образов подходящей универсальной спецификацией?

Теорема 89 ([56]). *Существует позитивно представимая модель, не обладающая вычислимыми представлениями, которая выделяется в классе своих собственных позитивно представимых гомоморфных образов подходящей универсальной спецификацией.*

Заметим, что теорему 89 можно усилить.

Следствие 90. *Существует позитивно представимая модель, не обладающая вычислимыми представлениями, которая выделяется в классе своих собственных позитивно представимых гомоморфных образов подходящей бескванторной спецификацией.*

Очевидно, что такая спецификация не может быть хорновской.

Таким образом, язык универсальных спецификаций оказывается существенно богаче языка универсальных хорновских предложений с точки зрения возможности адекватного описания позитивно представимых моделей.

5.2.1. УНИВЕРСАЛЬНЫЕ ХОРНОВСКИЕ СПЕЦИФИКАЦИИ. Выше было отмечено, что никакую невычислимую позитивную алгебру нельзя выделить в классе ее собственных позитивных фактор-алгебр никаким вычислимо перечислимым множеством универсальных хорновских предложений. Аналогично, никакую невычислимую позитивную алгебру нельзя выделить в классе ее собственных фактор-алгебр никаким вычислимо перечислимым множеством универсальных предложений. Оказалось, что универсальная хорновская определимость в классе собственных вычислимых фактор-алгебр не только возможна, но и весьма полезна.

Теорема 91 ([57]). *Всякая невычислимая позитивная алгебра, выделяемая подходящим вычислимо перечислимым множеством Q универсальных хорновских предложений в множестве своих вычислимых фактор-алгебр, имеет континуум Q -конгруэнций (т. е. таких конгруэнций, в факторах по которым реализуется Q).*

Например, подбирая подходящие эффективные системы универсальных хорновских предложений можно показать, что имеет место

Следствие 92. *Пусть (A, ν) – позитивная алгебра, удовлетворяющая хотя бы одному из следующих трех условий:*

- 1) ν не является вычислимо отделимой;
- 2) характеристическая трансверсаль $\text{tr}(\ker(\nu))$ иммунна, но не гипериммунна;
- 3) некоторое конечное обеднение (A, ν) имеет неэффективно бесконечную конечно порожденную подалгебру.

Тогда A имеет континуум конгруэнций.

Покажем, например, истинность п. 1). Если $\nu t \neq \nu n$ и t, n не отделяются никаким ν -замкнутым вычислимым множеством, то обогатим сигнатуру алгебры A двумя константными символами s, d , интерпретируя $s = \nu t, d = \nu n$. Тогда хорновское бескванторное предложение $s \neq d$ истинно в $(\langle A, s, d \rangle, \nu)$, но не реализуется ни в какой вычислимой фактор-алгебре нумерованной алгебры (A, ν) . Применяем теорему 91.

Следствие 93. *Всякая алгебра, обладающая позитивной нумерацией с совершенным ядром имеет континуум конгруэнций.*

Заметим, что из теоремы 91 также следует, что всякая позитивная алгебра со счетной решеткой конгруэнций аппроксимируется вычислимыми алгебрами.

Следствие 94. *Всякая конечно порожденная неэффективно бесконечная позитивная алгебра имеет континуум конгруэнций.*

Отметим, что условие конечной порожденности в следствии 94 существенно: имеются примеры неэффективно бесконечных позитивных алгебр со счетными решетками конгруэнций (даже алгебр с ненулевыми конгруэнциями только конечного индекса, см. теорему 28).

5.3. СПЕЦИФИКАЦИИ НЕГАТИВНО ПРЕДСТАВИМЫХ МОДЕЛЕЙ ДАННЫХ. Негативно представимые системы представляются во многих аспектах не менее важными, чем позитивные и понятие эффективно представимой модели отражает тот факт, что далее мы принимаем тезис о позитивности или негативности любой структуры данных, так как, во-первых, эти представления лежат на самых нижних этажах арифметической иерархии и, во-вторых, они достаточно емкие, чтобы содержать в себе значительную часть структур данных, возникающих на практике. Однако для негативно представимых моделей, в отличие от позитивно представимых, имеются трудности с однозначным определением (с точностью до изоморфизма) стандартной модели спецификации. Напомним, что стандартные модели мы необходимым образом рассматриваем в сигнатурах подходящих обогашений [49, 50].

Определение 95. Структура $\mathcal{M}$ сигнатуры Σ называется универсально (экзистенциально, $\exists\forall$ -, $\forall\exists$ - и т. д.) определимой, если существуют такое ее обогашение $\mathcal{M}^*$ в сигнатуре Σ^* и вычислимо перечислимое множество Φ универсальных (экзистенциальных, $\exists\forall$ -, $\forall\exists$ - и т. д.) предложений сигнатуры Σ^* , что $\mathcal{M}^* \models \Phi$ и для всякой Σ^* -структуры ее подструктура, порожденная константами либо изоморфна $\mathcal{M}^*$, либо не является Φ -структурой.

Отметим, что условие “либо изоморфна $\mathcal{M}^*$, либо не является Φ -структурой” может давать достаточно большой разброс элементарных свойств системы $\mathcal{M}^*$ и порожденной константами не Φ -системы, так как, в случае неизоморфности, они не являются элементарно эквивалентными.

5.3.1. УНИВЕРСАЛЬНАЯ И ЭКЗИСТЕНЦИАЛЬНАЯ ОПРЕДЕЛИМОСТЬ. Следующее утверждение очевидно.

Предложение 96. *Всякая вычислимо представимая структура универсально (экзистенциально) определима.*

Предложение 97 ([58]). *Существует экзистенциально определимая негативно представимая структура, не имеющая позитивных представлений.*

Предложение 98 ([58]). *Существует экзистенциально определимая позитивно представимая структура, не имеющая негативных представлений.*

Предложения 97 и 98 показывают, что в отличие от универсальной определимости невычислимых структур их экзистенциальная определимость возможна.

Теорема 99 ([58]). *Всякая негативно представимая структура экзистенциально определима.*

Известно, что существует такие позитивные алгебры, всякие обогащения которых (относительно данного представления) локально конечны [59], поэтому вопрос выбора позитивного представления алгебры имеет ключевое значение. Для негативных алгебр можно выбирать любую негативную нумерацию и обогатить относительно нее исходную алгебру так, что полученная алгебра будет конечно порожденной и конгруэнц-простой [60].

Автору неизвестен ответ на принципиальный вопрос:

всякая ли позитивно представимая структура экзистенциально определима?

Назовем позитивно (негативно) представимую структуру $\mathfrak{M}$ локально $\exists$ -неопределимой, если всякая конечная совокупность $\exists$ -предложений, реализующаяся в $\mathfrak{M}$, реализуется в некотором собственном гомоморфном образе (соответственно, прообразе) этой структуры.

Предложение 100 ([58]). *Существует позитивно (негативно), но не вычислимо представимая экзистенциально определимая структура, являющаяся локально $\exists$ -неопределимой.*

Заметим, что для систем, конечно порожденных значениями замкнутых термов можно говорить об их позитивности без привязки к конкретному алгоритмическому представлению, так как в этом случае существует единственное, с точностью до вычислимого изоморфизма, позитивное представление. Для негативных представлений это не так [42]. В общем случае для порожденных замкнутыми термами систем существует наименьшее (относительно сводимости классов эквивалентных нумераций) алгоритмическое представление, индуцированное геделевской нумерацией системы, порожденной значениями термов в абсолютно свободной алгебре ранга ноль (см. [2]).

Из предложения 100 и результатов работы [60] о представимости конечно порожденной и конгруэнц-простой алгебры над любой негативной эквивалентностью вытекает

Следствие 101. *Над любой невычислимой негативной эквивалентностью представима конечно порожденная конгруэнц-простая алгебра, не являющаяся универсально определимой.*

5.3.2. КОНЕЧНАЯ $\forall\exists$ -ОПРЕДЕЛИМОСТЬ НЕГАТИВНО ПРЕДСТАВИМЫХ СИСТЕМ. В теоретической информатике особую роль играют конечные спецификации [19, 44] или, говоря обычным математическим языком, формальные выражения (в частности, предложения логики первого порядка), адекватно описывающие специфицируемые понятия.

Пусть $\mathfrak{M}$ – система конечной сигнатуры Σ , порожденная значениями Σ -констант, μ – ее стандартная нумерация (т. е. лежащая в наименьшем классе эквивалентных алгоритмических представлений системы $\mathfrak{M}$ относительно сводимости нумераций или, что равносильно, подтверждающая каждое натуральное число значением подходящего

$T(\Sigma)$ -терма). Удобно считать, что замкнутый терм как синтаксическое выражение является “номером” или “кодом” класса эквивалентных в $\mathfrak{M}$ термов.

Структуру $\mathfrak{M}$ назовем конечно $\forall$ -($\exists$ -, $\exists\forall$ -, $\forall\exists$ - и т.д.) определимой, если соответствующее множество Φ^* из определения 95 в сигнатуре обогащения Σ^* можно выбрать конечным.

Сравнивая универсальную определимость в смысле определения 95 с конечной эквивариантной специфицируемостью [19] следует отметить, что второй метод, основанный на инициальной семантике, позволяет адекватно описывать и некоторые позитивно представимые невычислимы структуры. Но, в этом случае, эквивариантная спецификация реализуется в бесконечном числе собственных позитивных гомоморфных образов специфицируемой структуры. Методы $\forall$ -определимости и конечной $\forall$ -определимости лишены этого недостатка. Однако платой за точное выделение структуры в классе всех сигнатурно порожденных является сужение класса таких структур до вычислимо представимых.

В следующем предложении говоря о вычислимости структуры подразумеваем вычислимость ее стандартной нумерации.

Предложение 102 ([58]). *Для произвольной структуры $\mathfrak{M}$ следующие условия равносильны:*

- 1) μ вычислима;
- 2) $\mathfrak{M}$ является конечно $\forall$ -определимой.

Следствие 103. *Всякая вычислимо представимая система $\mathfrak{M}$ конечной сигнатуры имеет обогащение $\mathfrak{M}^*$, являющееся инициальной системой некоторого конечно-аксиоматизируемого универсального класса, во всех системах которого содержится изоморфная копия $\mathfrak{M}^*$.*

Иначе говоря, в более “синтаксической” терминологии, для всякой вычислимо представимой системы $\mathfrak{M}$ конечной сигнатуры существует обогащение $\mathfrak{M}^*$ и универсальное предложение φ такое, что $\mathfrak{M}^* \models p(\bar{t}) \Leftrightarrow \varphi \vdash p(\bar{t})$ и $\mathfrak{M}^* \models \neg p(\bar{t}) \Leftrightarrow \varphi \vdash \neg p(\bar{t})$, где $p(\bar{t})$ – атомарная формула от набора замкнутых термов $\bar{t}$.

Предложение 104 ([53]). *Если система имеет невычислимое негативное представление, то всякое $\exists\forall$ -предложение, реализующееся в ней, реализуется и в некотором собственном гомоморфном прообразе этой системы.*

Оказалось, что конечная $\forall\exists$ -определимость не обеспечивает вычислимость представления стандартной модели.

Предложение 105 ([58]). *Существует конечно $\forall\exists$ -определимая негативно представимая система, не имеющая позитивных представлений.*

Невычислимы негативные системы, вообще говоря, можно выделять в классе всех их собственных гомоморфных прообразов $\forall\exists$ -предложениями.

Следствие 106. *Существует $\forall\exists$ -предложение без вычислимо представимых моделей, реализующееся в негативно представимой системе.*

Следствие 107. *Существует негативно представимая система, не имеющая вычислимых представлений, в которой реализуется $\forall\exists$ -предложение, не реализующееся ни в каком собственном гомоморфном прообразе этой системы.*

Теорема 108 ([58]). *Всякая негативно представимая система, порожденная сигнатурными константами является конечно $\forall\exists$ -определимой.*

Важно отметить, что в рассматриваемых нами методах описания негативных систем фактически речь идет об обогащениях расширений. Вопрос существования обогащений над исходным носителем системы (т. е. всякая ли негативно представимая система имеет обогащение без новых сортов, являющееся конечно $\forall\exists$ -определимым?) является гораздо более тонким и его решение в настоящее время неизвестно.

5.4. ЛОГИЧЕСКИЕ СПЕЦИФИКАЦИИ ЭФФЕКТИВНО ОТДЕЛИМЫХ МОДЕЛЕЙ ДАННЫХ. С учетом вышесказанного, подчеркивая существенность наличия алгоритмически определяемых отделяющих окрестностей структур данных, заданных своими алгоритмическими представлениями, мы принимаем тезис о наличии эффективно отделимой нумерации любой структуры данных. Одним из обоснований этого направления в теоретической информатике является следующий факт.

Теорема 109 ([61]). *Всякая универсальная алгебра, имеющая эффективно отделимое алгоритмическое представление является $\exists\forall\exists$ -определимой.*

Список литературы

- [1] А.И. Мальцев, *Конструктивные алгебры. I*, УМН **16** (3), 3–60 (1961).
URL: <https://www.mathnet.ru/rus/rm6619>
- [2] Ю.Л. Ершов, *Проблемы разрешимости и конструктивные модели*, Наука, М., 1980.
- [3] Yu.L. Ershov, *Theory of numberings*, in: E.R. Griffor (ed.), *Handbook of computability theory* (Stud. Logic Found. Math., 140), Elsevier, Amsterdam, 1999, 473–503.
DOI: [https://doi.org/10.1016/S0049-237X\(99\)80030-5](https://doi.org/10.1016/S0049-237X(99)80030-5)
- [4] С.С. Гончаров, Ю.Л. Ершов, *Конструктивные модели*, Научная книга, Новосибирск, 1999.
- [5] Н.Г. Хисамиев, *Арифметическая иерархия абелевых групп*, Сиб. матем. журн. **29** (6), 144–159 (1988).
URL: <https://www.mathnet.ru/rus/smj7527>
- [6] С.П. Одинцов, В.Л. Селиванов, *Арифметическая иерархия и идеалы нумерованных булевых алгебр*, Сиб. матем. журн. **30** (6), 140–149 (1989).
URL: <https://www.mathnet.ru/rus/smj4672>

- [7] В.А. Успенский, *О вычислимых операциях*, ДАН СССР **103** (5), 773–776 (1955).
URL: https://archive.org/details/uspensky-1955-dan-103-5-computable-operations/Uspensky_1955_DAN_103_5_Typeset_by_Zolin/mode/2up
- [8] В.А. Успенский, *Системы перечислимых множеств и их нумерации*, ДАН СССР **105** (6), 1155–1158 (1955).
URL: https://archive.org/details/uspensky-1955-dan-105-6-enumerable-sets-numerations/Uspensky_1955_DAN_105_6_Typeset_by_Zolin/mode/2up
- [9] A. Nerode, *General topology and partial recursive functionals*, Summaries Summer Inst. Symbolic Logic **1957**, 247–251 (1960).
- [10] А.И. Мальцев, *К теории вычислимых семейств объектов*, Алгебра и логика **3** (4), 5–31 (1964).
URL: <https://www.mathnet.ru/rus/al1010>
- [11] Ю.Л. Ершов, *Теория нумераций*, Наука, М., 1977.
- [12] Н.Х. КАСЫМОВ, *Рекурсивно отделимые нумерованные алгебры*, УМН **51** (3), 145–176 (1996).
DOI: <https://doi.org/10.4213/rm971>
- [13] А. И. Мальцев, *Позитивные и негативные нумерации*, ДАН СССР **160** (2), 278–280 (1965).
URL: <https://www.mathnet.ru/rus/dan30557>
- [14] А.С. Морозов, *Об одном вопросе Хигмэна*, Алгебра и логика **29** (1), 29–34 (1990).
URL: <https://www.mathnet.ru/rus/al2089>
- [15] W. Baur, *Rekursive Algebren mit Kettenbedingungen*, Z. Math. Logik Grundlag. Math. **20** (1–3), 37–46 (1974).
DOI: <https://doi.org/10.1002/malq.19740200105>
- [16] W. Baur, *Über rekursive Strukturen*, Invent. Math. **23** (2), 89–95 (1974).
DOI: <https://doi.org/10.1007/BF01405162>
- [17] В.А. Успенский, А.Л. Семенов, *Теория алгоритмов: основные открытия и приложения*, Наука, М., 1987.
- [18] J.C.C. McKinsey, *The decision problem for some classes of sentences without quantifiers*, J. Symbol. Logic **8** (3), 61–76 (1943).
DOI: <https://doi.org/10.2307/2268172>
- [19] J.A. Bergstra, J.V. Tucker, *A characterization of computable data types by means of a finite, equational specification method*, Lecture Notes in Comput. Sci. **85**, 76–90 (1980).
DOI: https://doi.org/10.1007/3-540-10003-2_61
- [20] Н.Х. КАСЫМОВ, *О гомоморфизмах на негативные алгебры*, Алгебра и логика **31** (2), 132–144 (1992).
URL: <https://www.mathnet.ru/rus/al2186>

-
- [21] Н.Х. КАСЫМОВ, *О гомоморфизмах на эффективно отделимые алгебры*, Сиб. матем. журн. **57** (1), 47–66 (2016).
DOI: <https://doi.org/10.17377/smzh.2016.57.105>
- [22] Н.Х. КАСЫМОВ, *Об одной двойственной задаче теории конструктивных моделей*, Вычисл. системы **129**, 137–143 (1989).
URL: <https://zbmath.org/1052.03527>
- [23] U. Andrews, S. Lempp, J.S. Miller, K.M. Ng, L.S. Mauro, A. Sorbi, *Universal computably enumerable equivalence relations*, J. Symb. Logic **79** (1), 60–88 (2014).
DOI: <http://doi.org/10.1017/jsl.2013.8>
- [24] U. Andrews, A. Sorbi, *Joins and meets in the structure of ceers*, Computability **8** (3–4), 193–241 (2019).
DOI: <https://doi.org/10.3233/COM-180098>
- [25] U. Andrews, D.F. Belin, L. San Mauro, *On the structure of computable reducibility on equivalence relations of natural numbers*, J. Symb. Logic **88** (3), 1038–1063 (2023).
DOI: <https://doi.org/10.1017/jsl.2022.28>
- [26] Н.Х. КАСЫМОВ, Ф.Н. ИБРАГИМОВ, *Отделимые нумерации тел и эффективная вложимость в них колец*, Сиб. матем. журн. **60** (1), 82–94 (2019).
DOI: <https://doi.org/10.33048/smzh.2019.60.107>
- [27] Н.Х. КАСЫМОВ, А.С. МОРОЗОВ, И.А. ХОДЖАМУРАТОВА, *О T_1 -отделимых нумерациях подпрямых неразложимых алгебр*, Алгебра и логика **60** (4), 400–424 (2021).
DOI: <https://doi.org/10.33048/alglog.2021.60.402>
- [28] Н.Х. КАСЫМОВ, Р.Н. ДАДАЖАНОВ, С.Л. ДЖАВЛИЕВ, *Uniform m -equivalences and numberings of classical systems*, Сиб. электрон. матем. известия **19** (1), 49–65 (2022).
DOI: <http://doi.org/10.33048/semi.2022.19.005>
- [29] Н.Х. КАСЫМОВ, *Нумерованные алгебры с равномерно рекурсивно отделимыми классами*, Сиб. матем. журн. **34** (5), 85–102 (1993).
URL: <https://www.mathnet.ru/rus/smj836>
- [30] Н.Х. КАСЫМОВ, *Позитивные алгебры с конгруэнциями конечного индекса*, Алгебра и логика **30** (3), 293–305 (1991).
URL: <https://www.mathnet.ru/rus/al2151>
- [31] Н.Х. КАСЫМОВ, *Позитивные алгебры с нетеровыми решетками конгруэнций*, Сиб. матем. журн. **33** (2), 181–185 (1992).
URL: <https://www.mathnet.ru/rus/smj3208>
- [32] Н.Х. КАСЫМОВ, *Позитивные алгебры со счетными решетками конгруэнций*, Алгебра и логика **31** (1), 21–37 (1992).
URL: <https://www.mathnet.ru/rus/al2179>

- [33] Р.Н. Дадажанов, Н.Х. Касымов, И.А. Ходжамуратова, *Равномерно вычислимо отдельные алгебры с эффективно расщепляемыми семействами негативных конгруэнций*, Сиб. матем. журн. **63** (3), 562–575 (2022).
DOI: <https://doi.org/10.33048/smzh.2022.63.307>
- [34] C.G. Jockusch, *Semirecursive sets and positive reducibility*, Trans. Amer. Math. Soc. **131** (2), 420–436 (1968).
DOI: <https://doi.org/10.2307/1994957>
- [35] C.G. Jockusch, J.C. Owings, *Weakly semirecursive sets*, J. Symb. Logic **55** (2), 637–644 (1990).
DOI: <https://doi.org/10.2307/2274653>
- [36] Н.Х. Касымов, А.С. Морозов, *Нижние полурешетки отдельных конгруэнций нумерованных алгебр*, Сиб. матем. журн. **64** (4), 753–769 (2023).
DOI: <https://doi.org/10.33048/smzh.2023.64.408>
- [37] Н.Х. Касымов, *Вычислимо отдельные нумерации локально финитно отдельных алгебр*, Сиб. электрон. матем. изв. **21** (1), 315–346 (2024).
DOI: <https://doi.org/10.33048/semi.2024.21.024>
- [38] Н.Х. Касымов, *Локально конечные и финитно аппроксимируемые уноиды над вычислимо отдельными эквивалентностями*, Математика и теоретические компьютерные науки **2** (1), 55–74 (2024).
DOI: <https://doi.org/10.26907/2949-3919.2024.1.55-73>
- [39] Н.Х. Касымов, *Аксиомы отдельности и разбиения натурального ряда*, Сиб. матем. журн. **34** (3), 81–85 (1993).
URL: <https://www.mathnet.ru/rus/smjl654>
- [40] Н.Х. Касымов, И.А. Ходжамуратова, *Топологические пространства над алгоритмическими представлениями универсальных алгебр*, Итоги науки и техн. Соврем. мат. и ее прил. Темат. обз. **144**, 17–29 (2018).
URL: <https://www.mathnet.ru/rus/into268>
- [41] R.N. Dadazhanov, N.R. Karimova, N.Kh. Kasymov, *Effective compacts over co-immune sets*, Uzbek Math. J. **63** (3), 26–32 (2019).
DOI: <https://doi.org/10.29229/uzmj.2019-3-3>
- [42] B. Khoussainov, T. Slaman, P. Semukhin, $\prod_1^0$ -Presentations of Algebras, Arch. Math. Logic **45** (6), 769–781 (2006).
DOI: <https://doi.org/10.1007/s00153-006-0013-3>
- [43] A.I. Malcev, *On the immersion of an algebraic ring into a field*, Math. Ann. **113** (1), 686–691 (1937).
URL: <https://doi.org/10.1007/BF01571659>

-
- [44] S. Kamin, *Some definitions for algebraic data type specifications*, SIGPLAN Notes **14** (3), 28–37 (1979).
DOI: <https://doi.org/10.1145/988071.988075>
- [45] J.A. Goguen, J. Meseguer, *Completeness of many-sorted equational logic*, Houston J. Math. **11** (3), 307–334 (1985).
- [46] M. Broy, W. Dosch, H. Partsch, P. Pepper, M. Wirsing, *Existential quantifiers in abstract data types*, Lect. Notes in Comp. Sci. **71**, 73–87, (1979).
DOI: https://doi.org/10.1007/3-540-09510-1_7
- [47] С.С. Гончаров, *Модели данных и языки их описаний*, Вычисл. системы **107**, 52–70, (1985).
URL: <https://zbmath.org/0621.68020>
- [48] Н.Х. Касымов, А.С. Морозов, *Логические аспекты теории абстрактных типов данных*, Вычисл. системы **122**, 73–96 (1987).
URL: <https://zbmath.org/0712.68067>
- [49] M. Majster, *Data types, abstract data types and their specification problem*, Theor. Comp. Sci. **8** (1), 89–127 (1979).
DOI: [https://doi.org/10.1016/0304-3975\(79\)90059-8](https://doi.org/10.1016/0304-3975(79)90059-8)
- [50] D. Kapur, *Specifications of Majster’s traversable stack and Veloso’s traversable stack*, SIGPLAN Notes **14** (5), 46–53 (1979).
DOI: <https://doi.org/10.1145/988090.988096>
- [51] Н.Х. Касымов, *Об алгебрах с финитно аппроксимируемыми позитивно представляемыми обогащениями*, Алгебра и логика **26** (6), 715–730 (1987).
URL: <https://www.mathnet.ru/rus/al1999>
- [52] J.W. Lloyd, *Foundations of logic programming*, Springer-Verlag, Berlin, 1987.
DOI: <https://doi.org/10.1007/978-3-642-83189-8>
- [53] Н. Х. Касымов, *Позитивные модели и универсальные предложения*, Вычисл. системы **133**, 3–13 (1990).
URL: <https://zbmath.org/?q=an:0752.03016>
- [54] А.И. Мальцев, *Алгебраические системы*, Наука, М., 1970.
- [55] А.И. Мальцев, *Алгоритмы и рекурсивные функции*, Наука, М., 1986.
- [56] Н.Х. Касымов, Ф.Н. Ибрагимов, *Вычислимо отделимые модели*, СМФН **64** (4), 682–705 (2018).
DOI: <https://doi.org/10.22363/2413-3639-2018-64-4-682-705>
- [57] Н.Х. Касымов, *О числе Q -конгруэнций позитивных алгебр*, Алгебра и логика **31** (3), 297–305 (1992).
URL: <https://www.mathnet.ru/rus/al2194>

- [58] N. Kasymov, N. Karimova, B. Khoussainov, *Defining algorithmically presented structures in first-order logic*, Proceedings of the 39th Annual ACM/IEEE Symposium on Logic in Computer Science, 1–13, art. No. 47 (2024).
DOI: <https://doi.org/10.1145/3661814.3662120>
- [59] Н.Х. КАСЫМОВ, Б.М. ХУСАИНОВ, *Конечно порожденные перечислимые и абсолютно локально конечные алгебры*, Вычисл. системы **116**, 3–15 (1986).
URL: <http://old.math.nsc.ru/journals/vs/vs-cont1.html>
- [60] Н.Х. КАСЫМОВ, *Об алгебрах над негативными эквивалентностями*, Алгебра и логика **33** (1), 76–80 (1994).
URL: <https://www.mathnet.ru/rus/al2257>
- [61] Н.Х. КАСЫМОВ, *Логические спецификации эффективно отделимых моделей данных*, Изв. вузов. Матем. (6), 15–26 (2024).
DOI: <https://doi.org/10.26907/0021-3446-2024-6-15-26>

Надимулла Хабибуллаевич Касымов

Национальный университет Узбекистана им. Мирзо Улугбека,
ул. Университетская, д. 4, г. Ташкент, 100174, Республика Узбекистан,
e-mail: nadim59@mail.ru

Separable numberings of universal algebras

N.Kh. Kasymov

Abstract. The review outlines the foundations of the theory of separable numberings of universal algebras.

Keywords: separable numbered algebra, effectively separable numbering, negative and effectively separable approximability, translationally complete and pre-complete algebra, topological numbered algebra, subdirect indecomposability, Artinian congruence lattice, algebraic and logical data structure specifications.

DOI: 10.26907/2949-3919.2024.4.66-102

References

- [1] A.I. Malt'sev, *Constructive algebras*. I, Russian Math. Surveys, **16** (3), 77–129 (1961). DOI: <https://doi.org/10.1070/rm1961v016n03abeh001120>
- [2] Yu.L. Ershov, *Decidability problems and constructive models*, Nauka, M., 1980 [in Russian].
- [3] Yu.L. Ershov, *Theory of numberings*, in: E.R. Griffor (ed.), Handbook of computability theory (Stud. Logic Found. Math., 140), Elsevier, Amsterdam, 1999, 473–503. DOI: [https://doi.org/10.1016/S0049-237X\(99\)80030-5](https://doi.org/10.1016/S0049-237X(99)80030-5)
- [4] S.S. Goncharov, Yu.L. Ershov, *Constructive Models*, Siberian School of Algebra and Logic. Consultants Bureau, New York, 2000.
- [5] N.G. Khisamiev, *Arithmetic hierarchy of abelian groups*, Siberian Math. J. **29** (6), 987–999 (1988). DOI: <https://doi.org/10.1007/BF00972425>
- [6] S.P. Odintsov, V.L. Selivanov, *Arithmetic hierarchy and ideals of enumerated Boolean algebras*, Siberian Math. J. **30** (6), 952–960 (1989). DOI: <https://doi.org/10.1007/BF00970918>
- [7] V.A. Uspenskii, *On computable operations*, Dokl. AN SSSR **103** (5), 773–776 (1955) [in Russian]. URL: https://archive.org/details/uspensky-1955-dan-103-5-computable-operations/Uspensky_1955_DAN_103_5_TypeSet_by_Zolin/mode/2up

Acknowledgements. The work is performed under the development program of Volga Region Mathematical Center (agreement no. 075-02-2024-1438).

- [8] V.A. Uspenskii, *Systems of denumerable sets and their enumeration*, Dokl. AN SSSR **105** (6), 1155–1158 (1955) [in Russian].
URL: https://archive.org/details/uspensky-1955-dan-105-6-enumerable-sets-numerations/Uspensky_1955_DAN_105_6_Typeset_by_Zolin/mode/2up
- [9] A. Nerode, *General topology and partial recursive functionals*, Summaries Summer Inst. Symbolic Logic **1957**, 247–251 (1960).
- [10] A.I. Mal'tsev, *On the theory of computable families of objects*, Algebra Logic **3** (4), 5–31 (1964) [in Russian].
URL: <https://www.mathnet.ru/rus/al1010>
- [11] Yu.L. Ershov, *Theory of numberings*, Nauka, M., 1977 [in Russian].
- [12] N.Kh. Kasymov, *Recursively separable enumerated algebras*, Russian Math. Surveys **51** (3), 509–538 (1996).
DOI: <https://doi.org/10.1070/RM1996v051n03ABEH002913>
- [13] A.I. Mal'tsev, *Positive and negative enumerations*, Dokl. AN SSSR **160** (2), 278–280 (1965) [in Russian].
URL: <https://www.mathnet.ru/rus/dan30557>
- [14] A. S. Morozov, *A question of Higman*, Algebra Logic **29** (1), 22–26 (1990).
DOI: <https://doi.org/10.1007/BF01980217>
- [15] W. Baur, *Rekursive Algebren mit Kettenbedingungen*, Z. Math. Logik Grundlag. Math. **20** (1–3), 37–46 (1974).
DOI: <https://doi.org/10.1002/malq.19740200105>
- [16] W. Baur, *Über rekursive Strukturen*, Invent. Math. **23** (2), 89–95 (1974).
DOI: <https://doi.org/10.1007/BF01405162>
- [17] V.A. Uspenskii, A.L. Semenov, *Algorithm theory: key discoveries and applications*, Nauka, M., 1987 [in Russian].
- [18] J.C.C. McKinsey, *The decision problem for some classes of sentences without quantifiers*, J. Symbol. Logic **8** (3), 61–76 (1943).
DOI: <https://doi.org/10.2307/2268172>
- [19] J.A. Bergstra, J.V. Tucker, *A characterization of computable data types by means of a finite, equational specification method*, Lecture Notes in Comput. Sci. **85**, 76–90 (1980).
DOI: https://doi.org/10.1007/3-540-10003-2_61
- [20] N.Kh. Kasymov, *Homomorphisms onto negative algebras*, Algebra Logic **31** (2), 81–89 (1992).
DOI: <https://doi.org/10.1007/BF02259847>
- [21] N.Kh. Kasymov, *Homomorphisms onto effectively separable algebras*, Siberian Math. J. **57** (1), 36–50 (2016).
DOI: <https://doi.org/10.1134/S0037446616010055>

-
- [22] N.Kh. Kasymov, *A dual problem in the theory of constructive models*, Vychisl. Sist. **129**, 137–143 (1989) [in Russian].
URL: <https://zbmath.org/1052.03527>
- [23] U. Andrews, S. Lempp, J.S. Miller, K.M. Ng, L.S. Mauro, A. Sorbi, *Universal computably enumerable equivalence relations*, J. Symb. Logic **79** (1), 60–88 (2014).
DOI: <http://doi.org/10.1017/jsl.2013.8>
- [24] U. Andrews, A. Sorbi, *Joins and meets in the structure of ceers*, Computability **8** (3–4), 193–241 (2019).
DOI: <https://doi.org/10.3233/COM-180098>
- [25] U. Andrews, D.F. Belin, L. San Mauro, *On the structure of computable reducibility on equivalence relations of natural numbers*, J. Symb. Logic **88** (3), 1038–1063 (2023).
DOI: <https://doi.org/10.1017/jsl.2022.28>
- [26] N.Kh. Kasymov, F.N. Ibragimov, *Separable enumerations of division rings and effective embeddability of rings therein*, Siberian Math. J. **60** (1), 62–70 (2019).
DOI: <https://doi.org/10.1134/S0037446619010075>
- [27] N.Kh. Kasymov, A.S. Morozov, I.A. Khodzhamuratova, *T_1 -separable numberings of subdirectly indecomposable algebras*, Algebra Logic **60** (4), 263–278 (2021).
DOI: <https://doi.org/10.1007/s10469-021-09651-x>
- [28] N.Kh. Kasymov, R.N. Dadazhanov, S.K. Zhavliev, *Uniform m -equivalences and numberings of classical systems*, Sib. Electron. Math. Rep. **19** (1), 49–65 (2022).
DOI: <http://doi.org/10.33048/semi.2022.19.005>
- [29] N.Kh. Kasymov, *Enumerated algebras with uniformly recursive-separable classes*, Siberian Math. J. **34** (5), 869–882 (1993).
DOI: <https://doi.org/10.1007/BF00971403>
- [30] N.Kh. Kasymov, *Positive algebras with congruences of finite index*, Algebra Logic **30** (6), 190–199 (1991).
DOI: <https://doi.org/10.1007/BF01978852>
- [31] N.Kh. Kasymov, *Positive algebras with nonetherian congruence lattices*, Siberian Math. J. **33** (2), 338–341 (1992).
DOI: <https://doi.org/10.1007/BF00971109>
- [32] N.Kh. Kasymov, *Positive algebras with countable congruence lattices*, Algebra Logic **31** (1), 12–23 (1992).
DOI: <https://doi.org/10.1007/BF02259854>
- [33] R.N. Dadazhanov, N.Kh. Kasymov, I.A. Khodzhamuratova, *Uniformly computably separable algebras with effectively splittable families of negative congruences*, Siberian Math. J. **63** (3), 466–475 (2022).
DOI: <https://doi.org/10.1134/S0037446622030077>

- [34] C.G. Jockusch, *Semirecursive sets and positive reducibility*, Trans. Amer. Math. Soc. **131** (2), 420–436 (1968).
DOI: <https://doi.org/10.2307/1994957>
- [35] C.G. Jockusch, J.C. Owings, *Weakly semirecursive sets*, J. Symb. Logic **55** (2), 637–644 (1990).
DOI: <https://doi.org/10.2307/2274653>
- [36] N.Kh. Kasymov, A.S. Morozov, *Lower semilattices of separable congruences of numbered algebras*, Siberian Math. J. **64** (4), 864–876 (2023).
DOI: <https://doi.org/10.1134/S0037446623040080>
- [37] N.Kh. Kasymov, *Computably separable numberings of locally finite separable algebras*, Sib. Electron. Math. Rep. **21** (1), 315–346 (2024) [in Russian].
DOI: <https://doi.org/10.33048/semi.2024.21.024>
- [38] N.Kh. Kasymov, *Locally finite and residually finite unoids over computably separable equivalences*, MTCS **2** (1), 55–74 (2024) [in Russian].
DOI: <https://doi.org/10.26907/2949-3919.2024.1.55-73>
- [39] N.Kh. Kasymov, *Separation axioms and partitions of the set of natural numbers*, Siberian Math. J. **34** (3), 468–471 (1993).
DOI: <https://doi.org/10.1007/BF00971221>
- [40] N.Kh. Kasymov, I.A. Khodzhamuratova, *Topological spaces over algorithmic representations of universal algebras*, J. Math. Sci. **245** (3), 311–322 (2020).
DOI: <https://doi.org/10.1007/s10958-020-04692-6>
- [41] R.N. Dadazhanov, N.R. Karimova, N.Kh. Kasymov, *Effective compacts over co-immune sets*, Uzbek Math. J. **63** (3), 26–32 (2019).
DOI: <https://doi.org/10.29229/uzmj.2019-3-3>
- [42] B. Khoussainov, T. Slaman, P. Semukhin, $\prod_1^0$ -Presentations of Algebras, Arch. Math. Logic **45** (6), 769–781 (2006).
DOI: <https://doi.org/10.1007/s00153-006-0013-3>
- [43] A.I. Malcev, *On the immersion of an algebraic ring into a field*, Math. Ann. **113** (1), 686–691 (1937).
URL: <https://doi.org/10.1007/BF01571659>
- [44] S. Kamin, *Some definitions for algebraic data type specifications*, SIGPLAN Notes **14** (3), 28–37 (1979).
DOI: <https://doi.org/10.1145/988071.988075>
- [45] J.A. Goguen, J. Meseguer, *Completeness of many-sorted equational logic*, Houston J. Math. **11** (3), 307–334 (1985).
- [46] M. Broy, W. Dosch, H. Partsch, P. Pepper, M. Wirsing, *Existential quantifiers in abstract data types*, Lect. Notes in Comp. Sci. **71**, 73–87, (1979).
DOI: https://doi.org/10.1007/3-540-09510-1_7

-
- [47] S.S. Goncharov, *Data models and languages for their description*, Trans. Amer. Math. Soc. **143**, 139–152 (1989).
- [48] N.Kh. Kasymov, A.S. Morozov, *Logical aspects of the theory of abstract data types*, Vychisl. Sist. **122**, 73–96 (1987) [in Russian].
URL: <https://zbmath.org/0712.68067>
- [49] M. Majster, *Data types, abstract data types and their specification problem*, Theor. Comp. Sci. **8** (1), 89–127 (1979).
DOI: [https://doi.org/10.1016/0304-3975\(79\)90059-8](https://doi.org/10.1016/0304-3975(79)90059-8)
- [50] D. Kapur, *Specifications of Majster's traversable stack and Veloso's traversable stack*, SIGPLAN Notes **14** (5), 46–53 (1979).
DOI: <https://doi.org/10.1145/988090.988096>
- [51] N.Kh. Kasymov, *Algebras with finitely approximable positively representable enrichments*, Algebra Logic **26** (6), 441–450 (1987).
DOI: <https://doi.org/10.1007/BF01988315>
- [52] J.W. Lloyd, *Foundations of logic programming*, Springer-Verlag, Berlin, 1987.
DOI: <https://doi.org/10.1007/978-3-642-83189-8>
- [53] N.Kh. Kasymov, *Positive models and universal propositions*, Vychisl. Sist. **133**, 3–13 (1990) [in Russian].
URL: <https://zbmath.org/?q=an:0752.03016>
- [54] A.I. Mal'cev, *Algebraic Systems*, Springer-Verlag, New York–Heidelberg, 1973.
DOI: <https://doi.org/10.1007/978-3-642-65374-2>
- [55] A.I. Mal'cev, *Algorithms and recursive functions*, Wolters-Noordhoff Publishing, Groningen, 1970.
- [56] N.Kh. Kasymov, F.N. Ibragimov, *Computably separable models*, J. Math. Sci. **264** (6), 746–767 (2022).
DOI: <https://doi.org/10.1007/s10958-022-06033-1>
- [57] N.Kh. Kasymov, *The number of Q -congruences in positive algebras*, Algebra Logic **31** (3), 182–187 (1992).
DOI: <https://doi.org/10.1007/BF02259947>
- [58] N. Kasymov, N. Karimova, B. Khoussainov, *Defining algorithmically presented structures in first-order logic*, Proceedings of the 39th Annual ACM/IEEE Symposium on Logic in Computer Science, 1–13, art. No. 47 (2024).
DOI: <https://doi.org/10.1145/3661814.3662120>
- [59] N.Kh. Kasymov, B.M. Khoussainov, *Finitely generated enumerable and absolutely locally finite algebras*, Vychisl. Sist. **116**, 3–15 (1986) [in Russian].
URL: <https://zbmath.org/0646.03042>

- [60] N.Kh. Kasymov, *Algebras over negative equivalences*, Algebra Logic **33** (1), 46–48 (1994).
DOI: <https://doi.org/10.1007/BF00739416>
- [61] N.Kh. Kasymov, *Logical specifications of effectively separable data models*, Russ. Math. **68** (6), 11–20 (2024).
DOI: <https://doi.org/10.3103/S1066369X24700397>

Nadimulla Khabibullaevich Kasymov

National University of Uzbekistan,

4 Universitetskaya str., Tashkent 100174, Republic of Uzbekistan,

e-mail: nadim59@mail.ru

Относительно элементарная определимость класса универсальных частичных графовых полуавтоматов в классе полугрупп

В.А. Молчанов, Р.А. Фарахутдинов

Аннотация. Работа посвящена алгебраической теории структуризованных автоматов. Рассматриваются полугрупповые автоматы без выходных сигналов над графами, которые называются графовыми полуавтоматами. Изучаются частичные графовые полуавтоматы, каждый входной сигнал которых является частичным эндоморфизмом графа состояний. В категории частичных графовых полуавтоматов над графом $G = (X, \rho)$ особое внимание уделяется полуавтомату $\text{PAtm}(G) = (G, \text{PEnd}(G), \star)$ с полугруппой $\text{PEnd}(G)$ всех частичных эндоморфизмов графа G , так как он является универсально притягивающим объектом в данной категории и называется универсальным частичным графовым полуавтоматом. Основным результатом работы состоит в доказательстве относительно элементарной определимости класса универсальных частичных графовых полуавтоматов над нетривиальными рефлексивными графами в классе полугрупп и ее приложений.

Ключевые слова: полуавтомат, граф, частичный эндоморфизм, относительно элементарная определимость.

DOI: 10.26907/2949-3919.2024.4.103-123

Введение

Особое место в алгебраической теории автоматов занимает исследование автоматов в категориях [1], т. е. автоматов, основные множества которых наделены дополнительными математическими структурами из категории $\mathbf{K}$, а функции переходов и выходов являются морфизмами этой категории. В настоящей работе исследуются полугрупповые автоматы без выходных сигналов в категории графов – графовые полуавтоматы [2], у которых множество состояний наделено структурой графа, сохраняющегося функциями переходов полуавтомата.

При исследовании таких математических объектов естественно возникает интерес к их изучению с помощью производных алгебраических систем, связанных специальным образом с исходными объектами. Это направление имеет непосредственное отношение к проблеме С. Улама [3] характеристики математических объектов с помощью алгебр эндоморфизмов и автоморфизмов. Принципиальный вопрос состоит в том, как точно производная

алгебраическая система определяет исходный объект. Для решения этого вопроса проводятся исследования, которые позволяют оценить взаимосвязь исходного объекта с производной алгебраической системой. В частности, для групп автоморфизмов алгебраических систем, полугрупп эндоморфизмов графов, колец эндоморфизмов модулей подобные исследования проводились Б.И. Плоткиным [4], А.Г. Пинусом [5, 6], Ю.М. Важениным [7, 8], Л.М. Глускиным [9, 10], А.В. Михалёвым [11] и другими.

Хорошо известно [12], что эффективным способом решения проблем элементарной классификации исходных объектов с помощью теорий первого порядка производных алгебраических систем и проблем разрешимости теорий первого порядка производных алгебраических систем является метод относительно элементарной определимости одного класса моделей $\mathbf{K}$ в другом классе моделей $\mathbf{K}_1$, суть которого заключается в построении изоморфной копии исходной модели $A \in \mathbf{K}$ в ее производной алгебраической системе $S(A) \in \mathbf{K}_1$ с помощью средств узкого исчисления предикатов (УИП) сигнатуры класса $\mathbf{K}_1$ и некоторых фиксированных элементов модели $S(A)$.

В работе [13] доказана относительно элементарная определимость класса универсальных графовых полуавтоматов над нетривиальными квазибесконтурными рефлексивными графами в классе полугрупп. Настоящая работа продолжает исследование графовых полуавтоматов. Здесь рассматриваются частичные графовые полуавтоматы, т. е. такие полуавтоматы, у которых входные сигналы являются частичными эндоморфизмами графа состояний. Для класса универсальных частичных графовых полуавтоматов над нетривиальными рефлексивными графами решается вопрос его относительно элементарной определимости в классе полугрупп. Приводятся приложения этого результата к исследованию взаимосвязи свойств таких полуавтоматов и их полугрупп входных сигналов.

1. Основные понятия и определения

В работе используется общепринятая терминология теории алгебраических систем из [14], теории графов из [15], теории полугрупп из [16] и теории автоматов из [1].

Далее всюду под графом будем понимать ориентированный граф. Граф $G = (X, \rho)$ называется рефлексивным, если у каждой его вершины есть петля, т. е. для любого $x \in X$ выполняется условие $(x, x) \in \rho$. Граф $G = (X, \rho)$ называется симметричным, если для любых вершин $x, y \in X$ из условия $(x, y) \in \rho$ следует $(y, x) \in \rho$, т. е. у каждой дуги есть встречная дуга (петли встречны сами себе). Граф $\tilde{G} = (X, \rho^{-1})$ называется двойственным графом для графа $G = (X, \rho)$. Граф $G = (X, \rho)$ называется тривиальным, если $\rho = \emptyset$, или $\rho = \Delta_X$, или $\rho = X \times X$. Дугу графа будем называть собственной, если у нее нет встречной дуги.

Следуя [17], под частичным преобразованием множества X понимается однозначное бинарное отношение $f \subset X \times X$ с областью определения $\text{dom } f$ и множеством значений $\text{Im } f$. Частичное преобразование f множества X называется частичным эндоморфизмом графа $G = (X, \rho)$, если для любых $x, y \in \text{dom } f$ из $(x, y) \in \rho$ следует $(f(x), f(y)) \in \rho$.

Множество всех частичных эндоморфизмов графа G с композицией образуют полугруппу $\text{PEnd}(G)$, которая называется полугруппой частичных эндоморфизмов графа G .

В работе под частичным полуавтоматом понимается алгебраическая система $A = (X, S, \star)$, состоящая из непустого множества состояний X , полугруппы входных сигналов $S = (S, \cdot)$ и частичной функции переходов $\star : X \times S \rightarrow X$, согласованной с операцией умножения полугруппы по правилу $x \star (s_1 \cdot s_2) = (x \star s_1) \star s_2$ для любых $x \in X$, $s_1, s_2 \in S$, удовлетворяющих условию $(x, s_1), (x \star s_1, s_2), (x, s_1 \cdot s_2) \in \text{dom } \star$. Для каждого входного сигнала $s \in S$ частичного полуавтомата определена частичная функция переходов $\delta_s(x) = x \star s$, где $(x, s) \in \text{dom } \star$.

Далее рассматриваются полуавтоматы $A = (X, S, \star)$ без равнодействующих входных сигналов, в которых разные входные сигналы $s_1, s_2 \in S$ определяют разные функции переходов $\delta_{s_1} \neq \delta_{s_2}$. Для таких полуавтоматов входные сигналы можно отождествлять с определяемыми ими функциями переходов и полугруппу входных сигналов S рассматривать как полугруппу частичных преобразований множества состояний X . Полугруппа входных сигналов полуавтомата A обозначается символом $\text{Inp}(A)$.

Частичный полуавтомат $A = (X, S, \star)$ называется графовым, если множество его состояний X наделено такой структурой графа $G = (X, \rho)$, что для любого входного сигнала $s \in S$ частичная функция переходов δ_s является частичным эндоморфизмом графа G . Символически такие полуавтоматы обозначаются $A = (G, S, \star)$. Для графового полуавтомата $A = (G, S, \star)$ полуавтомат $\tilde{A} = (\tilde{G}, S, \star)$ называется двойственным полуавтоматом.

Согласно [1] частичный графовый полуавтомат $\text{PAtm}(G) = (G, \text{PEnd}(G), \star)$ с полугруппой входных сигналов $\text{PEnd}(G)$ и функцией переходов $x \star s = s(x)$ (здесь $x \in X$, $s \in S$ и $(x, s) \in \text{dom } \star$) является универсально притягивающим объектом в категории частичных графовых полуавтоматов над графом G и называется универсальным частичным графовым полуавтоматом.

Изоморфизмом графового полуавтомата $A_1 = (G_1, S_1, \star_1)$ над графом $G_1 = (X_1, \rho_1)$ на графовый полуавтомат $A_2 = (G_2, S_2, \star_2)$ над графом $G_2 = (X_2, \rho_2)$ называется пара отображений $\gamma = (f, g)$, где $f : G_1 \rightarrow G_2$ – изоморфизм графа G_1 на граф G_2 , $g : S_1 \rightarrow S_2$ – изоморфизм полугруппы S_1 на полугруппу S_2 , и для любых $x \in X$, $s \in S$ выполняются условия $f(x \star_1 s) = f(x) \star_2 g(s)$.

2. Относительно элементарная определимость

Введем следующие формулы языка элементарной теории полугрупп $\mathbf{L}_S$:

$$\begin{aligned} I(x) &= (x \neq 0 \wedge x \cdot x = x), \\ J(x) &= (I(x) \wedge (\forall y)(I(y) \wedge x \cdot y = y \Rightarrow y \cdot x = x)), \\ M(x) &= (J(x) \wedge (\forall y)(J(y) \wedge y \cdot x \neq 0 \Rightarrow y \cdot x = y)). \end{aligned}$$

Лемма 1. Для полугруппы $\text{PEnd}(G)$ частичных эндоморфизмов графа $G = (X, \rho)$ спра-

ведливы следующие утверждения:

- 1) для элемента $\varphi \in \text{PEnd}(G)$ выполнимость условия $J(\varphi)$ равносильна тому, что φ является непустым идемпотентным частичным эндоморфизмом графа G с одноэлементным множеством значений $\text{Im } \varphi = \{a\}$ для некоторого $a \in X$;
- 2) для элемента $\varphi \in \text{PEnd}(G)$ выполнимость условия $M(\varphi)$ равносильна тому, что φ является частичным одноэлементным тождественным эндоморфизмом графа G вида $\varphi = \begin{pmatrix} a \\ a \end{pmatrix}$ для некоторого $a \in X$.

Доказательство. Пусть частичный эндоморфизм $\varphi \in \text{PEnd}(G)$ удовлетворяет условию $J(\varphi)$. Тогда φ есть идемпотентный частичный эндоморфизм графа G с множеством значений $\text{Im } \varphi$, для которого $|\text{Im } \varphi| > 0$. Следовательно, $\text{Im } \varphi \subset \text{dom } \varphi$ и $\varphi \upharpoonright \text{Im } \varphi = \Delta_{\text{Im } \varphi}$. Для вершины $x \in \text{Im } \varphi$ выполняется $x \in \varphi^{-1}(x)$, и частичное преобразование $\psi = \begin{pmatrix} \varphi^{-1}(x) \\ x \end{pmatrix}$ является ненулевым идемпотентным частичным эндоморфизмом графа G , для которого выполняется равенство $\varphi\psi = \psi\varphi = \psi$. Так как полугруппа $\text{PEnd}(G)$ содержит все частичные тождественные эндоморфизмы графа G , в том числе $\Delta_{\varphi^{-1}(x)}$, то композиция $\psi = \Delta_{\varphi^{-1}(x)} \varphi$ тоже принадлежит полугруппе $\text{PEnd}(G)$. Тогда из условия $J(\varphi)$ следует равенство $\psi\varphi = \varphi$. Значит, $\varphi = \psi$ есть частичный эндоморфизм графа G с одноэлементным множеством значений $\text{Im } \varphi = \{x\}$.

Обратно, пусть частичный эндоморфизм $\varphi \in \text{PEnd}(G)$ имеет вид $\varphi = \begin{pmatrix} \varphi^{-1}(x) \\ x \end{pmatrix}$ для некоторого $x \in X$, и ненулевым идемпотентным частичным эндоморфизмом ψ графа G удовлетворяет условию $\varphi\psi = \psi$. Тогда $x \in \text{dom } \psi$, $\text{dom } \psi = \text{dom } \varphi = \varphi^{-1}(x)$. Следовательно, $\psi = \varphi$, $\psi\varphi = \varphi^2 = \varphi$. Значит, выполняется условие $J(\varphi)$. Таким образом, утверждение 1) доказано.

Пусть частичный эндоморфизм $\varphi \in \text{PEnd}(G)$ удовлетворяет условию $M(\varphi)$. Тогда φ есть идемпотентный частичный эндоморфизм графа G с одноэлементным множеством значений $\text{Im } \varphi = \{x_\varphi\}$ для некоторого $x_\varphi \in X$, и для любого идемпотентного частичного эндоморфизма ψ графа G с одноэлементным множеством значений $\text{Im } \psi = \{x_\psi\}$ ($x_\psi \in X$) из условия $\psi\varphi \neq 0$ следует $\psi\varphi = \psi$. Условие $\psi\varphi \neq 0$ эквивалентно тому, что $x_\psi \in \text{dom } \varphi$, а равенство $\psi\varphi = \psi$ равносильно тому, что $\text{Im } \varphi = \text{Im } \psi$. Следовательно, $x_\varphi = x_\psi$. Поскольку полугруппа $\text{PEnd}(G)$ содержит все частичные тождественные эндоморфизмы графа G , то для произвольной вершины $x \in \text{dom } \varphi$ частичный эндоморфизм $\psi = \begin{pmatrix} x \\ x \end{pmatrix}$ принадлежит полугруппе $\text{PEnd}(G)$ и удовлетворяет условию $\psi\varphi \neq 0$. Отсюда следует, что $x = x_\varphi$ и, в силу произвольности выбора $x \in \text{dom } \varphi$, выполняется $\text{dom } \varphi = \{x_\varphi\}$ и, как результат, $\varphi = \begin{pmatrix} x_\varphi \\ x_\varphi \end{pmatrix}$.

Обратно, пусть $\varphi \in \text{PEnd}(G)$ есть частичный одноэлементный тождественный эндо-

морфизм графа G вида $\varphi = \begin{pmatrix} x_\varphi \\ x_\varphi \end{pmatrix}$ для некоторого $x_\varphi \in X$. Тогда для любого идемпотентного частичного эндоморфизма ψ графа G с одноэлементным множеством значений $\text{Im } \psi = \{x_\psi\}$ из условия $\psi\varphi \neq 0$ следует $x_\psi = x_\varphi$. Следовательно, $\psi\varphi = \psi$. Значит, выполняется условие $M(\varphi)$. Таким образом, утверждение 2) доказано. $\square$

Для элемента $x \in X$ символом $\bar{x}$ обозначим одноэлементное тождественное преобразование $\begin{pmatrix} x \\ x \end{pmatrix}$ множества X . Легко видеть, что справедливо следующее утверждение.

Лемма 2. Для универсального частичного графового полуавтомата $\text{PAtm}(G) = (G, \text{PEnd}(G), \star)$ над графом $G = (X, \rho)$ при любых $x, y \in X$ и $s \in \text{PEnd}(G)$ условие $\bar{x} \cdot s \cdot \bar{y} \neq \emptyset$ равносильно тому, что $s(x) = y$, т. е. $x \star s = y$.

Доказательство. Пусть для произвольных $x, y \in X$ и $s \in \text{PEnd}(G)$ выполняется условие $\bar{x} \cdot s \cdot \bar{y} \neq \emptyset$. Это означает, что $x \in \text{dom } s$, $y = s(x)$. Тогда по определению функции переходов $\star$ графового полуавтомата $\text{PAtm}(G)$ получим $x \star s = s(x) = y$. $\square$

Для частичного полуавтомата $A = (X, S, \star)$ с полугруппой входных сигналов S на множестве состояний X определяются следующие канонические отношения:

$$\begin{aligned} \beta &= \{((x, y), (u, v)) \in X^2 \times X^2 : (\exists s \in S)(x \star s = u \wedge y \star s = v)\}, \\ P &= \{(x, y) \in X^2 \setminus \Delta_X : X^2 \subset \beta(x, y)\}, \\ R &= \{(x, y) \in X^2 : X^2 \setminus \Delta_X \subset \beta^{-1}(x, y)\}, \\ Q &= X^2 \setminus (P \cup R). \end{aligned}$$

Справедлива следующая лемма.

Лемма 3. Для универсального частичного графового полуавтомата $\text{PAtm}(G) = (G, \text{PEnd}(G), \star)$ над нетривиальным рефлексивным графом $G = (X, \rho)$ справедливы утверждения:

- 1) для элементов $x, y \in X$ условие $(x, y) \in P$ равносильно тому, что вершины x, y несмежны в графе G ;
- 2) для элементов $x, y \in X$ условие $(x, y) \in R$ равносильно тому, что вершины x, y в графе G соединяются встречными дугами;
- 3) для элементов $x, y \in X$ условие $(x, y) \in Q$ равносильно тому, что вершины x, y в графе G соединяются собственной дугой.

Доказательство. Пусть для элементов $x, y \in X$ выполняется условие $(x, y) \in P$. Поскольку граф G нетривиальный рефлексивный, найдутся такие элементы $c, d \in X$, что $(c, d) \notin \rho$. По определению отношения P это означает, что в полугруппе $\text{PEnd}(G)$ существуют частичные эндоморфизмы, отображающие пару вершин (x, y) в пару несмежных вершин

(c, d) . Следовательно, вершины x и y также несмежны. В обратную сторону очевидно. Таким образом, утверждение 1) доказано.

Пусть для элементов $x, y \in X$ выполняется условие $(x, y) \in R$. Если $x = y$, то утверждение 2) выполняется, поскольку петля встречна сама себе. Пусть теперь $x \neq y$. Поскольку граф G нетривиальный рефлексивный, то в нем найдется дуга, не являющаяся петлей, т. е. некоторая дуга $(a, b) \in \rho$, $a \neq b$. По определению отношения R это означает, что в полугруппе $\text{PEnd}(G)$ существуют частичные эндоморфизмы $\begin{pmatrix} a & b \\ x & y \end{pmatrix}, \begin{pmatrix} b & a \\ x & y \end{pmatrix} \in \text{PEnd}(G)$.

Следовательно, $(x, y) \in \rho \cap \rho^{-1}$. В обратную сторону доказательство очевидно. Таким образом, утверждение 2) доказано.

Пусть для элементов $x, y \in X$ выполняется условие $(x, y) \in Q$. Так как $(x, y) \notin P$, то из пункта 1) следует, что x и y смежны. Поскольку, кроме этого, $(x, y) \notin R$, то из пункта 2) следует, что x и y не соединяются встречными дугами. Следовательно, x и y соединяются собственной дугой. $\square$

Введем следующие формулы языка элементарной теории полугрупп L_S :

$$\begin{aligned} \Pi(x, y, u, v) &= (M(x) \wedge M(y) \wedge M(u) \wedge M(v) \wedge (\exists s)(x \cdot s \cdot u \neq 0 \wedge y \cdot s \cdot v \neq 0)), \\ \Phi_P(x, y) &= (x \neq y \wedge M(x) \wedge M(y) \wedge (\forall u, v)(M(u) \wedge M(v) \Rightarrow \Pi(x, y, u, v))), \\ \Phi_R(x, y) &= (M(x) \wedge M(y) \wedge (\forall u, v)(M(u) \wedge M(v) \wedge u \neq v \Rightarrow \Pi(u, v, x, y))), \\ \Phi_Q(x, y) &= \neg \Pi(x, y, y, x), \\ \Phi_0(x, y) &= \Phi_Q(x, y) \vee (\neg(\exists u, v) \Phi_Q(u, v) \wedge x \neq y \wedge \Phi_R(x, y)), \\ D(x, y, z) &= (M(x) \wedge M(z) \wedge x \cdot y \cdot z \neq 0). \end{aligned}$$

Имеет место следующая лемма.

Лемма 4. Для универсального частичного графового полуавтомата $\text{PAtm}(G)$ над нетривиальным рефлексивным графом $G = (X, \rho)$ с полугруппой входных сигналов $S = \text{PEnd}(G)$ справедливы утверждения:

- 1) для элементов $x_i \in S$, $i = \overline{1, 4}$ условие $\Pi(x_1, x_2, x_3, x_4)$ равносильно тому, что для некоторых элементов $a_i \in X$, $i = \overline{1, 4}$ и $s \in \text{PEnd}(G)$ выполняется $x_i = \overline{a_i}$, $i = \overline{1, 4}$ и $a_1 \star s = a_3$, $a_2 \star s = a_4$;
- 2) для элементов $x, y \in S$ условие $\Phi_P(x, y)$ равносильно тому, что выполняется $x = \overline{a}$, $y = \overline{b}$ для некоторых несмежных вершин $a, b \in X$ графа G ;
- 3) для элементов $x, y \in S$ условие $\Phi_R(x, y)$ равносильно тому, что выполняется $x = \overline{a}$, $y = \overline{b}$ для некоторых соединенных встречными дугами вершин $a, b \in X$ графа G ;
- 4) для элементов $x, y \in S$ условие $\Phi_Q(x, y)$ равносильно тому, что выполняется $x = \overline{a}$, $y = \overline{b}$ для некоторых соединенных собственной дугой вершин $a, b \in X$ графа G ;
- 5) формула $\Phi_0(x, y)$ выполнима в полугруппе $\text{PEnd}(G)$.

Доказательство. Пусть для элементов $x_i \in S, i = \overline{1, 4}$ выполняется условие $\Pi(x_1, x_2, x_3, x_4)$. Отсюда по определению следует, что для элементов x_i выполняются формулы $M(x_i)$. Тогда по лемме 1 выполняются равенства $x_i = \bar{a}_i$ для некоторых элементов $a_i \in X$. Более того, найдется $s \in S$ такой, что $\bar{a}_1 \cdot s \cdot \bar{a}_3 \neq 0$ и $\bar{a}_2 \cdot s \cdot \bar{a}_3 \neq 0$. Отсюда по лемме 2 получаем, что $a_1 \star s = a_3, a_2 \star s = a_4$. Утверждение 1) доказано.

Утверждения 2), 3) следуют непосредственно из леммы 3 и определения предикатов Φ_P, Φ_R , поскольку в этих формулах выражены теоретико-множественные определения этих предикатов. В силу леммы 3 для элементов $x, y \in S$ условие $\Phi(x, y) = \neg\Phi_P(x, y) \wedge \neg\Phi_R(x, y)$ равносильно тому, что выполняется $x = \bar{a}$ и $y = \bar{b}$ для некоторых соединенных собственной дугой вершин $a, b \in X$ графа G . С другой стороны, в силу леммы 3 в полугруппе S условие $\Pi(x, y, y, x)$ равносильно выполнимости формулы $\Phi_P(x, y) \vee \Phi_R(x, y)$. Отсюда следует, что условие $\Phi_Q(x, y)$ равносильно тому, что вершины a и b в графе G соединяются собственной дугой. Утверждение 4) доказано.

Докажем утверждение 5). Если нетривиальный рефлексивный граф G не симметричный, то в нем найдется собственная дуга $(a, b) \in \rho$. Тогда для элементов $x = \bar{a} \in S, y = \bar{b} \in S$ выполняется формула $\Phi_Q(x, y)$ и, следовательно, выполняется формула $\Phi_0(x, y)$. Если же граф G симметричный, то, очевидно, в нем нет ни одной собственной дуги, следовательно не найдется элементов $(u, v) \in S$, для которых выполняется формула $\Phi_Q(u, v)$. При этом в симметричном графе каждая дуга имеет встречную. Тогда по условию 3) для некоторых элементов $(x, y) \in S$ выполняется формула $\Phi_R(x, y)$ и, следовательно, выполняется формула $\Phi_0(x, y)$. Таким образом, формула $\Phi_0(x, y)$ в любом случае выполнима в полугруппе S . $\square$

Следующий результат доказывает относительно элементарную определимость класса универсальных частичных графовых полуавтоматов над нетривиальными рефлексивными графами в классе полугрупп.

Теорема 5. Для любого универсального частичного графового полуавтомата $\text{PAtm}(G)$ над нетривиальным рефлексивным графом $G = (X, \rho)$ выполняются следующие условия:

- 1) множество $\bar{X} = \{s \in \text{PEnd}(G) \mid M(s)\}$ непусто;
- 2) формула $D(x, y, z)$ определяет тернарное отношение $\bar{\star} \subset \bar{X} \times S \times \bar{X}$, удовлетворяющее условию $(x, y, z_1), (x, y, z_2) \in \bar{\star} \Rightarrow z_1 = z_2$;
- 3) в полугруппе входных сигналов $\text{PEnd}(G)$ найдутся такие элементы x_0, y_0 , что формула $\Pi(x_0, y_0, x, y)$ задает бинарное отношение $\bar{\rho}$ на множестве $\bar{X}$, для которого графовый полуавтомат $\bar{A} = (\bar{G}, \text{PEnd}(G), \bar{\star})$ над графом $\bar{G} = (\bar{X}, \bar{\rho})$ изоморфен полуавтомату $\text{PAtm}(G)$.

Доказательство. Пусть $A = \text{PAtm}(G)$ – универсальный частичный графовый полуавтомат над нетривиальным рефлексивным графом $G = (X, \rho)$ с полугруппой входных сигналов $S = \text{PEnd}(G)$. Так как полугруппа S содержит все тождественные преобразования $\bar{x}$ для всех вершин $x \in X$, то по лемме 1, условие 1) выполняется, т. е. множество

$\overline{X} = \{s \in \text{PEnd}(G) \mid M(s)\}$ непусто. Помимо этого, соответствие $x \mapsto \overline{x}$ ($x \in X$) определяет биективное отображение f множества вершин X на множество $\overline{X}$ всех одноэлементных частичных тождественных преобразований из S .

Формула $D(x, y, z)$ определяет в полугруппе S тернарное отношение $\bar{*} \subset \overline{X} \times S \times \overline{X}$, так как для любых $x, y, z \in S$ из $D(x, y, z)$ следует $x, z \in \overline{X}$. Тогда $x = \overline{u}$, $z = \overline{v}$ для некоторых $u, v \in X$. Кроме того, из выполнимости формулы $D(x, y, z)$ получаем

$$x \cdot y \cdot z = \overline{u} \cdot y \cdot \overline{v} = \begin{pmatrix} u \\ u \end{pmatrix} \cdot y \cdot \begin{pmatrix} v \\ v \end{pmatrix} \neq 0$$

и, следовательно, по лемме 2 $u \in \text{dom } y$ и $v = y(u)$. Таким образом, $z = \overline{y(u)}$. Поскольку $y \in S$ – преобразование множества X , удовлетворяющее свойству однозначности, то из $(x, y, z_1), (x, y, z_2) \in \bar{*}$ следует равенство $z_1 = z_2$. Тогда отношение $\bar{*}$ можно рассматривать как частичное отображение множества $\overline{X} \times S$ в множество $\overline{X}$. Значит, условие 2) выполняется.

Так как по условию теоремы $G = (X, \rho)$ – нетривиальный рефлексивный граф, то в нем найдется дуга $(a_0, b_0) \in \rho$, не являющаяся петлей (т. е. $a_0 \neq b_0$). Если граф G симметричный, то пусть (a_0, b_0) – это произвольная дуга $(a_0, b_0) \in (\rho \cap \rho^{-1}) \setminus \Delta_X$, в противном случае пусть (a_0, b_0) – произвольная собственная дуга $(a_0, b_0) \in \rho \setminus \rho^{-1}$. Обозначим, $f(a_0) = \overline{a_0} = x_0$, $f(b_0) = \overline{b_0} = y_0$.

Формула $\Pi(x_0, y_0, x, y)$ определяет в полугруппе S бинарное отношение $\bar{\rho} \subseteq \overline{X} \times \overline{X}$, так как для любых $x, y \in S$ из $\Pi(x_0, y_0, x, y)$ следует $x, y \in \overline{X}$.

Таким образом, получаем частичный графовый полуавтомат $\overline{A} = (\overline{G}, S, \bar{*})$ над графом $\overline{G} = (\overline{X}, \bar{\rho})$. Покажем, что этот полуавтомат изоморфен исходному универсальному частичному графовому полуавтомату $A = \text{PAtm}(G)$ над нетривиальным рефлексивным графом $G = (X, \rho)$.

Изоморфизм γ графовых полуавтоматов $\text{PAtm}(G)$ и $\overline{A} = (\overline{G}, S, \bar{*})$ определяется как изоморфизм двухосновных алгебраических систем $\text{PAtm}(G)$ и $\overline{A}$ упорядоченной парой $\gamma = (f_1, f_2)$ биекций $f_1 : G \rightarrow \overline{G}$, $f_2 : S \rightarrow S$, удовлетворяющих при любых $x, y \in X$, $s, t \in S$ условиям:

$$\begin{aligned} (x, y) \in \rho &\iff (f_1(x), f_1(y)) \in \bar{\rho}, \\ f_2(s \cdot t) &= f_2(s) \cdot f_2(t), \\ f_1(x \star s) &= f_1(x) \bar{*} f_2(s). \end{aligned}$$

Положим в нашем случае $f_1 = f$, $f_2 = \Delta_S$ и покажем, что $\gamma = (f, \Delta_S)$ является изоморфизмом $\text{PAtm}(G)$ на $\overline{A}$.

Во-первых, покажем, что отображение f определяет изоморфизм графа $G = (X, \rho)$ на граф $\overline{G} = (\overline{X}, \bar{\rho})$, т. е. для любых $x, y \in X$ выполняется условие $(x, y) \in \rho \iff (f(x), f(y)) \in \bar{\rho}$. Пусть для произвольных вершин $x, y \in X$ выполняется $(x, y) \in \rho$. Тогда для фиксирован-

ных ранее элементов $a_0, b_0 \in X$ существует частичный эндоморфизм $\varphi = \begin{pmatrix} a_0 & b_0 \\ x & y \end{pmatrix} \in S$, для которого выполняются следующие равенства:

$$\begin{aligned} x_0 \cdot \varphi \cdot \bar{x} &= \bar{a}_0 \cdot \varphi \cdot \bar{x} \neq 0, \\ y_0 \cdot \varphi \cdot \bar{y} &= \bar{b}_0 \cdot \varphi \cdot \bar{y} \neq 0, \end{aligned}$$

т. е. по лемме 2 $x = \varphi(a_0), y = \varphi(b_0)$. Это означает, что для элементов $f(x) = \bar{x}, f(y) = \bar{y}$ из множества $\bar{X}$ выполняется формула $\Pi(x_0, y_0, f(x), f(y))$, т. е. по определению отношения $\bar{\rho}$ выполняется $(f(x), f(y)) \in \bar{\rho}$.

С другой стороны, пусть для элементов $f(x) = \bar{x}, f(y) = \bar{y}$ из множества $\bar{X}$ выполняется $(f(x), f(y)) \in \bar{\rho}$. Покажем, что $(x, y) \in \rho$. По определению бинарного отношения $\bar{\rho}$ для некоторого частичного эндоморфизма $s \in S$ выполняются условия $x_0 \cdot s \cdot \bar{x} \neq 0, y_0 \cdot s \cdot \bar{y} \neq 0$. Значит, по лемме 2 $s(a_0) = x$ и $s(b_0) = y$. Так как $(a_0, b_0) \in \rho$ и s – частичный эндоморфизм графа $G = (X, \rho)$, то по определению частичного эндоморфизма $(x, y) \in \rho$. Таким образом, f – изоморфизм графа $G = (X, \rho)$ на граф $\bar{G} = (\bar{X}, \bar{\rho})$. Следовательно, $\bar{G} = (\bar{X}, \bar{\rho})$ также является нетривиальным рефлексивным графом.

Покажем, что изоморфизм γ согласован с функциями переходов полуавтоматов $\text{PAtm}(G)$ и $\bar{A}$. По определению функции переходов $\star$ в универсальном частичном графовом полуавтомате $\text{PAtm}(G)$ для любых $(x, s) \in \text{dom } \star$ выполняется $x \star s = s(x)$. Тогда по построению отображения f выполняется равенство $f(x \star s) = f(s(x)) = \overline{s(x)}$. С другой стороны, по определению функции переходов $\bar{\star}$ в полуавтомате $\bar{A}$ выполняется равенство $f(x) \bar{\star} \Delta_S(s) = \bar{x} \bar{\star} s = \overline{s(x)}$. Следовательно, $f(x \star s) = f(x) \bar{\star} \Delta_S(s)$ для любых $(x, s) \in \text{dom } \star$ (где $x \in X, s \in S$).

Значит, полуавтоматы $\text{PAtm}(G)$ и $\bar{A}$ изоморфны. $\square$

Таким образом, доказанная выше теорема показывает, что универсальный частичный графовый полуавтомат над нетривиальным рефлексивным графом с точностью до изоморфизма представляется как алгебраическая система, построенная в полугруппе входных сигналов этого полуавтомата.

С теоретико-модельной точки зрения частичный графовый полуавтомат $A = (G, S, \star)$ над графом $G = (X, \rho)$ с полугруппой входных сигналов $S = (S, \cdot)$ и частичной функцией переходов $\star : X \times S \rightarrow X$ рассматривается как двухосновная алгебраическая Ω -система $\mathbf{A} = (X, S, \Omega)$ с двумя базисными множествами X, S и сигнатурой $\Omega = \{B, \cdot, \star\}$. Здесь X – множество вершин графа состояний G , B – бинарный предикатный символ отношения смежности на множестве X , $\cdot$ – бинарный функциональный символ композиции элементов полугруппы, $\star$ – бинарный функциональный символ функции переходов. Элементарная теория универсальных частичных графовых полуавтоматов определяется в стиле аксиоматики Гильберта геометрии плоскости с помощью языка УИП с двухсортными переменными $\mathbf{L}_A$. Алфавит такого языка состоит из:

1) счетного множества индивидуальных переменных первого сорта для обозначения

- элементов множества вершин графа состояний полуавтомата;
- 2) счетного множества индивидуальных переменных второго сорта для обозначения входных сигналов полуавтомата;
 - 3) из двухместного предикатного символа B типа $(1, 1)$ для обозначения отношения смежности на множестве вершин графа состояний полуавтомата;
 - 4) из двухместного функционального символа $\cdot$ типа $(2, 2, 2)$ для обозначения композиции в полугруппе входных сигналов полуавтомата;
 - 5) из двухместного функционального символа $\star$ типа $(1, 2, 1)$ для обозначения функции переходов полуавтомата;
 - 6) из конечного множества логических и технических символов, таких как

$$\neg, \wedge, \vee, \implies, \iff, \forall^1, \exists^1, \forall^2, \exists^2, = \text{ и } (,).$$

Для языка $\mathbf{L_A}$ термы и формулы определяются аналогично тому, как это делается в работе [13]. Двойственной для формулы Φ называется формула $\bar{\Phi}$, которая получается из формулы Φ заменой всех ее атомарных подформул вида $B(t_1, t_2)$ формулами $B(t_2, t_1)$.

Формула Φ языка $\mathbf{L_A}$ истинна на алгебраической Ω -системе $\mathbf{A}$, если она образует истинное утверждение об этой системе при любой интерпретации ее свободных индивидуальных переменных в алгебраической системе $\mathbf{A}$. Такой факт символически описывается формулой $\mathbf{A} \models \Phi$.

Формула языка $\mathbf{L_A}$ без свободных переменных называется предложением. Множество всех предложений языка $\mathbf{L_A}$, истинных на алгебраической системе $\mathbf{A}$, обозначается через $\text{Th}(\mathbf{A})$ и называется элементарной теорией алгебраической Ω -системы $\mathbf{A}$. Полуавтоматы $\mathbf{A}$, $\mathbf{A}'$ называются элементарно эквивалентными (обозначается $\mathbf{A} \equiv \mathbf{A}'$), если $\text{Th}(\mathbf{A}) = \text{Th}(\mathbf{A}')$. Это означает, что полуавтоматы $\mathbf{A}$, $\mathbf{A}'$ не могут быть различимы с помощью свойств, выраженных формулами языка УИП $\mathbf{L_A}$.

Теорема 6. Для любой формулы Φ языка элементарной теории графовых полуавтоматов $\mathbf{L_A}$ существует эффективно построенная формула $\bar{\Phi}$ языка элементарной теории полугрупп $\mathbf{L_S}$ такая, что если формула Φ истинна на универсальном частичном графовом полуавтомате $\mathbf{A} = \text{PAtm}(G)$ над нетривиальным рефлексивным графом G , то формула $\bar{\Phi}$ истинна на его полугруппе входных сигналов $\text{Inp}(\mathbf{A}) = \text{PEnd}(G)$ и, с другой стороны, если формула $\bar{\Phi}$ истинна на полугруппе входных сигналов $\text{Inp}(\mathbf{A})$, то на универсальном частичном графовом полуавтомате $\mathbf{A}$ истинна формула Φ или двойственная ей формула $\bar{\Phi}$.

Доказательство. Для формул языка $\mathbf{L_A}$ элементарной теории графовых полуавтоматов рассмотрим следующую синтаксическую трансформацию в формулы языка $\mathbf{L_S}$ элементарной теории полугрупп. Пусть $t = t(y_1, \dots, y_n)$ – терм языка $\mathbf{L_A}$ с переменными $y_1, \dots, y_n$. Для такого терма t эффективно построим терм $\bar{t}$ сигнатуры языка $\mathbf{L_S}$ по следующему правилу:

- 1) если t является индивидуальной переменной y_i , обозначающей элемент множества вершин графа состояний полуавтомата, то $\bar{t}$ есть индивидуальная переменная y_i , обозначающая элемент полугруппы входных сигналов;
- 2) если t является индивидуальной переменной y_i , обозначающей входной сигнал полуавтомата, то $\bar{t}$ есть тот же самый терм y_i ;
- 3) если $t = t_1 \cdot t_2$ для термов t_1, t_2 второго сорта (обозначающих входные сигналы полуавтомата), то $\bar{t}$ есть терм $\bar{t}_1 \cdot \bar{t}_2$;
- 4) если $t = t_1 \star t_2$ для термина t_1 первого сорта (обозначающего элементы множества вершин графа состояний полуавтомата) и термина t_2 второго сорта (обозначающего входные сигналы полуавтомата), то $\bar{t}$ есть терм $\bar{t}_1 \cdot \bar{t}_2$.

Пусть теперь $\Phi = \Psi(y_1, \dots, y_n)$ – формула языка $\mathbf{L_A}$ с переменными $y_1, \dots, y_n$, бинарным предикатным символом B и двумя бинарными функциональными символами $\cdot, \star$. Для такой формулы Φ эффективно построим формулу $\check{\Phi}$ языка $\mathbf{L_S}$ по следующему правилу:

- 1) если Φ есть атомарная формула $t_1 = t_2$, то $\check{\Phi}$ есть формула $\bar{t}_1 = \bar{t}_2$;
- 2) если Φ есть атомарная формула $B(t_1, t_2)$ для двух термов t_1, t_2 первого сорта (обозначающих элементы множества вершин графа состояний полуавтомата), то $\check{\Phi}$ есть формула $\Pi(x_0, y_0, \bar{t}_1, \bar{t}_2)$;
- 3) если Φ есть формула $\Phi_1 \tau \Phi_2$, где τ – один из символов $\wedge, \vee, \Rightarrow, \Leftrightarrow$, то $\check{\Phi}$ есть формула $\check{\Phi}_1 \tau \check{\Phi}_2$;
- 4) если Φ есть формула $\neg \Phi$, то формула $\check{\Phi}$ есть формула $\neg \check{\Phi}$;
- 5) если Φ есть формула $(\forall^1 y_i) \Psi(y_1, \dots, y_n)$ (соответственно, $(\exists^1 y_i) \Psi(y_1, \dots, y_n)$) для индивидуальной переменной y_i , обозначающей элемент множества вершин графа состояний полуавтомата, то $\check{\Phi}$ есть формула $(\forall y_i)(M(y_i) \Rightarrow \check{\Psi})$ (соответственно, $(\exists y_i)(M(y_i) \wedge \check{\Psi})$);
- 6) если Φ есть формула $(\forall^2 y_i) \Psi(y_1, \dots, y_n)$ (соответственно, $(\exists^2 y_i) \Psi(y_1, \dots, y_n)$) для индивидуальной переменной y_i , обозначающей входной сигнал полуавтомата, то $\check{\Phi}$ есть формула $(\forall y_i) \check{\Psi}$ (соответственно, $(\exists y_i) \check{\Psi}$).

Таким образом, для каждой формулы Φ языка $\mathbf{L_A}$ элементарной теории графовых полуавтоматов можно определить формулу $\bar{\Phi}$ языка $\mathbf{L_S}$ элементарной теории полугрупп по правилу:

$$\bar{\Phi} = (\exists x_0, y_0)(\Phi_0(x_0, y_0) \wedge \check{\Phi}).$$

Поскольку изоморфные алгебраические системы $\mathbf{A} = \text{PAtm}(G)$ над графом $G = (X, \rho)$ и $\bar{\mathbf{A}} = (\bar{G}, \text{PEnd}(G), \bar{\star})$ над графом $\bar{G} = (\bar{X}, \bar{\rho})$ элементарно эквивалентны, то для любой формулы Φ языка $\mathbf{L_A}$ элементарной теории графовых полуавтоматов формула $\mathbf{A} \models \Phi$ равносильна формуле $\bar{\mathbf{A}} \models \bar{\Phi}$. По аналогии с доказательством [18, теорема 3.1.8], индукцией относительно порядка формулы Φ можно доказать следующее свойство:

$$\bar{\mathbf{A}} \models \Phi \iff \text{Inp}(\mathbf{A}) \models \bar{\Phi}.$$

Следовательно, если Φ истинна на универсальном частичном графовом полуавтомате $\mathbf{A}$,

то формула $\bar{\Phi}$ истинна на его полугруппе входных сигналов $\text{Inp}(\mathbf{A})$, т.е. выполняется условие

$$\mathbf{A} \models \Phi \implies \text{Inp}(\mathbf{A}) \models \bar{\Phi}.$$

С другой стороны, ввиду того, что $\text{Inp}(\mathbf{A}) = \text{Inp}(\tilde{\mathbf{A}})$ и либо $\mathbf{A}$ изоморфен $\bar{\mathbf{A}}$ при определении отношения смежности $\bar{\rho}$ с помощью формулы $\Pi(x_0, y_0, x, y)$ для $(x_0, y_0) \in \bar{\rho}$, $x_0 \neq y_0$, либо $\tilde{\mathbf{A}}$ изоморфен $\bar{\mathbf{A}}$ при определении $\bar{\rho}$ с помощью формулы $\Pi(x_0, y_0, x, y)$ для $(y_0, x_0) \in \bar{\rho}$, $x_0 \neq y_0$, выполняется условие

$$\text{Inp}(\mathbf{A}) \models \bar{\Phi} \implies (\mathbf{A} \models \Phi \vee \mathbf{A} \models \check{\Phi}). \quad \square$$

3. Приложения относительно элементарной определимости

Доказанная относительно элементарная определимость класса универсальных частичных графовых полуавтоматов в классе полугрупп и эффективное преобразование формул элементарной теории графовых полуавтоматов в формулы элементарной теории полугрупп позволяют исследовать такие вопросы, как определяемость универсальных частичных графовых полуавтоматов своими полугруппами входных сигналов, относительная аксиоматизируемость подклассов универсальных частичных графовых полуавтоматов над нетривиальными рефлексивными графами формулами языка элементарной теории полугрупп и другие.

Следующая теорема показывает взаимосвязь универсальных частичных графовых полуавтоматов, у которых изоморфны полугруппы входных сигналов.

Теорема 7. *Для любых универсальных частичных графовых полуавтоматов $A_1 = \text{PAtm}(G_1)$, $A_2 = \text{PAtm}(G_2)$ над рефлексивными графами $G_1 = (X_1, \rho_1)$, $G_2 = (X_2, \rho_2)$ такими, что хотя бы один из них нетривиален, следующие условия эквивалентны:*

- 1) *полугруппа $\text{Inp}(A_1)$ входных сигналов частичного полуавтомата A_1 изоморфна полугруппе $\text{Inp}(A_2)$ входных сигналов частичного полуавтомата A_2 ;*
- 2) *частичный полуавтомат A_1 изоморфен частичному полуавтомату A_2 или двойственному для него частичному полуавтомату $\tilde{A}_2$.*

Доказательство. Докажем $1) \implies 2)$. Пусть φ – изоморфизм полугруппы $\text{Inp}(A_1)$ на полугруппу $\text{Inp}(A_2)$, и пусть, для определенности, $G_1 = (X_1, \rho_1)$ – нетривиальный рефлексивный граф. Тогда найдется дуга $(a_0, b_0) \in \rho_1 \setminus \Delta_{X_1}$ и по лемме 4 для элементов $x_0 = \bar{a}_0$, $y_0 = \bar{b}_0$ в полугруппе $\text{Inp}(A_1)$ выполняется $\Phi_0(x_0, y_0)$. Следовательно, $\varphi(x_0) = \bar{c}_0$, $\varphi(y_0) = \bar{d}_0$ для вершин $c_0, d_0 \in X_2$. При этом в полугруппе $\text{Inp}(A_2)$ выполняется формула $\Phi_0(\varphi(x_0), \varphi(y_0))$. Тогда в силу леммы 4 $(c_0, d_0) \in \rho_2 \setminus \Delta_{X_2}$ или $(d_0, c_0) \in \rho_2 \setminus \Delta_{X_2}$.

В теореме 5 в полугруппе входных сигналов $\text{Inp}(A_1)$ полуавтомата A_1 с помощью формул языка элементарной теории полугрупп $\mathbf{L}_S$ и фиксированных элементов $x_0, y_0 \in \text{Inp}(A_1)$ строится изоморфный A_1 полуавтомат $\bar{A}_1$ над графом $\bar{G}_1 = (\bar{X}_1, \bar{\rho}_{X_1})$. Отношение смежности $\bar{\rho}_{X_1}$ определяется предикатом $\Pi(x_0, y_0, x, y)$ элементарной теории

полугрупп $\mathbf{L_S}$. Аналогично, используя формулы элементарной теории полугрупп $\mathbf{L_S}$, в полугруппе $\text{Inp}(A_2)$ с помощью элементов $\varphi(x_0)$ и $\varphi(y_0)$ определяется полуавтомат $\bar{A}_2$, такой, что A_2 изоморфен $\bar{A}_2$. Отношение смежности $\bar{\rho}_{X_2}$ графа $\bar{G}_2 = (\bar{X}_2, \bar{\rho}_{X_2})$ определяется предикатом $\Pi(\varphi(x_0), \varphi(y_0), x, y)$ элементарной теории полугрупп $\mathbf{L_S}$.

Поскольку полуавтоматы $\bar{A}_1$, $\bar{A}_2$ выражаются в соответствующих полугруппах $\text{Inp}(A_1)$, $\text{Inp}(A_2)$ формулами языка $\mathbf{L_S}$ элементарной теории полугрупп, определенными в теореме 5, и изоморфизм φ сохраняет выполнимость таких формул, то для любых $x, y \in X_1$ по определению отношения $\bar{\rho}_{X_1}$ условие $(x, y) \in \bar{\rho}_{X_1}$ равносильно тому, что предикат $\Pi(x_0, y_0, x, y)$ истинен в полугруппе $\text{Inp}(A_1)$, а это, в свою очередь, равносильно тому, что предикат $\Pi(\varphi(x_0), \varphi(y_0), \varphi(x), \varphi(y))$ истинен в полугруппе $\text{Inp}(A_2)$. Значит, либо $(\varphi(x), \varphi(y)) \in \bar{\rho}_{X_2}$, если $(\varphi(x_0), \varphi(y_0)) \in \bar{\rho}_{X_2}$ (когда $(c_0, d_0) \in \rho_2$), либо $(\varphi(y), \varphi(x)) \in \bar{\rho}_{X_2}$, если $(\varphi(y_0), \varphi(x_0)) \in \bar{\rho}_{X_2}$ (когда $(d_0, c_0) \in \rho_2$). Следовательно, если $(c_0, d_0) \in \rho_2$, то φ индуцирует изоморфизм полуавтомата $\bar{A}_1$ на полуавтомат $\bar{A}_2$, и A_1 изоморфен $\bar{A}_2$; если $(d_0, c_0) \in \rho_2$, то φ индуцирует изоморфизм полуавтомата $\bar{A}_1$ на полуавтомат $\tilde{\bar{A}}_2$, и A_1 изоморфен $\tilde{\bar{A}}_2$.

Докажем $2) \implies 1)$. Пусть полуавтомат A_1 изоморфен полуавтомату A_2 или двойственному для него полуавтомату $\tilde{\bar{A}}_2$. Так как $\text{Inp}(A_1) = \text{Inp}(\tilde{\bar{A}}_2)$, то по определению изоморфизма полуавтоматов получаем, что $\text{Inp}(A_1)$ изоморфна $\text{Inp}(A_2)$. $\square$

В работе [7] Ю.М. Важенин обозначил проблему взаимосвязи графов, у которых элементарно эквивалентны производные полугруппы специальных преобразований. Следующий результат решает эту проблему для универсальных частичных графовых полуавтоматов над нетривиальными рефлексивными графами.

Теорема 8. *Для любых универсальных частичных графовых полуавтоматов $A_1 = \text{PAtm}(G_1)$, $A_2 = \text{PAtm}(G_2)$ над рефлексивными графами $G_1 = (X_1, \rho_1)$, $G_2 = (X_2, \rho_2)$ такими, что хотя бы один из них нетривиален, следующие условия эквивалентны:*

- 1) *полугруппа $\text{Inp}(A_1)$ входных сигналов частичного полуавтомата A_1 элементарно эквивалентна полугруппе $\text{Inp}(A_2)$ входных сигналов частичного полуавтомата A_2 ;*
- 2) *частичный полуавтомат A_1 элементарно эквивалентен частичному полуавтомату A_2 или двойственному для него частичному полуавтомату $\tilde{\bar{A}}_2$.*

Доказательство. Докажем $1) \implies 2)$. Пусть $\text{Inp}(A_1) \equiv \text{Inp}(A_2)$. Рассмотрим формулу Ψ языка элементарной теории графовых полуавтоматов $\mathbf{L_A}$ такую, что $A_1 \models \Psi$. Тогда по теореме 6 $\text{Inp}(A_1) \models \bar{\Psi}$ и, следовательно, $\text{Inp}(A_2) \models \bar{\Psi}$. Значит, по теореме 6 $A_2 \models \Psi$ или $A_2 \models \check{\Psi}$.

В частности, если формула Ψ логически равносильна формуле $\check{\Psi}$, то она называется самодвойственной формулой и для нее выполняется условие $A_1 \models \Psi \iff A_2 \models \Psi$. Например, для произвольного предложения Φ языка элементарной теории полуавтоматов $\mathbf{L_A}$ формула $\Psi = (\Phi \iff \check{\Phi})$ является самодвойственной и, значит, предложение Φ является или не является равносильным предложению $\check{\Phi}$ одновременно на полуавтоматах A_1 , A_2 ,

т. е. предложения $\Phi, \check{\Phi}$ одновременно истинны или ложны как на полуавтомате A_1 , так и на полуавтомате A_2 .

Сначала предположим, что найдется предложение $\Psi_0 \in \text{Th}(A_1) \cup \text{Th}(A_2)$, которое не является самодвойственным. Пусть, для определенности, $\Psi_0 \in \text{Th}(A_1)$. Тогда формула $\Psi_0 \iff \check{\Psi}_0$ не выполняется на A_1 (и, следовательно, на A_2). Это означает, что как на полуавтомате A_1 , так и на полуавтомате A_2 , истинно только одно из предложений $\Psi_0, \check{\Psi}_0$. Тогда имеем $A_1 \models \Psi_0$ (по условию), $A_1 \not\models \check{\Psi}_0$ и либо $A_2 \models \Psi_0$, $A_2 \not\models \check{\Psi}_0$, либо $A_2 \models \check{\Psi}_0$, $A_2 \not\models \Psi_0$. Предположим, что $A_2 \models \Psi_0$, $A_2 \not\models \check{\Psi}_0$. Тогда для любой формулы Φ языка $\mathbf{L}_A$ элементарной теории полуавтоматов верно $A_2 \models \Phi \wedge \check{\Psi}_0$. Пусть $\Psi \in \text{Th}(A_1)$, тогда выполняются следующие условия: $A_1 \models \Psi$, $A_1 \models \Psi \wedge \Psi_0$. Так как двойственная для формулы $\Psi \wedge \Psi_0$ формула $\check{\Psi} \wedge \check{\Psi}_0$ не выполняется на A_2 (поскольку $A_2 \not\models \check{\Psi}_0$), то $A_2 \models \Psi \wedge \Psi_0$. Следовательно, $A_2 \models \Psi$ и $\Psi \in \text{Th}(A_2)$. Значит, $\text{Th}(A_1) \subset \text{Th}(A_2)$.

Теперь пусть $\Psi \in \text{Th}(A_2)$, тогда выполняются следующие условия: $A_2 \models \Psi$, $A_2 \models \Psi \wedge \Psi_0$. Так как двойственная для формулы $\Psi \wedge \Psi_0$ формула $\check{\Psi} \wedge \check{\Psi}_0$ не выполняется на A_1 (поскольку $A_1 \not\models \check{\Psi}_0$), то $A_1 \models \Psi \wedge \Psi_0$. Следовательно, $A_1 \models \Psi$ и $\Psi \in \text{Th}(A_1)$. Значит, $\text{Th}(A_2) \subset \text{Th}(A_1)$. В результате получаем равенство $\text{Th}(A_1) = \text{Th}(A_2)$, т. е. $A_1 \equiv A_2$.

Рассмотрим второй вариант – пусть $A_2 \models \check{\Psi}_0$, $A_2 \not\models \Psi_0$. Тогда $\tilde{A}_2 \models \Psi_0$ и для любой формулы Φ языка $\mathbf{L}_A$ элементарной теории полуавтоматов верно $A_2 \models \Phi \wedge \Psi_0$. Пусть $\Psi \in \text{Th}(A_1)$, тогда выполняются следующие условия: $A_1 \models \Psi$, $A_1 \models \Psi \wedge \Psi_0$. Так как двойственная для формулы $\check{\Psi} \wedge \check{\Psi}_0$ формула $\Psi \wedge \Psi_0$ не выполняется на A_2 (поскольку $A_2 \not\models \Psi_0$), то $A_2 \models \check{\Psi} \wedge \check{\Psi}_0$. Следовательно, $A_2 \models \check{\Psi}$, $\tilde{A}_2 \models \Psi$ и $\Psi \in \text{Th}(\tilde{A}_2)$. Значит, $\text{Th}(A_1) \subset \text{Th}(\tilde{A}_2)$.

Теперь пусть $\Psi \in \text{Th}(\tilde{A}_2)$, тогда выполняются следующие условия: $\tilde{A}_2 \models \Psi$, $A_2 \models \check{\Psi} \wedge \check{\Psi}_0$. Так как двойственная для формулы $\Psi \wedge \Psi_0$ формула $\check{\Psi} \wedge \check{\Psi}_0$ не выполняется на A_1 (поскольку $A_1 \not\models \check{\Psi}_0$), то $A_1 \models \Psi \wedge \Psi_0$. Следовательно, $A_1 \models \Psi$ и $\Psi \in \text{Th}(A_1)$. Значит, $\text{Th}(\tilde{A}_2) \subset \text{Th}(A_1)$. В результате получаем равенство $\text{Th}(A_1) = \text{Th}(\tilde{A}_2)$, т. е. $A_1 \equiv \tilde{A}_2$.

Теперь рассмотрим случай, когда все предложения $\Psi \in \text{Th}(A_1) \cup \text{Th}(A_2)$ самодвойственные. Тогда для любого такого предложения Ψ условия $A_1 \models \Psi$, $A_2 \models \Psi$ равносильны и, значит, выполняется равенство $\text{Th}(A_1) = \text{Th}(A_2)$, т. е. $A_1 \equiv A_2$.

Докажем $2) \implies 1)$. Пусть $A_1 \equiv A_2$ или $A_1 \equiv \tilde{A}_2$. Тогда $\text{Th}(A_1) = \text{Th}(A_2)$ или $\text{Th}(A_1) = \text{Th}(\tilde{A}_2)$ соответственно. Ясно, что элементарная теория $\text{Th}(\text{Inp}(A))$ полугруппы входных сигналов $\text{Inp}(A)$ любого графового полуавтомата A состоит из таких формул элементарной теории $\text{Th}(A)$ частичного графового полуавтомата A , в которых содержатся термы только второго сорта. Следовательно, из равенства $\text{Th}(A_1) = \text{Th}(A_2)$ (или $\text{Th}(A_1) = \text{Th}(\tilde{A}_2)$) следует равенство

$$\text{Th}(\text{Inp}(A_1)) = \text{Th}(\text{Inp}(A_2)) = \text{Th}(\text{Inp}(\tilde{A}_2)),$$

поскольку полугруппы входных сигналов двойственных полуавтоматов равны. Значит, $\text{Inp}(A_1) \equiv \text{Inp}(A_2)$. $\square$

Аксиомами языка $\mathbf{L_A}$ элементарной теории графовых полуавтоматов являются обычные аксиомы узкого исчисления предикатов с равенством [19]. Любое множество Σ формул языка $\mathbf{L_A}$ элементарной теории графовых полуавтоматов определяет класс $\text{Mod}(\Sigma)$ алгебраических Ω -систем, на которых истинны все формулы из Σ . В этом случае говорят, что класс алгебраических Ω -систем $\mathbf{K} = \text{Mod}(\Sigma)$ аксиоматизируется множеством формул Σ , которое, в свою очередь, называется системой аксиом класса $\mathbf{K}$.

Лемма 9. *Класс $\mathbf{K_G}$ всех универсальных частичных графовых полуавтоматов над рефлексивными графами аксиоматизируется следующим набором формул Σ_G :*

- 1) $A_1 = (\forall^1 x) B(x, x)$ – рефлексивность отношения смежности ρ ;
- 2) $A_2 = (\forall^2 x, y, z)((x \cdot y) \cdot z = x \cdot (y \cdot z))$ – ассоциативность операции композиции $\cdot$ полугруппы входных сигналов;
- 3) $A_3 = (\forall^1 x, y)(\forall^2 z)(B(x, y) \implies B(x \star z, y \star z))$ – согласованность функции переходов $\star$ с отношением смежности ρ ;
- 4) $A_4 = (\forall^1 x)(\forall^2 y, z)((x \star y) \star z = x \star (y \cdot z))$ – согласованность функции переходов $\star$ с операцией композиции $\cdot$ полугруппы входных сигналов.

Следствие 10. *Класс $\mathbf{K_{G_0}}$ всех универсальных частичных графовых полуавтоматов над нетривиальными рефлексивными графами аксиоматизируется набором формул Σ_G с добавлением следующей аксиомы:*

$$A_0 = (\exists^1 x, y)(x \neq y \wedge \neg B(x, y)).$$

Следствие 11. *Класс $\mathbf{K_{G_1}}$ всех универсальных частичных графовых полуавтоматов над рефлексивными симметричными графами аксиоматизируется набором формул Σ_G с добавлением следующей аксиомы:*

$$A_5 = (\forall^1 x, y)(B(x, y) \implies B(y, x)).$$

Следствие 12. *Класс $\mathbf{K_{G_2}}$ всех универсальных частичных графовых полуавтоматов над рефлексивными асимметричными графами аксиоматизируется набором формул Σ_G с добавлением следующей аксиомы:*

$$A_6 = (\exists^1 x, y)(x \neq y \implies (B(x, y) \wedge \neg B(y, x))).$$

Для каждого класса полуавтоматов $\mathbf{K} \subset \mathbf{K_{G_0}}$ определим класс полугрупп

$$\text{Inp}(\mathbf{K}) = \{\text{Inp}(A) : A \in \mathbf{K}\}.$$

Класс $\mathbf{K} \subset \mathbf{K_{G_0}}$ называется Inp -аксиоматизируемым, если соответствующий ему класс полугрупп $\text{Inp}(\mathbf{K})$ относительно аксиоматизируем в классе полугрупп $\mathbf{S_{G_0}} = \text{Inp}(\mathbf{K_{G_0}})$, т. е. $\text{Inp}(\mathbf{K}) = \mathbf{T} \cap \mathbf{S_{G_0}}$ для некоторого аксиоматизируемого класса полугрупп $\mathbf{T}$.

Множество Σ формул языка $\mathbf{L}_A$ элементарной теории полуавтоматов называется самодвойственным, если для любой формулы $\Psi \in \Sigma$ формула $\check{\Psi}$ логически равносильна некоторой формуле из класса Σ . В частности, если формула Ψ самодвойственна (т.е. выполняется $\Psi \iff \check{\Psi}$), то множество $\Sigma = \{\Psi\}$ самодвойственно.

Теорема 13. *Подклассы универсальных частичных графовых полуавтоматов $\mathbf{K}_{G_1}$, $\mathbf{K}_{G_2}$ класса $\mathbf{K}_{G_0}$ полуавтоматов Inp-аксиоматизируемы.*

Доказательство. В теореме 6 была определена эффективная трансформация $\Phi \mapsto \bar{\Phi}$ формул Φ языка $\mathbf{L}_A$ элементарной теории полуавтоматов в формулы $\bar{\Phi}$ языка $\mathbf{L}_S$ элементарной теории полуавтоматов так, что для любого универсального частичного графового полуавтомата $A = \text{PAtm}(G)$ над нетривиальным рефлексивным графом G выполняется условие:

$$A \models \Phi \vee A \models \check{\Phi} \iff \text{Inp}(A) \models \bar{\Phi}.$$

Если некоторый класс универсальных частичных графовых полуавтоматов $\mathbf{K}$ аксиоматизируется в классе $\mathbf{K}_{G_0}$ самодвойственным множеством формул Σ , то по теореме 6 для всех формул $\Phi \in \Sigma$ условие $A \models \Phi$ равносильно условию $\text{Inp}(A) \models \bar{\Phi}$. Значит, класс полугрупп входных сигналов $\text{Inp}(\mathbf{K})$ относительно аксиоматизируем в классе $\mathbf{S}_{G_0}$ множеством формул $\bar{\Sigma} = \{\bar{\Phi} : \Phi \in \Sigma\}$.

Поскольку классы $\mathbf{K}_{G_1}$, $\mathbf{K}_{G_2}$ аксиоматизируются в классе $\mathbf{K}_{G_0}$ самодвойственными аксиомами A_5 и A_6 , то они Inp-аксиоматизируются аксиомами

$$\begin{aligned} \bar{A}_5 &= (\forall x, y)(\Pi(x_0, y_0, x, y) \implies \Pi(x_0, y_0, y, x)), \\ \bar{A}_6 &= (\exists x, y)(x \neq y \implies (\Pi(x_0, y_0, x, y) \wedge \neg \Pi(x_0, y_0, y, x))) \end{aligned}$$

соответственно. □

Следующий результат показывает взаимосвязь проблем разрешимости [12] элементарных теорий классов графовых полуавтоматов и классов полугрупп.

Для формального языка $\mathbf{L}$ некоторой сигнатуры Ω символом P_L обозначим множество всех предложений этого языка. Теория T языка $\mathbf{L}$ называется разрешимой, если существует алгоритм для решения вопроса принадлежности предложения из P_L теории T . В противном случае теория T называется неразрешимой. Теория T называется наследственно неразрешимой, если любая подтеория теории T той же сигнатуры Ω неразрешима. Для класса $\mathbf{K}$ алгебраических систем сигнатуры Ω символом $\mathbf{K}_{fin}$ обозначается класс конечных систем из $\mathbf{K}$. Теория $\text{Th}(\mathbf{K})$ называется эффективно неотделимой, если рекурсивно неотделимы множества $\text{Th}(\mathbf{K})$ и $P_L \setminus \text{Th}(\mathbf{K}_{fin})$, т.е. не существует таких непересекающихся рекурсивных множеств $M, N \subset P_L$, что $\text{Th}(\mathbf{K}) \subset M$ и $P_L \setminus \text{Th}(\mathbf{K}_{fin}) \subset N$.

На основании теоремы 2 из §1 главы 5 книги [12] и теоремы 3.3.2 из статьи [19] получаем следующий результат.

Теорема 14. Для любого класса $\mathbf{K}$ универсальных частичных графовых полуавтоматов над нетривиальными рефлексивными графами справедливы следующие утверждения:

- 1) если элементарная теория класса $\mathbf{K}$ универсальных частичных графовых полуавтоматов наследственно неразрешима, то и элементарная теория класса $\text{Inp}(\mathbf{K})$ полугрупп наследственно неразрешима;
- 2) если элементарная теория класса $\mathbf{K}$ универсальных частичных графовых полуавтоматов эффективно неотделима, то и элементарная теория класса $\text{Inp}(\mathbf{K})$ полугрупп эффективно неотделима.

В заключение авторы выражают большую признательность рецензенту за его полезные замечания.

Список литературы

- [1] Б.И. Плоткин, Л.Я. Гринглаз, А.А. Гварамия, *Элементы алгебраической теории автоматов*, Высш. шк., М., 1994.
- [2] Р. Лидл, Г. Пильц, *Прикладная абстрактная алгебра*, Изд-во Урал. ун-та, Екатеринбург, 1996.
- [3] С. Улам, *Нерешенные математические задачи*, Наука, М., 1964.
- [4] Б.И. Плоткин, *Группы автоморфизмов алгебраических систем*, Наука, М., 1966.
- [5] А.Г. Пинус, *Об элементарной эквивалентности производных структур свободных полугрупп, унаров и групп*, Алгебра и логика **43** (6), 730–748 (2004).
URL: <https://www.mathnet.ru/rus/al107>
- [6] А.Г. Пинус, *Об элементарной эквивалентности производных структур свободных решеток*, Изв. вузов. Матем. (5), 44–47 (2002).
URL: <https://www.mathnet.ru/rus/ivm1014>
- [7] Ю.М. Важенин, *Элементарные свойства полугрупп преобразований упорядоченных множеств*, Алгебра и логика **9** (3), 281–301 (1970).
URL: <https://www.mathnet.ru/rus/al1245>
- [8] Ю.М. Важенин, *Об элементарной определяемости и элементарной характеризуемости классов рефлексивных графов*, Изв. вузов. Матем. (7), 3–11 (1972).
URL: <https://www.mathnet.ru/rus/ivm4076>
- [9] Л.М. Глускин, *Полугруппы и кольца эндоморфизмов линейных пространств*, Изв. АН СССР. Сер. матем. **23** (6), 841–870 (1959).
URL: <https://www.mathnet.ru/rus/im3817>
- [10] Л.М. Глускин, *Полугруппы изотонных преобразований*, УМН **16** (5), 157–162 (1961).
URL: <https://www.mathnet.ru/rus/rm6671>

- [11] В.Т. Марков, А.В. Михалёв, Л.А. Скорняков, А.А. Туганбаев, *Кольца эндоморфизмов модулей и структуры подмодулей*, Итоги науки и техн. Сер. Алгебра. Топол. Геом. **21**, 183–254 (1983).
URL: <https://www.mathnet.ru/rus/inta105>
- [12] Ю.Л. Ершов, *Проблемы разрешимости и конструктивные модели*, Наука, М., 1980.
- [13] Р.А. Фарахутдинов, *Относительно элементарная определимость класса универсальных графовых полуавтоматов в классе полугрупп*, Изв. вузов. Матем. (1), 74–84 (2022).
DOI: <https://doi.org/10.26907/0021-3446-2022-1-74-84>
- [14] А.И. Мальцев, *Алгебраические системы*, Наука, М., 1970.
- [15] Ф. Харари, *Теория графов*, Мир, М., 1973.
- [16] А. Клиффорд, Г. Престон, *Алгебраическая теория полугрупп*, Мир, М., 1972.
- [17] В.В. Вагнер, *Полугруппы частичных преобразований с симметричным отношением транзитивности*, Изв. вузов. Матем. (1), 81–88 (1957).
URL: <https://www.mathnet.ru/rus/ivm3022>
- [18] А. Робинсон, *Введение в теорию моделей и метаматематику алгебры*, Наука. Физматлит, М., 1967.
- [19] Ю.Л. Ершов, И.А. Лавров, А.Д. Тайманов, М.А. Тайцлин, *Элементарные теории*, УМН **20** (4), 37–108 (1965).
URL: <https://www.mathnet.ru/rus/rm6048>

Владимир Александрович Молчанов

Саратовский государственный университет им. Н.Г. Чернышевского,
ул. Астраханская, д. 83, г. Саратов, 410012, Россия,
e-mail: v.molchanov@inbox.ru

Ренат Абуханович Фарахутдинов

Саратовский государственный университет им. Н.Г. Чернышевского,
ул. Астраханская, д. 83, г. Саратов, 410012, Россия,
e-mail: renatfara@mail.ru

Relatively elementary definability of the class of universal partial graphic semiautomata in the class of semigroups

V.A. Molchanov, R.A. Farakhutdinov

Abstract. The work is devoted to the algebraic theory of structured automata. We consider semigroup automata without output signals over graphs, which are called graphic semiautomata. We study partial graphic semiautomata, each input signal of which is a partial endomorphism of the state graph. In the category of partial graphic semiautomata over the graph $G = (X, \rho)$, special attention is paid to the semiautomaton $\text{PAtm}(G) = (G, \text{PEnd}(G), \star)$ with semigroup $\text{PEnd}(G)$ of all partial endomorphisms of the graph G , since it is a universally attracting object in this category and is called a universal partial graphic semiautomaton. The main result of the work is the proof of the relatively elementary definability of the class of universal partial graphic semiautomata over nontrivial reflexive graphs in the class of semigroups, and applications of got relatively elementary definability.

Keywords: semiautomaton, graph, partial endomorphism, relatively elementary definability.

DOI: 10.26907/2949-3919.2024.4.103-123

References

- [1] B.I. Plotkin, L.Ja. Greenglaz, A.A. Gvaramija, *Elements of algebraic theory of automata*, Vysshaya shkola, M., 1994 [in Russian].
- [2] R. Lidl, G. Pilz, *Applied abstract algebra*, Springer-Verlag, New York, 1998.
DOI: <https://doi.org/10.1007/978-1-4757-2941-2>
- [3] S. Ulam, *A collection of mathematical problems*, Interscience Publ., New York, 1960.
- [4] B.I. Plotkin, *Groups of automorphisms of algebraic systems*, Wolters-Noordhoff Publ., Groningen, 1972.
- [5] A. G. Pinus, *Elementary equivalence of derived structures of free semigroups, unars, and groups*, Algebra Logic **43** (6), 408–417 (2004).
DOI: <https://doi.org/10.1023/B:ALLO.0000048829.60182.48>
- [6] A.G. Pinus, *Elementary equivalence of derived structures of free lattices*, Russ. Math. **46** (5), 42–45 (2002).

-
- [7] Yu.M. Vazhenin, *Elementary properties of semigroups of transformations of ordered sets*, Algebra Logic **9** (3), 281–301 (1970) [in Russian].
URL: <https://www.mathnet.ru/rus/al1245>
- [8] Yu.M. Vazhenin, *The elementary definability and elementary characterizability of classes of reflexive graphs*, Izv. Vyssh. Uchebn. Zaved. Mat. (7), 3–11 (1972) [in Russian].
URL: <https://www.mathnet.ru/rus/ivm4076>
- [9] L.M. Gluskin, *Semigroups and endomorphism rings of linear spaces*, Izv. Akad. Nauk SSSR Ser. Mat. **23** (6), 841–870 (1959) [in Russian].
URL: <https://www.mathnet.ru/rus/im3817>
- [10] L. M. Gluskin, *Semigroups of isotone transformations*, Uspekhi Mat. Nauk **16** (5), 157–162 (1961) [in Russian].
URL: <https://www.mathnet.ru/rus/rm6671>
- [11] V.T. Markov, A.V. Mikhalev, L.A. Skorniyakov, A.A. Tuganbaev, *Endomorphism rings of modules, and lattices of submodules*, J. Soviet Math. **31** (3), 3005–3051 (1985).
DOI: <https://doi.org/10.1007/BF02106808>
- [12] Yu.L. Ershov, *Decidability problems and constructive models*, Nauka, M., 1980 [in Russian].
- [13] R.A. Farakhutdinov, *Relatively elementary definability of the class of universal graphic semiautomata in the class of semigroups*, Russ. Math. **66** (1), 62–70 (2022).
DOI: <https://doi.org/10.3103/S1066369X22010029>
- [14] A.I. Mal'cev, *Algebraic Systems*, Springer-Verlag, New York–Heidelberg, 1973.
DOI: <https://doi.org/10.1007/978-3-642-65374-2>
- [15] F. Harary, *Graph theory*, Addison-Wesley Publ., 1969.
DOI: <https://doi.org/10.1201/9780429493768>
- [16] A.H. Clifford, G.B. Preston, *The algebraic theory of semigroups*, AMS, New York, 1967.
- [17] V.V. Vagner, *Semigroups of partial transformations with a symmetric transitivity relation*, Izv. Vyssh. Uchebn. Zaved. Mat. (1), 81–88 (1957) [in Russian].
URL: <https://www.mathnet.ru/rus/ivm3022>
- [18] A. Robinson, *Introduction to model theory and to the metamathematics of algebra*, North-Holland Publ., 1965.
- [19] Yu.L. Ershov, I.A. Lavrov, A.D. Taimanov, M.A. Taitslin, *Elementary theories*, Russ. Math. Surv. **20** (4), 35–105 (1965).
DOI: <https://doi.org/10.1070/RM1965v020n04ABEH001188>

Vladimir Aleksandrovich Molchanov

Saratov State University,
83 Astrakhanskaya str., Saratov 410012, Russia,
e-mail: v.molchanov@inbox.ru

Renat Abukhanovich Farakhutdinov

Saratov State University,
83 Astrakhanskaya str., Saratov 410012, Russia,
e-mail: renatfara@mail.ru

Объявление о Конкурсе 2025 года на соискание медали и премии имени Н.И. Лобачевского “За выдающиеся работы в области фундаментальной и прикладной математики”

Казанский федеральный университет объявляет очередной Конкурс на соискание медали и премии имени Н.И. Лобачевского “За выдающиеся работы в области фундаментальной и прикладной математики”.

Медаль имени Н.И. Лобачевского и соответствующая денежная премия в размере 75 000 (семьдесят пять тысяч) долларов США присуждаются Казанским федеральным университетом за выдающиеся работы в области фундаментальной и прикладной математики. Медаль и премия носят имя Николая Ивановича Лобачевского (1792–1856), гениального русского математика, основателя неевклидовой геометрии, ректора Казанского университета (1827–1845).

В конкурсе на соискание медали и премии имени Н.И. Лобачевского могут участвовать российские и зарубежные ученые персонально.

Право выдвижения кандидатов на соискание медали и премии предоставляется:

- а) академикам и членам-корреспондентам Российской академии наук и Академии наук Республики Татарстан, членам зарубежных государственных академий и государственных научных сообществ;
- б) российским и зарубежным научным учреждениям, высшим учебным заведениям;
- в) государственным научным и инженерно-техническим обществам;
- г) научным советам Российской академии наук и других ведомств по важнейшим проблемам науки;
- д) научно-техническим советам министерств, ведомств, высокотехнологичных компаний.

К участию в конкурсном отборе допускаются работы, освещающие результаты научных исследований, внесших значительный вклад в развитие фундаментальной и прикладной математики.

Медаль и премия, а также диплом об их присуждении, вручаются лицу, удостоенному награды, на торжественном заседании Ученого совета КФУ в конце ноября – начале декабря 2025 года по результатам мотивированного заключения жюри.

Выдвижение кандидатов для участия в конкурсном отборе принимаются по адресу электронной почты **medal@kpfu.ru** с момента публикации объявления о конкурсе. Интернет-адрес сайта медали и премии имени Н.И. Лобачевского:

<https://mathcenter.kpfu.ru/medal>

Организации или отдельные лица, выдвинувшие кандидата на соискание медали и премии, представляют в секретариат Конкурса (**medal@kpfu.ru**) следующую информацию (с пометкой “На соискание медали и премии имени Н.И. Лобачевского”):

- а) сведения об авторе (перечень основных научных работ, открытий, изобретений, место работы и занимаемая должность, домашний адрес, номера служебного и домашнего телефонов);
- б) опубликованную научную работу (серию работ) или ссылки на них, материалы научного открытия или изобретения;
- в) мотивированное представление, включающее научную характеристику работы, ее значение для развития науки и народного хозяйства.

Прием работ осуществляется **до 30 июня 2025 года** включительно. Работы, представленные на конкурс, не возвращаются.

Победитель конкурса будет определен **до 30 сентября 2025 года**.

Медаль, а также диплом о присуждении медали и соответствующая денежная премия вручаются лицу, удостоенному награды, по результатам мотивированного заключения Международного жюри конкурса на торжественном заседании Ученого совета КФУ в конце ноября — начале декабря 2025 года. Церемония вручения состоится в Александровском зале Казанского федерального университета. Медаль и премию вручают Председатель Попечительского совета и Председатель Ученого совета Казанского федерального университета.