

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 $\text{exr}_\emptyset \mathfrak{A}$, включая пустое множество. Однако, если хотя бы один из аргументов функции f в алгебре $\text{exr}_\emptyset \mathfrak{A}$ 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 $\text{exr}_\emptyset \mathfrak{A}$ подалгебру $\text{exr } \mathfrak{A}$. Если среди операций есть хоть одна f , имеющая местность два или больше, то пустое множество в $\text{exr}_\emptyset \mathfrak{A}$ определимо:

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

Следовательно, определима и подалгебра $\text{exr } \mathfrak{A}$. При этом, в силу однозначной определенности операций над пустым множеством, выразительная сила и алгоритмические свойства алгебр $\text{exr}_\emptyset \mathfrak{A}$ 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*

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

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 бесконечномерности $\mathfrak{L}$ 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/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] 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, algorithmin 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