УДК 510.65, 512.531.4

О ТЕОРИИ МОНОИДА КОНЕЧНЫХ ПОДМНОЖЕСТВ ДЛЯ ОДНОЙ АБЕЛЕВОЙ ГРУППЫ КРУЧЕНИЯ[1]

Дудаков С.М.
Тверской государственный университет, г. Тверь

Поступила в редакцию 15.04.2021, после переработки 15.05.2021.

Ранее был доказан следующий результат: если абелева группа $\mathfrak{G}$ не является группой кручения, то теория моноида ее конечных подмножеств позволяет интерпретировать элементарную арифметику. В настоящей работе мы приводим пример, который показывает, что аналогичный результат можно получить и, по крайней мере, для некоторых групп кручения.

Ключевые слова: группа кручения, моноид подмножеств, элементарная арифметика, неразрешимость.

Вестник ТвГУ. Серия: Прикладная математика. 2021. № 2. С. 39–55.
https://doi.org/10.26456/vtpmk615

Введение

Изучение алгоритмических особенностей логических языков для алгебраических систем является одной из центральных проблем математической логики. Эта отрасль имеет глубокие связи с практикой, так как тесно соотносится с теорией запросов к базам данных. Например, традиционная ныне реляционная модель базы данных фактически представляет собой конечную алгебраическую систему, которая вложена в бесконечный универсум — предметную область. Такой подход идёт ещё от основополагающих работ Э. Кодда [4] и П. Канеллакиса [10]. Язык запросов в этом случае является тем или иным диалектом языка логики первого порядка или её расширений, что тоже восходит к Э. Кодду. Поскольку при вложении базы данных в универсум может появиться возможность оперировать произвольными элементами последнего, то мы оказываемся в ситуации, когда формулы логического языка нужно анализировать для произвольной алгебраической системы.

Современные системы управления базами данных допускают широкие возможности в использовании сложных типов данных. Наряду с традиционными атомными типами (числами, строками) они позволяют оперировать массивами, множествами и более сложными структурами. С точки зрения математики такие данные таких типов представляют собой множества, векторы и другие объекты, которые

[1]Работа выполнена при финансовой поддержке РФФИ, проект 20-01-00435.

можно образовывать из атомных элементов универсума. Таким образом, универсум базы данных может состоять из производных объектов, например, подмножеств какого-то иного, исходного универсума.

Если рассматривать теории таких, производных систем по сравнению с исходными, то результаты могут весьма разниться. Например, одно из доказательств разрешимости арифметики Скулема заключается в представлении её в виде прямой суммы счётно бесконечного количества экземпляров арифметики Пресбургера [11], то есть множества векторов из натуральных чисел. Если в качестве исходного универсума взять множество строк, то его подмножества будут языками [9]. Некоторые результаты об алгоритмических свойствах алгебры языков получены в [6,7]. В зависимости от множества рассматриваемых операций могут получаться как разрешимые, так и неразрешимые теории.

Нужно уточнить, что рассмотрение алгебры подмножеств неэквивалентно монадической логике второго порядка [3, 12]. Дело в том, что язык этой алгебры может не содержать средств, позволяющих выделить объекты первого порядка или их эквиваленты. Например, в [1] построен пример, в котором теория алгебры подмножеств оказывается алгоритмически проще исходной, что для логики второго порядка невозможно.

В настоящей работе мы рассматриваем алгоритмические свойства теории конечных подмножеств, когда универсумом является одна из наиболее важных групп кручения — аддитивная группа рациональных чисел по модулю 1. Сами по себе группы кручения часто возникают в информатике, например, для ограниченных типов данных. Тривиальный пример — ограниченные (одно-, двух-, четырёхбайтовые и т. д.) целочисленные значения с операцией сложения, они как раз дают пример циклической группы. Составленные из них конечные векторы образуют с поэлементными операциями уже бесконечную группу кручения.

Ранее, в работах [2, 5, 8], мы уже рассматривали вопрос о выразительных возможностях алгебры конечных подмножеств некоторых моноидов. В [8] было доказано, что теория таких моноидов позволяет интерпретировать элементарную арифметику, в частности, она неразрешима. Условия, которые накладывались на исходные моноиды, были следующими: они должны быть коммутативными, допускать сокращение и иметь хотя бы один элемент бесконечного порядка. Например, такими моноидами являются все абелевы группы, которые не являются группами кручения. Вместе с тем не все перечисленные условия будут необходимыми для справедливости теоремы. Например, в работах [2] и [5] продемонстрировано, что то же самое выполняется для любых свободных моноидов, то есть моноидов слов с конкатенацией. Очевидно, что в случае неодносимвольных алфавитов коммутативность отсутствует.

Поэтому в [8] в качестве одного из открытых вопросов сформулирован такой: определить являются ли необходимыми остальные условия? В частности, необходимо ли наличие элемента бесконечного порядка? Иными словами, может ли для абелевой группы кручения моноид её конечных подмножеств позволять интерпретировать элементарную арифметику. Методы интерпретации, которые были использованы в предыдущих работах [5, 8], для групп кручения принципиально не подходят, так как базируются именно на некотором элементе бесконечного порядка и порожденных им.

В настоящей работе мы показываем, что, тем не менее, сформулированная вы-

ше теорема может быть справедлива и для групп кручения. Мы рассматриваем аддитивную группу рациональных чисел по модулю 1, или, что эквивалентно, полную группу корней из единицы на комплексной плоскости. Мы доказываем, что аддитивная алгебра конечных подмножеств этой группы позволяет интерпретировать элементарную арифметику.

1. Определения

Рассмотрим аддитивную группу $\mathfrak{Q} = (\mathbb{Q}, +, -, 0)$ рациональных чисел по модулю 1. Множество $\mathbb{Q}$ состоит из рациональных чисел, принадлежащих промежутку $[0; 1)$. Бинарной операцией является сложение $+$, если результат при этом будет больше или равен единице, то от него берётся дробная часть. Изоморфной является полная мультипликативная группа корней из единицы на комплексной плоскости.

Как обычно для аддитивных групп при помощи na или $n \cdot a$ для натурального n обозначаем кратную сумму:

$$na = \underbrace{a + \cdots + a}_{n}.$$

Группа $\mathfrak{Q}$ является группой кручения, так как для любого рационального $a = \frac{p}{q}$, получим $qa = q \cdot \frac{p}{q} = 0$. Очевидным является такое свойство: эта группа содержит элементы всех натуральных порядков. Порядок элемента a группы обозначаем с помощью $\operatorname{ord} a$.

Далее для удобства мы будем использовать буквы начала латинского алфавита a, b, c, d, e для обозначения элементов исходной группы; буквы конца алфавита u, v, w, x, y, z — для обозначения конечных подмножеств, составленных из этих элементов; буквы $i, j, k, \ell, m, n, p, q$ — для натуральных чисел, о чём иногда не будем специально упоминать.

Наше внимание будет сосредоточено на изучении моноида конечных подмножеств группы $\mathfrak{Q}$ с той же операцией $+$. Иными словами, носителем алгебры будет множество конечных подмножеств $\mathbb{Q}$, а операция над этими подмножествами определена так:

$$x + y = \{a + b : a \in x, b \in y\}.$$

Если одно из множеств является одноэлементным, то вместо $x + \{a\}$ или $\{a\} + y$ мы будем писать просто $x+a$ и $a+y$ соответственно. Аналогичным образом запись $x-a$ означает $x+\{-a\}$. Иными словами, при помощи $x \pm a$ мы обозначаем результат действия группы $\mathfrak{Q}$ на множестве своих подмножеств простыми сдвигами.

Нейтральным элементом является множество, состоящее из одного нуля: $E = \{0\}$. Поэтому полагаем $0x = E$.

Очевидно, что нулем в этом моноиде является пустое множество: $x + \varnothing = \varnothing$. С другой стороны, из непустых множеств с помощью $+$ пустое никогда не получится, поэтому непустые множества образуют определимый подмоноид $\mathfrak{Q}^* = (\mathbb{Q}^*, +, E)$, который мы и будем далее изучать.

Как и в любом моноиде определимы нейтральный элемент:

$$x = E \equiv (\forall y) x + y = y,$$

а также множество I обратимых элементов:

$$I(x) \equiv (\exists y)x + y = E.$$

2. Общие свойства подмножеств абелевых групп кручения

В этом параграфе мы рассматриваем несколько более общую ситуацию: произвольную аддитивную абелеву группу кручения $\mathfrak{G} = (G, +, -, 0)$ и моноид $\mathfrak{G}^*$ её непустых конечных подмножеств.

Подмножества в группах кручения. Установим ряд свойств элементов $\mathfrak{G}^*$.

Лемма 1. *Если x содержит 0, то $y \subseteq x + y$.*

Доказательство. Если $x = E \cup x'$, то $y = y + E \subseteq (y + E) \cup (y + x') = y + x$. □

Лемма 2. *Если x является подгруппой $\mathfrak{G}$, то $y+x = x$ выполнено тогда и только тогда, когда $y \subseteq x$.*

Доказательство. Так как x содержит 0, то из $x + y = x$ по предыдущей лемме получаем $y \subseteq x + y = x$. Обратное тривиально. □

Лемма 3. *Обратимыми элементами в $\mathfrak{G}^*$ являются в точности одноэлементные множества.*

Доказательство. Очевидно $\{a\}+\{-a\} = \{0\} = E$. Если x содержит два элемента, то $x+y$ тоже будет содержать не менее двух элементов, то есть не может совпадать с E. □

Лемма 4. *Равенство $x + x = x$ выполнено в моноиде $\mathfrak{G}^*$ тогда и только тогда, когда x — подгруппа в $\mathfrak{G}$.*

В частности, из $x + x = x$ следует $0 \in x$.

Доказательство. Пусть $x + x = x$, a, b — любые элементы x, тогда, очевидно, $a + b \in x + x = x$. Далее получаем $2a = a + a \in x + x = x$, $3a = 2a + a \in x + x = x$ и т. д. Следовательно, $na \in x$ для всех n, в частности, если $\operatorname{ord} a = q$, то $0 = qa \in x$ и $-a = (q - 1)a \in x$.

Обратное утверждение тривиально. □

Лемма 5. *Пусть x — конечное множество, содержащее 0. Тогда существует положительное натуральное число n такое, что $nx = (n + 1)x$.*

Доказательство. Если $x = \{0\}$, то $1x = 2x$.

В противном случае пусть x состоит из нуля и ненулевых элементов $a_1, \ldots, a_k$, где $\operatorname{ord} a_i = q_i$ для $i = 1, \ldots, k$. Тогда mx состоит в точности из сумм вида $j_1a_1 + \cdots + j_ka_k$, где $j_1 + \cdots + j_k \leq m$. Так как каждое из слагаемых j_ia_i может принимать q_i разных значений, то общее количество таких сумм не превосходит произведения $q_1 \ldots q_k$. Следовательно, всевозможных значений для mx конечно много. С другой стороны, так как $0 \in x$, то по лемме 1 имеем $mx \subseteq mx + x = (m + 1)x$, поэтому множества mx образуют неубывающую последовательность. Значит, на некотором шаге мы получим $mx = (m + 1)x$. □

Следствие 1. *Указанное в лемме множество* $y = nx = (n+1)x$ *является подгруппой, порожденной* x.

Доказательство. Из $nx + x = nx$ по индукции вытекает $nx + nx = nx$, по лемме 4 это означает, что nx — подгруппа.

С другой стороны, любая подгруппа z, включающая x, должна включать и все mx, следовательно, $nx \subseteq z$. □

Далее порождённую непустым множеством $x \subseteq G$ подгруппу обозначаем с помощью $\langle x \rangle$.

Лемма 6. *Пусть* x *— конечное множество. Тогда порожденная* x *подгруппа* $y = \langle x \rangle$ *— это наименьшее множество* y*, удовлетворяющее условиям* $x + y = y + y = y$.

Доказательство. Для $\langle x \rangle$ равенства $x + \langle x \rangle = \langle x \rangle + \langle x \rangle = \langle x \rangle$ непосредственно получаются из определения порождённой подгруппы.

Согласно лемме 4 из $y + y = y$ вытекает, что y — подгруппа. Так как $0 \in y$, то $x \subseteq x + y = y$. Следовательно, $\langle x \rangle \subseteq y$, а наименьшим из таких y и является подгруппа $\langle x \rangle$. □

Следствие 2. *Порожденная* x *подгруппа* $\langle x \rangle$ *определима в логике первого порядка в алгебре* $\mathfrak{G}^*$.

Доказательство. Определяющей формулой является:

$$y = \langle x \rangle \equiv y + y = y \wedge y + x = y \wedge (\forall z)(z + z = z \wedge z + x = z \to y + z = z).$$

Поскольку из $z + z = z$ вытекает, что z — подгруппа, то заключение импликации эквивалентно $y \subseteq z$ (лемма 2). □

Определение 1 (Ядро множества x, $\ker x$)**.** Ядром *множества* x *назовём наименьшую подгруппу* $\mathfrak{H}$ *такую, что* x *включено в один из смежных классов по* $\mathfrak{H}$. *Обозначаем ядро с помощью* $\ker x$.

Следствие 3. $\ker x \subseteq \langle x \rangle$.

Доказательство. Для $\langle x \rangle$ очевидно выполнено $x \subseteq 0 + \langle x \rangle$, поэтому $\ker x \subseteq \langle x \rangle$ по определению. □

Лемма 7. *Для любого множества* x *ядро* $\ker x$ *существует.*

Доказательство. Пусть $a \in x$. Рассмотрим совокупность всех подгрупп $\mathfrak{H}_i$, $i \in J$, обладающих необходимым свойством, то есть $x \subseteq a + \mathfrak{H}_i$ для всех $i \in J$. Следовательно,

$$x \subseteq \bigcap_i (a + \mathfrak{H}_i) = a + \bigcap_i \mathfrak{H}_i = a + \mathfrak{H}$$

для некоторой подгруппы $\mathfrak{H}$, которая и будет наименьшей, то есть ядром x. □

Следствие 4. *Если* $0 \in x$*, то* $\ker x = \langle x \rangle$.

Доказательство. Взяв 0 в качестве a в доказательстве леммы 7, мы получим $\mathfrak{H} = \bigcap\limits_i \mathfrak{H}_i$ для всех $\mathfrak{H}_i$, включающих x. Но последнее пересечение по определению и является порождённой x подгруппой $\langle x\rangle$. □

Лемма 8. *Если $a \in x$, то $\ker x = \langle x - a\rangle$ и эта подгруппа является наименьшей среди всевозможных $\langle x - b\rangle$, $b \in G$.*

Доказательство. Очевидно, что $\ker x = \ker(x - b)$ для любого $b \in G$, так как $x \subseteq a + \mathfrak{H}$ тогда и только тогда, когда $x - b \subseteq (a - b) + \mathfrak{H}$ для произвольной подгруппы $\mathfrak{H}$. С другой стороны, при $a \in x$ мы получаем $0 \in x - a$, согласно следствию 4 имеем $\ker x = \ker(x - a) = \langle x - a\rangle$.

Для произвольного $b \in G$ получаем $\ker x = \ker(x - b) \subseteq \langle x - b\rangle$. □

Следствие 5. *Ядро множества определимо в логике первого порядка в моноиде подмножеств $\mathfrak{G}^*$.*

Доказательство. Определяющей формулой является:

$$y = \ker x \equiv (\exists u)\Big(I(u) \wedge y = \langle x - u\rangle \wedge (\forall v)(I(v) \to \langle x - u\rangle + \langle x - v\rangle = \langle x - v\rangle)\Big).$$

Равенство $\langle x - u\rangle + \langle x - v\rangle = \langle x - v\rangle$ эквивалентно включению $\langle x - u\rangle \subseteq \langle x - v\rangle$, поскольку $0 \in \langle x - v\rangle$. □

Лемма 9. *Для любого x равенство $\langle x\rangle = \ker x$ имеет место тогда и только тогда, когда $\langle x\rangle = nx$ для всех натуральных n, начиная с некоторого.*

Доказательство. Пусть $\langle x\rangle = \ker x$, это означает $\langle x\rangle = \ker x = \langle x - a\rangle$ для любого $a \in x$ согласно лемме 8. Используя следствие 1, получим $\langle x - a\rangle = n(x - a)$ для всех n, начиная с некоторого n_0, так как $0 \in x - a$. Из $a \in x$ получаем $na \in \langle x\rangle$ для всех n, поэтому для всех $n \geq n_0$ мы получим

$$nx = n(a + (x - a)) = na + n(x - a) = na + \langle x - a\rangle = na + \langle x\rangle = \langle x\rangle\,,$$

что и требуется.

Пусть теперь $\langle x\rangle = nx$ для всех n, начиная с некоторого n_0. Возьмём любой $b \in G$, $\operatorname{ord} b = q$. Тогда для любого n большего n_0 и кратного q мы получим $n(x-b) = nx-nb = \langle x\rangle$, следовательно, $\langle x\rangle = n(x-b) \subseteq \langle x - b\rangle$. Итак, $\langle x\rangle$ является наименьшем среди всевозможных $\langle x - b\rangle$. По лемме 8 получаем $\ker x = \langle x\rangle$. □

Определимость в $\mathfrak{G}^*$. Следующим нашим шагом будет показать возможность определения в моноиде $\mathfrak{G}^*$ двухэлементных подмножеств и кратных им.

Лемма 10. *Для каждого n существует формула O_n такая, что $O_n(x)$ истинна в моноиде $\mathfrak{G}^*$ в том и только том случае, когда $\ker x$ содержит элемент порядка n или больше.*

Доказательство. Очевидно,

$$O_n(x) \equiv (\exists z)\Big(z + \ker x = \ker x \wedge I(z) \wedge \bigwedge_{i=1}^{n-1} iz \neq E\Big).$$ □

Лемма 11. *Для каждого n существует формула A_n такая, что $A_n(x)$ истинна в моноиде $\mathfrak{G}^*$ в том и только том случае, когда* $\ker x$ *содержит ровно n элементов.*

Доказательство. Очевидно,

$$A_n(x) \equiv (\exists z_1, \ldots, z_n)\Big(\bigwedge_{i\neq j} z_i \neq z_j \wedge \bigwedge_i \big(z_i + \ker x = \ker x \wedge I(z_i)\big) \wedge$$
$$\wedge\, (\forall z)\Big(\big(z + \ker x = \ker x \wedge I(z)\big) \to \bigvee_i z = z_i\Big)\Big). \qquad \square$$

Лемма 12. *Пусть* $\ker x$ *содержит только элементы порядка* 4 *или меньше. Множество x содержит два элемента тогда и только тогда, когда выполнено одно из условий*

1. $\ker x$ *содержит два элемента и $x = a + \ker x$ для некоторого $a \in G$;*
2. $\ker x$ *содержит три элемента,* $\ker x = \langle z\rangle = 2z$ *и $x = a + z$ для некоторых $z \neq \ker x$ и $a \in G$;*
3. $\ker x$ *содержит четыре элемента,* $\ker x = \langle z\rangle = 3z \neq 2z$ *и $x = a + z$ для некоторых z и $a \in G$.*

Доказательство. Пусть $x = a + \{0, b\}$. Тогда $\ker x = \langle 0, b\rangle$ и состоит из всевозможных элементов вида nb. По условию $\operatorname{ord} b \leq 4$, поэтому

- при $\operatorname{ord} b = 2$ получаем $\ker x = \{0, b\}$ и $x = a + \ker x$;
- при $\operatorname{ord} b = 3$ получаем $\ker x = \{0, b, 2b\}$, поэтому для $z = \{0, b\} \neq \ker x = \langle z\rangle$ имеем $x = a + z$, $\ker x = 2z$;
- при $\operatorname{ord} b = 4$ выполнено $\ker x = \{0, b, 2b, 3b\}$, поэтому для $z = \{0, b\}$ имеем $x = a + z$, $\ker x = \langle z\rangle = 3z$, $\ker x \neq 2z = \{0, b, 2b\}$.

Докажем утверждение в обратную сторону. Если $x = a + \ker x$, где $\ker x$ содержит два элемента, то x, очевидным образом, тоже содержит два элемента.

Если выполнен пункт 2), то $\ker x = \{0, b, 2b\}$ для некоторого b, так как любая группа порядка три является циклической. Получаем $z \subseteq \langle z\rangle = \ker x$, то есть z содержит не больше трёх элементов. Так как $2z = \ker x$, то z не может содержать один элемент. С другой стороны, z не может содержать три элемента, так как в этом случае $z = \ker x$. Поэтому z, как и x, содержит два элемента.

Пусть, наконец, выполнен пункт 3). Как и в предыдущем случае получаем $z \subseteq \langle z\rangle = \ker x$, то есть z содержит не больше четырёх элементов, но при этом не может содержать ровно один элемент или ровно четыре элемента. Допустим, что z содержит три элемента d_1, d_2, d_3, но не содержит $d_0 \in \langle z\rangle$. Так как из любой пары неравных элементов $d_i - d_1$ и $d_i - d_2$, $i = 0, 1, 2, 3$, множество z содержит хотя бы один, то $2z$ содержит все $d_i = (d_i - d_j) + d_j$, $j = 1, 2$, то есть совпадает с $\ker x$, что невозможно. Поэтому единственный возможный случай — z, как и x, содержит два элемента. $\square$

Лемма 13. *Пусть* $\ker x$ *содержит хотя бы один элемент порядка* 5 *или больше. Множество* x *содержит два элемента тогда и только тогда, когда кроме* $2x$ *существует еще ровно одно множество* u*, для которого* $3x = u + x$*.*

Доказательство. Пусть $x = a + \{0, b\}$, где $b \neq 0$. Сразу отметим, что в этом случае $\ker x$ состоит всех кратных b. В частности, это означает, что $\operatorname{ord} b \geq 5$.

Получаем $2x = 2a + \{0, b, 2b\}$. Положим $u = 2a + \{0, 2b\}$. Очевидно, $u \neq x$ и при этом $u + x = 3a + \{0, b, 2b, 3b\} = 3x$.

Допустим теперь, что $3x = v + x$ для некоторого v. Тогда $3a + \{0, b, 2b, 3b\} = a + (v \cup (b + v))$ и $2a + \{0, b, 2b, 3b\} = v \cup (b + v)$. Следовательно, $v \subseteq 2a + \{0, b, 2b, 3b\}$ и $b + v \subseteq 2a + \{0, b, 2b, 3b\}$. Последнее означает $v \subseteq 2a + \{0, b, 2b, -b\}$. Так как $\operatorname{ord} b \geq 5$, то $4b \neq 0$ и $3b \neq -b$. Поэтому $v \subseteq (2a + \{0, b, 2b, 3b\}) \cap (2a + \{0, b, 2b, -b\}) = 2a + \{0, b, 2b\}$. Так как $3x = v + x$, x содержит два элемента, а $3x$ — четыре, то v должно состоять как минимум из двух элементов. Поэтому есть четыре возможных значения для v:

- $v = 2a + \{0, b\}$, $v + x = 3a + \{0, b, 2b\} \neq 3x$;
- $v = 2a + \{0, 2b\} = u$, $v + x = 3a + \{0, b, 2b, 3b\} = 3x$;
- $v = 2a + \{b, 2b\}$, $v + x = 3a + \{b, 2b, 3b\} \neq 3x$;
- $v = 2a + \{0, b, 2b\} = 2x$, $v + x = 3a + \{0, b, 2b, 3b\} = 3x$.

Таким образом, v может принимать всего два значения: $2x$ и u, что и требуется.

Докажем теперь противоположное утверждение. Допустим, x содержит только один элемент a, тогда $3x = \{3a\}$ и равенство $u + x = 3x$ возможно только при $u = \{2a\} = 2x$, что противоречит условию.

Теперь допустим, что x содержит как минимум три элемента: $x = \{a, b, c, \dots\}$, где $a \neq b \neq c \neq a$. Рассмотрим множества $2x$, $u = 2x \setminus \{a + b\}$, $v = u \setminus \{a + c\}$. Так как $b \neq c$, то $a + c \neq a + b$, поэтому множества $2x, u, v$ попарно различны. Очевидно, $v \subseteq u \subseteq 2x$, поэтому $v + x \subseteq u + x \subseteq 2x + x = 3x$.

Покажем, что $3x \subseteq v + x$. Множество $3x$ состоит из всевозможных тройных сумм элементов x. Рассмотрим суммы вида $(a + b) + d \in 3x$, для которых первое слагаемое $a + b$ не принадлежит v. Есть следующие варианты:

- $d = a$. Так как a отличается от b и c, то $a + a$ отличается от $a + b$ и $a + c$, поэтому $a + a \in v$ и мы получаем $(a + b) + a = (a + a) + b \in v + x$.
- $d \neq a$ и $d + b \neq a + c$. Так как a отличается от d, то $d + b$ отличается от $a + b$, поэтому $d + b \in v$ и мы получаем $(a + b) + d = (d + b) + a \in v + x$.
- $d \neq a$ и $d + b = a + c$. Как и в первом случае $a + a \in v$, поэтому получаем $(a + b) + d = (d + b) + a = (a + c) + a = (a + a) + c \in v + x$.

Аналогично рассматриваются суммы вида $(a+c)+d$. Для сумм иных видов никаких преобразований не требуется.

Следовательно, кроме $2x$ существуют как минимум два множества u и v, для которых $3x = u + x = v + x$, что противоречит условию. □

Комбинируя две предыдущие леммы мы получаем

Теорема 1. *В моноиде $\mathfrak{G}^*$ существует формула $D(x)$, выделяющая в точности двухэлементные множества.*

Доказательство. Согласно леммам 12 и 13 в качестве искомой формулы может быть взята следующая:

$$\begin{aligned} D(x) \equiv \neg O_5(x) \wedge \Big(& A_2(x) \wedge (\exists a)(I(a) \wedge x = a + \ker x) \vee \\ & \vee A_3(x) \wedge (\exists a, z)(I(a) \wedge x = a + z \wedge \ker x = 2z \wedge \ker x \neq z \wedge \ker x = \langle z \rangle) \vee \\ & \vee A_4(x) \wedge (\exists a, z)(I(a) \wedge x = a + z \wedge \ker x = 3z \wedge \ker x \neq 2z \wedge \ker x = \langle z \rangle) \Big) \vee \\ & \vee O_5(x) \wedge (\exists u)\Big(3x = u + x \wedge u \neq 2x \wedge (\forall v)\big(3x = v + x \to v = 2x \vee v = u\big)\Big). \end{aligned}$$ □

Рассмотрим формулу

$$P(y, x) \equiv y + x \neq y \wedge (\forall u, v)\big(u + v = y \wedge \neg I(v) \to (\exists w) u + w + x = y\big).$$

Лемма 14. *Пусть x содержит два элемента, $\langle x \rangle = \ker x$ и формула $P(y, x)$ истинна в моноиде $\mathfrak{G}^*$. Тогда $y = mx + a$ для некоторых натурального m и $a \in G$.*

Доказательство. Согласно лемме 9 из $\langle x \rangle = \ker x$ вытекает $\langle x \rangle = nx$ для всех натуральных n, начиная с какого-то n_0.

Допустим, что формула $P(y, x)$ истинна. Если y обратим, то $y = \{a\}$ и $y = 0x + a$ для какого-то $a \in G$.

Пусть теперь y необратим. Тогда $y = E + y$ и, благодаря импликации, получаем $y = E + w_1 + x = w_1 + x$ для некоторого w_1. Если w_1 необратим, то из $y = x + w_1$ таким же образом получаем $y = x + w_2 + x = w_2 + 2x$. По индукции получим $y = w_m + mx$ для произвольного натурального m и подходящего w_m. Если для некоторого m получим обратимый $w_m = \{a\}$, то $y = mx + a$, что и требуется.

В противном случае для $m = n_0$ имеем $y = w_{n_0} + n_0 x = w_{n_0} + \langle x \rangle$. Но тогда $y + x = w_{n_0} + \langle x \rangle + x = w_{n_0} + \langle x \rangle = y$, что противоречит формуле $P(y, x)$. □

Лемма 15. *Пусть $x = \{0, d\}$, $y = \{0, d, 2d, \ldots, md\}$, $u, v \subseteq y$, $u + v = y$, где $d \in G$ и $m > 0$. Пусть также $\operatorname{ord} d > 2m$, а v необратим. Тогда $y = u + nx$ для некоторого натурального $n > 0$.*

Доказательство. Сразу отметим: из $\operatorname{ord} d > 2m$ вытекает, что все $0, d, 2d, \ldots, 2md$ попарно различны.

Так как $u, v \subseteq y = mx$, то мы можем выбрать числа $n_1 \leq m$ — наименьшее, для которого $u \subseteq n_1 x$, и $n_2 \leq m$ — наименьшее, для которого $v \subseteq n_2 x$. Заметим, что $n_1 d \in u$. В самом деле, выберем наибольшее $n_1' \geq 0$, для которого $n_1' d \in u$. Если предположить, что $n_1' < n_1$, то $u \subseteq \{0, d, 2d, \ldots, n_1' d\} = n_1' x$, что противоречит минимальности n_1. Если предположить, что $n_1' > n_1$, то u не может быть подмножеством $n_1 x$, поскольку $n_1' d \in u \setminus n_1 d$. Следовательно, $n_1' = n_1$ и $n_1 d \in u$. Аналогично доказывается, что $n_2 d \in v$. Так как v необратим, то v не является подмножеством $\{0\} = 0x$, поэтому $n_2 > 0$.

Поскольку $n_1 d \in u$ и $n_2 d \in v$, то $(n_1 + n_2)d = n_1 d + n_2 d \in u + v = y$. Из $n_1, n_2 \leq m$ получаем $n_1 + n_2 \leq 2m$. Но $(m+1)d, \ldots, 2md$ попарно не совпадают ни с какими из $0, d, 2d, \ldots, md$, поэтому $(m+1)d, \ldots, 2md$ не принадлежат y, значит,

$n_1 + n_2 \leq m$. С другой стороны, n_1 и n_2 являются наибольшими коэффициентами при d в множествах u и v соответственно, поэтому наибольший коэффициент при d в множестве $u + v$ будет равен $n_1 + n_2$ и мы получаем $n_1 + n_2 = m$.

Из определения n_2 сразу получаем включение $y = u + v \subseteq u + n_2 x$. Пусть теперь $kd \in u + n_2 x$, следовательно, $k = k_1 + k_2$, где $k_1 \leq n_1$ и $k_2 \leq n_2$. Получаем $k = k_1 + k_2 \leq n_1 + n_2 = m$. Значит, $kd \in y$. □

Лемма 16. *Пусть x содержит два элемента и $\langle x \rangle = \ker x$. Тогда для y следующие два условия эквивалентны:*

1. *y можно представить в виде $y = 2z + b$ или $y = 2z + x + b$ для некоторых $b \in G$ и z, для которого в $\mathfrak{G}^*$ выполнено $P(z, x)$;*

2. *y можно представить в виде $y = nx + a$ для некоторых натурального n и $a \in G$.*

Доказательство. Продемонстрируем, что из условия 1) следует 2). Пусть выполнено $P(z, x)$. Тогда по лемме 14 получаем $z = m'x + a'$ для некоторых m' и a'. Следовательно, возможны следующие два случая:

$$y = 2z + b = 2m'x + (2a' + b) \qquad \text{или}$$
$$y = 2z + x + b = (2m' + 1)x + (2a' + b).$$

Таким образом, y в любом случае имеет нужный вид из пункта 2).

Докажем теперь обратное: возьмём $y = nx + a$. Пусть $x = c + \{0, d\}$. Тогда $y = nx + a = nc + a + \{0, d, 2d, \ldots, md\}$. При этом мы полагаем, что все 0, d, $2d$, $\ldots$, md попарно различны, поэтому, возможно, $m < n$. Тогда $\operatorname{ord} d > m$. Если число m чётно, то положим $z = \{0, d, 2d, \ldots, \frac{m}{2}d\}$ и мы получим $y = 2z + (nc + a)$. Если же число m является нечётным, то положим $z = \{0, d, 2d, \ldots, \frac{m-1}{2}d\}$ и получим $y = 2z + x + (nc + a)$.

Осталось доказать, что в каждом из случаев выполнено $P(z, x)$. Будем рассматривать случай чётного m, для нечётного изменения будут заключаться только в замене $\frac{m}{2}$ на $\frac{m-1}{2}$. Сначала проверим условие $z + x \neq z$:

$$z + x = c + \Big\{0, d, 2d, \ldots, \frac{m}{2}d, \Big(\frac{m}{2} + 1\Big)d\Big\}.$$

Так как все $0, d, 2d, \ldots, md$ попарно различны и $\frac{m}{2} \leq m$, то единственный вариант, при котором $z + x = z$, заключается в том, что $(\frac{m}{2} + 1)d = 0$. Но это может быть только при $\frac{m}{2} = m$, то есть $m = 0$. Тогда $z = \{0\}$ и мы получаем $z + x = x \neq z$, что противоречит предположению $z + x = z$. Следовательно, $z + x \neq z$ в любом случае.

Наконец, проверим справедливость импликации. Допустим, $u + v = z$. Если z обратим, то u и v тоже обратимы, следовательно, условие импликации не может быть выполнено, а вся импликация истинна.

Пусть теперь v (и, следовательно, z) необратим. Возьмём $u' = u - e'$, где $e' \in u$, тогда множество u' содержит 0. Положим $v' = v + e'$. Тогда $u' + v' = u + v = z$. Так как $0 \in u'$, то $v' \subseteq u' + v' = z$, в частности, последнее включение означает, что v' состоит из элементов вида id. Выберем среди них kd — элемент с наименьшим k, — и положим $v'' = v' - kd$. Тогда $v'' \subseteq z$ и при этом v'' содержит 0. Далее получаем

$v'' = v' - kd = v - kd + e'$. Возьмём $u'' = u + kd - e'$. Тогда $u'' + v'' = u + v = z$. Так как v'' содержит 0, то $u'' \subseteq z$. Итак, $u'', v'' \subseteq z$ и $u'' + v'' \subseteq z$, где $z = \{0, d, 2d, \ldots, \frac{m}{2}d\}$. По лемме 15 получаем $u'' + \ell\{0, d\} = z$ для некоторого $\ell > 0$. Но тогда

$$z = u'' + \ell\{0, d\} = u + kd - e' + \ell(x - c) = u + ((\ell - 1)x - \ell c + kd - e') + x,$$

что и требуется. □

Теорема 2. *Существует формула $K(y, x)$, которая в моноиде $\mathfrak{G}^*$ означает:*

1. *x — двухэлементное множество;*
2. *для x выполнено $\ker x = \langle x \rangle$;*
3. *$y = nx + a$ для некоторого $a \in G$.*

Доказательство. В силу теоремы 1 и леммы 16 получаем

$$K(y, x) \equiv D(x) \wedge \ker x = \langle x \rangle \wedge \\ \wedge (\exists z, b)\Big(I(b) \wedge P(z, x) \wedge (y = 2z + b \vee y = 2z + x + b)\Big).$$ □

3. Интерпретация арифметики

Сейчас мы возвращаемся от произвольной абелевой группы кручения $\mathfrak{G}$ к конкретной группе $\mathfrak{Q} = (\mathbb{Q}, +, -, 0)$ и моноиду её непустых подмножеств $\mathfrak{Q}^*$. Сразу напомним, что все подгруппы $\mathfrak{Q}$ являются циклическими.

Нашей задачей будет построить в моноиде $\mathfrak{Q}^*$ интерпретацию элементарной арифметики. Для этого мы проинтерпретируем операции умножения и прибавления единицы.

Областью нашей интерпретации V будут подгруппы $\mathfrak{Q}$. Множество всех таких подгрупп определяется с помощью ker:

$$V(x) \equiv (\exists z)x = \ker z.$$

Положительное натуральное число n мы будем интерпретировать с помощью $\left\langle \frac{1}{n} \right\rangle$ — подгруппы n-го порядка. Заметим, что в $\mathfrak{Q}$ такая подгруппа единственна и состоит из всех дробей со знаменателем n. В моноиде $\mathfrak{Q}^*$ она легко определима:

$$x = \left\langle \frac{1}{n} \right\rangle \equiv V(x) \wedge A_n(x),$$

поскольку $\ker x = x$ для подгрупп. Очевидным образом определяется отношение делимости:

$$x \mid y \equiv V(x) \wedge V(y) \wedge x + y = y.$$

Из последнего легко получить определение взаимной простоты:

$$C(x, y) \equiv (\forall u)(u \mid x \wedge u \mid y \to u = E).$$

Далее, в такой интерпретации мы легко можем определить умножение для взаимно простых чисел:

$$M_c(x,y,z) \equiv V(y) \wedge V(z) \wedge C(y,z) \wedge x = y + z,$$

поскольку сумма двух подгрупп взаимно простых порядков является прямой, порядок результата равен произведению порядков исходных подгрупп.

Последнее, что мы определим, прежде чем окончательно перейти к арифметике, — это обычное отношение линейного порядка:

$$\begin{aligned} L(x,y) \equiv V(x) \wedge (\exists y', z', z)\Big(&D(y') \wedge y = \ker y' \wedge \ker z' + x = \ker z' \wedge \\ &\wedge \ker z' + y = \ker z' \wedge K(z,z') \wedge K(z+y',z') \wedge \\ &\wedge (\forall x')\big(D(x') \wedge x = \ker x' \to \neg K(x'+z,z')\big)\Big). \end{aligned}$$

Лемма 17. *Формула $L(x,y)$ выполнена в моноиде $\mathfrak{Q}^*$ для подгрупп x и y тогда и только тогда, когда* $\operatorname{ord} x < \operatorname{ord} y$.

Доказательство. Пусть $\operatorname{ord} x = N$, $\operatorname{ord} y = M$.

Допустим, что истинна формула $L(x,y)$. Из $D(y')$ и $y = \ker y'$ получаем $y' = d + \{0, b\}$ для некоторых $b \in y$ и $d \in \mathbb{Q}$, причём b является порождающим y элементом, то есть $\operatorname{ord} b = M$. Истинность $K(z,z')$ означает, что z' имеет вид $e + \{0, c\}$, где $e, c \in \mathbb{Q}$, c — порождающий $\ker z'$ элемент, допустим, что $\operatorname{ord} c = K$. Тогда $\ker z' + y = \ker z'$ означает, что $y \subseteq \ker z'$. Следовательно, y состоит из всевозможных элементов вида $i\frac{K}{M}c$, в частности, должно быть выполнено $m\frac{K}{M}c = b$ для какого-то натурального $m \leq M-1$. Согласно теореме 2 истинность формулы $K(z,z')$ означает, что $z = e + \{0, c, \ldots, \ell c\}$ для некоторого натурального ℓ. Далее получаем

$$z + y' = e + d + \Big\{0, c, \ldots, \ell c, m\frac{K}{M}c, \Big(m\frac{K}{M}+1\Big)c, \ldots, \Big(m\frac{K}{M}+\ell\Big)c\Big\}.$$

Из истинности формулы $K(z+y', z')$ вытекает, что элементы последнего множества должны быть последовательными кратными c. Это возможно в двух случаях: $m\frac{K}{M} \leq \ell+1$ (вторая часть элементов идёт после первой) или $m\frac{K}{M} \geq K-\ell-1$ (вторая часть идёт перед первой).

Из равенства $\ker z' + x = \ker z'$ получаем, что $x \subseteq \ker z'$, поэтому подгруппа x порождается элементом $\frac{K}{N}c$. Положим $x' = \{0, \frac{K}{N}c\}$, тогда будет выполнено $D(x')$ и $x = \ker x'$. Из истинности импликации делаем вывод о ложности $K(z+x', z')$. Далее получаем

$$z + x' = e + \Big\{0, c, \ldots, \ell c, \frac{K}{N}c, \Big(\frac{K}{N}+1\Big)c, \ldots, \Big(\frac{K}{N}+\ell\Big)c\Big\}.$$

Из ложности $K(z+x', z')$ следует, что элементы последнего множества не образуют последовательный набор кратных c, поэтому должно быть выполнено $\frac{K}{N} > \ell+1$.

С другой стороны, подгруппа x порождается и противоположным элементом $-\frac{K}{N}c = (K-\frac{K}{N})c$, поэтому по тем же причинам будет выполнено $K-\frac{K}{N} < K-\ell-1$.

Комбинируя полученные результаты, получаем, что должно быть справедливо одно из двух двойных неравенств:

$$m\frac{K}{M} \le \ell + 1 < \frac{K}{N};$$
$$m\frac{K}{M} \ge K - \ell - 1 > K - \frac{K}{N}.$$

В первом случае сразу получаем $\frac{m}{M} < \frac{1}{N}$ и $N < \frac{M}{m} \le M$. Во втором случае имеем

$$\frac{K}{N} > K - m\frac{K}{M} \ge K - (M-1)\frac{K}{M} = \frac{K}{M},$$

что снова означает $N < M$.

Теперь докажем лемму в обратную сторону, пусть $N < M$. Тогда в $\mathbb{Q}$ можно выбрать такие a, b, c, что $x = \langle a\rangle$, $y = \langle b\rangle$, $a = nc$, $b = mc$ для некоторых натуральных n и m. Так как $\operatorname{ord} c = Nn = Mm$, то из $N < M$ получаем $n > m$.

Положим $y' = \{0, b\} = \{0, mc\}$, $z' = \{0, c\}$, $z = (m-1)z' = \{0, c, \ldots, (m-1)c\}$. Тогда $z + y' = \{0, c, \ldots, (2m-1)c\} = (2m-1)z'$. По теореме 2 выполнено $K(z, z')$ и $K(z + y', z')$.

Возьмём теперь любое двухэлементное множество x' так, что $\ker x' = x$. Это означает, что $x' = d + \{0, ka\}$ для подходящих $d \in \mathbb{Q}$ и натурального $k \le N - 1$. Тогда

$$z + x' = \{0, c, \ldots, (m-1)c\} + d + \{0, knc\} =$$
$$= d + \{0, c, \ldots, (m-1)c, knc, (kn+1)c, \ldots, (kn+m-1)c\}.$$

Чтобы было выполнено $K(z + x', z')$, согласно теореме 2, необходимо и достаточно $kn \le m$ или $kn \ge Nn - m$. Первое невозможно, так как $kn \ge n > m$. Из второго получаем $k \ge N - \frac{m}{n}$, что означает $k \ge N$, так как k — натуральное, а $\frac{m}{n} < 1$. Это противоречит условию $k \le N - 1$. Следовательно, $K(x' + z, z')$ ложно, а вся импликация истинна. □

Следствие 6. *В интерпретации V определима s — операция прибавления единицы:*

$$y = s(x) \equiv L(x, y) \wedge (\forall z)(L(z, y) \to \neg L(x, z)).$$

В дальнейшем для простоты будет писать обычное $x < y$ вместо $L(x, y)$ и $x \le y$ вместо $L(x, y) \vee x = y$.

Осталось показать, как теперь можно интерпретировать умножение произвольных чисел. Сначала выделим множество степеней простых чисел:

$$W(x) \equiv V(x) \wedge (\forall y, z)(y \mid x \wedge z \mid x \to y \mid z \vee z \mid y).$$

Далее определим умножение для степеней одного и того же простого числа

$$M_p(x, y, z) \equiv z = E \wedge x = y \vee z \ne E \wedge (\exists w, u)\big(W(w) \wedge x \mid w \wedge y \mid w \wedge z \mid w \wedge$$
$$\wedge M_c(u, y, s(z)) \wedge x < u \wedge (\forall v)(v \mid w \to v \le x \vee u \le v)\big).$$

Здесь мы сказали, что x должно быть наибольшей степенью того же простого числа, которая меньше $y(z+1)$. Заметим, только, что если y и z являются степенями одного и того же простого числа, $z \neq 1$, то y и $z+1$ взаимно просты.

Наконец, мы в состоянии определить умножение для произвольных чисел:

$$M(x,y,z) \equiv (\forall u,u',v,v',w,w',t)\Big(W(t)\wedge \\ \wedge u \mid t \wedge v \mid t \wedge w \mid t \wedge C(u',t) \wedge C(v',t) \wedge C(w',t)\wedge \\ \wedge M_c(y,u,u') \wedge M_c(z,v,v') \wedge M_c(x,w,w') \to M_p(w,u,v)\Big).$$

Здесь мы записали, что при разложении на простые множители степень каждого простого числа в x равна произведению степеней этого же числа в y и z.

Окончательно мы можем сделать такой вывод:

Теорема 3. *В моноиде $\mathfrak{Q}^*$ интерпретируется элементарная арифметика. Следовательно, теория моноида $\mathfrak{Q}^*$ неразрешима.*

Доказательство. В [3] продемонстрировано, что с помощью умножения и прибавления единицы в алгебре $(\omega, +, s, \cdot)$ можно проинтерпретировать сложение. Следовательно, из интерпретируемости в $\mathfrak{Q}^*$ умножения и прибавления единицы следует, что в $\mathfrak{Q}^*$ интерпретируется вся элементарная арифметика. □

Заключение

Мы продемонстрировали, что для абелевых групп кручения может быть верен тот же результат, что и для других абелевых групп: моноид их подмножеств имеет теорию, в которой интерпретируется элементарная арифметика.

Вместе с тем очевидно, что не каждая группа кручения обладает таким свойством: оно тривиально не выполнено для конечных групп. Поэтому возникает вопрос, можно ли сформулировать какие-то общие условия, которые позволят выделить те группы кручения, для которых такое свойство верно. Следует отметить, что часть результатов, а именно — те, которые изложены в разделе 2, верны для любых групп кручения. Есть основания считать, что их можно применить для интерпретации элементарной арифметики в тех абелевых группах, которые имеют элементы кручения сколь угодно большого порядка.

Список литературы

[1] Дудаков С.М. Об алгоритмических свойствах алгебры конечных подмножеств некоторых уноидов // Вестник ТвГУ. Серия: Прикладная математика. 2019. № 4. С. 108–116. https://doi.org/10.26456/vtpmk550

[2] Дудаков С.М. Об определимости в алгебре конечных языков с конкатенацией множества односимвольных языков // Вестник ТвГУ. Серия: Прикладная математика. 2020. № 4. С. 5–13. https://doi.org/10.26456/vtpmk601

[3] Boolos G.S., Burgess J.P., Jeffrey R.C. Computability and Logic. 5th edition. New York: Cambridge University Press, 2007. 364 p.

[4] Codd E.F. Relational completeness of data base sublanguages // Database Systems. Ed. by R. Rustin. Prentice-Hall, 1972. Pp. 33–64.

[5] Dudakov S.M. On undecidability of concatenation theory for one-symbol languages // Lobachevskii Journal of Mathematics. 2020. Vol. 40, № 2. Pp. 168–175.

[6] Dudakov S.M., Karlov B.N. On Decidability of Regular Languages Theories // Proc. of 14th International Computer Science Symposium in Russia, CSR 2019. Series: LNCS. Vol. 11532. 2019. Pp. 119–130.

[7] Dudakov S., Karlov B. On decidability of theories of regular languages // Theory of Computing Systems. 2021. Vol. 65. Pp. 462–478. http://doi.org/10.1007/s00224-020-09995-4

[8] Dudakov S.M. On Undecidability of Subset Theory for Some Monoids // Journal of Physics: Conference Series. 2021. Vol. 1902, № 1. ID 012060. https://doi.org/10.1088/1742-6596/1902/1/012060

[9] Hopcroft J.E., Motwani R., Ullman J.D. Introduction to Automata Theory, Languages, and Computation. Harlow: Pearson, 2013. 560 p.

[10] Kanellakis P., Kuper G., Revesz P. Constraint query languages // Journal of Computer and System Sciences. 1995. Vol. 51. Pp. 26–52.

[11] Mostowski A. On direct products of theories // The Journal of Symbolic Logic. 1952. Vol. 17, № 3. Pp. 1–31.

[12] Rogers H. Theory of Recursive Functions and Effective Computability. Cambridge: MIT Press, 1987. 506 p.

Образец цитирования

Дудаков С.М. О теории моноида конечных подмножеств для одной абелевой группы кручения // Вестник ТвГУ. Серия: Прикладная математика. 2021. №2. С. 39–55. https://doi.org/10.26456/vtpmk615

Сведения об авторах

1. **Дудаков Сергей Михайлович**
декан факультета прикладной математики и кибернетики Тверского государственного университета.

Россия, 170100, г. Тверь, ул. Желябова, д. 33, ТвГУ.
E-mail: sergeydudakov@yandex.ru

ON THEORY OF FINITE SUBSETS MONOID FOR ONE TORSION ABELIAN GROUP

Dudakov Sergey Mikhailovich
Head of Applied Mathematics and Cybernetics Faculty, Tver State University
Russia, 170100, Tver, 33, Zhelyabova str., TverSU.
E-mail: sergeydudakov@yandex.ru

Received 15.04.2021, revised 15.05.2021.

Earlier it was proved the following claim. Let $\mathfrak{G}$ be a non-torsion abelian group and $\mathfrak{G}$ be the semigroup of finite subsets of $\mathfrak{G}$. Then elementary arithmetic can be interpreted in $\mathfrak{G}^*$, so the theory of $\mathfrak{G}^*$ is undecidable. Here we prove the same result for one torsion group, the multiplicative group of all roots of unity.

Keywords: torsion group, semigroup of subsets, elementary arithmetic, undecidability.

Citation

Dudakov S.M., "On theory of finite subsets monoid for one torsion abelian group", *Vestnik TvGU. Seriya: Prikladnaya Matematika [Herald of Tver State University. Series: Applied Mathematics]*, 2021, № 2, 39–55(in Russian). https://doi.org/10.26456/vtpmk615

References

[1] Dudakov S.M., "On algorithmic properties of finite subset algebra for some unoids", *Vestnik TvGU. Seriya: Prikladnaya Matematika [Herald of Tver State University. Series: Applied Mathematics]*, 2019, № 4, 108–116 (in Russian), https://doi.org/10.26456/vtpmk550.

[2] Dudakov S.M., "On definability of one-symbol languages in the monoid of finite languages with concatenation", *Vestnik TvGU. Seriya: Prikladnaya Matematika [Herald of Tver State University. Series: Applied Mathematics]*, 2020, № 4, 5–13 (in Russian), https://doi.org/10.26456/vtpmk601.

[3] Boolos G.S., Burgess J.P., Jeffrey R.C., *Computability and Logic*, 5th edition, Cambridge University Press, New York, 2007, 364 pp.

[4] Codd E.F., "Relational completeness of data base sublanguages", *Database Systems*, ed. R. Rustin, Prentice-Hall, 1972, 33–64.

[5] Dudakov S.M., "On undecidability of concatenation theory for one-symbol languages", *Lobachevskii Journal of Mathematics*, **40**:2 (2020), 168–175.

[6] Dudakov S.M., Karlov B.N., "On Decidability of Regular Languages Theories", *Proc. of 14th International Computer Science Symposium in Russia*. V. 11532, CSR 2019, LNCS, 2019, 119–130.

[7] Dudakov S., Karlov B., "On decidability of theories of regular languages", *Theory of Computing Systems*, **65** (2021), 462–478, http://doi.org/10.1007/s00224-020-09995-4.

[8] Dudakov S.M., "On Undecidability of Subset Theory for Some Monoids", *Journal of Physics: Conference Series*, **1902**:1 (2021), 012060, https://doi.org/10.1088/1742-6596/1902/1/012060.

[9] Hopcroft J.E., Motwani R., Ullman J.D., *Introduction to Automata Theory, Languages, and Computation*, Pearson, Harlow, 2013, 560 pp.

[10] Kanellakis P., Kuper G., Revesz P., "Constraint query languages", *Journal of Computer and System Sciences*, **51** (1995), 26–52.

[11] Mostowski A., "On direct products of theories", *The Journal of Symbolic Logic*, **17**:3 (1952), 1–31.

[12] Rogers H., *Theory of Recursive Functions and Effective Computability*, MIT Press, Cambridge, 1987, 506 pp.