УДК 510.665, 510.53, 510.65

# О РАЗРЕШИМОСТИ ТЕОРИИ КОНЕЧНЫХ ПОДМНОЖЕСТВ ДЛЯ ДИСКРЕТНОГО ЛИНЕЙНОГО ПОРЯДКА

**Авхимович Н.В.**
Тверской государственный университет, г. Тверь

*Поступила в редакцию 19.06.2022, после переработки 05.09.2022.*

Мы рассматриваем метод построения новых алгебраических систем как конечных подмножеств уже существующих. Берем исходные системы, обладающие дискретным линейным порядком, и вводим на них новое отношение для конечных подмножеств. Считаем, что два подмножества состоят в новом отношении тогда и только тогда, когда каждый элемент первого подмножества меньше каждого элемента второго. Для теорий таких систем мы доказываем, что они допускают эффективную элиминацию кванторов. Следовательно, такие теории являются разрешимыми.

**Ключевые слова:** теория, обогащение, дискретный линейный порядок, разрешимость, элиминация кванторов, конечное подмножество.

*Вестник ТвГУ. Серия: Прикладная математика. 2022. № 3. С. 91–104.*
https://doi.org/10.26456/vtpmk646

## Введение

Изучение теорий и их свойств является одной из главных задач математической логики. Эта задача интересна не только с теоретической точки зрения, но и с практической. На практике часто приходится работать с такими структурами данных как, например, массивы. Эти структуры из-за понятных ограничений конечны. Возникает интерес рассмотреть алгебраическую систему, носителем которой будут являться конечные подмножества некоторого бесконечного множества.

В работах [1–4] рассматриваются такие системы. Например, в [3] показано, что теория конечных подмножеств свободного циклического моноида будет эквивалентна элементарной арифметике. В работе [4] результат из [3] о циклических моноидах обобщается на коммутативные моноиды с сокращением, в которых есть хотя бы один элемент бесконечного порядка. В статье [2] получен аналогичный результат для абелевых групп кручения, имеющих элементы неограниченного порядка: для такой группы теория конечных подмножеств позволяет интерпретировать элементарную арифметику. Во всех этих случаях полученные теории оказываются неразрешимыми.

Мы рассматриваем алгебраические системы с отношениями. Ранее, в статье [1] мы рассматривали систему конечных подмножеств плотного линейно упорядоченного множества. Было показано, что теория данной системы допускает эффективную элиминацию кванторов. Теперь же мы рассмотрим следующее. В качестве универсума возьмем дискретно линейно упорядоченное множество, и построим систему, носителем которой будут конечные подмножества этого множества. Как известно (см. [6]), теория дискретного линейного порядка без первого и последнего элементов разрешима. В нашей работе доказывается, что если мы возьмем в качестве алгебраической системы множество конечных подмножеств дискретного линейно упорядоченного множества и рассмотрим новое отношение, которое означает, что все элементы одного множества меньше всех элементов другого множества, то получается новая система, теория которой допускает эффективную элиминацию кванторов, следовательно, разрешима.

Результат разрешимости можно получить как следствие работы [5]. Однако наш результат выявляет структуру теории данной системы, демонстрирующую возможность эффективной элиминации кванторов.

## 1. Основные определения

Напомним определения основных понятий, используемых в работе. Определения 1–4 взяты из книги [6].

*Определение* 1 (Теория алгебраической системы). Теория алгебраической системы $\mathfrak{A}$ — это множество истинных в $\mathfrak{A}$ замкнутых формул.

*Определение* 2 (Теория линейного порядка). Теория (нестрогого) линейного порядка задается аксиомами

$$
\begin{aligned}
&(\forall x) x \leq x;\\
&(\forall x)(\forall y)(x \leq y \wedge y \leq x \to x = y);\\
&(\forall x)(\forall y)(\forall z)(x \leq y \wedge y \leq z \to x \leq z);\\
&(\forall x)(\forall y)(x \leq y \vee y \leq x).
\end{aligned}
$$

Далее мы будем использовать знак «$<$» для строгого порядка, а знак «$\leq$» для соответствующего ему нестрогого.

*Определение* 3 (Теория дискретного линейного порядка). Теория дискретного линейного порядка без первого и последнего элементов получается из теории линейного порядка добавлением аксиом

$$
\begin{aligned}
&(\forall x)(\exists y)(x < y \wedge (\forall z)(x < z \to y \leq z));\\
&(\forall x)(\exists y)(y < x \wedge (\forall z)(z < x \to z \leq y)).
\end{aligned}
$$

*Определение* 4 (Эффективная элиминация кванторов). Теория $T$ допускает эффективную элиминацию кванторов, если по любой формуле можно алгоритмически построить бескванторную формулу, эквивалентную данной в теории $T$ и не содержащую новых свободных переменных

Известны (см., например, [6]) следующие результаты.

*Следствие* 1. Теория разрешима, если она допускает эффективную элиминацию кванторов.

*Лемма* 1. Пусть в теории $T$ любая формула вида $(\exists x)\varphi$ эквивалентна бескванторной формуле, где $\varphi$ — конъюнкция атомных формул и их отрицаний. Тогда теория $T$ допускает элиминацию кванторов.

**Теорема 1.** *Теория дискретного линейного порядка без первого и последнего элементов допускает элиминацию кванторов при добавлении одноместного функционального символа* $+1$*, означающего следующий элемент.*

## 2. Система конечных подмножеств дискретного линейного порядка

Мы рассматриваем дискретно линейно упорядоченное множество $\mathfrak{D}$ без первого и последнего элементов.

Сделаем одно замечание. В случаях, когда мы используем запись $X = \{x_1, \ldots, x_n\}$, мы считаем, что элементы $x_1, \ldots, x_n$ упорядочены по возрастанию.

Рассмотрим следующую алгебраическую структуру. В качестве носителя возьмем множество $\exp \mathfrak{D}$ — множество конечных подмножеств множества $\mathfrak{D}$.

Для элементов системы $\exp \mathfrak{D}$ введем отношение

$$A <^* B \Leftrightarrow (\forall a)(\forall b) a < b, \quad a \in A, b \in B,$$

то есть считаем, что одно множество меньше чем другое, если каждый элемент первого множества меньше любого элемента второго множества. Если не выполняется ни один из случаев $A <^* B$, $B <^* A$, $A = B$, то считаем, что множества $A$ и $B$ не сравнимы.

Получили алгебраическую систему $(\exp \mathfrak{D}, <^*)$.

В этой алгебраической системе определимо пустое множество — единственное множество, которое сравнимо со всеми другими:

$$X = \emptyset \Leftrightarrow (\forall Y) X <^* Y.$$

Пусть у нас есть бескванторная формула $\varphi$, содержащая переменную $X$, обозначающую некоторое множество. Это множество может содержать какие-то элементы, но может быть и пустым. Добавим в формулу $\varphi$ дизъюнкцию

$$\varphi \wedge (X = \emptyset \vee \neg X = \emptyset).$$

После раскрытия скобок и приведения формулы к ДНФ для каждой элементарной конъюнкции мы получим один из видов:

$$K \wedge X = \emptyset \text{ или } K \wedge \neg X = \emptyset.$$

Допустим, что множество $X$ пусто, то есть мы рассматриваем элементарную конъюнкцию $K \wedge X = \emptyset$. Покажем, как в такой ситуации исключить $X$. Переменная $X$ может входить в формулу следующими способами:

1. $X = t$, в этом случае заменяем это равенство на $t = \emptyset$;

2. $\neg X = t$, в этом случае делаем замену на $\neg t = \emptyset$;

3. $X < t$, это неравенство меняем на тождественно истинную формулу $\top$;

4. $\neg X < t$, заменяем на тождественно ложную формулу $\neg\top$;

5. $t < X$, меняем на $\top$;

6. $\neg t < X$, меняем на $\neg\top$;

7. $X = \emptyset$, в этом случае меняем равенство на $\top$;

8. $\neg X = \emptyset$, здесь же заменяем на $\neg\top$.

Мы рассмотрели все возможные варианты вхождения переменной, имеющей значение пустого множества, в элементарную конъюнкцию и показали, какие эквивалентные замены в этом случае следует произвести. Поэтому далее можем считать, что рассматриваемые нами переменные имеют значения непустых множеств.

Определим в системе $(\exp\mathfrak{D}, <^*)$ следующие функциональные символы: $f(X)$, $g(X)$, $+1$, $-1$, и построим для них определяющие формулы.

Функции $f(X)$ и $g(X)$ для множества $X = \{x_1, \ldots, x_n\}$ обозначают, соответственно, наименьший и наибольший элементы этого множества. Точнее говоря, функция $f(X)$ определяет одноэлементное множество $\{x_1\}$, а функция $g(X)$ определяет одноэлементное множество $\{x_n\}$.

*Лемма* 2. Пусть $X = \{x_1, \ldots, x_n\}$, тогда формула

$$\begin{aligned} f(X) = Z \Leftrightarrow (\forall Y)(Y <^* X \leftrightarrow Y <^* Z) \wedge (\forall U)(\forall V)((\neg V = U \wedge \\ \wedge \neg U <^* Z \wedge \neg U = Z \wedge \neg Z <^* U \wedge \neg V <^* Z \wedge \neg V = Z \wedge \neg Z <^* V) \rightarrow \\ \rightarrow \neg U <^* V \wedge \neg V <^* U) \quad (1) \end{aligned}$$

определяет одноэлементное множество, состоящее из наименьшего элемента множества $X$. Иначе говоря, $f(X) = \{x_1\}$.

*Доказательство.* Пусть $Z$ — одноэлементное множество, состоящее из наименьшего элемента множества $X$, то есть $Z = \{x_1\}$. Покажем, что в этом случае формула истинна. Первая часть формулы (1) утверждает: всякое множество $Y$ меньше множества $X$ в том и только том случае, если оно меньше множества $Z$. Допустим, что эта часть формулы ложна. Это допущение эквивалентно формуле

$$(\exists Y)((\neg Y <^* X \wedge Y <^* Z) \vee (\neg Y <^* Z \wedge Y <^* X)).$$

Определенное нами отношение $<^*$ для двух множеств истинно в том и только том случае, когда все элементы первого множества меньше всех элементов второго множества, то есть все элементы первого множества должны быть меньше наименьшего элемента второго множества. Мы также предположили, что $Z = \{x_1\}$. Тогда полученная нами формула эквивалентна формуле

$$(\exists Y)(\neg Y <^* \{x_1\} \wedge Y <^* \{x_1\}),$$

которая в свою очередь ложна. Следовательно, наше предположение о том, что формула (1) неверна — ошибочно.

Рассмотрим теперь вторую часть формулы, предполагая, что $Z = \{x_1\}$. Пусть $U = \{u_1, \ldots, u_k\}$, $V = \{v_1, \ldots, v_m\}$. Фрагмент

$$\neg U <^* \{x_1\} \wedge \neg U = \{x_1\} \wedge \neg \{x_1\} <^* U$$

означает, что $x_1 \in [u_1, u_k]$. Из аналогичного фрагмента для $V$ получаем $x_1 \in [v_1, v_m]$. Следовательно, неверно, что отрезок $[u_1, u_k]$ лежит строго правее (или левее) отрезка $[v_1, v_m]$. В терминах наших множеств, это означает, что

$$\neg U <^* V \wedge \neg V <^* U.$$

Тогда вторая часть формулы также является истинной.

Рассмотрим теперь обратное утверждение. Покажем, что из истинности формулы следует равенство $Z = \{x_1\}$.

Пусть формула

$$(\forall Y)(Y <^* X \leftrightarrow Y <^* Z) \tag{2}$$

истинна. Убедимся, что оба неравенства $Y <^* X$ и $Y <^* Z$ могут быть выполнены для любого множества $Y$ в том и только том случае, когда наименьшие элементы множеств $X = \{x_1, \ldots, x_n\}$ и $Z = \{z_1, \ldots, z_m\}$ совпадают. Допустим, что это не так и наименьший элемент множества $X$ не совпадает с наименьшим элементом множества $Z$: $x_1 \neq z_1$. Пусть $x_1 < z_1$. Мы предполагаем, что формула (2) истинна, значит, она истинна для любого множества $Y$. Рассмотрим множество $Y = \{z_1 - 1\}$. Тогда неравенство $Y <^* Z$ выполнено, а неравенство $Y <^* X$ — нет. Если же $z_1 < x_1$ в качестве множества $Y$ можно взять $Y = \{x_1 - 1\}$. В обоих случаях получаем противоречие с утверждением, что формула (2) истинна, следовательно, наше допущение о том, что $x_1 \neq z_1$ ложно.

На данный момент мы показали, что наименьший элемент множества $Z$ совпадает с наименьшим элементом множества $X$. Убедимся теперь, что множество $Z$ никаких других элементов не содержит. Докажем, что вторая часть формулы утверждает, что $Z$ — одноэлементное множество. Допустим, что $Z$ не одноэлементное множество: $Z = \{z_1, \ldots, z_m\}$. Тогда мы можем взять, например, такие $U$ и $V$, что $U = \{\ldots, z_1\}$, а $V = \{z_m, \ldots\}$, $U \neq V$. Тогда $U$ и $V$ не сравнимы с $Z$, но сравнимы друг с другом: $U <^* V$ и формула ложна.

Мы показали, что и в обратную сторону утверждение верно. □

Определяющая формула для функции $g(X)$ строится аналогичным образом.

С помощью символов $-1$ и $+1$ для множества $X$ обозначаем, соответственно, множество, состоящее из элемента предшествующего наименьшему элементу $X$ и множество, состоящее из элемента, следующего за наибольшим элементом $X$. Пусть $X = \{x_1, \ldots, x_n\}$. Тогда $X - 1$ — это одноэлементное множество $\{x_1 - 1\}$, соответственно, $X + 1 = \{x_n + 1\}$.

*Лемма* 3. Пусть $X = \{x_1, \ldots, x_n\}$, тогда формула

$$X - 1 = Z \Leftrightarrow f(Z) = g(Z) \wedge Z <^* X \wedge \neg(\exists Y)(Z <^* Y \wedge Y <^* X)$$

определяет операцию $-1$, то есть множество $Z = \{x_1 - 1\}$.

*Доказательство.* Рассмотрим сначала случай, когда выполнено $Z = \{x_1 - 1\}$. Первая часть формулы $f(Z) = g(Z)$ утверждает, что множество $Z$ одноэлементное, это верно. Далее утверждается, что $Z$ меньше $X$, что тоже верно, так как единственный элемент множества $Z$ меньше наименьшего элемента множества $X$: $x_1 - 1 < x_1$. Третья часть формулы

$$\neg(\exists Y)(Z <^* Y \wedge Y <^* X)$$

говорит, что не существует множества $Y$ между множествами $Z = \{x_1 - 1\}$ и $X$. Эта формула эквивалентна формуле

$$\neg(\exists Y)(\{x_1 - 1\} <^* Y <^* \{x_1\}),$$

которая утверждает, что не существует элемент на отрезке $[x_1 - 1, x_1]$ не равный $x_1 - 1$ и не равный $x_1$. Поскольку $x_1 - 1$ — элемент, предшествующий $x_1$, такое утверждение верно. Следовательно, формула истинна: такого $Y$ в самом деле не существует. Значит, истинна и вся формула.

Допустим теперь обратное: пусть истинна формула

$$f(Z) = g(Z) \wedge Z <^* X \wedge \neg(\exists Y)(Z <^* Y \wedge Y <^* X).$$

Первая часть формулы $f(Z) = g(Z)$ дает нам ограничение на количество элементов $Z$, пусть $Z = \{z_1\}$. Далее говорится, что $z_1$ меньше $x_1$. И, наконец, имеем утверждение, что между $z_1$ и $x_1$ нет никаких других элементов. Это верно в том и только том случае, когда $z_1$ это элемент, предшествующий $x_1$. Следовательно, $z_1 = x_1 - 1$. □

Для операции $X + 1$ определяющая формула строится аналогично.

Условимся также обозначать $\alpha$-кратное применение операции $+1$ (соответственно, $-1$) к множеству $X$ как $X + \alpha$ (соответственно, $X - \alpha$).

Теперь мы можем обогатить сигнатуру рассматриваемой системы четырьмя определимыми функциональными символами: $f$, $g$, $+1$, $-1$.

## 3. Элиминация кванторов

Мы хотим показать, что теория системы $(\exp \mathfrak{D}, <^*; f^{(1)}, g^{(1)}, +1, -1)$ допускает эффективную элиминацию кванторов. Согласно Лемме 1, нам достаточно показать, что любая формула вида $(\exists x)\varphi$ эквивалентна бескванторной, где $\varphi$ — это конъюнкция атомных формул и их отрицаний. Элементарная конъюнкция в нашем случае имеет следующий вид

$$\begin{gathered}(\exists X)(f(X) \pm \alpha_1 <^* t_1 \wedge \ldots \wedge f(X) \pm \alpha_a <^* t_a \wedge f(X) \pm \beta_1 = s_1 \wedge \ldots \wedge f(X) \pm \beta_m = s_m \wedge \\ \wedge\, l_1 <^* f(X) \pm \gamma_1 \wedge \ldots \wedge l_k <^* f(X) \pm \gamma_k \wedge g(X) \pm \alpha'_1 <^* d_1 \wedge \ldots \wedge g(X) \pm \alpha'_h <^* d_h \wedge \\ \wedge\, g(X) \pm \beta'_1 = e_1 \wedge \ldots \wedge g(X) \pm \beta'_v = e_v \wedge z_1 <^* g(X) \pm \gamma'_1 \wedge \ldots \wedge z_u <^* g(X) \pm \gamma'_u \wedge \\ \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p \wedge X = r_1 \wedge \ldots \wedge X = r_c \wedge \\ \wedge\, (f(X) \pm n = g(X) \vee f(X) \pm n <^* g(X) \vee g(X) \pm n <^* f(X))).\end{gathered}$$

Во-первых, мы можем считать значения термов $t_1, \ldots, t_a, \ldots, z_1, \ldots, z_u$ одноэлементными множествами. В противоположной стороне неравенства, для каждого из этих термов, находится одноэлементное множество, для сравнения с которым, у рассматриваемого терма достаточно оставить только один элемент, то есть применить к нему одну из функций $f$ или $g$.

Согласно вышесказанному, далее в формулах мы можем использовать знак «$<$» вместо знака «$<^*$».

Допустим, формула содержит фрагмент $g(X) \pm n \ <^* \ f(X)$, при этом либо $f(X) < g(X)$, либо $f(X) = g(X)$, то есть имеет место $g(X) \pm n < f(X) \wedge f(X) < g(X)$ или $g(X) \pm n < f(X) \wedge f(X) = g(X)$. Это возможно только в одном из случаев $f(X) = g(X) \vee f(X) = g(X) - 1 \vee \ldots \vee f(X) = g(X) - n$.

Если формула содержит фрагмент $X = r_1 \wedge \ldots \wedge X = r_c$ и хотя бы два $r_i$ не равны между собой, то формула ложна. В противном случае бескванторная формула строится заменой переменной $X$, например, на $r_1$.

Далее, мы не рассматриваем вложенные функции, например, $f(g(X - 1))$. Результатом применения любой из четырех определенных нами операций является одноэлементное множество, следовательно, после применения самой внутренней функции, в приведенном выше примере это $-1$, мы получим результат, который больше изменяться не будет.

Также считаем, что формула не содержит отрицаний перед неравенствами, например, $\neg f(X) < t$. Мы всегда можем заменить такого вида фрагмент на эквивалентный, но не содержащий знака $\neg$. Для приведенного примера эквивалентная формула $f(X) = t \vee t < f(X)$. Мы в самом деле можем производить такие замены, поскольку, напомним, мы считаем термы, обозначенные строчными латинскими буквами, одноэлементными множествами.

Заметим также, что, например, формула $f(X) \pm \alpha_1 < t_1$ эквивалентна формуле $f(X) < t'_1$. Действительно, перенесем всюду операции $\pm\vartheta$ в противоположные стороны, получим

$$
\begin{aligned}
&(\exists X)(f(X) < t_1 \wedge \ldots \wedge f(X) < t_a \wedge f(X) = s_1 \wedge \ldots \wedge f(X) = s_m \wedge \\
&\qquad \wedge l_1 < f(X) \wedge \ldots \wedge l_k < f(X) \wedge g(X) < d_1 \wedge \ldots \wedge g(X) < d_h \wedge \\
&\qquad \wedge g(X) = e_1 \wedge \ldots \wedge g(X) = e_v \wedge z_1 < g(X) \wedge \ldots \wedge z_u < g(X) \wedge \\
&\qquad\qquad\qquad \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p \wedge \\
&\qquad\qquad\qquad\qquad \wedge (f(X) + n = g(X) \vee f(X) + n < g(X))).
\end{aligned}
$$

Теперь воспользуемся соображениями, рассмотренными в статье [1], и упростим нашу формулу. Нам не обязательно рассматривать все неравенства вида $f(X) < t_1 \wedge \ldots \wedge f(X) < t_a$, вместо этого можно оставить только одно $f(X) < t$, где $t$ — наименьшее из $t_i$. Из неравенств $l_1 < f(X) \wedge \ldots \wedge l_k < f(X)$ оставляем только $l < f(X)$, где $l$ — наибольшее из $l_i$. От множества равенств $f(X) = s_1 \wedge \ldots \wedge f(X) = s_m$ мы тоже можем избавиться: оставляем одно $f(X) = s_1$, и добавляем условие, что все $s_i$ равны между собой. Для частей формулы с функцией $g(X)$ поступаем аналогичным образом.

После вышеупомянутых преобразований элементарная конъюнкция приобретет вид

$$(\exists X)(f(X) < t \wedge f(X) = s \wedge l < f(X) \wedge \\ \wedge\, g(X) < d \wedge g(X) = e \wedge z < g(X) \wedge \\ \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p \wedge \\ \wedge\, (f(X) + n = g(X) \vee f(X) + n < g(X))).$$

Эту формулу мы и будем исследовать.

Нам нужно рассмотреть два случая. Первый — когда в формулу входит фрагмент $f(X)+n = g(X)$, второй — когда $f(X)+n < g(X)$. Если формула не содержит ни одного из этих фрагментов, мы всегда можем добавить условие $f(X)-1 < g(X)$, сведя тем самым нашу формулу ко второму случаю.

Прежде чем перейти к основной теореме, докажем несколько вспомогательных лемм.

*Лемма* 4. Формула вида

$$(\exists X)(f(X) < t \wedge f(X) = s \wedge l < f(X) \wedge f(X) + n = g(X) \wedge \\ \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p) \quad (3)$$

эквивалентна бескванторной.

*Доказательство.* Рассматриваемая формула содержит равенство $f(X) = s$. Заменим в случаях, где это возможно, $f(X)$ на $s$ и вынесем за знак квантора не содержащие $X$ фрагменты. Получим

$$s < t \wedge l < s \wedge (\exists X)(f(X) = s \wedge f(X) + n = g(X) \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p).$$

Нам известен первый (наименьший) элемент множества $X$ — это $s$. Нам известен последний (наибольший) элемент множества $X$ — это $s+n$. Всего существует $2^{n-1}$ вариант множества $X$ вида $\{s, \ldots, s+n\}$. Наша задача состоит в том, чтобы среди этих множеств найти такое, которое не совпадает ни с одним из $w_1, \ldots, w_p$. Если такое множество найдется, то нужный нам $X$ существует. Нужно убедиться, что множества $w_1, \ldots, w_p$ перечисляют не все существующие множества нужного нам вида.

Для начала исключим из $w_1, \ldots, w_p$ те множества, которые не удовлетворяют условию $f(w_i) = s \wedge g(w_i) = s + n$. Чтобы это сделать, добавим к формуле конъюнкцию:

$$\bigwedge_i (f(w_i) = s \vee \neg f(w_i) = s) \wedge \bigwedge_i (g(w_i) = s + n \vee \neg g(w_i) = s + n).$$

Тогда после раскрытия скобок мы получим ДНФ, где в каждой элементарной конъюнкции для каждого $w_i$ будет содержаться один из четырех возможных фрагментов:

1. $f(w_i) = s \wedge g(w_i) = s + n$,
2. $f(w_i) = s \wedge \neg g(w_i) = s + n$,

3. $\neg f(w_i) = s \wedge g(w_i) = s + n$,

4. $\neg f(w_i) = s \wedge \neg g(w_i) = s + n$.

Нас будет интересовать только первый случай. Случаи 2–4 мы не рассматриваем, поскольку они ни на что не влияют: такие $w_i$ автоматически не совпадают с $X$.

Теперь надо выяснить, сколько среди оставшихся множеств $w_i$ различных. Для этого добавим в формулу фрагмент

$$\bigwedge_{i,j}(w_i = w_j \vee \neg w_i = w_j).$$

Раскроем скобки и приведем формулу к ДНФ. В получившихся элементарных конъюнкциях, для каждой пары $(w_i, w_j)$ мы будем точно знать равны они или нет.

Теперь нам остается лишь посчитать, сколько среди $w_i$ различных. Если меньше, чем $2^{n-1}$, то множество $X$ существует и формула под квантором эквивалентна $\top$. В противном случае, искомого множества $X$ нет и формула под квантором эквивалентна $\neg\top$. □

*Лемма* 5. Формула вида

$$(\exists X)(f(X) < t \wedge l < f(X) \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p \wedge f(X) + n = g(X))$$

эквивалентна бескванторной.

*Доказательство.* В этом случае рассматриваемая формула равенств не содержит. В идеале мы должны перебрать всевозможные варианты значения $f(X)$, то есть

$$\begin{gathered} f(X) = l + 1, \\ f(X) = l + 2, \\ \ldots \\ f(X) = t - 2, \\ f(X) = t - 1. \end{gathered}$$

Тогда в каждой элементарной конъюнкции мы бы получили формулу, аналогичную формуле в Лемме 4. Однако, мы не можем реализовать такой перебор напрямую, поскольку значения $l$ и $t$ нам неизвестны. Но мы можем осуществить это по-другому. Во-первых, «отсеим» случаи, когда множество $X$ при заданных условиях очевидно существует и дополнительных проверок не требуется. Мы точно знаем, что количество неравенств вида $\neg X = w_i$ равно $p$. Тогда имеет место один из двух случаев: $t-l > p+1$ или $t-l \leq p+1$. Чтобы отразить этот факт в формуле, добавим в нее дизъюнкцию

$$(t - p - 1 > l \vee t - p - 1 \leq l).$$

Если количество возможных значений $f(X)$ превышает количество неравенств вида $\neg X = w_i$, то есть если $t-p-1 > l$, то мы точно сможем найти такое множество $X$, которое удовлетворяло бы всем $\neg X = w_i$.

Тогда, согласно вышесказанному, после приведения формулы к ДНФ, нам останется рассмотреть лишь элементарные конъюнкции вида

$$(\exists X)(l < f(X) \wedge f(X) < t \wedge t - p - 1 \leq l \wedge \\ \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p \wedge f(X) + n = g(X)).$$

В этом случае может быть такая ситуация, что множества $w_1, \ldots, w_p$ перебирают все возможные при заданных условиях варианты множества $X$. Если бы нам удалось некоторым образом зафиксировать первый элемент (придать значение $f(X)$), мы бы свели нашу задачу к задаче в Лемме 4. Именно это мы сейчас и сделаем.

Добавим к формуле дизъюнкцию

$$\bigvee_{j=2}^{p+1}(l + j = t \wedge \bigvee_{\alpha=1}^{j-1} f(X) = l + \alpha).$$

Ситуацию, когда $j = 1$ не рассматриваем, так как в этом случае формула будет ложна. После раскрытия скобок и приведения формулы к ДНФ получим элементарные конъюнкции вида

$$(\exists X)(f(X) + n = g(X) \wedge f(X) < t \wedge l < f(X) \wedge \\ \wedge t - p - 1 \leq l \wedge l + j = t \wedge f(X) = l + \alpha \wedge \\ \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p),$$

где $j \in \{2, \ldots, p+1\}$, $\alpha \in \{1, \ldots, j-1\}$. После эквивалентных преобразований получим формулу такого же вида, что и в Лемме 4. $\square$

*Лемма* 6. Формула вида

$$(\exists X)(f(X) + n < g(X) \wedge f(X) = s \wedge l < f(X) < t \wedge \\ \wedge g(X) = e \wedge z < g(X) < d \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p)$$

эквивалентна бескванторной.

*Доказательство.* Так как формула содержит фрагмент $f(X) = s \wedge g(X) = e$, она эквивалентна формуле

$$s + n < e \wedge l < s < t \wedge z < e < d \wedge \\ \wedge (\exists X)(f(X) = s \wedge g(X) = e \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p).$$

Добавим в формулу дизъюнкцию

$$(s + p + 1 \leq e \vee s + p + 1 > e).$$

Тогда каждая элементарная конъюнкция будет иметь один из двух видов.

Первый вид: $(\exists X)(s+p+1 \leq e \wedge f(X) = s \wedge g(X) = e \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p)$.

В этом случае мы можем утверждать, что множество $X$ существует, поскольку $w_i$ не могут перебирать все возможные варианты множества $X$. Тогда формула эквивалентна $s + p + 1 \leq e$.

Второй вид: $(\exists X)(s+p+1 > e \wedge f(X) = s \wedge g(X) = e \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p)$. Добавим в формулу дизъюнкцию

$$\bigvee_{\alpha=1}^{p-1} (f(X) + \alpha = g(X)).$$

После раскрытия скобок и вынесения частей без $X$ получим элементарные конъюнкции следующего вида

$$(\exists X)(f(X) + \alpha = g(X) \wedge f(X) = s \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p),$$

где $\alpha \in \{1, \ldots, p-1\}$. Получили формулы, аналогичные формулам в Лемме 4. $\square$

Теперь мы можем сформулировать наш основной результат.

**Теорема 2.** *Теория конечных подмножеств дискретного линейного порядка без первого и последнего элементов допускает эффективную элиминацию кванторов в сигнатуре* $(<^*; f^{(1)}, g^{(1)}, +1, -1)$.

*Доказательство.* Пусть формула содержит фрагмент $f(X)+n = g(X)$. Мы можем заменить все вхождения $g(X)$ на $f(X) + n$. Тогда наша формула примет вид

$$(\exists X)(f(X) + n = g(X) \wedge f(X) < t \wedge f(X) = s \wedge l < f(X) \wedge \\ \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p).$$

Нужно рассмотреть отдельно ситуации, когда формула содержит равенство $f(X) = s$ и когда она этого равенства не содержит. В первом случае воспользуемся Леммой 4, во втором — Леммой 5, согласно которым, данные формулы эквивалентны бескванторным.

Пусть теперь формула содержит фрагмент $f(X) + n < g(X)$. В этом случае она имеет вид:

$$(\exists X)(f(X) + n < g(X) \wedge f(X) = s \wedge l < f(X) < t \wedge \\ \wedge g(X) = e \wedge z < g(X) < d \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p).$$

Здесь мы должны рассмотреть три случая.

Первый случай: формула содержит оба равенства, то есть она содержит фрагмент $f(X) = s \wedge g(X) = e$. Воспользуемся Леммой 6, согласно которой такая формула эквивалентна бескванторной.

Второй случай: формула содержит только одно равенство:

$$(\exists X)(f(X) + n < g(X) \wedge l < f(X) < t \wedge \\ \wedge z < g(X) < d \wedge g(X) = e \wedge \\ \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p).$$

Сделаем некоторые эквивалентные преобразования и получим в результате формулу

$$z < e < d \wedge (\exists X)(f(X) + n < e \wedge l < f(X) < t \wedge g(X) = e \wedge \\ \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p).$$

Заменим неравенство $f(X) < t$ на $f(X) < t'$, где $t' = \min\{t, e-n\}$. То есть $t'$ либо равняется $e-n$, либо меньше $e-n$. Тогда можем считать фрагмент $f(X)+n < e$ частным случаем фрагмента $f(X) < t'$.

Элементарная конъюнкция преобразуется в

$$t < e - n \wedge (\exists X)(g(X) = e \wedge l < f(X) < t' \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p).$$

Воспользуемся теми же приемами, что и в Лемме 5. Во-первых, будем считать, что значение константы $p$ невелико, то есть формула содержит фрагмент $t' - p - 1 \leq l$ (в противном случае, если также имеет место неравенство $l + 1 < t$, формула точно будет истинна, поскольку количество возможных вариантов состава множества $X$ будет превышать количество $w_i$). Далее, добавим к формуле дизъюнкцию

$$\bigvee_{j=2}^{p+1} (l + j = t' \wedge \bigvee_{\alpha=1}^{j-1} f(X) = l + \alpha).$$

Тогда в результате мы получим формулы следующего вида

$$(\exists X)(f(X) = l + \alpha \wedge g(X) = e \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p).$$

где $\alpha \in \{1, \ldots, j-1\}$. Данные формулы, аналогичны формуле, рассмотренной в Лемме 6.

Третий случай: формула не содержит равенств. Тогда имеем дело с формулой вида

$$(\exists X)(f(X) + n < g(X) \wedge l < f(X) < t \wedge z < g(X) < d \wedge \\ \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p).$$

Для того чтобы свести формулу к формулам уже рассмотренным, достаточно «зафиксировать» значение $g(X)$. Произведем действия аналогичные действиям в Лемме 5.

Рассмотрим интервал $(l+n, d)$. Если он достаточно велик, то есть $d-l-n > p+1$, и если при этом выполнено условие $l + 1 < t$, то множество $X$ гарантированно существует. В противном случае, когда $d - l - n \leq p + 1$, требуется дальнейшее рассмотрение формулы. Поэтому первое что мы сделаем — добавим в формулу дизъюнкцию

$$(d - n - p - 1 > l \vee d - n - p - 1 \leq l).$$

Тогда после раскрытия скобок будем рассматривать только элементарные конъюнкции, содержащие фрагмент $d - l - n \leq p + 1$.

Далее добавим в формулу следующую дизъюнкцию

$$\bigvee_{j=2}^{p+1} (l + n + j = d \wedge \bigvee_{\alpha=1}^{j-1} g(X) = l + n + \alpha).$$

В результате получим формулы вида

$$(\exists X)(f(X) + n < g(X) \wedge l < f(X) < t \wedge g(X) = l + n + \alpha \wedge \\ \wedge \neg X = w_1 \wedge \ldots \wedge \neg X = w_p).$$

Эти формулы аналогичны формулам, рассмотренным в предыдущем случае. □

*Следствие* 2. Теория конечных подмножеств дискретного линейного порядка без первого и последнего элементов разрешима.

### Заключение

Мы доказали возможность эффективной элиминации кванторов в теории конечных подмножеств дискретного линейно упорядоченного множества. Ранее нами был доказан аналогичный результат для теории конечных подмножеств плотного линейно упорядоченного множества.

В дальнейшем интересно было бы получить ответы на следующие вопросы.

Отношение, которое мы определяем на подмножествах, является частичным порядком. Можем ли мы определить отношение так, чтобы порядок был тотальным и будет ли такая теория допускать элиминацию кванторов?

Еще один не менее важный вопрос — исследовать сложность алгоритмов разрешения теории конечных подмножеств.

## Список литературы

[1] Авхимович Н.В. О разрешимости теории конечных подмножеств для плотного линейного порядка // Актуальные проблемы прикладной математики, информатики и механики: сборник трудов Международной научной конференции. Воронеж, 2022. С. 1521–1525.

[2] Dudakov S.M. On Undecidability of Finite Subsets Theory for Torsion Abelian Groups // Mathematics. 2022. Vol. 10, № 3. ID 533.

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

[4] 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

[5] Rabin M.O. Decidability of second-order theories and automata on infinite trees // Bulletin of the American Mathematical Society. 1968. Vol. 74. Pp. 1025–1029.

[6] Дудаков С.М. Основы теории моделей. Тверь: Твер. гос. ун-т, 2013. 480 с.

## Образец цитирования

Авхимович Н.В. О разрешимости теории конечных подмножеств для дискретного линейного порядка // Вестник ТвГУ. Серия: Прикладная математика. 2022. № 3. С. 91–104. https://doi.org/10.26456/vtpmk646

## Сведения об авторах

1. **Авхимович Николь Вадимовна**
магистрант факультета прикладной математики и кибернетики Тверского государственного университета.

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

# ON DECIDABILITY OF FINITE SUBSETS' THEORY FOR DISCRETE LINEAR ORDER

**Avkhimovich Nicole Vadimovna**
Master student of the Faculty of Applied Mathematics and Cybernetics,
Tver State University
*Russia, 170100, Tver, Zhelyabova str., 33, TvSU.*
*E-mail: nicoleavkhimovich@mail.ru*

*Received 19.06.2022, revised 05.09.2022.*

Let us consider a discrete linear ordered set. On finite subsets of such set we introduce a new binary relation. This relation says that all items of a first set is less than all items of a second one. We show that the theory of such constructed structure admits quantifier elimination. For this purpose, we expand the language with four definable functions. As a corollary we get the theory of finite subsets of a discrete linear order to be decidable.

**Keywords:** theory, finite subsets, quantifiers elimination, discrete linear order, decidability.

## Citation

Avkhimovich N.V., "On decidability of finite subsets' theory for discrete linear order", *Vestnik TvGU. Seriya: Prikladnaya Matematika [Herald of Tver State University. Series: Applied Mathematics]*, 2022, № 3, 91–104 (in Russian). https://doi.org/10.26456/vtpmk646

## References

[1] Avkhimovich N.V., "On the solvability of finite subset theory for dense linear order", *Aktualnye problemy prikladnoj matematiki, informatiki i mekhaniki: sbornik trudov Mezhdunarodnoj nauchnoj konferentsii [Actual problems of applied mathematics, computer science and Mechanics: proceedings of the International Scientific Conference]*, Voronezh, 2022, 1521–1525 (in Russian).

[2] Dudakov S.M., "On Undecidability of Finite Subsets Theory for Torsion Abelian Groups", *Mathematics*, **10**:3 (2022), 533.

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

[4] 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.

[5] Rabin M.O., "Decidability of second-order theories and automata on infinite trees", *Bulletin of the American Mathematical Society*, **74** (1968), 1025–1029.

[6] Dudakov S.M., *Osnovy teorii modelej [Fundamentals of model theory]*, Tver State University, Tver, 2013 (in Russian), 480 pp.