

УДК 510.53

## ОРБИТЫ ЛИНЕЙНЫХ ОТОБРАЖЕНИЙ И СВОЙСТВА РЕГУЛЯРНЫХ ЯЗЫКОВ <sup>\*)</sup>

М. Н. Вялый, С. П. Тарасов

**Аннотация.** Установлена эквивалентность задачи о протыкании полиэдрального множества орбитой линейного отображения и задачи о пересечении регулярного языка с языком перестановок двоичных слов (перестановочным фильтром). Алгоритмическая разрешимость для обеих задач неизвестна. Первая из них обобщает хорошо известные открытые проблемы Сколема и неотрицательности, относящиеся к линейным рекуррентным последовательностям.

**Ключевые слова:** линейная рекуррентная последовательность, линейное отображение, орбита, регулярный язык, алгоритмическая разрешимость.

### Введение

Действие степеней линейного отображения  $\Phi: V \rightarrow V$  на вектор  $x$  векторного пространства  $V$  задаёт *орбиту*  $\text{Orb}_\Phi x = \{\Phi^k x \mid k \in \mathbb{Z}^+\}$ .

Рассматриваются алгоритмические задачи об орбитах линейных отображений. Для конструктивного задания орбиты считаем  $V$  координатным пространством над полем рациональных чисел  $\mathbb{Q}$ . В этом случае и вектор  $x$ , и матрица отображения  $\Phi$  могут быть указаны явно.

Под задачей описания орбиты понимаем задачу поиска таких соотношений, которые выполняются для всех векторов орбиты или нарушаются хотя бы для одного элемента орбиты. Здесь рассматриваем простейший случай, когда соотношения построены из линейных равенств и неравенств с помощью булевых операций. Точную формулировку см. ниже в разд. 2. Отметим, что самым важным примером задачи описания орбиты является задача о протыкании полиэдральной камеры. Она состоит в том, чтобы проверить, пересекает ли орбита некоторое множество, заданное набором нестрогих линейных неравенств.

---

<sup>\*)</sup>Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проекты 08–01–00414 (оба автора) и 09–01–00709 (первый автор)), и программы «Ведущие научные школы» (проект НШ–5294.2008.1) (первый автор).

Задачи описания орбит связаны с задачами о линейных рекуррентных последовательностях.

Линейная рекуррентная последовательность (ЛРП)  $x_n$  степени  $d$  задаётся соотношениями

$$\begin{cases} x_n = \sum_{i=1}^d a_i x_{n-i} & \text{при } n > d, \\ x_n = b_n & \text{при } 1 \leq n \leq d, \end{cases} \quad (1)$$

где  $a_i, b_j$  — константы.

Наиболее известная алгоритмическая задача о ЛРП называется *проблемой Сколема*.

**Проблема Сколема.** Задана ЛРП с целочисленными коэффициентами и начальными данными. Спрашивается, существует ли такое  $n$ , что  $x_n = 0$ ?

В настоящее время неизвестно, является ли проблема Сколема алгоритмически разрешимой. Известна её разрешимость для степеней  $\leq 5$  (случаи степеней 3 и 4 разобраны Н. В. Верещагиным [1], а случай степени 5 — Халавой и др. [11]).

Что касается утверждений о трудности, то наилучшим известным в настоящее время результатом является NP-трудность проблемы Сколема [8].

ЛРП называется *неотрицательной*, если все её члены неотрицательны. Проверка неотрицательности ЛРП называется *проблемой неотрицательности*. Эта задача не проще проблемы Сколема. Точный смысл этого утверждения состоит в том, что проблема Сколема сводится по Тьюрингу к проблеме неотрицательности (см. ниже доказательство утверждения 6).

В статье используются стандартные для теории алгоритмов и теории сложности понятия: сводимость по Тьюрингу,  $m$ -сводимость, полиномиальная сводимость. В частности, сводимость по Тьюрингу означает, что сводящий алгоритм может обращаться к оракулу, дающему ответ для задачи, к которой строится сводимость (подробнее см. [2, 3]).

Известна разрешимость проблемы неотрицательности для ЛРП степени  $\leq 3$  [12].

Подробнее связи между задачами описания орбит и задачами о ЛРП изложены в разд. 2. Материал этого раздела в основном не нов и приводится для замкнутости изложения и для того, чтобы ввести необходимую в дальнейшем терминологию.

В разд. 1 мы напоминаем основные факты о ЛРП. Кроме того, этот раздел содержит результат, который должен быть известен, но мы не обнаружили его в литературе\*. Он состоит в том (теорема 1), что любая ЛРП есть разность двух производящих функций регулярных языков. (Необходимые сведения из теории регулярных языков и конечных автоматов можно найти в книгах [6, 7].) Технически нам более полезна модификация этого результата — теорема 3 из разд. 4.

Основным новым результатом данной работы является установление связи между задачей о протыкании камеры орбитой линейного отображения и задачами проверки свойств регулярных языков. Свойство, проверка которого оказывается алгоритмически эквивалентной задаче о протыкании, состоит в том, что регулярный язык содержит хотя бы одно слово из специального множества слов. Мы называем это множество *перестановочным фильтром*. Неформально говоря, каждое слово из перестановочного фильтра задаёт перестановку на множестве всех двоичных слов некоторой длины  $n$ . Точное определение см. ниже в разд. 3.

Обозначаем перестановочный фильтр через  $P_{\mathbb{B}}$ , а соответствующую задачу проверки свойства регулярного языка называем *задачей  $P_{\mathbb{B}}$ -реализуемости* (см. разд. 3).

Доказательство алгоритмической эквивалентности задачи  $P_{\mathbb{B}}$ -реализуемости и задачи о протыкании камеры (теорема 2 из разд. 3) оказывается довольно длинным.

В одну сторону удаётся построить полиномиальную сводимость задачи о протыкании к задаче  $P_{\mathbb{B}}$ -реализуемости. Построению этой сводимости посвящён разд. 4. Эта сводимость опирается на уже упомянутую теорему 3.

Следствием этой сводимости, представляющим самостоятельный интерес, является теорема 4, которая утверждает, что задача  $P_{\mathbb{B}}$ -реализуемости NP-трудна.

При сводимости в другую сторону — задачи  $P_{\mathbb{B}}$ -реализуемости к задаче о протыкании — возникает дополнительная трудность. Естественная конструкция, описанная в п. 5.1, даёт сводимость задачи  $P_{\mathbb{B}}$ -реализуемости к задаче о протыкании сдвига целочисленного конуса, заданного образующими. Свести эту задачу к задаче о протыкании сдвига рационального конуса оказывается непросто. Построение этой сводимости описано в п. 5.2. В качестве промежуточного шага мы строим такую своди-

---

\*Пока статья готовилась к печати, мы узнали от проф. Дж. Шаллита, что этот факт приводится в книге [13], см. следствие 8.2. Авторы благодарны проф. Дж. Шаллиту.

мость для случая симплицального конуса, образующие которого линейно независимы. Общий случай сводится к симплицальному с помощью представления произвольного целочисленного конуса как объединения конечного множества и конечного набора сдвигов симплицальных целочисленных конусов (теорема 6). Этот результат имеет самостоятельный интерес и может рассматриваться как новый целочисленный вариант теоремы Каратеодори (более непосредственный целочисленный вариант теоремы Каратеодори активно изучается, см., например, [9, 10]; он имеет важные приложения в комбинаторной оптимизации).

### 1. Алгебраические и комбинаторные свойства ЛРП

ЛРП обладают многими замечательными алгебраическими и комбинаторными свойствами. Приведём те из них, которые понадобятся в дальнейшем. Об этих и других свойствах ЛРП см. [5, 7, 11].

1. Если  $A$  — линейный оператор на пространстве  $V$ ,  $x, y \in V$ ,  $h$  — линейный функционал на  $V$ , то производящая функция

$$f_{A,x,y}(t) = \sum_{r \geq 0} h(A^r x - y) t^r \quad (2)$$

рациональна.

2. Коэффициенты ряда Тейлора любой рациональной функции образуют ЛРП, и производящая функция любой ЛРП рациональна.

3. Множество ЛРП замкнуто относительно почленных операций сложения и умножения (т. е. адамарова произведения последовательностей).

Во введении мы сформулировали проблему Сколема в стандартном виде — для целочисленных последовательностей. Если нас интересуют знаки членов последовательности, то разницы между целочисленными и рациональными ЛРП нет.

Действительно, пусть (1) имеет рациональные коэффициенты и начальные данные. Обозначим через  $N$  наименьшее общее кратное знаменателей всех этих чисел. Построим целочисленную ЛРП

$$y_n = \begin{cases} \sum_{i=1}^d N^i a_i y_{n-i} & \text{при } n > d, \\ y_n = N^{n+1} b_n & \text{при } 1 \leq n \leq d, \end{cases} \quad (3)$$

**Утверждение 1.** Для всех  $n$  выполнено  $N^{n+1} x_n = y_n$ .

**Доказательство.** Для  $1 \leq n \leq d$  утверждение следует из определения (3).

Для  $n > d$  утверждение леммы проверяется по индукции. Предполагая, что оно выполнено для всех  $n < k$ , получаем для  $k$  следующую цепочку равенств:

$$y_k = \sum_{i=1}^d N^i a_i y_{k-i} = \sum_{i=1}^d N^i a_i (x_{k-i} N^{k-i+1}) = \sum_{i=1}^d N^{k+1} a_i x_{k-i} = N^{k+1} x_k,$$

из которой следует выполнение утверждения леммы при  $n = k$ . Утверждение 1 доказано.

**Замечание 1.** НОК строится за полиномиальное от длины записи чисел время с использованием алгоритма Евклида и равенства

$$\text{НОК}(x, y) = \frac{xy}{\text{НОД}(x, y)}.$$

Поэтому указанная в утверждении 1 последовательность  $y_n$  строится по последовательности  $x_n$  за полиномиальное время.

Некоторые ЛРП являются решением перечислительных комбинаторных задач и потому неотрицательны. Таковы, например,  $\mathbb{N}$ -рациональные последовательности, которые совпадают с производящими функциями для регулярных языков [7]. Будем называть  $\mathbb{N}$ -рациональные последовательности *регулярными*.

Более точно, детерминированный автомат  $A$  в алфавите  $\Sigma$  определяет ЛРП  $s_n$ , где

$$s_n(A) = \#\{w \mid A(w) \wedge |w| = n\}. \quad (4)$$

Последовательности вида (4) и будем называть *регулярными*.

Общая ЛРП не является регулярной хотя бы потому, что все автоматные последовательности неотрицательны. Однако имеет место следующая

**Теорема 1** [13, следствие 8.2]. *Любая ЛРП является разностью двух регулярных последовательностей.*

По набору целых чисел  $a_1, \dots, a_d, b_1, \dots, b_d$  построим алфавит  $\mathcal{P}$  следующим образом:

$$\mathcal{P} = \bigcup_{i=1}^d A_i \bigcup_{j=1}^d B_j, \quad |A_i| = |a_i|, \quad |B_j| = |b_j|,$$

$$A_i \cap A_j = B_i \cap B_j = \emptyset \quad (\text{при } i \neq j), \quad A_i \cap B_j = \emptyset.$$

Символ из  $A_i$  или  $B_j$  будем называть *положительным*, если  $a_i > 0$  (соответственно  $b_j > 0$ ), и *отрицательным*, если  $a_i < 0$  (соответственно  $b_j < 0$ ). Введём также *функцию длины* на алфавите  $\mathcal{P}$ :

$$\ell(x) = \begin{cases} i, & x \in A_i, \\ j, & x \in B_j. \end{cases}$$

**Определение 1.** *Каноническим* назовём слово вида

$$\beta^{\ell(\beta)} \alpha_1^{\ell(\alpha_1)} \alpha_2^{\ell(\alpha_2)} \dots \alpha_k^{\ell(\alpha_k)}, \text{ где } k \geq 0, \quad (5)$$

$\beta \in \bigcup_j B_j$ ,  $\alpha_i \in \bigcup_i A_i$ , причём в случае  $k > 0$  выполняется неравенство  $\ell(\beta) + \ell(\alpha_1) > d$ . Если среди символов  $\beta, \alpha_1, \dots, \alpha_k$  содержится чётное число отрицательных символов, то слово будем считать *положительным*, в противном случае — *отрицательным*.

**Утверждение 2.** *Количество положительных (отрицательных) канонических слов длины  $n$  — регулярная последовательность.*

Это утверждение очевидно вытекает из определения, поскольку (5) легко переписывается в виде регулярного выражения, а подсчёт чётности числа положительных (отрицательных) символов среди  $\beta, \alpha_1, \dots, \alpha_k$  может быть выполнен конечным автоматом.

**Утверждение 3.** *Пусть последовательность  $x_n$  задана соотношениями (1) для целых  $a_i, b_j$ . Тогда  $x_n$  равно разности количества положительных и отрицательных канонических слов длины  $n$ , построенных по числам  $a_i, b_j$ .*

**ДОКАЗАТЕЛЬСТВО.** Обозначим через  $p_k$  ( $n_k$ ) число положительных (отрицательных) канонических слов. Равенство

$$x_k = p_k - n_k \quad (6)$$

будем доказывать по индукции.

Для  $1 \leq k \leq d$  (6) следует из определения.

Пусть (6) доказано для  $k < N$ . Имеем цепочку равенств

$$\begin{aligned} x_N &= \sum_{i=1}^d a_i x_{N-i} = \sum_{i=1}^d a_i (p_{N-i} - n_{N-i}) \\ &= \left( \sum_{i:a_i>0} a_i p_{N-i} + \sum_{i:a_i<0} (-a_i) n_{N-i} \right) - \left( \sum_{i:a_i>0} a_i n_{N-i} + \sum_{i:a_i<0} (-a_i) p_{N-i} \right) \\ &= p_N - n_N. \end{aligned}$$

Здесь первое равенство — определение ЛРП (1), второе — предположение индукции, а последнее следует из определения канонического слова. Утверждение 3 доказано.

Теорема 1 следует из утверждения 3.

## 2. Орбиты линейных отображений и ЛРП

В этом разделе дадим точную формулировку задач описания орбиты линейного отображения, введём родственную задачу о протыкании камеры и установим связь между этими задачами и задачами о ЛРП.

Пусть дан набор  $h_1, \dots, h_m$  линейных (необязательно однородных) функций на координатном пространстве  $\mathbb{Q}^d$ . Наборы знаков этих функций определяют разбиение пространства  $\mathbb{Q}^d$  на камеры. Более точно, пусть  $s \in \{\pm 1, 0\}^m$ . Тогда камера  $H_s$  — это множество

$$\{x \in \mathbb{Q}^d \mid \text{sign}(h_i(x)) = s_i \text{ для } 1 \leq i \leq m\},$$

где  $\text{sign}(t)$  — стандартная функция знака:

$$\text{sign}(t) = \begin{cases} 1 & \text{при } t > 0, \\ 0 & \text{при } t = 0, \\ -1 & \text{при } t < 0. \end{cases}$$

**Задача описания орбиты (ЗОО).** Даны матрица  $\Phi$  порядка  $d$ , вектор  $x_0$  размерности  $d$ , множество линейных функций  $h_1, \dots, h_m$  от  $d$  переменных и набор знаковых векторов  $s_1, \dots, s_r \in \{\pm 1, 0\}^m$ .

Требуется проверить, что любая точка орбиты  $\text{Orb}_\Phi x_0$  лежит в объединении камер  $H_{s_1}, \dots, H_{s_r}$ .

**Задача о протыкании камеры (ЗПК).** Даны матрица  $\Phi$  порядка  $d$ , вектор  $x_0$  размерности  $d$ , множество линейных функций  $h_1, \dots, h_m$  от  $d$  переменных и знаковый вектор  $s$ .

Требуется проверить, что орбита  $\text{Orb}_\Phi x_0$  пересекает камеру  $H_s$ .

**Утверждение 4.** ЗПК сводима по Тьюрингу к ЗОО, и наоборот.

**ДОКАЗАТЕЛЬСТВО.** Чтобы свести ЗПК к ЗОО возьмём дополнение в множестве  $\{\pm 1, 0\}^m$  к знаковому вектору камеры, заданной в ЗПК. Остальные данные для ЗОО сохраним те же, что и в ЗПК. Ясно, что ответ в построенной задаче ЗОО противоположен ответу в исходной задаче ЗПК: орбита не протыкает камеру тогда и только тогда, когда она целиком лежит в дополнении к этой камере.

В обратную сторону рассуждаем аналогично. Для каждой камеры, не входящей в заданный набор камер, решаем задачу ЗПК. Если ответы во всех этих задачах негативные, то это означает, что орбита лежит в объединении камер из заданного набора, так что ответ в ЗОО позитивный. Если же хотя бы один из ответов в построенном наборе ЗПК позитивный, то ответ в ЗОО негативный. Утверждение 4 доказано.

Теперь укажем связь между проблемами Сколема, неотрицательности и приведёнными выше задачами.

**Утверждение 5.** Проблема неотрицательности эквивалентна ЗОО с одной линейной функцией и нестрогим неравенством (камеры  $H_0, H_{+1}$ ).

Проблема Сколема эквивалентна ЗПК с одной линейной функцией и равенством (камера  $H_0$ ).

**Доказательство.** С ЛРП (1) свяжем линейный оператор  $A$ , действующий на  $d$ -мерном координатном пространстве. Матрица этого оператора имеет вид

$$A = \begin{pmatrix} a_1 & a_2 & \dots & a_{d-1} & a_d \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ & & \dots & & \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}. \quad (7)$$

Легко проверить по индукции, что

$$A^k(b_d, \dots, b_1)^T = (x_{k+d}, x_{k+d-1}, \dots, x_{k+1})^T.$$

Поэтому проблема Сколема для ЛРП (1) сводится к ЗПК, в которой  $\Phi = A$ ,  $x_0 = (b_d, \dots, b_1)^T$ ,  $h_1 = x_d$  и камера  $H_0$ .

Аналогично, проблема неотрицательности сводится к ЗОО с теми же данными и набором камер  $H_0, H_{+1}$ .

Доказательство обратной сводимости опирается на стандартные факты о ЛРП, которые приведены в разд. 1. Действительно, производящая функция  $\sum_n h(A^n x_0) t^n$  рациональна. Следовательно, последовательность  $h(A^n x_0)$  является ЛРП, откуда получаем сводимость. Утверждение 5 доказано.

В настоящее время неизвестна сводимость общих задач описания орбиты и протыкания камеры к проблеме неотрицательности и проблеме



Сколема соответственно. Однако можно указать несколько случаев, когда такая сводимость имеет место.

**Задача о протыкании объединения подпространств (ЗПП).** Даны матрица  $\Phi$  порядка  $d$ , вектор  $x_0$  размерности  $d$ , множество линейных функций  $h_{jk}$  от  $d$  переменных,  $1 \leq j \leq m$ ,  $1 \leq k \leq r_j$ .

Требуется проверить, что орбита  $\text{Orb}_\Phi x_0$  пересекает камеру, которая является объединением аффинных подпространств:

$$\bigcup_{j=1}^m \{x \mid h_{j1}(x) = h_{j2}(x) = \dots = h_{jr_j}(x) = 0\}.$$

**Лемма 1.** ЗПП сводится к проблеме Сколема.

**ДОКАЗАТЕЛЬСТВО.** Из указанных в разд. 1 фактов следует, что последовательности  $\varphi_n(j, k) = h_{jk}(\Phi^n x_0)$  являются ЛРП. Но тогда последовательность

$$\varphi_n = \prod_{j=0}^m \sum_{k=1}^{s_j} \varphi_n(j, k)^2$$

также является ЛРП в силу замкнутости множества ЛРП относительно почленного сложения и умножения.

Заметим, что представление последовательности  $\varphi_n$  в виде (1) строится алгоритмически по данным ЗПП.

А так как  $\varphi_n = 0$  тогда и только тогда, когда для некоторого  $j$  выполняется

$$\varphi_n(j, 1) = \varphi_n(j, 2) = \dots = \varphi_n(j, s_j) = 0,$$

мы получили сводимость задачи ЗПП к проблеме Сколема. Лемма 1 доказана.

**Замечание 2.** В доказательстве леммы 1 построена  $m$ -сводимость. Однако она не является полиномиальной: степень последовательности  $\varphi$  может оказаться экспоненциально большой по сравнению с размерностью пространства.

Впрочем, можно заметить, что ответ в общей ЗПП является дизъюнкцией ответов в наборе задач о протыкании одного подпространства. Для этого частного случая описанная выше сводимость полиномиальна. ЗПП может быть решена за полиномиальное время с оракулом проблемы Сколема. Другими словами, ЗПП полиномиально сводится к проблеме Сколема по Тьюрингу.

Известная теорема Сколема — Леха — Малера [7, 11, 13] утверждает, что множество нулей ЛРП является объединением конечного множества

и конечного числа арифметических прогрессий. Из доказательства леммы 1 легко извлечь аналогичное следствие для задачи о протыкании объединения подпространств.

**Следствие** (теорема Сколема — Леха — Малера для задачи о протыкании). *Множество тех  $k$ , для которых  $\Phi^k x_0$  принадлежит объединению подпространств  $V_1, \dots, V_m$ , является объединением конечного множества и конечного числа арифметических прогрессий.*

**Задача об описании полиэдром (ЗОП).** Это частный случай ЗОО, когда набор камер состоит ровно из одной замкнутой камеры (т.е. все неравенства нестрогие).

**Лемма 2.** *ЗОП сводится к проблеме неотрицательности.*

**Доказательство.** Без ограничения общности можно считать, что камера в ЗОП задаётся знаковым вектором  $(+1, \dots, +1)$  (внутренность полиэдра) и векторами, в которых часть единиц заменена нулями (границы полиэдра). Действительно, переменной знака линейной функции можно убрать из знакового вектора все отрицательные компоненты. А нулевые компоненты убираются после проверки того, что орбита лежит в (аффинном) подпространстве, которое является решением соответствующей системы уравнений. Последняя задача алгоритмически разрешима, так как аффинная оболочка орбиты совпадает с аффинной оболочкой первых  $d + 1$  элементов орбиты.

Из последовательностей  $\varphi_n(j) = h_j(\Phi^n x_0)$  составим одну последовательность  $\varphi_n$ , размещая члены последовательности  $\varphi_n(j)$  на местах, индексы которых дают остаток  $j$  по модулю  $m$ . Полученная последовательность является ЛРП. Действительно, обозначим производящую функцию для  $\varphi_n(j)$  через  $f_j(t)$ , а производящую функцию для  $\varphi_n$  — через  $f(t)$ . Тогда функция

$$f(t) = \sum_{j=1}^m t^j f_j(t^m)$$

рациональна как сумма рациональных функций. Лемма 2 доказана.

Проблема Сколема — самая слабая из рассмотренных нами задач. Легко заметить, что для её разрешимости достаточно перечислимости множества неотрицательных ЛРП или позитивных случаев ЗОП (поскольку в лемме 2 фактически построена  $m$ -сводимость).

**Утверждение 6.** *Если множество неотрицательных ЛРП перечислимо, то проблема Сколема разрешима.*

ДОКАЗАТЕЛЬСТВО. Если  $x_n$  — ЛРП, то и  $x_n^2 - 1$  тоже является ЛРП, так как множество ЛРП замкнуто относительно почленного (адамарова) произведения и взятия сумм/разностей, см. разд. 1.

Но  $x_n^2 - 1$  неотрицательна тогда и только тогда, когда  $x_n \neq 0$  для всех  $n$ .

Далее применяем теорему Поста [2].

Перечисляя все неотрицательные последовательности и сравнивая их с  $x_n^2 - 1$ , а также параллельно перечисляя все последовательности, принимающие значение 0, мы рано или поздно обнаружим данную последовательность либо в одном, либо в другом списке. Утверждение 6 доказано.

### 3. ЗПК и регулярные языки

Установим связь между проблемой Сколема и свойствами регулярных языков. Более точно, рассмотрим алгоритмические задачи *регулярной реализуемости*: существует ли в данном регулярном языке слово, удовлетворяющее некоторому заданному свойству.

Технически задачу регулярной реализуемости удобнее задать так. Пусть  $L$  — язык в конечном алфавите  $\Sigma$ . Входом задачи  $L$ -реализуемости является описание некоторого регулярного языка  $R$  в алфавите  $\Sigma$ . По этому описанию необходимо проверить непустоту пересечения  $L \cap R$ .

**Замечание 3.** В зависимости от способа задания регулярного языка получаем разные, вообще говоря, варианты задачи  $L$ -реализуемости. Мы принимаем в качестве основного способа задания языка описание полного детерминированного автомата, принимающего этот язык. Разумеется, это уточнение несущественно, когда речь идёт лишь об алгоритмической разрешимости, и становится важным при анализе вычислительной сложности разрешимых задач.

Определим *перестановочный фильтр*  $P_{\mathbb{B}}$  как множество слов в алфавите  $\{\#, 0, 1\}$  вида  $\#w_1\#w_2\#\dots w_N\#$ , где  $N = 2^n$  для некоторого  $n \geq 1$ , а множество слов  $w_i$  совпадает с множеством двоичных слов длины  $n$ .

Неформально говоря, каждое слово из языка  $P_{\mathbb{B}}$  задаёт перестановку на множестве всех двоичных слов некоторой длины  $n$ .

**Теорема 2.** Задача  $P_{\mathbb{B}}$ -реализуемости и ЗПК взаимно сводятся по Тьюрингу.

Две указанные в теореме 2 сводимости имеют существенно разную сложность.

В следующем разделе мы построим полиномиальную сводимость ЗПК к задаче  $P_{\mathbb{B}}$ -реализуемости. Отсюда, как следствие, получается NP-труд-

ность задачи  $P_{\mathbb{B}}$ -реализуемости. Действительно, из утверждения 5 следует, что проблема Сколема полиномиально сводится к ЗПК, а проблема Сколема NP-трудна [8].

В разд. 5 построим сводимость в обратную сторону. Однако эта сводимость требует сверхэкспоненциального времени.

#### 4. Полиномиальная сводимость ЗПК к задаче $P_{\mathbb{B}}$ -реализуемости

Общее описание сводимости таково: по каждому неравенству (или равенству), задающему камеру, и линейному отображению строится ЛРП, задающая последовательность коэффициентов степенного ряда (2). Она, точнее, связанная с нею по утверждению 1 целочисленная последовательность (3), может быть представлена как разность двух регулярных ЛРП по теореме 1. Однако для построения полиномиальной сводимости этого недостаточно, и мы представим данную последовательность как разность значений двух регулярных последовательностей на некоторой арифметической прогрессии их номеров, что уже можно сделать за полиномиальное время. Затем строится специальный автомат, который по некоторому, предположительно перестановочному, слову сравнивает количество слов в двух регулярных языках. Этого окажется достаточным для построения сводимости проблемы Сколема к задаче  $P_{\mathbb{B}}$ -реализуемости. Для завершения сводимости в общем случае потребуется еще конструкция, объединяющая несколько таких автоматов в один.

Теперь приступим к реализации этого плана.

Прежде всего нужно проверить, что если все компоненты квадратной матрицы  $A$  порядка  $d$ , вектора  $x_0$  и линейной функции  $h$  рациональны, то существует полиномиальный алгоритм, который находит коэффициенты ЛРП для последовательности  $h(A^n x_0)$ . Действительно, степень такой ЛРП не превосходит порядка матрицы. Значит, коэффициенты ЛРП и начальные данные находятся из решения системы линейных уравнений относительно первых  $2d$  членов последовательности.

Далее рассматриваем только ЛРП с целочисленными коэффициентами и начальными данными, что в силу утверждения 1 не ограничивает общности, так как нас интересует только функция знака от  $h(A^n x_0)$  (напомним, что функция  $h$  не обязательно однородная).

Покажем, что любая ЛРП может быть представлена как сумма весов маршрутов длины  $n$  по некоторому графу, начало и конец которых фиксированы. Вес маршрута определяется так: на рёбрах графа заданы целочисленные веса  $c: E \rightarrow \mathbb{Z}$ , *вес маршрута* — произведение весов вхо-

дящих в него рёбер. Заметим, что мы рассматриваем ориентированные графы, в которых допустимы петли и параллельные рёбра.

**Лемма 3.** Существует полиномиальный алгоритм, который по ЛРП  $x_n$  с целочисленными коэффициентами и начальными данными строит такой взвешенный граф  $G_x$  с двумя отмеченными вершинами  $u, v$ , что сумма весов маршрутов длины  $n$  между  $u$  и  $v$  равна  $x_n$  для любого  $n \geq 1$ .

**Доказательство.** Рассмотрим ЛРП вида (1) с целочисленными коэффициентами и начальными данными. Построим по ней граф следующим образом.

Между начальной  $u$  и конечной  $v$  вершинами проведём  $d$  вершинно не пересекающихся путей  $P_1, \dots, P_d$  таких, что длина пути  $P_i$  равна  $i$ . Проведём также  $d$  вершинно не пересекающихся циклов  $C_1, \dots, C_d$ , проходящих через  $b$ . Длина цикла  $C_i$  также равна  $i$ . Циклы  $C_i$  не имеют общих вершин с путями  $P_j$  за исключением вершины  $v$ .

Весы всех рёбер на путях и циклах полагаем равными 1, за исключением первых рёбер. Обозначим вес первого ребра пути  $P_i$  через  $p_i$ , а вес первого ребра цикла  $C_i$  через  $q_i$ .

Вычислим сумму весов маршрутов длины  $n$  из  $u$  в  $v$ , которую обозначим через  $z_n$ . Такая сумма выражается через суммы весов более коротких маршрутов. При  $n \leq d$  существуют маршруты по путям из  $u$  в  $v$ , а при  $n > d$  любой маршрут длины  $n$  получается из более короткого маршрута добавлением одного из циклов длины  $1, \dots, d$ . Поэтому

$$z_i = \begin{cases} p_i + \sum_{j=1}^{i-1} q_{i-j} z_j & \text{при } 1 \leq i \leq d, \\ \sum_{j=1}^d q_j z_{n-j} & \text{при } n > d. \end{cases}$$

Чтобы добиться равенств  $z_n = x_n$ , необходимо положить  $q_j = a_j$ .

При  $1 \leq i \leq d$  должно выполняться  $z_i = b_i$ , поэтому

$$\begin{aligned} p_1 &= b_1, \\ p_2 &= b_2 - q_1 b_1, \\ p_3 &= b_3 - q_1 b_2 - q_2 b_1, \\ &\dots \end{aligned}$$

Для завершения доказательства заметим, что все указанные вычисления можно проделать за полиномиальное время. Лемма 3 доказана.

Для построения сводимости нам потребуется также представление заданного положительного целого числа как числа путей между двумя вершинами в графе.

**Лемма 4.** Существует полиномиальный алгоритм, который по положительным целым числам  $n$  (в двоичной записи),  $k$  (в унарной записи) при условии  $k > \log_2 n$  строит граф с начальной и конечной вершинами  $u, v$  такой, что число путей из  $u$  в  $v$  длины  $k$  равно  $n$ .

**ДОКАЗАТЕЛЬСТВО.** Прежде всего для каждого  $k$  выберем такой граф и такие его вершины, между которыми ровно  $2^k$  маршрутов. Подходит, например, граф  $L_k$ , который получается из ориентированного пути длины  $k$  добавлением к каждому ребру параллельного ему ребра.

Теперь для каждого ненулевого разряда  $j$  в двоичной записи  $n$  дополним граф  $L_j$  путём длины  $k - j$ . Склеим все начальные вершины полученных графов в вершину  $u$ , а все конечные — в вершину  $v$ . Количество путей из вершины  $u$  в вершину  $v$  в полученном графе равно сумме  $2^j$  по графам  $L_j$ . По построению это число равно  $n$ .

Ясно, что описанный алгоритм может быть реализован за полиномиальное время. Лемма 4 доказана.

Используя представление ЛРП как суммы весов маршрутов в графе и представление любого положительного числа как числа маршрутов в графе, можно доказать следующий вариант теоремы 1.

**Теорема 3.** Существует полиномиальный алгоритм, который по ЛРП  $x_n$  с целочисленными коэффициентами и начальными данными строит число  $\ell$  и автоматы  $A$  и  $B$  в алфавите  $\{0, 1\}$  такие, что

$$x_n = s_{\ell n}(A) - s_{\ell n}(B)$$

для любого  $n \geq 1$ . При этом число  $\ell$  полиномиально ограничено длиной записи данных ЛРП (коэффициентов и начальных данных).

**ДОКАЗАТЕЛЬСТВО.** Первый шаг описан в лемме 3. Получаем граф  $H$ . Далее используем лемму 4 и заменяем граф  $H$  таким, у вершин которого все полустепени исхода равны 2, а веса рёбер по модулю равны 1.

Опишем это преобразование более подробно. Полагаем  $\ell = m + k$ , где  $m > \log_2 \max\{|a_1|, \dots, |a_d|, |b_1|, \dots, |b_d|\}$  и  $k > \log_2(2md)$ . По лемме 4 построим для  $|a_i|, |b_i|$  графы  $A_i, B_i$  с нужным числом путей длины  $m$  между начальной и конечной вершинами.

В графе  $H$  для всех  $i$  заменим первое ребро пути  $P_i$  на граф  $B_i$  так, чтобы начальная вершина  $B_i$  совпадала с начальной вершиной ребра, а конечная — с конечной вершиной ребра; аналогично заменим первое ребро цикла  $C_i$  на граф  $A_i$ . Остальные рёбра заменим путями длины  $\ell$ .

Заменим начальную и конечную вершины преобразованного графа  $H'$  (степени этих вершин не превосходят  $2md$ ) на корневые направленные

двоичные деревья глубины  $k$ , листья которых соответствуют выходящим из вершины рёбрам.

В построенном графе есть вершины с полустепенью исхода 1. Добавим вспомогательную вершину  $f$  и рёбра из всех вершин с полустепенью исхода 1 в  $f$ . Добавим также две петли в  $f$ , чтобы её полустепень исхода также равнялась 2.

Веса рёбер полученного графа полагаем равными 1 за исключением тех рёбер, которые выходят из листьев деревьев, вклеенных в начальную (конечную) вершину. Таким рёбрам приписывается вес, который совпадает со знаком  $a_i$  (соответственно  $b_i$ ), где  $i$  — номер графа  $A_i$  (соответственно  $B_i$ ), из которого взято данное ребро.

Обозначим полученный граф через  $G$ . Из построения ясно, что сумма весов маршрутов из  $u$  в  $v$  длины  $\ell n$  равна  $x_n$ .

Теперь построим автоматы  $A$  и  $B$  с множеством состояний  $\{\pm 1\} \times V(G)$ . Разметим рёбра графа  $G$  числами 0 и 1 так, чтобы из каждой вершины выходило ровно одно ребро с меткой 1 и ровно одно ребро с меткой 0.

Опишем правила работы автомата  $A$ . Начальное состояние  $(+1, u)$ , принимающее состояние  $(+1, v)$ . Из состояния  $(\sigma, w)$  автомат  $A$  переходит в состояние  $(\sigma, w')$ , если он читает символ  $\alpha$ , а в графе  $G$  есть ребро  $(w, w')$  положительного веса, размеченное символом  $\alpha$ . Из состояния  $(\sigma, w)$  автомат  $A$  переходит в состояние  $(-\sigma, w')$ , если он читает символ  $\alpha$ , а в графе  $G$  есть ребро  $(w, w')$  отрицательного веса, размеченное символом  $\alpha$ .

Аналогично устроен автомат  $B$ . Но в этом случае принимающим состоянием будет  $(-1, v)$ .

Все описанные построения можно выполнить эффективно (за полиномиальное от длины входа время).

Заметим также, что по построению графа  $G$  все слова, принимаемые автоматами  $A$  и  $B$ , имеют длину, кратную  $\ell$ .

Кроме того,  $x_n$  равно разности между количеством слов длины  $\ell n$ , принимаемых автоматами  $A$  и  $B$ . Действительно, маршруты отрицательного веса отвечают словам, принимаемым автоматом  $B$ , а маршруты положительного веса — словам, принимаемым автоматом  $A$ . Теорема 3 доказана.

Опишем полиномиальную сводимость проблемы Сколема к задаче  $P_{\mathbb{F}}$ -реализуемости.

Из теоремы 3 следует, что достаточно указать такой полиномиальный по времени алгоритм, который по паре автоматов  $A, B$  в алфавите

$\{0, 1\}$  и числу  $\ell$ , представленному в унарной записи, строит такой автомат  $C$ , что  $L(C) \cap P_{\mathbb{B}} \neq \emptyset$  тогда и только тогда, когда для некоторого  $n$  выполняется  $s_{\ell n}(A) = s_{\ell n}(B)$ .

Идея построения состоит в том, что если  $s_{\ell n}(A) = s_{\ell n}(B)$ , то для удачной перестановки двоичных слов длины  $\ell n$  это свойство проверяется автоматом: нужно расположить парами слова из симметрической разности языков, принимаемых автоматами  $A$ ,  $B$ . Ясно также, что такое расположение возможно лишь при  $s_{\ell n}(A) = s_{\ell n}(B)$  (делимость длины на  $\ell$  будет проверяться отдельно).

Для реализации этой идеи нам нужен автомат  $C$ , который моделирует работу обоих автоматов  $A$  и  $B$ , а на каждом символе  $\#$  проверяет условия корректности.

Опишем этот автомат подробнее. Обозначим множества состояний автоматов  $A$  и  $B$  через  $Q(A)$  и  $Q(B)$  соответственно. Множество состояний автомата  $C$  состоит из множества  $Q(A) \times Q(B) \times [0, \dots, \ell - 1] \times S$ , элементы множества  $S$  мы для наглядности обозначим словами

нет, да, возможно, В.

Начальным состоянием автомата  $C$  является четвёрка

$$(q(0, A), q(0, B), 0, \text{возможно}),$$

здесь  $q(0, A)$ ,  $q(0, B)$  обозначают начальные состояния автоматов  $A$  и  $B$  соответственно.

Принимающими состояниями автомата  $C$  являются состояния с четвёртой компонентой **да**.

Когда автомат  $C$  читает символ из множества  $\{0, 1\}$ , он изменяет первые две компоненты своего состояния в соответствии с таблицами переходов автоматов  $A$  и  $B$ , третью увеличивает на 1 по модулю  $\ell$ , а четвёртую не меняет.

Когда автомат  $C$  читает символ  $\#$ , четвёртая компонента изменяется по следующим правилам:

- (i) если четвёртая компонента **нет**, то она не меняется;
- (ii) если третья компонента не равна 0, то четвёртая компонента изменяется на **нет**;
- (iii) если четвёртая компонента **возможно**, то она меняется на **да**;
- (iv) если первая компонента не принадлежит множеству принимающих состояний  $A$ , а вторая компонента принадлежит множеству принимающих состояний  $B$ , то четвёртая компонента **В** заменяется на **да**, а все остальные — на **нет**;



(v) если первая компонента принадлежит множеству принимающих состояний  $A$ , а вторая компонента не принадлежит множеству принимающих состояний  $B$ , то четвёртая компонента **да** заменяется на **В**, а все остальные — на **нет**;

(vi) если обе первые компоненты одновременно принадлежат или не принадлежат множествам принимающих состояний автоматов  $A$  и  $B$ , то четвёртая компонента не меняется.

При чтении  $\#$  первые две компоненты состояния автомата  $C$  изменяются на  $q(0, A)$ ,  $q(0, B)$  соответственно, а третья — на 0.

Из приведённого описания автомата можно заключить, что он принимает лишь такие слова  $\#w_1\#w_2\#\dots w_N\#$  из перестановочного фильтра, для которых выполняются условия: длина слов  $\log_2 N$  кратна  $\ell$ , слова из симметрической разности языков  $L(A)$  и  $L(B)$  разбиты на пары так, что в последовательности  $w_i$  вначале встречается элемент пары из  $L(A) \setminus L(B)$ , а потом второй элемент пары из  $L(B) \setminus L(A)$ , причём все слова между ними принадлежат дополнению к симметрической разности.

Но эти условия равносильны тому, что автоматы  $A$  и  $B$  принимают одинаковое количество слов длины  $\log_2 N$ , которая кратна  $\ell$ . Таким образом, автомат  $C$  удовлетворяет требуемым свойствам.

Из доказанного в этом разделе и результатов [8] следует

**Теорема 4.** *Задача  $P_{\mathbb{B}}$ -реализуемости NP-трудна.*

Конструкцию автомата  $C$  легко модифицировать так, чтобы он принимал слово из перестановочного фильтра при условии  $s_{\ell n}(A) < s_{\ell n}(B)$ . Условие корректности для этого случая будет иметь вид: если из последовательности  $w_i$  удалить все слова из дополнения к симметрической разности  $L(A)$  и  $L(B)$ , то после каждого слова из  $L(A) \setminus L(B)$  следует слово из  $L(B) \setminus L(A)$  и после всех таких пар найдётся слово из  $L(B) \setminus L(A)$ . Ясно, что такое условие регулярно и размер автомата, который его проверяет, не более чем в константу раз превосходит размер описанного выше автомата  $C$ . Четвёртые компоненты **да** и **В** нужно в данном случае заменить множеством состояний автомата, принимающего регулярный язык  $(01)^*1^+$ .

Чтобы завершить построение сводимости ЗПК к задаче  $P_{\mathbb{B}}$ -реализуемости, нужно построить автомат, который комбинирует проверку нескольких условий вида  $s_{\ell n}(A) = s_{\ell n}(B)$  или  $s_{\ell n}(A) < s_{\ell n}(B)$ .

По неравенствам вида  $h_i(\Phi^n x_0) < 0$  (или равенствам  $h_i(\Phi^n x_0) = 0$ ), задающим камеру, построим пары автоматов  $A_i$ ,  $B_i$  и общее для всех них число  $\ell$  таким образом, что выполнение  $h_i(\Phi^n x_0) < 0$  ( $h_i(\Phi^n x_0) = 0$ )

равносильно выполнению  $s_{\ell n}(A) < s_{\ell n}(B)$  ( $s_{\ell n}(A) = s_{\ell n}(B)$ ).

Новым здесь является то, что нужно выбрать число  $\ell$  одинаковым для всех пар автоматов. Этого легко добиться, поскольку условия на  $\ell$  в доказательстве теоремы 3 нежесткие. Достаточно взять  $\ell$ , которое больше утроенного максимума логарифмов данных всех ЛРП и их степеней. Модификация конструкции из доказательства теоремы 3 очевидна — нужно увеличить параметры  $k$  и  $m$  до  $\ell/2$ , добавляя при необходимости пути к конечным вершинам деревьев и вспомогательных графов, построенных по лемме 4.

По каждой паре  $A_i, B_i$  построим автомат  $C_i$ , который проверяет либо неравенство  $s_{\ell n}(A) < s_{\ell n}(B)$ , либо равенство  $s_{\ell n}(A) = s_{\ell n}(B)$ .

Эти автоматы нужно объединить в один, который будет проверять одновременное выполнение всех условий для некоторой длины  $\ell n$ .

Комбинированный автомат  $C$  принимает слово  $\#w_1\#w_2\#\dots w_N\#$  из перестановочного фильтра, удовлетворяющее следующим условиям:

(i) слово  $w_i$  представляется в виде  $u_i v_i$ , где префикс  $u_i$  имеет длину  $p = \lceil \log_2 m \rceil$  ( $m$  — количество линейных условий, задающих камеру), а длина суффикса  $v_i$  кратна  $\ell$ ;

(ii) префиксы  $u_i$  образуют неубывающую последовательность в лексикографическом порядке;

(iii) слово  $\#v_j\#\dots\#v_{j+k}$ , составленное из суффиксов тех слов  $w_i$ , которые имеют общий префикс  $z$ , принимается автоматом  $C_r$ , где  $r$  получается из двоичной записи  $z$  прибавлением 1 (при  $r > m$  автомат  $C_r$  не меняет полученный от предыдущего автомата ответ — это добавление необходимо, так как  $m$  может не быть точной степенью 2).

Для реализации такого автомата нужно умножить множество состояний каждого автомата  $C_i$  на счётчик  $K_i$  и последовательно соединить полученные автоматы. Счётчик  $K_i$  проверяет, что первые  $p$  символов двоичного слова  $w_j$  в последовательности являются двоичной записью числа  $i - 1$  или  $i$ . В последнем случае он отдаёт управление следующему автомату, скомбинированному из  $C_{i+1}$  и счётчика  $K_{i+1}$ . При работе счётчика состояния  $C_i$  не меняются. Когда счётчик прочитал  $p$  символов, он останавливается (его состояние не изменяется), и начинает работать автомат  $C_i$ .

Число состояний в автомате  $C$  можно оценить как  $O(Mm \log m)$ , где  $M$  — максимальный размер автоматов  $C_i$ . Действительно, всего нужно последовательно соединить  $2^p = O(m)$  композиций  $C_i$  и счётчиков, причём каждый счётчик можно реализовать на  $O(p) = O(\log m)$  состояниях.

### 5. Сводимость задачи $P_{\mathbb{B}}$ -реализуемости к ЗПК

Пусть имеется регулярный язык  $R$  в алфавите  $\{0, 1, \#\}$ , принимаемый детерминированным автоматом с множеством состояний  $Q$ . Этот автомат задаётся отображениями переходов  $f_0, f_1, f_{\#}$  множества  $Q$  в себя, которые отвечают чтению соответствующего символа алфавита. Мы покажем, как свести проверку  $R \cap P_{\mathbb{B}} \neq \emptyset$  к решению нескольких ЗПК.

Начнём с того, что выразим условие  $R \cap P_{\mathbb{B}} \neq \emptyset$  в терминах отображений  $f_0, f_1, f_{\#}$ . Будем использовать при этом обозначение

$$f(w) = \prod_{i=1}^{\ell} f_{w_{\ell-i+1}}$$

для отображения на множестве состояний автомата, определяемого чтением слова  $w = w_1 w_2 \dots w_{\ell} \in \{0, 1\}^{\ell}$ .

Обозначим через  $q_s$  начальное состояние автомата, а через  $Q_a$  — множество принимающих состояний. Поскольку мы строим сводимость по Тьюрингу, достаточно рассмотреть условие попадания в одно из принимающих состояний  $q_f \in Q_a$ . Это условие означает, что для некоторого слова  $\#w_1\#w_2\#\dots w_N\# \in P_{\mathbb{B}}$  (напомним, что  $N = 2^n$ ) выполняется

$$q_f = \left( \prod_{i=0}^{N-1} f_{\#} f(w_{N-i}) \right) f_{\#} q_s. \quad (8)$$

Заметим, что для проверки этого условия не обязательно знать слова  $w_i$ . Достаточно для каждого отображения  $g \in Q^Q$  вычислить количество  $\#_n(g)$  его представлений в виде  $f(w)$ ,  $w \in \{0, 1\}^n$ . Тогда условие (8) можно будет записать в виде

$$q_f = \left( \prod_{i=0}^{N-1} f_{\#} g_i \right) f_{\#} q_s, \quad (9)$$

где каждое из отображений  $g \in Q^Q$  входит ровно  $\#_n g$  раз в последовательность  $g_i$  из произведения (9).

Теперь выразим числа  $\#_n g$  как компоненты векторов из орбиты некоторого линейного отображения.

Рассмотрим линейное пространство над  $\mathbb{Q}$  с базисом, индексированным отображениями из  $Q^Q$ . Базисные вектора обозначим через  $e(f)$ ,  $f \in Q^Q$ . Зададим линейное отображение  $\Phi$  действием на базисных векторах:

$$\Phi e(f) = e(f f_0) + e(f f_1). \quad (10)$$

Уточним, что композицию отображений мы вычисляем справа налево, как это обычно и делается для отображений.

**Утверждение 7.** Число  $\#_n g$  равно коэффициенту при  $e(g)$  в векторе  $\Phi^n e(\text{id})$ , где  $\text{id}$  — тождественное отображение.

ДОКАЗАТЕЛЬСТВО. Индукция по  $n$ . Случай  $n = 0$  очевиден. Если утверждение выполняется для  $n = k - 1 \geq 0$ , то оно выполняется и для  $n = k$ :

$$\begin{aligned} \Phi^k e(\text{id}) &= \Phi \sum_{g \in Q^Q} \#_{k-1} g e(g) = \sum_{w \in \{0,1\}^{k-1}} \Phi e(f(w)) \\ &= \sum_{w \in \{0,1\}^{k-1}} (e(f(w)f_0) + e(f(w)f_1)) = \sum_{w \in \{0,1\}^{k-1}} (e(f(w0)) + e(f(w1))) \\ &= \sum_{w \in \{0,1\}^k} e(f(w)) = \sum_{g \in Q^Q} \#_k g e(g). \end{aligned}$$

Утверждение 7 доказано.

**5.1. Задача о протыкании маршрутов.** Утверждение 7 позволяет свести проверку условия (9) к задаче о протыкании орбитой линейного отображения множества маршрутов в графе.

Задача состоит в следующем. Заданы ориентированный граф  $\Gamma(V, E)$ , рёбра которого раскрашены в  $s$  цветов, две вершины  $a, b$  этого графа, целочисленная матрица  $\Phi$  порядка  $s$  и целочисленный вектор  $x_0$  размерности  $s$ . Требуется узнать, существует ли такое  $n$ , что в графе  $\Gamma$  есть такой маршрут  $\tau$  длины  $n$  из вершины  $a$  в вершину  $b$ , что число рёбер цвета  $i$ , входящих в маршрут  $\tau$ , равно  $i$ -й компоненте вектора  $\Phi^n x_0$ . Заметим, что в графе  $\Gamma$  допускаются петли и параллельные рёбра.

Для маршрута  $\tau$  по графу  $\Gamma$ , рёбра которого раскрашены в цвета  $1, 2, \dots, s$ , определим его вес  $w(\tau) \in \mathbb{Z}^s$  как набор кратностей меток вдоль этого маршрута:

$$w(\tau) = \sum_i \nu_i(\tau) e_i,$$

где  $\nu_i(\tau)$  — число рёбер цвета  $i$  на маршруте  $\tau$ .

В этих обозначениях требование задачи о протыкании маршрутов записывается так:

$$w(\tau) = \Phi^n x_0 \text{ для некоторого } n \text{ и маршрута } \tau \text{ из } a \text{ в } b. \quad (11)$$

**Лемма 5.** *Задача  $P_{\mathbb{B}}$ -реализуемости сводится по Тьюрингу к задаче о протыкании маршрутов.*

Доказательство леммы основано на следующей конструкции. Зафиксируем некоторое подмножество  $E = \{g_1, \dots, g_m\} \subseteq Q^Q$  отображений конечного множества  $Q$  в себя. Композиции отображений из этого множества вместе с тождественным отображением образуют моноид  $G$  с системой образующих  $E$ , поэтому естественно возникает граф Кэли  $\Gamma$  этого моноида. Вершинами графа  $\Gamma$  являются элементы  $G$ , а (направленные) рёбра связывают  $h$  и  $g_i h$ . Заметим, что на рёбрах графа Кэли возникают естественным образом метки, указывающие на образующую  $g_i$  для этого ребра. Граф Кэли моноида может иметь параллельные рёбра, поскольку в данном случае возможны равенства  $g_i h = g_j h$  при  $i \neq j$ .

**ДОКАЗАТЕЛЬСТВО ЛЕММЫ 5.** Построим полугруппу  $M_{01}$ , порождённую заданными в задаче  $P_{\mathbb{B}}$ -реализуемости отображениями  $f_0, f_1$ . Эта полугруппа конечна и её можно охарактеризовать как наименьшее множество отображений из  $Q$  в  $Q$ , содержащее отображения  $f_0, f_1$  и замкнутое относительно умножения на  $f_0, f_1$ .

Решение задачи  $P_{\mathbb{B}}$ -реализуемости будем получать из решений нескольких задач о протыкании маршрутов.

Каждая такая задача задаётся принимающим состоянием  $q_f$  автомата, принимающего язык  $R$  из условия задачи  $P_{\mathbb{B}}$ -реализуемости, и таким отображением  $h \in Q^Q$ , что  $h(f_{\#}(q_s)) = q_f$ . При этом  $h$  должно принадлежать моноиду  $M$ , который порождён тождественным отображением и отображениями  $f_{\#}f, f \in M_{01}$ . (Моноид  $M$  строится аналогично полугруппе  $M_{01}$ .)

Данные задачи о протыкании маршрутов таковы: граф — это граф Кэли моноида  $M$ , цвета — множество  $E = \{g \mid g = f_{\#}f, f \in M_{01}\}$ , начальная вершина —  $\text{id}$ , конечная —  $h$ , матрица  $\Phi$  задаётся уравнением (10), вектор  $x_0$  равен  $e(\text{id})$ .

Если для одной из таких задач о протыкании маршрутов получен положительный ответ, то в силу утверждения 7 выполняется условие (9) и задача  $P_{\mathbb{B}}$ -реализуемости имеет положительное решение. Если же для всех таких задач ответ отрицательный, то и задача  $P_{\mathbb{B}}$ -реализуемости имеет отрицательное решение, что прямо вытекает из определения графа Кэли моноида  $M$  и утверждения 7. Лемма 5 доказана.

Связь задачи о протыкании маршрутов с ЗПК основана на следующей лемме, которая выражает веса маршрутов в виде конечного объединения сдвигов целочисленных конусов в  $\mathbb{Z}^s$ . Под *целочисленным кону-*

сом  $\mathbb{N}(v_1, \dots, v_r)$  мы понимаем множество векторов вида  $\sum_{i=1}^r a_i v_i$ ,  $a_i \geq 0$ ,  $a_i \in \mathbb{Z}$ . (Обозначаем множество неотрицательных целых чисел через  $\mathbb{N}$ .)

**Лемма 6.** Пусть  $a, b$  — вершины графа  $\Gamma$ . Тогда множество  $W(a, b)$  весов маршрутов, начинающихся в  $a$  и заканчивающихся в  $b$ , является конечным объединением сдвигов целочисленных конусов в  $\mathbb{Z}^s$ . Список векторов сдвига и образующих этих конусов находится конструктивно.

**Доказательство.** Обозначим через  $T(S, a, b)$ ,  $S \subseteq E$ , множество тех маршрутов в графе  $\Gamma$ , которые начинаются в вершине  $a$ , заканчиваются в вершине  $b$ , проходят по рёбрам, которые образуют множество  $S$ , причём длина маршрута не превосходит  $|S|^2$ . Через  $W(S)$ ,  $S \subseteq E$ , обозначим целочисленный конус в  $\mathbb{Z}^s$ , порождённый весами замкнутых простых по рёбрам маршрутов, проходящих только по рёбрам из множества  $S$ .

В этих обозначениях

$$W(a, b) = \bigcup_{S \subseteq E} \bigcup_{\tau_0 \in T(S, a, b)} (w(\tau_0) + W(S)). \quad (12)$$

Заметим, что разложение (12) даёт требуемое в условии леммы представление, причём множество векторов сдвигов  $T(S, a, b)$  и конус  $W(S)$  строятся алгоритмически.

Вес вида

$$w = w(\tau_0) + \sum_i \alpha_i w(\gamma_i), \quad \text{где } \alpha_i \in \mathbb{N},$$

а  $\gamma_i$  — замкнутые маршруты на множестве рёбер маршрута  $\tau_0$ , является весом маршрута, который получается из  $\tau_0$  вклейкой  $\alpha_i$  копий  $\gamma_i$ . Отсюда следует включение  $\supseteq$  в (12).

Для проверки обратного включения разложим произвольный маршрут  $\tau$  из  $a$  в  $b$  на маршруты указанного вида. Пусть рёбра маршрута  $\tau$  образуют множество  $S$ . Будем последовательно выделять из маршрута замкнутые подмаршруты и построим последовательность маршрутов  $\tau = \tau_1, \tau_2, \dots, \tau_N$ . Если маршрут  $\tau_n$  имеет вид

$$e_1, e_2, \dots, e_k, \gamma_n, e_{k+1}, \dots, e_t$$

для некоторого замкнутого простого по рёбрам маршрута  $\gamma_n$ , причём начальная  $e_1, \dots, e_k$  и конечная  $e_{k+1}, \dots, e_t$  части маршрута дают в объединении всё множество  $S$ , то полагаем

$$\tau_{n+1} = e_1, e_2, \dots, e_k, e_{k+1}, \dots, e_t.$$

Такие шаги повторяются до тех пор, пока это возможно.

Из построения ясно, что

$$w(\tau) = w(\tau_N) + \sum_{i=1}^{N-1} w(\gamma_i) \in w(\tau_N) + W(S).$$

Для завершения доказательства достаточно проверить, что длина маршрута  $\tau_N$  не превосходит  $|S|^2$ .

Действительно, отметим на маршруте  $\tau_N$  по одному ребру из множества  $S$ , начиная с первого ребра. Каждый из  $|S|$  промежутков между отмеченными рёбрами имеет длину не более  $|S| - 1$ , так как в противном случае из промежутка можно было бы выделить простой по рёбрам замкнутый подмаршрут. Лемма 6 доказана.

Из леммы 6 следует, что проверка условия (11) распадается на ряд проверок условий вида

$$\Phi^n x_0 \in v_0 + W, \quad (13)$$

где  $v_0$  — целочисленный  $s$ -мерный вектор, а  $W$  — целочисленный конус в  $\mathbb{Z}^s$ . Естественнее назвать такую задачу целочисленной задачей о протыкании конуса (ЦЗПК). В следующем подразделе мы покажем, что целочисленная задача о протыкании сводится к ЗПК.

**5.2. Целочисленная ЗПК.** Сформулируем ЦЗПК более точно.

Пусть матрица  $\Phi$  и векторы  $x_0, v_0$  имеют целочисленные компоненты. Целочисленный конус в  $\mathbb{Z}^s$  задан образующими  $v_1, \dots, v_r$ :

$$W = \left\{ x \in \mathbb{Z}^s \mid x = v_0 + \sum_{i=1}^r \lambda_i v_i, \text{ где } \lambda_i \in \mathbb{Z}_+, v_i \in \mathbb{Z}^s \right\}. \quad (14)$$

Требуется проверить выполнение условия (13) при некотором  $n$ .

Основным результатом данного пункта является следующая теорема, из которой непосредственно следует наш главный результат — теорема 2.

**Теорема 5.** ЦЗПК сводится к ЗПК по Тьюрингу.

Обозначим через  $W_{\mathbb{Q}}$  рациональный конус, порождённый в пространстве  $\mathbb{Q}^s$  векторами  $v_1, \dots, v_r$ . Этот конус может быть описан как полиэдр, и построение системы линейных неравенств, задающих  $W_{\mathbb{Q}}$ , конструктивно (см., например, [4, т. 1, §7.2]).

Однако попадание орбиты  $\Phi$  в  $W_{\mathbb{Q}}$  не равносильно условию целочисленного протыкания (13): в конусе  $W_{\mathbb{Q}}$  могут находиться целочисленные точки, которые не принадлежат  $W$ .

Начнём с анализа более лёгкого случая целочисленного симплицеального конуса, когда векторы  $v_i$  линейно независимы. В этом случае выполняется следующее простое

**Утверждение 8.** Если  $v_1, \dots, v_r$  линейно независимы, то условие  $x = \sum_i a_i v_i$ ,  $a_i \in \mathbb{N}$ , равносильно одновременному выполнению двух условий:

$$x = \sum_i b_i v_i, \quad b_i \in \mathbb{Q}_+, \quad x = \sum_i c_i v_i, \quad c_i \in \mathbb{Z}.$$

**ДОКАЗАТЕЛЬСТВО.** В одну сторону утверждение очевидно. В другую сторону нужно заметить, что из  $\sum_i b_i v_i = \sum_i c_i v_i$  в силу линейной независимости векторов  $v_i$  следуют равенства  $b_i = c_i$ . Утверждение 8 доказано.

Условие  $x = \sum_i c_i v_i$ ,  $c_i \in \mathbb{Z}$ , означает, что вектор  $x$  принадлежит подгруппе  $G$ , порождённой векторами  $v_i$  в группе  $\mathbb{Z}^s$ . Это условие также является конъюнкцией двух условий, одно из которых формулируется просто: вектор  $x$  принадлежит подпространству, порождённому векторами  $v_i$  в векторном пространстве  $\mathbb{Q}^s$ . Чтобы сформулировать второе условие, расширим группу  $G$  до группы  $\tilde{G}$ , добавив к образующим  $v_i$  такой набор единичных векторов из координатного базиса в  $\mathbb{Z}^s$ , что система векторов, состоящая из  $v_i$  и добавленных векторов  $e_j$ , линейно независима. Это возможно в силу линейной независимости векторов  $v_i$ .

**Утверждение 9.** Вектор  $x$  принадлежит подгруппе  $G$ , порождённой векторами  $v_i$  в группе  $\mathbb{Z}^s$  тогда и только тогда, когда  $x$  принадлежит подпространству, порождённому векторами  $v_i$  в векторном пространстве  $\mathbb{Q}^s$ , и  $x$  принадлежит группе  $\tilde{G}$ .

**ДОКАЗАТЕЛЬСТВО.** В одну сторону утверждение очевидно. Теперь предположим, что  $x \in \tilde{G}$ . По построению группы  $\tilde{G}$  это означает, что

$$x = g + \sum_j x_j e_j,$$

где  $g \in G$ , а  $e_j$  — те единичные векторы, которые были добавлены при построении группы  $\tilde{G}$ . Поскольку мы потребовали, чтобы  $v_i$  и  $e_j$  были линейно независимы, из принадлежности  $x$  подпространству, порождённому векторами  $v_i$  в векторном пространстве  $\mathbb{Q}^s$ , следует, что все  $x_j$  равны 0, а вектор  $x$  принадлежит группе  $G$ . Утверждение 9 доказано.



Утверждения 8 и 9 показывают, что условие принадлежности целочисленной конической оболочке векторов  $v_i$  равносильно одновременно выполнению трёх условий, два из которых являются  $\mathbb{Q}$ -линейными условиями и означают принадлежность вектора конусу  $W_{\mathbb{Q}}$ , а третье состоит в том, что вектор принадлежит некоторой подгруппе  $\mathbb{Z}^s$  полного ранга (фактор-группа конечна). Проверка первых двух условий для орбиты линейного отображения является ЗПК, а третье условие выполняется для хорошо описываемого множества показателей  $n$ .

**Утверждение 10.** Пусть  $G = \langle v_1, \dots, v_s \rangle \subseteq \mathbb{Z}^s$  — подгруппа  $\mathbb{Z}^s$  ранга  $s$ ,  $v_0$  — целочисленный вектор в  $\mathbb{Z}^s$ , а  $\Phi$  — целочисленная матрица порядка  $s$ .

Тогда множество

$$H = \{n \mid \Phi^n x_0 \in v_0 + G\}$$

является конечным объединением арифметических прогрессий и конечного множества, причём существует алгоритм, который строит эти прогрессии и множества по указанным выше данным.

**Доказательство.** Рассмотрим случай диагональной подгруппы, матрица образующих которой имеет вид

$$D = \begin{pmatrix} q_1 & 0 & \dots & 0 \\ 0 & q_2 & \dots & 0 \\ & & \dots & \\ 0 & 0 & \dots & q_s \end{pmatrix}$$

(столбцы матрицы являются образующими группы). Сдвиг такой подгруппы задаётся условиями

$$x_i \equiv \xi_i \pmod{q_i}, \quad 1 \leq i \leq s. \quad (15)$$

Обозначим через  $q$  наименьшее общее кратное  $q_i$ . Вычисляя  $\Phi^k x_0$  по модулю  $q$ , выберем конечное множество арифметических прогрессий, отвечающих тем  $k$ , для которых выполняются условия (15). Кроме этих арифметических прогрессий в множество  $H$  могут входить лишь те числа, которые меньше первых членов построенных арифметических прогрессий. Это даёт дополнительное конечное множество, которое может быть построено перебором всех указанных чисел.

Общий случай сводится к диагональному построением нормальной формы Смита (см. [4, т. 1, §4.4]) для матрицы  $M$  образующих группы  $G$ .

Нормальная форма Смита даёт для подгруппы полного ранга представление вида

$$M = UDV, \quad (16)$$

где  $U, V$  — унимодулярные матрицы, а  $D$  — диагональная невырожденная матрица. При этом матрица  $V$  отвечает элементарным преобразованиям столбцов и потому задаёт некоторую новую систему образующих  $\tilde{v}_1, \dots, \tilde{v}_s$  группы  $G$ . Матрица  $U$  отвечает элементарным преобразованиям строк и задаёт выражение базисных векторов  $e_i$  исходного базиса через новые базисные векторы  $\tilde{e}_i$ :

$$(e_1, \dots, e_s) = (\tilde{e}_1, \dots, \tilde{e}_s)U.$$

Уравнение (16) означает, что матрица образующих  $\tilde{v}_i$  группы  $G$  в базисе  $\tilde{e}_i$  диагональна.

Сводимость общего случая к диагональному завершается выражением матрицы  $\Phi$  и векторов  $x_0, v_0$  в базисе  $\tilde{e}_i$ . Утверждение 10 доказано.

**Лемма 7.** ЦЗПК в случае линейно независимых векторов  $v_1, \dots, v_r$  сводится к ЗПК.

**ДОКАЗАТЕЛЬСТВО.** Опишем алгоритм с ЗПК-оракулом, решающий ЦЗПК в предположении линейной независимости векторов  $v_1, \dots, v_r$ .

Прежде всего найдём множество  $H$  из утверждения 10. Оно состоит из конечного подмножества  $H_0$ , для которого условие (13) проверяется непосредственно, и конечного числа арифметических прогрессий.

Для каждой такой прогрессии  $n = n_0 + Nk$ ,  $k = 0, 1, \dots$ , построим вектор  $x_1 = \Phi^{n_0}$  и матрицу  $\Phi_1 = \Phi^N$ . Используя оракул ЗПК, проверим существование такого  $k$ , что  $\Phi_1^k x_1 - v_0$  принадлежит конусу  $W_{\mathbb{Q}}$ . Если хотя бы одна из таких проверок даёт положительный ответ, то выдаём положительный ответ для ЦЗПК. В противном случае выдаём отрицательный ответ.

Проверим корректность изложенного алгоритма. Из утверждений 9 и 10 следует, что если все проверки дали отрицательный ответ, то орбита  $\Phi^n x_0$  либо вообще не попадает в конус  $W_{\mathbb{Q}}$ , либо попадает в него при таких  $n$ , что  $\Phi^n x_0 - v_0$  не лежит в группе  $G$ . Поэтому ответ в исходной ЦЗПК отрицательный.

Если же одна из проверок дала положительный ответ, то фактически найдено такое  $n$ , что  $\Phi^n x_0 - v_0$  лежит в группе  $G$  и конусе  $W_{\mathbb{Q}}$ . Из утверждения 8 следует, что у исходной ЦЗПК ответ положительный. Лемма 7 доказана.

Теперь вернёмся к анализу общего случая. Пусть  $W_{\mathbb{N}} = \mathbb{N}(v_1, \dots, v_r)$  — множество целочисленных линейных комбинаций  $v_i$  с неотрицательными коэффициентами (целочисленный конус с образующими  $v_i$ ). Наша цель состоит в том, чтобы представить целочисленный конус  $W_{\mathbb{N}}$  как объединение конечного множества исключительных точек  $W_0$  и конечного набора сдвигов целочисленных симплицальных конусов  $u_i + \mathbb{N}(v_{i_1}, \dots, v_{i_t})$ . Для построения алгоритма решения ЦЗПК необходимо также, чтобы такое представление было конструктивно.

Напомним, что по теореме Каратеодори (см. [4, т. 1, §7.7]) любой вектор из  $\mathbb{Q}_+(v_1, \dots, v_r)$  является неотрицательной линейной комбинацией некоторых линейно независимых векторов из системы  $v_1, \dots, v_r$ .

Поскольку из  $r$  векторов в  $s$ -мерном пространстве можно составить не более чем  $\binom{r}{s}$  систем линейно независимых векторов, указанное выше представление достаточно найти для пересечений целочисленного конуса  $W_{\mathbb{N}}$  с рациональными симплицальными конусами, образующие которых выбираются из множества векторов  $v_1, \dots, v_r$ .

Рассмотрим один из таких конусов  $K$  и обозначим его образующие через  $\tilde{v}_1, \dots, \tilde{v}_t$ . Конус  $K$  содержит  $\mathbb{N}(\tilde{v}_1, \dots, \tilde{v}_t)$ , но помимо этого может содержать и другие целочисленные точки. Однако для конуса  $K$  существует *базис Гильберта* — такой набор целочисленных векторов  $u_1, \dots, u_m$ , что

$$K \cap \mathbb{Z}^s = \mathbb{N}(u_1, \dots, u_m). \quad (17)$$

В частности, уравнение (17) означает, что

$$K \cap \mathbb{Z}^s = \bigcup_{i=1}^m (u_i + \mathbb{N}(\tilde{v}_1, \dots, \tilde{v}_t)).$$

Важно отметить, что базис Гильберта находится по конусу  $K$  конструктивно, поскольку он совпадает с множеством целочисленных точек в политопе  $\{\lambda_1 \tilde{v}_1 + \lambda_2 \tilde{v}_2 + \dots + \lambda_t \tilde{v}_t \mid 0 \leq \lambda_i \leq 1\}$ . Некоторые из векторов базиса Гильберта принадлежат подгруппе  $\mathbb{Z}^s$ , порождённой векторами  $v_i$  (т. е. целочисленной оболочке  $v_i$ ). Проверка принадлежности такой подгруппе сводится к решению системы линейных диофантовых уравнений и потому конструктивна.

Рассмотрим один такой вектор  $u = \sum_i b_i v_i$ . Обозначим через  $B$  максимум модулей  $b_i$ . Тогда все точки из пересечения  $u + \mathbb{N}(\tilde{v}_1, \dots, \tilde{v}_t)$  и  $W_{\mathbb{N}}$  принадлежат объединению конечного множества

$$\left\{ x : x = u + \sum_{i=1}^t a_i \tilde{v}_i, \ 0 \leq a_i \leq B \right\}, \quad (18)$$

целочисленного конуса

$$u + (B + 1) \sum_i \tilde{v}_i + \mathbb{N}(\tilde{v}_1, \dots, \tilde{v}_t) \quad (19)$$

и  $(B + 1)t$  множеств вида

$$(u + a\tilde{v}_i + \mathbb{Q}_+(\tilde{v}_1, \tilde{v}_2, \dots, \tilde{v}_{i-1}, \tilde{v}_{i+1}, \dots, \tilde{v}_t)) \cap W_{\mathbb{N}}, \quad 0 \leq a \leq B, \quad 1 \leq i \leq t, \quad (20)$$

каждое из которых является пересечением исходного целочисленного конуса  $W_{\mathbb{N}}$  и сдвига рационального симплицеального конуса размерности  $t - 1$ .

Теперь можно описать алгоритм, который выражает пересечение целочисленного конуса  $W_{\mathbb{N}}$  и сдвига некоторого рационального симплицеального конуса с образующими, которые взяты из числа образующих  $W_{\mathbb{N}}$ , в виде объединения конечного множества  $W_0$  и конечного набора сдвигов симплицеальных целочисленных конусов.

Алгоритм рекурсивен. Применяя его к пересечению  $W_{\mathbb{N}}$  с  $t$ -мерным рациональным симплицеальным конусом  $K$ , находим базис Гильберта для  $K$ . Для каждого вектора из базиса Гильберта, который принадлежит целочисленной оболочке векторов  $v_1, \dots, v_r$ , строим разложение на множества (18)–(20).

Множество вида (18) добавляется к множеству исключительных точек  $W_0$ . Симплицеальный целочисленный конус (19) включается в искомый набор симплицеальных целочисленных конусов. После этого применяем алгоритм рекурсивно ко всем множествам (20).

Конечность рекурсии обеспечивается тем, что для конуса размерности 1 в указанном выше разложении нет множеств вида (20). Поэтому дерево рекурсии имеет конечную глубину и конечное ветвление.

Итак, доказана следующая

**Теорема 6.** *Целочисленный сдвиг целочисленного конуса*

$$v_0 + \mathbb{N}(v_1, \dots, v_r)$$

представляется как объединение конечного множества и конечного набора сдвигов симплицеальных целочисленных конусов. Существует алгоритм, который по векторам  $v_0, v_1, \dots, v_r$  строит указанное представление.

Из полученных результатов легко следует основной результат этого пункта.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 5. Используя алгоритм из теоремы 6, построим разложение камеры (14) на конечное множество исключительных точек и конечный набор сдвигов симплицальных целочисленных конусов.

Для каждого из построенных симплицальных целочисленных конусов проверим протыкание орбиты, применяя алгоритм с ЗПК-оракулом из леммы 7.

Проверка протыкания орбитой точки (а значит, и конечного множества точек) также сводится к решению ЗПК, поскольку точка является частным случаем камеры. Теорема 5 доказана.

### ЛИТЕРАТУРА

1. **Верецагин Н. К.** О проблеме появления нуля в линейной рекуррентной последовательности // Мат. заметки. — 1985. — Т. 38, №2. — С. 177–189.
2. **Верецагин Н. В., Шень А.** Лекции по математической логике и теории алгоритмов. Часть 3. Вычислимые функции. — М.: МЦНМО, 2008. — 192 с.
3. **Гэри М., Джонсон Д.** Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982. — 416 с.
4. **Схрейвер А.** Теория линейного и целочисленного программирования. Т. 1, 2. — М.: Мир, 1991. — 360 с., 342 с.
5. **Стенли Р.** Перечислительная комбинаторика. — М.: Мир, 1990. — 440 с.
6. **Хопкрофт Д., Мотвани Р., Ульман Д.** Введение в теорию автоматов, языков и вычислений. — М.: Вильямс, 2002. — 528 с.
7. **Berstel J., Reutenauer Ch.** Rational series and their languages. — New York, Heidelberg, Berlin: Springer-Verl., 1988. — 151 p.
8. **Blondel V. D., Portier N.** The presence of a zero in an integer linear recurrent sequence is NP-hard to decide // Linear Algebra Appl. — 2002. — Vol. 351–352. — P. 91–98.
9. **Cook W., Fonlupt J., Schrijver A.** An integer analogue of Carathéodory's theorem // J. Comb. Theory. Ser. B. — 1986. — Vol. 40, N 1. — P. 63–70.
10. **Eisenbrand F., Shmonin G.** Carathéodory bounds for integer cones // Oper. Res. Lett. — 2006. — Vol. 34. — P. 564–568.
11. **Halava V., Harju T., Hirvensalo M., Karhumäki J.** Skolem's problem — on the border between decidability and undecidability // TUCS Tech. Rep. — N 683. — 2005. — 42 p.
12. **Laohakosol V., Tangsupphathawat P.** Positivity of third order linear recurrence sequences // Discrete Appl. Math. — 2009. — Vol. 157, N 15. — P. 3239–3248.
13. **Salomaa A., Soittola M.** Automata-theoretic aspects of formal power series. — New York, Heidelberg, Berlin: Springer-Verl., 1978. — 176 p.

14. **Тao Т.** Open question: effective Skolem–Mahler–Lech theorem // <http://terrytao.wordpress.com/2007/05/25/open-question-effective-skolem-mahler-lech-theorem/>

*Вялый Михаил Николаевич,*  
e-mail: [vyalyi@gmail.com](mailto:vyalyi@gmail.com)  
*Тарасов Сергей Павлович,*  
e-mail: [serge99meister@gmail.com](mailto:serge99meister@gmail.com)

Статья поступила  
11 мая 2010 г.