

О проблеме вложения допустимых классов

П. С. Дергач

В статье рассматриваются две проблемы: проблема вложения допустимых классов алфавитного кодирования и проблема вложения допустимых классов регулярных языков. В первом случае для произвольной пары регулярных языков в общем алфавите необходимо понять, верно ли, что любое алфавитное кодирование, биективное на первом языке, будет биективно и на втором. Во втором случае для произвольной пары алфавитных кодирований в общих входном и выходном алфавитах необходимо понять, верно ли, что произвольный регулярный язык, на котором первое кодирование биективно, будет обладать тем же свойством и при втором кодировании. Показано, что первая проблема алгоритмически разрешима для случая, когда мощность входного алфавита равна двум. Во втором случае показано, что проблема всегда алгоритмически разрешима.

Ключевые слова: алфавитное кодирование, регулярные языки, проблема вложения, допустимые классы.

Введение

В данной работе изучаются две проблемы вложения: проблема вложения классов допустимых регулярных языков, заданных функциями алфавитного кодирования и проблема вложения классов допустимых функций алфавитного кодирования, заданных регулярными языками. Познакомиться с понятием регулярных языков можно в [1]. Понятие алфавитного кодирования, в свою очередь, есть в [2].

В статье в явном виде показывается, что первая проблема алгоритмически разрешима. При доказательстве этого факта автор ссылается на то, что отношение синонимии, возникающее на языке при алфавитном кодировании, регулярно в его обобщенном алфавите.

Этот результат принадлежит Александру Александровичу Маркову и о нем можно прочитать в [3]. Необходимо отметить, что в приводимом ниже доказательстве не используется тот факт, что допустимые языки регулярны. Рассуждение пройдет и в общем случае, когда это произвольные языки. Акцентирование внимания на регулярном случае обусловлено тем фактом, что именно такие языки встречаются в большинстве приложений, использующих алфавитное кодирование. Об этом можно прочитать, например, в [4].

Далее в статье приводится результат об алгоритмической разрешимости второй проблемы для случая, когда мощность входного алфавита равна двум. При этом используются три известных факта из общей теории контекстно-свободных языков. Первый факт состоит в том, что множество контекстно-свободных языков совпадает с множеством языков, представимых автоматами с магазинной памятью. Второй — в том, что пересечение контекстно-свободного и регулярного языков будет контекстно-свободным. Третий — в том, что проблема проверки пустоты контекстно-свободного языка, заданного автоматом с магазинной памятью, алгоритмически разрешима. Подробно об этих результатах можно прочитать, например, в [5]. Удастся описать классы допустимых функций кодирования в терминах подмножеств рациональных чисел. Таким образом, проверка вложения допустимых классов сводится к проверке вложения подмножеств рациональных чисел. При доказательстве этого факта автор ссылается на некоторые утверждения, полученные им ранее в [6]. Для доказательства правильности реализации этой проверки используется теорема Дирихле о простых числах в арифметической прогрессии. О ней можно прочитать, например, в [7].

В будущем автором и его учениками планируется написание программы, вычисляющей по регулярному языку подмножество рациональных чисел, задающее соответствующий класс допустимых функций алфавитного кодирования. И программ, доставляющих решение приведенных выше проблем проверки вложения. Автор благодарит своего научного руководителя Кудрявцева Валерия Борисовича и коллектив кафедры МаТИС при механико-математическом факультете МГУ за оказанное внимание к изложенным в статье результатам.

1. Основные понятия и результаты

Понятия регулярного языка, регулярного выражения, контекстно-свободного языка, автомата, автомата с магазинной памятью и обобщенного источника считаем общеизвестными и здесь не приводим. Их можно найти, например, в [1, 5].

Пусть A, B — конечные непустые множества. В дальнейшем будем называть A *входным алфавитом*, а B — *выходным алфавитом*. Множество слов (включая пустое) входного алфавита обозначаем через A^* , а множество слов (включая пустое) выходного алфавита — через B^* . Пустое слово обозначаем через λ . Пусть $\alpha = a(1) \dots a(k)$. Говорим, что k — *длина слова* α и обозначаем ее через $l(\alpha)$.

Через \mathbf{R} обозначаем множество всех не содержащих пустое слово регулярных языков в алфавите A :

$$\mathbf{R} := \{P \subseteq A^* \setminus \{\lambda\} \mid P \text{ — регулярно}\}.$$

Через \mathbf{F} обозначаем множество всех отображений из алфавита A в $B^* \setminus \{\lambda\}$:

$$\mathbf{F} := \{f \mid f : A \rightarrow B^* \setminus \{\lambda\}\}.$$

Элементы из \mathbf{F} называем *схемами кодирования*. Для произвольной схемы $f \in \mathbf{F}$ доопределяем ее до функции $\tilde{f} : A^* \setminus \{\lambda\} \rightarrow B^*$ следующим образом:

$$\forall \alpha = a(1) \dots a(k) \in A^* \setminus \{\lambda\} \quad \tilde{f}(\alpha) := f(a(1)) \dots f(a(k)).$$

Называем \tilde{f} *функцией алфавитного кодирования по схеме f* .

Для произвольного $P \in \mathbf{R}$ обозначаем через $(f)_P$ функцию $(\tilde{f})_P : P \rightarrow B^*$, полученную из \tilde{f} сужением на P . Пусть f — схема кодирования. Обозначаем через $\mathbb{R}(f)$ множество

$$\mathbb{R}(f) := \{P \in \mathbf{R} \mid (f)_P \text{ — инъекция}\},$$

называемое *классом допустимых регулярных языков для схемы f* .

Пусть $f_1, f_2 \in \mathbf{F}$. Говорим, что f_1 *вкладывается в f_2* и пишем $f_1 \leq f_2$, если

$$\mathbb{R}(f_1) \subseteq \mathbb{R}(f_2).$$

Пусть $P \in \mathbf{R}$. Обозначим через $\mathbb{F}(P)$ множество

$$\mathbb{F}(P) := \{f \in \mathbf{F} \mid (f)_P \text{ — инъекция}\},$$

называемое *классом допустимых схем кодирования для языка P* .

Пусть $P_1, P_2 \in \mathbf{R}$. Говорим, что P_1 *вкладывается* в P_2 и пишем $P_1 \leq P_2$, если

$$\mathbb{F}(P_1) \subseteq \mathbb{F}(P_2).$$

Для произвольного регулярного выражения \mathfrak{P} в алфавите A через $|\mathfrak{P}|$ обозначаем соответствующее ему регулярное множество в алфавите A .

Называем *обобщенным алфавитом* \tilde{A} множество $A \times \{\lambda\} \cup \{\lambda\} \times A$. Каждому слову в обобщенном алфавите можно естественным образом сопоставить упорядоченную пару слов в алфавите A в силу того факта, что $\tilde{A} \subset A^* \times A^*$.

Пусть f — схема кодирования. Называем *отношением синонимии* на f множество $S(f)$:

$$S(f) := \{(\alpha, \beta) \in A^* \times A^* \mid \tilde{f}(\alpha) = \tilde{f}(\beta)\}.$$

Пусть α, β — непустые слова в алфавите A . Говорим, что β является *измельчением* α , если существует $k \in \mathbb{N}$ такое, что $\alpha = \beta^k$. Если $k > 1$, то говорим, что измельчение *собственное*. Говорим, что измельчение β слова α *минимально*, если у α нет измельчения меньшей длины, чем длина измельчения β . Очевидно, что у любого непустого слова в алфавите A существует единственное минимальное измельчение.

Пусть α, β — непустые слова в алфавите A . Говорим, что α, β *соизмеримы*, если их минимальные измельчения совпадают.

Пусть $P \subseteq A^*$. Говорим, что P *измеримо*, если любые два непустых слова из этого множества соизмеримы.

Для случая, когда $A = \{a_1, a_2\}$, вводим особые обозначения:

$$\mathbf{F}_1 := \{f \in \mathbf{F} \mid f(a_1), f(a_2) \text{ соизмеримы}\},$$

$$\mathbf{F}_2 := \{f \in \mathbf{F} \mid f(a_1), f(a_2) \text{ не соизмеримы}\}.$$

Для $\alpha \in \{a_1, a_2\}^*$ обозначаем через $n_1(\alpha)$ количество букв a_1 в слове α и через $n_2(\alpha)$ — количество букв a_2 в слове α .

Называем множество $P \subseteq \{a_1, a_2\}^*$ *примитивным*, если для любых $\alpha, \beta \in P$ из одновременного выполнения равенств $n_1(\alpha) = n_1(\beta)$, $n_2(\alpha) = n_2(\beta)$ следует равенство $\alpha = \beta$. Через $T(P)$ обозначаем множество $\{(n_1(\alpha), n_2(\alpha)) \mid \alpha \in P\}$.

Называем подмножество натурального ряда $T \subseteq \mathbb{N}$ *периодическим*, если существуют $n_0, d \in \mathbb{N}$ такие, что для любого натурального

$t \geq n_0$ из $t \in T$ следует $t + d \in T$. Число d называется *длиной периода для T* . Множество $\{t \in T \mid t < n_0\}$ называется *предпериодом для T* . Множество $\{t \in T \mid n_0 \leq t < n_0 + d\}$ называется *периодом для T* .

Через \mathbf{K} обозначаем множество всех не содержащих пустое слово контекстно-свободных языков в алфавите $A \times A$:

$$\mathbf{K} := \{P \subseteq (A \times A)^* \setminus \{\lambda\} \mid P \text{ — контекстно-свободно}\}.$$

Через \mathbb{N}^+ обозначаем множество $\mathbb{N} \cup \{0\}$. Пусть $k \in \mathbb{N}$ и $\hat{v}, \hat{v}_1, \dots, \hat{v}_k \in \mathbb{N}^+ \times \mathbb{N}^+$ — двумерные вектора с неотрицательными целочисленными координатами. Положим $V = \{\hat{v}_1, \dots, \hat{v}_k\}$. Тогда множество

$$\left\{ \hat{v} + \sum_{i=1}^k c_i \hat{v}_i \mid c_i \in \mathbb{N}^+ \right\}$$

называем *пучком с началом в \hat{v} и базисом V* и обозначаем через $L(\hat{v}, V)$.

Пусть $C \subseteq \mathbb{N}^+ \times \mathbb{N}^+$. Через $\mathbb{H}(C)$ обозначаем множество

$$\mathbb{H}(C) := \{x \in \mathbb{Q} \mid x < 0\} \cap \left\{ \frac{u_1 - w_1}{u_2 - w_2} \mid (u_1, u_2), (w_1, w_2) \in C, u_2 \neq w_2 \right\}.$$

Называем два вектора $\hat{v}_1, \hat{v}_2 \in \mathbb{N}^+ \times \mathbb{N}^+$ *коллинеарными*, если существует $\alpha \in \mathbb{R}$, для которого $\hat{v}_1 = \alpha \cdot \hat{v}_2$. Если такого α не существует, то называем вектора *неколлинеарными*.

Для $x \in \mathbb{R}$ через $\lfloor x \rfloor$ обозначаем целую часть сверху от числа x .

Для $a, b \in \mathbb{Z}$ пишем $a|b$, если b делится нацело на a .

Теорема 1. *Проблема проверки вложения $\mathbb{R}(f_1) \subseteq \mathbb{R}(f_2)$ по произвольным $f_1, f_2 \in \mathbf{F}$ алгоритмически разрешима.*

Теорема 2. *Пусть $|A| = 2$. Тогда проблема проверки вложения $\mathbb{F}(P_1) \subseteq \mathbb{F}(P_2)$ по произвольным $P_1, P_2 \in \mathbf{R}$ алгоритмически разрешима.*

2. Доказательство вспомогательных утверждений

Лемма 1. *Пусть $\alpha, \beta \in A^* \setminus \{\lambda\}$ и $\alpha^k = \beta^m$ для некоторых $k, m \in \mathbb{N}$. Тогда существует $\nu \in A^* \setminus \{\lambda\}$ такое, что $l(\nu) = (l(\alpha), l(\beta))$, $\alpha = \nu^{\frac{l(\alpha)}{l(\nu)}}$, $\beta = \nu^{\frac{l(\beta)}{l(\nu)}}$.*

Доказательство леммы приведено в [6].

Лемма 2. Пусть

$$x_1, \dots, x_k \in \mathbb{N}, \quad r = \text{НОД}(x_1, \dots, x_k), \\ H = \{a_1 \cdot x_1 + \dots + a_k \cdot x_k \mid a_1, \dots, a_k \in \mathbb{N} \cup \{0\}\}.$$

Тогда существует $n_0 \in \mathbb{N}$ такое, что для любых $n \geq n_0$ из $r|n$ следует $n \in H$.

Доказательство леммы приведено в [6].

Лемма 3. Пусть $f \in \mathbf{F}$. Тогда существует обобщенный источник в обобщенном алфавите \tilde{A} , представляющий событие $S(f)$.

Доказательство леммы приведено в [3].

Лемма 4. Проблема проверки вложения двух регулярных множеств в общем алфавите алгоритмически разрешима.

Доказательство леммы приведено в [1].

Лемма 5. Пусть P — регулярное множество в алфавите A . Тогда оно представимо регулярным выражением вида

$$\bigvee_{i=1}^k \alpha_{i,1} \cdot (\mathfrak{P}_{i,1})^* \cdot \alpha_{i,2} \cdot \dots \cdot \alpha_{i,s(i)-1} \cdot (\mathfrak{P}_{i,s(i)-1})^* \cdot \alpha_{i,s(i)},$$

где $k, s(1), \dots, s(k)$ — произвольные натуральные числа,
 $\alpha_{1,1}, \dots, \alpha_{k,s(k)}$ — произвольные слова (возможно пустые) в алфавите A , $\mathfrak{P}_{1,1}, \dots, \mathfrak{P}_{k,s(k)-1}$ — произвольные регулярные выражения в алфавите A .

Доказательство леммы приведено в [6].

Лемма 6. Пусть $f_1, f_2 \in \mathbf{F}$. Тогда

$$f_1 \leq f_2 \Leftrightarrow S(f_2) \subseteq S(f_1).$$

Доказательство. Пусть $f_1 \leq f_2$. По определению получаем, что $\mathbb{R}(f_1) \subseteq \mathbb{R}(f_2)$. Возьмем произвольную пару слов $(\alpha, \beta) \in S(f_2)$. Допустим, что $(\alpha, \beta) \notin S(f_1)$. Отсюда получаем $f_1(\alpha) \neq f_1(\beta)$, $f_2(\alpha) = f_2(\beta)$. Обозначаем $P = \{\alpha, \beta\}$. Тогда $P \in \mathbb{R}(f_1)$ и $P \notin \mathbb{R}(f_2)$. Тогда неверно, что $\mathbb{R}(f_1) \subseteq \mathbb{R}(f_2)$. Полученное противоречие доказывает, что $S(f_2) \subseteq S(f_1)$.

Пусть теперь $S(f_2) \subseteq S(f_1)$ и при этом неверно, что $\mathbb{R}(f_1) \subseteq \mathbb{R}(f_2)$. Тогда существует $P \in \mathbb{R}(f_1)$, для которого $P \notin \mathbb{R}(f_2)$. Так как $P \in \mathbb{R}(f_1)$, то P регулярно. Но $P \notin \mathbb{R}(f_2)$, то есть $(\tilde{f}_2)_P$ — не инъекция. Поэтому существуют $\alpha, \beta \in P$, $\alpha \neq \beta$ такие, что $\tilde{f}_2(\alpha) = \tilde{f}_2(\beta)$. Значит $(\alpha, \beta) \in S(f_2)$. Так как $S(f_2) \subseteq S(f_1)$, то и $(\alpha, \beta) \in S(f_1)$. Поэтому $\tilde{f}_1(\alpha) = \tilde{f}_1(\beta)$. Значит $(\tilde{f}_1)_P$ — не инъекция, то есть $P \notin \mathbb{R}(f_1)$. Полученное противоречие завершает доказательство леммы.

Лемма 7. $P \subseteq A^*$ измеримо тогда только тогда, когда существует $\alpha \in A^*$, для которого $P \subseteq \{\alpha\}^*$.

Доказательство. Пусть $P \subseteq A^*$ измеримо. Если P пустое, то утверждение очевидно. Пусть P непустое. Возьмем произвольное $\alpha \in P$. Обозначим через ν его минимальное измельчение. Для любого другого слова $\beta \in P \setminus \{\alpha\}$ из измеримости P следует, что минимальное измельчение β совпадает с ν . Поэтому $P \subseteq \{\nu\}^*$.

Пусть теперь для некоторого $\alpha \in A^*$ верно $P \subseteq \{\alpha\}^*$. Обозначим через ν минимальное измельчение слова α . Тогда для некоторого $k \in \mathbb{N}$ имеем $\alpha = \nu^k$. Возьмем любое слово $\beta \in P \setminus \{\alpha\}$. Так как $P \subseteq \{\alpha\}^*$, то для некоторого $m \in \mathbb{N}$ имеем $\beta = \alpha^m$. Тогда $\beta = \nu^{km}$. Пусть ν' — минимальное измельчение слова β и $\beta = (\nu')^n$ для некоторого $n \in \mathbb{N}$. Тогда $(\nu')^n = \nu^{km}$. Из леммы 1 следует, что существует $\nu'' \in A^*$ такое, что $l(\nu'') = (l(\nu), l(\nu'))$ и $\nu = (\nu'')^{\frac{l(\nu)}{l(\nu'')}}$, $\nu' = (\nu'')^{\frac{l(\nu')}{l(\nu'')}}$. Поэтому $l(\nu'') \leq l(\nu)$ и $\alpha = (\nu'')^{\frac{l(\nu)}{l(\nu'')}} \cdot k$. Отсюда и из того, что ν — минимальное измельчение слова α получаем $\nu = \nu''$. Итак, $\beta = (\nu')^n = (\nu'')^{\frac{l(\nu')}{l(\nu'')}} \cdot n = \nu^{\frac{l(\nu')}{l(\nu'')}} \cdot n$. Но $l(\nu) = l(\nu'') \leq l(\nu')$. Отсюда и из того, что ν' — минимальное измельчение слова β получаем $\nu = \nu'$. Значит минимальное измельчение любого непустого слова из P совпадает с ν . Поэтому P измеримо. Утверждение леммы 7 доказано.

Лемма 8. *Проблема проверки на измеримость по произвольному $P \in \mathbf{R}$ алгоритмически разрешима.*

Доказательство. Если множество P пусто, то оно измеримо. Пусть теперь P непусто. Возьмем произвольное $\alpha \in P$. Обозначим через ν минимальное измельчение слова α . Очевидно, что его можно найти. Из доказательства предыдущей леммы следует, что множество P будет измеримо тогда только тогда, когда $P \subseteq \{\nu\}^*$. Но множество $\{\nu\}^*$ регулярно в алфавите A . Осталось заметить, что проверка на вложенность двух регулярных множеств в общем алфавите алгоритмически разрешима (см. [1]). Утверждение леммы 8 доказано.

Лемма 9. *Множество $P \subseteq A^* \setminus \{\lambda\}$ будет регулярным измеримым множеством в том и только в том случае, когда найдутся $\alpha \in A^*$ и периодическое $T \subseteq \mathbb{N}$, для которых выполнено $P = \{\alpha^t \mid t \in T\}$.*

Доказательство. Пусть $P = \{\alpha^t \mid t \in T\}$ для некоторых $\alpha \in A^*$ и периодического $T \subseteq \mathbb{N}$. Из леммы 7 следует, что P измеримо. Покажем, что P регулярно. Так как T периодическое, то существуют $n_0, d \in \mathbb{N}$ такие, что для любого $t \geq n_0$ из $t \in T$ следует $t + d \in T$. Пусть T' — предпериод множества T , равный $\{t \in T \mid t < n_0\}$. Пусть, кроме того, T'' — период множества T , равный $\{t \in T \mid n_0 \leq t < n_0 + d\}$. Обозначаем через M множество $\{\alpha^k \mid k \in T'\}$. Так как M конечно, то $M \in \mathbf{R}$. Для каждого $t \in T''$ обозначаем через M_t множество $\{\alpha^{t+id} \mid i \in \mathbb{N}^+\}$. Так как $\{\alpha^{t+id} \mid i \in \mathbb{N}^+\} = \{\alpha^t\} \cdot \{\alpha^d\}^*$, то для всех $t \in T''$ имеем $M_t \in \mathbf{R}$. Осталось заметить, что $P = M \cup (\bigcup_{t \in T''} M_t)$ и $|T''| < \infty$. Значит $P \in \mathbf{R}$.

Пусть теперь P — регулярное измеримое множество. Из леммы 7 следует существование $\alpha \in A^*$, для которого $P \subseteq \{\alpha\}^*$. Так как P регулярно, то по теореме Клини (см. [1]) существует абстрактный инициальный конечный автомат $V = (A, Q, \{0, 1\}, \varphi, \psi, q)$, представляющий по множеству $\{1\}$ множество P . Для всех $t \in \mathbb{N}$ обозначаем через $q(t)$ состояние $\varphi(q, \alpha^t)$. Так как $|Q| < \infty$, то существуют $m, n \in \mathbb{N}$ такие, что $q(m) = q(m+n)$. Тогда для любого натурального $m_0 \geq m$ верно

$$\begin{aligned} q(m_0 + n) &= \varphi(q, \alpha^{m_0+n}) = \varphi(q, \alpha^{(m+n)+(m_0-m)}) = \\ &= \varphi(\varphi(q, \alpha^{m+n}), \alpha^{m_0-m}) = \varphi(q(m+n), \alpha^{m_0-m}) = \end{aligned}$$

$$\begin{aligned} &= \varphi(q(m), \alpha^{m_0-m}) = \varphi(\varphi(q, \alpha^m), \alpha^{m_0-m}) = \\ &= \varphi(q, \alpha^{m+(m_0-m)}) = \varphi(q, \alpha^{m_0}) = q(m_0). \end{aligned}$$

Через T обозначаем множество $\{t \in \mathbb{N} \mid \alpha^t \in P\}$. Также через T' обозначаем множество $\{t \in \mathbb{N} \mid t \leq m, \alpha^t \in P\}$, через T'' — множество $\{t \in \mathbb{N} \mid m < t \leq m+n, \alpha^t \in P\}$. Докажем, что T — периодическое множество с предпериодом T' , периодом T'' и длиной периода n . В самом деле, пусть $k > m$, $k \in T$. Тогда $\alpha^k \in P$ и $\psi(q, \alpha^k) = 1$. Отсюда получаем:

$$\begin{aligned} \psi(q, \alpha^{k+n}) &= \psi(\varphi(q, \alpha^{k+n-1}), \alpha) = \psi(q(k+n-1), \alpha) = \\ &= \psi(q(k-1), \alpha) = \psi(\varphi(q, \alpha^{k-1}), \alpha) = \psi(q, \alpha^k) = 1. \end{aligned}$$

Здесь $q(k+n-1) = q(k-1)$, так как $k-1 \geq m$ и выше мы показали, что для любого натурального $m_0 \geq m$ верно $q(m_0+n) = q(m_0)$. Окончательно заключаем, что $\psi(q, \alpha^{k+n}) = 1$ и $\alpha^{k+n} \in P$. Значит $k+n \in T$. Поэтому T периодическое. Утверждение леммы 9 доказано.

Лемма 10. Пусть $|A| = 2$, $f \in \mathbf{F}$, $\gamma, \delta \in A^* \setminus \{\lambda\}$, $\gamma \neq \delta$ и $\tilde{f}(\gamma) = \tilde{f}(\delta)$. Тогда $f \in \mathbf{F}_1$.

Доказательство. Будем доказывать утверждение индукцией по длине $|\tilde{f}(\gamma)| = |\tilde{f}(\delta)|$. Обозначаем эту длину через n .

База индукции. $n = 1$:

Тогда $|\gamma| = |\delta| = 1$. Так как $\gamma \neq \delta$, то без ограничения общности считаем $\gamma = a_1$, $\delta = a_2$. Тогда $f(a_1) = \tilde{f}(\gamma) = \tilde{f}(\delta) = f(a_2)$. Поэтому $f(a_1)$, $f(a_2)$ соизмеримы и $f \in \mathbf{F}_1$.

Переход индукции. $n \rightarrow n+1$:

Пусть $|\tilde{f}(\gamma)| = |\tilde{f}(\delta)| = n+1$. Разбираем два случая.

Случай 1.

Первые буквы слов γ и δ совпадают и, без ограничения общности, равны a_1 . Обозначаем через γ' , δ' слова, получающиеся из γ , δ отбрасыванием первой буквы. Предположим, что слово γ' пустое. Тогда $\gamma = a_1$ и $f(a_1) = \tilde{f}(\gamma) = \tilde{f}(\delta)$. Значит $a_1 = \delta$. Это противоречит тому, что $\gamma \neq \delta$. Значит слово γ' не пустое. Аналогично, слово δ' не пустое. Так как $\gamma \neq \delta$, то и $\gamma' \neq \delta'$. Слова $\tilde{f}(\gamma')$, $\tilde{f}(\delta')$ равны, так как получаются из одинаковых слов $\tilde{f}(\gamma)$, $\tilde{f}(\delta)$ откидыванием общего префикса $\tilde{f}(a_1)$. Наконец, $|\tilde{f}(\gamma')| = |\tilde{f}(\delta')| < |\tilde{f}(\gamma)| = |\tilde{f}(\delta)| = n+1$. Значит к паре слов γ' , δ' можно применить предположение индукции и получить

$f \in \mathbf{F}_1$. В этом случае переход индукции доказан.

Случай 2.

Первые буквы слов γ и δ различны. Без ограничения общности считаем, что γ начинается с a_1 , а δ начинается с a_2 . Пусть $|\tilde{f}(a_1)| = |\tilde{f}(a_2)|$. Так как эти слова являются префиксами слова $\tilde{f}(\gamma) = \tilde{f}(\delta)$, то они равны. Значит $f \in \mathbf{F}_1$. Поэтому далее, без ограничения общности, считаем, что $|\tilde{f}(a_1)| > |\tilde{f}(a_2)|$. Тогда слово $\tilde{f}(a_2)$ будет собственным префиксом слова $\tilde{f}(a_1)$ и найдется $\rho \in B^* \setminus \{\lambda\}$, для которого $\tilde{f}(a_1) = \tilde{f}(a_2)\rho$. Определяем новую функцию $\tilde{f}' \in \mathbf{F} : \tilde{f}'(a_1) = \rho$, $\tilde{f}'(a_2) = \tilde{f}(a_2)$. Заменим в словах γ, δ каждую букву a_1 на слово a_2a_1 . Полученные в результате слова обозначаем как γ', δ' . Во-первых, эти слова различны, так как γ' начинается с a_2a_1 , а δ' начинается с a_2a_2 . Во-вторых, $\tilde{f}'(\gamma') = \tilde{f}(\gamma) = \tilde{f}(\delta) = \tilde{f}'(\delta')$, так как $\tilde{f}(a_1) = \tilde{f}(a_2)\rho = \tilde{f}'(a_2)\tilde{f}'(a_1) = \tilde{f}'(a_2a_1)$ и $\tilde{f}(a_2) = \tilde{f}'(a_2)$. Теперь убираем из слов γ', δ' общую первую букву a_2 . Новые слова обозначаем через γ'', δ'' . Они непусты и для них по-прежнему верно, что $\gamma'' \neq \delta''$ и $\tilde{f}'(\gamma'') = \tilde{f}'(\delta'')$. При этом, $|\tilde{f}'(\gamma'')| = |\tilde{f}'(\delta'')| < |\tilde{f}'(\delta')| = |\tilde{f}(\delta)| = n + 1$. Значит к паре слов γ'', δ'' можно применить предположение индукции и получить $\tilde{f}' \in \mathbf{F}_1$. То есть слова $\tilde{f}'(a_1) = \rho$ и $\tilde{f}'(a_2) = \tilde{f}(a_2)$ соизмеримы. Тогда и слова $\tilde{f}(a_2), \tilde{f}(a_2)\rho$ соизмеримы. Но $\tilde{f}(a_2)\rho = \tilde{f}(a_1)$ и значит $f \in \mathbf{F}_1$. Переход индукции доказан. Утверждение леммы 10 доказано.

Лемма 11. Пусть $f \in \mathbf{F}_1$ и множество $P \in \mathbf{R}$ представимо в виде

$$P = \bigcup_{i=1}^k C_{i,1} \cdot (P_{i,1})^* \cdot C_{i,2} \cdot \dots \cdot C_{i,s(i)-1} \cdot (P_{i,s(i)-1})^* \cdot C_{i,s(i)},$$

где $k, s(1), \dots, s(k)$ — натуральные числа, все $C_{i,j}, P_{i,j}$ — непустые множества слов в алфавите A и для некоторой пары (i_0, j_0) $1 \leq i_0 \leq k, 1 \leq j_0 < s(i_0)$ множество P_{i_0, j_0} не измеримо. Тогда $f \notin \mathbb{F}(P)$.

Доказательство. Так как $f \in \mathbf{F}_1$, то для некоторых $r, m \in \mathbb{N}$ и $\nu \in A^* \setminus \{\lambda\}$ имеем $f(a_1) = \nu^r$ и $f(a_2) = \nu^m$. Так как множество P_{i_0, j_0} не измеримо, то в нем найдутся два непустых различных не соизмеримых слова α, β . Заметим, что

$$\begin{aligned} \tilde{f}(\alpha\beta) &= \tilde{f}(\alpha)\tilde{f}(\beta) = (f(a_1))^{n_1(\alpha)}(f(a_2))^{n_2(\alpha)}(f(a_1))^{n_1(\beta)}(f(a_2))^{n_2(\beta)} = \\ &= (\nu^r)^{n_1(\alpha)}(\nu^m)^{n_2(\alpha)}(\nu^r)^{n_1(\beta)}(\nu^m)^{n_2(\beta)} = \nu^{r \cdot n_1(\alpha) + m \cdot n_2(\alpha)} \nu^{r \cdot n_1(\beta) + m \cdot n_2(\beta)} = \end{aligned}$$

$$\begin{aligned}
 &= \nu^{r \cdot (n_1(\alpha) + n_1(\beta)) + m \cdot (n_2(\alpha) + n_2(\beta))} = \nu^{r \cdot n_1(\beta) + m \cdot n_2(\beta)} \nu^{r \cdot n_1(\alpha) + m \cdot n_2(\alpha)} = \\
 &= (f(a_1))^{n_1(\beta)} (f(a_2))^{n_2(\beta)} (f(a_1))^{n_1(\alpha)} (f(a_2))^{n_2(\alpha)} = \tilde{f}(\beta) \tilde{f}(\alpha) = \tilde{f}(\beta\alpha).
 \end{aligned}$$

Докажем, что $\alpha\beta \neq \beta\alpha$. Если это не так, то в лемме 10 мы можем положить $\gamma = a_1a_2$, $\delta = a_2a_1$, $f(a_1) = \alpha$, $f(a_2) = \beta$ и получим $f \in \mathbf{F}_1$. Это вступает в противоречие с тем фактом, что слова α, β не соизмеримы. Итак, $\alpha\beta \neq \beta\alpha$. Теперь для каждого $1 \leq j \leq s(i_0)$ возьмем по одному произвольному элементу α_j из $C_{i_0, j}$. А для каждого $1 \leq j < s(i_0)$, $j \neq j_0$ — по одному произвольному элементу β_j из $P_{i_0, j}$. Обозначаем через α', β' слова

$$\begin{aligned}
 \alpha' &= \alpha_1\beta_1 \dots \alpha_{j_0-1}\beta_{j_0-1}\alpha_{j_0}\alpha\beta\alpha_{j_0+1}\beta_{j_0+1} \dots \alpha_{s(i_0)-1}\beta_{s(i_0)}\alpha_{s(i_0)}, \\
 \beta' &= \alpha_1\beta_1 \dots \alpha_{j_0-1}\beta_{j_0-1}\alpha_{j_0}\beta\alpha\alpha_{j_0+1}\beta_{j_0+1} \dots \alpha_{s(i_0)-1}\beta_{s(i_0)}\alpha_{s(i_0)}.
 \end{aligned}$$

Ясно, что $\alpha', \beta' \in P$. Замечаем, что $\alpha' \neq \beta'$, так как $\alpha\beta \neq \beta\alpha$. Кроме того, $\tilde{f}(\alpha') = \tilde{f}(\beta')$, ведь $\tilde{f}(\alpha\beta) = \tilde{f}(\beta\alpha)$. Поэтому $f \notin \mathbb{F}(P)$. Утверждение леммы 11 доказано.

Лемма 12. Пусть $A = \{a_1, a_2\}$, $P \in \mathbf{R}$ — не примитивный язык, $f \in \mathbb{F}(P)$. Тогда $f \in \mathbf{F}_2$.

Доказательство. Предположим, что $f \notin \mathbf{F}_2$, то есть $f \in \mathbf{F}_1$. Тогда для некоторых $\nu \in A^* \setminus \{\lambda\}$, $k, m \in \mathbb{N}$ верно $f(a_1) = \nu^k$, $f(a_2) = \nu^m$. Так как $P \in \mathbf{R}$ — не примитивный язык, то существуют $\alpha, \beta \in P$, для которых $n_1(\alpha) = n_1(\beta)$, $n_2(\alpha) = n_2(\beta)$ и $\alpha \neq \beta$. Тогда

$$\tilde{f}(\alpha) = (f(a_1))^{n_1(\alpha)} (f(a_2))^{n_2(\alpha)} = (f(a_1))^{n_1(\beta)} (f(a_2))^{n_2(\beta)} = \tilde{f}(\beta).$$

Значит $f \notin \mathbb{F}(P)$. Полученное противоречие завершает доказательство леммы.

Лемма 13. Пусть $A = \{a_1, a_2\}$. Тогда множество

$$\{(\alpha, \beta) \in A^* \times A^* \mid n_1(\alpha) = n_1(\beta), n_2(\alpha) = n_2(\beta)\}$$

будет контекстно-свободным в алфавите $A \times A$.

Доказательство. Для доказательства леммы достаточно построить автомат с магазинной памятью, представляющий множество $\{(\alpha, \beta) \in A^* \times A^* \mid n_1(\alpha) = n_1(\beta), n_2(\alpha) = n_2(\beta)\}$. Алфавитом обрабатываемой

на ленте записи будет $A \times A$, алфавитом стека будет $\{1\}$, у автомата будет три состояния q_1, q_2, q_3 и принимать запись на ленте автомат будет в том и только том случае, когда по окончании обработки записи стек будет пустым. Состояние q_1 соответствует тому, что в уже обработанном начале записи одинаковое количество букв a_1 и a_2 в первой и второй позициях. Состояние q_2 соответствует тому, что в уже обработанном начале записи в первой позиции больше букв a_1 , чем во второй позиции. Состояние q_3 соответствует тому, что в уже обработанном начале записи в первой позиции больше букв a_2 , чем во второй позиции. В начальный момент времени автомат находится в состоянии q_1 и стек пуст. Опишем функционирование автомата.

текущее состояние ленты	текущий символ ленты	последний символ в стеке	новое состояние	действие над стеком
q_1, q_2 или q_3	(a_1, a_1)	пусто	q_1	ничего
q_1, q_2 или q_3	(a_1, a_2)	пусто	q_2	пишем 1
q_1, q_2 или q_3	(a_2, a_1)	пусто	q_3	пишем 1
q_1, q_2 или q_3	(a_2, a_2)	пусто	q_1	ничего
q_2	(a_1, a_1)	1	q_2	ничего
q_2	(a_1, a_2)	1	q_2	пишем 1
q_2	(a_2, a_1)	1	q_2	стираем 1
q_2	(a_2, a_2)	1	q_2	ничего
q_3	(a_1, a_1)	1	q_3	ничего
q_3	(a_1, a_2)	1	q_3	стираем 1
q_3	(a_2, a_1)	1	q_3	пишем 1
q_3	(a_2, a_2)	1	q_3	ничего

Автомат следит за разницей для уже обработанной части ленты между количеством букв a_1 в первой и второй позициях и хранит эту разницу в стеке. Ясно, что стек автомата пуст тогда и только тогда, когда разница равна 0. Значит автомат функционирует правильно и распознает те и только те пары слов, в которых одинаковое количество букв a_1 и одинаковое количество букв a_2 . Утверждение леммы 13 доказано.

Лемма 14. Пусть $f \in \mathbf{F}_1$, $P \in \mathbf{R}$ — примитивный язык и для некоторых $\nu \in A^* \setminus \{\lambda\}$, $k, m \in \mathbb{N}$ верно $f(a_1) = \nu^k$, $f(a_2) = \nu^m$. Тогда

$f \notin \mathbb{F}(P)$ тогда и только тогда когда в P найдется пара слов α, β , для которой

$$\frac{n_1(\alpha) - n_1(\beta)}{n_2(\alpha) - n_2(\beta)} = -\frac{m}{k}.$$

Доказательство. Пусть для $\alpha, \beta \in P$ верно

$$\frac{n_1(\alpha) - n_1(\beta)}{n_2(\alpha) - n_2(\beta)} = -\frac{m}{k}.$$

Тогда

$$\begin{aligned} (n_1(\alpha) - n_1(\beta))k &= -(n_2(\alpha) - n_2(\beta))m, \\ n_1(\alpha)k + n_2(\alpha)m &= n_1(\beta)k + n_2(\beta)m. \end{aligned}$$

Значит

$$\begin{aligned} \tilde{f}(\alpha) &= (f(a_1))^{n_1(\alpha)}(f(a_2))^{n_2(\alpha)} = (\nu^k)^{n_1(\alpha)}(\nu^m)^{n_2(\alpha)} = \nu^{n_1(\alpha)k + n_2(\alpha)m} = \\ &= \nu^{n_1(\beta)k + n_2(\beta)m} = (\nu^k)^{n_1(\beta)}(\nu^m)^{n_2(\beta)} = (f(a_1))^{n_1(\beta)}(f(a_2))^{n_2(\beta)} = \tilde{f}(\beta). \end{aligned}$$

При этом $n_2(\alpha) - n_2(\beta) \neq 0$, то есть $\alpha \neq \beta$. Значит $f \notin \mathbb{F}(P)$.

Пусть теперь $f \notin \mathbb{F}(P)$. Тогда существуют $\alpha, \beta \in P$, $\alpha \neq \beta$, для которых $\tilde{f}(\alpha) = \tilde{f}(\beta)$. Значит

$$\begin{aligned} \nu^{n_1(\alpha)k + n_2(\alpha)m} &= (\nu^k)^{n_1(\alpha)}(\nu^m)^{n_2(\alpha)} = (f(a_1))^{n_1(\alpha)}(f(a_2))^{n_2(\alpha)} = \tilde{f}(\alpha) = \\ &= \tilde{f}(\beta) = (f(a_1))^{n_1(\beta)}(f(a_2))^{n_2(\beta)} = (\nu^k)^{n_1(\beta)}(\nu^m)^{n_2(\beta)} = \nu^{n_1(\beta)k + n_2(\beta)m}. \end{aligned}$$

Тогда

$$\begin{aligned} n_1(\alpha)k + n_2(\alpha)m &= n_1(\beta)k + n_2(\beta)m, \\ (n_1(\alpha) - n_1(\beta))k &= -(n_2(\alpha) - n_2(\beta))m. \end{aligned}$$

Если $n_2(\alpha) - n_2(\beta) = 0$, то и $n_1(\alpha) - n_1(\beta) = 0$. Это противоречит примитивности языка P . Значит $n_2(\alpha) - n_2(\beta) \neq 0$ и

$$\frac{n_1(\alpha) - n_1(\beta)}{n_2(\alpha) - n_2(\beta)} = -\frac{m}{k}.$$

Утверждение леммы 14 доказано.

Лемма 15. Пусть $f \in \mathbf{F}_2$ и $P \in \mathbf{R}$. Тогда $f \in \mathbb{F}(P)$.

Доказательство. Допустим, что $f \notin \mathbb{F}(P)$. Тогда $(\tilde{f})_P$ — не инъекция. Значит существуют $\alpha, \beta \in P$, $\alpha \neq \beta$, для которых $\tilde{f}(\alpha) = \tilde{f}(\beta)$. Так как $P \subseteq A^* \setminus \{\lambda\}$, то из леммы 10 следует, что $f \in \mathbf{F}_1$. Но это невозможно. Полученное противоречие завершает доказательство леммы.

Лемма 16. *Проблема проверки на примитивность по произвольному $P \in \mathbf{R}$ алгоритмически разрешима.*

Доказательство. Пусть $P \in \mathbf{R}$. Вводим обозначения:

$$\mathbf{C} = \{(\alpha, \beta) \in A^* \times A^* \mid n_1(\alpha) = n_1(\beta), n_2(\alpha) = n_2(\beta)\},$$

$$\mathbf{I} = \{(\alpha, \alpha) \mid \alpha \in A^*\}.$$

Так как $(P \times P) \cap \mathbf{C} = \{(\alpha, \beta) \in P \times P \mid n_1(\alpha) = n_1(\beta), n_2(\alpha) = n_2(\beta)\}$, то P примитивно тогда и только тогда, когда $(P \times P) \cap \mathbf{C} \subseteq \mathbf{I}$. Таким образом, исходная проблема свелась к проверке на пустоту множества $((P \times P) \cap \mathbf{C}) \setminus \mathbf{I}$. Из леммы 13 следует, что $\mathbf{C} \in \mathbf{K}$. Но множества $P \times P$ и \mathbf{I} регулярны в алфавите $A \times A$, а пересечение и разность контекстно-свободного и регулярного языков в свою очередь контекстно-свободны. Отсюда следует, что $((P \times P) \cap \mathbf{C}) \setminus \mathbf{I} \in \mathbf{K}$. Доказательство завершает тот факт, что проблема проверки на пустоту контекстно-свободного языка алгоритмически разрешима. Утверждение леммы 16 доказано.

Лемма 17. *Пусть L — пучок с началом \hat{v} и базисом V . Пусть $\hat{v}_1, \hat{v}_2 \in V$ — пара неколлинеарных векторов. Тогда*

$$\mathbb{H}(L) = \{x \in \mathbb{Q} \mid x < 0\}.$$

Доказательство. Очевидно, что $\mathbb{H}(L) \subseteq \{x \in \mathbb{Q} \mid x < 0\}$. Покажем, что для любых $k, l \in \mathbb{N}$ верно $-\frac{k}{l} \in \mathbb{H}(L)$. Пусть $\hat{v} = (x_0, y_0)$, $\hat{v}_1 = (x_1, y_1)$, $\hat{v}_2 = (x_2, y_2)$. Обозначим через n максимум из чисел ky_1, lx_1 . Вводим обозначения:

$$(u_1, u_2) = \hat{u} := \hat{v} + ky_2\hat{v}_1 + (n - ky_1)\hat{v}_2,$$

$$(w_1, w_2) = \hat{w} := \hat{v} + lx_2\hat{v}_1 + (n - lx_1)\hat{v}_2.$$

Очевидно, что $\hat{u}, \hat{w} \in L$. Покажем, что $u_2 \neq w_2$.

$$u_2 - w_2 = (y_0 + ky_2y_1 + (n - ky_1)y_2) - (y_0 + lx_2y_1 + (n - lx_1)y_2) =$$

$$= l(x_2y_1 - x_1y_2).$$

Рассмотрим семь случаев.

1. $x_1 = x_2 = 0$. Тогда вектора $\hat{v}_1, \hat{v}_2 \in V$ коллинеарны, что неверно.
 2. $x_1 = y_1 = 0$. Тогда вектора $\hat{v}_1, \hat{v}_2 \in V$ коллинеарны, что неверно.
 3. $x_1 = 0, y_1 \neq 0, x_2 \neq 0$. Тогда $l(x_2y_1 - x_1y_2) \neq 0$. 4. $x_1 \neq 0, y_1 = y_2 = 0$. Тогда вектора $\hat{v}_1, \hat{v}_2 \in V$ коллинеарны, что неверно.
 5. $x_1 \neq 0, y_1 = 0, y_2 \neq 0, x_2 = 0$. Тогда $l(x_2y_1 - x_1y_2) \neq 0$.
 6. $x_1 \neq 0, y_1 = 0, y_2 \neq 0, x_2 \neq 0$. Тогда $\frac{x_1}{x_2} \neq \frac{y_1}{y_2}$, так как иначе вектора $\hat{v}_1, \hat{v}_2 \in V$ коллинеарны, что неверно. Значит $l(x_2y_1 - x_1y_2) \neq 0$.
 7. $x_1 \neq 0, y_1 \neq 0$. Тогда $\frac{x_2}{x_1} \neq \frac{y_2}{y_1}$, так как иначе вектора $\hat{v}_1, \hat{v}_2 \in V$ коллинеарны, что неверно. Значит $l(x_2y_1 - x_1y_2) \neq 0$.
- Итак, $u_2 \neq w_2$. Далее

$$\begin{aligned} u_1 - w_1 &= (x_0 + ky_2x_1 + (n - ky_1)x_2) - (x_0 + lx_2x_1 + (n - lx_1)x_2) = \\ &= k(y_2x_1 - x_2y_1). \end{aligned}$$

Значит

$$\frac{u_1 - w_1}{u_2 - w_2} = \frac{k(y_2x_1 - x_2y_1)}{l(x_2y_1 - x_1y_2)} = -\frac{k}{l}.$$

То есть $-\frac{k}{l} \in \mathbb{H}(L)$. Утверждение леммы 17 доказано.

Лемма 18. Пусть $k \in \mathbb{N}$ и $\hat{v}_1, \dots, \hat{v}_k \in \mathbb{N}^+ \times \mathbb{N}^+$ — семейство попарно коллинеарных векторов. Тогда существуют $\hat{v} \in \mathbb{N}^+ \times \mathbb{N}^+$ и $n_1, \dots, n_k \in \mathbb{N}^+$ такие, что

$$\hat{v}_i = n_i \hat{v} \quad \text{при } 1 \leq i \leq k.$$

Доказательство. Если в семействе есть нулевые векторы $\hat{v} = (0, 0)$, то для них берем $n_i := 0$. Поэтому далее считаем, что все \hat{v}_i не равны $(0, 0)$. Здесь и далее везде, где это не обговорено отдельно, подразумеваем, что равенства выполнены при всех $1 \leq i \leq k$. Обозначаем через x_i, y_i координаты вектора v_i . Разберем три случая.

Случай 1. $x_1 = 0$. Тогда в силу попарной коллинеарности векторов v_i верно $x_i = 0$. Положим

$$\hat{v} := (0, 1),$$

$$n_i := y_i.$$

Очевидно, что

$$\hat{v}_i = (0, y_i) = (0, n_i) = n_i \hat{v}.$$

Случай 2. $y_1 = 0$. Этот случай сводится к случаю 1 перестановкой координат.

Случай 3. $x_1 \neq 0, y_1 \neq 0$. Из попарной коллинеарности векторов следует, что существуют $c_i \in \mathbb{R}$, для которых

$$(x_i, y_i) = (c_i x_1, c_i y_1).$$

Так как $\hat{v}_i \neq (0, 0)$, то $c_i \neq 0$. Тогда $c_i = \frac{x_i}{x_1} \in \mathbb{Q}$ и существуют $m_i, l_i \in \mathbb{N}$, для которых

$$c_i = \frac{m_i}{l_i}, \quad \text{НОД}(m_i, l_i) = 1.$$

Тогда $(x_i, y_i) = (\frac{m_i}{l_i} x_1, \frac{m_i}{l_i} y_1)$, откуда получаем, что l_i делит x_1 и l_i делит y_1 . Значит l_i делит $\text{НОД}(x_1, y_1)$. Положим

$$\hat{v} := \left(\frac{x_1}{\text{НОД}(x_1, y_1)}, \frac{y_1}{\text{НОД}(x_1, y_1)} \right)$$

и

$$n_i := \frac{m_i \cdot \text{НОД}(x_1, y_1)}{l_i}.$$

Выше мы показали, что $n_i \in \mathbb{N}$. Осталось заметить, что

$$\begin{aligned} \hat{v}_i = (x_i, y_i) &= \left(\frac{m_i}{l_i} x_1, \frac{m_i}{l_i} y_1 \right) = \\ &= \left(\frac{m_i \cdot \text{НОД}(x_1, y_1)}{l_i} \frac{x_1}{\text{НОД}(x_1, y_1)}, \frac{m_i \cdot \text{НОД}(x_1, y_1)}{l_i} \frac{y_1}{\text{НОД}(x_1, y_1)} \right) = \\ &= n_i \hat{v}. \end{aligned}$$

Разбор случаев завершен. Утверждение леммы 18 доказано.

Лемма 19. Пусть

$$L = \left\{ \sum_{i=1}^k c_i \hat{v}_i \mid c_i \in \mathbb{N}^+ \right\},$$

где $k \in \mathbb{N}$, $\hat{v}_1, \dots, \hat{v}_k \in \mathbb{N}^+ \times \mathbb{N}^+$ — семейство попарно коллинеарных векторов и для всех $1 \leq i \leq k$ верно $\hat{v}_i \neq (0, 0)$. Тогда существуют $c_0 \in \mathbb{R}$, $D \subseteq \{i \in \mathbb{N} \mid 1 \leq i < c_0\}$, $\hat{u} \in (\mathbb{N}^+ \times \mathbb{N}^+) \setminus (0, 0)$, для которых

$$L = \{n\hat{u} \mid n \in D\} \cup \{n\hat{u} \mid n \geq c_0\}.$$

Доказательство. Здесь и далее везде, где это не обговорено отдельно, подразумеваем, что равенства выполнены при всех $1 \leq i \leq k$. В силу леммы 18 существуют $\hat{v} \in \mathbb{N}^+ \times \mathbb{N}^+$ и $n_i \in \mathbb{N}^+$ такие, что $\hat{v}_i = n_i \hat{v}$. Так как $\hat{v}_i \neq (0, 0)$, то $n_i \neq 0$.

Пусть $H = \{c_1 \cdot n_1 + \dots + c_k \cdot n_k \mid c_1, \dots, c_k \in \mathbb{N}^+\}$. Имеем

$$L = \left\{ \sum_{i=1}^k c_i \hat{v}_i \mid c_i \in \mathbb{N}^+ \right\} = \left\{ \sum_{i=1}^k c_i n_i \hat{v} \mid c_i \in \mathbb{N}^+ \right\} = \{h\hat{v} \mid h \in H\}.$$

Обозначаем

$$r := \text{НОД}(n_1, \dots, n_k).$$

В силу леммы 2 существует $n_0 \in \mathbb{N}$ такое, что для любых $n \geq n_0$ из $r|n$ следует $n \in H$. С другой стороны, если $n \in H$, то $r|n$. Поэтому при $n \geq n_0$ получаем

$$r|n \Leftrightarrow n \in H.$$

Обозначаем

$$\hat{u} := r\hat{v}, \quad c_0 := \frac{n_0}{r}, \quad D := \left\{ \frac{h}{r} \mid h \in H, h < n_0 \right\}.$$

Очевидно, что

$$D \subseteq \{i \in \mathbb{N} \mid 1 \leq i < c_0\}.$$

Далее

$$\begin{aligned} L &= \{h\hat{v} \mid h \in H\} = \{h\hat{v} \mid h \in H, h < n_0\} \cup \{h\hat{v} \mid h \in H, h \geq n_0\} = \\ &= \left\{ r \frac{h}{r} \hat{v} \mid h \in H, h < n_0 \right\} \cup \{rn\hat{v} \mid rn \geq n_0\} = \\ &= \{rn\hat{v} \mid n \in D\} \cup \left\{ rn\hat{v} \mid n \geq \frac{n_0}{r} \right\} = \{n\hat{u} \mid n \in D\} \cup \{n\hat{u} \mid n \geq c_0\}. \end{aligned}$$

Утверждение леммы 19 доказано.

Лемма 20. Пусть L — пучок с началом \hat{v} и базисом V . Пусть любая пара \hat{v}_1, \hat{v}_2 векторов из V коллинеарна. Тогда L представимо в виде конечного объединения

$$L = \bigcup_{i=1}^k L_i,$$

где $k \in \mathbb{N}$ и все L_i — пучки с одноэлементными базисами.

Доказательство. Если базис V одноэлементен, то утверждение очевидно. Далее считаем, что $|V| \geq 2$. Если в базисе V есть нулевой вектор $(0, 0)$, то его можно отсюда выкинуть, получив при этом тот же самый пучок L . Поэтому далее считаем, что $(0, 0) \notin V$. В силу леммы 19 существуют $c_0 \in \mathbb{R}$, $D \subseteq \{i \in \mathbb{N} \mid 1 \leq i < c_0\}$, $\hat{u} \in \mathbb{N}^+ \times \mathbb{N}^+$ такие, что $\hat{u} \neq (0, 0)$ и

$$L = \{n\hat{u} \mid n \in D\} \cup \{n\hat{u} \mid n \geq c_0\}.$$

Заметим, что $\{n\hat{u} \mid n \geq c_0\}$ — пучок с началом $\hat{v} +]c_0[\hat{u}$ и одноэлементным базисом $\{\hat{u}\}$. Обозначаем его через L_0 . Пусть $|D| = m$. Если $m = 0$, то $L = L_0$, $k = 1$ и утверждение доказано. Пусть $m \in \mathbb{N}$. Упорядочим элементы множества D :

$$D = \{d_1, d_2, \dots, d_m\}.$$

Тогда для $1 \leq i \leq m$ через L_i обозначаем пучок с началом $\hat{v} + d_i\hat{u}$ и одноэлементным базисом $\{(0, 0)\}$. Тогда $L = \bigcup_{i=1}^m L_i \cup L_0$, $k = m + 1$.

Утверждение леммы 20 доказано.

Лемма 21. Пусть

L_1 — пучок с началом $\hat{v} = (a_1, b_1)$ и базисом $V = \{a_2, b_2\}$,

L_2 — пучок с началом $\hat{v} = (c_1, b_1)$ и базисом $V = \{c_2, d_2\}$

и $(a_2, b_2) \neq (0, 0)$, $(c_2, d_2) \neq (0, 0)$, $L_1 \cap L_2 = \emptyset$. Тогда при $a, b \in \mathbb{N}$ верно:

$$-\frac{a}{b} \in \mathbb{H}(L_1 \cup L_2) \Leftrightarrow \text{НОД}(ab_2 + ba_2, ad_2 + bc_2) \mid (bc_1 - ba_1 + ad_1 - ab_1).$$

Доказательство. Пусть при $a, b \in \mathbb{N}$ верно $-\frac{a}{b} \in \mathbb{H}(L_1 \cup L_2)$. Тогда существуют $(s_1, s_2), (s_3, s_4) \in L_1 \cup L_2$ такие, что $s_2 \neq s_4$ и $\frac{s_1 - s_3}{s_2 - s_4} = -\frac{a}{b}$. Разбираем три случая.

Случай 1. $(s_1, s_2), (s_3, s_4) \in L_1$. Тогда существуют $m, n \in \mathbb{N}^+$ такие, что

$$\begin{aligned} (s_1, s_2) &= (a_1 + ma_2, b_1 + mb_2), \\ (s_3, s_4) &= (a_1 + na_2, b_1 + nb_2). \end{aligned}$$

Имеем

$$-\frac{a}{b} = \frac{s_1 - s_3}{s_2 - s_4} = \frac{(a_1 + ma_2) - (a_1 + na_2)}{(b_1 + mb_2) - (b_1 + nb_2)} = \frac{(m - n)a_2}{(m - n)b_2} = \frac{a_2}{b_2} \geq 0,$$

что невозможно.

Случай 2. $(s_1, s_2), (s_3, s_4) \in L_2$. Этот случай разбирается точно так же как и предыдущий.

Случай 3. $(s_1, s_2) \in L_1, (s_3, s_4) \in L_2$. Тогда существуют $m, n \in \mathbb{N}^+$ такие, что

$$\begin{aligned}(s_1, s_2) &= (a_1 + ma_2, b_1 + mb_2), \\(s_3, s_4) &= (c_1 + nc_2, d_1 + nd_2).\end{aligned}$$

Имеем

$$-\frac{a}{b} = \frac{s_1 - s_3}{s_2 - s_4} = \frac{(a_1 + ma_2) - (c_1 + nc_2)}{(b_1 + mb_2) - (d_1 + nd_2)}.$$

Тогда

$$\begin{aligned}-a(b_1 - d_1 - nd_2 + mb_2) &= b(a_1 - c_1 - nc_2 + ma_2) \text{ и} \\m(ab_2 + ba_2) - n(ad_2 + bc_2) &= bc_1 - ba_1 + ad_1 - ab_1.\end{aligned}$$

Значит

$$\text{НОД}(ab_2 + ba_2, ad_2 + bc_2) \mid (bc_1 - ba_1 + ad_1 - ab_1).$$

Обратно, пусть при $a, b \in \mathbb{N}$ верно

$$\text{НОД}(ab_2 + ba_2, ad_2 + bc_2) \mid (bc_1 - ba_1 + ad_1 - ab_1).$$

Так как $(a_2, b_2) \neq (0, 0)$, $(c_2, d_2) \neq (0, 0)$, то $ab_2 + ba_2, ad_2 + bc_2 \in \mathbb{N}$. Поэтому из расширенного алгоритма Евклида следует, что существуют $m, n \in \mathbb{N}^+$ такие, что

$$m(ab_2 + ba_2) - n(ad_2 + bc_2) = bc_1 - ba_1 + ad_1 - ab_1.$$

Отсюда

$$-a(b_1 - d_1 - nd_2 + mb_2) = b(a_1 - c_1 - nc_2 + ma_2).$$

Если бы $b_1 - d_1 - nd_2 + mb_2$ было равно 0, то и $a_1 - c_1 - nc_2 + ma_2$ было бы равно 0. Значит $b_1 + mb_2 = d_1 + nd_2$ и $a_1 + ma_2 = a_1 + na_2$. Это противоречит тому, что $L_1 \cap L_2 = \emptyset$. Значит $b_1 - d_1 - nd_2 + mb_2 \neq 0$ и

$$-\frac{a}{b} = \frac{a_1 - c_1 - nc_2 + ma_2}{b_1 - d_1 - nd_2 + mb_2} = \frac{(a_1 + ma_2) - (c_1 + nc_2)}{(b_1 + mb_2) - (d_1 + nd_2)}.$$

Но $(a_1 + ma_2, b_1 + mb_2) \in L_1$, $(c_1 + nc_2, d_1 + nd_2) \in L_2$. Поэтому $-\frac{a}{b} \in \mathbb{H}(L_1 \cup L_2)$. Утверждение леммы 21 доказано.

Лемма 22. Пусть $a_1, b_1, a_2, b_2, c_1, b_1, c_2, d_2 \in \mathbb{N}^+$ и $(a_2, b_2) \neq (0, 0)$, $(c_2, d_2) \neq (0, 0)$. Тогда существуют $q_1, q_2 \in \{0, 1\}$, $k \in \mathbb{N}$, $s, e_1, f_1, \dots, e_k, f_k \in \mathbb{N}^+$ такие, что при $a, b \in \mathbb{N}$, $\text{НОД}(a, b) = 1$ верно

$$\begin{aligned} \text{НОД}(ab_2 + ba_2, ad_2 + bc_2) | (bc_1 - ba_1 + ad_1 - ab_1) &\Leftrightarrow \\ &\Leftrightarrow (a, b) \in \bigcup_{i=1}^k \left\{ (msq_1 + e_i, nsq_2 + f_i) \mid m, n \in \mathbb{N}^+ \right\}. \end{aligned}$$

Доказательство. Здесь и далее исходим из того, что во всех выкладках наложено дополнительное условие $a, b \in \mathbb{N}$, $\text{НОД}(a, b) = 1$. Возможны два случая.

Случай 1. $\text{НОД}(ab_2 + ba_2, ad_2 + bc_2) = ta + ub$ для некоторых $t, u \in \mathbb{N}^+$ как выражение относительно переменных a, b . Так как $(a_2, b_2) \neq (0, 0)$, $(c_2, d_2) \neq (0, 0)$, то $(t, u) \neq (0, 0)$. Тогда

$$\begin{aligned} \text{НОД}(ab_2 + ba_2, ad_2 + bc_2) | (bc_1 - ba_1 + ad_1 - ab_1) &\Leftrightarrow \\ &\Leftrightarrow (ta + ub) | (bc_1 - ba_1 + ad_1 - ab_1). \end{aligned}$$

Возникает два подслучая.

Случай 1.1. $b(c_1 - a_1) + a(d_1 - b_1)$ делится нацело на $ta + ub$ как выражение относительно переменных a, b . Тогда $\text{НОД}(ab_2 + ba_2, ad_2 + bc_2) | (bc_1 - ba_1 + ad_1 - ab_1)$ при любых натуральных a, b и в утверждении леммы можно положить $q_1 = q_2 = 1$, $s = k = 1$, $e_1 = f_1 = 0$.

Случай 1.2. $b(c_1 - a_1) + a(d_1 - b_1)$ не делится нацело на $ta + ub$ как выражение относительно переменных a, b . Тогда

$$\begin{aligned} (ta + ub) | (bc_1 - ba_1 + ad_1 - ab_1) &\Leftrightarrow \\ &\Leftrightarrow \exists s \in \mathbb{Z} \text{ такое, что } (d_1 - b_1 - ts)a + (c_1 - a_1 - us)b = 0 \Leftrightarrow \\ &\Leftrightarrow \frac{a}{b} = \frac{us - c_1 + a_1}{d_1 - b_1 - ts}. \end{aligned}$$

Потери корней от деления на ноль не происходит, так при $d_1 - b_1 - ts = 0$ также получаем и $c_1 - a_1 - us = 0$, а это противоречит исходному предположению о том, что $b(c_1 - a_1) + a(d_1 - b_1)$ не делится нацело на $ta + ub$. Если $t > 0, u > 0$, то $\frac{us - c_1 + a_1}{d_1 - b_1 - ts} > 0$ лишь при конечном множестве значений для s и в утверждении леммы нужно положить $q_1 = q_2 = 0$. Если $t = 0$, то $u > 0, \frac{a}{b} = \frac{us - c_1 + a_1}{d_1 - b_1}$ и в утверждении леммы нужно положить $q_1 = 1, q_2 = 0$. Остальные константы подбираются тривиально. Если $u = 0$, то тогда $t > 0, \frac{a}{b} = \frac{a_1 - c_1}{d_1 - b_1 - ts}$ и в утверждении леммы нужно положить $q_1 = 0, q_2 = 1$. Остальные константы подбираются тривиально.

Случай 2. $\text{НОД}(ab_2 + ba_2, ad_2 + bc_2) = \text{НОД}(rb, ma + nb)$ для некоторых $m, n, r \in \mathbb{Z} \setminus \{0\}$. Здесь мы воспользовались алгоритмом Евклида, примененным к паре чисел (b_2, d_2) . Случай с $m = 0$ уже был разобран выше. Получаем

$$\begin{aligned} \text{НОД}(ab_2 + ba_2, ad_2 + bc_2) | (bc_1 - ba_1 + ad_1 - ab_1) &\Leftrightarrow \\ &\Leftrightarrow \text{НОД}(rb, ma + nb) | (bc_1 - ba_1 + ad_1 - ab_1). \end{aligned}$$

Пусть (a, b) — какое-то конкретное решение. Через m'_1 обозначаем $\text{НОД}(b, m)$. Тогда для некоторых \hat{b}, \hat{m} выполнено $b = m'_1 \hat{b}, m = m'_1 \hat{m}, \text{НОД}(\hat{b}, \hat{m}) = 1$. Получаем:

$$m'_1 \text{НОД}(r\hat{b}, m'_1 a + \hat{b}n) | (bc_1 - ba_1 + ad_1 - ab_1).$$

Так как $\text{НОД}(\hat{b}, m'_1) = 1, \text{НОД}(\hat{b}, a) = \text{НОД}(b, a) = 1$, то $\text{НОД}(\hat{b}, m'_1 a + \hat{b}n) = 1$. Получаем:

$$m'_1 \text{НОД}(r, m'_1 a + \hat{b}n) | (m'_1 \hat{b}(c_1 - a_1) + a(d_1 - b_1)).$$

Если (a, b') удовлетворяет этому условию, то ему будут удовлетворять и $a, b' + r, a + r, b'$. Поэтому все подходящие (a, b') распадаются на серии

$$\begin{aligned} a &= ir + r_1, \\ b' &= jr + r_2 \end{aligned}$$

для некоторых $0 \leq r_1 < r, 0 \leq r_2 < r$. Количество этих серий конечно и они совпадают с множествами из формулировки леммы для $q_1 = q_2 = 1$. Значит при фиксированном m' общее решение $(a, b) = (a, b'm')$ распадается на конечное множество серий. Но и вариантов для $m'_1 \text{НОД}(b, m)$ конечно. Утверждение леммы 22 доказано.

Лемма 23. Пусть

$$\begin{aligned} L_1 & - \text{пучок с началом } \hat{v} = (a_1, b_1) \text{ и базисом } V = \{0, 0\}, \\ L_2 & - \text{пучок с началом } \hat{v} = (c_1, b_1) \text{ и базисом } V = \{c_2, d_2\}, \\ L_1 \cap L_2 & = \emptyset, \quad \mathbb{H}(L_1 \cup L_2) \neq \emptyset. \end{aligned}$$

Тогда существуют $q_1, q_2 \in \{0, 1\}$, $k, s_1, \dots, s_k \in \mathbb{N}$, $e_1, f_1 \dots e_k, f_k \in \mathbb{N}^+$ такие, что при $a, b \in \mathbb{N}$, $\text{НОД}(a, b) = 1$ верно

$$-\frac{a}{b} \in \mathbb{H}(L_1 \cup L_2) \Leftrightarrow (a, b) \in \bigcup_{i=1}^k \{(ms_i q_1 + e_i), (ns_i q_2 + f_i) \mid m, n \in \mathbb{N}^+\}.$$

Доказательство. Разбираем случаи.

Случай 1. $c_2 = d_2 = 0$. Тогда из непустоты множества $\mathbb{H}(L_1 \cup L_2)$ получаем, что $b_1 \neq d_1$ и

$$\mathbb{H}(L_1 \cup L_2) = \left\{ -\frac{a_1 - c_1}{b_1 - d_1} \right\},$$

причем $\frac{a_1 - c_1}{b_1 - d_1} < 0$. Осталось положить $q_1 = q_2 = 0$, $k = s_1 = 1$, $e_1 = \frac{|a_1 - c_1|}{c}$, $f_1 = \frac{|b_1 - d_1|}{c}$, где $c = \text{НОД}(|a_1 - c_1|, |b_1 - d_1|)$.

Случай 2. $c_2 = 0$, $d_2 \neq 0$, $a_1 < c_1$, $b_1 \leq d_1$. Тогда

$$\begin{aligned} \mathbb{H}(L_1 \cup L_2) & = \\ & = \{x \in \mathbb{Q} \mid x < 0\} \cap \left\{ \frac{u_1 - w_1}{u_2 - w_2} \mid (u_1, u_2), (w_1, w_2) \in L_1 \cup L_2, u_2 \neq w_2 \right\} = \\ & = \{x \in \mathbb{Q} \mid x < 0\} \cap \left\{ \frac{u_1 - w_1}{u_2 - w_2} \mid (u_1, u_2) \in L_1, (w_1, w_2) \in L_2, u_2 \neq w_2 \right\} = \\ & = \{x \in \mathbb{Q} \mid x < 0\} \cap \left\{ \frac{a_1 - c_1}{b_1 - d_1 - nd_2} \mid n \in \mathbb{N}^+, b_1 - d_1 - nd_2 \neq 0 \right\} = \emptyset, \end{aligned}$$

так как $a_1 - c_1 < 0$, $b_1 - d_1 - nd_2 < 0$ при любом $n \in \mathbb{N}^+$. Этот случай невозможен.

Случай 3. $c_2 = 0$, $d_2 \neq 0$, $a_1 < c_1$, $b_1 > d_1$. Тогда

$$\begin{aligned} \mathbb{H}(L_1 \cup L_2) & = \\ & = \{x \in \mathbb{Q} \mid x < 0\} \cap \left\{ \frac{a_1 - c_1}{b_1 - d_1 - nd_2} \mid n \in \mathbb{N}^+, b_1 - d_1 - nd_2 \neq 0 \right\} = \\ & = \left\{ \frac{a_1 - c_1}{b_1 - d_1 - nd_2} \mid n \in \mathbb{N}^+, n < \frac{b_1 - d_1}{d_2} \right\}. \end{aligned}$$

Поэтому $\mathbb{H}(L_1 \cup L_2)$ конечно и непусто. Пусть n_0 — максимальное целое неотрицательное число, для которого $n_0 < \frac{b_1 - d_1}{d_2}$. Осталось положить $k = n_0 + 1$, $s_1 = \dots = s_k = 1$, $q_1 = q_2 = 0$, $e_i = \frac{a_1 - c_1}{c_i}$, $f_i = \frac{b_1 - d_1 - (i-1)d_2}{c_i}$, где $c_i = \text{НОД}(a_1 - c_1, b_1 - d_1 - (i-1)d_2)$ при $1 \leq i \leq k$.
Случай 4. $c_2 = 0$, $d_2 \neq 0$, $a_1 = c_1$. Тогда

$$\begin{aligned} \mathbb{H}(L_1 \cup L_2) &= \\ &= \{x \in \mathbb{Q} \mid x < 0\} \cap \left\{ \frac{a_1 - c_1}{b_1 - d_1 - nd_2} \mid n \in \mathbb{N}^+, b_1 - d_1 - nd_2 \neq 0 \right\} = \emptyset. \end{aligned}$$

Этот случай невозможен.

Случай 5. $c_2 = 0$, $d_2 \neq 0$, $a_1 > c_1$, $b_1 < d_1$. Тогда

$$\begin{aligned} \mathbb{H}(L_1 \cup L_2) &= \\ &= \{x \in \mathbb{Q} \mid x < 0\} \cap \left\{ \frac{a_1 - c_1}{b_1 - d_1 - nd_2} \mid n \in \mathbb{N}^+, b_1 - d_1 - nd_2 \neq 0 \right\} = \\ &= \left\{ \frac{c_1 - a_1}{nd_2 + d_1 - b_1} \mid n \in \mathbb{N}^+ \right\} = \\ &= \bigcup_{i=0}^{c_1 - a_1 - 1} \left\{ \frac{c_1 - a_1}{n(c_1 - a_1)d_2 + id_2 + d_1 - b_1} \mid n \in \mathbb{N}^+ \right\}. \end{aligned}$$

При $0 \leq i < c_1 - a_1$ через c_i обозначаем $\text{НОД}(c_1 - a_1, id_2 + d_1 - b_1)$, через k_i обозначаем $\frac{c_1 - a_1}{c_i}$, через l_i обозначаем $\frac{id_2 + d_1 - b_1}{c_i}$. Имеем:

$$\begin{aligned} \bigcup_{i=0}^{c_1 - a_1 - 1} \left\{ \frac{c_1 - a_1}{n(c_1 - a_1)d_2 + id_2 + d_1 - b_1} \mid n \in \mathbb{N}^+ \right\} &= \\ &= \bigcup_{i=0}^{c_1 - a_1 - 1} \left\{ \frac{k_i}{nk_i d_2 + l_i} \mid n \in \mathbb{N}^+ \right\}. \end{aligned}$$

Так как при всех $0 \leq i < c_1 - a_1$ верно $\text{НОД}(k_i, nk_i d_2 + l_i) = \text{НОД}(k_i, l_i) = 1$, то это искомое представление. Осталось положить $q_1 = 0$, $q_2 = 1$, $k = c_1 - a_1$, $s_i = k_{i-1}d_2$, $e_i = k_{i-1}$, $f_i = l_{i-1}$ при $1 \leq i \leq k$.

Случай 6. $c_2 = 0, d_2 \neq 0, a_1 > c_1, b_1 \geq d_1$. Тогда

$$\begin{aligned} \mathbb{H}(L_1 \cup L_2) &= \\ &= \{x \in \mathbb{Q} \mid x < 0\} \cap \left\{ \frac{a_1 - c_1}{b_1 - d_1 - nd_2} \mid n \in \mathbb{N}^+, b_1 - d_1 - nd_2 \neq 0 \right\} = \\ &= \left\{ \frac{c_1 - a_1}{nd_2 + n_0d_2 + d_1 - b_1} \mid n \in \mathbb{N}^+ \right\}, \end{aligned}$$

где n_0 — минимальное целое неотрицательное число, для которого $n_0 > \frac{b_1 - d_1}{d_2}$. Для всех $0 \leq i < c_1 - a_1$ через c_i обозначаем $\text{НОД}(c_1 - a_1, id_2 + n_0d_2 + d_1 - b_1)$, через k_i обозначаем $\frac{c_1 - a_1}{c_i}$, через l_i обозначаем $\frac{id_2 + n_0d_2 + d_1 - b_1}{c_i}$. Имеем:

$$\begin{aligned} \bigcup_{i=0}^{c_1 - a_1 - 1} \left\{ \frac{c_1 - a_1}{n(c_1 - a_1)d_2 + n_0d_2 + id_2 + d_1 - b_1} \mid n \in \mathbb{N}^+ \right\} &= \\ &= \bigcup_{i=0}^{c_1 - a_1 - 1} \left\{ \frac{k_i}{nk_id_2 + l_i} \mid n \in \mathbb{N}^+ \right\}. \end{aligned}$$

Так как при всех $0 \leq i < c_1 - a_1$ верно $\text{НОД}(k_i, nk_id_2 + l_i) = \text{НОД}(k_i, l_i) = 1$, то это искомое представление. Осталось положить $q_1 = 0, q_2 = 1, k = c_1 - a_1, s_i = k_{i-1}d_2, e_i = k_{i-1}, f_i = l_{i-1}$ при $1 \leq i \leq k$.

Случай 7. $c_2 \neq 0, d_2 = 0$. Заменой координат и изменением порядка переменных в (a, b) этот случай сводится к предыдущим.

Случай 8. $c_2 \neq 0, d_2 \neq 0$. Тогда

$$\begin{aligned} \mathbb{H}(L_1 \cup L_2) &= \\ &= \{x \in \mathbb{Q} \mid x < 0\} \cap \left\{ \frac{a_1 - c_1 - mc_2}{b_1 - d_1 - nd_2} \mid n \in \mathbb{N}^+, b_1 - d_1 - nd_2 \neq 0 \right\}. \end{aligned}$$

Так как $c_2 \neq 0, d_2 \neq 0$, то существует $n_0 \in \mathbb{N}^+$ такое, что для всех $n \geq n_0$ верно $a_1 - c_1 - mc_2 < 0$ и $b_1 - d_1 - nd_2 < 0$. Значит $|\mathbb{H}(L_1 \cup L_2)| < \infty$. Далее случай разбирается так же, как и случаи 2, 3.

Разбор случаев закончен. Утверждение леммы 23 доказано.

Лемма 24. Пусть $w_1, w_2 \in \{0, 1\}$, $u \in \mathbb{N}$, $a, b \in \mathbb{N}^+$. Тогда существует алгоритм, который определяет, существуют ли $m, n \in \mathbb{N}^+$ такие, что

$$\begin{aligned}uw_1n + a &> 0, \\uw_2m + b &> 0, \\НОД(uw_1n + a, uw_2m + b) &= 1.\end{aligned}$$

Доказательство. Разбираем случаи.

Случай 1. $w_1 = w_2 = 0$. Тогда при всех $m, n \in \mathbb{N}^+$ верно

$$\text{НОД}(uw_1n + a, uw_2m + b) = \text{НОД}(a, b).$$

В этом случае утверждение очевидно.

Случай 2. $w_1 = 0, w_2 \neq 0, a = 0$. В этом случае искомым $m, n \in \mathbb{N}^+$, очевидно, не существует.

Случай 3. $w_1 = 0, w_2 \neq 0, a > 0, b > 0$. Проверяем, верно ли, что существует $k \in \mathbb{N}^+, 0 \leq k < a$ такое, что $(a, b + ku) = 1$. Если да, то искомые $m, n \in \mathbb{N}^+$ найдены. Если нет, то таких $m, n \in \mathbb{N}^+$ не существует, так как при $k \in \mathbb{N}, k \geq a$ верно

$$\text{НОД}(a, b + ku) = \text{НОД}(a, b + (k - a)u).$$

Случай 4. $w_1 = 0, w_2 \neq 0, a > 0, b = 0$. Случай сводится к предыдущему заменой b на $b + u$.

Случай 5. $w_1 = 1, w_2 = 0$. Случай сводится к предыдущим перестановкой w_1 и w_2 .

Случай 6. $w_1 = 1, w_2 = 1, a = b = 0$. Если $u = 1$, то в качестве искомым $m, n \in \mathbb{N}^+$ можно взять, например, 1. Если $u > 1$, то таких $m, n \in \mathbb{N}^+$, очевидно, не существует.

Случай 7. $w_1 = 1, w_2 = 1, a = 0, b > 0$. Проверяем, верно ли, что $\text{НОД}(u, b) > 1$. Если нет, то в качестве искомым $m, n \in \mathbb{N}^+$ можно взять $n = 1$ и $m = 0$. Если да, то тогда при всех $k \in \mathbb{N}^+$ верно $\text{НОД}(u, b + uk) = \text{НОД}(u, b) > 1$ и искомым $m, n \in \mathbb{N}^+$ не существует.

Случай 8. $w_1 = 1, w_2 = 1, a > 0, b = 0$. Случай сводится к предыдущему перестановкой w_1 и w_2 .

Случай 9. $w_1 = 1, w_2 = 1, a = 1, b > 0$. Тогда в качестве искомым $m, n \in \mathbb{N}^+$ можно взять, например, 0.

Случай 10. $w_1 = 1, w_2 = 1, a > 0, b = 1$. Случай сводится к предыдущему перестановкой w_1 и w_2 .

Случай 11. $w_1 = 1, w_2 = 1, a = b > 1$. Проверяем, верно ли, что

$\text{НОД}(a, a + u) > 1$. Если нет, то в качестве искомым $m, n \in \mathbb{N}^+$ можно взять $n = 0$ и $m = 1$. Если да, то тогда при всех $k \in \mathbb{N}^+$ верно $\text{НОД}(a, a + uk) > 1$ и искомым $m, n \in \mathbb{N}^+$ не существует.

Случай 12. $w_1 = 1, w_2 = 1, a > b > 1$. Обозначим $\text{НОД}(a, u)$ через c_1 и $\text{НОД}(b, u)$ через c_2 . Если $\text{НОД}(c_1, c_2) > 1$, то тогда при всех $k, l \in \mathbb{N}^+$ верно $\text{НОД}(a + ul, b + uk) \geq \text{НОД}(b, u) > 1$ и искомым $m, n \in \mathbb{N}^+$ не существует. Пусть теперь $\text{НОД}(c_1, c_2) = 1$. По теореме Дирихле о простых числах в арифметических прогрессиях существует $n_0 \in \mathbb{N}^+$ такое, что $a + un_0 = c_1 p_1$, где p_1 — простое число, большее c_2 . По этой же теореме существует $m_0 \in \mathbb{N}^+$ такое, что $b + um_0 = c_2 p_2$, где p_2 — простое число, большее p_1 и c_1 . Тогда $\text{НОД}(a + un_0, b + um_0) = \text{НОД}(c_1 p_1, c_2 p_2) = 1$ и в качестве искомым $m, n \in \mathbb{N}^+$ можно взять $n = n_0$ и $m = m_0$.

Разбор случаев закончен. Утверждение леммы 24 доказано.

3. Доказательство основных утверждений

Теорема 2. *Проблема проверки вложения $\mathbb{R}(f_1) \subseteq \mathbb{R}(f_2)$ по произвольным $f_1, f_2 \in \mathbf{F}$ алгоритмически разрешима.*

Доказательство. В силу леммы 6 достаточно проверить верно ли, что $S(f_2) \subseteq S(f_1)$. Из леммы 3 следует, что множества $S(f_1), S(f_2)$ регулярны в обобщенном алфавите \bar{A} . Доказательство теоремы завершает применение леммы 4.

Теорема 3. *Пусть $|A| = 2$. Тогда проблема проверки вложения $\mathbb{F}(P_1) \subseteq \mathbb{F}(P_2)$ по произвольным $P_1, P_2 \in \mathbf{R}$ алгоритмически разрешима.*

Доказательство. Прежде всего заметим, что приводимый ниже алгоритм не претендует на оптимальность и в дальнейшем будет оптимизироваться. Также планируется написание реализующей его программы. Здесь же мы приводим лишь общее рассуждение, доставляющее решение проблемы проверки вложения.

Пусть $P_1, P_2 \in \mathbf{R}$ — произвольные регулярные языки в алфавите A , не содержащие пустое слово. Из леммы 16 следует, что мы можем проверить P_1 на примитивность. Пусть множество P_1 не примитивно. Тогда возьмем произвольную схему $f \in \mathbb{F}(P_1)$. В силу леммы 12

$f \in \mathbf{F}_2$. Из леммы 15 следует, что $f \in \mathbb{F}(P_2)$. Значит $\mathbb{F}(P_1) \subseteq \mathbb{F}(P_2)$ и алгоритм завершен. Пусть теперь множество P_1 примитивно. Используем лемму 5. Из нее следует, что P_1 представимо регулярным выражением вида

$$\bigvee_{i=1}^k \alpha_{i,1} \cdot (\mathfrak{P}_{i,1})^* \cdot \alpha_{i,2} \cdot \dots \cdot \alpha_{i,s(i)-1} \cdot (\mathfrak{P}_{i,s(i)-1})^* \cdot \alpha_{i,s(i)},$$

где $k, s(1), \dots, s(k)$ — натуральные числа, $\alpha_{1,1}, \dots, \alpha_{k,s(k)}$ — некоторые слова (возможно пустые) в алфавите A , $\mathfrak{P}_{1,1}, \dots, \mathfrak{P}_{k,s(k)-1}$ — некоторые регулярные выражения в алфавите A . Поэтому

$$P_1 = \bigcup_{i=1}^k \{\alpha_{i,1}\} \cdot |\mathfrak{P}_{i,1}|^* \cdot \{\alpha_{i,2}\} \cdot \dots \cdot \{\alpha_{i,s(i)-1}\} \cdot |\mathfrak{P}_{i,s(i)-1}|^* \cdot \{\alpha_{i,s(i)}\}.$$

Если для некоторой пары (i_0, j_0) $1 \leq i_0 \leq k$, $1 \leq j_0 < s(i_0)$ множество $|\mathfrak{P}_{i_0, j_0}|$ не измеримо, то по лемме 11 для произвольного $f \in \mathbb{F}(P_1)$ верно $f \notin \mathbf{F}_1$, то есть $f \in \mathbf{F}_2$. Тогда в силу леммы 15 $f \in \mathbb{F}(P_2)$, а значит $\mathbb{F}(P_1) \subseteq \mathbb{F}(P_2)$ и алгоритм завершен. Поэтому считаем теперь, что множества $|\mathfrak{P}_{i_0, j_0}|$ измеримы. Здесь и далее это выполнено при всех $1 \leq i_0 \leq k$, $1 \leq j_0 < s(i_0)$. Значит и множества $|\mathfrak{P}_{i_0, j_0}|^*$ измеримы. Из леммы 9 получаем, что найдутся $\alpha_{i_0, j_0} \in A^*$ и периодические $T_{i_0, j_0} \subseteq \mathbb{N}$, для которых выполнено

$$|\mathfrak{P}_{i_0, j_0}|^* = \{\alpha_{i_0, j_0}^t \mid t \in T_{i_0, j_0}\}.$$

Из доказательства этой леммы также следует, что

$$|\mathfrak{P}_{i_0, j_0}|^* = \left\{ \alpha_{i_0, j_0}^k \mid k \in T'_{i_0, j_0} \right\} \cup \left(\bigcup_{t \in T''_{i_0, j_0}} \left\{ \alpha^{t+id_{i_0, j_0}} \mid i \in \mathbb{N}^+ \right\} \right),$$

где $T'_{i_0, j_0}, T''_{i_0, j_0}, d_{i_0, j_0}$ — предпериод, период и длина периода множества $|\mathfrak{P}_{i_0, j_0}|^*$ соответственно. Так как период и предпериод — конечные множества, то, подставляя эти выражения в формулу для P_1 и используя дистрибутивность, получаем

$$P_1 = \bigcup_{i=1}^n \{\beta_{i,1}\} \cdot \{\gamma_{i,1}\}^* \cdot \{\beta_{i,2}\} \cdot \dots \cdot \{\beta_{i,r(i)-1}\} \cdot \{\gamma_{i,r(i)-1}\}^* \cdot \{\beta_{i,r(i)}\},$$

где $n, r(1), \dots, r(n)$ — натуральные числа, $\beta_{1,1}, \dots, \beta_{n,r(n)}$ — некоторые слова (возможно пустые) в алфавите A , $\gamma_{1,1}, \dots, \gamma_{n,r(n)-1}$ — некоторые непустые слова в алфавите A .

Если $f \in \mathbb{F}(P_1) \cap \mathbf{F}_2$, то из леммы 15 следует, что $f \in \mathbb{F}(P_2)$. Поэтому нам достаточно проверить, верно ли, что для любого $f \in \mathbb{F}(P_1)$ из $f \in \mathbf{F}_1$ получаем $f \in \mathbb{F}(P_2)$. Отсюда и из леммы 14 получаем, что при сделанных выше предположениях

$$\mathbb{F}(P_1) \subseteq \mathbb{F}(P_2) \Leftrightarrow \mathbb{H}(T(P_2)) \subseteq \mathbb{H}(T(P_1)).$$

Заметим, что

$$\begin{aligned} T\left(\bigcup_{i=1}^n \{\beta_{i,1}\} \cdot \{\gamma_{i,1}\}^* \cdot \{\beta_{i,2}\} \cdot \dots \cdot \{\beta_{i,r(i)-1}\} \cdot \{\gamma_{i,r(i)-1}\}^* \cdot \{\beta_{i,r(i)}\}\right) &= \\ &= \left\{ (n_1(\alpha), n_2(\alpha)) \mid \alpha \in \bigcup_{i=1}^n \{\beta_{i,1}\} \cdot \{\gamma_{i,1}\}^* \cdot \{\beta_{i,2}\} \cdot \dots \right. \\ &\quad \left. \dots \cdot \{\beta_{i,r(i)-1}\} \cdot \{\gamma_{i,r(i)-1}\}^* \cdot \{\beta_{i,r(i)}\} \right\} = \\ &= \bigcup_{i=1}^n \left\{ \left(\sum_{j=1}^{r(i)} n_1(\beta_{i,j}) + \sum_{j=1}^{r(i)-1} m_j n_1(\gamma_{i,j}), \right. \right. \\ &\quad \left. \left. \sum_{j=1}^{r(i)} n_2(\beta_{i,j}) + \sum_{j=1}^{r(i)-1} m_j n_2(\gamma_{i,j}) \right) \mid m_j \in \mathbb{N}^+ \right\} = \\ &= \bigcup_{i=1}^n L \left(\left(\sum_{j=1}^{r(i)} n_1(\beta_{i,j}), \sum_{j=1}^{r(i)} n_2(\beta_{i,j}) \right), \left\{ (n_1(\gamma_{i,j}), n_2(\gamma_{i,j})) \mid 1 \leq j < r(i) \right\} \right). \end{aligned}$$

Таким образом, задача свелась к тому, чтобы по двум конечным семействам пучков X_1, X_2 проверить, верно ли, что $\mathbb{H}(X_1) \subseteq \mathbb{H}(X_2)$. Если в каком-то из пучков $L \in X_2$ в базисе есть неколлинеарные векторы, то по лемме 17

$$\mathbb{H}(L) = \{x \in \mathbb{Q} \mid x < 0\}$$

и значит

$$\mathbb{H}(X_1) \subseteq \{x \in \mathbb{Q} \mid x < 0\} = \mathbb{H}(X_2).$$

В этом случае алгоритм завершен. Если в каком-то из пучков $L \in X_2$ в базисе есть неколлинеарные векторы, то, аналогично,

$$\mathbb{H}(X_1) = \{x \in \mathbb{Q} \mid x < 0\}.$$

Тогда

$$\mathbb{H}(X_1) \subseteq \mathbb{H}(X_2) \Leftrightarrow \mathbb{H}(X_2) = \{x \in \mathbb{Q} \mid x < 0\}.$$

В этом случае алгоритм работает тривиально по общей схеме, которую мы приведем ниже. Считаем теперь, что в базисах пучков из X_1, X_2 нет неколлинеарных векторов. Тогда в силу леммы 20 можно считать, что базисы всех пучков одноэлементны. Далее, разбиваем пучки из X_1 на классы эквивалентности: в один и тот же класс попадают пучки, базисные векторы которых коллинеарны. Разбираем два случая.

1. Какие-то два пучка L_1, L_2 из разных классов пересекаются. Тогда X_1 содержит в себе пучок, у которого есть два базисных неколлинеарных вектора. Применение леммы 17 завершает исследование этого случая.

2. Любые два пучка L_1, L_2 из разных классов не пересекаются. С каждым из классов эквивалентности теперь можно разбираться отдельно. Все пучки делятся на два типа: одноэлементные (базисный вектор равен $(0, 0)$) и бесконечные (базисный вектор не равен $(0, 0)$). Если одноэлементный пучок L_1 пересекается с каким-то другим пучком L_2 , то $L_1 \subseteq L_2$. Значит L_1 можно просто выкинуть. Поэтому далее считаем, что все одноэлементные пучки изолированы от остальных. Далее, если два бесконечных пучка L_1, L_2 пересекаются, то их пересечение тоже будет бесконечным пучком с одноэлементным базисом. Тогда их разность можно разбить в конечное объединение уже непересекающихся пучков с одноэлементным базисом. Значит и объединение конечного количества пучков из общего класса эквивалентности можно разбить в конечное объединение непересекающихся пучков с одноэлементным базисом. (Замечание. Аккуратное доказательство этого факта полностью идентично доказательству леммы 16 из [6] про прогрессивные множества.)

Теперь считаем, что все пучки из X_1 попарно не пересекаются. Тот же самый процесс можно применить и к X_2 . Поэтому считаем, что и все пучки из X_2 попарно не пересекаются. Теперь можно применить леммы 21, 22, 23. Из них следует, что $\mathbb{H}(X_1)$ и $\mathbb{H}(X_2)$ разбиваются в конечное объединение серий вида

$$(a, b) \in \{(ms_iq_1 + e_i), (ns_iq_2 + f_i) \mid m, n \in \mathbb{N}^+\}, \quad \text{НОД}(a, b) = 1.$$

Здесь $q_1, q_2 \in \{0, 1\}$, $k, s_1, \dots, s_k \in \mathbb{N}$, $e_1, f_1 \dots e_k, f_k \in \mathbb{N}^+$. Ясно, что разность любых двух серий такого вида можно в свою очередь разложить в конечное объединение непересекающихся серий. Значит и разность $\mathbb{H}(X_1) \setminus \mathbb{H}(X_2)$ разбивается в конечное объединение непересекающихся серий. Доказательство теоремы завершает применение леммы 24 о проверке серий на пустоту.

В завершение приводим краткое описание алгоритма.

Шаг 1. Проверяем P_1 на примитивность. Если P_1 не примитивно, то $\mathbb{F}(P_1) \subseteq \mathbb{F}(P_2)$ и алгоритм завершен. Иначе шаг 2.

Шаг 2. Представляем P_1 в виде

$$P_1 = \bigcup_{i=1}^k \{\alpha_{i,1}\} \cdot |\mathfrak{P}_{i,1}|^* \cdot \{\alpha_{i,2}\} \cdot \dots \cdot \{\alpha_{i,s(i)-1}\} \cdot |\mathfrak{P}_{i,s(i)-1}|^* \cdot \{\alpha_{i,s(i)}\}.$$

Далее шаг 3.

Шаг 3. Проверяем множества $|\mathfrak{P}_{i_0, j_0}|$, $1 \leq i_0 \leq k$, $1 \leq j_0 < s(i_0)$ на измеримость. Если хоть одно из них не измеримо, то $\mathbb{F}(P_1) \subseteq \mathbb{F}(P_2)$ и алгоритм завершен. Иначе шаг 4.

Шаг 4. Представляем P_1 и P_2 в виде

$$\bigcup_{i=1}^n \{\beta_{i,1}\} \cdot \{\gamma_{i,1}\}^* \cdot \{\beta_{i,2}\} \cdot \dots \cdot \{\beta_{i,r(i)-1}\} \cdot \{\gamma_{i,r(i)-1}\}^* \cdot \{\beta_{i,r(i)}\},$$

где $n, r(1), \dots, r(n)$ — натуральные числа, $\beta_{1,1}, \dots, \beta_{n,r(n)}$ — некоторые слова (возможно пустые) в алфавите A , $\gamma_{1,1}, \dots, \gamma_{n,r(n)-1}$ — некоторые непустые слова в алфавите A . Далее шаг 5.

Шаг 5. Составляем для P_1 и P_2 пучки X_2 и X_1 соответственно по формулам

$$L \left(\left(\sum_{j=1}^{r(i)} n_1(\beta_{i,j}), \sum_{j=1}^{r(i)} n_2(\beta_{i,j}) \right), \left\{ (n_1(\gamma_{i,j}), n_2(\gamma_{i,j})) \mid 1 \leq j < r(i) \right\} \right).$$

Далее шаг 6.

Шаг 6. Если в каком-то из пучков $L \in X_2$ в базисе есть неколлинеарные векторы, то $\mathbb{F}(P_1) \subseteq \mathbb{F}(P_2)$ и алгоритм завершен. Иначе шаг 7.

Шаг 7. Если в каком-то из пучков $L \in X_1$ в базисе есть неколлинеарные векторы, то $\mathbb{H}(X_1) = \{x \in \mathbb{Q} \mid x < 0\}$ и $\mathbb{H}(X_1)$ задается тривиальной серией

$$(a, b) \in \{(m + 1, n + 1) \mid m, n \in \mathbb{N}^+\}, \quad \text{НОД}(a, b) = 1.$$

Далее шаг 11. Иначе шаг 8.

Шаг 8. Если в X_2 есть пересекающиеся пучки с неколлинеарными базисными векторами, то $\mathbb{F}(P_1) \subseteq \mathbb{F}(P_2)$ и алгоритм завершен. Иначе шаг 9.

Шаг 9. Если в X_1 есть пересекающиеся пучки с неколлинеарными базисными векторами, то $\mathbb{H}(X_1)$ задается тривиальной серией

$$(a, b) \in \{(m + 1, n + 1) \mid m, n \in \mathbb{N}^+\}, \quad \text{НОД}(a, b) = 1.$$

Далее шаг 11. Иначе шаг 10.

Шаг 10. Выкидываем все дублирующие одноэлементные пучки. Оставшиеся пучки разбиваем на непересекающиеся. Далее шаг 11.

Шаг 11. Разбиваем $\mathbb{H}(X_1) \setminus \mathbb{H}(X_2)$ в конечное объединение непересекающихся серий. Далее шаг 12.

Шаг 12. Проверяем серии на пустоту. Если хоть одна непуста, то $\mathbb{F}(P_1) \not\subseteq \mathbb{F}(P_2)$ и алгоритм завершен. Иначе $\mathbb{F}(P_1) \subseteq \mathbb{F}(P_2)$ и алгоритм завершен.

Список литературы

- [1] Кудрявцев В.Б., Алешин С.В., Подколзин А.С. Введение в теорию автоматов. — М.: Наука, 1985.
- [2] Яблонский С.В. Введение в дискретную математику. — М.: Наука, 1986.
- [3] Марков Ал. А. Введение в теорию кодирования. — М.: Наука, 1982.
- [4] Дергач П.С. Об однозначности алфавитного декодирования // Интеллектуальные системы. — 2011. Т. 15, вып. 1–4. — С. 349–361.
- [5] Bar-Hillel Y., Perles M., Shamir E. On formal properties of simple phrase-structure grammars // Z. Phonetic. Sprachwiss. Kommunikationsforsch. — 1961. 14. — P. 143–172.

- [6] Дергач П. С. О каноническом регулярном представлении s -тонких языков // Интеллектуальные системы. — 2014. Т. 18, вып. 1. — С. 211–242.
- [7] Постников М. М. Теорема Ферма. Введение в теорию алгебраических чисел. — М.: Наука, 1986.