

Атомарная теория левого деления двусторонних идеалов полуколец с единицей*

А. Е. ПЕНТУС, М. Р. ПЕНТУС

Московский государственный университет
им. М. В. Ломоносова
e-mail: apentus@mech.math.msu.su

УДК 512+510.64

Ключевые слова: идеал полукольца, исчисление Ламбека.

Аннотация

В статье рассматриваются двусторонние идеалы полуколец с единицей. Изучается теория двусторонних идеалов в сигнатуре, состоящей из двуместного предикатного символа, обозначающего отношение «быть подмножеством», и двуместного функционального символа, обозначающего левое деление идеалов. Доказывается, что проблема распознавания истинности атомарной формулы этой сигнатуры на всех полукольцах с единицей при всех оценках разрешима за полиномиальное время. Аналогичный результат верен для атомарных формул с правым делением, но без левого деления.

Abstract

A. E. Pentus, M. R. Pentus, *The atomic theory of left division of two-sided ideals of semirings with unit*, Fundamentalnaya i prikladnaya matematika, vol. 17 (2011/2012), no. 5, pp. 129—146.

We consider two-sided ideals of semirings with unit. We study the theory of two-sided ideals in the signature consisting of the binary predicate symbol $\subseteq$ and a binary function symbol that denotes the left division of ideals. We prove the polynomial-time decidability of the problem of deciding whether a given atomic formula in this signature is valid for all semirings with unit and all valuations. A similar result holds for atomic formulas with the right division, but without the left division.

Введение

В данной статье рассматриваются только полукольца с нулём и единицей (для краткости будем называть их просто полукольцами). На множестве всех двусторонних идеалов произвольного заданного полукольца S можно определить операцию правого деления ($I/J = \{c \in S \mid c \cdot J \subseteq I\}$) и операцию левого деления ($J \backslash I = \{c \in S \mid J \cdot c \subseteq I\}$). Цель статьи — найти эффективный способ проверки тождественной истинности соотношений, формулируемых

*Работа выполнена при частичной поддержке РФФИ (проекты 11-01-00281-а, 11-01-00958-а, 12-01-00888-а, НШ-5593.2012.1).

в терминах отношения $\subseteq$ и только левого деления (или отношения $\subseteq$ и только правого деления). Мы докажем, что для соотношений с делениями только одного направления существует быстрый алгоритм (время его работы ограничено полиномом от длины записи соотношения).

В разделе 1 даются определения, касающиеся полуколец с единицей и их двусторонних идеалов. В разделе 2 вводится исчисление $LM^*(\setminus)$ — монотонное исчисление Ламбека с левым делением, допускающее пустые антецеденты. В разделе 3 доказывается корректность и полнота исчисления $LM^*(\setminus)$ относительно интерпретации на множестве идеалов полукольца с единицей. В разделе 4 доказывается критерий выводимости для исчисления $LM^*(\setminus)$, основанный на графах специального вида. В разделе 5 показывается, как за полиномиальное время можно проверить условие критерия из раздела 4.

1. Полукольца

Определение 1.1. В этой статье *полукольцом с единицей* (или, для краткости, просто *полукольцом*) называется алгебра $\langle S, +, \cdot, 0, 1 \rangle$ с выделенными элементами 0 и 1 и бинарными операциями $+$ и $\cdot$, удовлетворяющими следующим аксиомам (где a, b, c — произвольные элементы множества S):

- 1) $a + b = b + a$;
- 2) $a + 0 = a$;
- 3) $(a + b) + c = a + (b + c)$;
- 4) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
- 5) $a \cdot 1 = a$;
- 6) $1 \cdot a = a$;
- 7) $a \cdot (b + c) = a \cdot b + a \cdot c$;
- 8) $(b + c) \cdot a = b \cdot a + c \cdot a$;
- 9) $a \cdot 0 = 0$;
- 10) $0 \cdot a = 0$.

Пример 1.2. Через $\mathbb{N}$ обозначим множество всех натуральных чисел (ноль считаем натуральным числом). Множество $\mathbb{N}$ с обычными операциями сложения и умножения, нулём и единицей образует полукольцо.

Определение 1.3. Множество $I \subseteq S$ называется *двусторонним идеалом* полукольца $\langle S, +, \cdot, 0, 1 \rangle$, если выполнены следующие условия:

- 1) $0 \in I$;
- 2) $a + b \in I$ для любых $a \in I$ и $b \in I$;
- 3) $a \cdot b \in I$ для любых $a \in I$ и $b \in S$;
- 4) $a \cdot b \in I$ для любых $a \in S$ и $b \in I$.

Пример 1.4. Определим на множестве $\{0, 1, 2, 3, 4, \infty\}$ две бинарные операции $\oplus$ и $\odot$ следующим образом:

$\oplus$	0	1	2	3	4	∞	$\odot$	0	1	2	3	4	∞
0	0	1	2	3	4	∞	0	0	0	0	0	0	0
1	1	2	3	4	∞	∞	1	0	1	2	3	4	∞
2	2	3	4	∞	∞	∞	2	0	2	4	∞	∞	∞
3	3	4	∞	∞	∞	∞	3	0	3	∞	∞	∞	∞
4	4	∞	∞	∞	∞	∞	4	0	4	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞

Тогда $\langle \{0, 1, 2, 3, 4, \infty\}, \oplus, \odot, 0, 1 \rangle$ — полукольцо. Его идеалами являются следующие восемь множеств: $I_0 = \{0\}$, $I_\infty = \{0, \infty\}$, $I_4 = \{0, 4, \infty\}$, $I_3 = \{0, 3, \infty\}$, $I_{3,4} = \{0, 3, 4, \infty\}$, $I_2 = \{0, 2, 4, \infty\}$, $I_{2,3} = \{0, 2, 3, 4, \infty\}$, $I_1 = \{0, 1, 2, 3, 4, \infty\}$.

Определение 1.5. Пусть I и J — некоторые двусторонние идеалы полукольца $\langle S, +, \cdot, 0, 1 \rangle$. Произведение идеала I и идеала J (обозначение $I \cdot J$) определяется как подмножество полукольца S , состоящее из всех конечных сумм $\sum_{k=1}^n a_k \cdot b_k$, где $a_k \in I$ и $b_k \in J$ для всех k (здесь $n \geq 1$).

Замечание 1.6. Пусть I — двусторонний идеал полукольца S . Так как S содержит единицу, легко убедиться, что $I \cdot S = I$ и $S \cdot I = I$.

Определение 1.7. Пусть $\langle S, +, \cdot, 0, 1 \rangle$ — некоторое полукольцо, $c \in S$ и $D \subseteq S$. Тогда через $c \cdot D$ обозначается множество

$$\{a \in S \mid a = c \cdot d \text{ для некоторого } d \in D\}$$

и через $D \cdot c$ — множество

$$\{a \in S \mid a = d \cdot c \text{ для некоторого } d \in D\}.$$

Определение 1.8. Пусть I и J — некоторые двусторонние идеалы полукольца $\langle S, +, \cdot, 0, 1 \rangle$. Правое частное идеала I по идеалу J определяется формулой

$$I/J = \{c \in S \mid c \cdot J \subseteq I\}.$$

Левое частное идеала I по идеалу J определяется формулой

$$J \backslash I = \{c \in S \mid J \cdot c \subseteq I\}.$$

Иногда вместо I/J пишут $I : J$, а вместо $J \backslash I$ — $I :: J$ (см. [6, гл. XII]).

Пример 1.9. Рассмотрим идеалы полукольца из примера 1.4. Согласно определению имеем $I_4/I_2 = I_2 \backslash I_4 = I_{2,3}$, $I_3/I_{2,3} = I_{2,3} \backslash I_3 = I_{3,4}$ и $I_0/I_0 = I_0 \backslash I_0 = I_1$.

Лемма 1.10. Если I и J — двусторонние идеалы некоторого полукольца, то множества I/J и $J \backslash I$ тоже двусторонние идеалы этого полукольца.

Доказательство. Доказательство можно найти в [3]. $\square$

2. Исчисление

Рассмотрим исчисление Ламбека с левым делением, допускающее пустые антецеденты. Оно обозначается $L^*(\backslash)$. Типы этого исчисления строятся из примитивных типов $p_1, p_2, \dots$ с помощью одной бинарной связки $\backslash$. Обозначим множество всех типов, построенных таким образом, через $\text{Tr}(\backslash)$. Прописные буквы латинского алфавита будем использовать для обозначения типов, а прописные греческие буквы — для обозначения конечных последовательностей типов. Множество всех конечных последовательностей типов обозначается $\text{Tr}(\backslash)^*$. Пустая последовательность обозначается Λ .

Выводимыми объектами исчисления Ламбека с левым делением, допускающего пустые антецеденты, являются *секвенции* вида $\Gamma \rightarrow A$. (При этом Γ называется *антецедентом*, а A — *сукцедентом* данной секвенции.) Аксиомы имеют вид $A \rightarrow A$. Выводы строятся с помощью следующих правил:

$$\frac{A\Gamma \rightarrow B}{\Pi \rightarrow A \backslash B} (\rightarrow \backslash), \quad \frac{\Pi \rightarrow A \quad \Gamma B \Delta \rightarrow C}{\Gamma \Pi(A \backslash B) \Delta \rightarrow C} (\backslash \rightarrow),$$

$$\frac{\Pi \rightarrow B \quad \Gamma B \Delta \rightarrow A}{\Gamma \Pi \Delta \rightarrow A} (\text{cut}).$$

Правило (cut) называется *правилом сечения*.

Монотонное исчисление Ламбека с левым делением, допускающее пустые антецеденты (обозначим его $LM^*(\backslash)$), получается из исчисления $L^*(\backslash)$ добавлением правила

$$\frac{\Gamma \Delta \rightarrow A}{\Gamma B \Delta \rightarrow A} (M).$$

Иногда правило М называют *правилом монотонности* (см. [7, с. 47]) или *правилом ослабления* (см. [9, с. 359]).

Пример 2.1. Вывод

$$\frac{\frac{p_1 \rightarrow p_1}{\rightarrow p_1 \backslash p_1} (\rightarrow \backslash) \quad p_2 \rightarrow p_2}{(p_1 \backslash p_1) \backslash p_2 \rightarrow p_2} (\backslash \rightarrow)$$

показывает, что $L^*(\backslash) \vdash (p_1 \backslash p_1) \backslash p_2 \rightarrow p_2$.

Пример 2.2. Вывод

$$\frac{\frac{p_2 \rightarrow p_2}{(p_1 \backslash p_1) p_2 \rightarrow p_2} (M)}{p_2 \rightarrow (p_1 \backslash p_1) \backslash p_2} (\rightarrow \backslash)$$

показывает, что $LM^*(\backslash) \vdash p_2 \rightarrow (p_1 \backslash p_1) \backslash p_2$.

Теорема 2.3 (теорема об устранимости правила сечения). Удаление правила (cut) из исчисления $LM^*(\backslash)$ не меняет множества выводимых секвенций.

Эта теорема является частным случаем следствия 4.8 из [10]. Её можно также доказать индукцией по суммарной сложности типов в правиле сечения, аналогично теореме об устранимости сечения в исчислении Ламбека (см. [1]).

Следствие 2.4. Множество секвенций, выводимых в исчислении $LM^*(\backslash)$, разрешимо.

Доказательство. При движении снизу вверх (от заключения правила к его посылкам) уменьшается сложность секвенций, понимаемая как суммарное число вхождений примитивных типов и знаков операций. Поэтому для любой данной секвенции известно ограничение на длину вывода и можно перебрать все потенциальные выводы этой секвенции. $\square$

3. Модели

Определение 3.1. Оценкой на полукольце S называется произвольная функция v , ставящая в соответствие примитивным типам $p_1, p_2, \dots$ некоторые двусторонние идеалы этого полукольца. Естественное продолжение оценки v на множество всех типов будем тоже обозначать через v . Оно задаётся соотношением $v(A \backslash B) = v(A) \backslash v(B)$, где $A \in \text{Tr}$ и $B \in \text{Tr}$. На множество всех конечных последовательностей типов оценка продолжается следующим образом:

- 1) $v(\Lambda) = S$,
- 2) $v(\Pi A) = v(\Pi) \cdot v(A)$, где $\Pi \in \text{Tr}^*$ и $A \in \text{Tr}$.

Моделью на полукольце (или, для краткости, просто моделью) называется произвольное полукольцо вместе с оценкой на нём.

Пример 3.2. Рассмотрим модель на полукольце $\langle \mathbb{N}, +, \cdot, 0, 1 \rangle$ с оценкой v , заданной следующим образом:

$$v(p_i) = \{2k + 4i \mid k \geq 0\} \cup \{0\}.$$

В этой модели $v(p_2 \backslash p_7) = \{k \mid k \geq 4\} \cup \{0\}$ и $v(p_7 \backslash p_2) = \mathbb{N}$.

Определение 3.3. Секвенция $\Gamma \rightarrow B$ называется *истинной* в модели с оценкой v , если $v(\Gamma) \subseteq v(B)$. В частности, секвенция $A \rightarrow B$, где $A \in \text{Tr}$ и $B \in \text{Tr}$, истинна, если $v(A) \subseteq v(B)$.

Пример 3.4. Рассмотрим модель из примера 3.2. В этой модели секвенция $p_2 \backslash p_7 \rightarrow p_7 \backslash p_2$ истинна, а секвенция $p_7 \backslash p_2 \rightarrow p_2 \backslash p_7$ ложна.

Пример 3.5. Следующие секвенции истинны во всех моделях на полукольцах:

- 1) $\rightarrow p_1 \backslash p_1$;
- 2) $p_1 \rightarrow p_2 \backslash p_1$;
- 3) $p_2 \backslash p_1 \rightarrow (p_3 \backslash p_2) \backslash (p_3 \backslash p_1)$.

Определение 3.6. Равенство типов $A = B$, где $A \in \text{Tr}$ и $B \in \text{Tr}$, называется *истинным* в модели с оценкой v , если $v(A) = v(B)$.

Пример 3.7. Рассмотрим модель из примера 3.2. Равенство $p_1 \backslash p_4 = p_2 \backslash p_7$ истинно в этой модели.

Пример 3.8. Следующие равенства типов истинны во всех моделях на полукольцах:

- 1) $p_1 \setminus p_1 = p_2 \setminus p_2$;
- 2) $(p_1 \setminus p_1) \setminus p_1 = p_1$.

Теорема 3.9. *Исчисление $LM^*(\setminus)$ корректно относительно моделей на полукольцах (т. е. каждая выводимая в исчислении $LM^*(\setminus)$ секвенция истинна на всех полукольцах при всех оценках).*

Доказательство. Пусть даны полукольцо $\langle S, +, \cdot, 0, 1 \rangle$ и оценка v . Нетрудно доказать, что для любых двусторонних идеалов I, J, K выполняются следующие соотношения:

- 1) $(I \cdot J) \cdot K = I \cdot (J \cdot K)$;
- 2) $I \cdot J \subseteq K$ тогда и только тогда, когда $J \subseteq I \setminus K$;
- 3) $I \cdot J \subseteq I$;
- 4) $I \cdot J \subseteq J$.

Из них выводятся соотношения

- 5) если $I \subseteq J$; то $I \cdot K \subseteq J \cdot K$ и $K \cdot I \subseteq K \cdot J$;
- 6) $J \cdot (J \setminus I) \subseteq I$.

Используя приведённые соотношения и замечание 1.6, можно индукцией по длине вывода доказать, что если $LM^*(\setminus) \vdash \Gamma \rightarrow B$, то $v(\Gamma) \subseteq v(B)$. $\square$

Теорема 3.10. *Исчисление $LM^*(\setminus)$ полно относительно моделей на полукольцах (т. е. каждая секвенция, истинная на всех полукольцах при всех оценках, выводится в исчислении $LM^*(\setminus)$).*

Доказательство. Эта теорема доказывается аналогично теореме 4.1 из [3], но вместо множества $\text{Tr}(\setminus, /)^+$ используется множество $\text{Tr}(\setminus)^*$. $\square$

Из теорем 3.9 и 3.10 сразу следует, что алгоритмическая проблема проверки тождественной истинности соотношений, формулируемых в терминах отношения $\subseteq$ и левого деления идеалов полуколец, разрешима (и даже принадлежит классу NP). Основная цель данной статьи — усилить этот результат, доказав, что данная проблема разрешима за полиномиальное время. Для этого сформулируем критерий выводимости в исчислении $LM^*(\setminus)$, аналогичный критериям для $L(\setminus)$ и $L^*(\setminus)$, открытым Ю. В. Саватеевым (см. [4, 5]).

4. Сети

Сформулируем критерий выводимости для исчисления $LM^*(\setminus)$, основанный на графах специального вида. Следуя традиции, принятой в линейной логике, такой граф будем называть *сетью доказательства* (или, для краткости, просто *сетью*). В конце этого раздела будет доказано, что секвенция выводится в $LM^*(\setminus)$ тогда и только тогда, когда существует сеть, соответствующая данной секвенции.

Формально говоря, сеть доказательства состоит из ориентированного дерева $\langle V, O \rangle$, разметки $\text{label}: V \rightarrow \{p_1, p_2, \dots\}$, строгого линейного порядка $<$ на множестве V и бинарного отношения $S \subseteq V \times V$. Обозначим корень дерева $\langle V, O \rangle$ через $\overset{\circ}{g}$. Здесь дерево $\langle V, O \rangle$ задаётся множеством вершин V и множеством рёбер O , при этом рёбра направлены в сторону корня дерева, то есть бинарное отношение O является графиком функции из множества $V \setminus \{\overset{\circ}{g}\}$ в множество V (эту функцию будем также обозначать через O) и для любого элемента $a \in V$ найдётся такое натуральное число n , что

$$\underbrace{O(\dots O(a) \dots)}_{n \text{ раз}} = \overset{\circ}{g}.$$

Отметим, что функция label может не быть инъективной.

Первые три компоненты (дерево $\langle V, O \rangle$, разметка label и линейный порядок $<$) строятся по секвенции (однозначно) следующим образом. Сеть для секвенции

$$A_1 \dots A_{n-1} A_n \rightarrow B$$

совпадает с сетью для типа

$$A_n \setminus (A_{n-1} \setminus \dots \setminus (A_1 \setminus B) \dots),$$

а упорядоченные размеченные деревья для типов строятся индукцией по построению типа. Примитивному типу соответствует дерево с одной вершиной (она помечена этим примитивным типом). Дерево для типа $A \setminus B$ получается из дизъюнктного объединения деревьев для A и B добавлением ребра, ведущего из корня дерева для A в корень дерева для B . Порядок определяется как сумма перевёрнутого порядка из дерева для A и (неперевёрнутого) порядка из дерева для B . Формально,

$$\begin{aligned} c <_{A \setminus B} d &\Leftrightarrow \\ &\Leftrightarrow (c \in V_A \wedge d \in V_B) \vee (c \in V_A \wedge d \in V_A \wedge d <_A c) \vee (c \in V_B \wedge d \in V_B \wedge c <_B d). \end{aligned}$$

Глубину вершины a (число рёбер на пути из a до корня) обозначим через $d(a)$. Например, $d(\overset{\circ}{g}) = 0$.

Через $\leq$ обозначим рефлексивное замыкание отношения $<$. Через O^+ обозначим транзитивное замыкание отношения O . Через O^* обозначим рефлексивно-транзитивное замыкание отношения O .

Легко проверить (индукцией по построению типа), что в любой сети истинны следующие утверждения.

D1. Если $a \leq b \leq c$, $a O^* d$ и $c O^* d$, то $b O^* d$.

D2. Если $a O^+ b$ и $d(b) = 2n$, то $a < b$.

D3. Если $a O^+ b$ и $d(b) = 2n + 1$, то $b < a$.

Обозначим через $\text{pr}_1(S)$ первую проекцию бинарного отношения S . Формально, $\text{pr}_1(S) = \{a \mid \exists b (a, b) \in S\}$.

В качестве четвёртой компоненты сети можно взять любое бинарное отношение S на множестве V , удовлетворяющее следующим условиям.

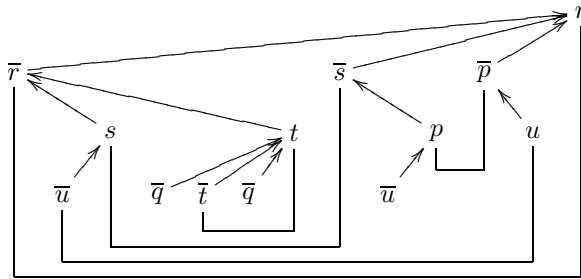
- PN1. Если $(a, b) \in S$, то $(b, a) \in S$ (отношение S симметрично).
 PN2. Если $(a, b) \in S$ и $(a, c) \in S$, то $b = c$ (отношение S функционально).
 PN3. Если $(a, b) \in S$, $(c, d) \in S$ и $a < c < b$, то $a < d < b$.
 PN4. Если $(a, b) \in S$, то $\text{label}(a) = \text{label}(b)$.
 PN5. Если $(a, b) \in S$ и $a < b$, то $d(a) = d(b) + 1$.
 PN6. Если $a < b < O(a)$ и $(b, O(a)) \in S$, то $a \notin \text{pr}_1(S)$.
 PN7. $S \neq \emptyset$.
 PN8. Если $a \in \text{pr}_1(S)$, то $O(a) \in \text{pr}_1(S)$.
 PN9. Если $d(a) = 2n$ и $O(a) \in \text{pr}_1(S)$, то $a \in \text{pr}_1(S)$.

Согласно PN2 отношение S является графиком частичной функции. Эту частичную функцию будем также обозначать через S .

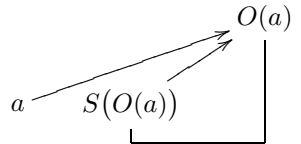
Для минимума, максимума, интервала, отрезка и открытого справа полуинтервала относительно линейного порядка $<$ будем использовать обозначения $\min$, $\max$, $(a; b)$, $[a; b]$ и $[a; b)$. Если $a \in V$ и $\beta \subseteq V$, то запись $a < \beta$ означает, что для всех $b \in \beta$ имеет место $a < b$.

На диаграммах будем располагать вершины на плоскости так, что движение слева направо соответствует линейному порядку $<$ (если $a < b$, то a левее, чем b), а движение сверху вниз соответствует увеличению значения d (если $d(a) < d(b)$, то a выше, чем b). На диаграмме вершину v представляет $\text{label}(v)$ (с чёрточкой сверху, если глубина нечётная). Бинарное отношение O изображается прямыми стрелками, а отношение S — трёхзвенными ломаными линиями.

Пример 4.1. Ниже изображена одна из возможных сетей для выводимой секвенции $(u \setminus p) ((u \setminus p) \setminus s) (((q \setminus (t \setminus (q \setminus t))) \setminus ((u \setminus s) \setminus r)) \rightarrow r$.



Условие PN6 можно изобразить графически. Оно утверждает, что если сеть содержит конфигурацию



то $a \notin \text{pr}_1(S)$.

Лемма 4.2. Каждая сеть для секвенции $\Pi \rightarrow A \setminus B$ является сетью также для секвенции $A \Pi \rightarrow B$, и наоборот.

Теорема 4.3. Пусть $\text{LM}^*(\setminus) \vdash \Phi \rightarrow D$. Тогда существует сеть, соответствующая секвенции $\Phi \rightarrow D$.

Доказательство. Индукция по длине вывода. Рассмотрим в шаге индукции случай правила

$$\frac{\Pi \rightarrow A \quad \Gamma B \Delta \rightarrow C}{\Gamma \Pi(A \setminus B) \Delta \rightarrow C} (\setminus \rightarrow).$$

Пусть для секвенций $\Pi \rightarrow A$ и $\Gamma B \Delta \rightarrow C$ предположение индукции даёт бинарные отношения S' и S'' соответственно. Если корень поддерева, соответствующего типу B , принадлежит $\text{pr}_1(S'')$, то зададим отношение S для $\Gamma \Pi(A \setminus B) \Delta \rightarrow C$ как объединение естественных образов отношений S' и S'' , иначе зададим отношение S как естественный образ отношения S'' .

Остальные случаи в шаге индукции доказываются легко. $\square$

Теорема 4.4. Пусть существует сеть, соответствующая секвенции $\Phi \rightarrow D$. Тогда $\text{LM}^*(\setminus) \vdash \Phi \rightarrow D$.

Теорема 4.4 доказывается индукцией по суммарному количеству связок в Φ и D . Оставшаяся часть раздела 4 посвящена доказательству шага индукции. Согласно лемме 4.2 достаточно ограничиться секвенциями, где сукцедент D является примитивным типом. Рассмотрим произвольную секвенцию $\Phi \rightarrow p_i$ и произвольную соответствующую ей сеть $\langle V, O, \text{label}, <, S \rangle$ и предположим, что для всех секвенций с меньшим количеством связок теорема уже доказана.

Лемма 4.5. $g \in \text{pr}_1(S)$.

Доказательство. Утверждение следует из PN7 и PN8. $\square$

Лемма 4.6. Если $a < b < S(a)$ и $a O^+ b$, то найдётся такая вершина c , что $(b, c) \in S$ и $b < c < S(a)$.

Доказательство. Согласно PN8 из $a \in \text{pr}_1(S)$ следует $b \in \text{pr}_1(S)$. Обозначим $c = S(b)$. Согласно PN3 имеем, что $a < c < S(a)$. Если $b < c$, то лемма доказана. В силу PN5 случай $c = b$ невозможен. Осталось рассмотреть случай $c < b$. Из того, что $a O^+ b$, следует, что существует такой элемент a' , что $a O^* a'$ и $O(a') = b$.

Из D3 следует, что $d(b)$ чётно. Из нечётности $d(a')$ согласно D3 получаем, что $a' \leq a$. Следовательно, $a' < c$. Из того, что $a' < c < O(a')$ и $(c, O(a')) \in S$, согласно PN6 получаем, что $a' \notin \text{pr}_1(S)$, что противоречит PN8. $\square$

Обозначим $\delta = \{a \mid O(a) = S(g)\}$.

Лемма 4.7. Пусть $\delta = \emptyset$. Тогда исходная секвенция $\Phi \rightarrow p_i$ имеет вид $\Theta p_i \Xi \rightarrow p_i$.

Доказательство. Очевидно, $\text{label}(g) = p_i$. Согласно PN4 и PN5 имеем, что $\text{label}(S(g)) = p_i$ и $d(S(g)) = 1$. Следовательно, условие $\delta = \emptyset$ означает, что

в рассматриваемой секвенции с примитивным сукцедентом $\Phi \rightarrow p_i$ вершине $S(\overset{0}{g})$ соответствует примитивный тип p_i в антецеденте на верхнем уровне. $\square$

Осталось рассмотреть случай, когда $\delta \neq \emptyset$. Обозначим

$$\overset{2}{e} = \max \delta.$$

Другими словами, $\overset{2}{e}$ — самая правая из вершин a со свойством $O(a) = S(\overset{0}{g})$.

В следующих леммах (до конца раздела 4) предполагается, что $\delta \neq \emptyset$.

Лемма 4.8. $d(\overset{2}{e}) = 2$.

Доказательство. Утверждение следует из того, что $d(S(\overset{0}{g})) = 1$. $\square$

Обозначим

$$\alpha = \{a \mid a O^* \overset{2}{e}\}, \quad \varphi = \{a \in \text{pr}_1(S) \mid \overset{2}{e} < a, S(a) < \alpha\}.$$

Лемма 4.9. Пусть $a \in \alpha$. Тогда $S(\overset{0}{g}) < a < \overset{0}{g}$.

Доказательство. Пусть $a \in \alpha$, т. е. $a O^* \overset{2}{e}$. Так как $\overset{2}{e} \in \delta$, имеем $O(\overset{2}{e}) = S(\overset{0}{g})$. Из $a O^+ S(\overset{0}{g})$ согласно D3 получаем, что $S(\overset{0}{g}) < a$.

Аналогично из $a O^+ \overset{0}{g}$ согласно D2 получаем, что $a < \overset{0}{g}$. $\square$

Лемма 4.10. Множество φ непусто.

Доказательство. Докажем, что $\overset{0}{g} \in \varphi$. Из D2 получаем, что $\overset{2}{e} < \overset{0}{g}$. Согласно лемме 4.9 имеем, что $S(\overset{0}{g}) < \alpha$. $\square$

Обозначим

$$f = \min \varphi, \quad \pi = (\overset{2}{e}; f).$$

Лемма 4.11. $d(f) \leq 1$.

Доказательство. Допустим, от противного, что $d(f) \geq 2$. Согласно PN5 имеем, что $d(S(f)) \geq 3$. Обозначим через c элемент, удовлетворяющий условиям $S(f) O^+ c$ и $d(c) = 2$. Из того, что $S(f) < \overset{2}{e}$, $S(f) O^+ c$ и $d(c) = d(\overset{2}{e})$, согласно D1 получаем, что $c \leq \overset{2}{e}$. Из того, что $S(f) \notin \alpha$, получаем, что $c \neq \overset{2}{e}$. Итого, $c < \overset{2}{e}$, и даже $c < \alpha$.

Из того, что $S(f) < f < \overset{0}{g}$, согласно PN3 получаем, что $S(\overset{0}{g}) < S(f)$. Согласно D2 имеем $S(f) < c$. Согласно лемме 4.6 имеем $c < S(c)$. Итого, $S(\overset{0}{g}) < S(c)$. Из того, что $S(\overset{0}{g}) < S(c)$, $\overset{2}{e} O^+ S(\overset{0}{g})$ и $d(S(\overset{0}{g})) = d(S(c))$, согласно D1 получаем, что $\overset{2}{e} < S(c)$.

Мы доказали, что $S(c) \in \varphi$. Следовательно, $f \leq S(c)$. Имеем $S(f) < c < f \leq S(c)$, что противоречит PN3. $\square$

Лемма 4.12. Пусть $a \in \alpha \cup \pi$. Тогда $a < f$.

Доказательство. Случай $a \in \pi$ очевиден. Пусть $a \in \alpha$, т. е. $a O^* \overset{2}{e}$. По лемме 4.8 согласно D2 получаем, что $a \leq \overset{2}{e}$. Так как $f \in \varphi$, то $\overset{2}{e} < f$, что влечёт $a < f$. $\square$

Лемма 4.13. Пусть $a \leq b \leq c$, $a \in \alpha \cup \pi$ и $c \in \alpha \cup \pi$. Тогда $b \in \alpha \cup \pi$.

Доказательство. Сначала рассмотрим случай $b \leq \overset{2}{e}$. Так как $a \notin \pi$, имеем $a \in \alpha$. По D1 получаем, что $b O^* \overset{2}{e}$, т. е. $b \in \alpha$.

Теперь рассмотрим случай $\overset{2}{e} < b$. Согласно лемме 4.12 имеем $c < f$. Получаем, что $\overset{2}{e} < b < f$, т. е. $b \in \pi$. $\square$

Лемма 4.14. Пусть $(a, b) \in S$ и $a \in \alpha \cup \pi$. Тогда $b \in \alpha \cup \pi$.

Доказательство. Сначала рассмотрим случай $a < b$. Если $b < f$, то из того, что $a < b \leq \max[\overset{2}{e}; f]$, согласно лемме 4.13 получаем, что $b \in \alpha \cup \pi$. Пусть $f \leq b$. Согласно PN3 имеем $a \leq S(f) < b$. Так как $f \in \varphi$, имеем $S(f) < \alpha$, что влечёт $a < \alpha$, а это противоречит предположению $a \in \alpha \cup \pi$.

Теперь рассмотрим случай $b < a$. Допустим, от противного, что $b \notin \alpha \cup \pi$. Согласно лемме 4.13 имеем, что $b < \alpha$.

Если $\overset{2}{e} < a$, то $a \in \varphi$, что влечёт $f \leq a$, а это противоречит лемме 4.12. Осталось рассмотреть случай $a \leq \overset{2}{e}$. Очевидно, $a \in \alpha$, т. е. $a O^* \overset{2}{e}$. Согласно лемме 4.8 имеем, что $d(a) \geq 2$. По PN5 получаем, что $d(b) \geq 3$. Обозначим через c элемент, удовлетворяющий условиям $b O^+ c$ и $d(c) = 2$. Из $b \notin \alpha$ следует, что $c \neq \overset{2}{e}$. Из $b < \overset{2}{e}$ и $b O^+ c$ по D1 получаем, что $c \leq \overset{2}{e}$ (так как неверно, что $e O^+ c$). Из $c < \overset{2}{e}$ и $d(c) = d(\overset{2}{e})$ получаем, что $c < \alpha$ и, в частности, $c < a$. Из D2 получаем, что $b < c$. Из того, что $b < c < a = S(b)$ и $b O^+ c$, по лемме 4.6 получаем, что $c \in \text{pr}_1(S)$ и $c < S(c) < a$. По PN5 имеем $d(S(c)) = 1$. Из леммы 4.9 по PN3 получаем, что $S(\overset{0}{g}) < b$. Следовательно, $S(\overset{0}{g}) < S(c)$. Из того, что $S(\overset{0}{g}) < S(c) < \overset{2}{e}$, согласно D1 получаем, что $S(c) O^* S(\overset{0}{g})$. Так как $d(S(c)) = d(S(\overset{0}{g}))$, получаем, что $S(c) = S(\overset{0}{g})$, противоречие. $\square$

Лемма 4.15. Пусть $b O^+ a$ и $d(a) = 1$. Тогда условия $a \in \pi$ и $b \in \pi$ равносильны.

Доказательство. В силу D3 имеем, что $a < b$.

Сначала допустим, от противного, что $a \in \pi$, но $b \notin \pi$. Очевидно, $f \leq b$. Согласно условию леммы $d(b) \neq 0$, т. е. $b \neq \overset{0}{g}$. Следовательно, $b < \overset{0}{g}$. Получаем, что $f \neq \overset{0}{g}$, т. е. $d(f) \neq 0$. Согласно лемме 4.11 имеем $d(f) = 1$. Из $f \leq b$, $b O^+ a$ и $d(f) = d(a)$ согласно D1 выводим, что $f \leq a$, что противоречит условию $a \in \pi$.

Теперь допустим, от противного, что $b \in \pi$, но $a \notin \pi$. Очевидно, $a \leq \overset{2}{e} < b$. По D1 получаем, что $\overset{2}{e} O^* a$. Из леммы 4.8 и того, что $d(a) = 1$, получаем, что $a = O(\overset{2}{e}) = S(\overset{0}{g})$. Обозначим через c элемент, удовлетворяющий условиям $b O^* c$ и $O(c) = a$. Очевидно, $c \in \delta$. Следовательно, $c \leq \overset{2}{e} < b$. Так как $d(c) = 2$, то $c < b$ противоречит D2. $\square$

Лемма 4.16. Ограничение сети $\langle V, O, \text{label}, <, S \rangle$ на множество $V \setminus (\alpha \cup \pi)$ является сетью для некоторой секвенции.

Доказательство. Согласно построению вершина $S(\overset{0}{g})$ является корнем некоторого поддерева, соответствующего некоторому типу вида $A \setminus B$ из антецедента. При этом множество α соответствует типу A . Согласно лемме 4.15 исходная секвенция имеет вид $\Gamma \Pi(A \setminus B) \Delta \rightarrow p_i$, где множество π соответствует последовательности Π . Следовательно, множество $V \setminus (\alpha \cup \pi)$ соответствует секвенции $\Gamma B \Delta \rightarrow p_i$. Для ограничения сети $\langle V, O, \text{label}, <, S \rangle$ на множество $V \setminus (\alpha \cup \pi)$ легко проверить условия PN1—PN9. Например, при проверке PN8 и PN9 используется лемма 4.14. $\square$

Лемма 4.17. *Найдутся такие типы A и B и последовательности Γ и Π , что $\Phi = \Gamma \Pi(A \setminus B) \Delta$ и существуют сети для секвенций $\Pi \rightarrow A$ и $\Gamma B \Delta \rightarrow p_i$.*

Доказательство. Определим A и Π как в доказательстве леммы 4.16, где предъявлена сеть для секвенции $\Gamma B \Delta \rightarrow p_i$. Сеть для секвенции $\Pi \rightarrow A$ получается из ограничения сети $\langle V, O, \text{label}, <, S \rangle$ на множество $\alpha \cup \pi$ очевидными преобразованиями: перестановкой двух частей (α и π) в смысле отношения $<$ и объявлением вершины $\overset{2}{e}$ корнем всего дерева, что приводит к уменьшению глубины каждой вершины из α на 2.

Формально говоря, пусть секвенции $\Pi \rightarrow A$ соответствуют дерево $\langle V', O' \rangle$, разметка label' и линейный порядок $<'$. Глубину вершины a в дереве $\langle V', O' \rangle$ обозначим через $d'(a)$. Легко доказать, что существует биекция $\mathfrak{h}: V' \rightarrow \alpha \cup \pi$ со следующими свойствами:

$$\begin{aligned} a O' b &\Leftrightarrow (\mathfrak{h}(a) O \mathfrak{h}(b) \wedge \mathfrak{h}(a) \in \alpha \wedge \mathfrak{h}(b) \in \alpha) \\ &\quad \vee (\mathfrak{h}(a) O \mathfrak{h}(b) \wedge \mathfrak{h}(a) \in \pi \wedge \mathfrak{h}(b) \in \pi) \\ &\quad \vee (\mathfrak{h}(a) O \overset{0}{g} \wedge \mathfrak{h}(b) = \overset{2}{e}), \\ a <' b &\Leftrightarrow (\mathfrak{h}(a) < \mathfrak{h}(b) \wedge \mathfrak{h}(a) \in \alpha \wedge \mathfrak{h}(b) \in \alpha) \\ &\quad \vee (\mathfrak{h}(a) < \mathfrak{h}(b) \wedge \mathfrak{h}(a) \in \pi \wedge \mathfrak{h}(b) \in \pi) \\ &\quad \vee (\mathfrak{h}(a) \in \pi \wedge \mathfrak{h}(b) \in \alpha), \\ \text{label}'(a) &= \text{label}(\mathfrak{h}(a)), \\ d'(a) &= \begin{cases} d(\mathfrak{h}(a)) - 2, & \text{if } \mathfrak{h}(a) \in \alpha, \\ d(\mathfrak{h}(a)), & \text{if } \mathfrak{h}(a) \in \pi. \end{cases} \end{aligned}$$

Искомая сеть для секвенции $\Pi \rightarrow A$ задаётся бинарным отношением

$$S' = \{(a, b) \mid (\mathfrak{h}(a), \mathfrak{h}(b)) \in S\}.$$

Осталось проверить условия PN1—PN9 для S' .

Докажем PN8 для S' . Пусть $a \in \text{pr}_1(S')$. Если $\mathfrak{h}(a) \in \alpha$ и $\mathfrak{h}(O'(a)) \in \alpha$, то $O'(a) \in \text{pr}_1(S')$ следует из условия PN8 для S . Аналогично если $\mathfrak{h}(a) \in \pi$ и $\mathfrak{h}(O'(a)) \in \pi$, то $O'(a) \in \text{pr}_1(S')$ следует из условия PN8 для S . Если же $\mathfrak{h}(a) \in \pi$ и $\mathfrak{h}(O'(a)) \in \alpha$, то $\mathfrak{h}(O'(a)) = \overset{2}{e} \in \text{pr}_1(S)$, что влечёт $O'(a) \in \text{pr}_1(S')$.

Докажем PN6 для S' . Допустим, от противного, что $a \in V'$, $b \in V'$, $a <' b <' O'(a)$, $(b, O'(a)) \in S'$ и $a \in \text{pr}_1(S')$. Если $\mathfrak{h}(O'(a)) \in \pi$, то можно

применить PN6 для S , $\mathfrak{h}(a)$ и $\mathfrak{h}(b)$, так как согласно критерию для $<'$ имеем $\mathfrak{h}(a) \in \pi$ и $\mathfrak{h}(b) \in \pi$. Если $\mathfrak{h}(a) \in \alpha$ и $\mathfrak{h}(O'(a)) \in \alpha$, то можно применить PN6 для S , $\mathfrak{h}(a)$ и $\mathfrak{h}(b)$, так как согласно критерию для $<'$ имеем $\mathfrak{h}(b) \in \alpha$.

Осталось рассмотреть случай, когда $\mathfrak{h}(a) \in \pi$ и $\mathfrak{h}(O'(a)) \in \alpha$. Согласно критерию для O' это возможно только при $\mathfrak{h}(O'(a)) = \overset{2}{e}$ и $O(\mathfrak{h}(a)) = \overset{0}{g}$. Обозначим

$$\gamma = \{c \in \text{pr}_1(S') \mid \mathfrak{h}(c) \in \pi, c <' b, d'(c) = 1\}.$$

Очевидно, $\gamma \neq \emptyset$, так как $a \in \gamma$. Обозначим через a_1 элемент множества γ , минимальный в смысле отношения $<'$. Так как $a_1 \in \text{pr}_1(S')$, можно рассмотреть элемент $S'(a_1)$. Согласно PN5 глубина $S'(a_1)$ равна 0 или 2. Если $d'(S'(a_1)) = 0$, то $S'(a_1) = O'(a)$, т. е. $a_1 = S'(O'(a)) = b$, что невозможно, так как $a_1 \in \gamma$. Следовательно, $d'(S'(a_1)) = 2$ и $S'(a_1) <' a_1$. По D3 имеем $O'(S'(a_1)) <' S'(a_1)$, что влечёт $O'(S'(a_1)) <' a_1 <' b$. По PN8 имеем $O'(S'(a_1)) \in \text{pr}_1(S')$. В силу леммы 4.15 $\mathfrak{h}(O'(S'(a_1))) \in \pi$. Получаем, что $O'(S'(a_1)) \in \gamma$, что противоречит минимальности a_1 . Тем самым мы доказали PN6.

Условие PN7, т. е. $S' \neq \emptyset$, следует из того, что $\overset{2}{e} \in \alpha$ и $\overset{2}{e} \in \text{pr}_1(S)$.

Остальные условия из определения сети проверяются легко. $\square$

Для завершения доказательства теоремы 4.4 достаточно заметить, что шаг индукции следует из лемм 4.7 и 4.17. Если $\delta = \emptyset$, то исходная секвенция $\Phi \rightarrow p_i$ выводится из аксиомы многократным применением правила (M), иначе секвенция $\Phi \rightarrow p_i$ получается по правилу $(\setminus \rightarrow)$ из двух более коротких секвенций, к которым применимо предположение индукции. Теорема 4.4 доказана.

5. Алгоритм

Условия критерия выводимости, сформулированные в разделе 4, можно проверить методом динамического программирования.

По данной секвенции построим дерево $\langle V, O \rangle$, разметку label и линейный порядок $<$ как в определении сети.

Обозначим через Q рефлексивно-транзитивное замыкание бинарного отношения $O \cup \{(a, b) \mid b O a, d(b) \text{ чётно}\}$.

Определим четырёхместный предикат P на множестве V , положив $P(e_1, e_2, e_3, e_4)$ истинным тогда и только тогда, когда $e_1 \leq e_4$ и существует бинарное отношение S на множестве V , удовлетворяющее следующим условиям.

- F1. Если $(a, b) \in S$, то $e_1 \leq a < e_4$ и $e_1 \leq b < e_4$.
- F2. Если $(a, b) \in S$, то $(b, a) \in S$.
- F3. Если $(a, b) \in S$ и $(a, c) \in S$, то $b = c$.
- F4. Если $(a, b) \in S$, $(c, d) \in S$ и $a < c < b$, то $a < d < b$.
- F5. Если $(a, b) \in S$, то $\text{label}(a) = \text{label}(b)$.
- F6. Если $(a, b) \in S$ и $a < b$, то $d(a) = d(b) + 1$.

F7. Если $a < b < O(a)$ и $(b, O(a)) \in S$, то $a \notin \text{pr}_1(S)$ и $e_1 \leq a$.

F8. Если $a Q b$, $a \in \text{pr}_1(S)$ и $e_1 \leq b < e_4$, то $b \in \text{pr}_1(S)$.

F9. $e_2 = \max\{a \in V \mid a \leq e_4, [e_1; a] \cap \text{pr}_1(S) = \emptyset\}$.

F10. $e_3 = \min\{a \in V \mid e_1 \leq a, [a; e_4] \cap \text{pr}_1(S) = \emptyset\}$.

Лемма 5.1. Пусть $e_1 \leq e_4$. Тогда $P(e_1, e_4, e_1, e_4)$.

Доказательство. Положим $S = \emptyset$. $\square$

Лемма 5.2. Пусть даны e_1, e_2, e_3 и e_4 . Пусть для некоторого отношения S выполнены условия F9 и F10. Тогда $e_1 \leq e_2 \leq e_4$ и $e_1 \leq e_3 \leq e_4$. Условия $e_2 = e_4$ и $e_3 = e_1$ равносильны.

Лемма 5.3. Пусть $a Q b$ и неверно, что $a O^* b$. Тогда $a O^*(O(b))$ и $d(b)$ чётно.

Доказательство. Рассмотрим кратчайший путь из a в b в ориентированном графе с множеством рёбер $O \cup \{(a, b) \mid b O a, d(b) \text{ чётно}\}$. Так как бинарное отношение O является функциональным, то в этом пути ребро из $\{(a, b) \mid b O a, d(b) \text{ чётно}\}$ может быть только последним. $\square$

Лемма 5.4. Пусть $a \leq b \leq c$ или $c \leq b \leq a$. Пусть $a Q c$. Тогда $b Q c$.

Доказательство. Если $a O^* c$, то по D1 имеем, что $b O^* c$. Пусть неверно, что $a O^* c$. Согласно лемме 5.3 получаем, что $a O^*(O(c))$ и $d(c)$ чётно. По D1 имеем, что $b O^*(O(c))$. $\square$

Лемма 5.5. Пусть некоторое отношение S удовлетворяет условиям F1 и F8 для четвёрки, состоящей из e_1, e_2, e_3 и e_4 . Пусть $a Q b$, $a < b < e_4$, и $b \notin \text{pr}_1(S)$. Тогда $[a; b] \cap \text{pr}_1(S) = \emptyset$.

Доказательство. Допустим, от противного, что $c \in [a; b] \cap \text{pr}_1(S)$. По F1 имеем $e_1 \leq c$. Следовательно, $e_1 \leq b$. Согласно лемме 5.4 предположение $a Q b$ влечёт $c Q b$, что противоречит условию F8. $\square$

Лемма 5.6. Пусть некоторое отношение S удовлетворяет условиям F8, F9 и F10 для четвёрки, состоящей из e_1, e_2, e_3 и e_4 . Пусть $a Q b$. Пусть $a \leq e_2 \leq b < e_4$ или $e_1 \leq b < e_3 \leq a$. Тогда $b \in \text{pr}_1(S)$.

Доказательство. Рассмотрим случай $a \leq e_2 \leq b < e_4$. Согласно лемме 5.2 имеем $e_1 \leq e_2 \leq b$. Из того, что $e_2 \neq e_4$, и F9 получаем, что $e_2 \in \text{pr}_1(S)$. По лемме 5.4 имеем $e_2 Q b$. По F8 получаем, что $b \in \text{pr}_1(S)$.

Теперь рассмотрим случай $e_1 \leq b < e_3 \leq a$. Согласно лемме 5.2 имеем $b < e_4$. Обозначим через c элемент, удовлетворяющий условиям $c < e_3$ и $(c; e_3) = \emptyset$. Очевидно, $b \leq c$. По F10 заключаем, что $c \in \text{pr}_1(S)$. Согласно лемме 5.4 имеем, что $c Q b$. По F8 получаем, что $b \in \text{pr}_1(S)$. $\square$

Лемма 5.7. Пусть некоторое отношение S удовлетворяет условиям F1, F7 и F8 для четвёрки, состоящей из e_1, e_2, e_3 и e_4 . Пусть $a < b < O(a)$ и $(b, O(a)) \in S$. Тогда $[a; b] \cap \text{pr}_1(S) = \emptyset$.

Доказательство. Допустим, от противного, что $a \leq c < b$ и $c \in \text{pr}_1(S)$. По D1 имеем, что $c \in O^+(O(a))$. Следовательно, найдётся такой элемент c' , что $c \in O^* c'$ и $O(c') = O(a)$. Из D3 следует, что $d(O(a))$ чётно. Из нечётности $d(c')$ согласно D3 следует, что $c' \leq c$. Согласно условию F1 имеем $c < e_4$ и, следовательно, $c' < e_4$. Так как $c' < b < O(c')$ и $(b, O(c')) \in S$, то по F7 имеем $e_1 \leq c'$ и $c' \notin \text{pr}_1(S)$. Это противоречит условию F8, так как $c \in Q c' \in \text{pr}_1(S)$ и $e_1 \leq c' < e_4$. $\square$

Лемма 5.8. Истинность $P(e_1, e_2, e_3, e_4)$ равносильна истинности формулы

$$\begin{aligned}
 & e_1 = e_2 = e_3 = e_4 \vee \\
 & \vee \exists b_4 (P(e_1, \min(e_2, b_4), e_3, b_4) \wedge b_4 < e_4 \wedge (b_4; e_4) = \emptyset \wedge e_2 \neq b_4 \wedge e_2 \leq e_4 \wedge \\
 & \quad \wedge \neg(\exists c \in [e_1; e_3]) c \in Q b_4) \vee \\
 & \vee \exists a_3 \exists a_4 \exists b_1 \exists b_2 \exists b_3 \exists b_4 (P(e_1, e_2, a_3, a_4) \wedge P(b_1, b_2, b_3, b_4) \wedge \\
 & \quad \wedge a_4 < b_1 \wedge (a_4; b_1) = \emptyset \wedge b_4 < e_4 \wedge (b_4; e_4) = \emptyset \wedge \\
 & \quad \wedge e_3 = e_4 \wedge \text{label}(a_4) = \text{label}(b_4) \wedge d(a_4) = d(b_4) + 1 \wedge \\
 & \quad \wedge \neg(\exists c < a_3) O(c) = b_4 \wedge \\
 & \quad \wedge \neg(\exists c \in [a_3; a_4] \cup [b_1; b_2]) a_4 \in Q c \wedge \neg(\exists c \in [b_3; b_4]) b_4 \in Q c). \tag{1}
 \end{aligned}$$

Доказательство. Сначала докажем, что формула (1) следует из истинности $P(e_1, e_2, e_3, e_4)$. Пусть $P(e_1, e_2, e_3, e_4)$. Если $e_1 = e_4$, то согласно лемме 5.2 имеем $e_1 = e_2 = e_3 = e_4$.

Пусть $e_1 < e_4$. Обозначим через b_4 элемент, удовлетворяющий условиям $b_4 < e_4$ и $(b_4; e_4) = \emptyset$. Зафиксируем какое-нибудь отношение S , удовлетворяющее условиям F1–F10. Рассмотрим отдельно случаи $b_4 \notin \text{pr}_1(S)$ и $b_4 \in \text{pr}_1(S)$.

Пусть $b_4 \notin \text{pr}_1(S)$. Докажем, что истинен второй дизъюнктивный член формулы (1). Если $e_2 = e_4$, то $S = \emptyset$, $e_3 = e_1$, $P(e_1, b_4, e_1, b_4)$. Если же $e_2 < e_4$, то отношение S удовлетворяет условиям F1–F10 также для четвёрки, состоящей из e_1 , e_2 , e_3 и b_4 . Рассмотрим произвольный элемент $c \in [e_1; e_3]$ и допустим, от противного, что $c \in Q b_4$. Согласно лемме 5.5 имеем, что $[c; b_4] \cap \text{pr}_1(S) = \emptyset$. По F10 имеем, что $e_3 \leq c$, что противоречит условию $c \in [e_1; e_3]$.

Пусть $b_4 \in \text{pr}_1(S)$. Докажем, что истинен третий дизъюнктивный член формулы (1). Обозначим $a_4 = S(b_4)$. Из того, что $a_4 < e_4$ и $a_4 \neq b_4$, получаем, что $a_4 < b_4$. Обозначим через b_1 элемент, удовлетворяющий условиям $a_4 < b_1$ и $(a_4; b_1) = \emptyset$. Положим

$$\begin{aligned}
 S' &= S \cap ([e_1; a_4] \times [e_1; a_4]), \\
 S'' &= S \cap ([b_1; b_4] \times [b_1; b_4]), \\
 a_3 &= \min\{a \in V \mid e_1 \leq a, [a; a_4] \cap \text{pr}_1(S) = \emptyset\}, \\
 b_2 &= \max\{a \in V \mid a \leq b_4, [b_1; a] \cap \text{pr}_1(S) = \emptyset\}, \\
 b_3 &= \min\{a \in V \mid b_1 \leq a, [a; b_4] \cap \text{pr}_1(S) = \emptyset\}.
 \end{aligned}$$

Заметим, что согласно PN3 имеем

$$S = S' \cup S'' \cup \{(a_4, b_4), (b_4, a_4)\}.$$

Докажем, что $\neg(\exists c < a_3) O(c) = b_4$. Пусть, от противного, $c < a_3$ и $O(c) = b_4$. По лемме 5.7 получаем, что $[c; a_4) \cap \text{pr}_1(S) = \emptyset$. По выбору a_3 имеем, что $a_3 \leq c$, противоречие.

Так как $a_4 \in \text{pr}_1(S)$, $[a_3; a_4) \cap \text{pr}_1(S) = \emptyset$ и $[b_1; b_2) \cap \text{pr}_1(S) = \emptyset$, то в силу F8 истинна формула $\neg(\exists c \in [a_3; a_4) \cup [b_1; b_2)) a_4 Q c$. Так как $b_4 \in \text{pr}_1(S)$ и $[b_3; b_4) \cap \text{pr}_1(S) = \emptyset$, то в силу F8 истинна формула $\neg(\exists c \in [b_3; b_4)) b_4 Q c$. Осталось проверить, что отношение S' удовлетворяет условиям F1–F10 для четвёрки, состоящей из e_1, e_2, a_3 и a_4 , а отношение S'' удовлетворяет условиям F1–F10 для четвёрки, состоящей из b_1, b_2, b_3 и b_4 .

Докажем истинность условия F7 для отношения S'' . Пусть $a < b$, $b_1 \leq b < O(a) < b_4$ и $(b, O(a)) \in S$. Согласно условию F7 для отношения S имеем $a \notin \text{pr}_1(S)$. По лемме 5.7 получаем, что $[a; b) \cap \text{pr}_1(S) = \emptyset$. Так как $a_4 \in \text{pr}_1(S)$ и $a_4 < b$, имеем $a_4 < a$. Следовательно, $b_1 \leq a$.

Остальные условия для отношений S' и S'' проверяются легко.

Теперь докажем, что $P(e_1, e_2, e_3, e_4)$ следует из формулы (1). Рассмотрим три случая, соответствующие трём дизъюнктивным членам формулы (1).

Первый случай очевиден.

Второй случай. Если $b_4 \leq e_2$, то из условий $(b_4; e_4) = \emptyset$, $e_2 \neq b_4$ и $e_2 \leq e_4$ получаем, что $e_2 = e_4$, а из $P(e_1, b_4, e_3, b_4)$ и леммы 5.2 получаем, что $e_3 = e_1$. Остаётся применить лемму 5.1. Пусть теперь $e_2 < b_4$. Зафиксируем какое-нибудь отношение S , удовлетворяющее условиям F1–F10 для четвёрки, состоящей из e_1, e_2, e_3 и b_4 . Можно проверить, что отношение S удовлетворяет условиям F1–F10 также для четвёрки, состоящей из e_1, e_2, e_3 и e_4 . Докажем, например, условие F8. Пусть $a Q b$, $a \in \text{pr}_1(S)$ и $e_1 \leq b < e_4$. Если $b < b_4$, то можно применить условие F8 для четвёрки, состоящей из e_1, e_2, e_3 и b_4 . Пусть $b = b_4$. Согласно F10 из $a \in \text{pr}_1(S)$ следует, что $a < e_3$. Мы получили противоречие с формулой $\neg(\exists c \in [e_1; e_3)) c Q b_4$.

Третий случай. Зафиксируем какое-нибудь отношение S' , удовлетворяющее условиям F1–F10 для четвёрки, состоящей из e_1, e_2, a_3 и a_4 , и какое-нибудь отношение S'' , удовлетворяющее условиям F1–F10 для четвёрки, состоящей из b_1, b_2, b_3 и b_4 . Положим $S = S' \cup S'' \cup \{(a_4, b_4), (b_4, a_4)\}$ и проверим условия F1–F10 для четвёрки, состоящей из e_1, e_2, e_3 и e_4 .

Докажем истинность условия F7. Пусть $a < b < O(a)$ и $(b, O(a)) \in S$. Если $O(a) \in \text{pr}_1(S')$, то $b \in \text{pr}_1(S')$, и можно применить условие F7 для S' . Если $O(a) \in \text{pr}_1(S'')$, то $b \in \text{pr}_1(S'')$, и можно применить условие F7 для S'' . Если $O(a) = a_4$, то $b = b_4$, что противоречит условию $b < O(a)$. Осталось рассмотреть случай $O(a) = b_4$. Очевидно, $b = a_4$. Так как $\neg(\exists c < a_3) O(c) = b_4$, то $a_3 \leq a$. Согласно условию F10 для S' из $a_3 \leq a < a_4$ получаем, что $a \notin \text{pr}_1(S')$. Следовательно, $a \notin \text{pr}_1(S)$.

Докажем истинность условия F8. Пусть $a Q b$, $a \in \text{pr}_1(S)$ и $e_1 \leq b < e_4$. Случаи $b = a_4$ и $b = b_4$ очевидны. Если $e_1 \leq a < a_4$ и $e_1 \leq b < a_4$, то

применим условие F8 для S' . Если $b_1 \leq a < b_4$ и $b_1 \leq b < b_4$, то применим условие F8 для S'' . Если $e_1 \leq b < a_3$ и $a_4 \leq a$, то применим лемму 5.6 для S' . Если $a_3 \leq b < a_4$ и $a_4 \leq a$, то согласно лемме 5.4 имеем, что $a_4 Q b$, что противоречит формуле (1). Если $b_1 \leq b < b_3$ и $a = b_4$, то применим лемму 5.6 для S'' . Случай $b_3 \leq b < b_4$ и $a = b_4$ противоречит формуле (1). Если $b_1 \leq b < b_2$ и $a < b_1$, то согласно лемме 5.4 имеем $a_4 Q b$, что противоречит формуле (1). Если $b_2 \leq b < b_4$ и $a < b_1$, то применим лемму 5.6 для S'' . Мы доказали, что во всех случаях $b \in \text{pr}_1(S)$.

Докажем истинность условия F9. Согласно условию F9 для S' имеем

$$\begin{aligned} e_2 &= \max\{a \in V \mid a \leq a_4, [e_1; a] \cap \text{pr}_1(S') = \emptyset\} = \\ &= \max\{a \in V \mid a \leq a_4, [e_1; a] \cap \text{pr}_1(S) = \emptyset\}. \end{aligned}$$

Так как $a_4 \in \text{pr}_1(S)$, то при $a_4 < a$ имеем $[e_1; a] \cap \text{pr}_1(S) \neq \emptyset$. Следовательно, $e_2 = \max\{a \in V \mid a \leq e_4, [e_1; a] \cap \text{pr}_1(S) = \emptyset\}$.

Условие F10 следует из того, что $b_4 \in \text{pr}_1(S)$, $(b_4; e_4) = \emptyset$ и $e_3 = e_4$.

Остальные условия из определения предиката P проверяются легко. $\square$

Лемма 5.9. Для исходной секвенции $\Phi \rightarrow p_i$ существует сеть тогда и только тогда, когда истинна формула

$$\begin{aligned} \exists a_4 \exists b_1 \exists b_2 \exists b_3 (P(b_1, b_2, b_3, g) \wedge a_4 < b_1 \wedge (a_4; b_1) = \emptyset \wedge \\ \wedge \text{label}(a_4) = \text{label}(g) \wedge d(a_4) = 1 \wedge \neg(\exists c < b_2) a_4 = O(c)). \end{aligned}$$

Лемма 5.9 доказывается аналогично лемме 5.8.

В алгоритме вычислим $P(e_1, e_2, e_3, e_4)$ для всех значений e_1, e_2, e_3 и e_4 из V , причём во внешнем цикле значение $[[e_1; e_4]]$ возрастает от 1 до $|V|$, а во внутренних циклах e_1, e_2 и e_3 пробегают все возможные значения. Легко понять, что на вычисление $P(e_1, e_2, e_3, e_4)$ по критерию из леммы 5.8 каждый раз тратится полиномиальное время. В конце алгоритма используем критерий из леммы 5.9, чтобы узнать, существует ли сеть для исходной секвенции.

Согласно теореме 4.3 описанный выше алгоритм отвечает на вопрос о выводимости в исчислении $\text{LM}^*(\backslash)$. Согласно теоремам 3.9 и 3.10 этот же алгоритм отвечает на вопрос об истинности атомарной формулы рассматриваемой сигнатуры (состоящей из двуместного предикатного символа, обозначающего отношение «быть подмножеством», и двуместного функционального символа, обозначающего левое деление идеалов) на всех полукольцах при всех оценках.

Литература

- [1] Ламбек И. Математическое исследование структуры предложения // Математическая лингвистика: Сборник переводов / Под ред. Ю. А. Шрейдера и др. — М.: Мир, 1964. — С. 47—68.
- [2] Ламбек И. Кольца и модули. — М.: Мир, 1971.

- [3] Пентус А. Е., Пентус М. Р. Атомарная теория деления двусторонних идеалов полуколец // *Фундамент. и прикл. мат.* — 2006. — Т. 12, вып. 2. — С. 201—208.
- [4] Саватеев Ю. В. Распознавание выводимости для исчисления Ламбека с одним делением // *Вестн. Моск. ун-та. Сер. 1. Математика, механика.* — 2009. — № 2. — С. 59—62.
- [5] Саватеев Ю. В. Применение сетей доказательств для исследования фрагментов исчисления Ламбека // *Изв. РАН. Сер. мат.* — 2011. — Т. 75, № 3. — С. 189—222.
- [6] Фукс Л. Частично упорядоченные алгебраические системы. — М.: Мир, 1965.
- [7] Van Benthem J. *Language in Action. Categories, Lambdas and Dynamic Logic.* — Amsterdam: North-Holland, 1991. — (Stud. Logic Foundations Math.; Vol. 130).
- [8] Buszkowski W. Completeness results for Lambek syntactic calculus // *Z. Math. Logik Grundlag. Math.* — 1986. — Vol. 32. — P. 13—28.
- [9] Buszkowski W. Type logics in grammar // *Trends in Logic: 50 Years of Studia Logica* / V. F. Hendricks, J. Malinowski, eds. — Kluwer Academic, 2003. — P. 337—382.
- [10] Galatos N., Ono H. Cut elimination and strong separation for substructural logics: an algebraic approach // *Ann. Pure Appl. Logic.* — 2010. — Vol. 161, no. 9. — P. 1097—1133.