Атомарная теория умножения и деления двусторонних идеалов полуколец*

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. Изучается теория двусторонних идеалов в сигнатуре, состоящей из предикатного символа $\subseteq$ и трёх функциональных символов, обозначающих умножение, правое деление и левое деление идеалов. Доказывается, что множество атомарных формул этой сигнатуры, истинных на всех полукольцах при всех оценках, разрешимо.

Abstract

A. E. Pentus, M. R. Pentus, The atomic theory of multiplication and division of semiring ideals, Fundamentalnaya i prikladnaya matematika, vol. 15 (2009), no. 2, pp. 169—189.

We consider two-sided ideals of semirings. More precisely, we study the theory of two-sided ideals in the signature consisting of the predicate symbol $\subseteq$ and three function symbols that denote the multiplication, right division, and left division of ideals. We prove that the set of those atomic formulas in this signature that are valid for all semirings and all valuations is decidable.

Введение

На множестве всех двусторонних идеалов произвольного заданного полукольца S можно определить операцию умножения ($I \cdot J$ — минимальный идеал, содержащий попарные произведения элементов из идеалов I и J), 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 данной статьи — указать эффективный способ проверки тождественной истинности соотношений, формулируемых в терминах умножения, правого деления, левого деления и отношения $\subseteq$. Эта задача для случая без умножения была решена в [3].

*Работа выполнена при частичной поддержке РФФИ (проекты 08-01-00399, НШ-845.2008.1, 06-01-72554-НЦНИЛ).

Фундаментальная и прикладная математика, 2009, том 15, № 2, с. 169—189.

В разделе 1 даются определения, касающиеся полуколец и их двусторонних идеалов. В разделе 2 вводится исчисление LM — исчисление Ламбека с добавленным правилом монотонности. В разделе 3 приводится доказательство корректности исчисления LM относительно интерпретации на множестве идеалов полукольца. В разделе 4 строится универсальная модель на множестве идеалов конкретного полукольца. В разделе 5 доказываются вспомогательные леммы. В разделе 6 доказывается, что в исчислении LM выводятся все тождественно истинные свойства двусторонних идеалов полуколец, записываемые в указанной сигнатуре как атомарные формулы. (Доказательство основано на том, что невыводимые в LM свойства опровергаются в модели, построенной в разделе 4.) Так как множество выводимых секвенций исчисления LM разрешимо, оказывается установленной разрешимость атомарной теории умножения и деления двусторонних идеалов.

1. Полукольца

Определение 1.1. В этой статье *полукольцом* называется алгебра $\langle S, +, \cdot, 0\rangle$ с выделенным элементом 0 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) $a \cdot (b + c) = a \cdot b + a \cdot c$;
6) $(b + c) \cdot a = b \cdot a + c \cdot a$;
7) $a \cdot 0 = 0$;
8) $0 \cdot a = 0$.

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

Пример 1.3. Определим на множестве $\{0, 1, 2, 3, 4\}$ две бинарные операции $\oplus$ и $\odot$ следующим образом:

$$\begin{array}{c|ccccc} \oplus & 0 & 1 & 2 & 3 & 4 \\ \hline 0 & 0 & 1 & 2 & 3 & 4 \\ 1 & 1 & 1 & 2 & 3 & 4 \\ 2 & 2 & 2 & 2 & 3 & 4 \\ 3 & 3 & 3 & 3 & 3 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 \end{array}\,, \qquad \begin{array}{c|ccccc} \odot & 0 & 1 & 2 & 3 & 4 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 2 & 3 & 4 & 4 \\ 2 & 0 & 3 & 4 & 4 & 4 \\ 3 & 0 & 4 & 4 & 4 & 4 \\ 4 & 0 & 4 & 4 & 4 & 4 \end{array}\,.$$

Тогда $\langle\{0, 1, 2, 3, 4\}, \oplus, \odot, 0\rangle$ является полукольцом.

Определение 1.4. Множество $I \subseteq S$ называется *двусторонним идеалом* полукольца $\langle S, +, \cdot, 0\rangle$, 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 1.5. Определим на множестве $\{0, 1, 2, 3, 4, \infty\}$ две бинарные операции $\oplus$ и $\odot$ следующим образом:

$$\begin{array}{c|cccccc}
\oplus & 0 & 1 & 2 & 3 & 4 & \infty \\
\hline
0 & 0 & 1 & 2 & 3 & 4 & \infty \\
1 & 1 & 2 & 3 & 4 & \infty & \infty \\
2 & 2 & 3 & 4 & \infty & \infty & \infty \\
3 & 3 & 4 & \infty & \infty & \infty & \infty \\
4 & 4 & \infty & \infty & \infty & \infty & \infty \\
\infty & \infty & \infty & \infty & \infty & \infty & \infty
\end{array}, \qquad
\begin{array}{c|cccccc}
\odot & 0 & 1 & 2 & 3 & 4 & \infty \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 & \infty \\
2 & 0 & 2 & 4 & \infty & \infty & \infty \\
3 & 0 & 3 & \infty & \infty & \infty & \infty \\
4 & 0 & 4 & \infty & \infty & \infty & \infty \\
\infty & 0 & \infty & \infty & \infty & \infty & \infty
\end{array}.$$

Тогда $\langle\{0, 1, 2, 3, 4, \infty\}, \oplus, \odot, 0\rangle$ является полукольцом. Идеалами этого полукольца являются следующие восемь множеств:

$$I_0 = \{0\}, \quad I_\infty = \{0, \infty\}, \quad I_4 = \{0, 4, \infty\}, \quad I_3 = \{0, 3, \infty\},$$
$$I_{3,4} = \{0, 3, 4, \infty\}, \quad I_2 = \{0, 2, 4, \infty\}, \quad I_{2,3} = \{0, 2, 3, 4, \infty\}, \quad I_1 = \{0, 1, 2, 3, 4, \infty\}.$$

Определение 1.6. Пусть I и J — некоторые двусторонние идеалы полукольца $\langle S, +, \cdot, 0\rangle$. *Произведение идеала I и идеала J* (обозначение $I \cdot J$) определяется как подмножество полукольца S, состоящее из всех конечных сумм $\sum\limits_{k=1}^{n} a_k \cdot b_k$, где $a_k \in I$ и $b_k \in J$ для всех k (здесь $n \geqslant 1$).

Пример 1.7. Рассмотрим идеалы полукольца из примера 1.5. Согласно определению $I_2 \cdot I_2 = I_4$ и $I_{2,3} \cdot I_{3,4} = I_\infty$.

Определение 1.8. Пусть $\langle S, +, \cdot, 0\rangle$ — 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 1.9. Пусть I и J — некоторые двусторонние идеалы полукольца $\langle S, +, \cdot, 0\rangle$. *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. [4, гл. XII]).

Пример 1.10. Рассмотрим идеалы полукольца из примера 1.5. Согласно определению $I_4/I_2 = I_2\backslash I_4 = I_{2,3}$, $I_3/I_{2,3} = I_{2,3}\backslash I_3 = I_{3,4}$ и $I_0/I_0 = I_0\backslash I_0 = I_1$.

Лемма 1.11. *Если I и J — двусторонние идеалы некоторого полукольца, то множества $I \cdot J$, I/J и $J\backslash I$ тоже двусторонние идеалы этого полукольца.*

Доказательство. Пусть I и J — двусторонние идеалы полукольца $\langle S, +, \cdot, 0\rangle$.

Докажем, что $I \cdot J$ является двусторонним идеалом.

Свойство $0 \in I \cdot J$ следует из того, что $0 = 0 \cdot 0 \in I \cdot J$.

Аксиома 2) для $I \cdot J$ следует из того, что сумма двух конечных сумм снова является конечной суммой.

Проверим аксиому 3). Пусть $a \in S$ и $b \in I \cdot J$. Последнее означает, что $b = \sum\limits_{k=1}^{n} c_k \cdot d_k$, где $c_k \in I$ и $d_k \in J$ для всех k. Так как I — идеал, то $a \cdot c_k \in I$ для всех k. Следовательно,

$$a \cdot b = a \cdot \sum_{k=1}^{n} c_k \cdot d_k = \sum_{k=1}^{n} a \cdot (c_k \cdot d_k) = \sum_{k=1}^{n} (a \cdot c_k) \cdot d_k \in I \cdot J.$$

Аксиома 4) проверяется аналогично.

Теперь докажем, что I/J является двусторонним идеалом.

Свойство $0 \in I/J$ следует из того, что $0 \cdot J = \{0\} \subseteq I$.

Проверим аксиому 2) из определения 1.4. Пусть $a \in I/J$ и $b \in I/J$. Для любого элемента $d \in J$ имеем $a \cdot d \in I$, $b \cdot d \in I$ и, следовательно, $(a + b) \cdot d = a \cdot d + b \cdot d \in I$. Поэтому $a + b \in I/J$.

Проверим аксиому 3). Пусть $a \in S$ и $b \in I/J$. Для любого элемента $d \in J$ имеем $b \cdot d \in I$ и, следовательно, $(a \cdot b) \cdot d = a \cdot (b \cdot d) \in I$. Поэтому $a \cdot b \in I/J$.

Проверим аксиому 4). Пусть $a \in S$ и $b \in I/J$. Для любого элемента $d \in J$ имеем $a \cdot d \in J$ и, следовательно, $(b \cdot a) \cdot d = b \cdot (a \cdot d) \in I$. Поэтому $b \cdot a \in I/J$.

Доказательство для $J\backslash I$ аналогично. □

2. Исчисление Ламбека

Рассмотрим синтаксическое исчисление, введённое в [1] И. Ламбеком. *Типы* исчисления Ламбека строятся из примитивных типов $p_1, p_2, \ldots$ с помощью трёх бинарных связок $\boldsymbol{\cdot}$, $\backslash$, $/$. Обозначим множество всех типов, построенных таким образом, через Tp. Прописные буквы латинского алфавита будем использовать для обозначения типов исчисления Ламбека, а прописные греческие буквы — для обозначения конечных последовательностей типов. Символ Λ будет всегда обозначать пустую последовательность типов.

Выводимыми объектами исчисления Ламбека являются *секвенции* вида $\Gamma \to A$, где $\Gamma \neq \Lambda$. Аксиомы имеют вид $A \to A$. Выводы строятся с помощью следующих правил:

$$\frac{A\Pi \to B}{\Pi \to A\backslash B}\ (\to \backslash),\ \text{где } \Pi \neq \Lambda, \qquad \frac{\Phi \to A \quad \Gamma B \Delta \to C}{\Gamma \Phi (A\backslash B) \Delta \to C}\ (\backslash \to),$$

$$\frac{\Pi A \to B}{\Pi \to B/A}\ (\to /),\ \text{где } \Pi \neq \Lambda, \qquad \frac{\Phi \to A \quad \Gamma B \Delta \to C}{\Gamma (B/A) \Phi \Delta \to C}\ (/ \to),$$

$$\frac{\Gamma \to A \quad \Delta \to B}{\Gamma \Delta \to A \cdot B}\ (\to \cdot), \qquad \frac{\Gamma A B \Delta \to C}{\Gamma (A \cdot B) \Delta \to C}\ (\cdot \to),$$

$$\frac{\Pi \to B \quad \Gamma B \Delta \to A}{\Gamma \Pi \Delta \to A}\ (\mathrm{cut}).$$

Правило (cut) называется *правилом сечения*.

Через LM обозначается исчисление, полученное из исчисления Ламбека добавлением правила

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

Иногда это правило называют *правилом монотонности* (см. [7, с. 47]) или *правилом ослабления* (см. [6, с. 359]).

Пример 2.1. Вывод

$$\dfrac{\dfrac{\dfrac{p_2 \to p_2}{p_1\, p_2 \to p_2}\ (\mathrm{M})}{p_1 \cdot p_2 \to p_2}\ (\cdot \to) \qquad \dfrac{\dfrac{p_2 \to p_2}{p_2\, p_3 \to p_2}\ (\mathrm{M})}{p_2 \to p_2/p_3}\ (\to /)}{p_1 \cdot p_2 \to p_2/p_3}\ (\mathrm{cut})$$

показывает, что $\mathrm{LM} \vdash p_1 \cdot p_2 \to p_2/p_3$.

Теорема 2.2 (теорема об устранимости правила сечения). *Удаление правила* (cut) *из исчисления* LM *не меняет множества выводимых секвенций.*

Эта теорема доказывается аналогично теореме об устранимости сечения в исчислении Ламбека (см. [1]).

Пример 2.3. Секвенция $p_1 \cdot p_2 \to p_2/p_3$ выводится и без применения правила (cut):

$$\dfrac{\dfrac{\dfrac{\dfrac{p_2 \to p_2}{p_2\, p_3 \to p_2}\ (\mathrm{M})}{p_1\, p_2\, p_3 \to p_2}\ (\mathrm{M})}{p_1\, p_2 \to p_2/p_3}\ (\to /)}{p_1 \cdot p_2 \to p_2/p_3}\ (\cdot \to).$$

Следствие 2.4. *Множество секвенций, выводимых в исчислении* LM*, 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 заданной секвенции известно ограничение на длину вывода, и можно перебрать все потенциальные выводы этой секвенции. □

3. Модели

Определение 3.1. *Оценкой* на полукольце называется произвольная функция v, ставящая в соответствие примитивным типам $p_1, p_2, \ldots$ некоторые двусторонние идеалы этого полукольца. Естественное продолжение оценки v на множество всех типов будем тоже обозначать через v. Оно задаётся следующими соотношениями:

1) $v(A \boldsymbol{\cdot} B) = v(A) \cdot v(B)$,
2) $v(A \backslash B) = v(A) \backslash v(B)$,
3) $v(B / A) = v(B) / v(A)$,

где $A \in \mathrm{Tp}$ и $B \in \mathrm{Tp}$. *Моделью на полукольце* (или, для краткости, просто *моделью*) будем называть произвольное полукольцо вместе с оценкой на нём.

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

$$v(p_i) = \{k \mid k \geqslant i\} \cup \{0\}.$$

В этой модели

$$\begin{aligned} v(p_3 \boldsymbol{\cdot} p_1) &= \{k \mid k \geqslant 3\} \cup \{0\}, \\ v((p_3 \boldsymbol{\cdot} p_1)/p_2) &= \{k \mid k \geqslant 2\} \cup \{0\}, \\ v(p_1/p_2) &= \mathbb{N}, \\ v(p_3 \boldsymbol{\cdot} (p_1/p_2)) &= \{k \mid k \geqslant 3\} \cup \{0\}. \end{aligned}$$

Определение 3.3. Секвенция $A_1 \ldots A_n \to B$ называется *истинной* в модели с оценкой v, если $v(A_1) \cdot \ldots \cdot v(A_n) \subseteq v(B)$. В частности, секвенция $A \to B$, где $A \in \mathrm{Tp}$ и $B \in \mathrm{Tp}$, истинна, если $v(A) \subseteq v(B)$.

Пример 3.4. Рассмотрим модель из примера 3.2. В этой модели секвенция $p_3 \boldsymbol{\cdot} (p_1/p_2) \to (p_3 \boldsymbol{\cdot} p_1)/p_2$ истинна, а секвенция $(p_3 \boldsymbol{\cdot} p_1)/p_2 \to p_3 \boldsymbol{\cdot} (p_1/p_2)$ ложна.

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

1) $p_1 \boldsymbol{\cdot} p_2 \to p_1$;
2) $p_1 \boldsymbol{\cdot} p_2 \to p_2$;
3) $p_1 \to (p_1 \boldsymbol{\cdot} p_2)/p_2$;
4) $p_1 \to p_2 \backslash (p_2 \boldsymbol{\cdot} p_1)$;
5) $p_2 \to (p_1/p_2) \backslash p_1$;
6) $p_2 \to p_1/(p_2 \backslash p_1)$;
7) $p_1 \boldsymbol{\cdot} (p_2/p_3) \to (p_1 \boldsymbol{\cdot} p_2)/p_3$;
8) $(p_3 \backslash p_2) \boldsymbol{\cdot} p_1 \to p_3 \backslash (p_2 \boldsymbol{\cdot} p_1)$;
9) $p_1/p_2 \to (p_1/p_3)/(p_2/p_3)$;
10) $p_2 \backslash p_1 \to (p_3 \backslash p_2) \backslash (p_3 \backslash p_1)$.

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

Пример 3.7. Рассмотрим модель из примера 3.2. Равенство $p_9/p_3 = p_4\backslash p_9$ истинно в этой модели.

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

1) $(p_1/p_2)/p_3 = p_1/(p_3 \boldsymbol{\cdot} p_2)$;
2) $p_3\backslash(p_2\backslash p_1) = (p_2 \boldsymbol{\cdot} p_3)\backslash p_1$;
3) $(p_1\backslash p_2)/p_3 = p_1\backslash(p_2/p_3)$;
4) $p_1/((p_1/p_2)\backslash p_1) = p_1/p_2$;
5) $(p_1/(p_2\backslash p_1))\backslash p_1 = p_2\backslash p_1$.

Для случая идеалов кольца с единицей первые три из этих равенств сформулированы в [2, § 1.2].

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

Доказательство. Пусть даны полукольцо $\langle S, +, \cdot, 0\rangle$ 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 $I \subseteq K/J$;
3) $I \cdot J \subseteq K$ тогда и только тогда, когда $J \subseteq I\backslash K$;
4) $I \cdot J \subseteq I$;
5) $I \cdot J \subseteq J$.

Из них выводятся соотношения

6) если $I \subseteq J$, то $I \cdot K \subseteq J \cdot K$ и $K \cdot I \subseteq K \cdot J$;
7) $(I/J) \cdot J \subseteq I$;
8) $J \cdot (J\backslash I) \subseteq I$.

Используя приведённые соотношения, можно индукцией по длине вывода доказать, что если $\mathrm{LM} \vdash A_1 \ldots A_n \to B$, то $v(A_1) \cdot \ldots \cdot v(A_n) \subseteq v(B)$. □

Основная цель данной статьи — доказать обратную теорему (см. следствие 6.5).

4. Построение универсальной модели

Построим модель на полукольце, в которой ложны все невыводимые в исчислении LM секвенции. При построении полукольца будут использоваться термы (основными элементами полукольца будут упорядоченные пары термов). Аналогичная техника (но с другим набором функциональных символов) применялась В. Бушковским в [5] для построения универсальной модели для исчисления Ламбека.

Нам понадобятся две серии одноместных функциональных символов, каждая из которых индексирована элементами Tp и натуральными числами. Обозначим эти функциональные символы l_ξ^A и r_ξ^A, где $A \in \mathrm{Tp}$ и $\xi \in \mathbb{N}$. Никакие операции к натуральным числам, используемым в нижних индексах, применяться не будут, важно лишь то, что они образуют счётное множество. Обозначим через Tm множество замкнутых термов в сигнатуре, состоящей из этих функциональных символов и константы o. Другими словами, множество Tm — наименьшее множество, удовлетворяющее следующим требованиям:

1) $o \in \mathrm{Tm}$;
2) если $t \in \mathrm{Tm}$, $A \in \mathrm{Tp}$ и $\xi \in \mathbb{N}$, то $l_\xi^A(t) \in \mathrm{Tm}$;
3) если $t \in \mathrm{Tm}$, $A \in \mathrm{Tp}$ и $\xi \in \mathbb{N}$, то $r_\xi^A(t) \in \mathrm{Tm}$.

Нам понадобится специальный линейный порядок на множестве термов. Сначала зафиксируем какое-нибудь взаимно-однозначное соответствие между множеством всех функциональных символов

$$\{l_\xi^A \mid A \in \mathrm{Tp},\ \xi \in \mathbb{N}\} \cup \{r_\xi^A \mid A \in \mathrm{Tp},\ \xi \in \mathbb{N}\}$$

и множеством положительных целых чисел. Назовём положительное целое число, соответствующее функциональному символу, его *весом*. Назовём *весом* терма из Tm сумму весов всех входящих в него функциональных символов (естественно, терм o получит нулевой вес). Зафиксируем на множестве Tm какой-нибудь линейный порядок $\prec$, согласованный с весами в следующем смысле: если вес терма s меньше веса терма t, то $s \prec t$.

Лемма 4.1. *Пусть $t \in \mathrm{Tm}$, $A \in \mathrm{Tp}$ и $\xi \in \mathbb{N}$. Тогда $t \prec l_\xi^A(t)$ и $t \prec r_\xi^A(t)$.*

Лемма 4.2. *Пусть $t \in \mathrm{Tm}$. Тогда множество $\{s \in \mathrm{Tm} \mid s \prec t\}$ конечно.*

Введём обозначения $\preceq$ и $\max$ стандартным образом:

$$s \preceq t \iff s \prec t \vee s = t, \qquad \max(s,t) = \begin{cases} t, & \text{если } s \prec t, \\ s, & \text{если } t \preceq s. \end{cases}$$

При построении искомой модели будем использовать вспомогательное исчисление, выводимыми объектами которого являются упорядоченные тройки из $\mathrm{Tm} \times \mathrm{Tm} \times \mathrm{Tp}$. Выводимость тройки $\langle s, t, A\rangle$ (где $s \in \mathrm{Tm}$, $t \in \mathrm{Tm}$ и $A \in \mathrm{Tp}$) будет обозначаться $s, t \Vdash A$. Содержательно $s, t \Vdash A$ означает, что пара $\langle s, t\rangle$ принадлежит идеалу, который соответствует типу A. На схемах утверждение $s, t \Vdash A$ будет обозначаться стрелкой с меткой A из вершины s в вершину t. Если известно, что $s \prec t$, то на схеме вершина t размещается выше вершины s.

Приведём аксиомы и правила этого вспомогательное исчисления.

A1. Если $t \in \mathrm{Tm}$, $A \in \mathrm{Tp}$ и $\xi \in \mathbb{N}$, то $l_\xi^A(t), t \Vdash A$.

$$\begin{tikzcd} l_\xi^A(t) \arrow[dr, "A"'] & \\ & t \end{tikzcd}$$

A2. Если $t \in \mathrm{Tm}$, $A \in \mathrm{Tp}$ и $\xi \in \mathbb{N}$, то $t, r_\xi^A(t) \Vdash A$.

$$\begin{tikzcd} & r_\xi^A(t) \\ t \arrow[ur, "A"'] & \end{tikzcd}$$

R1. Если $\mathrm{LM} \vdash A \to B$ и $t_1, t_2 \Vdash A$, то $t_1, t_2 \Vdash B$.

R2. Если $t_2 \prec \max(t_1, t_3)$, $t_1, t_2 \Vdash A$ и $t_2, t_3 \Vdash B$, то $t_1, t_3 \Vdash A \bullet B$.

$$\begin{tikzcd} t_1 \arrow[rr, "A \bullet B"] \arrow[dr, "A"'] & & t_3 \\ & t_2 \arrow[ur, "B"'] & \end{tikzcd}$$

R3. Если $t_2 = r_\xi^A(t_1)$, $t_3 \prec t_2$ и $t_1, t_3 \Vdash A \bullet B$, то $t_2, t_3 \Vdash B$.

$$\begin{tikzcd} & r_\xi^A(t_1) \arrow[dr, "B"] & \\ t_1 \arrow[rr, "A \bullet B"'] & & t_3 \end{tikzcd}$$

Лемма 4.3. *Если $s, t \Vdash E$ получено по аксиоме* A1 *или правилу* R3*, то $t \prec s$. Если $s, t \Vdash E$ получено по аксиоме* A2*, то $s \prec t$.*

Доказательство. Для аксиом это следует из леммы 4.1, для правила R3 — из условия при этом правиле. □

Построим искомое полукольцо на множестве

$$S = S_- \cup \{0, \infty\},$$

где

$$S_- = \{\langle t_1, t_2 \rangle \mid t_1, t_2 \Vdash A \text{ для некоторого } A\},$$

а 0 и ∞ — два новых элемента, не принадлежащих множеству $\mathrm{Tm} \times \mathrm{Tm}$. Сложение в полукольце S задаём следующим образом:

$$a + b = \begin{cases} b, & \text{если } a = 0, \\ a, & \text{если } b = 0, \\ \infty, & \text{если } a \neq 0 \text{ и } b \neq 0. \end{cases}$$

Умножение в полукольце S задаём следующим образом:

$$a \cdot b = \begin{cases} 0, & \text{если } a = 0 \text{ или } b = 0, \\ \langle s_1, s_3 \rangle, & \text{если } a = \langle s_1, s_2 \rangle \text{ и } b = \langle s_2, s_3 \rangle, \\ \infty & \text{в остальных случаях.} \end{cases}$$

Рассмотрим следующую оценку v, ставящую в соответствие переменным $p_1, p_2, \ldots$ подмножества множества S:

$$v(p_i) = \{\langle t_1, t_2 \rangle \mid t_1, t_2 \Vdash p_i\} \cup \{0, \infty\}. \tag{1}$$

Осталось доказать, что

1) $\langle S, +, \cdot, 0 \rangle$ является полукольцом (лемма 6.1),
2) для каждого i множество $v(p_i)$ является идеалом этого полукольца (лемма 6.2) и
3) если $\mathrm{LM} \nvdash A \to B$, то $v(A) \nsubseteq v(B)$ (теорема 6.4).

Для установления последнего свойства нам понадобится аналог соотношения (1) для произвольных типов (лемма 6.3).

5. Свойства вспомогательного исчисления

Лемма 5.1. *Пусть $s_1 \preceq s_2$ и $s_3 \preceq s_2$. Пусть существует вывод $s_1, s_2 \Vdash C$, содержащий m_1 применений правила* R2 *и n_1 применений правила* R3. *Пусть существует вывод $s_2, s_3 \Vdash D$, содержащий m_2 применений правила* R2 *и n_2 применений правила* R3. *Тогда существует вывод $s_1, s_3 \Vdash C \cdot D$, содержащий не более $m_1 + m_2$ применений правила* R2 *и не более $n_1 + n_2$ применений правила* R3.

$$\begin{tikzcd}
& s_2 \arrow[dr, "D^{m_2}_{n_2}"] & \\
s_1 \arrow[ur, "C^{m_1}_{n_1}"] \arrow[rr, "(C \cdot D)^{m_1+m_2}_{n_1+n_2}"'] & & s_3
\end{tikzcd}$$

(*Здесь и далее на схемах выражения в верхнем и нижнем индексе при типе указывают оценку количества применений правила* R2 *и применений правила* R3 *соответственно.*)

Доказательство. Предположим, от противного, что существует контрпример, т. е. пара выводов $s_1, s_2 \Vdash C$ и $s_2, s_3 \Vdash D$, для которой заключение леммы не выполняется. Рассмотрим те контрпримеры, у которых значение n_1+n_2 минимально. Среди них выделим те контрпримеры, у которых значение m_1+m_2 минимально. Среди них выберем какой-нибудь контрпример, состоящий из выводов $s_1, s_2 \Vdash C$ и $s_2, s_3 \Vdash D$ с минимальным суммарным количеством применений правила R1.

Рассмотрим пять случаев, соответствующих тому, какое правило является последним в выводе $s_1, s_2 \Vdash C$.

Случай 1: правило R1.

Пусть $s_1, s_2 \Vdash C$ получено по правилу R1 из $s_1, s_2 \Vdash A$, где $\mathrm{LM} \vdash A \to C$.

$$\begin{tikzcd}
 & s_2 \arrow[dr, "D"] & \\
s_1 \arrow[ur, "A"'] \arrow[ur, bend left, "C"] \arrow[rr, "A\cdot D"] \arrow[rr, bend right, "C\cdot D"'] & & s_3
\end{tikzcd}$$

Так как вывод $s_1, s_2 \Vdash A$ содержит столько же применений правил R2 и R3, сколько вывод $s_1, s_2 \Vdash C$, но меньше применений правила R1, то пара, состоящая из выводов $s_1, s_2 \Vdash A$ и $s_2, s_3 \Vdash D$, не является контрпримером (поскольку рассматриваемый контрпример выбран минимальным). Следовательно, существует вывод $s_1, s_3 \Vdash A\cdot D$, содержащий не более $m_1 + m_2$ применений правила R2 и не более $n_1 + n_2$ применений правила R3. Проверим, что $\mathrm{LM} \vdash A\cdot D \to C\cdot D$:

$$\cfrac{\cfrac{A \to C \quad D \to D}{A\,D \to C\cdot D}\,(\to \cdot)}{A\cdot D \to C\cdot D}\,(\cdot \to).$$

По правилу R1 из $s_1, s_3 \Vdash A\cdot D$ получим вывод $s_1, s_3 \Vdash C\cdot D$, содержащий не более $m_1 + m_2$ применений правила R2 и не более $n_1 + n_2$ применений правила R3. Противоречие.

Случай 2: правило R2.

Пусть $C = A\cdot B$ и $s_1, s_2 \Vdash C$ получено по правилу R2 из вывода $s_1, t_2 \Vdash A$, содержащего m_1' применений правила R2 и n_1' применений правила R3, и вывода $t_2, s_2 \Vdash B$, содержащего m_1'' применений правила R2 и n_1'' применений правила R3, где $t_2 \prec \max(s_1, s_2)$, $m_1 = m_1' + m_1'' + 1$ и $n_1 = n_1' + n_1''$.

$$\begin{tikzcd}
 & & s_2 \arrow[dr, "D^{m_2}_{n_2}"] & \\
s_1 \arrow[r, "A^{m_1'}_{n_1'}"] & t_2 \arrow[ur, "B^{m_1''}_{n_1''}"] \arrow[rr, "(B\cdot D)^{m_1''+m_2}_{n_1''+n_2}"'] & & s_3
\end{tikzcd}$$

Так как $\mathrm{LM} \vdash A\cdot(B\cdot D) \to (A\cdot B)\cdot D$, то для получения противоречия достаточно доказать, что существует вывод $s_1, s_3 \Vdash A\cdot(B\cdot D)$, содержащий не более $m_1 + m_2$ (т. е. $m_1' + m_1'' + m_2 + 1$) применений правила R2 и не более $n_1 + n_2$ (т. е. $n_1' + n_1'' + n_2$) применений правила R3 (искомый вывод получится применением правила R1).

Согласно условиям леммы $\max(s_1, s_2) = s_2$. Следовательно, $t_2 \prec s_2$. Так как $n_1'' + n_2 \leqslant n_1 + n_2$ и $m_1'' + m_2 < m_1 + m_2$, то пара, состоящая из рассматриваемых выводов $t_2, s_2 \Vdash B$ и $s_2, s_3 \Vdash D$, не является контрпримером (поскольку рассматриваемый контрпример выбран минимальным). Следовательно, существует вывод $t_2, s_3 \Vdash B\cdot D$, содержащий не более $m_1'' + m_2$ применений правила R2 и не более $n_1'' + n_2$ применений правила R3. Рассмотрим два подслучая.

Случай 2.1: $t_2 \prec \max(s_1, s_3)$.

По правилу R2 из $s_1, t_2 \Vdash A$ и $t_2, s_3 \Vdash B\cdot D$ получим вывод $s_1, s_3 \Vdash A\cdot(B\cdot D)$, содержащий не более $m_1' + (m_1'' + m_2) + 1$ применений правила R2 и не более $n_1' + (n_1'' + n_2)$ применений правила R3.

Случай 2.2: $\max(s_1, s_3) \preceq t_2$.

Так как $n_1' + (n_1'' + n_2) = n_1 + n_2$ и $m_1' + (m_1'' + m_2) < m_1 + m_2$, то пара, состоящая из рассматриваемых выводов $s_1, t_2 \Vdash A$ и $t_2, s_3 \Vdash B \cdot D$, не является контрпримером (поскольку рассматриваемый контрпример выбран минимальным). Следовательно, существует вывод $s_1, s_3 \Vdash A \cdot (B \cdot D)$, содержащий не более $m_1' + (m_1'' + m_2)$ применений правила R2 и не более $n_1' + (n_1'' + n_2)$ применений правила R3.

Случай 3: правило R3.

Согласно лемме 4.3 $s_2 \prec s_1$, что противоречит условию $s_1 \preceq s_2$.

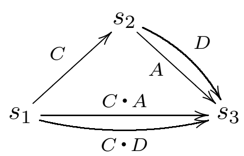
Случай 4: аксиома A1.

Этот случай невозможен согласно лемме 4.3.

Случай 5: аксиома A2.

Заметим, что $m_1 = 0$ и $n_1 = 0$. Рассмотрим пять подслучаев, соответствующих тому, какое правило является последним в выводе $s_2, s_3 \Vdash D$.

Случай 5.1: правило R1.

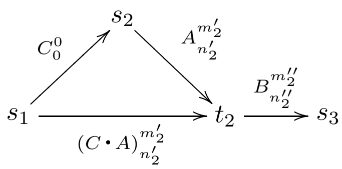


Рассуждаем аналогично случаю 1. Пусть $s_2, s_3 \Vdash D$ получено по правилу R1 из $s_2, s_3 \Vdash A$, где $\mathrm{LM} \vdash A \to D$. Так как вывод $s_2, s_3 \Vdash A$ содержит столько же применений правил R2 и R3, сколько вывод $s_2, s_3 \Vdash D$, но меньше применений правила R1, то пара, состоящая из выводов $s_1, s_2 \Vdash C$ и $s_2, s_3 \Vdash A$, не является контрпримером (поскольку рассматриваемый контрпример выбран минимальным). Следовательно, существует вывод $s_1, s_3 \Vdash C \cdot A$, содержащий не более m_2 применений правила R2 и не более n_2 применений правила R3. Проверим, что $\mathrm{LM} \vdash C \cdot A \to C \cdot D$:

$$\dfrac{\dfrac{C \to C \quad A \to D}{C\, A \to C \cdot D}\,(\to \cdot)}{C \cdot A \to C \cdot D}\,(\cdot \to).$$

По правилу R1 из $s_1, s_3 \Vdash C \cdot A$ получим искомый вывод $s_1, s_3 \Vdash C \cdot D$. Противоречие.

Случай 5.2: правило R2.



Рассуждаем аналогично случаю 2. Пусть $D = A \cdot B$ и $s_2, s_3 \Vdash D$ получено по правилу R2 из вывода $s_2, t_2 \Vdash A$, содержащего m_2' применений правила R2 и

n_2' применений правила R3, и вывода $t_2, s_3 \Vdash B$, содержащего m_2'' применений правила R2 и n_2'' применений правила R3, где $t_2 \prec \max(s_2, s_3)$, $m_2 = m_2' + m_2'' + 1$ и $n_2 = n_2' + n_2''$.

Проверим, что $\mathrm{LM} \vdash (C \cdot A) \cdot B \to C \cdot (A \cdot B)$:

$$\dfrac{\dfrac{\dfrac{C \to C \qquad \dfrac{A \to A \quad B \to B}{A\,B \to A \cdot B}\,(\to \cdot)}{C\,A\,B \to C \cdot (A \cdot B)}\,(\to \cdot)}{(C \cdot A)\,B \to C \cdot (A \cdot B)}\,(\cdot \to)}{(C \cdot A) \cdot B \to C \cdot (A \cdot B)}\,(\cdot \to).$$

Для получения противоречия достаточно доказать, что существует вывод $s_1, s_3 \Vdash (C \cdot A) \cdot B$, содержащий не более m_2 (т. е. $m_2' + m_2'' + 1$) применений правила R2 и не более n_2 (т. е. $n_2' + n_2''$) применений правила R3 (искомый вывод получится применением правила R1).

Согласно условиям леммы $\max(s_2, s_3) = s_2$. Следовательно, $t_2 \prec s_2$. Так как $n_2' \leqslant n_2$ и $m_2' < m_2$, то пара, состоящая из рассматриваемых выводов $s_1, s_2 \Vdash C$ и $s_2, t_2 \Vdash A$, не является контрпримером (поскольку рассматриваемый контрпример выбран минимальным). Следовательно, существует вывод $s_1, t_2 \Vdash C \cdot A$, содержащий не более m_2' применений правила R2 и не более n_2' применений правила R3. Рассмотрим два подслучая.

Случай 5.2.1: $t_2 \prec \max(s_1, s_3)$.

По правилу R2 из $s_1, t_2 \Vdash C \cdot A$ и $t_2, s_3 \Vdash B$ получим вывод $s_1, s_3 \Vdash (C \cdot A) \cdot B$, содержащий не более $m_2' + m_2'' + 1$ применений правила R2 и не более $n_2' + n_2''$ применений правила R3.

Случай 5.2.2: $\max(s_1, s_3) \preceq t_2$.

Так как $n_2' + n_2'' = n_2$ и $m_2' + m_2'' < m_2$, то пара, состоящая из рассматриваемых выводов $s_1, t_2 \Vdash C \cdot A$ и $t_2, s_3 \Vdash B$, не является контрпримером (поскольку рассматриваемый контрпример выбран минимальным). Следовательно, существует вывод $s_1, s_3 \Vdash (C \cdot A) \cdot B$, содержащий не более $m_2' + m_2''$ применений правила R2 и не более $n_2' + n_2''$ применений правила R3.

Случай 5.3: правило R3.

Пусть для некоторых $t_1 \in \mathrm{Tm}$, $A \in \mathrm{Tp}$ и $\xi \in \mathbb{N}$ вывод $s_2, s_3 \Vdash D$ получен по правилу R3 из $t_1, s_3 \Vdash A \cdot D$, где $s_2 = r_\xi^A(t_1)$.

$$\begin{tikzcd}
 & s_2 \arrow[dr, "D^{m_2}_{n_2}"] & \\
t_1 \arrow[ur, "A^0_0"] \arrow[rr, "(A \cdot D)^{m_2}_{n_2 - 1}"'] & & s_3
\end{tikzcd}$$

С другой стороны, так как $s_1, s_2 \Vdash C$ является частным случаем аксиомы A2, имеем $s_2 = r_\zeta^C(s_1)$ для некоторого $\zeta \in \mathbb{N}$. Равенство $r_\xi^A(t_1) = s_2 = r_\zeta^C(s_1)$ означает, что $A = C$, $\xi = \zeta$ и $t_1 = s_1$. Следовательно, вывод $t_1, s_3 \Vdash A \cdot D$ является выводом $s_1, s_3 \Vdash C \cdot D$, причём он содержит $n_2 - 1$ применений правила R3. Противоречие.

Случай 5.4: аксиома A1.

Так как $s_2, s_3 \Vdash D$ является частным случаем аксиомы A1, имеем $s_2 = l_\xi^D(s_3)$ для некоторого $\xi \in \mathbb{N}$. С другой стороны, так как $s_1, s_2 \Vdash C$ является частным случаем аксиомы A2, имеем $s_2 = r_\zeta^C(s_1)$ для некоторого $\zeta \in \mathbb{N}$. Но равенство $l_\xi^D(s_3) = r_\zeta^C(s_1)$ невозможно, так как l_ξ^D и r_ζ^C — различные функциональные символы. Противоречие.

Случай 5.5: аксиома A2.

Согласно лемме 4.3 $s_2 \prec s_3$, что противоречит условию $s_3 \preceq s_2$. □

Лемма 5.2. *Пусть $s_1, s_2 \Vdash C$ и $s_2, s_3 \Vdash D$. Тогда $s_1, s_3 \Vdash C \bullet D$.*

Доказательство. Если $s_2 \prec \max(s_1, s_3)$, то применим правило R2. Если $\max(s_1, s_3) \preceq s_2$, то применим лемму 5.1. □

Лемма 5.3. *Ни для каких $s \in \mathrm{Tm}$ и $C \in \mathrm{Tp}$ не выполняется $s, s \Vdash C$.*

Доказательство. Назовём вывод $s_1, s_2 \Vdash C$ *плохим*, если $s_1 = s_2$. Допустим, от противного, что существует плохой вывод. Пусть минимальное количество применений правила R3 в плохом выводе равно n. Среди плохих выводов, содержащих ровно n применений правила R3, выделим те, которые содержат минимальное количество применений правила R2. Пусть это количество равно m. Среди плохих выводов, содержащих ровно n применений правила R3 и ровно m применений правила R2, выберем какой-нибудь вывод, содержащий минимальное количество применений правила R1. Пусть это вывод $s, s \Vdash C$.

Рассмотрим случаи, соответствующие тому, какое правило является последним в выводе $s, s \Vdash C$. Случаи аксиом A1 и A2 и правила R3 невозможны по лемме 4.3. Остались два случая.

Случай 1: правило R1.

Пусть $s, s \Vdash C$ получено по правилу R1 из $s, s \Vdash A$, где $\mathrm{LM} \vdash A \to C$. Так как плохой вывод $s, s \Vdash A$ содержит столько же применений правил R2 и R3, сколько вывод $s, s \Vdash C$, но меньше применений правила R1, то вывод $s, s \Vdash C$ не является минимальным плохим выводом. Противоречие.

Случай 2: правило R2.

Пусть $C = A \bullet B$ и $s, s \Vdash C$ получено по правилу R2 из вывода $s, t_2 \Vdash A$, содержащего m' применений правила R2 и n' применений правила R3, и вывода $t_2, s \Vdash B$, содержащего m'' применений правила R2 и n'' применений правила R3, где $t_2 \prec \max(s, s) = s$, $m = m' + m'' + 1$ и $n = n' + n''$.

$$\begin{tikzcd} s \arrow[d, bend right, "A^{m'}_{n'}"'] \\ t_2 \arrow[u, bend right, "B^{m''}_{n''}"'] \end{tikzcd}$$

Применим лемму 5.2 к выводам $t_2, s \Vdash B$ и $s, t_2 \Vdash A$, положив $s_1 = t_2$, $s_2 = s$, $s_3 = t_2$, $C = B$, $D = A$, $m_1 = m''$, $n_1 = n''$, $m_2 = m'$, $n_2 = n'$. Согласно лемме 5.1 найдётся вывод $t_2, t_2 \Vdash B \bullet A$, содержащий не более $m'' + m'$ применений правила R2 и не более $n'' + n'$ применений правила R3. Так как этот вывод является плохим, содержит столько же применений правила R3, сколько вывод $s, s \Vdash C$, но меньше применений правила R2, то вывод $s, s \Vdash C$ не является минимальным плохим выводом. Противоречие. $\square$

Лемма 5.4. *Пусть* $s_1 = l_\xi^C(s_2)$, $s_3 \prec s_1$ *и* $s_1, s_3 \Vdash D$. *Если* $s_2 = s_3$, *то* $\mathrm{LM} \vdash C \to D$. *Если* $s_2 \neq s_3$, *то* $s_2, s_3 \Vdash C \backslash D$.

$$\begin{tikzcd}
s_1 \arrow[d, "C"'] \arrow[dr, "D"] & \\
s_2 & s_3
\end{tikzcd}$$

Доказательство. Применим индукцию по длине вывода $s_1, s_3 \Vdash D$. Рассмотрим пять случаев, соответствующих тому, какое правило является последним в этом выводе.

Случай 1: правило R1.

Пусть $s_1, s_3 \Vdash D$ получено по правилу R1 из $s_1, s_3 \Vdash A$, где $\mathrm{LM} \vdash A \to D$. Применив предположение индукции к $s_1, s_3 \Vdash A$, получим, что либо $s_2 = s_3$ и $\mathrm{LM} \vdash C \to A$, либо $s_2 \neq s_3$ и $s_2, s_3 \Vdash C \backslash A$. Рассмотрим два подслучая.

Случай 1.1: $s_2 = s_3$.

Тогда $\mathrm{LM} \vdash C \to A$. Проверим, что $\mathrm{LM} \vdash C \to D$:

$$\frac{C \to A \quad A \to D}{C \to D}\ (\mathrm{cut}).$$

Случай 1.2: $s_2 \neq s_3$.

Тогда $s_2, s_3 \Vdash C \backslash A$. Проверим, что $\mathrm{LM} \vdash C \backslash A \to C \backslash D$:

$$\cfrac{\cfrac{C \to C \quad A \to D}{C\,(C \backslash A) \to D}\ (\backslash \to)}{C \backslash A \to C \backslash D}\ (\to \backslash).$$

По правилу R1 из $s_2, s_3 \Vdash C \backslash A$ получаем $s_2, s_3 \Vdash C \backslash D$.

Случай 2: правило R2.

Для некоторых A, B и t_2 имеем, что $D = A \boldsymbol{\cdot} B$ и вывод $s_1, s_3 \Vdash D$ получен по правилу R2 из $s_1, t_2 \Vdash A$ и $t_2, s_3 \Vdash B$.

$$\begin{tikzcd}
s_1 \arrow[d, "C"'] \arrow[dr, "A"] & & \\
s_2 & t_2 \arrow[r, "B"] & s_3
\end{tikzcd}$$

Применив предположение индукции к $s_1, t_2 \Vdash A$, получим, что либо $s_2 = t_2$ и $\mathrm{LM} \vdash C \to A$, либо $s_2 \neq t_2$ и $s_2, t_2 \Vdash C \backslash A$. Рассмотрим два подслучая.

Случай 2.1: $s_2 = t_2$.

Тогда $\mathrm{LM} \vdash C \to A$. Проверим, что $\mathrm{LM} \vdash B \to C \backslash (A \boldsymbol{\cdot} B)$:

$$\cfrac{\cfrac{C \to A \quad B \to B}{C\,B \to A \boldsymbol{\cdot} B}\ (\to \boldsymbol{\cdot})}{B \to C \backslash (A \boldsymbol{\cdot} B)}\ (\to \backslash).$$

По правилу R1 из $t_2, s_3 \Vdash B$ получаем $t_2, s_3 \Vdash C\backslash(A\cdot B)$, т. е. $s_2, s_3 \Vdash C\backslash D$. Согласно лемме 5.3 $s_2 \neq s_3$.

Случай 2.2: $s_2 \neq t_2$.

Тогда $s_2, t_2 \Vdash C\backslash A$. По лемме 5.2 из $s_2, t_2 \Vdash C\backslash A$ и $t_2, s_3 \Vdash B$ получаем $s_2, s_3 \Vdash (C\backslash A)\cdot B$. Проверим, что $\mathrm{LM} \vdash (C\backslash A)\cdot B \to C\backslash(A\cdot B)$:

$$\cfrac{\cfrac{\cfrac{C \to C \qquad \cfrac{A \to A \quad B \to B}{A\,B \to A\cdot B}\ (\to\cdot)}{C\,(C\backslash A)\,B \to A\cdot B}\ (\backslash\to)}{(C\backslash A)\,B \to C\backslash(A\cdot B)}\ (\to\backslash)}{(C\backslash A)\cdot B \to C\backslash(A\cdot B)}\ (\cdot\to).$$

По правилу R1 получаем $s_2, s_3 \Vdash C\backslash(A\cdot B)$, т. е. $s_2, s_3 \Vdash C\backslash D$. Снова согласно лемме 5.3 $s_2 \neq s_3$.

Случай 3: правило R3.

Тогда $s_1 = r^A_\zeta(t_1)$ для некоторых $A \in \mathrm{Tp}$, $\zeta \in \mathbb{N}$ и $t_1 \in \mathrm{Tm}$. Но равенство $r^A_\zeta(t_1) = s_1 = l^C_\xi(s_2)$ невозможно, так как r^A_ζ и l^C_ξ — различные функциональные символы. Противоречие.

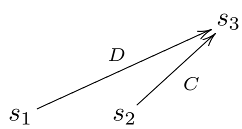
Случай 4: аксиома A1.

Тогда для некоторого $\zeta \in \mathbb{N}$ имеем $s_1 = l^D_\zeta(s_3)$. Из $l^C_\xi(s_2) = s_1$ получаем равенство $l^C_\xi(s_2) = l^D_\zeta(s_3)$, которое означает, что $C = D$, $\xi = \zeta$ и $s_2 = s_3$. Очевидно, $\mathrm{LM} \vdash C \to D$, так как $C = D$.

Случай 5: аксиома A2.

Согласно лемме 4.3 $s_1 \prec s_3$, что противоречит условию $s_3 \prec s_1$. □

Лемма 5.5. *Пусть* $s_3 = r^C_\xi(s_2)$, $s_1 \prec s_3$ *и* $s_1, s_3 \Vdash D$. *Если* $s_1 = s_2$, *то* $\mathrm{LM} \vdash C \to D$. *Если* $s_1 \neq s_2$, *то* $s_1, s_2 \Vdash D/C$.



Доказательство. Рассуждаем индукцией по длине вывода $s_1, s_3 \Vdash D$. Рассмотрим пять случаев, соответствующих тому, какое правило является последним в этом выводе.

Случай 1: правило R1.

Пусть $s_1, s_3 \Vdash D$ получено по правилу R1 из $s_1, s_3 \Vdash A$, где $\mathrm{LM} \vdash A \to D$. Применив предположение индукции к $s_1, s_3 \Vdash A$, получим, что либо $s_1 = s_2$ и $\mathrm{LM} \vdash C \to A$, либо $s_1 \neq s_2$ и $s_1, s_2 \Vdash A/C$. Рассмотрим два подслучая.

Случай 1.1: $s_1 = s_2$.

В этом случае $\mathrm{LM} \vdash C \to A$. Проверим, что $\mathrm{LM} \vdash C \to D$:

$$\frac{C \to A \quad A \to D}{C \to D}\ (\mathrm{cut}).$$

Случай 1.2: $s_1 \neq s_2$.

В этом случае $s_1, s_2 \Vdash A/C$. Проверим, что $\mathrm{LM} \vdash A/C \to D/C$:

$$\dfrac{\dfrac{C \to C \quad A \to D}{(A/C)\,C \to D}\,(/ \to)}{A/C \to D/C}\,(\to /).$$

По правилу R1 из $s_1, s_2 \Vdash A/C$ получаем $s_1, s_2 \Vdash D/C$.

Случай 2: правило R2.

В этом случае для некоторых A, B и t_2 имеем $D = A{\cdot}B$ и вывод $s_1, s_3 \Vdash D$ получен по правилу R2 из $s_1, t_2 \Vdash A$ и $t_2, s_3 \Vdash B$.

$$\begin{tikzcd} & & & s_3 \\ s_1 \arrow[r, "A"] & t_2 \arrow[urr, "B"] & s_2 \arrow[ur, "C"'] & \end{tikzcd}$$

Применив предположение индукции к $t_2, s_3 \Vdash B$, получим, что либо $t_2 = s_2$ и $\mathrm{LM} \vdash C \to B$, либо $t_2 \neq s_2$ и $t_2, s_2 \Vdash B/C$. Рассмотрим два подслучая.

Случай 2.1: $t_2 = s_2$.

В этом случае $\mathrm{LM} \vdash C \to B$. Проверим, что $\mathrm{LM} \vdash A \to (A{\cdot}B)/C$:

$$\dfrac{\dfrac{A \to A \quad C \to B}{A\,C \to A{\cdot}B}\,(\to \cdot)}{A \to (A{\cdot}B)/C}\,(\to /).$$

По правилу R1 из $s_1, t_2 \Vdash A$ получаем $s_1, t_2 \Vdash (A{\cdot}B)/C$, то есть $s_1, s_2 \Vdash D/C$. Согласно лемме 5.3, $s_1 \neq s_2$.

Случай 2.2: $t_2 \neq s_2$.

В этом случае $t_2, s_2 \Vdash B/C$. По лемме 5.2 из $s_1, t_2 \Vdash A$ и $t_2, s_2 \Vdash B/C$ получаем $s_1, s_2 \Vdash A{\cdot}(B/C)$. Проверим, что $\mathrm{LM} \vdash A{\cdot}(B/C) \to (A{\cdot}B)/C$:

$$\dfrac{\dfrac{\dfrac{C \to C \quad \dfrac{A \to A \quad B \to B}{A\,B \to A{\cdot}B}\,(\to \cdot)}{A\,(B/C)\,C \to A{\cdot}B}\,(/ \to)}{A\,(B/C) \to (A{\cdot}B)/C}\,(\to /)}{A{\cdot}(B/C) \to (A{\cdot}B)/C}\,(\cdot \to).$$

По правилу R1 получаем $s_1, s_2 \Vdash (A{\cdot}B)/C$, то есть $s_1, s_2 \Vdash D/C$. Снова, согласно лемме 5.3, $s_1 \neq s_2$.

Случай 3: правило R3.

Этот случай невозможен в силу леммы 4.3.

Случай 4: аксиома A1.

Этот случай невозможен в силу леммы 4.3.

Случай 5: аксиома A2.

Тогда для некоторого $\zeta \in \mathbb{N}$ имеем $s_3 = r^D_\zeta(s_1)$. Из $r^C_\xi(s_2) = s_3$ получаем равенство $r^C_\xi(s_2) = r^D_\zeta(s_1)$, которое означает, что $C = D$, $\xi = \zeta$ и $s_2 = s_1$. Очевидно, $\mathrm{LM} \vdash C \to D$, так как $C = D$. □

6. Доказательство основной теоремы

Лемма 6.1. *Построенная в разделе 4 алгебраическая система $\langle S, +, \cdot, 0\rangle$ является полукольцом.*

Доказательство. Очевидно, что множество S замкнуто относительно операции $+$. Проверим замкнутость относительно операции $\cdot$. Если $a \in \{0, \infty\}$ или $b \in \{0, \infty\}$, то $a \cdot b \in \{0, \infty\} \subseteq S$. Пусть $a = \langle t_1, t_2\rangle \in S_-$ и $b = \langle t_3, t_4\rangle \in S_-$. Это означает, что $t_1, t_2 \Vdash A$ и $t_3, t_4 \Vdash B$ для некоторых $A \in \mathrm{Tp}$ и $B \in \mathrm{Tp}$. Если $t_2 \neq t_3$, то $a \cdot b = \infty \in S$. Пусть $t_2 = t_3$. По лемме 5.2 из $t_1, t_2 \Vdash A$ и $t_2, t_4 \Vdash B$ получим $t_1, t_4 \Vdash A \bullet B$. Следовательно, $a \cdot b = \langle t_1, t_4\rangle \in S_- \subseteq S$.

Очевидно, что выполняются аксиомы 2, 7, 8 из определения 1.1. Аксиомы 1 и 3 проверяются легко.

Проверим аксиому 4. Если хотя бы один из элементов a, b, c есть 0, то $(a \cdot b) \cdot c = 0$ и $a \cdot (b \cdot c) = 0$. Если $a = \langle t_1, t_2\rangle \in S_-$, $b = \langle t_2, t_3\rangle \in S_-$ и $c = \langle t_3, t_4\rangle \in S_-$ для некоторых t_1, t_2, t_3, t_4, то $(a \cdot b) \cdot c = \langle t_1, t_4\rangle = a \cdot (b \cdot c)$. В остальных случаях $(a \cdot b) \cdot c = \infty$ и $a \cdot (b \cdot c) = \infty$.

Проверим аксиому 5. Если $a = 0$, то $a \cdot (b+c) = 0$ и $a \cdot b + a \cdot c = 0+0 = 0$. Если $b = 0$, то $a \cdot (b+c) = a \cdot c$ и $a \cdot b + a \cdot c = 0 + a \cdot c = a \cdot c$. Аналогично рассматривается случай $c = 0$. Если же $a \neq 0$, $b \neq 0$ и $c \neq 0$, то $a \cdot (b+c) = a \cdot \infty = \infty$ и, с другой стороны, $a \cdot b \neq 0$, $a \cdot c \neq 0$, поэтому $a \cdot b + a \cdot c = \infty$.

Аксиома 6 проверяется аналогично. □

Лемма 6.2. *Пусть* $A \in \mathrm{Tp}$. *Тогда множество*

$$I = \{\langle t_1, t_2\rangle \mid t_1, t_2 \Vdash A\} \cup \{0, \infty\}$$

является идеалом полукольца $\langle S, +, \cdot, 0\rangle$.

Доказательство. Пусть $a \in I$ и $b \in I$. Проверим, что $a + b \in I$. Если $a = 0$, то $a+b = b \in I$. Если $b = 0$, то $a+b = a \in I$. Если $a \neq 0$ и $b \neq 0$, то $a+b = \infty \in I$.

Пусть теперь $a \in I$ и $b \in S$. Проверим, что $a \cdot b \in I$. Если $a \in \{0, \infty\}$ или $b \in \{0, \infty\}$, то $a \cdot b \in \{0, \infty\} \subseteq I$. Пусть $a = \langle t_1, t_2\rangle$ и $b = \langle t_3, t_4\rangle \in S_-$. Это означает, что $t_1, t_2 \Vdash A$ и $t_3, t_4 \Vdash B$ для некоторого $B \in \mathrm{Tp}$. Если $t_2 \neq t_3$, то $a \cdot b = \infty \in I$. Пусть $t_2 = t_3$. По лемме 5.2 из $t_1, t_2 \Vdash A$ и $t_2, t_4 \Vdash B$ получим $t_1, t_4 \Vdash A \bullet B$. Проверим, что $\mathrm{LM} \vdash A \bullet B \to A$:

$$\cfrac{\cfrac{A \to A}{A\,B \to A}\,(\mathrm{M})}{A \bullet B \to A}\,(\bullet \to).$$

По правилу R1 из $t_1, t_4 \Vdash A \bullet B$ получаем $t_1, t_4 \Vdash A$. Следовательно, $a \cdot b = \langle t_1, t_4\rangle \in I$.

Аналогично доказывается, что если $a \in S$ и $b \in I$, то $a \cdot b \in I$. □

Лемма 6.3. *Для каждого* $C \in \mathrm{Tp}$ *выполняется равенство*

$$v(C) = \{\langle t_1, t_2\rangle \mid t_1, t_2 \Vdash C\} \cup \{0, \infty\}$$

и $v(C)$ *является идеалом полукольца* $\langle S, +, \cdot, 0\rangle$.

Доказательство. В силу леммы 6.2 достаточно доказать равенство. Рассуждаем индукцией по построению типа C. Рассмотрим четыре случая.

Случай 1: $C = p_i$.

Тогда равенство обеспечивается непосредственно конструкцией оценки v.

Случай 2: $C = A \bullet B$.

По предположению индукции

$$v(A) = \{\langle t_1, t_2\rangle \mid t_1, t_2 \Vdash A\} \cup \{0, \infty\},$$
$$v(B) = \{\langle t_1, t_2\rangle \mid t_1, t_2 \Vdash B\} \cup \{0, \infty\}.$$

Согласно определению $v(A \bullet B) = v(A) \cdot v(B)$. Поэтому достаточно проверить, что $v(A) \cdot v(B) = \{\langle t_1, t_2\rangle \mid t_1, t_2 \Vdash A \bullet B\} \cup \{0, \infty\}$. Докажем сначала, что

$$v(A) \cdot v(B) \subseteq \{\langle t_1, t_2\rangle \mid t_1, t_2 \Vdash A \bullet B\} \cup \{0, \infty\}. \tag{2}$$

Рассмотрим произвольный элемент левого множества, т. е. произвольную конечную сумму $\sum\limits_{k=1}^{n} a_k \cdot b_k$, где $a_k \in v(A)$ и $b_k \in v(B)$ для всех k. Если $n \geqslant 2$, то без ограничения общности можно предположить, что все слагаемые ненулевые, а тогда сумма равна ∞. Осталось рассмотреть случай, когда $n = 1$. Надо проверить, что $a_1 \cdot b_1 \in \{\langle t_1, t_2\rangle \mid t_1, t_2 \Vdash A \bullet B\} \cup \{0, \infty\}$. Если $a_1 \in \{0, \infty\}$ или $b_1 \in \{0, \infty\}$, то $a_1 \cdot b_1 \in \{0, \infty\}$. Пусть $a_1 = \langle t_1, t_2\rangle$ и $b_1 = \langle t_3, t_4\rangle$. Это означает, что $t_1, t_2 \Vdash A$ и $t_3, t_4 \Vdash B$. Если $t_2 \neq t_3$, то $a_1 \cdot b_1 = \infty$. Пусть $t_2 = t_3$ (тогда $a_1 \cdot b_1 = \langle t_1, t_4\rangle$). По лемме 5.2 из $t_1, t_2 \Vdash A$ и $t_2, t_4 \Vdash B$ получим $t_1, t_4 \Vdash A \bullet B$, что завершает доказательство соотношения (2).

Теперь докажем обратное включение:

$$\{\langle t_1, t_3\rangle \mid t_1, t_3 \Vdash A \bullet B\} \cup \{0, \infty\} \subseteq v(A) \cdot v(B). \tag{3}$$

Так как $\infty \in v(A)$ и $\infty \in v(B)$, то $\infty = \infty \cdot \infty \in v(A) \cdot v(B)$. Аналогично $0 = 0 \cdot 0 \in v(A) \cdot v(B)$. Осталось рассмотреть случай, когда $t_1, t_3 \Vdash A \bullet B$. Необходимо найти терм t_2, для которого $t_1, t_2 \Vdash A$ и $t_2, t_3 \Vdash B$. Рассмотрим бесконечное множество термов $\{r_\xi^A(t_1) \mid \xi \in \mathbb{N}\}$. Согласно лемме 4.2 лишь конечное число из этих термов удовлетворяет неравенству $r_\xi^A(t_1) \preceq t_3$. Поэтому можно выбрать такое значение ξ, что $t_3 \prec r_\xi^A(t_1)$. Положим $t_2 = r_\xi^A(t_1)$. По правилу R3 из $t_1, t_3 \Vdash A \bullet B$ получаем $t_2, t_3 \Vdash B$. По аксиоме A1 получаем $t_1, t_2 \Vdash A$. Мы показали, что $\langle t_1, t_3\rangle = \langle t_1, t_2\rangle \cdot \langle t_2, t_3\rangle \in v(A) \cdot v(B)$, что завершает доказательство соотношения (3).

Случай 3: $C = A \backslash B$.

По предположению индукции

$$v(A) = \{\langle t_1, t_2\rangle \mid t_1, t_2 \Vdash A\} \cup \{0, \infty\},$$
$$v(B) = \{\langle t_1, t_2\rangle \mid t_1, t_2 \Vdash B\} \cup \{0, \infty\}.$$

Согласно определению $v(A \backslash B) = v(A) \backslash v(B)$. Поэтому достаточно проверить, что $v(A) \backslash v(B) = \{\langle t_1, t_2\rangle \mid t_1, t_2 \Vdash A \backslash B\} \cup \{0, \infty\}$. Докажем сначала, что

$$v(A) \backslash v(B) \subseteq \{\langle t_1, t_2\rangle \mid t_1, t_2 \Vdash A \backslash B\} \cup \{0, \infty\}. \tag{4}$$

Для элементов 0 и ∞ принадлежность правой части очевидна. Рассмотрим произвольный элемент $\langle s_2, s_3 \rangle \in S_-$, принадлежащий множеству $v(A)\backslash v(B)$. Согласно определению 1.9 $v(A) \cdot \langle s_2, s_3 \rangle \subseteq v(B)$. Выберем такое значение $\xi \in \mathbb{N}$, что $s_3 \prec l_\xi^A(s_2)$ (это возможно согласно лемме 4.2). Обозначим $s_1 = l_\xi^A(s_2)$. По лемме 5.4 $s_2, s_3 \Vdash A\backslash B$ (здесь мы использовали неравенство $s_2 \neq s_3$, которое можно получить из леммы 5.3, поскольку $\langle s_2, s_3 \rangle \in S_-$). Доказательство соотношения (4) завершено.

Теперь докажем обратное включение:

$$\{\langle t_1, t_2 \rangle \mid t_1, t_2 \Vdash A\backslash B\} \cup \{0, \infty\} \subseteq v(A)\backslash v(B). \tag{5}$$

Очевидно, что $v(A) \cdot 0 = \{0\} \subseteq v(B)$ и, следовательно, $0 \in v(A)\backslash v(B)$. Очевидно, что $v(A) \cdot \infty = \{0, \infty\} \subseteq v(B)$, следовательно, $\infty \in v(A)\backslash v(B)$. Наконец, пусть $s_2, s_3 \Vdash A\backslash B$. Согласно определению 1.9, для того чтобы доказать $\langle s_2, s_3 \rangle \in v(A)\backslash v(B)$, достаточно установить, что $a \cdot \langle s_2, s_3 \rangle \in v(B)$ для всех $a \in v(A)$.

Пусть $a \in v(A)$. Если $a = 0$, $a = \infty$ или $a = \langle s_1, t_2 \rangle$, где $t_2 \neq s_2$, то, очевидно, $a \cdot \langle s_2, s_3 \rangle \in \{0, \infty\} \subseteq v(B)$. Осталось рассмотреть случай, когда $a = \langle s_1, s_2 \rangle$ для некоторого терма s_1. Тогда $s_1, s_2 \Vdash A$. По лемме 5.2 из $s_1, s_2 \Vdash A$ и $s_2, s_3 \Vdash A\backslash B$ получаем $s_1, s_3 \Vdash A \bullet (A\backslash B)$. Проверим, что $\mathrm{LM} \vdash A \bullet (A\backslash B) \to B$:

$$\dfrac{\dfrac{A \to A \quad B \to B}{A\,(A\backslash B) \to B}\,(\backslash \to)}{A \bullet (A\backslash B) \to B}\,(\bullet \to).$$

По правилу R1 получаем $s_1, s_3 \Vdash B$. Следовательно, $a \cdot \langle s_2, s_3 \rangle = \langle s_1, s_3 \rangle \in v(B)$, что завершает доказательство соотношения (5).

Случай 4: $C = B/A$.

Этот случай аналогичен предыдущему. Вместо леммы 5.4 используем лемму 5.5, а вместо $\mathrm{LM} \vdash A \bullet (A\backslash B) \to B$ используем $\mathrm{LM} \vdash (B/A) \bullet A \to B$:

$$\dfrac{\dfrac{A \to A \quad B \to B}{(B/A)\,A \to B}\,(/ \to)}{(B/A) \bullet A \to B}\,(\bullet \to).$$

□

Теорема 6.4. *Существует модель на полукольце, относительно которой исчисление* LM *полно* (*т. е. каждая истинная в этой модели секвенция выводима в исчислении* LM).

Доказательство. Рассмотрим построенную в разделе 4 модель с оценкой v над полукольцом $\langle S, +, \cdot, 0 \rangle$. Пусть секвенция $A_1 \ldots A_n \to B$ истинна в этой модели. В силу определений 3.3 и 3.1, это равносильно истинности секвенции $A \to B$, где $A = A_1 \bullet \ldots \bullet A_n$. Осталось доказать, что $\mathrm{LM} \vdash A \to B$ (тогда выводимость исходной секвенции $A_1 \ldots A_n \to B$ получится из $\mathrm{LM} \vdash A_1 \ldots A_n \to A$ и $\mathrm{LM} \vdash A \to B$ по правилу сечения).

Положим $t_1 = l_0^A(o)$ и $t_2 = o$. По аксиоме A1 получаем $t_1, t_2 \Vdash A$. Согласно лемме 6.3 это означает, что $\langle t_1, t_2 \rangle \in v(A)$. Так как секвенция $A \to B$ истинна в рассматриваемой модели, то $\langle t_1, t_2 \rangle \in v(B)$. Согласно лемме 6.3 $t_1, t_2 \Vdash B$. Применим лемму 5.4 к выводу $t_1, t_2 \Vdash B$, положив $s_1 = t_1$, $s_2 = t_2$, $s_3 = t_2$, $C = A$, $D = B$. Получаем $\mathrm{LM} \vdash A \to B$. □

Следствие 6.5. *Исчисление* LM *полно относительно класса всех моделей на полукольцах (т. е. каждая секвенция, истинная на всех полукольцах при всех оценках, выводима в исчислении* LM*).*

Следствие 6.6. *Рассмотрим множество секвенций вида $A_1 \ldots A_n \to B$, где $B \in \mathrm{Tp}$ и $A_i \in \mathrm{Tp}$ для всех i. Выделим среди них множество тех секвенций, которые истинны во всех моделях на полукольцах. Это множество разрешимо.*

Доказательство. Утверждение вытекает из следствий 6.5 и 2.4. □

Следствие 6.7. *Рассмотрим множество равенств вида $A = B$, где $A \in \mathrm{Tp}$ и $B \in \mathrm{Tp}$. Выделим среди них множество тех равенств, которые истинны во всех моделях на полукольцах. Это множество разрешимо.*

Доказательство. Пусть $A \in \mathrm{Tp}$ и $B \in \mathrm{Tp}$. Равенство $A = B$ истинно во всех моделях на полукольцах тогда и только тогда, когда секвенции $A \to B$ и $B \to A$ истинны во всех моделях на полукольцах. □

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] Фукс Л. Частично упорядоченные алгебраические системы. — М.: Мир, 1965.

[5] Buszkowski W. Completeness results for Lambek syntactic calculus // Z. Math. Logik Grundlag. Math. — 1986. — Vol. 32. — P. 13—28.

[6] Buszkowski W. Type logics in grammar // Trends in Logic: 50 Years of Studia Logica / V. F. Hendricks, J. Malinowski, eds. — Dordrecht: Kluwer Academic, 2003. — P. 337—382.

[7] Van Benthem J. Language in Action. Categories, Lambdas and Dynamic Logic. — Amsterdam: North-Holland, 1991. — (Stud. Logic Foundations Math.; Vol. 130).