

Московский государственный университет им. М. В. Ломоносова
Механико-математический факультет

УДК 519.766

С. Л. Кузнецов
Исчисление Ламбека с операцией обращения

Автор _____ С. Л. Кузнецов

Москва, 2012

Депонированная научная работа

УДК 519.766

Исчисление Ламбека с операцией обращения / Кузнецов С. Л.; МГУ. — М., 2012. — 17 с. — Библиогр.: 9 назв. — Рус. — Деп. в ВИНТИ

Содержание

1	Исчисление L и его фрагменты	3
2	Категориальные грамматики Ламбека	4
3	L -модели для исчисления L	6
4	Исчисление L^R	7
5	Нормальная форма типов исчисления L^R	8
6	L -полнота исчисления L^R (доказательство)	10
7	Исчисление L^R : грамматики и сложность	16

1 Исчисление L и его фрагменты

Определим *исчисление Ламбека* L , впервые введённое в [5]. Счётное множество $\text{Pr} \Leftarrow \{p_1, p_2, p_3, \dots\}$ называется множеством *примитивных типов* (здесь и далее значок « \Leftarrow » означает «равно по определению»). *Типы* исчисления Ламбека образуются из примитивных с помощью двуместных связок \backslash (левое деление), $/$ (правое деление) и \cdot (умножение); их множество обозначается Tr . Формально множество Tr определяется индуктивно как наименьшее в смысле включения множество, удовлетворяющее следующим двум условиям:

1. $\text{Pr} \subset \text{Tr}$;
2. если $A, B \in \text{Tr}$, то $(A \backslash B), (B / A), (A \cdot B) \in \text{Tr}$.

Типы обозначаются большими латинскими буквами, их конечные (возможно пустые) последовательности — заглавными греческими; пустая последовательность обозначается буквой Λ . Выводимыми объектами в исчислении Ламбека являются *секвенции* — выражения вида $\Pi \rightarrow C$; Π называется *антецедентом*, а C — *сукцедентом* секвенции.

Исчисление L задаётся аксиомами вида $p_i \rightarrow p_i$ (обозначение: (акс.)) и правилами вывода

$$\begin{array}{l} \frac{A \Pi \rightarrow B}{\Pi \rightarrow A \backslash B} (\rightarrow \backslash), \text{ где } \Pi \neq \Lambda; \\ \frac{\Pi A \rightarrow B}{\Pi \rightarrow B / A} (\rightarrow /), \text{ где } \Pi \neq \Lambda; \\ \frac{\Gamma \rightarrow A \quad \Delta \rightarrow B}{\Gamma \Delta \rightarrow A \cdot B} (\rightarrow \cdot); \\ \frac{\Pi \rightarrow A \quad \Gamma B \Delta \rightarrow C}{\Gamma \Pi (A \backslash B) \Delta \rightarrow C} (\backslash \rightarrow); \\ \frac{\Pi \rightarrow A \quad \Gamma B \Delta \rightarrow C}{\Gamma (B / A) \Pi \Delta \rightarrow C} (/ \rightarrow); \\ \frac{\Gamma A B \Delta \rightarrow C}{\Gamma (A \cdot B) \Delta \rightarrow C} (\cdot \rightarrow); \\ \frac{\Pi \rightarrow A \quad \Gamma A \Delta \rightarrow C}{\Gamma \Pi \Delta \rightarrow C} (\text{cut}). \end{array}$$

Легко видеть, что секвенции с пустыми антецедентами в L выводиться не могут.

Правило (cut), называемое *правилом сечения*, устранимо:

Теорема 1 (И. Ламбек, 1958). *Если секвенция выводима в L , то она выводима без применения правила (cut).* [5]

Обозначим через $\text{Tr}(\backslash)$ множество типов, не содержащих ни \cdot , ни $/$. Исчисление, заданное аксиомами (акс.) и правилами $(\backslash \rightarrow)$ и $(\rightarrow \backslash)$, обозначается $L(\backslash)$. Вместо \backslash

можно рассматривать другое деление $/$, при этом получится полностью симметричная теория; мы будем везде рассматривать левое деление \backslash . Аналогичным образом определяются исчисления $L(\cdot, \backslash)$ и $L(\backslash, /)$.

Метапеременная \mathcal{L} будет обозначать один из вариантов исчисления Ламбека: L , $L(\backslash)$, $L(\cdot, \backslash)$, $L(\backslash, /)$, а также исчисление L^R , которое мы определим позже. обозначать множество типов, соответствующее исчислению \mathcal{L} (Tr для L и L^* , $\text{Tr}(\backslash)$ для $L(\backslash)$ и т. д.).

Определение. Исчисление \mathcal{L}_1 называется *фрагментом* исчисления \mathcal{L}_2 (соответственно, \mathcal{L}_2 называется *расширением* \mathcal{L}_1), если $\text{Tr}_{\mathcal{L}_1} \subseteq \text{Tr}_{\mathcal{L}_2}$ и всякая секвенция, выводимая в \mathcal{L}_1 , выводима в \mathcal{L}_2 . Фрагмент (соответственно, расширение) называется *консервативным*, если, кроме того, для секвенций, составленных исключительно из типов из множества $\text{Tr}_{\mathcal{L}_1}$, выводимость в \mathcal{L}_1 равносильна выводимости в \mathcal{L}_2 .

Из теоремы 1 следует, например, что исчисление $L(\backslash)$ является консервативным фрагментом исчисления L .

2 Категориальные грамматики Ламбека

Алфавитом называется произвольное непустое конечное множество. Множество всех конечных последовательностей (включая пустую), составленных из элементов алфавита Σ (*слов над алфавитом Σ*) обозначается Σ^* . Пустое слово обозначается через ε . Множество всех слов, кроме пустого, обозначается Σ^+ . Подмножества Σ^* называются *формальными языками* (или просто *языками*) над алфавитом Σ .

Для конечного описания формальных языков (как правило бесконечных как множества) используются формальные грамматики различных видов. Исчисление Ламбека и его варианты служат основой для *категориальных грамматик Ламбека*.

Определение. *Грамматикой, основанной на исчислении \mathcal{L} , (\mathcal{L} -грамматикой)* называется тройка $\mathcal{G} = \langle \Sigma, H, \triangleright \rangle$, где Σ — некоторое непустое конечное множество (алфавит), $H \in \text{Tr}_{\mathcal{L}}$, а $\triangleright \subset \text{Tr}_{\mathcal{L}} \times \Sigma$ — произвольное конечное бинарное соответствие. Язык, порождаемый грамматикой \mathcal{G} , есть $\mathcal{Y}(\mathcal{G}) \Leftarrow \{a_1 \dots a_k \in \Sigma^* \mid \exists B_1, \dots, B_k: B_i \triangleright a_i \text{ и } \mathcal{L} \vdash B_1 \dots B_k \rightarrow H\}$. Такие языки называются *\mathcal{L} -языками*.

Предложение 1. *Если исчисление \mathcal{L} является консервативным фрагментом исчисления \mathcal{L}' , то любой \mathcal{L} -язык является \mathcal{L}' -языком.*

Доказательство. Всякую \mathcal{L} -грамматику можно рассмотреть как \mathcal{L}' -грамматику. Из-за консервативности язык при этом не изменится. \square

И наоборот, если в \mathcal{L}' -грамматике встречаются только типы из $\text{Tr}_{\mathcal{L}}$, то эту грамматику можно рассмотреть как \mathcal{L} -грамматику, задающую тот же язык.

Наряду с категориальными грамматиками, основанными на исчислении Ламбека и его вариантах, широко известно также семейство формализмов, называемое *иерархией Хомского* [4]. Мы будем рассматривать грамматики Хомского типа 2, называемые также контекстно-свободными грамматиками.

Определение. *Контекстно-свободной грамматикой* называется четвёрка

$$G = \langle N, \Sigma, P, S \rangle,$$

где N и Σ — непересекающиеся алфавиты (элементы N и Σ называются, соответственно, *нетерминальными* и *терминальными* символами), P — конечное подмножество декартова произведения $N \times (N \cup \Sigma)^*$ и $S \in N$. Пары $\langle A, \alpha \rangle \in P$ называются *правилами* (*продукциями*) грамматики G и записываются так: $A \rightarrow \alpha$. Пусть $\varphi, \psi \in (N \cup \Sigma)^*$. Слово ψ *непосредственно выводимо* из φ в грамматике G (обозначение: $\varphi \Rightarrow_G \psi$), если найдутся такие $\alpha, \gamma, \delta \in (N \cup \Sigma)^*$ и $A \in N$, что $\varphi = \gamma A \delta$, $\psi = \gamma \alpha \delta$ и $(A \rightarrow \alpha) \in P$. Бинарное отношение \Rightarrow_G^* есть рефлексивно-транзитивное замыкание отношения \Rightarrow_G . Если $\varphi \Rightarrow_G^* \psi$, говорят, что ψ *выводимо* из φ в грамматике G . Язык, порождаемый грамматикой G , есть множество всех слов, составленных только из нетерминальных символов и выводимых в грамматике G из однобуквенного слова S : $\mathcal{Y}(G) \Leftarrow \{w \in \Sigma^* \mid S \Rightarrow_G^* w\}$. Такие языки называются *контекстно-свободными*.

Интересен вопрос о взаимном включении классов языков, задаваемых, с одной стороны, контекстно-свободными грамматиками, и, с другой стороны, \mathcal{L} -грамматиками для различных исчислений \mathcal{L} . Для $\mathcal{L} = \text{L}$ и $\mathcal{L} = \text{L}(\backslash)$ ответ на этот вопрос дают следующие теоремы:

Теорема 2 (Х. Гайфман, 1960; В. Бушковский, 1985). *Всякий контекстно-свободный язык, не содержащий пустого слова, является $\text{L}(\backslash)$ -языком.* [1][3]

Теорема 3 (М. Р. Пентус, 1993). *Всякий L -язык контекстно-свободен и не содержит пустого слова.* [8]

В силу предложения 1 получаем, что классы L -языков, $\text{L}(\backslash)$ -языков и контекстно-свободных языков без пустого слова совпадают.

3 L-модели для исчисления L

В этом и следующих трёх разделах алфавит Σ считается произвольным непустым конечным *или счётным* множеством. Три связки исчисления L соответствуют трём операциям над языками без пустого слова ($M, N \subseteq \Sigma^+$): $M \cdot N \Leftrightarrow \{uv \mid u \in M, v \in N\}$, $M \setminus N \Leftrightarrow \{u \in \Sigma^+ \mid (\forall v \in M) vu \in N\}$, $N \setminus M \Leftrightarrow \{u \in \Sigma^+ \mid (\forall v \in M) uv \in N\}$.

Определение. L-моделью называется пара $\mathcal{M} = \langle \Sigma, w \rangle$, где Σ — алфавит, а w — отображение типов исчисления Ламбека в формальные языки над Σ , не содержащие пустого слова, причём для любых $A, B \in \text{Tr}$ выполняются соотношения $w(A \cdot B) = w(A) \cdot w(B)$, $w(A \setminus B) = w(A) \setminus w(B)$ и $w(B / A) = w(B) / w(A)$. Отображение w называется *интерпретацией* типов языками над Σ .

Отображение w определяется произвольным образом на примитивных типах, а на остальные типы распространяется единственным образом.

Поскольку множество Σ^+ с операцией приписывания слов является свободной полугруппой, порождённой алфавитом Σ , L-модели также называются *моделями на подмножествах свободных полугрупп*.

Определение. Секвенция вида $F \rightarrow G$ считается *истинной* в модели $\mathcal{M} = \langle \Sigma, w \rangle$ (обозначение: $\mathcal{M} \models F \rightarrow G$), если $w(F) \subseteq w(G)$.

Исчисление L корректно и полно относительно класса L-моделей (далее мы кратко будем называть это свойство «L-полнотой»):

Теорема 4 (М. Р. Пентус, 1995). *Секвенция $F \rightarrow G$ выводима в L тогда и только тогда, когда она истинна во всех L-моделях.*

Эта теорема доказана в [9]; доказательство для частного случая — исчисления Ламбека без операции умножения — гораздо проще и приведено в [2].

Заметим, что, хотя теорема 4 сформулирована только для секвенций вида $F \rightarrow G$ (с одним типом в антецеденте), её легко обобщить на случай секвенции произвольного вида, потому что секвенция $F_1 F_2 \dots F_n \rightarrow G$ выводима в исчислении Ламбека тогда и только тогда, когда выводима секвенция $F_1 \cdot F_2 \cdot \dots \cdot F_n \rightarrow G$ (в силу ассоциативности операции умножения расстановка скобок в левой части не имеет значения) Определение интерпретации также естественно распространяется на последовательности типов: $\bar{w}(F_1 F_2 \dots F_n) \Leftrightarrow w(F_1) \cdot w(F_2) \cdot \dots \cdot w(F_n)$, и окончательно получаем, что $L \vdash \Pi \rightarrow G$, если и только если для любой модели $\mathcal{M} = \langle \Sigma, w \rangle$ имеем $\mathcal{M} \models \Pi \rightarrow G$, т. е. $\bar{w}(\Pi) \subseteq w(G)$. В силу этого соображения достаточно рассматривать только секвенции вида $F \rightarrow G$.

4 Исчисление L^R

Рассмотрим ещё одну операцию над формальными языками — *обращение* языка. Для $u = a_1 a_2 \dots a_n$ ($a_1, \dots, a_n \in \Sigma$, $n \geq 1$) положим $u^R \Leftarrow a_n \dots a_2 a_1$; для $M \subseteq \Sigma^+$ положим $M^R \Leftarrow \{u^R \mid u \in M\}$. Добавим к языку исчисления Ламбека новую одноместную связку R (записывается в постфиксной форме: A^R); новое множество типов обозначим через Tr^R . Если $\Gamma = A_1 A_2 \dots A_n$, положим $\Gamma^R \Leftarrow A_n^R \dots A_2^R A_1^R$.

Понятие L -модели обобщается естественным образом — добавлением условия $w(A^R) = w(A)^R$ на интерпретацию типов (уже из расширенного множества Tr^R).

Исчисление L^R получается из исчисления L добавлением трёх новых правил для новой связки R :

$$\frac{\Gamma \rightarrow C}{\Gamma^R \rightarrow C^R} \text{ (}^R \rightarrow \text{)} \quad \frac{\Gamma A \Delta \rightarrow C}{\Gamma A^{RR} \Delta \rightarrow C} \text{ (}^{RR} \rightarrow \text{)} \quad \frac{\Gamma \rightarrow C}{\Gamma \rightarrow C^{RR}} \text{ (} \rightarrow \text{ }^{RR} \text{)}$$

Легко видеть, что исчисление L^R корректно относительно L -моделей (любая L^R -выводимая секвенция истинна во всех моделях).

Предложение 2. *Исчисление L^R является консервативным расширением исчисления L .*

Доказательство. Очевидно, что L есть фрагмент L^R . Докажем консервативность. Пусть секвенция $F \rightarrow G$ выводима в L^R , причём $F, G \in \text{Tr}$. Тогда эта секвенция истинна во всех L -моделях и, в силу теоремы 4 выводима в L .

Случай секвенций со многими типами в антецеденте сводится к уже рассмотренному (см. окончание предыдущего раздела). \square

Заметим, что, поскольку правило сечения в приведённом выше исчислении неустраимо (например, выводимая (см. лемму 3) секвенция $(p_1 \cdot p_2)^R \rightarrow p_2^R \cdot p_1^R$ не имеет вывода без применений правила сечения), консервативность L^R над L нетривиальна. Вопрос о построении исчисления без правила сечения, эквивалентного исчислению L^R , открыт.

L -полнота фрагмента исчисления L^R без умножения доказана в [7] с помощью модифицированного метода Бушковского [2]; там же доказана L -полнота вырожденного фрагмента, в котором из связок оставлены только умножение и обращение. Мы докажем L -полноту всего исчисления L^R :

Теорема 5. *Секвенция $F \rightarrow G$ ($F, G \in \text{Tr}^R$) выводима в L^R тогда и только тогда, когда она истинна во всех L -моделях.*

5 Нормальная форма типов исчисления \mathbb{L}^R

Два типа $A, B \in \text{Tr}^R$ называются *эквивалентными* в исчислении \mathbb{L}^R (обозначение: $A \leftrightarrow_{\mathbb{L}^R} B$), если $\mathbb{L}^R \vdash A \rightarrow B$ и $\mathbb{L}^R \vdash B \rightarrow A$. Отношение $\leftrightarrow_{\mathbb{L}^R}$ является отношением эквивалентности, а также конгруэнцией относительно всех связок.

Лемма 3. В \mathbb{L}^R имеют место следующие эквивалентности (A и B — произвольные типы из Tr^R):

1. $A^{\text{RR}} \leftrightarrow A$;
2. $(A \cdot B)^R \leftrightarrow B^R \cdot A^R$;
3. $(A \setminus B)^R \leftrightarrow B^R / A^R$;
4. $(B / A)^R \leftrightarrow A^R \setminus B^R$.

Доказательство. Первая эквивалентность очевидна из правил $(^{\text{RR}} \rightarrow)$ и $(\rightarrow^{\text{RR}})$. Вторая и третья эквивалентности устанавливаются следующими выводами:

$$\frac{A \rightarrow A^{\text{RR}} \quad \frac{B \rightarrow B^{\text{RR}} \quad \frac{A^R \rightarrow B^R \quad \frac{B^R A^R \rightarrow B^R \cdot A^R}{A^{\text{RR}} B^{\text{RR}} \rightarrow (B^R \cdot A^R)^R}}{A^{\text{RR}} B \rightarrow (B^R \cdot A^R)^R}}{AB \rightarrow (B^R \cdot A^R)^R} \quad \frac{(B^R \cdot A^R)^{\text{RR}} \rightarrow B^R \cdot A^R}{(A \cdot B)^R \rightarrow (B^R \cdot A^R)^{\text{RR}}}}{(A \cdot B)^R \rightarrow B^R \cdot A^R}$$

$$\frac{\frac{A \rightarrow A \quad B \rightarrow B}{AB \rightarrow A \cdot B} \quad \frac{B^R A^R \rightarrow (A \cdot B)^R}{B^R \cdot A^R \rightarrow (A \cdot B)^R}}{\frac{A \rightarrow A \quad B \rightarrow B}{A(A \setminus B) \rightarrow B} \quad \frac{(A \setminus B)^R A^R \rightarrow B^R}{(A \setminus B)^R \rightarrow B^R / A^R}}$$

$$\frac{
\frac{
\frac{
\frac{
A^R \rightarrow A^R \quad B^R \rightarrow B^R}{(B^R / A^R) A^R \rightarrow B^R}
}{A^{RR} (B^R / A^R)^R \rightarrow B^{RR}} \quad B^{RR} \rightarrow B
}{A^{RR} (B^R / A^R)^R \rightarrow B}
}{A \rightarrow A^{RR}}
\frac{
\frac{
A (B^R / A^R)^R \rightarrow B}{(B^R / A^R)^R \rightarrow A \setminus B}
}{(B^R / A^R)^{RR} \rightarrow (A \setminus B)^R}
}{B^R / A^R \rightarrow (B^R / A^R)^{RR}}
\frac{
}{B^R / A^R \rightarrow (A \setminus B)^R}$$

Четвёртая эквивалентность симметрична третьей. □

Определение. Для произвольного типа $A \in \text{Tr}^R$ определим тип $tr(A)$ индуктивно по числу связей в A :

1. $tr(p_i) \Leftarrow p_i$;
2. $tr(p_i^R) \Leftarrow p_i^R$;
3. $tr(A \cdot B) \Leftarrow tr(A) \cdot tr(B)$;
4. $tr(A \setminus B) \Leftarrow tr(A) \setminus tr(B)$;
5. $tr(B / A) \Leftarrow tr(B) / tr(A)$;
6. $tr((A \cdot B)^R) \Leftarrow tr(B^R) \cdot tr(A^R)$;
7. $tr((A \setminus B)^R) \Leftarrow tr(B^R) / tr(A^R)$;
8. $tr((B / A)^R) \Leftarrow tr(A^R) \setminus tr(B^R)$;
9. $tr(A^{RR}) \Leftarrow tr(A)$.

Следующее утверждение доказывается индукцией по количеству связей в типе A ; на шаге индукции применяется лемма 3:

Предложение 4. *Всякий тип $A \in \text{Tr}^R$ эквивалентен в исчислении L^R типу $tr(A)$.*

Будем называть $tr(A)$ *нормальной формой* типа A . В нормальной форме связка R может появляться только непосредственно у примитивных типов.

6 L-полнота исчисления L^R (доказательство)

Докажем теорему 5 от противного. Пусть $L^R \not\vdash F_0 \rightarrow G_0$. Необходимо построить *контр-модель* для секвенции $F_0 \rightarrow G_0$, т. е. модель, в которой эта секвенция ложна.

Пусть $\text{Pr}' \Leftarrow \text{Pr} \cup \{p^R \mid p \in \text{Pr}\}$ и пусть L' есть исчисление Ламбека с Pr' вместо Pr в качестве множества примитивных типов. Здесь R не является связкой, и p^R рассматривается как новый, независимый от p примитивный тип. Очевидно, что если $L' \vdash F \rightarrow G$, то $L^R \vdash F \rightarrow G$.

Положим $F \Leftarrow \text{tr}(F_0)$, $G \Leftarrow \text{tr}(G_0)$. Тогда $L^R \not\vdash F \rightarrow G$, и, следовательно, $L' \not\vdash F \rightarrow G$. Исчисление L' по сути совпадает с L , поэтому в силу теоремы 4 существует структура $\mathcal{M} = \langle \Sigma, w \rangle$ такая, что $w(F) \not\subseteq w(G)$. В \mathcal{M} секвенция $F \rightarrow G$ ложна, однако \mathcal{M} не является моделью в смысле расширенной сигнатуры: некоторые из условий $w(p_i^R) = w(p_i)^R$ могут не выполняться.

Обозначим через Φ множество всех подтипов секвенции $F \rightarrow G$ (включая сами F и G). Конструкция \mathcal{M} такова (см. [9]), что $w(A) \neq \emptyset$ для любого $A \in \Phi$. Других особых свойств модели \mathcal{M} нам не потребуется.

Определим счётчик $f(A)$, $A \in \Phi$, индукцией по построению типа A : $f(p_i) \Leftarrow 1$, $f(p_i^R) \Leftarrow 1$, $f(A \cdot B) \Leftarrow f(A) + f(B) + 10$, $f(A \setminus B) \Leftarrow f(B)$, $f(B / A) \Leftarrow f(B)$. Пусть $K \Leftarrow \max\{f(A) \mid A \in \Phi\}$ и $N \Leftarrow 2K + 25$ (N выбирается нечётным, бóльшим K и достаточно бóльшим само по себе).

Положим $\Sigma_1 \Leftarrow \Sigma \times \{1, \dots, N\}$. Пару $\langle a, j \rangle \in \Sigma_1$ будем обозначать $a^{(j)}$. Элементы Σ и Σ_1 условимся называть *буквами* и *символами* соответственно. Символ будем называть *чётным* или *нечётным* в зависимости от чётности его верхнего индекса.

Рассмотрим гомоморфизм $h: \Sigma^+ \rightarrow \Sigma_1^+$, определяемый следующим образом: $h(a) \Leftarrow a^{(1)}a^{(2)} \dots a^{(N)}$ ($a \in \Sigma$), $h(a_1 \dots a_n) \Leftarrow h(a_1) \dots h(a_n)$. Положим $P \Leftarrow h(\Sigma^+) = \{a_1^{(1)} \dots a_1^{(N)} \dots a_n^{(1)} \dots a_n^{(N)} \mid n \geq 1, a_i \in \Sigma\}$. Отображение h является взаимно-однозначным соответствием между Σ^+ и P .

Лемма 5. *Для любых $M, N \subseteq \Sigma^+$ имеют место соотношения:*

1. $h(M \cdot N) = h(M) \cdot h(N)$;
2. если $M \neq \emptyset$, то $h(M \setminus N) = h(M) \setminus h(N)$ и $h(N / M) = h(N) / h(M)$.

Доказательство.

1. По определению гомоморфизма.

2. $\boxed{\subseteq}$ Пусть $u \in h(M \setminus N)$. Тогда $u = h(u')$ для некоторого $u' \in M \setminus N$. Для всех $v' \in M$ имеем $v'u' \in N$. Возьмём произвольное $v \in h(M)$, $v = h(v')$ для некоторого $v' \in M$. Поскольку $u' \in M \setminus N$, $v'u' \in N$, следовательно, $vu = h(v')h(u') = h(v'u') \in h(N)$. Значит, $u \in h(M) \setminus h(N)$.

$\boxed{\supseteq}$ Пусть $u \in h(M) \setminus h(N)$. Сначала покажем, что $u \in P$. Предположим противное: $u \notin P$. Возьмём $v' \in M$ (множество M непусто по условию). Поскольку $v = h(v') \in P$, $vu \notin P$. С другой стороны, $vu \in h(N) \subseteq P$, что приводит нас к противоречию.

Поскольку $u \in P$, $u = h(u')$ для некоторого $u' \in \Sigma^+$. Для произвольного $v' \in M$ и $v = h(v')$ имеем $h(v'u') = vu \in h(N)$, откуда $v'u' \in N$. Следовательно, $u' \in M \setminus N$. Значит, $u = h(u') \in h(M \setminus N)$.

Случай / рассматривается аналогичным образом.

□

Построим новую модель $\mathcal{M}_1 = \langle \Sigma_1, w_1 \rangle$, где $w_1(z) \Leftrightarrow h(w(z))$ ($z \in \text{Pr}'$). В силу леммы 5 $w_1(A) = h(w(A))$ для всех $A \in \Phi$, поэтому $w_1(F) = h(w(F)) \not\subseteq h(w(G)) = w_1(G)$ (иначе говоря, \mathcal{M}_1 , как и \mathcal{M} является контрмоделью для секвенции $F \rightarrow G$ в сигнатуре без связки R).

Введём в рассмотрение несколько дополнительных подмножеств Σ_1^+ . Через $\text{Subw}(M)$ обозначим множество всех непустых подслов слов из M , т.е. $\text{Subw}(M) \Leftrightarrow \{u \in \Sigma_1^+ \mid (\exists v_1, v_2 \in \Sigma^*) v_1 u v_2 \in M\}$. Положим

$$T_1 \Leftrightarrow \{u \in \Sigma_1^+ \mid u \notin \text{Subw}(P \cup P^{\text{R}})\};$$

$$T_2 \Leftrightarrow \{u \in \text{Subw}(P \cup P^{\text{R}}) \mid \text{первый или последний символ слова } u \text{ чётен}\};$$

$$E \Leftrightarrow \{u \in \text{Subw}(P \cup P^{\text{R}}) - (P \cup P^{\text{R}}) \mid \text{первый и последний символы слова } u \text{ нечётны}\}.$$

Множества Σ^+ разбито на пять непересекающихся подмножеств P , P^{R} , T_1 , T_2 и E . Например, $a^{(1)}b^{(10)}a^{(2)} \in T_1$, $a^{(N)}b^{(1)} \dots b^{(N-1)} \in T_2$, $a^{(7)}a^{(6)}a^{(5)} \in E$ ($a, b \in \Sigma$).

Положим $T \Leftrightarrow T_1 \cup T_2$, $T_i(k) \Leftrightarrow \{u \in T_i \mid |u| \geq k\}$ ($i = 1, 2$, через $|u|$ обозначена длина слова u), $T(k) \Leftrightarrow T_1(k) \cup T_2(k) = \{u \in T \mid |u| \geq k\}$.

Заметим, что если первый или последний символы слова u чётен, то это слово лежит в T независимо от того, лежит ли оно в $\text{Subw}(P \cup P^{\text{R}})$.

Буква k (возможно, с нижними индексами) далее будет обозначать натуральное число от 1 до K . Для всех таких k имеем $T(k) \supseteq T(K)$.

Лемма 6. *Рассматриваемые множества обладают следующими свойствами:*

1. $P \cdot P \subseteq P, P^{\mathbb{R}} \cdot P^{\mathbb{R}} \subseteq P^{\mathbb{R}};$
2. $T^{\mathbb{R}} = T, T(k)^{\mathbb{R}} = T(k);$
3. $P \cdot P^{\mathbb{R}} \subseteq T(K), P^{\mathbb{R}} \cdot P \subseteq T(K);$
4. $P \cdot T \subseteq T(K), T \cdot P \subseteq T(K);$
5. $P^{\mathbb{R}} \cdot T \subseteq T(K), T \cdot P^{\mathbb{R}} \subseteq T(K);$
6. $T \cdot T \subseteq T;$

Доказательство.

1. Очевидно.
2. Непосредственно следует из определения.
3. Любой элемент $P \cdot P^{\mathbb{R}}$ или $P^{\mathbb{R}} \cdot P$ не принадлежит множеству $\text{Subw}(P \cup P^{\mathbb{R}})$ и имеет длину хотя бы $2N > K$. Следовательно, он принадлежит $T_1(K) \subseteq T(K)$.
4. Пусть $u \in P$ и $v \in T$. Если $v \in T_1$, то uv также лежит в T_1 . Пусть $v \in T_2$. Если последний символ v чётен, то $uv \in T$. В противном случае чётен первый символ v , поэтому $uv \notin \text{Subw}(P \cup P^{\mathbb{R}})$, следовательно, $uv \in T_1 \subseteq T$. Поскольку $|uv| > |u| \geq N > K$, получаем, что $uv \in T(K)$.

Утверждение $T \cdot P \subseteq T$ доказывается симметричным образом.

5. $P^{\mathbb{R}} \cdot T = P^{\mathbb{R}} \cdot T^{\mathbb{R}} = (T \cdot P)^{\mathbb{R}} \subseteq T(K)^{\mathbb{R}} = T(K)^{\mathbb{R}}; T \cdot P^{\mathbb{R}} = T^{\mathbb{R}} \cdot P^{\mathbb{R}} = (P \cdot T)^{\mathbb{R}} \subseteq T(K)^{\mathbb{R}} = T(K).$
6. Пусть $u, v \in T$. Если хотя бы одно из этих двух слов лежит в T_1 , то $uv \in T_1$. Пусть $u, v \in T_2$. Если первый символ u или последний символ v чётен, то $uv \in T$. В противном случае последний символ u и первый символ v чётны, и в слове uv встречаются два чётных символа подряд. Значит, $uv \notin \text{Subw}(P \cup P^{\mathbb{R}})$, т. е. $uv \in T_1 \subseteq T$.

□

Назовём слова вида $a^{(i)}a^{(i+1)}a^{(i+2)}, a^{(N-1)}a^{(N)}b^{(1)}$ и $a^{(N)}b^{(1)}b^{(2)}$ ($a, b \in \Sigma, 1 \leq i \leq N-2$) *допустимыми тройками типа I*, а обращённые допустимые тройки типа I (а именно, слова вида $a^{(i+2)}a^{(i+1)}a^{(i)}, b(1)a^{(N)}a^{(N-1)}$ и $b^{(2)}b^{(1)}a^{(N)}$) *допустимыми тройками типа II*.

Допустимые тройки типа I (типа II) в точности являются возможными трёхбуквенными подсловами слов из P (соответственно, P^R).

Лемма 7. Пусть $|u| \geq 3$. Тогда $u \in \text{Subw}(P \cup P^R)$ в том и только в том случае, когда все трёхбуквенные подслова слова u являются допустимыми тройками типа I или II.

Доказательство. Нетривиальна импликация справа налево. Рассуждаем индукцией по длине слова u . База индукции ($|u| = 3$) очевидна. Пусть теперь u — слово длины $t + 1$, удовлетворяющее условию и пусть $x \in \Sigma_1$ — последний его символ ($u = u'x$). По индуктивному предположению $u' \in \text{Subw}(P \cup P^R)$. Пусть $u' \in \text{Subw}(P)$ (второй случай симметричен), иначе говоря, u' является подсловом некоторого слова $v \in P$. Рассмотрим три последних символа u . Поскольку первые два из них принадлежат также u' и, следовательно, v , это трёхсимвольное слово является допустимой тройкой типа I, а не типа II. Если она имеет вид $a^{(i)}a^{(i+1)}a^{(i+2)}$ или $a^{(N)}b^{(1)}b^{(2)}$, то x совпадает с символом, следующим за вхождением u' в v , следовательно, слово $u = u'x$ также является подсловом v . Если же эта тройка имеет вид $a^{(N-1)}a^{(N)}b^{(1)}$, то, представив слово v в виде $v_1u'v_2$, мы видим, что $v'u$ также лежит в P , и слово $v_1u'b^{(1)}b^{(2)} \dots b^{(N)} \in P$ содержит слово $u = u'b^{(1)}$ в качестве подслова. Итак, во всех случаях $u \in \text{Subw}(P)$. Индуктивный переход обоснован. \square

Построим ещё одну модель — $\mathcal{M}_2 = \langle \Sigma_1, w_2 \rangle$, где $w_2(p_i) \Leftarrow w_1(p_i) \cup w_1(p_i^R)^R \cup T$, $w_2(p_i^R) \Leftarrow w_1(p_i)^R \cup w_1(p_i^R) \cup T$. Эта модель, в отличие от \mathcal{M} и \mathcal{M}_1 , удовлетворяет условиям $w_2(A^R) \Leftarrow w_2(A)^R$, т.е. является L-моделью в смысле расширенной сигнатуры. Для завершения доказательства теоремы 5 достаточно показать, что $\mathcal{M}_2 \not\equiv F \rightarrow G$.

Лемма 8. Для любого $A \in \Phi$ верны следующие утверждения:

1. $w_2(A) \subseteq P \cup P^R \cup T$;
2. $w_2(A) \supseteq T(f(A))$;
3. $w_2(A) \cap P = w_1(A)$ (в частности, $w_2(A) \cap P \neq \emptyset$);
4. $w_2(A) \cap P^R = w_1(\text{tr}(A^R))^R$ (в частности, $w_2(A) \cap P^R \neq \emptyset$).

Доказательство. Будем доказывать эти четыре утверждения совместной индукцией по построению типа A . База индукции тривиальна. В дальнейшем мы будем обозначать i -е утверждение из предположения индукции через «ИП- i ».

1. Рассмотрим три случая:

а) $A = B \cdot C$. Тогда $w_2(A) = w_2(B) \cdot w_2(C) \subseteq (P \cup P^R \cup T) \cdot (P \cup P^R \cup T) \subseteq P \cup P^R \cup T$ (лемма 6).

б) $A = B \setminus C$. Предположим противное: в $w_2(A)$ есть элемент $u \in E$. Тогда $vu \in w_2(C)$ для любого $v \in w_2(C)$. Рассмотрим несколько подслучаев, и в каждом из них получим противоречие.

i) $u \in \text{Subw}(P)$, причём верхний индекс первого символа слова u не равен 1. Пусть первый символ u есть $a^{(i)}$. Заметим, что i нечётно. Возьмём $v = a^{(3)} \dots a^{(N)} a^{(1)} \dots a^{(i-1)}$. Длина слова v не меньше $N - 2 \geq K$, и слово v оканчивается нечётным символом. Следовательно, $v \in T(K) \subseteq T(f(B)) \subseteq w_2(B)$ (ИП-2). С другой стороны, $vu \in \text{Subw}(P)$, и первый и последний символы vu нечётны. Значит, $vu \in E$ и $vu \in w_2(C)$. Противоречие: $w_2(C) \cap E = \emptyset$ (ИП-1).

ii) $u \in \text{Subw}(P)$, и первый символ слова u есть $a^{(1)}$. Значит, верхний индекс последнего символа u не равен N , потому что иначе $u \in P$. Возьмём произвольное слово $v \in w_2(B) \cap P$ (это множество непусто в силу ИП-3). Первый и последний символы слова vu нечётны, и $vu \in \text{Subw}(P) - P$, следовательно, $vu \in E$. Противоречие.

iii) $u \in \text{Subw}(P^R)$, верхний индекс первого символа u не равен N (первый символ u есть $a^{(i)}$, i нечётно). Возьмём $v = a^{(N-2)} \dots a^{(1)} a^{(N)} \dots a^{(i+1)}$. $vu \in E$.

iv) $u \in \text{Subw}(P^R)$ и u начинается с $a^{(N)}$. Возьмём $v \in w_2(B) \cap P^R$ (непусто по ИП-4). $vu \in E$.

в) $A = C / B$. Симметрично.

2. Рассмотрим три случая.

а) $A = B \cdot C$. Пусть $k_1 \Leftrightarrow f(B)$, $k_2 \Leftrightarrow f(C)$, $k \Leftrightarrow k_1 + k_2 + 10 = f(A)$. По ИП-2 $w_2(B) \supseteq T(k_1)$, $w_2(C) \supseteq T(k_2)$. Возьмём $u \in T(k)$. Докажем, что $u \in w_2(A)$. Рассмотрим несколько подслучаев.

i) $u \in T_1(k)$. По лемме 7 ($|u| \geq k > 3$ и $u \notin \text{Subw}(P \cup P^R)$) в u есть трёхсимвольное подслово xuz , не являющееся допустимой тройкой типа I или II. Разделим слово u на две части, $u = u_1 u_2$, таким образом, что $|u_1| \geq k_1 + 5$ и $|u_2| \geq k_2 + 5$. При необходимости сдвинем границу между частями u_1 и u_2 на один символ влево или вправо, чтобы подслово xuz оказалось целиком в одной из частей (после этого $|u_1| \geq k_1 + 4$, $|u_2| \geq k_2 + 4$). Пусть это будет часть u_2 (другой случай рассматривается симметричным образом). Тогда $u_2 \in T_1(k_2)$. Если u_1 также лежит в T_1 , доказательство на этом заканчивается. Рассмотрим другой случай: $u_1 \in \text{Subw}(P \cup P^R)$. Заметим, что среди любых трёх подряд идущих символов слова из $\text{Subw}(P \cup P^R)$ есть хотя бы один чётный. Сдвинем границу

частей u_1 и u_2 влево на 0, 1 или 2 символа так, чтобы последний символ u_1 оказался чётным. После этого слово u_2 останется в $T_1(k_2)$ (оно не укоротится и по-прежнему содержит подслово xuz), а слово u_1 окажется в $T(k_1)$, потому что его последний символ чётен. Значит, $u = u_1u_2 \in T(k_1) \cdot T(k_2) \subseteq w_2(B) \cdot w_2(C) = w_2(A)$.

ii) $u \in T_2(k)$. Пусть u оканчивается чётным символом (второй случай симметричен). Разделим u на две части, $u = u_1u_2$, $u_1 \geq k_1+5$, $u_2 \geq k_2+5$, и сдвинем границу так, чтобы u_1 заканчивалось чётным символом. Тогда оба слова u_1 и u_2 оканчиваются чётными символами, поэтому $u_1 \in T(k_1)$ и $u_2 \in T(k_2)$. Значит, $u = u_1u_2 \in T(k_1) \cdot T(k_2) \subseteq w_2(B) \cdot w_2(C) = w_2(A)$.

б) $A = B \setminus C$. Пусть $k \Leftrightarrow f(C) = f(A)$. В силу ИП-2 $w_2(C) \supseteq T(k)$. Возьмём $u \in T(k)$ и произвольное $v \in w_2(B) \subseteq P \cup P^R \cup T$. Имеем $vu \in (P \cup P^R \cup T) \cdot T \subseteq T$ (лемма 6.4-6), а поскольку $|vu| > |u| \geq k$, $vu \in T(k) \subseteq w_2(C)$. Значит, $u \in w_2(A)$.

в) $A = C / B$. Симметрично.

3. Рассмотрим три случая.

а) $A = B \cdot C$.

\supseteq $u \in w_1(A) = w_1(B) \cdot w_1(C) \subseteq w_2(B) \cdot w_2(C) = w_2(A)$ (ИП-3); $u \in P$.

\subseteq Пусть $u \in P$, $u \in w_2(A) = w_2(B) \cdot w_2(C)$. Тогда $u = u_1u_2$, где $u_1 \in w_2(B)$, $u_2 \in w_2(C)$. Сначала докажем, что $u_1 \in P$. Предположим противное: $u_1 \notin P$. Тогда $u_1 \in P^R \cup T$ (ИП-1), $u_2 \in P \cup P^R \cup T$, откуда $u = u_1u_2 \in (P^R \cup T) \cdot (P \cup P^R \cup T) \in P^R \cup T$ (лемма 6). Противоречие ($u \in P$). Значит, $u_1 \in P$, а потому и $u_2 \in P$, и по ИП-3 получаем, что $u_1 \in w_1(B)$, $u_2 \in w_1(C)$, откуда $u = u_1u_2 \in w_1(A)$.

б) $A = B \setminus C$.

\supseteq Пусть $u \in w_1(B \setminus C)$. Значит, для любого $v \in w_1(B)$ имеем $vu \in w_1(C)$. Покажем, что $u \in w_2(B \setminus C)$. Возьмём $v \in w_2(B) \subseteq P \cup P^R \cup T$ (ИП-1).

Если $v \in P$, то $v \in w_1(B)$ (ИП-3), поэтому $vu \in w_1(C) \subseteq w_2(C)$.

Если же $v \in P^R \cup T$, то $vu \in (P^R \cup T) \cdot P \subseteq T(K) \subseteq w_2(C)$ (лемма 6 и ИП-2).

\subseteq . Если $u \in w_2(B \setminus C)$ и $u \in P$, то для любого $v \in w_1(B) \subseteq w_2(B)$ имеем $vu \in w_2(C)$. Поскольку $v, u \in P$, то $vu \in P$, откуда $vu \in w_1(C)$ (ИП-3). Значит, $u \in w_1(B \setminus C)$.

в) $A = C / B$. Симметрично.

4. Симметрично. □

Поскольку $w_1(F) \not\subseteq w_1(G)$, существует такое слово u_0 , что $u_0 \in w_1(F)$ и $u_0 \notin w_1(G)$. Кроме того, $u_0 \in P$, поэтому (в силу только что доказанной леммы) $u_0 \in w_2(F)$ и $u_0 \notin w_2(G)$. Следовательно, $w_2(F) \not\subseteq w_2(G)$, т. е. $\mathcal{M}_2 \not\equiv F \rightarrow G$. Поскольку $F_0 \leftrightarrow F$,

$G_0 \leftrightarrow G$ и исчисление L^R корректно относительно L -моделей, $M_2 \not\equiv F_0 \rightarrow G_0$. Теорема 5 доказана: M_2 является искомой контрмоделью.

Заметим, что мы построили контрмодель (в смысле расширенной сигнатуры) не только для секвенций, невыводимых в исчислении L^R , но и для секвенций в нормальной форме, невыводимых в а priori более слабом исчислении L' . Отсюда получается следующее утверждение:

Предложение 9. *Секвенция $A_1 \dots A_n \rightarrow B$ выводима в L^R тогда и только тогда, когда в L' выводима секвенция $tr(A_1) \dots tr(A_n) \rightarrow tr(B)$.*

7 Исчисление L^R : грамматики и сложность

Теорема 6. *Класс L^R -языков совпадает с классом контекстно-свободных языков, не содержащих пустого слова.*

Доказательство. Включение класса контекстно-свободных языков без пустого слова в класс L^R -языков следует из теоремы 2 и консервативности L^R над $L(\setminus)$.

Обратное включение следует из предложения 9: заменив в L^R -грамматике все типы C на $tr(C)$, получим грамматику, основанную на исчислении L (точнее говоря, на L' , отличающемся от L только обозначениями примитивных типов), задающую тот же язык — и этот язык является контекстно-свободным по теореме 3. \square

Фрагменты исчисления L^R с ограниченными наборами связок определяются так же, как и для L .

Теорема 7. *Проблемы выводимости в исчислениях $L^R(\setminus)$, L^R , а также всех промежуточных исчислениях, являющихся консервативными фрагментами L^R и консервативными расширениями $L^R(\setminus)$, NP-полны.*

Доказательство. Принадлежность проблемы выводимости в исчислении L^R к классу NP следует из предложения 9 и того факта, что проблема выводимости в L лежит в NP (в силу теоремы об устранении сечения).

NP-полнота проблемы выводимости в исчислении $L^R(\setminus)$ следует из эквивалентности $B/A \leftrightarrow_{L^R} (A^R \setminus B^R)^R$, сводящей к выводимости в $L^R(\setminus)$ выводимость в $L(\setminus, /)$, и NP-полноты проблемы выводимости для последнего [6]. \square

Список литературы

- [1] Y. Bar-Hillel, C. Gaifman, E. Shamir. On the categorial and phrase-structure grammars. *Bulletin of the Research Council of Israel, Section F*. Vol. 9F, 1960. — P. 1–16.
- [2] W. Buszkowski. Compatibility of a categorial grammar with an associated category system. *Zeitschrift für mathematische Logik und Grundlagen der Mathematik*. Vol. 28, 1982. — P. 229–238.
- [3] W. Buszkowski. The equivalence of unidirectional Lambek categorial grammars and context-free grammars, *Zeitschrift für mathematische Logik und Grundlagen der Mathematik*. Vol. 31, 1985. — P. 369–384.
- [4] N. Chomsky. Three models for the description of language. *IRE Transactions on Information Theory*. Vol. I T-2, No. 3, 1956. — P. 113–124.
Русский перевод: Н. Хомский. Три модели описания языка. *Кибернетический сборник*, вып. 2. — М.: ИЛ, 1961. — С. 237–266.
- [5] J. Lambek. The mathematics of sentence structure. *American Mathematical Monthly*. Vol. 65, No. 3, 1958. — P. 154–170.
Русский перевод: И. Ламбек. Математическое исследование структуры предложений. *Математическая лингвистика: сборник переводов*, под ред. Ю. А. Шрейдера и др. — М.: Мир, 1964. — С. 47–68.
- [6] Yu. Savateev. Product-free Lambek calculus is NP-complete. *Proceedings of the International Symposium “Logical Foundations of Computer Science” (LFCS 2009)*, ed. by S. N. Artemov and A. Nerode. *Lecture Notes in Computer Science*. Vol. 5407. Berlin: Springer, 2009. — P. 380–394.
- [7] В. А. Минина. Полнота синтаксического исчисления Ламбека с операцией инволюции. Дипломная работа, кафедра математической логики и теории алгоритмов МГУ им. Ломоносова. — М., 2001. — 13 с.
- [8] М. Р. Пентус. Исчисление Ламбека и формальные грамматики. *Фундаментальная и прикладная математика*. Том 1, № 3, 1995. — С. 729–751.
- [9] М. Р. Пентус. Полнота синтаксического исчисления Ламбека. *Фундаментальная и прикладная математика*. Том 5, № 1, 1999. — С. 193–219.