МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ им. М. В. ЛОМОНОСОВА

Механико-математический факультет

На правах рукописи

УДК 510.662

Саватеев Юрий Вячеславович

Алгоритмическая сложность фрагментов исчисления Ламбека

Специальность 01.01.06 — математическая логика, алгебра и теория чисел

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва 2009

Работа выполнена на кафедре математической логики и теории алгоритмов Механико-математического факультета Московского государственного университета имени М. В. Ломоносова

Научный руководитель:	доктор физико-математических наук, профессор Пентус Мати Рейнович
Официальные оппоненты:	доктор физико-математических наук Лысенок Игорь Геронтьевич
	кандидат физико-математических наук Кудинов Андрей Валерьевич
Ведущая организация:	Институт математики имени С. Л. Соболева Сибирского отделения РАН

Защита диссертации состоится 11 декабря 2009 года в 16 часов 45 минут на заседании диссертационного совета Д.501.001.84 при Московском государственном университете имени М. В. Ломоносова по адресу: Российская Федерация, 119991, Москва, ГСП-1, Ленинские горы, д. 1, МГУ имени М. В. Ломоносова, Механико-математический факультет, аудитория 14-08.

С диссертацией можно ознакомиться в библиотеке Механико-математического факультета МГУ (Главное здание, 14 этаж).

Автореферат разослан 11 ноября 2009 года.

Ученый секретарь диссертационного
совета Д.501.001.84 при МГУ,
доктор физико-математических наук,
профессор

А. О. Иванов

Общая характеристика работы

Актуальность темы. Диссертация посвящена исследованию алгоритмической сложности фрагментов исчисления Ламбека.

Исчисление Ламбека L было введено в 1958 году[1]. Оно активно используется в качестве основы для создания категориальных грамматик, описывающих синтаксические структуры естественных языков[2] [3]. Категориальные грамматики имеют ряд преимуществ перед другими способами, такими как контекстно-свободные грамматики, ввиду лексикализации — вся необходимая информация хранится в лексиконе, поэтому нет необходимости использовать всю имеющуюся информацию — достаточно только той, что относится к данному случаю. Также это позволяет параллельно с анализом синтаксической структуры вести семантический анализ, используя, например, грамматику Монтегю[4].

Класс языков, порождаемых категориальными грамматиками, основанными на исчислении Ламбека, в точности совпадает с классом контекстно-свободных языков[5]. Исчисление Ламбека также тесно связано с линейной логикой Жирара[6] — оно эквивалентно интуиционистскому некоммутативному фрагменту мультипликативной линейной логики.

В исчислении Ламбека используются синтаксические типы, построенные из примитивных с помощью трех бинарных связок — умножения, левого деления и правого деления. Естественно рассматривать фрагменты исчисления Ламбека с ограниченным набором связок. В настоящей работе будут рассмотрены так называемый левосторонний фрагмент $\mathrm{L}(\cdot, \backslash)$, фрагмент без умножения $\mathrm{L}(\backslash, /)$, который является особенно важным для лингвистических приложений (большинство грамматик, описывающих естественные языки, основаны именно на этом фрагменте), и фрагмент исчисления Ламбека с одним делением $\mathrm{L}(\backslash)$. Также рассматриваются их варианты — фрагменты исчисления Ламбека с разрешенными пустыми антецедентами $\mathrm{L}^*(\cdot, \backslash)$, $\mathrm{L}^*(\backslash, /)$, и $\mathrm{L}^*(\backslash)$.

В категориальных грамматиках синтаксический разбор предложения

[1] Lambek J. The mathematics of sentence structure // American Mathematical Monthly. — 1958. — Vol. 65, № 3. — P. 154—170. — Русский перевод: Ламбек И. Математическое исследование структуры предложений // Математическая лингвистика: Сборник переводов / Под ред. Ю. А. Шрейдера и др. — М.: Мир, 1964. —- С. 47—68.

[2] Moortgat M. Categorial type logic, // Handbook of Logic and Language / Editors J. van Benthem, A. ter Meulen. — Elsevier. — 1997. — P. 93—177.

[3] Morrill G. Type Logical Grammar: Categorial Logic of Signs // Berlin: Springer. — 1994. — 328 p.

[4] Montague R. English as a Formal Language // Linguaggi nella societa e nella tecnica. — / Editor Bruno Visentini. — Milan: Edizioni di Comunità, 1970. — P. 189—223.

[5] Pentus M. Lambek grammars are context free // Proceedings of the 8th Annual IEEE Symposium on Logic in Computer Science: June 19—23, 1993. Montreal, Canada. — Los Alamitos, California: IEEE Computer Society Press, 1993. — P. 429—433.

[6] Girard J.-Y. Linear logic // Theoretical Computer Science. — 1987. — Vol. 50, № 1. — P. 1—102.

сводится к поиску вывода в исчислении, лежащем в их основе. Поэтому вопрос об алгоритмической сложности задачи распознавания выводимости особенно важен для лингвистических приложений, так как напрямую связан с эффективностью работы ситаксических анализаторов, основанных на категориальных грамматиках.

Для неассоциативного варианта исчисления Ламбека де Гроотом было показано, что задача распознавания выводимости может быть решена за полиномиальное время[7]. Для фрагмента неассоциативного исчисления без умножения это было доказано ранее Аартсом и Траутвейном[8]. Для самого исчисления Ламбека (где умножение является ассоциативным), а также для его варианта L^*, разрешающего пустые антецеденты, была доказана NP-полнота задачи распознавания выводимости[9].

Мы докажем, что классическая NP-полная задача SAT (о выполнимости булевых формул в конъюнктивной нормальной форме) за полиномиальное время может быть сведена к задачам распознавания выводимости в $L(\cdot, \backslash)$, $L(\backslash, /)$, $L^*(\cdot, \backslash)$ и $L^*(\backslash, /)$, и тем самым покажем, что задача распознавания выводимости для этих фрагментов NP-полна. Все конструкции и доказательства, которые мы используем при рассмотрении $L(\cdot, \backslash)$ и $L^*(\cdot, \backslash)$, могут быть явно переписаны для правостороннего фрагмента $L(\cdot, /)$. Таким образом задача распознавания выводимости для $L(\cdot, /)$ и $L^*(\cdot, /)$ также является NP-полной.

Для фрагмента с одним делением мы строим полиномиальный алгоритм, решающий более общую задачу, а именно, задачу распознавания принадлежности данного слова языку, порождаемому данной грамматикой, основанной на этом фрагменте. Это возможно благодаря более простой струтуре секвенций, выводимых в этом исчислении.

Таким образом, теперь для всех фрагментов исчисления Ламбека, заданных ограничениями набора связок, установлены точные оценки алгоритмической сложности задачи распознавания выводимости.

В качестве основной техники для исследования выводимости во фрагментах ассоциативного исчисления Ламбека мы используем так называемые сети доказательства — метод, позволяющий наглядно и компактно представлять вывод формулы в данном исчислении, полностью пе-

[7] de Groote Ph. The non-associative Lambek calculus with product in polynomial time // Automated Reasoning with Analytic Tableaux and Related Methods / Editor N. V. Murray. — Berlin: Springer, 1999. — P. 128—139. — (Lecture Notes in Computer Science; vol. 1617).

[8] Aarts E., Trautwein K. Non-associative Lambek categorial grammar in polynomial time // Mathematical logic Quarterly. — 1995. — Vol. 41, № 4. — P. 476—484.

[9] Pentus M. Lambek calculus is NP-complete // Theoretical Computer Science. — 2006. — Vol. 357, № 1/3. — P. 186—201.

редавая его принципиальную структуру[10 11]. В 2005 году Пенном была предпринята попытка применить данный метод для исследования выводимости во фрагменте исчисления Ламбека без умножения, однако там не было получено никаких результатов, связанных с алгоритмической сложностью[12]. Еще один критерий (близкий к критерию, предложенному автором[13], однако формально неверный) для этого фрагмента был предложен Леконтом в 1993 году[14].

Открытый вопрос об NP-полноте задачи распознавания выводимости во фрагменте исчисления Ламбека без умножения упоминается в статьях многих математиков и лингвистов, изучающих исчисление Ламбека[7 8 9 12].

Цель работы. Получение оценок алгоритмической сложности задач распознавания выводимости и распознавания принадлежности данного слова языку, порождаемому данной категориальной грамматикой, для различных фрагментов исчисления Ламбека.

Научная новизна. Результаты диссертации являются новыми, среди них:

1. Задачи распознавания выводимости в исчислении NP-полны для $\mathrm{L}(\cdot, \backslash), \mathrm{L}(\backslash, /), \mathrm{L}(\cdot, /), \mathrm{L}^*(\cdot, \backslash), \mathrm{L}^*(\backslash, /), \mathrm{L}^*(\cdot, /)$.

2. Задачи распознавания принадлежности данного слова языку, порождаемому данной категориальной грамматикой, NP-полны для $\mathrm{L}(\cdot, \backslash), \mathrm{L}(\backslash, /), \mathrm{L}(\cdot, /), \mathrm{L}^*(\cdot, \backslash), \mathrm{L}^*(\backslash, /), \mathrm{L}^*(\cdot, /)$.

3. Задачи распознавания выводимости в исчислении разрешимы за полиномиальное время для $\mathrm{L}(\backslash), \mathrm{L}^*(\backslash), \mathrm{L}(/), \mathrm{L}^*(/)$.

4. Задачи распознавания принадлежности данного слова языку, порождаемому данной категориальной грамматикой, разрешимы за полиномиальное время для $\mathrm{L}(\backslash), \mathrm{L}^*(\backslash), \mathrm{L}(/), \mathrm{L}^*(/)$.

Методы исследования. В работе применяются методы теории доказательств. Основным инструментом исследования выводимости является

[10] Roorda D. Resource Logics: Proof-theoretical Investigations: Ph.D. thesis. — Amsterdam, 1991. — 138 p.

[11] Métayer F. Polynomial equivalence among systems LLNC, LLNC_a and LLNC_0 // Theoretical Computer Science. — 1999. — Vol. 227, № 1. — P. 221—229.

[12] Penn G. A Graph-Theoretic Approach to Polynomial-Time Recognition with the Lambek Calculus // Electronic Notes in Theoretical Computer Science. — Elsevier. — 2005. — Vol. 53.

[13] Savateev Y. Product-free Lambek calculus is NP-complete // Logical Foundations of Computer Science, International Symposium, LFCS 2009, Deerfield Beach, FL, USA, January 3—6, 2009. Proceedings / Editors S. N. Artemov and A. Nerode. — Berlin: Springer, 2009. — P. 380—394. — (Lecture Notes in Computer Science; vol. 5407).

[14] Lecomte A. Towards efficient parsing with proof-nets // EACL 1993, 6th Conference of the European Chapter of the Association for Computational Linguistics, April 21-23, 1993. — Utrecht: OTS — Research Institute for Language and Speech, Utrecht University, 1993. — P. 269—276.

построение так называемых сетей доказательства с различными свойствами, отвечающими конкретному фрагменту исчисления Ламбека.

Теоретическая и практическая ценность. Работа носит теоретический характер. Результаты, полученные в диссертационной работе, могут найти применение в математической логики и лингвистике.

Апробация диссертации. Результаты диссертации докладывались на следующих семинарах и конференциях:

- На международном семинаре "Вычислительные интерпретации доказательств" (Computational Interpretations of Proofs), Париж, Франция, 29–30 ноября 2007 года.

- На международной конференции "Логические модели доказательств и вычислений" (LMRC-2008) Москва, Россия, 5–8 мая 2008 года.

- На международной конференции "Компьютерные науки в России" (CSR-2008), Москва, Россия, 7–12 июня 2008 года.

- На семинаре "Алгоритмические вопросы алгебры и логики"под руководством академика РАН С.И. Адяна (2008, 2009).

- На международной конференции "Логические основы компьютерных наук" (LFCS-2009), Дирфилд Бич, США, 3–6 января 2009 года.

- На Европейской летней школе по логике, лингвистике и информатике (ESSLLI-2009), Бордо, Франция, 20–31 июля 2009 года.

- На научно-исследовательском семинаре кафедры математической логики и теории алгоритмов под руководством академика РАН С. И. Адяна, члена-корреспондента РАН Л. Д. Беклемишева и профессора В. А. Успенского (2009).

Публикации. Основные результаты диссертации опубликованы в работах [1]–[3].

Структура диссертации. Работа состоит из введения, 5 глав, содержащих 12 разделов, и списка литературы. Библиография содержит 17 наименований. Текст диссертации изложен на 75 страницах.

Содержание работы

В **главе 1** вводятся нужные нам понятия и обозначения.

В **разделе 1.1** формулируются аксиомы и правила исчисления Ламбека.

Ассоциативное исчисление Ламбека можно построить следующим образом. Пусть задано счетное множество *примитивных типов* $\mathbf{P} = \{p_0, p_1, \ldots\}$. Определим множество Tp L-типов (также называемых L-термами): (1) $\mathbf{P} \subset \mathrm{Tp}$; (2) если $A, B \in \mathrm{Tp}$, то $(A/B), (A\backslash B), (A \cdot B) \in \mathrm{Tp}$.

Примитивные типы будем обозначать строчными латинскими буквами ($p, q, r, \ldots$), L-типы — заглавными латинскими буквами ($A, B, C \ldots$). Заглавными греческими буквами ($\Pi, \Gamma, \Delta, \ldots$) будем обозначать последовательности (возможно пустые) L-типов. Выражения вида $\Pi \to A$, где Π непусто, называются L-формулами или секвенциями. Конечную последовательность L-типов $A_1, \ldots, A_n$ условимся обозначать $A_1 \ldots A_n$.

Аксиомы и правила вывода в L таковы:

$$A \to A, \qquad \frac{\Phi \to B \quad \Gamma B \Delta \to A}{\Gamma \Phi \Delta \to A}\ (\mathrm{CUT}),$$

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

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

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

В посылках и выводах правил стоят L-формулы, Γ и Δ могут быть пустыми.

Запись $\mathrm{L} \vdash \Pi \to A$ означает, что секвенция $\Pi \to A$ выводима в исчислении L.

Исчисление L^* отличается от L тем, что в нем разрешены пустые антецеденты, то есть выражения вида $\to A$, где A — некоторый тип, также считаются формулами. Правило сечения (CUT) является устранимым в обоих этих исчислениях.

В **разделе 1.2** описываются интересующие нас фрагменты исчисления Ламбека.

- Левосторонний фрагмент исчисления Ламбека. В этом фрагменте для образования сложных типов используются только две операции — умножение и левое деление. Все секвенции, выводимые в этом фрагменте, не содержат знака /, поэтому правила $(\to /)$ и $(/ \to)$ отсутствуют в этом фрагменте.

- Фрагмент исчисления Ламбека без умножения. То же самое, только здесь отсутсвует умножение.

- Фрагмент исчисления Ламбека с одним делением. Здесь для образования сложных типов используется только одна операция — левое деление.

Так же мы рассматриваем варианты этих фрагментов, допускающие пустые антецеденты.

В **разделе 1.3** показывается как строятся грамматики на основе исчисления Ламбека и какие языки они порождают.

Грамматика Ламбека это четверка $(\Sigma, \mathbf{P}, R, B)$, где Σ это алфавит, $\mathbf{P}$ — набор примитивных типов, $R\colon \Sigma \to 2^{\mathrm{Tp}}$ — отображение, сопоставляющее каждой букве алфавита конечное множество L-типов, построенных из $\mathbf{P}$, B — выделенный L-тип. Слово $x_1, \ldots, x_n \in \Sigma^*$ принадлежит языку, порождаемому данной грамматикой, если существуют $A_i \in R(x_i)$ такие, что секвенция $A_1 \ldots A_n \to B$ выводится в исчислении Ламбека.

В **разделе 1.4** вводится понятие структурно эквивалентных секвенций, которое потребуется нам при доказательстве критерия выводимости.

В **главе 2** вводится понятие сети доказательства.

В **разделе 2.1** описывается представление секвенций исчисления Ламбека как множества начал некоторого слова и доказываем свойства этого представления. В этом же разделе вводится понятие сети доказательства и формулируются так называемые доказательные условия — свойства сетей доказательства, которые будут использоваться для определения выводимости исходной секвенции.

Обозначим за $\mathbb{N}$ множество натуральных чисел (0 является натуральным числом). За $\mathbb{Z}$ обозначим множество целых чисел.

Пусть даны $p \in \mathrm{Tp}$, $i \in \mathbb{N}$ и $j \in \mathbb{Z}$. Тогда назовем *атомом* символ $p^{\lfloor j \rfloor}_{\lceil i \rceil}$. Определим множество At как множество всех атомов.

Определим FS как множество всех конечных слов в алфавите At.

Элементы FS будем обозначать буквами $\mathbb{A}$, $\mathbb{B}$, $\mathbb{C}$ и так далее, символом ε будем обозначать пустую строку.

Определим три отображения $t : \mathrm{FS} \to \mathbf{P}$, $d : \mathrm{FS} \to \mathbb{N}$ и $g : \mathrm{FS} \to \mathbb{Z}$ следующим образом:

$$t(\mathbb{A}p^{\lfloor j \rfloor}_{\lceil i \rceil}) = p; \quad d(\mathbb{A}p^{\lfloor j \rfloor}_{\lceil i \rceil}) = j; \quad g(\mathbb{A}p^{\lfloor j \rfloor}_{\lceil i \rceil}) = i.$$

На пустом слове значение этих функций не определено.

Пусть $\mathbb{A} \sqsubset \mathbb{B}$ обозначает, что $\mathbb{A}$ является собственным началом $\mathbb{B}$, то есть существует $\mathbb{C} \neq \varepsilon$, такое что $\mathbb{B} = \mathbb{A}\mathbb{C}$. Выражение $\mathbb{A} \sqsubseteq \mathbb{B}$ значит, что либо $\mathbb{A} \sqsubset \mathbb{B}$, либо $\mathbb{A} = \mathbb{B}$.

Пусть $\mathcal{P}_{\mathbb{A}} = \{\mathbb{B} \mid \varepsilon \sqsubset \mathbb{B} \sqsubseteq \mathbb{A}\}$ — множество всех непустых начал $\mathbb{A}$. На множестве $\mathcal{P}_{\mathbb{A}}$ отношение $\sqsubset$ является строгим линейным порядком. Тем самым, определены понятия $\min_{\sqsubset}$, $\max_{\sqsubset}$ и $[\mathbb{B}, \mathbb{C}]_{\sqsubset}$. Последнее означает множество $\{\mathbb{D} \in \mathcal{P}_{\mathbb{A}} \mid \mathbb{B} \sqsubseteq \mathbb{D} \sqsubseteq \mathbb{C}\}$. Полуинтервал $(\mathbb{B}, \mathbb{C}]_{\sqsubset}$ определяется аналогично.

Если γ — бинарное отношение на некотором множестве X, то γ^+ означает его транзитивное замыкание, а γ^* — его транзитивно-рефлексивное замыкание.

Пусть $(\cdot)^{\langle n \rangle} (n \in \mathbb{Z})$ — семейство функций на FS, заданное следующими соотношениями:

$$\begin{gathered}
(p^{\lfloor 0 \rfloor}_{\lceil i \rceil})^{\langle n \rangle} = p^{\lfloor 1 \rfloor}_{\lceil n \rceil}, \\
(p^{\lfloor j \rfloor}_{\lceil i \rceil})^{\langle n \rangle} = p^{\lfloor j+1 \rfloor}_{\lceil -i \rceil}, \text{для } j \neq 0, \\
(\mathbb{A}\mathbb{B})^{\langle n \rangle} = (\mathbb{B})^{\langle n \rangle}(\mathbb{A})^{\langle n \rangle}.
\end{gathered}$$

Определим следующую функцию $h : \mathrm{Tp} \to \mathbb{N}$:

$$h(p) = 1; \quad h(A/B) = h(B\backslash A) = h(A); \quad h(A \cdot B) = h(A) + h(B).$$

Перевод L-типов в элементы FS осуществляется с помощью следующего отображения $[\![\cdot]\!]$:

$$\begin{aligned}
[\![p]\!] &= p^{\lfloor 0 \rfloor}_{\lceil 0 \rceil}; \\
[\![(A/B)]\!] &= [\![B]\!]^{\langle h(A) \rangle}[\![A]\!]; \\
[\![(A\backslash B)]\!] &= [\![B]\!][\![A]\!]^{\langle -h(B) \rangle}; \\
[\![(A \cdot B)]\!] &= [\![B]\!][\![A]\!].
\end{aligned}$$

Пусть $\mathcal{N}_{\mathbb{A}} = \{\mathbb{B} \in \mathcal{P}_{\mathbb{A}} \mid d(\mathbb{B}) \text{ нечетно}\}$.

Определим бинарное отношение φ на множестве $\mathcal{P}_{\mathbb{A}}$ следующим образом:

$$\mathbb{B}\,\varphi\,\mathbb{C} \Leftrightarrow \begin{cases}
(\mathbb{B} \sqsubset \mathbb{C}) \wedge (d(\mathbb{C}) = d(\mathbb{B}) - 1) \wedge \\
\qquad \wedge (|\{\mathbb{D} \mid \mathbb{B} \sqsubset \mathbb{D} \sqsubset \mathbb{C}, d(\mathbb{D}) = d(\mathbb{C})\}| < |g(\mathbb{B})|), & \text{если } g(\mathbb{B}) \geq 0; \\
(\mathbb{C} \sqsubset \mathbb{B}) \wedge (d(\mathbb{C}) = d(\mathbb{B}) - 1) \wedge \\
\qquad \wedge (|\{\mathbb{D} \mid \mathbb{C} \sqsubset \mathbb{D} \sqsubset \mathbb{B}, d(\mathbb{D}) = d(\mathbb{C})\}| < |g(\mathbb{B})|), & \text{если } g(\mathbb{B}) < 0.
\end{cases}$$

Пусть $\Phi(\mathbb{B}) = \{\mathbb{C} \mid \mathbb{B}\,\varphi\,\mathbb{C}\}$.

Рассмотрим секвенцию $A_1 \dots A_n \to B$. Пусть

$$\mathbb{W} = [\![A_1]\!]^{\langle 0 \rangle} \dots [\![A_n]\!]^{\langle 0 \rangle}[\![B]\!].$$

На множестве $\mathcal{P}_{\mathbb{W}}$ определены отношение φ, функция Φ, а также множество $\mathcal{N}_{\mathbb{W}}$.

Множество $\mathcal{G} \subset \mathcal{P}_{\mathbb{W}}$ называется φ-замкнутым, если из $\mathbb{A} \in \mathcal{G}$ и $\mathbb{B}\,\varphi\,\mathbb{A}$ следует, что $\mathbb{B} \in \mathcal{G}$.

Определим отношение $\beta \subseteq \mathcal{P}_{\mathbb{W}} \times \mathcal{P}_{\mathbb{W}}$ следующим образом:

$$\mathbb{A}\,\beta\,\mathbb{B} \Leftrightarrow (\mathbb{A} = \mathbb{B}) \vee \exists\mathbb{C}(\mathbb{C}\,\varphi\,\mathbb{A} \wedge \mathbb{C}\,\varphi\,\mathbb{B}).$$

Определим отношение $\beta' \subseteq \mathcal{P}_{\mathbb{W}} \times \mathcal{P}_{\mathbb{W}}$ следующим образом:

$$\mathbb{A}\,\beta'\,\mathbb{B} \Leftrightarrow (\mathbb{A}\beta\mathbb{B}) \wedge \forall\mathbb{C}(\mathbb{C}\,\varphi\,\mathbb{A} \to \mathbb{C}\,\varphi\,\mathbb{B}).$$

Для $\mathbb{A} \in \mathcal{P}_{\mathbb{W}}$ определим следующее множество:

$$\mathcal{F}_{\varphi}(\mathbb{A}) = \{\mathbb{B} \mid \exists\mathbb{C}(\mathbb{B}\,\varphi^{*}\mathbb{C} \wedge \mathbb{A}\,\beta'\,\mathbb{C}) \wedge \forall\mathbb{D}((\mathbb{B}\,\varphi^{*}\,\mathbb{D} \wedge \mathbb{A}\,\beta\,\mathbb{D}) \to \mathbb{A}\,\beta'\,\mathbb{D})\}.$$

Пусть π функция из $\mathcal{N}_{\mathbb{W}}$ в $\mathcal{P}_{\mathbb{W}}$. Пусть ψ бинарное отношение на $\mathcal{P}_{\mathbb{W}}$, определяемое следующим соотношением:

$$\mathbb{A}\,\psi\,\mathbb{B} \Leftrightarrow \begin{cases} \mathbb{B} = \pi(\mathbb{A}), & \text{если } \mathbb{A} \in \mathcal{N}_{\mathbb{W}}; \\ \mathbb{A}\varphi\mathbb{B}, & \text{если } \mathbb{A} \notin \mathcal{N}_{\mathbb{W}} \text{ и } d(\mathbb{A}) \neq 0. \end{cases}$$

Определение 2.1.1. Тройку (π, φ, ψ) будем называть сетью доказательства для слова $\mathbb{W}$.

Определим

$$\mu_{\pi}^{-}(\mathbb{A}) = \min_{\sqsubset}\{\mathbb{A}; \pi(\mathbb{A})\};$$
$$\mu_{\pi}^{+}(\mathbb{A}) = \max_{\sqsubset}\{\mathbb{A}; \pi(\mathbb{A})\}.$$

Назовем *доказательными условиями* следующие ограничения на сеть доказательства.

1. Функция π является биекцией между $\mathcal{N}_{\mathbb{W}}$ и $\mathcal{P}_{\mathbb{W}} \setminus \mathcal{N}_{\mathbb{W}}$.

2. Для любого $\mathbb{A} \in \mathcal{N}_{\mathbb{W}}$ верно, что $t(\pi(\mathbb{A})) = t(\mathbb{A})$.

3. $\mu_{\pi}^{-}(\mathbb{A}) \sqsubset \mu_{\pi}^{-}(\mathbb{B}) \Rightarrow \mu_{\pi}^{+}(\mathbb{A}) \sqsubset \mu_{\pi}^{-}(\mathbb{B}) \vee \mu_{\pi}^{+}(\mathbb{B}) \sqsubset \mu_{\pi}^{+}(\mathbb{A})$.

4. Отношение $(\varphi \cup \psi)^{+}$ иррефлексивно.

5. Для любого $\mathbb{A} \in \mathcal{N}_{\mathbb{W}}$, такого что $g(\mathbb{A}) \neq 0$, для любого $\mathbb{B} \in \mathcal{P}_{\mathbb{W}} \setminus \mathcal{N}_{\mathbb{W}}$, такого что $\mathbb{A}\psi^{+}\mathbb{B}$, верно, что $\mathbb{A}\varphi\mathbb{B} \vee \forall\mathbb{C}(\mathbb{A}\varphi\mathbb{C} \to \mathbb{C}\psi^{+}\mathbb{B}) \vee \forall\mathbb{B}'(\mathbb{B}\varphi\mathbb{B}' \to \exists\mathbb{C}(\mathbb{A}\varphi\mathbb{C} \wedge \mathbb{B}'\psi^{+}\mathbb{C}))$

6. Для любого $\mathbb{A} \in \mathcal{P}_{\mathbb{W}} \setminus \mathcal{N}_{\mathbb{W}}$ существуют $\mathbb{B} \in \mathcal{F}_{\varphi}(\mathbb{A})$ и $\mathbb{C} \notin \mathcal{F}_{\varphi}(\mathbb{A})$, такие что $\mathbb{C}\psi^{*}\mathbb{B}$.

В **разделе 2.2** формулируется и доказывается критерий выводимости секвенций на основе доказательных условий.

Теорема 1. $\mathrm{L}^* \vdash A_1 \dots A_n \to B$, *если и только если для слова* $\mathbb{W} = [\![A_1]\!]^{\langle 0\rangle} \dots [\![A_n]\!]^{\langle 0\rangle}[\![B]\!]$ *существует сеть доказательства* (π, φ, ψ), *удовлетворяющая доказательным условиям (1)–(5).*

$\mathrm{L} \vdash A_1 \dots A_n \to B$, *если и только если для слова* $\mathbb{W} = [\![A_1]\!]^{\langle 0\rangle} \dots [\![A_n]\!]^{\langle 0\rangle}[\![B]\!]$ *существует сеть доказательства* (π, φ, ψ), *удовлетворяющая доказательным условиям (1)–(6).*

В **главе 3** доказывается NP-полнота задач распознавания выводимости для лево- и правостороннего фрагментов исчисления Ламбека и их вариантов, допускающих пустые антецеденты.

Теорема 2. *Задача распознавания выводимости секвенций в* $\mathrm{L}(\cdot, \backslash)$, $\mathrm{L}(\cdot, /)$, $\mathrm{L}^*(\cdot, \backslash)$ *и* $\mathrm{L}^*(\cdot, /)$ *NP-полна.*

Следствие 1. *Задача распознавания принадлежности данного слова языку, порожденному данной грамматикой, основанной на* $\mathrm{L}(\cdot, \backslash)$, $\mathrm{L}(\cdot, /)$, $\mathrm{L}^*(\cdot, \backslash)$ *или* $\mathrm{L}^*(\cdot, /)$, *NP-полна.*

В **разделе 3.1** приводится конструкция, с помощью которой сводится известная NP-полная задача SAT к задаче распознавания выводимости в данном фрагменте. Для правостороннего фрагмента работает конструкция, симметричная построенной.

Для каждой булевой переменной x_i пусть $\neg_0 x_i$ обозначает литерал $\neg x_i$, а $\neg_1 x_i$ обозначает литерал x_i.

Пусть p_i^j, r_i, где $0 \le i \le n+1, 0 \le j \le m$ — различные примитивные типы из $\mathbf{P}$.

Определим следующие семейства типов:

$$
\begin{aligned}
G^0 &= (p_0^0 \backslash p_{n+1}^0);\\
G^j &= ((p_0^j \backslash G^{j-1}) \cdot p_{n+1}^j); \quad G = G^m;\\
H_i^0 &= (p_{i-1}^0 \backslash p_i^0);\\
H_i^j &= (p_{i-1}^j \backslash (H^{j-1} \cdot p_i^j)); \quad H_i = H_i^m;\\
E_i^0(t) &= (p_{i-1}^0 \backslash p_i^0);\\
E_i^j(t) &= \begin{cases} ((p_{i-1}^j \backslash E_i^{j-1}(t)) \cdot p_i^j), & \text{если } \neg_t x_i \text{ присутствует в } c_j,\\ (p_{i-1}^j \backslash (E_i^{j-1}(t) \cdot p_i^j)), & \text{если } \neg_t x_i \text{ не присутствует в } c_j; \end{cases}\\
E_i(t) &= E_i^m(t);\\
F_1 &= (E_1(0) \cdot ((E_1(0) \backslash E_1(1)) \cdot (H_1 \backslash r_1)));\\
F_i &= (((E_{i-1}(0) \backslash r_{i-1}) \backslash E_i(0)) \cdot ((E_i(0) \backslash E_i(1)) \cdot (H_i \backslash r_i))),\\
&\quad \text{для } 1 < i < n+1;\\
F_{n+1} &= ((E_n(0) \backslash r_n) \backslash H_{n+1}).
\end{aligned}
$$

Лемма 3.1.1. *Следующие утверждения эквивалентны:*

1. $c_1 \wedge \ldots \wedge c_m$ *выполнима.*
2. $\mathrm{L}(\cdot, \backslash) \vdash F_1 \ldots F_{n+1} \to G$
3. $\mathrm{L}^*(\cdot, \backslash) \vdash F_1 \ldots F_{n+1} \to G$

Раздел 3.2 посвящен доказательству леммы 3.1.1.

В **главе 4** доказывается NP-полнота задачи распознавания выводимости для фрагмента исчисления Ламбека без умножения и его варианта, допускающего пустые антецеденты.

Теорема 3. *Задача распознавания выводимости секвенций в* $\mathrm{L}(\backslash, /)$ *и* $\mathrm{L}^*(\backslash, /)$ *NP-полна.*

Следствие 2. *Задача распознавания принадлежности данного слова языку, порожденному данной грамматикой, основанной на* $\mathrm{L}(\backslash, /)$ *или* $\mathrm{L}^*(\backslash, /)$*, NP-полна.*

Эта теорема доказывается также с помощью сведения задачи SAT к задаче распознавания выводимости в этих фрагментах.

В **разделе 4.1** приводится конструкция, необходимая для такого сведения.

Пусть $p_i^j, q_i^j, a_i^j, b_i^j$, где $0 \le i \le n, 0 < j \le m$ — различные примитивные типы из $\mathbf{P}$.

Определим следующие семейства типов:

$$
\begin{aligned}
G^0 &= (p_0^0 \backslash p_n^0) \\
G^j &= (q_n^j / ((q_0^j \backslash p_0^j) \backslash G^{j-1})) \backslash p_n^j \\
G &= G^m \\
A_i^0 &= (a_i^0 \backslash p_i^0) \\
A_i^j &= (q_i^j / ((b_i^j \backslash a_i^j) \backslash A_i^{j-1})) \backslash p_i^j \\
A_i &= A_i^m \\
E_i^0(t) &= p_{i-1}^0 \\
E_i^j(t) &= \begin{cases} q_i^j / (((q_{i-1}^j / E_i^{j-1}(t)) \backslash p_{i-1}^j) \backslash p_i^{j-1}), & \text{если } \neg_t x_i \text{ есть в } c_j \\ (q_{i-1}^j / (q_i^j / (E_i^{j-1}(t) \backslash p_i^{j-1}))) \backslash p_{i-1}^j, & \text{если } \neg_t x_i \text{ нет в } c_j \end{cases} \\
F_i^j(t) &= (E_i^j(t) \backslash p_i^j) \\
F_i(t) &= F_i^m(t) \\
B_i^0 &= a_i^0 \\
B_i^j &= q_{i-1}^j / (((b_i^j / B_i^{j-1}) \backslash a_i^j) \backslash p_{i-1}^{j-1}) \\
B_i &= B_i^m \backslash p_{i-1}^m
\end{aligned}
$$

Пусть Π_i обозначает следующие последовательности типов:

$$(F_i(0)/(B_i\backslash A_i))\ F_i(0)\ (F_i(0)\backslash F_i(1)).$$

Лемма 4.1.1. *Следующие утверждения эквивалентны:*

$$c_1 \wedge \ldots \wedge c_m \text{ выполнима}$$
$$\mathrm{L}(\backslash,/) \vdash \Pi_1 \ldots \Pi_n \to G$$
$$\mathrm{L}^*(\backslash,/) \vdash \Pi_1 \ldots \Pi_n \to G$$

Раздел 4.2 посвящен доказательству леммы 4.1.1.

В **главе 5** рассматривается фрагмент исчисления Ламбека с одним делением.

В **разделе 5.1** доказывается новый критерий выводимости для этого фрагмента с использованием другого представления секвенций и других доказательных условий.

Рассмотрим отображение $[\![\cdot]\!]' \colon \mathrm{Tp}(\backslash) \to \mathrm{FS}$:

$$[\![p]\!]' = p^{\lfloor 1 \rfloor}_{\lceil 0 \rceil};$$
$$[\![(A\backslash B)]\!]' = [\![B]\!]'([\![A]\!]')^{\langle 0 \rangle};$$

Секвенции $A_1 \ldots A_n \to B$ мы поставим в соответствие строку $\mathbb{W} = [\![A_1]\!]' \ldots [\![A_n]\!]'([\![B]\!]')^{\langle 0 \rangle}$.

Функция π будет определена на всем множестве $\mathcal{P}_{\mathbb{W}}$. Сетью доказательства мы будем называть саму функцию π.

Доказательные условия:

1'. Для всех $\mathbb{A} \in \mathcal{P}_{\mathbb{W}}$ верно, что $\pi^2(\mathbb{A}) = \mathbb{A}$.

2'. Для всех $\mathbb{A} \in \mathcal{P}_{\mathbb{W}}$ верно, что $t(\pi(\mathbb{A})) = t(\mathbb{A})$.

3'. $\mu^-_\pi(\mathbb{A}) \sqsubset \mu^-_\pi(\mathbb{B}) \Rightarrow \mu^+_\pi(\mathbb{A}) \sqsubset \mu^-_\pi(\mathbb{B}) \vee \mu^+_\pi(\mathbb{B}) \sqsubset \mu^+_\pi(\mathbb{A})$.

4'. $d(\mu^+_\pi(\mathbb{A})) = d(\mu^-_\pi(\mathbb{A})) + 1$.

5'. Если $d(\mu^+_\pi(\mathbb{A})) = 2j$ для некоторого $j > 0$, то существует такое $\mathbb{B} \in (\mu^-_\pi(\mathbb{A}), \mu^+_\pi(\mathbb{A}))_\sqsubset$, что $d(\mathbb{B}) < 2j$.

6'. Если $d(\mu^+_\pi(\mathbb{A})) = 2j$ для некоторого $j > 0$, то либо существует такое $\mathbb{B} \in (\mu^-_\pi(\mathbb{A}), \mu^+_\pi(\mathbb{A}))_\sqsubset$, что $d(\mathbb{B}) < 2j$, либо

$$\pi(\mathbb{A}) = \max_\sqsubset\{\mathbb{B} \mid \forall \mathbb{C} \in (\mathbb{A}, \mathbb{B}]_\sqsubset d(\mathbb{C}) > d(\mathbb{A})\}.$$

Теорема 4. $\mathrm{L}(\backslash) \vdash A_1 \ldots A_n \to B$, *если и только если* $n > 0$ *и для*

$$\mathbb{W} = [\![A_1]\!]' \ldots [\![A_n]\!]'([\![B]\!]')^{\langle 0 \rangle}$$

существует сеть доказательства π, *удовлетворяющая доказательным условиям (1')-(5').*

Теорема 5. $\mathrm{L}^*(\backslash) \vdash A_1 \ldots A_n \to B$, *если и только если для*

$$\mathbb{W} = [\![A_1]\!]' \ldots [\![A_n]\!]'([\![B]\!]')^{\langle 0 \rangle}$$

существует сеть доказательства π, *удовлетворяющая доказательным условиям (1')-(4') и (6').*

В **разделе 5.2** строится полиномиальный алгоритм, позволяющий определять принадлежность слова языку, порожденному данной грамматикой, за полиномиальное время, и доказывается его корректность.

Пусть $(\Sigma, \mathbf{P}, R, B)$ — грамматика Ламбека, основанная на $\mathrm{L}(\backslash)$ или $\mathrm{L}^*(\backslash)$.

Размером грамматики назовем число $|[\![B]\!]'| + \sum_{a \in \Sigma} \sum_{A \in R(a)} |[\![A]\!]'|$.

Теорема 6. *Существует алгоритм, который по данному слову и данной грамматике, основанной на* $\mathrm{L}(\backslash)$ *или* $\mathrm{L}^*(\backslash)$, *распознает принадлежность этого слова языку, порожденному данной грамматикой, за время, ограниченное полиномом от длины слова и размера грамматики.*

Автор благодарит своего научного руководителя профессора М. Р. Пентуса за постановку задачи, поддержку и внимание к работе.

Работы автора по теме диссертации

[1] Саватеев Ю. В. Распознавание выводимости для исчисления Ламбека с одним делением // Вестник Московского университета. Серия 1, Математика. Механика. — 2009. — № 2. — С. 59—62.

[2] Savateev Y. Lambek grammars with one division are decidable in polynomial time // Computer Science — Theory and Applications / Editors E.A. Hirsch et al.. — Berlin: Springer, 2008. — P. 273—282. — (Lecture Notes in Computer Science; vol. 5010).

[3] Savateev Y. Product-free Lambek calculus is NP-complete // Logical Foundations of Computer Science, International Symposium, LFCS 2009, Deerfield Beach, FL, USA, January 3—6, 2009. Proceedings / Editors S. N. Artemov and A. Nerode. — Berlin: Springer, 2009. — P. 380—394. — (Lecture Notes in Computer Science; vol. 5407).