DOI: 10.5862/JCSTCS.234.7
УДК 004.832.32

В.А. Павлов, В.Г. Пак

ЭКСПЕРИМЕНТАЛЬНАЯ ПРОГРАММА ДЛЯ ДОКАЗАТЕЛЬСТВА ТЕОРЕМ ИНТУИЦИОНИСТСКОЙ ЛОГИКИ ОБРАТНЫМ МЕТОДОМ МАСЛОВА

V.A. Pavlov, V.G. Pak

AN EXPERIMENTAL COMPUTER PROGRAM FOR AUTOMATED REASONING IN INTUITIONISTIC LOGIC USING THE INVERSE METHOD

Статья посвящена обратному методу Маслова, который подходит для автоматизации доказательств в различных логических исчислениях: логика высказываний, классическая логика первого порядка, интуиционистская логика, модальные логики и т. д. Приведен обзор основных публикаций по обратному методу, рассмотрено разработанное авторами исчисление обратного метода для интуиционистской логики первого порядка. Предложены адаптированные и оригинальные стратегии оптимизации для этого исчисления. Рассмотрены алгоритм логического вывода в полученном исчислении и разработанная на его основе программа автоматического доказательства теорем WhaleProver. Приведены результаты сравнения разработанной программы с существующими аналогами на задачах из библиотеки ILTP.

АВТОМАТИЧЕСКОЕ ДОКАЗАТЕЛЬСТВО ТЕОРЕМ; ЛОГИЧЕСКИЙ ВЫВОД; ОБРАТНЫЙ МЕТОД; МЕТОД МАСЛОВА; ИНТУИЦИОНИСТСКАЯ ЛОГИКА.

We discuss the inverse method of automated theorem-proving that was invented by S. Maslov. The inverse method can be applied to various logics: propositional logic, first-order logic, modal logics, intuitionistic logic, etc. In the current article, we present an overview of the key publications on the inverse method, describe in detail an inverse method calculus for first-order intuitionistic logic. We propose adapted as well as original optimizing strategies for the developed calculus. We discuss a proof search algorithm for the proposed calculus and our program implementation named WhaleProver. We compare WhaleProver with state-of-the-art intuitionistic theorem provers on problems from the ILTP library, which is a common benchmarking library for testing intuitionistic theorem provers.

AUTOMATED THEOREM PROVING; SEQUENT CALCULUS; INVERSE METHOD; INTUITIONISTIC LOGIC; ILTP.

Автоматическое доказательство теорем (АДТ) – активно развивающееся направление математической логики и искусственного интеллекта. Основные задачи АДТ заключаются в разработке методик, алгоритмов и компьютерных программ (*систем АДТ*), автоматизирующих доказательство утверждений в той или иной формальной теории.

Системы АДТ применяются не только в математике как «умные помощники» ученых, но и для решения актуальных практических задач: верификации программного, аппаратного обеспечения и сетевых протоколов, планирования, представления знаний (в частности, логического вывода в базах знаний и семантических сетях), обработки естественного языка и т. д.

Читателям, не знакомым близко с темой автоматического доказательства теорем, а также желающим расширить свои знания в этой области, мы можем порекомендовать книги по теме [5, 12, 25].

Автоматический логический вывод в интуиционистской логике имеет особое значение для верификации программного обеспечения благодаря существованию изоморфизма Карри–Ховарда. Естественным приложением интуиционистской логики в математике является формализация

конструктивных математических теорий.

Следует отметить, что наиболее разработанный метод логического вывода для классической логики первого порядка – метод резолюций – в чистом виде неприменим к интуиционистской логике. Большинство систем АДТ для интуиционистской логики первого порядка используют табличные методы логического вывода, однако существующие реализации пока не способны конкурировать по эффективности с наиболее совершенными системами для классической логики.

В связи с приведенной выше проблемой, особенный научный и практический интерес представляют исследования обратного метода логического вывода, предложенного советским ученым С.Ю. Масловым еще в 1964 г., но активно применяющегося в практических системах АДТ лишь в течение последних лет.

Определения и используемые обозначения

В статье используется стандартный язык логики первого порядка, с символами логических операций $\neg$, $\vee$, $\wedge$, $\supset$; кванторами $\forall$ и $\exists$; логической константой $\perp$; предикатными символами P, Q, R и т. д.; переменными x, y, z и т. д.; функциональными символами f, g, h; символами для произвольных термов r, s, t; символами для произвольных формул A, B, C и т. д.

Интуиционистская логика первого порядка представляет собой формализацию интуиционистского (или конструктивного) типа рассуждений, в которой стандартные логические связки интерпретируются отличным от классической логики образом. Так, интуиционистское доказательство утверждения $\exists x\, P(x)$ заключается в предоставлении конкретного примера x такого, что $P(x)$, или, по крайней мере, указывает метод, позволяющий в принципе найти такой пример. В интуиционистской логике неприемлем закон исключенного третьего $A \vee \neg A$ и закон двойного отрицания $(\neg\neg A) \supset A$.

Вхождение переменной x в выражение называется *связанным*, если оно совпадает с конструкцией вида $\forall x$ или $\exists x$, либо входит в область действия такого квантора. Вхождение переменной называется *свободным*, если оно не связано. Переменная свободна в выражении E, если она входит свободно в E. Переменная связана в E, если она входит связанно в E.

Замкнутая формула – формула, которая не содержит свободных переменных. *Ректифицированная формула* – замкнутая формула, в которой все кванторы связывают разные переменные.

Подстановка вместо переменных $x_1, ..., x_n$ – это выражение вида $\{x_1/t_1, ..., x_n/t_n\}$, где все переменные x_i различны и $x_i \neq t_i$ для всех $i = 1, .., n$. Для произвольного выражения E и подстановки $\theta = \{x_1/t_1, ..., x_n/t_n\}$, выражение $E\theta$ обозначает результат одновременной подстановки термов $t_1, ..., t_n$ в места всех свободных вхождений переменных $x_1, ..., x_n$ в выражении E.

Запись σ_{-x} обозначает подстановку, полученную из σ «вычеркиванием» элемента с $x_i = x$ (если таковой имеется).

Наиболее общий унификатор подстановок σ и τ – это наиболее общий унификатор (см. подробнее [12]) упорядоченных наборов $(x_1\sigma, ..., x_n\sigma)$ и $(x_1\tau, ..., x_n\tau)$, где $\{x_1, ..., x_n\}$ – объединение областей определения σ и τ.

Свободной подформулой формулы F является любая формула G, входящая в F. *Подформулами* F являются все такие формулы G', которые получаются из ее подформул применением некоторой подстановки вместо переменных. Для фиксированной формулы F *знаки* ее подформул определяются так: положительный знак имеют подформулы, не входящие в подформулы вида $\neg A$ или в левую часть подформул вида $A \supset B$, либо имеющие четное число вхождений в подформулы указанного вида; отрицательный знак имеют все остальные подформулы.

Секвенция – это условное суждение вида $A_1, ..., A_n \vdash B_1, ..., B_m$, где A_i $(i = 1, .., n)$ и B_j $(j = 1, .., m)$ – формулы. Секвенция интерпретируется как утверждение «если A_1 и ... и A_n истинны, то B_1 или ... или B_m истинны».

Секвенциальное исчисление – логическое исчисление, выводимыми объектами в ко-

тором являются секвенции.

Свойство подформульности логического исчисления выполняется, если для каждой выводимой в исчислении формулы *F* существует доказательство, содержащее только подформулы *F*.

Обратный метод Маслова

Историческая справка. Обратный метод был изобретен советским математиком С.Ю. Масловым в 1964 г. [6]. Свое название метод получил благодаря тому, что строит логический вывод в направлении «сверху вниз» (от аксиом к доказываемой формуле), обратном традиционному направлению поиска вывода в секвенциальных исчислениях.

Первый вариант обратного метода [6] был предназначен для доказательства предваренных формул логики первого порядка. Впоследствии С.Ю. Маслов обобщил свой метод на произвольные *секвенциальные исчисления* без правила сечения, обладающие свойством *подформульности* [7]. Общая схема метода может быть конкретизирована для любой подходящей логики.

Долгое время обратный метод оставался в тени метода резолюций [12, 25] и табличных методов [1, 4, 5, 14]. Развитием метода занималась лишь небольшая группа коллег Маслова. Однако в последние годы интерес к обратному методу стал постепенно возрастать, в том числе и за рубежом.

Отметим некоторые преимущества обратного метода, в частности, важные при автоматизации логического вывода в интуиционистской логике:

1) метод эффективно использует свойство подформульности, позволяя избежать порождения множества избыточных секвенций, не имеющих отношения к самой формуле;

2) хорошо подходит для автоматизации логического вывода в неклассических логиках (интуиционистская логика, различные модальные логики и т. д.);

3) строит вывод в естественном направлении: от аксиом к доказываемой формуле;

4) метод лишен ряда недостатков, характерных для табличных методов: является локальным, не требует использования механизмов отката в случае неудачи, контроля над возникновением циклов;

5) имеет широкие теоретические возможности для исследования выводимых классов формул.

Впоследствии С.Ю. Масловым и другими учеными были построены конкретизации общей схемы обратного метода для различных логических исчислений. В приложениях к [12] изложена относительно простая формулировка обратного метода для предваренных формул логики первого порядка. В более современной, но близкой по содержанию статье [19] приведена альтернативная формулировка с кратким доказательством полноты. В [15] приведены «резолютивноподобные» (т. е. похожие на резолютивные методы, resolution-like) исчисления обратного метода для логики высказываний и классической логики первого порядка. Статья также содержит важный исторический обзор развития идей обратного метода.

Работа [13], наряду с [7], на настоящее время может считаться одним из наиболее значимых и фундаментальных трудов по обратному методу. В ней ее авторы, А. Дегтярёв и А. Воронков, обобщили результаты работ по обратному методу за последние десятилетия и продемонстрировали, как использовать «универсальный рецепт» [11] для построения различных исчислений обратного метода.

Обратный метод Маслова, как и метод резолюций, оказался недостаточно эффективным без использования специальных *стратегий оптимизации*, направленных на сужение пространства поиска вывода. Ранние работы, посвященные стратегиям для обратного метода (С.Ю. Маслов использует термин «тактики»), включают [8–10].

А. Воронков в статье [27] предложил общий подход адаптации некоторых стратегий из метода резолюций для обратного метода и доказал несколько общих теорем, определяющих стратегии сужения пространства поиска вывода для обратного метода. В той же работе автор продемонстрировал, как могут выглядеть конкретизации этих стратегий, на примере классической

логики первого порядка и модальной логики S4. В статье указано, что общий подход можно применить и к другим логикам, в частности, к интуиционистской логике.

Обратному методу для интуиционистской логики первого порядка посвящены работы [18, 23 и 17].

Г. Минц в работе [18] предложил несколько стратегий для интуиционистской логики (высказываний и первого порядка). Однако в той части статьи, которая посвящена стратегиям для интуиционистской логики первого порядка, рассмотрены стратегии только для «резолютивноподобной» модификации обратного метода.

Т. Таммет предложил исчисление обратного метода и несколько стратегий для интуиционистской логики первого порядка [23].

В [17] рассмотрено применение стратегий, носящих название *поляризации* (polarization) и *фокусировки* (focusing), к интуиционистскому исчислению обратного метода.

Для классической логики в разные периоды времени было разработано несколько реализаций обратного метода, например, [2, 26].

Для интуиционистской логики первого порядка также существуют реализации. В [23] Т. Таммет реализовал систему АДТ для интуиционистской логики на базе своей программы Gandalf для классической логики. К сожалению, корректность этой реализации подвергается сомнению [24]. Согласно [13], используемое в [23] интуиционистское исчисление не обладает свойством полноты. В другой работе [17] описана эффективная реализация, но при этом не используются многие важные теоретические результаты, полученные в работах других указанных выше авторов.

Все изложенное выше раскрывает актуальную потребность разработки эффективных и корректных алгоритмов вывода формул интуиционистской логики первого порядка, реализующих наиболее существенные и универсальные достижения в теории логического вывода обратным методом Маслова. Ликвидация указанного пробела между теорией и практикой позволит увеличить эффективность алгоритмов и расширить область применения систем АДТ для интуиционистской логики первого порядка.

Многосукцедентное исчисление обратного метода для вывода формул интуиционистской логики первого порядка. Для построения исчисления мы применяем «универсальный рецепт автоматической дедукции» ([11], также [13]). Согласно этому рецепту, на первом шаге нужно выбрать какое-либо секвенциальное исчисление, предназначенное для построения выводов «снизу вверх», и построить на его основе исчисление обратного метода для вывода *замкнутых* формул в направлении «сверху вниз». Затем следует определить свойство подформульности и процедуру унификации, после чего перейти от исчисления для вывода замкнутых формул к полноценному исчислению для вывода произвольных формул.

В качестве базового интуиционистского исчисления в [13] взято исчисление *G*3 из [5], в котором выводимые секвенции могут иметь не более одной формулы в сукцеденте. Мы выбрали в качестве базового многосукцедентное исчисление *m-G3i* из [25], представляющее собой модификацию исчисления GHPC, предложенного А.Г. Драгалиным [3].

В данной статье для экономии места мы опускаем изложение промежуточного исчисления для замкнутых формул. Его нетрудно восстановить из приведенного ниже исчисления *m-G3i-inv*.

Пусть F – *ректифицированная* формула интуиционистской логики первого порядка, доказательство которой требуется вывести. Исчисление обратного метода строится индивидуально для формулы F таким образом, чтобы в доказательстве участвовали только подформулы F.

Выводимые объекты исчисления – это *секвенции с подстановками*:

$$A_1 \circ \theta_1, \ldots, A_n \circ \theta_n \vdash B_1 \circ \sigma_1, \ldots, B_m \circ \sigma_m,$$

где A_i ($i = 1..n$) – отрицательные свободные подформулы F; B_i ($i = 1..m$) – положительные свободные подформулы F; θ_i ($i = 1..n$) и σ_i ($i = 1..m$) – подстановки; символ «$\circ$» обозначает операцию применения подстанов-

ки. Секвенции с подстановками определяются однозначно с точностью до порядка следования формул и могут содержать повторяющиеся элементы.

На рис. 1 представлены правила вывода (включая аксиомы) исчисления *m-G3i-inv*. Во всех правилах посылки и заключения являются секвенциями с подстановками. В *Px* каждый из символов *P* и *Q* обозначает атомарную подформулу формулы *F* или подформулу, являющуюся логической константой $\bot$; подстановка ρ переименовывает в *P* переменные, совпадающие с переменными из *Q*; подстановка θ – наиболее общий унификатор формул $P\rho$ и *Q*. Во всех правилах посылки не имеют общих переменных как друг с другом, так и с множеством переменных формулы *F*. Подстановка θ – наиболее общий унификатор подстановок σ_1 и σ_2. Γ и Δ – произвольные последовательности формул, возможно пустые. В правилах $L\exists$ и $R\forall$ должно выполняться *ограничение на собственную переменную*: $x\sigma$ – это переменная, которая не входит *свободно* в заключение правил.

Кроме приведенных правил, в исчислении действует неявное правило переименования, разрешающее переименовывать переменные в секвенциях.

Теорема. Полнота исчисления *m-G3i-inv. Пусть F – замкнутая ректифицированная формула интуиционистской логики. Секвенция* $\vdash F \circ \varepsilon$ *выводима в исчислении m-G3i-inv тогда и только тогда, когда секвенция* $\vdash F$ *выводима в исчислении GHPC.*

При доказательстве теоремы могут быть использованы идеи из [13], где дано доказательство полноты односукцедентного исчисления для вывода формул интуиционистской логики. Отметим, что полнота исчисления GHPC доказана в [3].

Полученное нами исчисление отличается от интуиционистского исчисления из [13] и от ряда других, встречающихся в публикациях по обратному методу [17, 23], следующим:

- исчисление *m-G3i-inv* является *многосукцедентным*, что позволяет сократить

$$Px\quad P\circ\rho\theta\vdash Q\circ\theta \qquad L\bot\quad \bot\vdash$$

$$LC\quad \frac{\Gamma, A\circ\sigma_1, A\circ\sigma_2\vdash\Delta}{\Gamma\theta, A\circ\sigma_1\theta\vdash\Delta\theta} \qquad RC\quad \frac{\Gamma\vdash\Delta, A\circ\sigma_1, A\circ\sigma_2}{\Gamma\theta\vdash\Delta\theta, A\circ\sigma_1\theta}$$

$$L\wedge_1\quad \frac{\Gamma, A\circ\sigma\vdash\Delta}{\Gamma, A\wedge B\circ\sigma\vdash\Delta} \qquad L\wedge_2\quad \frac{\Gamma, B\circ\sigma\vdash\Delta}{\Gamma, A\wedge B\circ\sigma\vdash\Delta}$$

$$R\wedge\quad \frac{\Gamma_1\vdash\Delta_1, A\circ\sigma_1 \quad \Gamma_2\vdash\Delta_2, B\circ\sigma_2}{\Gamma_1\theta, \Gamma_2\theta\vdash\Delta_1\theta, \Delta_2\theta, A\wedge B\circ\sigma_1\theta} \qquad L\vee\quad \frac{\Gamma_1, A\circ\sigma_1\vdash\Delta_1 \quad \Gamma_2, B\circ\sigma_2\vdash\Delta_2}{\Gamma_1\theta, \Gamma_2\theta, A\vee B\circ\sigma_1\theta\vdash\Delta_1\theta, \Delta_2\theta}$$

$$R\vee_1\quad \frac{\Gamma\vdash\Delta, A\circ\sigma}{\Gamma\vdash\Delta, A\vee B\circ\sigma} \qquad R\vee_2\quad \frac{\Gamma\vdash\Delta, B\circ\sigma}{\Gamma\vdash\Delta, A\vee B\circ\sigma}$$

$$L\supset\quad \frac{\Gamma_1\vdash\Delta_1, A\circ\sigma_1 \quad \Gamma_2, B\circ\sigma_2\vdash\Delta_2}{\Gamma_1\theta, \Gamma_2\theta, A\supset B\circ\sigma_1\theta\vdash\Delta_1\theta, \Delta_2\theta}$$

$$R\supset_1\quad \frac{\Gamma\vdash B\circ\sigma}{\Gamma\vdash A\supset B\circ\sigma} \qquad R\supset_2\quad \frac{\Gamma, A\circ\sigma\vdash}{\Gamma\vdash A\supset B\circ\sigma}$$

$$R\supset_3\quad \frac{\Gamma, A\circ\sigma_1\vdash A\supset B\circ\sigma_2}{\Gamma\theta\vdash A\supset B\circ\sigma_2\theta}$$

$$L\forall\quad \frac{\Gamma, A\circ\sigma\vdash\Delta}{\Gamma, \forall xA\circ\sigma_{-x}\vdash\Delta} \qquad R\forall\quad \frac{\Gamma\vdash A\circ\sigma}{\Gamma\vdash\forall xA\circ\sigma_{-x}}$$

$$L\exists\quad \frac{\Gamma, A\circ\sigma\vdash\Delta}{\Gamma, \exists xA\circ\sigma_{-x}\vdash\Delta} \qquad R\exists\quad \frac{\Gamma\vdash\Delta, A\circ\sigma}{\Gamma\vdash\Delta, \exists xA\circ\sigma_{-x}}$$

Рис. 1. Исчисление *m-G3i-inv*

число правил вывода;

• в исчислении используется логическая константа $\bot$, а не связка $\neg$, отрицание при этом определяется через импликацию: $\neg A \equiv A \supset \bot$.

Стратегии оптимизации для полученного исчисления. Для разработки эффективного алгоритма автоматического логического вывода одного исчисления недостаточно: необходимо дополнить его стратегиями оптимизации, позволяющими уменьшить размер дерева вывода.

Как было отмечено ранее в обзоре, в [27] А. Воронков сформулировал общие условия к нескольким стратегиям для обратного метода, но не разработал стратегии для интуиционистской логики. Данный раздел посвящен изложению стратегий, адаптированных к интуиционистскому исчислению *m-G3i-inv*.

Большинство стратегий используют отношение поглощения на множестве секвенций, позволяющее определить, какие секвенции являются более общими по сравнению с другими.

Определение. *Отношение поглощения* $\prec_I$. В исчислении *m-G3i-inv* секвенция с подстановками $S' = \Gamma' \vdash \Delta'$ поглощает секвенцию с подстановками $S = \Gamma \vdash \Delta$ (пишется $S \prec_I S'$) тогда и только тогда, когда существует подстановка τ такая, что

1) для каждой формулы $\varphi' \circ \sigma' \in S'$ найдется такая формула $\varphi \circ \sigma \in S$, что φ является (свободной) подформулой φ' и $(\sigma' \circ \tau)\big|_{free\,(\varphi')} \equiv \sigma\big|_{free\,(\varphi')}$ (назовем формулу $\varphi \circ \sigma$ *конкретизирующим образом* формулы $\varphi' \circ \sigma'$ в секвенции S);

2) для каждой пары формул $\Phi'_1 = \varphi' \circ \sigma'_1$ и $\Phi'_2 = \varphi' \circ \sigma'_2$ из секвенции S' соответствующие им конкретизирующие образы в секвенции S различны;

3) если $\varphi' \circ \sigma' \in \Delta'$, то соответствующий ей конкретизирующий образ $\varphi \circ \sigma \in \Delta$ и выполняется хотя бы одно из условий:

1. $\varphi = \varphi'$ или формула φ не имеет вид $A \supset B$;
2. не существует формулы φ'' вида $A \supset B$ или $\forall x\, A$ такой, что $\varphi \neq \varphi''$, φ является свободной подформулой φ'', φ'' является свободной подформулой φ';
3. Секвенция S не имеет вид $\bot \vdash$.

Адаптированная стратегия поглощения секвенций (subsumption) определяется так: разрешается удалять из пространства поиска вывода секвенцию S, если уже выведена такая секвенция S', что $S \prec_I S'$.

Приведенное выше отношение поглощения является более общим по сравнению с формулировками, предложенными в [17, 18, 23], поэтому позволяет устранять больше избыточных секвенций.

Основное отличие отношения $\prec_I$ от отношения $\prec_C$ для классической логики, предложенного в [27], заключается в дополнительных ограничениях 2 и 3 (см. определение выше). Учитывая это различие, на основе стратегий для классической логики из [27] можно сформулировать адаптированные стратегии оптимизации для исчисления *m-G3i-inv*:

1) стратегия упрощения немаксимальных секвенций;

2) стратегия удаления «бесполезных» (useless) секвенций, основанная на множестве U_1 из [27].

Также в данной работе мы используем следующую стратегию: если в секвенции встречаются подстановки, в которых различные собственные переменные (т. е. такие, которые участвуют в правилах $L\exists$ и $R\forall$) заменяются на одну и ту же переменную, то такую секвенцию можно удалить. Соответствующее данной стратегии множество бесполезных секвенций назовем множеством U_3, и тем же символом обозначим саму стратегию. Стратегия U_3 является ослаблением стратегии использования допустимых наборов и удаления недопустимых (см. [2, 6, 7]), при этом позволяет устранить достаточное число избыточных секвенций при экономных затратах ресурсов (памяти и времени).

Полезно также оптимизировать правила сокращения *LC* и *RC*: применять их неявно к каждой вновь порожденной секвенции, а в случае их обратимости замещать исходную секвенцию ее сокращенным вариантом. Эта оптимизация не является принципиально новой, похожие идеи есть в [23].

Все используемые в работе стратегии оптимизации являются совместимыми, поскольку согласуются с отношением по-

глощения $\prec_I$. Для доказательства полноты стратегий достаточно показать, что они удовлетворяют соответствующим общим определениям из [27].

Экспериментальная программа для автоматического доказательства теорем в интуиционистской логике первого порядка

Мы расширили разработанную ранее систему АДТ для классической логики предикатов [20, 21], добавив возможность доказывать формулы интуиционистской логики в исчислении *m-G3i-inv*. Разработанная система АДТ называется WhaleProver (whale – кит). Программа разработана с применением объектно-ориентированного подхода на языке C++.

В программе используется адаптированный вариант алгоритма, называемого в англоязычной литературе Otter loop или given clause algorithm [16], и используемый в современных резолютивных системах АДТ, таких как Prover9 (ранее Otter) и E. Согласно этому алгоритму, все участвующие в доказательстве секвенции делятся на два списка: активные секвенции и использованные секвенции.

Полный алгоритм логического вывода, реализованный в программе, включает в себя несколько основных шагов.

1. Переменные в исходной замкнутой формуле переименовываются так, чтобы все кванторы связывали разные переменные. Устраняются кванторы, связывающие неиспользуемые переменные. Получается «ректифицированная» формула *F*.

2. Порождаются все возможные аксиомы исчисления и помещаются в конец списка активных секвенций.

3. Каждая активная секвенция «упрощается», т. е. к ней применяются все приведенные в предыдущем разделе стратегии оптимизации.

4. Из активного списка выбирается секвенция. Если она не поглощается никакой из использованных секвенций, выполняется шаг 5. Иначе секвенция удаляется, и шаг 4 повторяется. Если список пуст, алгоритм завершает работу и выдает результат: «формула не является теоремой».

5. Выбранная секвенция переносится в список использованных секвенций. Применяются все правила вывода, в которых хотя бы одна из посылок совпадает с выбранной секвенцией.

6. Каждая порожденная на шаге 5 секвенция «упрощается» (см. шаг 3), оставшиеся секвенции помещаются в конец активного списка.

7. Если среди вновь выведенных секвенций встречается $\vdash F$, алгоритм завершает работу с результатом «формула является теоремой», при этом вывод формулы *F* восстанавливается в обратном порядке. В противном случае алгоритм возвращается к шагу 4.

Был проведен ряд экспериментов с разработанной АДТ WhaleProver на задачах из библиотеки ILTP [22] версии 1.1.2. Всего в библиотеке 2550 задач, из которых 1787 пока не решены. Эксперименты проводились на компьютере с процессором Intel Core 2 Duo 2.67 ГГц, ОС Windows 7 и 3 Гб ОЗУ.

На репрезентативной выборке из 253 задач различной сложности были проведены эксперименты по сравнению стратегий оптимизации для обратного метода. Эффективность стратегий определялась по критериям:

1) средний размер пространства поиска вывода (объем используемой памяти может считаться пропорциональным этому параметру);

2) среднее время доказательства;

3) средняя длина доказательства;

4) средняя глубина вывода.

Результаты экспериментов показали, что по основным критериям 1 и 2 эффективность адаптированной стратегии поглощения более чем в два раза превосходит эффективность стратегий поглощения из работ [17, 18, 23].

Использование адаптированной стратегии упрощения немаксимальных секвенций совместно со стратегией поглощения позволяет увеличить эффективность по всем критериям в четыре раза и более, по сравнению с использованием только стратегии поглощения. В тех же условиях оптимизация правил сокращения позволяет получить выигрыш по критериям 1 и 2

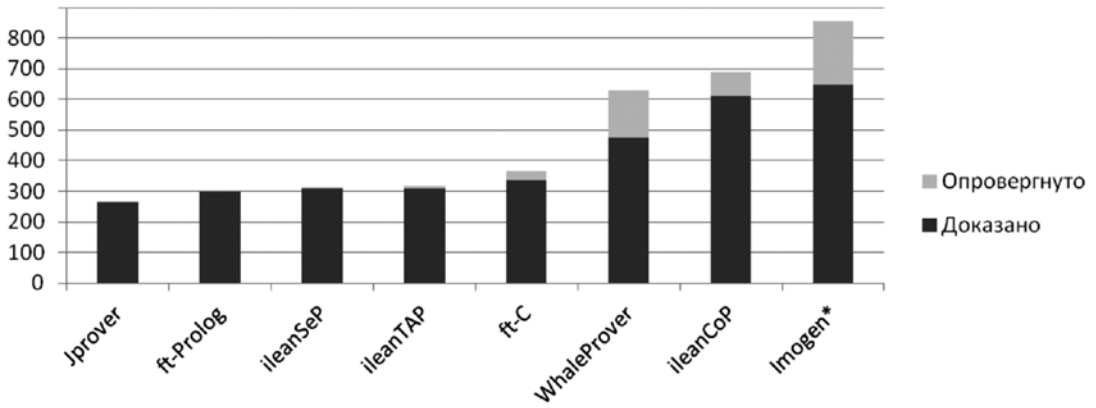

Рис. 2. Сравнение количества решенных задач системами АДТ

примерно в 1,5 раза. Стратегия U_3 позволяет сэкономить в среднем 15 % памяти и времени, а на ряде задач дает выигрыш в несколько раз. При этом адаптированная стратегия удаления бесполезных секвенций не оказывает значительного влияния на оцениваемые показатели.

На рис. 2 приведены результаты сравнения на задачах из ILTP системы АДТ WhaleProver с лучшими системами АДТ для интуиционистской логики первого порядка. При тестировании нашей программы на каждую задачу был выделен лимит времени 100 с. Другие системы АДТ тестировались на отличных конфигурациях компьютеров (см. подробнее [17, 24]) и с лимитом времени 600 с. Несмотря на эти различия, рис. 2 демонстрирует качественный уровень разработанной системы АДТ.

Для всех систем, кроме Imogen*, на сайте ILTP [24] имеется детальная информация по решенным ими задачам. В таблице приведено подробное сравнение результатов системы АДТ WhaleProver с этими системами.

В таблице нижние четыре строки содержат количество решенных задач в областях: KRS – представление знаний, NLP – обработка естественного языка, SWV – верификация ПО, GEJ – конструктивная геометрия Яна вон Плато. В трех из них программа WhaleProver решила больше задач, чем другие системы АДТ. В доменах KRS и NLP программа решила соответственно 24 и 36 задач, которые другие программы решить не смогли. Кроме того, система АДТ WhaleProver смогла опровергнуть значительно больше ложных утверждений. В целом разработанная система решила 94 задачи, которые не были решены до этого ни одной системой из ILTP.

Детальные результаты сравнения систем АДТ

	JProver	ft-Prolog	ft-C	ileanSeP	ileanTAP	ileanCoP	WhaleProver
Решено задач	268	299	364	313	315	690	628
Доказано	264	299	334	309	311	610	476
Опровергнуто	4	0	30	4	4	80	152
Решено задач (таймаут 100 с)	262	295	364	301	312	647	628
KRS	33	26	26	18	19	42	58
NLP	7	7	7	3	11	3	42
SWV	1	48	48	82	49	132	57
GEJ	5	13	15	9	11	70	73

В данной статье мы рассмотрели один из методов автоматического доказательства теорем – обратный метод Маслова. В статье сделан обзор ключевых работ по обратному методу, сформулировано оригинальное исчисление обратного метода для интуиционистской логики первого порядка. Предложены адаптированные стратегии оптимизации для этого исчисления. Описан алгоритм доказательства теорем в полученном исчислении и разработанная на его основе система АДТ WhaleProver.

В соответствии с признанными мировыми практиками проведена апробация разработанной системы АДТ на задачах из библиотеки ILTP. Приведены результаты сравнения стратегий оптимизации, а также сравнения с существующими системами АДТ. Приведенные данные демонстрируют важный результат: система АДТ на базе обратного метода при использовании подходящих стратегий оптимизации позволяет расширить границы применения систем АДТ для интуиционистской логики. Для ряда задач система АДТ WhaleProver позволяет значительно сократить время доказательства. Программа решила почти 100 задач, не поддающихся решению других систем АДТ для интуиционистской логики за разумное время. Особенно много новых результатов относится к конструктивной геометрии и таким областям искусственного интеллекта, как представление знаний и обработка естественного языка.

Все сказанное выше позволяет рекомендовать разработанную систему АДТ в дополнение к уже существующим системам АДТ для интуиционистской логики, для формализации конструктивных математических теорий и решения актуальных задач, возникающих в различных направлениях искусственного интеллекта.

СПИСОК ЛИТЕРАТУРЫ

1. **Бет Э.** Метод семантических таблиц // Математическая теория логического вывода. М.: Наука, 1967. С. 191–199.

2. **Давыдов Г.В., Маслов С.Ю., Минц Г.Е., Оревков В.П., Слисенко А.О.** Машинный алгорифм установления выводимости на основе обратного метода // Исследования по конструктивной математике и математической логике. Зап. науч. сем. ЛОМИ. 1969. Т. 16. С. 8–19.

3. **Драгалин А.Г.** Математический интуиционизм. Введение в теорию доказательств. М.: Наука, 1979.

4. **Кангер С.** Упрощенный метод доказательства для элементарной логики // Математическая теория логического вывода. М.: Наука, 1967. С. 200–207.

5. **Клини С.** Математическая логика. М.: Мир, 1973.

6. **Маслов С.Ю.** Обратный метод установления выводимости в классическом исчислении предикатов // ДАН СССР. 1964. Т. 159. № 1. С. 17–20.

7. **Маслов С.Ю.** Обратный метод установления выводимости для логических исчислений // Труды МИАН СССР. 1968. Т. 98. С. 26–87.

8. **Маслов С.Ю.** Тактики поиска вывода, основанные на унификации порядка членов в благоприятном наборе// Зап. науч. сем. ЛОМИ. 1969. Т. 16. С. 126–136.

9. **Маслов С.Ю.** Связь между тактиками обратного метода и метода резолюций // Зап. науч. сем. ЛОМИ. 1969.Т. 16. С. 137–146.

10. **Маслов С.Ю.** Обратный метод и тактики установления выводимости для исчисления с функциональными знаками // Труды МИАН СССР. 1972. Т. 121. С. 14–56.

11. **Маслов С.Ю.** О поиске вывода в исчислениях общего типа // Зап. науч. сем. ЛОМИ. 1972. Т. 32. С. 59–65.

12. **Чень Ч., Ли Р.** Математическая логика и автоматическое доказательство теорем. Пер. с англ. М.: Наука, 1983. 360 с.

13. **Degtyarev A., Voronkov A.** The inverse method // Handbook of Automated Reasoning. Elsevier, Amsterdam, 2001. Vol. 1. Pp. 179–272.

14. **Hähnle R.** Tableaux and Related Methods // Handbook of Automated Reasoning. Elsevier, Amsterdam, 2001. Vol. 1. Pp. 101–177.

15. **Lifschitz V.** What is the inverse method? // Journal of Automated Reasoning. 1989. No. 5(1). Pp. 1–23.

16. **McCune W.** Prover9 and Mace4 [электронный ресурс]/ URL: http://www.cs.unm.edu/~mccune/Prover9, 2005-2010. (дата обращения: 19.12.2015).

17. **McLaughlin S., Pfenning F.** Efficient Intuitionistic Theorem Proving with the Polarized Inverse Method // CADE-22. LNCS. Springer, Heidelberg, 2009. Vol. 5663. Pp. 230–244.

18. **Mints G.** Resolution strategies for the Intuitionistic Logic // Constraint Programming. NATO

ASI Series. Springer, Heidelberg, 1994. Vol. 131. Pp. 289–311.

19. **Mints G.** Decidability of the Class E by Maslov's Inverse Method. Essays Dedicated to Yuri Gurevich on the Occasion of His 70th Birthday // LNCS. Springer, Heidelberg, 2010. Vol. 6300. Pp. 529–537.

20. **Pavlov V., Schukin A., Cherkasova T.** Exploring Automated Reasoning in First-Order Logic: Tools, Techniques and Application Areas // 4th Internat. Conf. KESW 2013. CCIS. Springer, Heidelberg, 2013. Vol. 394. Pp. 102–116.

21. **Pavlov V., Pak V.** The Inverse Method and First-Order Logic Theorem Proving // Nonlinear Dynamics and Applications. 2014. Vol. 20. Pp. 127–135.

22. **Raths T., Otten J., Kreitz C.** The ILTP Library: Benchmarking Theorem Provers for Intuitionistic Logic // Automated Reasoning with Analytic Tableaux and Related Methods. TABLEAUX 2005. LNAI. Springer Verlag, 2005. Vol. 3702. Pp. 333–337.

23. **Tammet T.** A resolution theorem prover for intuitionistic logic // CADE-13. LNCS. Springer, Heidelberg, 1996. Vol. 1104. Pp. 2–16.

24. The ILTP Library. Provers and Results [электронный ресурс]/ URL: http://www.cs.uni-potsdam.de/ti/iltp/results.html. (дата обращения: 19.12.2015).

25. **Troelstra A.S., Schwichtenberg H.** Basic Proof Theory. Cambridge University Press, 2000.

26. **Voronkov A.A.** Liss – the logic inference search system // Proceedings. LNCS. Springer, Heidelberg, 1990. Vol. 449. Pp. 677–678.

27. **Voronkov A.** Theorem proving in non-standard logics based on the inverse method // CADE-11. LNCS. Springer, Heidelberg, 1992. Vol. 607. Pp. 648–662.

REFERENCES

1. **Beth E.** Metod semanticheskikh tablits [The method of semantic tables]. *Matematicheskaya teoriya logicheskogo vyvoda* [*The mathematical theory of inference*]. Moscow: Nauka Publ., 1967, Pp. 191–199. (rus)

2. **Davydov G.V., Maslov S.Yu., Mints G.E., Orevkov V.P., Slisenko A.O.** Mashinnyy algorifm ustanovleniya vyvodimosti na osnove obratnogo metoda [Machine algorithm for establishing deducibility based on the inverse method]. *Issledovaniya po konstruktivnoy matematike i matematicheskoy logike. Zap. nauchn. sem. LOMI*, 1969, Vol. 16, Pp. 8–19. (rus)

3. **Dragalin A.G.** *Matematicheskiy intuitsionizm. Vvedeniye v teoriyu dokazatelstv.* [*Mathematical intuitionism. Introduction to the theory of evidence*], Moscow: Nauka Publ., 1979. (rus)

4. **Kanger S.** Uproshchennyy metod dokazatelstva dlya elementarnoy logiki [Simplified method of proof for elementary logic]. *Matematicheskaya teoriya logicheskogo vyvoda* [*The mathematical theory of inference*]. Moscow: Nauka Publ., 1967, Pp. 200–207. (rus)

5. **Kleene S.** *Matematicheskaya logika* [*Mathematical logic*]. Moscow: Mir Publ., 1973. (rus)

6. **Maslov S.Yu.** Obratnyy metod ustanovleniya vyvodimosti v klassicheskom ischislenii predikatov [The inverse method for the classical predicate calculus]. *DAN SSSR*, 1964, Vol. 159, No. 1, Pp. 17–20. (rus)

7. **Maslov S.Yu.** Obratnyy metod ustanovleniya vyvodimosti dlya logicheskikh ischisleniy [The inverse method for establishing deducibility for logical calculus]. *Tr. MIAN SSSR*, 1968, Vol. 98, Pp. 26–87. (rus)

8. **Maslov S.Yu.** Taktiki poiska vyvoda, osnovannyye na unifikatsii poryadka chlenov v blagopriyatnom nabore [Deduction search tactics based on the unification of the order of members in favorable sets]. *Zap. nauchn. sem. LOMI*, 1969, Vol. 16, Pp. 126–136. (rus)

9. **Maslov S.Yu.** Svyaz mezhdu taktikami obratnogo metoda i metoda rezolyutsiy [A connection between tactics of the inverse method and the resolution method]. *Zap. nauchn. sem. LOMI*, 1969, Vol. 16, Pp. 137–146. (rus)

10. **Maslov S.Yu.** Obratnyy metod i taktiki ustanovleniya vyvodimosti dlya ischisleniya s funktsionalnymi znakami [The inverse method, and tactics for establishing deducibility for a calculus with functional signs]. *Tr. MIAN SSSR*, 1972, Vol. 121, Pp. 14–56. (rus)

11. **Maslov S.Yu.** O poiske vyvoda v ischisleniyakh obshchego tipa [The search for a deduction in the general type]. *Zap. nauchn. sem. LOMI*, 1972, Vol. 32, Pp. 59–65. (rus)

12. **Chang C., Lee R.** *Matematicheskaya logika i avtomaticheskoye dokazatelstvo teorem* [*Mathematical logic and automated theorem proving*]. Moscow: Nauka Publ., 1983, 360 p. (rus)

13. **Degtyarev A., Voronkov A.** The inverse method. *Handbook of Automated Reasoning*, Elsevier, Amsterdam, 2001, Vol. 1, Pp. 179–272.

14. **Hähnle R.** Tableaux and Related Methods. *Handbook of Automated Reasoning*, Elsevier, Amsterdam, 2001, Vol. 1, Pp. 101–177.

15. **Lifschitz V.** What is the inverse method? *Journal of Automated Reasoning*, 1989, No. 5(1), Pp. 1–23.

16. **McCune W.** *Prover9 and Mace4.* Available: http://www.cs.unm.edu/~mccune/Prover9, 2005–2010 (Accessed: 19.12.2015).

17. **McLaughlin S., Pfenning F.** Efficient Intuitionistic Theorem Proving with the Polarized Inverse Method. *CADE-22. LNCS*, Springer, Heidelberg, 2009, Vol. 5663, Pp. 230–244.

18. **Mints G.** Resolution strategies for the Intuitionistic Logic. *Constraint Programming. NATO ASI Series.* Springer, Heidelberg, 1994, Vol. 131, Pp. 289–311.

19. **Mints G.** Decidability of the Class E by Maslov's Inverse Method. Essays Dedicated to Yuri Gurevich on the Occasion of His 70th Birthday. *LNCS*, Springer, Heidelberg, 2010, Vol. 6300, Pp. 529–537.

20. **Pavlov V., Schukin A., Cherkasova T.** Exploring Automated Reasoning in First-Order Logic: Tools, Techniques and Application Areas. *4th International Conference, KESW 2013. CCIS*, Springer, Heidelberg, 2013, Vol. 394, Pp. 102–116.

21. **Pavlov V., Pak V.** The Inverse Method and First-Order Logic Theorem Proving. *Nonlinear Dynamics and Applications*, 2014, Vol. 20, Pp. 127–135.

22. **Raths T., Otten J., Kreitz C.** The ILTP Library: Benchmarking Theorem Provers for Intuitionistic Logic. *Automated Reasoning with Analytic Tableaux and Related Methods, TABLEAUX 2005, LNAI*, Springer Verlag, 2005, Vol. 3702, Pp. 333–337.

23. **Tammet T.** A resolution theorem prover for intuitionistic logic. *CADE-13. LNCS*, Springer, Heidelberg, 1996, Vol. 1104, Pp. 2–16.

24. *The ILTP Library. Provers and Results.* Available: http://www.cs.uni-potsdam.de/ti/iltp/results.html (Accessed: 19.12.2015).

25. **Troelstra A.S., Schwichtenberg H.** *Basic Proof Theory.* Cambridge University Press, 2000.

26. **Voronkov A.A.** Liss – the logic inference search system. *Proceedings. LNCS*, Springer, Heidelberg, 1990, Vol. 449, Pp. 677–678.

27. **Voronkov A.** Theorem proving in non-standard logics based on the inverse method. *CADE-11. LNCS.* Springer, Heidelberg, 1992, Vol. 607, Pp. 648–662.

ПАВЛОВ Владимир Александрович – *аспирант кафедры компьютерных интеллектуальных технологий Института компьютерных наук и технологий Санкт-Петербургского политехнического университета Петра Великого.*

195251, Россия, Санкт-Петербург, ул. Политехническая, д. 29.
E-mail: vlapav239@gmail.com

PAVLOV Vladimir A. *Peter the Great St. Petersburg Polytechnic University.*
195251, Politekhnicheskaya Str. 29, St. Petersburg, Russia.
E-mail: vlapav239@gmail.com

ПАК Вадим Геннадьевич – *доцент кафедры компьютерных интеллектуальных технологий Института компьютерных наук и технологий Санкт-Петербургского политехнического университета Петра Великого, кандидат физико-математических наук.*

195251, Россия, Санкт-Петербург, ул. Политехническая, д. 29.
E-mail: vadimpak917@gmail.com

PAK Vadim G. *Peter the Great St. Petersburg Polytechnic University.*
195251, Politekhnicheskaya Str. 29, St. Petersburg, Russia.
E-mail: vadimpak917@gmail.com