Math-Net.Ru

Общероссийский математический портал

В. Н. Крупский, О символических моделях для функциональной логики доказательств, *Матем. сб.*, 2011, том 202, номер 5, 63–76

DOI: <https://doi.org/10.4213/sm7665>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.209.158.208

26 апреля 2023 г., 12:45:11

УДК 510.64+510.67

В. Н. Крупский

О символических моделях для функциональной логики доказательств

В работе определяется понятие символической модели для функциональных логик доказательств. Получены результаты о корректности и полноте указанных логик относительно соответствующих классов символических моделей. Эта техника применяется для доказательства корректности использования термов функциональной логики доказательств в качестве обозначений для ее собственных выводов.

Библиография: 17 названий.

Ключевые слова: формальный вывод, предикат доказательств, функциональная логика доказательств, модель Мкртычева, свойство интернализации выводов.

§ 1. Введение

Пропозициональные логики доказательств (см. обзор [1]) описывают инвариантные, т.е. не зависящие от выбора конкретной дедуктики, свойства арифметического предиката доказательств, рассматриваемого совместно с вычислимыми операциями над доказательствами, порожденными допустимыми правилами вывода. Пропозициональный язык расширяется новой конструкцией формул $t: F$ (читается “ t доказывает F ”), где F – формула, а t – терм, структура которого отражает процесс построения соответствующего вывода с помощью фиксированного набора базисных операций. Типичными примерами последних являются бинарная операция $:$, состоящая в применении правила *modus ponens*, и унарная операция $!$, реализующая поиск вывода формулы $t: F$ по известному терму t .

Исторически первой системой такого рода является логика доказательств LP (см. [2]–[4]), соответствующая многозначным предикатам доказательств. Доказательствами в этом смысле являются конечные множества арифметических выводов, а язык LP содержит дополнительную операцию $+$, объединяющую два доказательства в одно. Однако традиционно в формальной арифметике используют “стандартные” предикаты доказательств $\text{Pr } f(x, y)$ вида

x есть номер вывода, а y – номер его последней формулы,

которые не попадают в этот класс. Им отвечают функциональные логики доказательств – FLP и ее расширения (см. [5]–[8]), где за основу принято свойство

Работа выполнена при поддержке Российского фонда фундаментальных исследований (грант № 11-01-00281).

функциональности (однозначности) предиката доказательств, выраженное посредством аксиом унификации (см. §3).

Непротиворечивость логики LP (и большинства других логик доказательств) нетрудно установить с помощью “забывающего” перевода, который заменяет все подформулы вида $t: F$ на F . Он преобразует теоремы LP в тавтологии классической логики высказываний. Это обстоятельство позволяет непротиворечивым образом расширять логику LP с помощью аксиом вида $c_i: A_i$, объявляющих константы c_i в качестве обозначений для доказательств тождественно истинных формул A_i .

Для функциональной логики доказательств FLP и ее расширений этот подход неприменим – мешают аксиомы унификации, выражающие условие функциональности предиката доказательств. Указанный перевод преобразует аксиомы унификации в формулы с произвольной таблицей истинности. Непротиворечивость функциональных логик доказательств устанавливает другой перевод – замена всех подформул вида $t: F$ на $\perp$, однако он не позволяет установить непротиворечивость расширений аксиомами вида $t: F$, так как переводит последние в тождественно ложные формулы. Здесь требуется более сложная модельная техника, содержательно использующая значение связки $:$.

Арифметические доказуемостные интерпретации для функциональных логик доказательств исследованы в работах [6], [8]. В настоящей работе описывается соответствующая символическая семантика. Построение символических моделей технически проще, чем соответствующих арифметических, поэтому их естественнее использовать при изучении вопросов о непротиворечивости расширений.

Идея интерпретации формул языка логики доказательств как утверждений об абстрактной ссылочной структуре изложена в [9]. Определение символической модели для логики LP (М-модели, модели Мкртычева) предложено в [10] и адаптировано для других нефункциональных логик доказательств в работах [11]–[14]. Его обобщение на случай эпистемических логик со свидетельствами (модели Крипке–Фиттинга) рассмотрены в [15]–[17].

Мы восполняем пробел, развивая технику символических моделей для функциональных логик доказательств. Существенно новым моментом является разделение языка самой логики и языка модели, что порождает дополнительный параметр модели – отображение, которое переводит формулы одного языка в другой, конкретизируя значения переменных. Использование таких переводов позволяет упростить формулировку свойства функциональности модели, обеспечивающего истинность аксиом унификации. Для логики FLP и ее расширений функциональными переменными (ссылочными конструкциями; см. [7]) доказана их корректность относительно символических моделей. В случае FLP также приведено доказательство полноты. Рассмотрен пример применения предлагаемой техники, устанавливающий корректность использования термов функциональной логики доказательств в качестве обозначений для ее собственных выводов.

§ 2. Язык $L(\text{FLP})$

Язык $L(\text{FLP})$ функциональной логики доказательств FLP содержит два сорта объектов – термы и формулы. Имеются переменные обоих сортов $x_0, x_1, \dots$ и $p_0, p_1, \dots$ соответственно. Множества всех термов Tm и всех формул Fm задаются следующей грамматикой:

$$\text{Tm} ::= x_i \mid (\text{Tm} \cdot \text{Tm}) \mid (!\text{Tm}), \quad \text{Fm} ::= \perp \mid p_i \mid (\text{Fm} \rightarrow \text{Fm}) \mid (\text{Tm} : \text{Fm}).$$

Мы будем опускать часть скобок, руководствуясь следующим упорядочением символов по их приоритету: $!$, $\cdot$, $\rightarrow$, $:$, а также использовать записи $\top$, $\neg F$, $F \vee G$ и $F \wedge G$ в качестве сокращений для $\perp \rightarrow \perp$, $F \rightarrow \perp$, $\neg F \rightarrow G$ и $\neg(F \rightarrow \neg G)$ соответственно.

Термы и формулы условимся называть *выражениями языка*, $\text{Expr} = \text{Tm} \cup \text{Fm}$. Выражения $e \in \text{Expr}$ представляют собой термы в сигнатуре $\Omega = \{\perp, \rightarrow, :, !, \cdot\}$. В этом контексте *подстановка* – это сохраняющий сорта гомоморфизм свободных алгебр термов сигнатуры Ω , т.е. заданное на множестве Expr отображение, которое термы переводит в термы, формулы – в формулы, а также коммутирует с символами из Ω . Подстановка σ называется *конечной*, если множество

$$\text{Dom}(\sigma) = \{v \mid v \text{ – переменная и } v\sigma \neq v\}$$

конечно, и называется *бесконечной* в противном случае. Пусть

$$\text{Var}(\sigma) = \bigcup_{v \in \text{Dom}(\sigma)} \text{Var}(v\sigma) \cup \text{Dom}(\sigma),$$

где $\text{Var}(e)$ обозначает множество всех переменных, встречающихся в выражении $e \in \text{Expr}$.

Для $e, e' \in \text{Expr}$ запись $e' < e$ означает, что выражение e' является собственным подвыражением (подтермом или подформулой) выражения e , а запись $e' \equiv e$ – графическое равенство выражений e и e' .

ОПРЕДЕЛЕНИЕ 2.1. *Задачей условной унификации* называется система условных равенств вида

$$A_i = B_i \implies C_i = D_i, \quad i = 1, \dots, n, \quad (1)$$

где $A_i, B_i, C_i, D_i \in \text{Expr}$.

ОПРЕДЕЛЕНИЕ 2.2. Отношение эквивалентности $\sim$, заданное на множестве Expr , условимся называть *правильным*, если выполнены следующие условия:

- (i) для каждого функционального символа $f \in \Omega$ ариности $n > 0$ и любых $e_1, \dots, e_n, e'_1, \dots, e'_n \in \text{Expr}$ справедливо

$$f(e_1, \dots, e_n) \sim f(e'_1, \dots, e'_n) \iff e_1 \sim e'_1 \wedge \dots \wedge e_n \sim e'_n;$$

- (ii) $f(e_1, \dots, e_n) \not\sim g(e'_1, \dots, e'_m)$ при $f \neq g$;

- (iii) отношение $<$ индуцирует строгий фундированный частичный порядок $\prec$ на фактор-множестве $\text{Exrg} / \sim$, где $[e] \sim \prec [e'] \sim$ для классов эквивалентности $[e] \sim$ и $[e'] \sim$ означает, что

$$e \equiv e_0 \sim e'_0 < e_1 \sim e'_1 < \dots < e_n \sim e'_n \equiv e'$$

для некоторой последовательности выражений $e_0, e'_0, e_1, e'_1, \dots, e_n, e'_n$ и $n > 0$.

ЛЕММА 2.3. Пусть $\text{Exrg}, \text{Exrg}'$ – свободные алгебры термов сигнатуры Ω . Каждая подстановка $\sigma: \text{Exrg} \rightarrow \text{Exrg}'$ задает правильное отношение эквивалентности $\sim_\sigma$ на множестве Exrg :

$$e \sim_\sigma e' \iff e\sigma \equiv e'\sigma. \quad (2)$$

ДОКАЗАТЕЛЬСТВО. Легко видеть, что $\sim_\sigma$ является отношением эквивалентности, для которого выполнены условия (i), (ii). Отношение $\prec$ транзитивно по построению. Его рефлексивность и фундированность следуют из того факта, что неравенство $[e]_{\sim_\sigma} \prec [e']_{\sim_\sigma}$ влечет $e\sigma < e'\sigma$. Тем самым, справедливо условие (iii).

ОПРЕДЕЛЕНИЕ 2.4. Решением задачи (1) будем считать такое правильное отношение эквивалентности $\sim$, для которого при каждом $i = 1, \dots, n$ справедливо одно из условий: $A_i \not\sim B_i$ или $C_i \sim D_i$. В этом случае система условных равенств (1) называется *унифицируемой*, а соответствующее отношение – *унифицирующим* отношением эквивалентности.

Классическая задача (безусловной) унификации является частным случаем приведенных определений при $A_i \equiv B_i$. В [6] показано, что основные результаты классической теории унификации переносятся на случай условных задач. В частности, справедливы следующие факты (см. [6], [8]).

- Свойство унифицируемости для задач условной унификации разрешимо.
- Если задача (1) унифицируема, то в классе унифицирующих ее отношений эквивалентности существует наименьший элемент $\sim_0$, который порождается некоторой конечной подстановкой σ_0 :

$$e \sim_0 e' \iff e\sigma_0 \equiv e'\sigma_0.$$

Подстановка σ_0 эффективно строится по системе (1). Ее можно выбрать идемпотентной ($\sigma_0^2 = \sigma_0$) и консервативной (все переменные из $\text{Var}(\sigma_0)$ встречаются в (1)).

- Подстановка σ_0 является наиболее общим унификатором системы (1) в следующем смысле: если конечная подстановка σ является унификатором, т.е. порождает отношение эквивалентности, унифицирующее систему (1), то ее можно представить в виде $\sigma = \sigma_0\lambda$, где λ – некоторая подстановка. (Обратное в общем случае неверно.)

ОПРЕДЕЛЕНИЕ 2.5. Для системы условных равенств S вида (1) и $A, B \in \text{Exrg}$ пусть $A = B \bmod S$ означает, что $A \sim B$ для всех правильных отношений эквивалентности $\sim$, унифицирующих систему S .

ЛЕММА 2.6 (см. [6]). *Отношение $A = B \bmod S$ разрешимо.*

ДОКАЗАТЕЛЬСТВО. Свойство унифицируемости систем вида (1) разрешимо. Если система S не унифицируема, то $A = B \bmod S$ истинно для всех $A, B \in \text{Ехрг}$. Для унифицируемой системы следует восстановить ее наиболее общий унификатор σ_0 и проверить условие $A\sigma_0 \equiv B\sigma_0$.

§ 3. Функциональная логика доказательств FLP

С каждой формулой вида $G = \bigwedge_{i=1}^n t_i : F_i$ свяжем систему условных равенств:

$$t_i = t_j \implies F_i = F_j, \quad i, j = 1, \dots, n. \quad (3)$$

Будем писать $A = B \bmod G$, если $A = B \bmod S$, где S – система условных равенств (3).

Функциональная логика доказательств FLP задается следующим исчислением (см. [6]).

(A0) Схемы аксиом классического исчисления высказываний.

(A1) $t : F \rightarrow F$.

(A2) $t : (F \rightarrow G) \rightarrow (s : F \rightarrow ts : G)$.

(A3) $t : F \rightarrow !t : t : F$.

(A4) Аксиома унификации: $t_1 : F_1 \wedge \dots \wedge t_n : F_n \rightarrow (A \leftrightarrow B)$, если $A = B \bmod (\bigwedge_{i=1}^n t_i : F_i)$.

Правило вывода: (MP) $F \rightarrow G, F \vdash G$.

§ 4. Функциональные M-модели

ОПРЕДЕЛЕНИЕ 4.1. Фиксируем два множества констант, $S^c = \{S_0, S_1, \dots\}$ и $P^c = \{a_0, a_1, \dots\}$, элементы которых будут использоваться в качестве атомарных обозначений для высказываний и доказательств. Термы и формулы языка $L(S^c, P^c)$ получаются из термов и формул языка логики FLP заменой всех переменных на константы соответствующих сортов.

ОПРЕДЕЛЕНИЕ 4.2. M-моделью (моделью Мкртычева; см. [10]) называется тройка $M = \langle L(S^c, P^c), \mathcal{E}, v \rangle$. Здесь $L(S^c, P^c)$ – определенный выше язык, $v : S^c \rightarrow \{0, 1\}$ – истинностная оценка пропозициональных констант, а $\mathcal{E} : \text{Tm} \rightarrow 2^{\text{Fm}}$ – свидетельская функция. Функция $\mathcal{E}$ сопоставляет произвольному терму t языка $L(S^c, P^c)$ семейство формул, свидетелем истинности которых в модели M считается терм t . На свидетельскую функцию накладываются следующие ограничения:

- если $F \rightarrow G \in \mathcal{E}(t)$ и $F \in \mathcal{E}(s)$, то $G \in \mathcal{E}(t \cdot s)$;
- если $F \in \mathcal{E}(t)$, то $t : F \in \mathcal{E}(!t)$.

M-модель называется *функциональной*, если для каждого терма t множество $\mathcal{E}(t)$ содержит не более одного элемента.

Отношение истинности $\models$ формул языка $L(S^c, P^c)$ в М-модели M определяется следующим образом:

$$\begin{aligned} M &\not\models \perp; \\ M &\models S_i &\iff v(S_i) = 1; \\ M &\models F \rightarrow G &\iff M \not\models F \text{ или } M \models G; \\ M &\models t: F &\iff F \in \mathcal{E}(t) \text{ и } M \models F. \end{aligned}$$

ОПРЕДЕЛЕНИЕ 4.3. Символической моделью языка $L(\text{FLP})$ условимся называть пару $\langle \sigma, M \rangle$, где $M = \langle L(S^c, P^c), \mathcal{E}, v \rangle$ – функциональная М-модель, а $\sigma: L(\text{FLP}) \rightarrow L(S^c, P^c)$ – интерпретирующее отображение. Отображение σ представляет собой бесконечную подстановку, которая замещает переменные x_i языка $L(\text{FLP})$ термами языка $L(S^c, P^c)$, а переменные p_i языка $L(\text{FLP})$ – формулами языка $L(S^c, P^c)$. Истинность формулы F языка $L(\text{FLP})$ в символической модели $\langle \sigma, M \rangle$ определяется так:

$$\langle \sigma, M \rangle \models F \iff M \models F\sigma.$$

ЗАМЕЧАНИЕ 4.4. Для нефункциональных логик доказательств в качестве символических моделей обычно используются М-модели с тождественным интерпретирующим отображением. Наше определение также может быть приведено к подобному виду: отношение истинности в символической модели $\langle \sigma, M \rangle$ совпадает с отношением истинности в М-модели $\langle L(\text{FLP}), \mathcal{E}', v' \rangle$, где $\mathcal{E}'(t) = \{F \mid F\sigma \in \mathcal{E}(t\sigma)\}$, $v'(p_i) = v(p_i\sigma)$. В этом смысле семантика, порожденная определением 4.3, оказывается частным случаем общей символической семантики для логик доказательств, основанной на моделях Мкртычева.

ТЕОРЕМА 4.5. Если $\text{FLP} \vdash F$, то формула F истинна в каждой символической модели языка $L(\text{FLP})$.

ДОКАЗАТЕЛЬСТВО. Аксиомы (A0)–(A3) и правило (MP) присутствуют в логике доказательств LP, которая корректна и полна относительно класса всех М-моделей (см. [10]). Проверим корректность аксиомы (A4).

Пусть $\langle \sigma, M \rangle$ – символическая модель функциональной логики доказательств и $\langle \sigma, M \rangle \models \bigwedge_{i=1}^n t_i: F_i$. Рассмотрим отношение эквивалентности (2). Оно правильное согласно лемме 2.3 и унифицирует систему (3), так как M – функциональная М-модель. Поэтому $A \sim_\sigma B$, что означает совпадение формул $A\sigma$ и $B\sigma$. Отсюда получаем $\langle \sigma, M \rangle \models A \leftrightarrow B$.

§ 5. Расширение функциональными переменными

Расширение правил образования термов и формул за счет добавления функциональных переменных $\alpha_i: \text{Tm} \rightarrow \text{Fm}$ и $\beta_j: \text{Tm} \rightarrow \text{Tm}$, $i \in I$, $j \in J$, где I , J – конечные или счетные множества индексов, существенно повышает выразительные возможности языка (см. [7], [8]). В частности, появляется возможность аксиоматического описания операции $\text{goal} = \alpha_0$ извлечения из доказательства

той формулы, которую оно доказывает. Это достигается с помощью схемы аксиом

$$t: F \rightarrow t: \text{goal}(t), \quad t \in \text{Tm}, \quad F \in \text{Fm}, \quad (4)$$

используемой совместно с аксиомами унификации: формулы F и $\text{goal}(t)$ оказываются эквивалентными в любом контексте, в котором выводима формула $t: F$.

Другим примером такого рода является аксиоматизация операции рефлексии $\text{refl} = \beta_0$, извлекающей доказательство формулы F из доказательства формулы $t: F$,

$$t_1: t: F \rightarrow t_1: \text{refl}(t_1): F, \quad t, t_1 \in \text{Tm}, \quad F \in \text{Fm}. \quad (5)$$

Потребность для этих целей именно в функциональных переменных, а не константах, объясняется спецификой аксиом унификации, в которых требуется допустить возможность унификации выражений вида $\text{goal}(t)$, $\text{refl}(t)$ с выражениями, чья главная связка отлична от goal и refl соответственно. Иначе, например, при $F \equiv F_1 \wedge F_2$ из (4) и формулы

$$t: F \wedge t: \text{goal}(t) \rightarrow (\top \leftrightarrow \perp),$$

которая в этом случае оказывается одной из аксиом унификации, будет следовать $\neg(t: F)$ для всех F указанного вида и произвольного t .

В функциональной М-модели $M = \langle L(S^c, P^c), \mathcal{E}, v \rangle$ функциональные переменные α_i, β_j означают произвольные функции α_i^* и β_j^* соответствующих типов; α_i^* отображает термы языка $L(S^c, P^c)$ в формулы, а β_j^* – в термы языка $L(S^c, P^c)$. Аналогичным образом модифицируется определение символической модели.

ОПРЕДЕЛЕНИЕ 5.1. Путь $L(\text{FLP}_2)$ – расширение языка $L(\text{FLP})$ функциональными переменными α_i, β_j , где $i \in I, j \in J$. Множества термов (Tm_2) и формул (Fm_2) этого языка задаются грамматикой

$$\begin{aligned} \text{Tm}_2 &::= x_i \mid (\text{Tm}_2 \cdot \text{Tm}_2) \mid (!\text{Tm}_2) \mid \beta_j(\text{Tm}_2), \\ \text{Fm}_2 &::= \perp \mid p_i \mid (\text{Fm}_2 \rightarrow \text{Fm}_2) \mid (\text{Tm}_2 : \text{Fm}_2) \mid \alpha_i(\text{Tm}_2). \end{aligned}$$

Символическая модель языка $L(\text{FLP}_2)$ задается набором $\langle \sigma, \overline{M} \rangle$, где

$$\overline{M} = \langle M, \{\alpha_i^*\}_{i \in I}, \{\beta_j^*\}_{j \in J} \rangle$$

– М-модель с заданными значениями функциональных переменных, а σ – отображение, интерпретирующее язык $L(\text{FLP})$ в М-модели M в смысле определения 4.3 и продолженное на выражения языка $L(\text{FLP}_2)$ следующим образом:

$$\alpha_i(t) \sigma = \alpha_i^*(t\sigma), \quad \beta_i(t) \sigma = \beta_i^*(t\sigma), \quad t \in \text{Tm}_2. \quad (6)$$

Формула F языка $L(\text{FLP}_2)$ истинна в символической модели, если $M \models F\sigma$.

ЗАМЕЧАНИЕ 5.2. Для функциональных переменных α_i, β_j выражения $\alpha_i(t)$ и $\beta_j(t)$ играют роль обыкновенных переменных 1-го порядка. Язык $L(\text{FLP}_2)$ получается в результате добавления всех таких первопорядковых переменных к языку $L(\text{FLP})$. Интерпретирующее отображение σ из определения 5.1 оказывается бесконечной подстановкой, которая замещает не только переменные x_i, p_i , но и добавленные переменные $\alpha_i(t), \beta_j(t)$. Значения σ на дополнительных переменных задаются рекурсивными соотношениями (6), использующими функции α_i^*, β_j^* . В качестве альтернативы можно было бы первоначально задавать значения σ на дополнительных переменных произвольно с соблюдением условия согласованности

$$t_1\sigma = t_2\sigma \implies \alpha_i(t_1)\sigma = \alpha_i(t_2)\sigma \wedge \beta_j(t_1)\sigma = \beta_j(t_2)\sigma,$$

после чего подобрать соответствующие функции α_i^*, β_j^* на основании (6).

ОПРЕДЕЛЕНИЕ 5.3. Пусть $\text{Expr}_2 = \text{Term}_2 \cup \text{Fm}_2$ – множество выражений языка $L(\text{FLP}_2)$, рассматриваемых как термы в сигнатуре Ω . Тем самым, выражения вида $\alpha_i(t)$ и $\beta_j(t)$ считаются атомарными и не имеют собственных подвыражений. Отношение эквивалентности $\sim$ на множестве Expr_2 называется *правильным*, если кроме условий (i), (ii), (iii) из определения 2.2 выполнено условие согласованности:

(iv) если $t_1 \sim t_2$, то $\alpha_i(t_1) \sim \alpha_i(t_2)$ и $\beta_j(t_1) \sim \beta_j(t_2)$ при $i \in I, j \in J$.

Соответственно модифицируются определения отношения $A = B \bmod G$ для формул языка $L(\text{FLP}_2)$ и множества аксиом унификации (A4) – в них используются правильные отношения эквивалентности на множестве Expr_2 . При этом сохраняется разрешимость отношения $A = B \bmod G$ (см. [8]).

ОПРЕДЕЛЕНИЕ 5.4. Логика FLP_2 задается схемами аксиом (A0)–(A4) и правилом вывода (MP), в которых допускается использовать термы и формулы языка $L(\text{FLP}_2)$.

ТЕОРЕМА 5.5. Если $\text{FLP}_2 \vdash F$, то формула F истинна в каждой символической модели языка $L(\text{FLP}_2)$.

ДОКАЗАТЕЛЬСТВО повторяет рассуждение, устанавливающее теорему 4.5. Дополнительно требуется заметить, что в случае языка $L(\text{FLP}_2)$ отношение эквивалентности $e \sim_\sigma e' \iff e\sigma \equiv e'\sigma$, порожденное интерпретирующим отображением σ , удовлетворяет условию (iv). Это следует из равенств (6).

Под логикой FLP_2^+ будем понимать систему в языке $L(\text{FLP}_2)$ с двумя функциональными переменными goal и refl , расширяющую логику FLP_2 схемами аксиом (4) и (5). Из теоремы 5.5 немедленно следует корректность FLP_2^+ относительно символических моделей языка, в которых значения функциональных переменных goal^* и refl^* выбраны в соответствии с (4) и (5), т.е. $\text{goal}^*(t) = F$ при $\mathcal{E}(t) = \{F\}$ и $\text{refl}^*(t_1) = t$ при $\mathcal{E}(t_1) = \{t : F\}$. Такие символические модели условимся называть *моделями логики FLP_2^+* .

§ 6. Полнота

Рассмотренные выше функциональные логики доказательств полны относительно соответствующих классов символических моделей. Это вытекает из конструкций насыщения, использованных в доказательствах арифметической полноты указанных логик (см. [6], [8]). Мы приведем доказательство полноты FLP как технически менее сложное.

Отметим, что используемые для доказательства полноты нефункциональных логик доказательства методы, связанные со стандартным построением максимальных непротиворечивых множеств, здесь не работают, так как приводят к необходимости искать интерпретирующее отображение в виде решения бесконечной системы условных равенств, про которую известна лишь совместность каждого ее конечного фрагмента, что не гарантирует совместности всей системы в целом. Процедура насыщения позволяет ограничиться системой специального вида, совместность которой уже следует из совместности подходящего ее конечного фрагмента.

ТЕОРЕМА 6.1. *Пусть $F \in \text{Fm}$. Если $\text{FLP} \not\models F$, то существует символическая модель языка $L(\text{FLP})$, в которой формула F ложна.*

ДОКАЗАТЕЛЬСТВО. В [6; раздел 6] предложена процедура насыщения для логики FLP. Она преобразует каждую невыводимую в FLP формулу F в тройку $\langle \Gamma, \Delta, \sigma \rangle$, где Γ, Δ – непересекающиеся множества формул, а σ – конечная идемпотентная подстановка. При этом выполняются следующие условия насыщенности.

- Если $X \rightarrow Y \in \Gamma$, то $X \in \Delta$ или $Y \in \Gamma$. Если $X \rightarrow Y \in \Delta$, то $X \in \Gamma$ и $Y \in \Delta$. Если $t: X \in \Gamma$, то $X \in \Gamma$.
- Если $t: (X \rightarrow Y) \in \Gamma$ и $s: X \in \Gamma$, то $t \cdot s: Y \in \Gamma$. Если $t: X \in \Gamma$, то $!t: t: X \in \Gamma$.
- $\Gamma\sigma = \Gamma$, $\Delta\sigma = \Delta$, $\{\perp, F\sigma\} \subseteq \Delta$.
- Множество Γ для каждого терма вида $t\sigma$ содержит не более одной формулы вида $t\sigma: X$.

Фиксируем невыводимую в FLP формулу F и соответствующую тройку $\langle \Gamma, \Delta, \sigma \rangle$. Для каждой переменной ξ языка $L(\text{FLP})$, которая не меняется под действием подстановки σ , введем новую, отличную от всех остальных константу $\bar{\xi}$. Для выражения $e \in \text{Expr}$ пусть $\bar{e}$ означает результат замены в нем всех переменных ξ , для которых $\xi\sigma = \xi$, на $\bar{\xi}$. Рассмотрим язык $L(S^c, P^c)$, где

$$S^c = \{\bar{p}_i \mid p_i\sigma = p_i, i \in \omega\}, \quad P^c = \{\bar{x}_i \mid x_i\sigma = x_i, i \in \omega\},$$

и бесконечную подстановку $\bar{\sigma}$, для которой $e\bar{\sigma} = \bar{e}\bar{\sigma}$, $e \in \text{Expr}$. В силу идемпотентности σ выражение $\bar{e}\bar{\sigma}$ при любом $e \in \text{Expr}$ принадлежит языку $L(S^c, P^c)$. Для термов $\bar{t}$ языка $L(S^c, P^c)$ определим значение свидетельской функции $\mathcal{E}(\bar{t}) = \{\bar{X} \mid t: X \in \Gamma\}$ и зададим истинностную оценку v для констант $\bar{p}_i \in S^c$, положив $v(\bar{p}_i) = 1$ в том и только том случае, когда $p_i \in \Gamma$. Условия насыщенности обеспечивают выполнение ограничений, накладываемых на свидетельскую

функцию определением 4.2, и условия функциональности. Таким образом, пара $\langle \bar{\sigma}, M \rangle$, где $M = \langle L(S^c, P^c), \mathcal{E}, v \rangle$, является символической моделью языка $L(\text{FLP})$.

Индукцией по построению формулы G нетрудно показать, что если $G \in \Gamma$, то $M \models \bar{G}$, а если $G \in \Delta$, то $M \not\models \bar{G}$. Например, разберем случай G вида $t: X$. Если $t: X \in \Gamma$, то также $X \in \Gamma$, поэтому $M \models \bar{X}$ по предположению индукции. Кроме того, $\bar{X} \in \mathcal{E}(\bar{t})$ согласно определению свидетельской функции, откуда $M \models \overline{t: X}$. Пусть теперь $t: X \in \Delta$. Если при этом $M \models \overline{t: X}$, то $\bar{X} \in \mathcal{E}(\bar{t})$ и $t: X \in \Gamma$, что противоречит условию $\Gamma \cap \Delta = \emptyset$.

Осталось заметить, что $F\bar{\sigma} = \bar{F}\bar{\sigma}$ и $F\sigma \in \Delta$, откуда $M \not\models F\bar{\sigma}$.

ЗАМЕЧАНИЕ 6.2. Метод насыщения для языка $L(\text{FLP}_2)$ описан в [8], где он применяется к расширению логики FLP_2 дополнительными схемами аксиом (4), (5) и аналогичными, специфицирующими значения других функциональных переменных. Для доказательства полноты логик FLP_2 и FLP_2^+ достаточно использовать этот метод, опуская шаги, соответствующие отсутствующим дополнительным аксиомам, после чего конструкция символической модели извлекается из насыщенной тройки $\langle \Gamma, \Delta, \sigma \rangle$ аналогично тому, как это сделано в доказательстве теоремы 6.1.

§ 7. Пример: непротиворечивость контекстов при интернализации выводов

Логика доказательств позволяют формализовать рассуждения о своих собственных выводах, используя их представление термами языка самой логики. Возможность такого представления, известная как свойство интернализации выводов (см. [1]), для рассматриваемых функциональных логик доказательств формулируется в виде следующего утверждения, в котором $\vdash$ означает выводимость в одной из логик FLP , FLP_2 или FLP_2^+ .

ЛЕММА 7.1. *Если $\vdash F$, то найдется терм $t(c_1, \dots, c_n)$, для которого*

$$c_1: A_1, \dots, c_n: A_n \vdash t(c_1, \dots, c_n): F, \quad (7)$$

где $A_1, \dots, A_n$ – список всех аксиом, встретившихся в выводе формулы F , а список $c_1, \dots, c_n$ состоит из попарно различных переменных, не встречающихся в этом выводе, причем терм $t(c_1, \dots, c_n)$ не содержит других переменных, кроме указанных.

ДОКАЗАТЕЛЬСТВО. Пусть $F_1, \dots, F_m$ – вывод формулы F , а аксиомы A_i и переменные c_i удовлетворяют условию леммы. Для $k = 1, \dots, m$ определим термы t_k следующим образом. Если F_k есть одна из аксиом A_i , то положим $t_k = c_i$. В противном случае F_k получено по правилу (MP) из формул F_i и F_j для некоторых $i, j < k$. Положим $t_k = t_i \cdot t_j$. С помощью схемы аксиом (A2) индукцией по k нетрудно установить, что $c_1: A_1, \dots, c_n: A_n \vdash t_k: F_k$. Тем самым, терм t_m является искомым.

Корректное использование такого представления требует доказательства непротиворечивости множества гипотез в (7). Этот факт можно установить с помощью предложения 7.2.

Для каждой из рассматриваемых логик под *выполнимостью* множеств формул языка этой логики условимся понимать выполнимость в соответствующем логике классе символических моделей.

ПРЕДЛОЖЕНИЕ 7.2. *Для каждой из логик FLP , FLP_2 , FLP_2^+ справедливо следующее: если множество формул Γ выполнимо, $F \in \Gamma$, а переменная x_i не встречается в формулах из множества Γ , то множество $\Gamma \cup \{x_i: F\}$ также выполнимо.*

ДОКАЗАТЕЛЬСТВО. Пусть $\langle \sigma, M \rangle$ – символическая модель, в которой истинны все формулы из множества Γ . В случае FLP функциональная М-модель M задается языком $L(S^c, P^c)$, свидетельской функцией $\mathcal{E}$ и оценкой истинности пропозициональных констант v . Расширим язык $L(FLP)$, добавив новую переменную y к списку переменных, участвующих в образовании термов. Аналогично расширим язык модели $L(S^c, P^c)$, добавив новую константу d к множеству P^c .

Определим продолжение $\mathcal{E}'$ свидетельской функции $\mathcal{E}$ на термы расширенного языка модели, задав значения $\mathcal{E}'(t)$ для термов t , содержащих константу d , следующим образом:

$$\begin{aligned} \mathcal{E}'(d) &= \{F\sigma\}; & \mathcal{E}'(t_1 \cdot t_2) &= \{Y\} \text{ при } \mathcal{E}'(t_1) = \{X \rightarrow Y\} \text{ и } \mathcal{E}'(t_2) = \{X\}; \\ \mathcal{E}'(!t) &= \{t: X\} \text{ при } \mathcal{E}'(t) = \{X\}. \end{aligned}$$

В остальных случаях $\mathcal{E}'(t)$ есть $\emptyset$, если терм t содержит константу d , и совпадает с $\mathcal{E}(t)$, если t – терм языка $L(S^c, P^c)$. Нетрудно проверить, что $M' = \langle L(S^c, P^c \cup \{d\}), \mathcal{E}', v \rangle$ является функциональной М-моделью и $M' \models d: F\sigma$. При переходе от M к M' истинностные значения формул, не содержащих константы d , сохраняются, поэтому $M' \models G\sigma$ для всех формул $G \in \Gamma$.

Доопределим подстановку σ до интерпретирующего отображения σ' расширенного языка, положив $y\sigma' = d$ и $z\sigma' = z\sigma$ для всех переменных z языка $L(FLP)$. Тогда $\langle \sigma', M' \rangle$ будет символической моделью расширенного языка, в которой истинны все формулы множества $\Gamma \cup \{y: F\}$. Для возврата к исходному языку достаточно рассмотреть его интерпретирующее отображение вида $\theta\sigma'$, где подстановка θ заменяет x_i на y , оставляя на месте все остальные переменные. Для формул F языка $L(FLP)$ справедливо

$$\langle \theta\sigma', M' \rangle \models F \iff \langle \sigma', M' \rangle \models F\theta,$$

причем $\Gamma\theta = \Gamma$, поэтому в символической модели $\langle \theta\sigma', M' \rangle$ истинны все формулы из множества $\Gamma \cup \{x_i: F\}$.

Та же конструкция годится и для логик FLP_2 и FLP_2^+ , но требует учета дополнительного оснащения М-моделей функциями α_i^* , β_j^* . При построении модели M' надо доопределить значения $\alpha_i^*(t)$, $\beta_j^*(t)$ для термов t , содержащих константу d . Эти значения не используются при вычислении истинностных

значений формул из $\Gamma \cup \{x_i : F\}$, поэтому в случае FLP_2 их можно задать произвольно, а в случае FLP_2^+ – так, чтобы $\text{goal}^*(t) = F$ при $\mathcal{E}(t) = \{F\}$ и $\text{refl}^*(t) = t_1$ при $\mathcal{E}(t) = \{t_1 : F\}$. Остальные рассуждения проходят без изменений.

СЛЕДСТВИЕ 7.3. *В условиях леммы 7.1 множество гипотез $\{c_1 : A_1, \dots, c_n : A_n\}$ является непротиворечивым.*

ДОКАЗАТЕЛЬСТВО. В силу корректности рассматриваемых логик относительно соответствующих классов символических моделей достаточно установить выполнимость множества $\{c_1 : A_1, \dots, c_n : A_n\}$. Согласно предложению 7.2 для этого достаточно установить выполнимость множества аксиом $\{A_1, \dots, A_n\}$, что также следует из упомянутой корректности при условии непустоты класса символических моделей логики.

Логика FLP имеет, в частности, тривиальные символические модели с языком $L(S^c, P^c) = L(\text{FLP})$, тождественным интерпретирующим отображением и свидетельской функцией $\mathcal{E}(t) = \emptyset$ для всех термов t . Каждую из них можно достроить до модели языка $L(\text{FLP}_2)$, задав функции α_i^* , $i \in I$, и β_j^* , $j \in J$, соответствующих типов произвольно. В ней все формулы вида $t : F$ ложны, поэтому в случае языка с двумя функциональными переменными goal и refl она оказывается моделью логики FLP_2^+ .

ОПРЕДЕЛЕНИЕ 7.4. Пусть фиксирована одна из логик FLP , FLP_2 , FLP_2^+ . Ниже под *контекстом* понимается произвольное множество формул вида $c : A$, где c – переменная, а A – аксиома рассматриваемой логики. Условимся говорить, что контекст *адекватен аксиоматике*, если для каждой аксиомы A в контексте присутствует формула $c : A$ с некоторой переменной c .

Если адекватный аксиоматике контекст добавить к логике в качестве дополнительных аксиом, то для полученного таким образом расширения справедливо свойство интернализации выводов в сильной форме – без гипотез в условии (7). Однако при этом возникает вопрос о непротиворечивости расширения. Отметим, что именно так построена логика нефункциональных (многозначных) доказательств LP – как расширение ее ядра LP_0 за счет добавления максимального адекватного аксиоматике контекста, состоящего из всех формул вида $c : A$, где c – переменная, а A – аксиома LP_0 . Непротиворечивость расширения любым контекстом в этом случае устанавливается тривиально с помощью забывающей проекции. Для функциональных логик доказательств вопрос о непротиворечивости расширений оказывается более сложным (см. введение).

ТЕОРЕМА 7.5. *Для каждой из логик FLP , FLP_2 , FLP_2^+ существует непротиворечивый контекст, который адекватен аксиоматике.*

ДОКАЗАТЕЛЬСТВО. Пусть выбрана одна из перечисленных логик. Обозначим через c_j^i переменную $x_{2^i 3^j}$, $i, j \in \omega$. Пусть также $A_0^i, A_1^i, \dots$ – пересчет в лексикографическом порядке всех аксиом, не содержащих переменных c_j^k при $k \geq i$. Покажем, что адекватный аксиоматике контекст $CS = \{c_j^i : A_j^i \mid i, j \in \omega\}$ является непротиворечивым. Так как вывод противоречия может содержать лишь конечное множество формул, то достаточно проверить выполнимость

каждого из конечных множеств $\{c_j^i : A_j^i \mid i, j < k\}$. Последнее устанавливается простой индукцией по k , шаг которой разобран в предложении 7.2.

СЛЕДСТВИЕ 7.6. *Каждая из логик FLP , FLP_2 , FLP_2^+ имеет непротиворечивое рекурсивно аксиоматизируемое расширение, обладающее сильным свойством интернализации выводов: для каждой выводимой в нем формулы F существует терм t , для которого формула $t : F$ также выводима.*

ДОКАЗАТЕЛЬСТВО. Построенный в теореме 7.5 контекст CS является разрешимым множеством, поэтому непротиворечивая теория T , полученная в результате расширения рассматриваемой логики дополнительными аксиомами $c : A \in CS$, является рекурсивно аксиоматизируемой. Сильное свойство интернализации для T устанавливается аналогично лемме 7.1 индукцией по выводу формулы F . Изменится лишь разбор случая, когда очередная формула в выводе является аксиомой: если это A , одна из аксиом исходной логики, то $c : A \in CS$ для некоторой переменной c и в качестве t следует выбрать c ; если это формула $c : A \in CS$, то в качестве t надо взять терм $!c$.

Список литературы

- [1] S. Artemov, L. Beklemishev, “Provability logic”, *Handbook of philosophical logic*, v. 13, Springer-Verlag, Berlin, 2005, 189–360.
- [2] S. Artemov, “Operational modal logic”, *Technical report MSI 95–29*, Cornell University, Ithaca, NY, 1995.
- [3] S. Artemov, “Logic of proofs: a unified semantics for modality and λ -terms”, *Technical report CFIS 98–06*, Cornell University, Ithaca, NY, 1998.
- [4] S. N. Artemov, “Explicit provability and constructive semantics”, *Bull. Symbolic Logic*, **7**:1 (2001), 1–36.
- [5] V. N. Krupski, “Operational logic of proofs with functionality condition on proof predicate”, *Logical foundations of computer science* (Yaroslavl, Russia, 1997), Lecture Notes in Comput. Sci., **1234**, Springer-Verlag, Berlin, 1997, 167–177.
- [6] V. N. Krupski, “The single-conclusion proof logic and inference rules specification”, *Ann. Pure Appl. Logic*, **113**:1–3 (2001), 181–206.
- [7] V. N. Krupski, “Reference constructions in the single-conclusion proof logic”, *J. Logic Comput.*, **16**:5 (2006), 645–661.
- [8] V. N. Krupski, “Referential logic of proofs”, *Theoret. Comput. Sci.*, **357**:1–3 (2006), 143–166.
- [9] S. Artëmov, V. Krupski, “Data storage interpretation of labeled modal logic”, *Ann. Pure Appl. Logic*, **78**:1–3 (1996), 57–71.
- [10] A. Mkrtichev, “Models for the logic of proofs”, *Logical foundations of computer science* (Yaroslavl, Russia, 1997), Lecture Notes in Comput. Sci., **1234**, Springer-Verlag, Berlin, 1997, 266–275.
- [11] R. Kuznets, “On the complexity of explicit modal logics”, *Computer science logic* (Fischbachau, Germany, 2000), Lecture Notes in Comput. Sci., **1862**, Springer-Verlag, Berlin, 2000, 371–383.
- [12] T. Yavorskaya (Sidon), “Negative operations on proofs and labels”, *J. Logic Comput.*, **15**:4 (2005), 517–537.
- [13] T. Yavorskaya (Sidon), N. Rubtsova, “Operations on proofs and labels”, *J. Appl. Non-Classical Logics*, **17**:3 (2007), 283–316.

- [14] Н. М. Рубцова, “Логика доказательств с операцией подстановки”, *Матем. заметки*, **82**:6 (2007), 905–915; англ. пер.: N. M. Rubtsova, “Logic of proofs with substitution”, *Math. Notes*, **82**:5–6 (2007), 816–826.
- [15] M. Fitting, “The logic of proofs, semantically”, *Ann. Pure Appl. Logic*, **132**:1 (2005), 1–25.
- [16] S. Artemov, E. Nogina, “Introducing justification into epistemic logic”, *J. Logic Comput.*, **15**:6 (2005), 1059–1073.
- [17] N. Rubtsova, “On realization of *S5*-modality by evidence terms”, *J. Logic Comput.*, **16**:5 (2006), 671–684.

В. Н. Крупский (V. N. Krupskii)

Механико-математический факультет

Московского государственного университета

им. М. В. Ломоносова

E-mail: krupski@lpcs.math.msu.su

Поступила в редакцию

13.12.2009