Math-Net.Ru

Общероссийский математический портал

Н. М. Рубцова, Логика доказательств с операцией подстановки, *Матем. заметки*, 2007, том 82, выпуск 6, 905–915

DOI: <https://doi.org/10.4213/mzm4190>

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: 54.198.64.247

26 апреля 2023 г., 11:47:00

Логика доказательств с операцией подстановки

Н. М. Рубцова

Рассматривается аксиоматизация операции подстановки в логике доказательств. Для полученной системы вводится символическая семантика и доказывается теорема о полноте.

Библиография: 8 названий.

1. Введение. Логика доказательств $\mathcal{LP}$ была предложена Артемовым в 1995 г. (детальное описание см. в [1], [2]). Она формулируется в пропозициональном языке, расширенном формулами вида $\llbracket t \rrbracket F$ с интерпретацией “ t является доказательством F ”. В этой формуле t – это *терм*, представляющий доказательство. Термы строятся из *переменных по доказательствам* и из *констант по доказательствам* с помощью трех функциональных символов, представляющих элементарные вычислимые операции над доказательствами: бинарные “ $\cdot$ ”, “ $+$ ”, и унарную “ $!$ ”. Логика доказательств $\mathcal{LP}$ содержит, помимо аксиом классического исчисления высказываний, следующие аксиомы:

- *принцип слабой рефлексии*

$$\llbracket t \rrbracket F \rightarrow F;$$

- *аксиомы для операций:*

$$\llbracket t \rrbracket (F \rightarrow G) \rightarrow (\llbracket s \rrbracket F \rightarrow \llbracket t \cdot s \rrbracket G);$$

$$\llbracket t \rrbracket F \rightarrow \llbracket t + s \rrbracket F;$$

$$\llbracket s \rrbracket F \rightarrow \llbracket t + s \rrbracket F;$$

$$\llbracket t \rrbracket F \rightarrow \llbracket !t \rrbracket \llbracket t \rrbracket F.$$

В [2] доказано, что $\mathcal{LP}$ полна относительно класса арифметических интерпретаций, в которых формулы $\llbracket t \rrbracket F$ интерпретируются при помощи арифметического предиката доказательств. В [3] Артемов предложил эпистемическую семантику для $\mathcal{LP}$, в которой формула $\llbracket t \rrbracket F$ интерпретируется как “ t является свидетельством для F ” (так называемое “знание с подтверждением”). Этот подход позволил рассматривать мультиагентные системы, в которых знание агентов описывается одной из эпистемических модальных логик, а $\mathcal{LP}$ аксиоматизирует свидетельскую часть. В [2] также показано, что модальным аналогом $\mathcal{LP}$ является логика $S4$. А именно, для любой $\mathcal{LP}$ -формулы F верно, что $\mathcal{LP} \vdash F \Leftrightarrow S4 \vdash F^\circ$. Через F° обозначается перевод, заменяющий все подформулы вида $\llbracket t \rrbracket G$ на $\Box G$. Этот факт обеспечивает $S4$, а следовательно, и интуиционистскую логику, точной доказуемостной семантикой.

Работа выполнена при поддержке Российского фонда фундаментальных исследований и фонда ИНТАС (грант № 05-1000008-8144).

Важным свойством логики доказательств $\mathcal{LP}$ является интернализация выводов: если $\mathcal{LP} \vdash F$, то существует терм t такой, что $\mathcal{LP} \vdash \llbracket t \rrbracket F$. Терм t моделирует вывод формулы F и строится из аксиомных констант (которые служат элементарными доказательствами аксиом) при помощи двух операций: “.” и “!”. Таким образом, фрагмент логики доказательств $\mathcal{LP}$ без “+” является тем минимальным ядром, которое обеспечивает свойство интернализации выводов. Операция “+” оказывается дополнительной и используется только на этапе реализации модальной логики S4.

Нетрудно заметить, что минимальный набор операций, обеспечивающий свойство интернализации выводов, зависит от формулировки исчисления высказываний. Логика $\mathcal{LP}$ построена на основе стандартной формулировки исчисления высказываний с бесконечным множеством аксиом, заданным конечным числом схем и одним правилом вывода *modus ponens* (MP). Не менее естественной является формулировка исчисления высказываний с конечным числом аксиом и двумя правилами вывода: MP и правилом подстановки. Последнее имеет вид $\vdash F \Rightarrow \vdash F(G/S_i)$, где $F(G/S_i)$ означает результат подстановки в формулу F формулы G вместо всех вхождений пропозициональной переменной S_i . Для того, чтобы описать соответствующую операцию над доказательствами, нам необходимо добавить функциональный символ, строящий доказательство формулы $F(G/S_i)$ из формулы G и доказательства формулы F . В языке $\mathcal{LP}$ нет средств, чтобы описать зависимость операции от формулы. Поэтому мы используем расширение этого языка так называемым предикатом ссылки, введенное в [4], [5]. Этот язык содержит новые квазиатомарные формулы вида $x \ni F$, со значением “ x ссылается на F ”, где x – переменная для ссылок, а F – формула. Мы добавляем в этот язык счетное множество функциональных символов $\text{subst}_i(\cdot, \cdot)$, $i = 1, 2, \dots$, типа *доказательство* $\rightarrow$ (*ссылка* $\rightarrow$ *доказательство*) для обозначения операций подстановки формул в выводы. Действие операции подстановки subst_i описывается следующей аксиомой:

$$\llbracket t \rrbracket F \wedge (x \ni G) \rightarrow \llbracket \text{subst}_i(t, x) \rrbracket F(G/S_i).$$

Формулы вида $\llbracket t \rrbracket F$ читаются теперь как “ t является доказательством схемы F ”.

В данной работе рассматривается логика доказательств $\mathcal{LP}_{\text{sub}}$, содержащая, кроме стандартных операций $\mathcal{LP}$ (операция ! переобозначена p_+ в $\mathcal{LP}_{\text{sub}}$) и операций подстановки, позитивную верификацию $!_+$ для ссылок, описываемую аксиомой

$$x \ni F \rightarrow \llbracket !_+(x) \rrbracket (x \ni F),$$

и негативную верификацию p_- для доказательств и $!_-$ для ссылок с аксиомами

$$\begin{aligned} \neg \llbracket t \rrbracket F \wedge x \ni F &\rightarrow \llbracket p_-(t, x) \rrbracket \neg \llbracket t \rrbracket F, \\ x \ni F \wedge \neg(y \ni F) &\rightarrow \llbracket !_-(x, y) \rrbracket \neg(y \ni F). \end{aligned}$$

Последние позволяют ограничить число аксиомных констант конечным набором (по одной константе на каждую пропозициональную аксиому), что соответствует формулировке логики с конечным набором аксиом и правилом подстановки.

Фрагмент логики $\mathcal{LP}_{\text{sub}}$, описывающий отдельно операцию подстановки, был введен и изучен в [4]. Для него предложены арифметическая и символическая семантики, доказаны соответствующие теоремы о полноте и установлена разрешимость. Фрагмент $\mathcal{LP}_{\text{sub}}$, содержащий все операции кроме подстановки, по существу совпадает с логикой, изученной в [6].

Структура данной статьи следующая. В разделе 2 мы определяем логику доказательств с операцией подстановки $\mathcal{LP}_{\text{sub}}$ и показываем, что она обладает свойством интернализации. В разделе 3 мы даем определение символической семантики и доказываем теорему о полноте, опираясь на методы, предложенные в [5].

2. Логика доказательств с операцией подстановки.

ОПРЕДЕЛЕНИЕ 1. Язык логики доказательств с операцией подстановки содержит объекты трех типов: предложения, доказательства и ссылки. Он содержит пропозициональные переменные $\text{SVar} = \{S_1, S_2, \dots\}$, переменные для ссылок $\text{LVar} = \{x_1, x_2, \dots\}$, переменные по доказательствам $\text{PVar} = \{p_1, p_2, \dots\}$, константы по доказательствам $\text{PConst} = \{c_1, c_2, c_3\}$; булевы связки $\neg$ и $\rightarrow$ (остальные связки и булевы константы $\top$, $\perp$ выражаются стандартным способом); функциональные символы: бинарные $\cdot$, $+$, p_- , l_- , subst_i , унарные p_+ , l_+ ; два операторных символа: $\llbracket \cdot \rrbracket(\cdot)$ и $(\cdot) \ni (\cdot)$.

Термы определяются индуктивно: термом является любая переменная или константа по доказательствам; если x, y – ссылки, t, s – термы, то $t \cdot s$, $t + s$, $p_+(t)$, $p_-(t, x)$, $l_+(x)$, $l_-(x, y)$, $\text{subst}_i(t, x)$ также являются термами. Множество всех термов обозначим через Tm .

Формулы строятся из булевых констант, пропозициональных переменных и квазиатомарных формул с помощью булевых связок. *Квазиатомарные* (q -атомарных) формулы строятся по следующему правилу: если t – терм, x – ссылка и F – формула, то $\llbracket t \rrbracket F$ и $x \ni F$ являются q -атомарными формулами. Множество всех формул обозначим через Fm .

В отличие от логики доказательств $\mathcal{LP}$, в нашем случае операторы $\llbracket t \rrbracket F$ и $x \ni F$ связывают вхождения пропозициональных переменных в формулу F , т.е. делают их недоступными для подстановки. А именно, определим *свободные и связанные вхождения* пропозициональной переменной S в формулу F следующим образом:

- если F совпадает с S , то вхождение S в F считается свободным;
- булевы связки не меняют связанности переменных;
- если F имеет вид $\llbracket t \rrbracket G$ или $x \ni G$, то все вхождения переменной S в F считаются связанными.

Пусть F, G – формулы, S – пропозициональная переменная. Подстановка формулы G в формулу F вместо переменной S состоит в замене всех свободных вхождений S в F на формулу G . Полученную формулу будем обозначать $F(G/S)$. Пусть $\vec{G} = G_1, \dots, G_n$ – список формул, $\vec{S} = S_1, \dots, S_n$ – список пропозициональных переменных. Тогда $F(\vec{G}/\vec{S})$ обозначает результат одновременной подстановки формул G_i вместо свободных вхождений соответствующих переменных S_i в формулу F .

Введем следующие обозначения для пропозициональных аксиом:

- $\text{Ax}_1 = S_1 \rightarrow (S_2 \rightarrow S_1)$;
- $\text{Ax}_2 = (S_1 \rightarrow (S_2 \rightarrow S_3)) \rightarrow ((S_1 \rightarrow S_2) \rightarrow (S_1 \rightarrow S_3))$;
- $\text{Ax}_3 = (\neg S_1 \rightarrow S_2) \rightarrow ((\neg S_1 \rightarrow \neg S_2) \rightarrow S_1)$.

ОПРЕДЕЛЕНИЕ 2. Аксиомы и правила логики $\mathcal{LP}_{\text{sub}}$ следующие.

I. *Общие аксиомы:*

- A1 $\llbracket t \rrbracket F \rightarrow F(\vec{G}/\vec{S})$, где $\vec{G}$ – произвольный набор формул;
- A2 $\llbracket c_1 \rrbracket \text{Ax}_1$;
- A3 $\llbracket c_2 \rrbracket \text{Ax}_2$;
- A4 $\llbracket c_3 \rrbracket \text{Ax}_3$.

II. Аксиомы для операций:

A5 $\llbracket t \rrbracket(F \rightarrow G) \wedge \llbracket s \rrbracket F \rightarrow \llbracket t \cdot s \rrbracket G$;

A6 $\llbracket t \rrbracket F \vee \llbracket s \rrbracket F \rightarrow \llbracket t + s \rrbracket F$;

A7 $\llbracket t \rrbracket F \rightarrow \llbracket p_+(t) \rrbracket \llbracket t \rrbracket F$;

A8 $\neg \llbracket t \rrbracket F \wedge x \ni F \rightarrow \llbracket p_-(t, x) \rrbracket \neg \llbracket t \rrbracket F$;

A9 $x \ni F \rightarrow \llbracket l_+(x) \rrbracket (x \ni F)$;

A10 $x \ni F \wedge \neg(y \ni F) \rightarrow \llbracket l_-(x, y) \rrbracket \neg(y \ni F)$;

A11 $\llbracket t \rrbracket F \wedge x \ni G \rightarrow \llbracket \text{subst}_i(t, x) \rrbracket F(G/S_i), i = 1, 2, \dots$

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

ЗАМЕЧАНИЕ 1. Объясним, почему мы запрещаем подстановке действовать на переменные, находящиеся под операторами доказательств и хранения. Предположим, что подстановка (G/S) заменяет все вхождения переменной S на формулу G . Тогда следующий принцип должен быть верным

$$\llbracket p \rrbracket \llbracket q \rrbracket (S_1 \rightarrow S_1) \wedge x \ni B \rightarrow \llbracket \text{subst}_1(p, x) \rrbracket \llbracket q \rrbracket (B \rightarrow B).$$

Это означает, что если терм q доказывает конкретную формулу $S_1 \rightarrow S_1$, то он должен доказывать и все формулы вида $B \rightarrow B$, что противоречит представлению о доказательстве как конечном объекте, доказывающем лишь конечное число формул.

По этой причине, в логиках $\mathcal{LP}_{\text{sub}}$ и $\mathcal{LP}$ различается смысл формул вида $\llbracket t \rrbracket F$. А именно, в $\mathcal{LP}$ формула $\llbracket t \rrbracket F$ означает, что " t является доказательством формулы F ", в то время как в $\mathcal{LP}_{\text{sub}}$ та же формула означает, что " t является доказательством схемы F ". То есть в $\mathcal{LP}_{\text{sub}}$ из того, что $\llbracket t \rrbracket F$ является выводимой формулой, мы можем заключить, что доказуема схема F , тогда выводим также и любой ее подстановочный пример $F(\vec{G}/\vec{S})$. Однако в $\mathcal{LP}$ из выводимости $\llbracket t \rrbracket F$ следует выводимость только конкретной формулы F .

ЗАМЕЧАНИЕ 2. Формулировка логики $\mathcal{LP}_{\text{sub}}$ не содержит аксиом исчисления высказываний, однако все они в ней выводимы с помощью аксиом A1–A4, а следовательно, в ней выводимы и все тавтологии.

ЗАМЕЧАНИЕ 3. Для логики $\mathcal{LP}_{\text{sub}}$ верны теоремы о дедукции и подстановке в следующих формулировках.

ТЕОРЕМА О ДЕДУКЦИИ. Пусть Γ – конечное множество формул. Тогда

$$\mathcal{LP}_{\text{sub}} + \Gamma \vdash F \Leftrightarrow \mathcal{LP}_{\text{sub}} \vdash \bigwedge \Gamma \rightarrow F.$$

ТЕОРЕМА О ПОДСТАНОВКЕ. Пусть $\mathcal{LP}_{\text{sub}} \vdash F$. Тогда $\mathcal{LP}_{\text{sub}} \vdash F(\vec{G}/\vec{S})$, где $\vec{S}$ – список свободных переменных формулы F , а $\vec{G}$ – произвольный список формул, имеющий ту же длину, что и $\vec{S}$.

Важной особенностью логики доказательств $\mathcal{LP}$ является свойство интернализации. Логика доказательств с операцией подстановки также обладает этим свойством, но в отличие от $\mathcal{LP}$, в которой оно получается довольно легко (см. [2]), в $\mathcal{LP}_{\text{sub}}$ его доказательство требует дополнительных усилий.

ОПРЕДЕЛЕНИЕ 3. Любое конечное множество квазиатомарных формул вида $x \ni F$ условимся называть *таблицей ссылок*.

ОПРЕДЕЛЕНИЕ 4. Терм t называется *замкнутым*, если он не содержит переменных по доказательствам.

ТЕОРЕМА 1 (Свойство интернализации). Пусть $\mathcal{DB}$ – таблица ссылок. Тогда если $\mathcal{LP}_{\text{sub}} + \mathcal{DB} \vdash F$, то существует терм t и таблица ссылок $\mathcal{DB}'$ такие, что $\mathcal{LP}_{\text{sub}} + \mathcal{DB}' \vdash [t]F$.

Доказательство теоремы базируется на следующих леммах.

ЛЕММА 1. Пусть G является подстановочным примером пропозициональной тавтологии в языке $\mathcal{LP}_{\text{sub}}$. Тогда существует замкнутый терм s и таблица ссылок $\mathcal{DB}$ такие, что $\mathcal{LP}_{\text{sub}} + \mathcal{DB} \vdash [s]G$.

ДОКАЗАТЕЛЬСТВО. Индукция по выводу формулы G . Если G – подстановочный пример аксиомы исчисления высказываний, то воспользовавшись одной из аксиом A2–A4, соответствующей формуле G , и аксиомой A11, получим утверждение леммы. Если G получена по правилу МР, то применим аксиому A2.

ЛЕММА 2. Пусть δ является булевой комбинацией q -атомарных формул. Тогда существует замкнутый терм s и таблица ссылок $\mathcal{DB}$ такие, что $\mathcal{LP}_{\text{sub}} + \mathcal{DB} \vdash \delta \rightarrow [s]\delta$.

ДОКАЗАТЕЛЬСТВО. Для начала предположим, что δ является $\{\vee, \wedge\}$ -комбинацией q -атомарных формул или их отрицаний. Утверждение может быть доказано индукцией по числу $\wedge, \vee$. Если δ – q -атомарная формула или ее отрицание, т.е. является одной из формул вида $[t]B$, $x \ni B$, $\neg[t]G$, $\neg(x \ni G)$, то положим $\mathcal{DB} = \{y \ni G\}$ для новой ссылки y . Тогда воспользовавшись аксиомами A7–A10 получим

$$\begin{aligned} \mathcal{LP}_{\text{sub}} + \mathcal{DB} \vdash [t]B \rightarrow [\mathbf{p}_+(t)][t]B, & \quad x \ni B \rightarrow [\mathbf{l}_+(x)](x \ni B), \\ \mathcal{LP}_{\text{sub}} + \mathcal{DB} \vdash \neg[t]G \rightarrow [\mathbf{p}_-(t, y)]\neg[t]G, & \quad \neg(x \ni G) \rightarrow [\mathbf{l}_-(y, x)]\neg(x \ni G). \end{aligned}$$

Предположим, что δ имеет вид $\delta_1 \wedge \delta_2$ или $\delta_1 \vee \delta_2$. По предположению индукции существуют термы t_1, t_2 и таблица ссылок $\mathcal{DB}$ такие, что

$$\mathcal{LP}_{\text{sub}} + \mathcal{DB} \vdash \delta_1 \rightarrow [t_1]\delta_1 \quad \text{и} \quad \mathcal{LP}_{\text{sub}} + \mathcal{DB} \vdash \delta_2 \rightarrow [t_2]\delta_2. \quad (\text{IH})$$

Пусть $\delta = \delta_1 \wedge \delta_2$ (если необходимо, то расширяем $\mathcal{DB}$):

1. $\delta_1 \rightarrow (\delta_2 \rightarrow \delta_1 \wedge \delta_2)$, тавтология;
2. $[u](\delta_1 \rightarrow (\delta_2 \rightarrow \delta_1 \wedge \delta_2))$, лемма 1;
3. $[t_1]\delta_1 \rightarrow ([t_2]\delta_2 \rightarrow [(u \cdot t_1) \cdot t_2](\delta_1 \wedge \delta_2))$, аксиома A5, примененная дважды;
4. $\delta_1 \wedge \delta_2 \rightarrow [(u \cdot t_1) \cdot t_2](\delta_1 \wedge \delta_2)$, из (IH) и предыдущей формулы.

Пусть $\delta = \delta_1 \vee \delta_2$:

1. $\delta_i \rightarrow \delta_1 \vee \delta_2$, $i = 1, 2$, тавтология;
2. $[u_i](\delta_i \rightarrow \delta_1 \vee \delta_2)$, $i = 1, 2$, лемма 1;
3. $[t_i]\delta_i \rightarrow [u_i \cdot t_i](\delta_i \vee \delta_2)$, $i = 1, 2$, аксиома A5;
4. $[t_1]\delta_1 \vee [t_2]\delta_2 \rightarrow [u_1 \cdot t_1 + u_2 \cdot t_2](\delta_1 \vee \delta_2)$, аксиома A6;
5. $\delta_1 \vee \delta_2 \rightarrow [u_1 \cdot t_1 + u_2 \cdot t_2](\delta_1 \vee \delta_2)$, (IH).

Пусть теперь δ – произвольная булева комбинация q -атомарных формул $Q_1, \dots, Q_n$. Рассматривая их как пропозициональные атомы, можно построить дизъюнктивную нормальную форму $D = D(Q_1, \dots, Q_n)$ для δ такую, что формула $\delta \leftrightarrow D$

доказуема в исчислении высказываний. По лемме 1 существует терм u и таблица ссылок $\mathcal{DB}$ такие, что $\mathcal{LP}_{\text{sub}} + \mathcal{DB} \vdash \llbracket u \rrbracket (D \rightarrow \delta)$. Как было доказано выше, существует терм s и расширенная таблица ссылок $\mathcal{DB}' \supseteq \mathcal{DB}$ такие, что $\mathcal{LP}_{\text{sub}} + \mathcal{DB}' \vdash D \rightarrow \llbracket s \rrbracket D$. Таким образом $\mathcal{LP}_{\text{sub}} + \mathcal{DB}' \vdash \delta \rightarrow \llbracket u \cdot s \rrbracket \delta$.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1. Индукция по выводу формулы F . Если F – одна из аксиом A2–A11 или принадлежит $\mathcal{DB}$, то F является булевой комбинацией q -атомарных формул, и можно воспользоваться леммой 2. Предположим, что F является примером аксиомы рефлексии, а именно, F имеет вид $\llbracket s \rrbracket B \rightarrow B(C/S_i)$. Тогда мы последовательно выведем

1. $B(C/S_i) \rightarrow (\llbracket s \rrbracket B \rightarrow B(C/S_i))$, тавтология;
2. $\llbracket u \rrbracket (B(C/S_i) \rightarrow (\llbracket s \rrbracket B \rightarrow B(C/S_i)))$, лемма 1;
3. $\llbracket s \rrbracket B \rightarrow \llbracket \text{subst}_i(s, x) \rrbracket B(C/S_i)$, аксиома A11,
 $\mathcal{DB}' := \mathcal{DB} \cup \{x \ni C\}$;
4. $\llbracket \text{subst}_i(s, x) \rrbracket B(C/S_i) \rightarrow \llbracket u \cdot \text{subst}_i(s, x) \rrbracket (\llbracket s \rrbracket B \rightarrow B(C/S_i))$, аксиома A5;
5. $\llbracket s \rrbracket B \rightarrow \llbracket u \cdot \text{subst}_i(s, x) \rrbracket (\llbracket s \rrbracket B \rightarrow B(C/S_i))$.

С другой стороны,

6. $\neg \llbracket s \rrbracket B \rightarrow (\llbracket s \rrbracket B \rightarrow B(C/S_i))$, тавтология;
7. $\llbracket v \rrbracket (\neg \llbracket s \rrbracket B \rightarrow (\llbracket s \rrbracket B \rightarrow B(C/S_i)))$, лемма 1;
8. $\neg \llbracket s \rrbracket B \rightarrow \llbracket p_-(s, y) \rrbracket \neg \llbracket s \rrbracket B$, аксиома A8,
 $\mathcal{DB}' := \mathcal{DB}' \cup \{y \ni B\}$;
9. $\neg \llbracket s \rrbracket B \rightarrow \llbracket v \cdot p_-(s, y) \rrbracket (\llbracket s \rrbracket B \rightarrow B(C/S_i))$, аксиома A5.

Обозначим $w = u \cdot \text{subst}_i(s, x) + v \cdot p_-(s, y)$. Из формул 5 и 9 по аксиоме A6 получим, что

$$\mathcal{LP}_{\text{sub}} + \mathcal{DB}' \vdash \llbracket s \rrbracket B \vee \neg \llbracket s \rrbracket B \rightarrow \llbracket w \rrbracket (\llbracket s \rrbracket B \rightarrow B(C/S_i)).$$

Следовательно, $\mathcal{LP}_{\text{sub}} + \mathcal{DB}' \vdash \llbracket w \rrbracket (\llbracket s \rrbracket B \rightarrow B(C/S_i))$.

ЗАМЕЧАНИЕ 4. Для любой конечной таблицы ссылок $\mathcal{DB}$ логика $\mathcal{LP}_{\text{sub}} + \mathcal{DB}$ непротиворечива (см. теорему 4 ниже).

3. Символическая семантика. Так называемая символическая семантика для логики доказательств $\mathcal{LP}$ была предложена Мкртычевым в [7]. Модель состоит из таблицы приписываний, описывающей возможные доказательства утверждений, и оценки пропозициональных переменных. Доказано, что $\mathcal{LP}$ полна относительно такого класса моделей. В дальнейшем этот подход был развит Фиттингом в [8], предложившим модели типа Крипке для $\mathcal{LP}$ и доказавшим полноту логики относительно них. В этом разделе приводится символическая семантика для логики доказательств с операцией подстановки $\mathcal{LP}_{\text{sub}}$.

ОПРЕДЕЛЕНИЕ 5. Символическая модель $\mathcal{M} = (\#, v)$ логики $\mathcal{LP}_{\text{sub}}$ состоит из двух объектов: функции $\# : \text{Tm} \cup \text{LVar} \rightarrow 2^{\text{Fm}}$, ставящей в соответствие термам и переменным для ссылок множества формул, и истинностной оценки пропозициональных переменных v . Функция $\#$ называется *таблицей приписывания* и удовлетворяет условиям, выражающим *согласованность* $\#$ с операциями и константами по доказательствам. Для констант требуется, чтобы $\text{Ax}_i \in \#(c_i)$, $i = 1, 2, 3$, а условия на операции считываются с аксиом A5 – A11:

- если $F \rightarrow G \in \#(t)$ и $F \in \#(s)$, то $G \in \#(t \cdot s)$,
- $\#(t) \cup \#(s) \subseteq \#(t + s)$,

- если $F \in \#(t)$, то $\llbracket t \rrbracket F \in \#(\mathbf{p}_+(t))$,
- если $F \notin \#(t)$ и $F \in \#(x)$, то $\neg \llbracket t \rrbracket F \in \#(\mathbf{p}_-(t, x))$,
- если $F \in \#(x)$, то $(x \ni F) \in \#(\mathbf{l}_+(x))$,
- если $F \in \#(x)$ и $F \notin \#(y)$, то $\neg(y \ni F) \in \#(\mathbf{l}_-(x, y))$,
- если $F \in \#(t)$ и $G \in \#(x)$, то $F(G/S_i) \in \#(\text{subst}_i(t, x))$, $i = 1, 2, \dots$.

Определим истинность формулы F в модели $\mathcal{M}$ (обозначение $\mathcal{M} \models F$) индукцией по построению формулы F :

- для пропозициональных переменных $\mathcal{M} \models S \Leftrightarrow v(S) = \text{true}$,
- $\models$ коммутирует с булевыми связками,
- $\mathcal{M} \models x \ni F \Leftrightarrow F \in \#(x)$,
- $\mathcal{M} \models \llbracket t \rrbracket F \Leftrightarrow F \in \#(t)$ и $\mathcal{M} \models F(\vec{\sigma}/\vec{S})$ для всех $\vec{\sigma}$ – произвольных наборов булевых констант.

Модель $\mathcal{M} = (\#, v)$ называется *конечно-порожденной* если

- множество $\{x \in \text{PVar} \cup \text{LVar} \mid \#(x) \neq \emptyset\}$ конечно,
- для всех $e \in \text{LVar} \cup \text{Tm}$ множества $\#(e)$ конечны,
- множество $\{S \in \text{SVar} \mid v(S) = \text{true}\}$ конечно.

ОПРЕДЕЛЕНИЕ 6. Модель $\mathcal{M} = (\#, v)$ называется *рефлексивной*, если из того, что $F \in \#(t)$ следует $\mathcal{M} \models F(\vec{\sigma}/\vec{S})$ для всех термов t , формул F и всех наборов булевых констант $\vec{\sigma}$.

ОПРЕДЕЛЕНИЕ 7. Модель $\mathcal{M} = (\#, v)$ *согласована с таблицей ссылок $\mathcal{DB}$* , если $F \in \#(x)$ для всех формул $(x \ni F) \in \mathcal{DB}$.

Заметим, что из факта непротиворечивости теорий вида $\mathcal{LP}_{\text{sub}} + \mathcal{DB}$ и теоремы полноты (теорема 3) следует, что рефлексивная модель, согласованная с произвольной таблицей ссылок $\mathcal{DB}$, существует.

ТЕОРЕМА 2 (Корректность). Пусть $\mathcal{LP}_{\text{sub}} + \mathcal{DB} \vdash F$. Тогда $\mathcal{M} \models F$ для любой рефлексивной модели $\mathcal{M}$, согласованной с таблицей ссылок $\mathcal{DB}$.

ДОКАЗАТЕЛЬСТВО. Стандартная индукция по выводу в логике $\mathcal{LP}_{\text{sub}} + \mathcal{DB}$ формулы F .

ТЕОРЕМА 3 (Полнота). Пусть $\mathcal{LP}_{\text{sub}} \not\vdash F$. Тогда существует конечно-порожденная рефлексивная модель $\mathcal{M}$ такая, что $\mathcal{M} \not\models F$.

СЛЕДСТВИЕ 1. Пусть $\mathcal{LP}_{\text{sub}} + \mathcal{DB} \not\vdash F$. Тогда существует конечно-порожденная рефлексивная модель $\mathcal{M}$, согласованная с $\mathcal{DB}$ такая, что $\mathcal{M} \not\models F$.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 3 состоит из трех шагов. На шаге 1 с помощью алгоритма построения адекватного множества строится конечное множество формул $\mathcal{A}_F$. На шаге 2 строится так называемая *частичная модель* для формул из множества $\mathcal{A}_F$, в которой опровергается формула F . На шаге 3 частичная модель пополняется до модели, опровергающей формулу F , и доказывается, что построенная модель является конечно-порожденной и рефлексивной.

В дальнейшем нам понадобятся подстановки, заменяющие все свободные пропозициональные переменные формулы F на булевы константы $\top$ и $\perp$. Результат действия одной из таких подстановок мы будем обозначать через $F(\vec{\sigma})$, где $\vec{\sigma}$ – соответствующий набор булевых констант. Заметим, что $F(\vec{\sigma})$ не содержит свободных пропозициональных переменных. Через $\text{Eval } F$ мы обозначим множество всех

формул, полученных из F подстановкой булевых констант вместо всех свободных пропозициональных переменных. Условие $\mathcal{M} \models \text{Eval } F$ означает, что $\mathcal{M} \models F(\vec{\sigma})$ для всех формул $F(\vec{\sigma}) \in \text{Eval } F$.

Шаг 1: Алгоритм построения адекватного множества. По данной формуле F алгоритм строит множество формул $\mathcal{A}_F$, которое называется *адекватным множеством*. Нам потребуются следующие обозначения: пусть $\mathcal{T}_F$ есть множество всех термов вида $t\theta$, где t – терм, входящий в формулу F , а $\theta: \text{LVar}(F) \rightarrow \text{LVar}(F)$ – некоторая подстановка ссылочных переменных. Пусть M – множество формул, через $M\theta$ и $\text{Eval } M$ обозначим $\{F\theta \mid F \in M\}$ и $\bigcup_{F \in M} \text{Eval } F$ соответственно. Через $\text{SubFm}(F)$ обозначим множество всех подформул формулы F .

Алгоритм работает следующим образом.

1. Инициализация. Положим $\mathcal{A}_F := \text{SubFm}(F) \cup \neg \text{SubFm}(F)$, а затем $\mathcal{A}_F := \mathcal{A}_F\theta \cup \text{Eval } \mathcal{A}_F\theta$ для всех подстановок θ .
2. Вычислим $\mathcal{T}_F$. Если $(x \ni X) \in \mathcal{A}_F$, то добавим к множеству $\mathcal{A}_F$ все формулы вида $\llbracket t \rrbracket X$ и $\neg \llbracket t \rrbracket X$, где $t \in \mathcal{T}_F$.
3. Пусть $t_1, \dots, t_N$ – список всех термов из $\mathcal{T}_F$ такой, что если t_i – подтерм терма t_j , то $i < j$. Для каждого $l = 1, \dots, N$ расширим множество формул $\mathcal{A}_F$ следующим образом:
 - если t_l – переменная или константа по доказательствам, то к множеству $\mathcal{A}_F$ ничего не добавляем;
 - если $t_l = t \cdot s$ и $\llbracket t \rrbracket (X \rightarrow Y), \llbracket s \rrbracket X \in \mathcal{A}_F$, то добавим $\llbracket t \cdot s \rrbracket Y$ к множеству $\mathcal{A}_F$;
 - если $t_l = t + s$, $\llbracket t \rrbracket X \in \mathcal{A}_F$ или $\llbracket s \rrbracket X \in \mathcal{A}_F$, то добавим $\llbracket t + s \rrbracket X$ к множеству $\mathcal{A}_F$;
 - если $t_l = p_+(t)$ и $\llbracket t \rrbracket X \in \mathcal{A}_F$, то добавим $\llbracket p_+(t) \rrbracket \llbracket t \rrbracket X$ к множеству $\mathcal{A}_F$;
 - если $t_l = p_-(t, x)$ и $(x \ni X) \in \mathcal{A}_F$, то добавим $\llbracket p_-(t, x) \rrbracket \neg \llbracket t \rrbracket X$ к множеству $\mathcal{A}_F$;
 - если $t_l = l_+(x)$ и $(x \ni X) \in \mathcal{A}_F$, то добавим $\llbracket l_+(x) \rrbracket (x \ni X)$ к множеству $\mathcal{A}_F$;
 - если $t_l = l_-(x, y)$ и $(x \ni X) \in \mathcal{A}_F$, то добавим $\llbracket l_-(x, y) \rrbracket \neg(y \ni X)$ к множеству $\mathcal{A}_F$;
 - если $t_l = \text{subst}_i(t, x)$ и $\llbracket t \rrbracket X, (x \ni Y) \in \mathcal{A}_F$, то добавим $\text{SubFm}(\llbracket \text{subst}_i(t, x) \rrbracket X(Y/S_i))$ и $\text{SubFm}(\text{Eval } X(Y/S_i))$ к множеству $\mathcal{A}_F$.

Адекватное множество $\mathcal{A}_F$ получается в результате выполнения шагов 1–3. “шаги” уже заняты, и был пока только один?

Пусть $\mathcal{A}_{-1}, \mathcal{A}_0$ – это множество $\mathcal{A}_F$ после шага 1 и 2 алгоритма соответственно. Для $l = 1, \dots, N$ пусть $\mathcal{A}_l$ – это множество $\mathcal{A}_F$ после l -й итерации шага 3 (разбора терма t_l).

ЛЕММА 3. 1. $\mathcal{A}_0 \setminus \mathcal{A}_{-1}$ состоит из формул вида $\llbracket t \rrbracket E$ и $\neg \llbracket t \rrbracket E$.

2. Для $l = 0, \dots, N$ следующие утверждения верны:

- (a) $\mathcal{A}_l$ замкнуто относительно подформул;
- (b) если $\llbracket t \rrbracket X \in \mathcal{A}_l$, то $\text{Eval } X \subseteq \mathcal{A}_l$;
- (c) если $(x \ni X) \in \mathcal{A}_l$, то $\llbracket t \rrbracket X, \neg \llbracket t \rrbracket X, y \ni X, \neg(y \ni X) \in \mathcal{A}_l$ для каждого терма $t \in \mathcal{T}_F$ и каждой ссылки $y \in \text{LVar}(F)$;
- (d) если $Z \in \mathcal{A}_{l+1} \setminus \mathcal{A}_l$, то либо Z имеет вид $\llbracket t_{l+1} \rrbracket E$, либо $Z = X(Y/S_i)$, либо $Z \in \text{Eval } X(Y/S_i)$, где $X \in \mathcal{A}_l$, X не является q -атомарной формулой и существует ссылка x такая, что $(x \ni Y) \in \mathcal{A}_l$.

ДОКАЗАТЕЛЬСТВО. Утверждение пункта 1 очевидно следует из построения множества $\mathcal{A}_0$ на шаге 2 алгоритма построения адекватного множества. Доказательство пункта 2 проводится совместной индукцией по l .

ЛЕММА 4. Адекватное множество $\mathcal{A}_F$ согласованно с аксиомами для операций (группа II) в следующем смысле: если терм, представляющий операцию, принадлежит $\mathcal{T}_F$, а посылки соответствующей аксиомы принадлежат $\mathcal{A}_F$, то в адекватном множестве окажется и заключение аксиомы. Например, для операции p_- имеем, что если $p_-(t, x) \in \mathcal{T}_F$ и $x \in X$, $\neg \llbracket t \rrbracket X \in \mathcal{A}_F$, то $\llbracket p_-(t, x) \rrbracket \neg \llbracket t \rrbracket X \in \mathcal{A}_F$.

Шаг 2. Частичная модель.

ОПРЕДЕЛЕНИЕ 8. Предположим, что $LV \subseteq LVar$, $SV \subseteq SVar$ и T – множество термов такое, что $LVar(T) \subseteq LV$ и T замкнуто относительно подтермов и переименования ссылок из LV . Через $Fm(SV, LV, T)$ мы обозначим множество всех формул X , для которых $LVar(X) \subseteq LV$, $SVar(X) \subseteq SV$ и $SubTm(X) \subseteq T$. Положим

$$Fm(SV, LV, T) := Fm(SV, LV, T) \cup \{Eval X \mid X \in Fm(SV, LV, T)\}.$$

Частичная модель $\mathcal{M}_p = (\#_p, v_p)$ для $Fm(SV, LV, T)$ состоит из двух объектов: $\#_p$ – функции из $T \cup LV$ в множества формул из $Fm(SV, LV, T)$ и v_p – истинностной оценки пропозициональных переменных из SV . Функция $\#_p$ должна удовлетворять условиям из определения 5, ограниченным на термы из T .

Отношение “ $\mathcal{M}_p \models X$ ” определяется для $X \in Fm(SV, LV, T)$ так же, как и для обычных моделей. Определение конечно-порожденной частичной модели и рефлексивной частичной модели получается ограничением соответствующих определений для обычных моделей на множества SV , LV , T и $Fm(SV, LV, T)$.

Для любой формулы F обозначим $Fm(SVar(F), LVar(F), \mathcal{T}(F))$ как Fm_F .

ЛЕММА 5. Пусть $\mathcal{LP}_{sub} \not\models F$. Тогда существует конечно-порожденная рефлексивная частичная модель $\mathcal{M}_p$ для Fm_F такая, что $\mathcal{M}_p \not\models F$.

ДОКАЗАТЕЛЬСТВО. Предположим, что $\mathcal{LP}_{sub} \not\models F$. Запустим алгоритм построения адекватного множества на входе F , результатом будет множество $\mathcal{A}_F \subseteq Fm_F$. Для каждой формулы $\llbracket t \rrbracket X \in Fm_F$ и $(x \ni X) \in Fm_F$ зарезервируем новые пропозициональные переменные $p_{t,x}$ и $s_{x,X}$ соответственно. Пусть $X \in Fm_F$. Через X^0 обозначим результат замены всех внешних вхождений q -атомарных формул в X на соответствующие пропозициональные переменные.

Через $AX(F)$ обозначим конъюнкцию всех аксиом для операций логики $\mathcal{LP}_{sub}$, все q -атомарные подформулы которых входят в $\mathcal{A}_F$, и всех аксиом рефлексии вида $\llbracket t \rrbracket X \rightarrow X(\vec{\sigma})$, где $\llbracket t \rrbracket X \in \mathcal{A}_F$. Для любой $X \in Fm_F$ определим

$$\tilde{X} \Rightarrow (AX(F) \rightarrow X)^0.$$

Так как $\mathcal{LP}_{sub} \not\models F$, то $IB \not\models \tilde{F}$. Тогда существует оценка пропозициональных переменных w такая, что $w(\tilde{F}) = \text{false}$. Можно считать, что $w(S) = \text{false}$ для всех пропозициональных переменных S , не входящих в формулу $(AX(F))^0 \rightarrow F^0$. Построим следующие два множества:

$$\Gamma \Rightarrow \{X \mid X \in Fm_F, w(X^0) = \text{true}\},$$

$$\Delta \Rightarrow \{X \mid X \in Fm_F, w(X^0) = \text{false}\}.$$

Теперь определим искомую частичную модель $\mathcal{M}_p$: для $x \in \text{LVar}(F)$, $S \in \text{SVar}(F)$ и $t \in \mathcal{T}_F$ положим

$$\begin{aligned} X \in \#_p(x) &\Leftrightarrow (x \ni X) \in \Gamma, \\ X \in \#_p(t) &\Leftrightarrow \llbracket t \rrbracket X \in \Gamma, \\ v_p(S) &\Leftrightarrow S \in \Gamma. \end{aligned}$$

Заметим, что если $X \in \#_p(x)$, $Y \in \#_p(t)$, то формулы $x \ni X$ и $\llbracket t \rrbracket Y$ принадлежат множеству $\mathcal{A}_F$.

Индукцией по формуле $X \in \mathcal{A}_F$ проверяется, что

$$\begin{aligned} X \in \Gamma &\Rightarrow \mathcal{M}_p \models X, \\ X \in \Delta &\Rightarrow \mathcal{M}_p \not\models X. \end{aligned}$$

Осталось проверить, что $\mathcal{M}_p$ является рефлексивной конечно-порожденной частичной моделью. Индукцией по построению терма несложно доказать, что $\#_p$ удовлетворяет условиям на таблицу приписываний. Легко видеть, что $\mathcal{M}_p$ является конечно-порожденной моделью, так как множество $\mathcal{T}_F$ конечно и для любого терма $t \in \mathcal{T}_F$ множество $\#_p(t)$ конечно. Покажем, что $\mathcal{M}_p$ – рефлексивная модель. Пусть $\#_p(t, X)$, тогда $\llbracket t \rrbracket X \in \Gamma_0$ и множество $AX(F)$ содержит все аксиомы вида $\llbracket t \rrbracket X \rightarrow X(\vec{\sigma})$, где $\vec{\sigma}$ – произвольный набор булевых констант. Следовательно, $\text{Eval } X \subseteq \Gamma_0$, откуда $\mathcal{M}_p \models \text{Eval } X$.

Шаг 3. Пополнение.

ЛЕММА 6. Пусть $\mathcal{M}_p = (\#_p, v_p)$ – частичная модель для $\text{Fm}(SV, LV, T)$. Тогда существует модель $\mathcal{M} = (\#, v)$ такая, что для любой формулы $F \in \text{Fm}(SV, LV, T)$ выполняется следующая эквивалентность: $\mathcal{M} \models F \Leftrightarrow \mathcal{M}_p \models F$. Более того, если $\mathcal{M}_p$ является конечно-порожденной моделью, тогда такой же будет и $\mathcal{M}$, и если $\mathcal{M}_p$ – рефлексивная, то $\mathcal{M}$ также является рефлексивной моделью.

ДОКАЗАТЕЛЬСТВО. Определим таблицу приписываний $\#$ следующим образом: для всех $x \in \text{LVar} \cup \text{PVar}$ и для всех $t \in T$ положим

$$\begin{aligned} F \in \#(x) &\Leftrightarrow F \in \#_p(x), \\ F \in \#(t) &\Leftrightarrow F \in \#_p(t). \end{aligned}$$

Для оставшихся термов определим $\#$ индукцией по сложности терма так, чтобы выполнялись условия определения 5. Например, $\#(\mathbf{p}_-(t, x)) = \{\neg \llbracket t \rrbracket F \mid F \in \#(x), F \notin \#(t)\}$.

Теперь определим оценку v : для пропозициональной переменной S положим

$$v(S) = \text{true} \Leftrightarrow v_p(S) = \text{true}.$$

Индукцией по построению формулы $F \in \text{Fm}(SV, LV, T)$ доказывается, что

$$\mathcal{M} \models F \Leftrightarrow \mathcal{M}_p \models F.$$

Справедливость условий из определения 5, а также конечную порожденность $\mathcal{M}$ (если $\mathcal{M}_p$ такова) нетрудно установить индукцией по сложности соответствующих термов.

Осталось доказать, что $\mathcal{M}$ является рефлексивной моделью, если частичная модель $\mathcal{M}_p$ рефлексивна. Предположим, что $\#(s, G)$; нам необходимо проверить, что $\mathcal{M} \models G(\vec{\sigma})$ для любого набора булевых констант $\vec{\sigma}$. Это делается индукцией по построению терма s . Случаи, когда s является переменной или константой или $s \in T$ немедленно следуют из определения $\#$ и рефлексивности $\mathcal{M}_p$. Проверим утверждение для случая, когда $s = p_-(t, x)$ и $s \notin T$. Пусть $s = p_-(t, x)$, тогда по определению $\#$ имеем, что $\neg\#(t, F)$, $\#(x, F)$ и $G = \neg\llbracket t \rrbracket F$. Из $\neg\#(t, F)$ следует, что $\mathcal{M} \not\models \llbracket t \rrbracket F$, т.е. $\mathcal{M} \models \neg\llbracket t \rrbracket F$, а так как подстановка констант вместо пропозициональных переменных ничего в формуле G не меняет, мы получим желаемое утверждение. Остальные операции разбираются аналогично.

ТЕОРЕМА 4 (Непротиворечивость). Пусть $\mathcal{DB}$ – любая конечная таблица ссылок. Тогда $\mathcal{LP}_{\text{sub}} + \mathcal{DB}$ непротиворечива.

ДОКАЗАТЕЛЬСТВО. Достаточно построить рефлексивную модель $\mathcal{M} = (\#, v)$ такую, что $\mathcal{M} \models \bigwedge \mathcal{DB}$. Пусть таблица ссылок $\mathcal{DB}$ состоит из формул $x_1 \ni F_1, \dots, x_n \ni F_n$. Тогда положим $F_1 \in \#(x_1), \dots, F_n \in \#(x_n)$, а на термах определим $\#$ индукцией по сложности терма так, чтобы выполнялись условия определения 5 (аналогично тому, как это делалось в лемме 6). Положим $v(S) = \text{true}$ для любой пропозициональной переменной S . Осталось проверить, что модель $\mathcal{M}$ является рефлексивной, т.е. $\mathcal{M} \models \llbracket t \rrbracket F \Rightarrow \mathcal{M} \models \text{Eval } F$. Это делается индукцией по построению терма t .

КОММЕНТАРИЙ 1. Рассматриваемая логика $\mathcal{LP}_{\text{sub}}$ имеет арифметическую семантику, относительно которой логика корректна и полна. Однако эти результаты предполагается опубликовать в другой работе.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] S. Artemov, “Uniform provability realization of intuitionistic logic, modality and λ -terms”, *Electron. Notes Theor. Comput. Sci.*, **23**:1 (1999), 3–12.
- [2] S. Artemov, “Explicit provability and constructive semantics”, *Bulletine of Symbolic Logic*, **7**:1 (2001), 1–36.
- [3] S. Artemov, *Evidence-based common knowledge*, Technical Report TR-2004018, Graduate Center CUNY, New York, NY, 2005.
- [4] N. Rubtsova, T. Yavorskaya, “Operations on proofs and labels”, *J. Appl. Nonclass. Logic* (to appear).
- [5] T. Yavorskaya, “Negative operations on proofs and labels”, *J. Logic Comput.*, **15**:4 (2005), 517–537.
- [6] T. Yavorskaya, “Logic of proofs and labels with a complete set of operations”, *Journal of Logic and Computation*, **16**:5 (2006), 697–710.
- [7] A. Mkrtychev, “Models for the Logic of Proofs”, *Logical foundations of computer science*, Yaroslavl, 1997, Lecture Notes in Comput. Sci., **1234**, 1997, 266–275.
- [8] M. Fitting, “The logic of proofs, semantically”, *Ann. Pure Appl. Logic*, **132**:1 (2005), 1–25.

Н. М. Рубцова

Московский государственный университет

им. М. В. Ломоносова

E-mail: natalya_rubtsova@mail.ru

Поступило

05.02.2007

Исправленный вариант

13.06.2007