10. *Li S., Lu Y., Garrido J.* A review of discrete-time risk models // Rev. Real Acad. Ciencias Naturales. Ser. A. Matemáticas. 2009. **103**. 321–337.
11. *Dickson D.-C.-M., Waters H.-R.* Some optimal dividends problems // ASTIN Bull. 2004. **34**. 49–74.
12. *Булинская Е.В.* Теория риска и перестрахование. М.: ООО "Мэйлор", 2008.
13. *Беллман Р.* Динамическое программирование. М.: ИЛ, 1960.
14. *Rachev S., Stoyanov S., Fabozzi F.* A probability metrics approach to financial risk measures. Oxford, UK: John Wiley & Sons, 2011.
15. *Billingsley P.* Convergence of probability measures. 2nd ed. N.Y.: Wiley, 1999.
16. *Cramer H.* Collective risk theory: A survey of the theory from the point of view of the theory of stochastic process. Stockholm: Ab Nordiska Bokhandeln, 1955.
17. *Palmowski Z., Ramsden L., Papaioannou A.D.* Parisian ruin for the dual risk process in discrete-time // arXiv:1708. 06785v1 [math.PR] 19 Aug 2017.
18. *Fahim A., Zhu Li.* Optimal investment in a dual risk model // arXiv:1510. 04924v2 [q-fin.RM] 2 Feb 2023.
19. *Avanzi B., Gerber H.U., Shiu E.S.* Optimal dividends in the dual model // Insurance: Mathematics and Economics. 2007. **41**, N 1. 111–123.
20. *Bergel A.I., Rodrigues-Martinez E.V., Egidio dos Reis A.D.* On dividends in the phase-type dual risk model // Scand. Actuar. J. 2017. **2017**. 1–24.
21. *Cheung E.C., Drekic S.* Dividend moments in the dual risk model: exact and approximate approaches // ASTIN Bull. 2008. **38**, N 2. 399–422.
22. *Ng A.C.* On a dual model with a dividend threshold // Insurance: Mathematics and Economics. 2009. **44**, N 2. 315–324.
23. *Bulinskaya E.V.* New dividend strategies // Applied Modeling Techniques and Data Analysis 2. London: Willey, 2021. 39–52.
24. *Albrecher H., Badescu A., Landriault D.* On the dual risk model with tax payment // Insurance: Mathematics and Economics. 2008. **42**, N 3. 1086–1094.
25. *Willmot G.E.* Ruin probabilities in the compound binomial model // Insurance: Mathematics and Economics. 1993. **12**, N 2. 133–142.
26. *Li S., Sendova K.P.* The finite-time ruin probability under the compound binomial risk model // Eur. Actuar. J. 2013. **3**, N 1. 249–271.
27. *Shaked M., Shantikumar J.G.* Stochastic orders. Springer Series Statistics. N.Y.: Springer, 2007.
28. *Mulero J., Sordo M.A.* Two stochastic dominance criteria based on tail comparisons // Appl. Stochast. Models in Business and Industry. 2017. **33**, N 6. 575–589.

Поступила в редакцию
07.06.2023

УДК 510.649

НОРМАЛИЗАЦИЯ ТЕРМОВ В ТОЧНЫХ МОДЕЛЯХ ЛОГИКИ ДОКАЗАТЕЛЬСТВ LP

В. Н. Крупский[1]

Базисная модель логики свидетельств является точной, если конструкторы свидетельских термов $\cdot, +, !$ в модели интерпретируются в точности в соответствии с их неформальным пониманием как применение правила *modus ponens*, объединение и верификация свидетельств. В статье строится пример точной базисной модели для логики доказательств LP и доказывается, что в точных моделях LP каждый терм эквивалентен некоторому полиному доказательств.

Ключевые слова: эпистемическая логика, логика доказательств, базисная модель логики свидетельств, свойство точности, полином доказательств.

A basic justification model is sharp when the evidence term constructors $\cdot, +, !$ in it mean exactly the application of *modus ponens* rule, the union and the verification of evidences. We

---

[1] *Крупский Владимир Николаевич* — канд. физ.-мат. наук, доцент каф. математической логики и теории алгоритмов мех.-мат. ф-та МГУ, e-mail: vladimir.krupski@math.msu.ru.

Krupski Vladimir Nikolaevich — Candidate of Physical and Mathematical Sciences, Associate Professor, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Logic and Theory of Algorithms.

construct an example of a sharp model for the logic of proofs LP and establish that in any sharp model of LP every proof term is equivalent to some proof polynomial.

Key words: epistemic logic, logic of proofs, basic justification model, sharpness, proof polynomial.

DOI: 10.55959/MSU0579-9368-1-64-6-7

Логика доказательств LP — исторически первая логика свидетельств — была предложена С.Н. Артемовым [1] в качестве формализма, описывающего пропозициональные свойства арифметических предикатов доказательств вместе с вычислимыми операциями над доказательствами: "$\cdot$" (применение правила *modus ponens*), "+" (объединение двух доказательств в единое целое), " ! " (верификация доказательств). Язык LP содержит выражения двух сортов — термы (Tm) и формулы (Fm), определяемые грамматикой

$$Tm ::= J \mid Tm \cdot Tm \mid Tm + Tm \mid !Tm, \quad Fm ::= \bot \mid P \mid Fm \to Fm \mid Tm{:}Fm,$$

где J — множество атомарных доказательств, а P — множество атомарных высказываний. Бинарная связка ":" выражает арифметический предикат доказательств "x доказывает y".

Базисная часть LP задается исчислением LP_0 со схемами аксиом:

A1 — A10: аксиомы классического исчисления высказываний в языке LP,
A11: $t{:}F \to F$,
A12: $s{:}(F \to G) \to (t{:}F \to (s \cdot t){:}G)$,
A13: $s{:}F \to (s+t){:}F, \quad t{:}F \to (s+t){:}F$,
A14: $t{:}F \to !t{:}(t{:}F)$

и правилом вывода *modus ponens*: $F \to G,\ F \vdash G$.

В множестве J выделяется подмножество $Cnst \subset J$ так называемых констант; остальные элементы считаются переменными. Спецификацией констант называется множество CS, состоящее из формул вида $c{:}\ A$, где $c \in Cnst$, а A — одна из аксиом системы LP_0. Логика доказательств $\mathsf{LP} = \mathsf{LP}_0(CS)$ получается в результате добавления к системе LP_0 всех формул $c{:}\ A \in CS$ в качестве аксиом. Множество CS фиксирует выбор имен для атомарных доказательств аксиом. При этом предполагается, что каждая аксиома A входит в некоторую формулу $c{:}A \in CS$.[2]

Для наших целей необходим более детальный выбор имен, связанных с аксиомами **A12 — A14**. Дополнительно потребуем, чтобы для каждых $s, t \in Tm$ существовали выделенные константы $\mathbf{o_{s,t}}$, $\mathbf{l_{s,t}}$, $\mathbf{r_{s,t}}$ и $\mathbf{c_t}$, для которых CS содержит все формулы одного из видов

$$\begin{array}{ll} \mathbf{o_{s,t}}{:}(s{:}(F \to G) \to (t{:}\ F \to (s \cdot t){:}G)), & \\ \mathbf{l_{s,t}}{:}(s{:}F \to (s+t){:}F), & \mathbf{r_{s,t}}{:}(t{:}F \to (s+t){:}F), \\ \mathbf{c_t}{:}(t{:}F \to !t{:}(t{:}F)) & \end{array}$$

и не содержит никаких других формул $c{:}A$, где c — одна из выделенных констант.

Символическая семантика для логики LP (модели Мкртычева) была предложена в [2]. Мы используем эквивалентное определение базисной модели из [3]. Модель задается интерпретирующим отображением $*\colon Fm \to \{0,1\}$, $*\colon Tm \to 2^{Fm}$. Истинностные значения для булевых связок вычисляются в соответствии с классической логикой, причем $(t{:}F)^* = 1 \Leftrightarrow F \in t^*$. При этом на отображение $*$ накладываются дополнительные условия, обеспечивающие истинность аксиом **A11 — A14** и CS. Пусть $S, T \subseteq Fm$, $t \in Tm$. Положим

$$S \rhd T = \{G \mid F \to G \in S \text{ и } F \in T \text{ для некоторой формулы } F\}$$

и $\nabla t = \{t{:}F \mid F \in t^*\}$. Требуется выполнение следующих условий: $c{:}A \in CS \Rightarrow A \in c^*$, $\quad F \in t^* \Rightarrow F^* = 1$,

$$s^* \rhd t^* \subseteq (s \cdot t)^*, \quad s^* \cup t^* \subseteq (s+t)^*, \quad \nabla t \subseteq (!t)^*. \tag{1}$$

[2]В исходной работе [1] использовалась спецификация, содержащая все формулы указанного вида, что затрудняет отслеживание конкретных аксиом в выводе.

В [2] установлено существование таких моделей, а также корректность и полнота логики LP относительно символической семантики (см. также [3]).

Точные модели. При неформальном использовании языка логики свидетельств для моделирования эпистемических сценариев (см. [4]) операции $\cdot, +, !$ обычно понимают как $\rhd$, $\cup$, ∇. Это соответствует определению *точной модели*, которое отличается от приведенного выше заменой "$\subseteq$" на "$=$" в условиях (1), а также условием точности интерпретации констант: $c^* = \{A \mid c\colon A \in CS\}$. Мы строим пример точной модели для логики LP.

Отраженным фрагментом логики LP называется множество всех формул вида $t\colon F$, выводимых в логике LP. В [5] найдено независимое дедуктивное описание отраженного фрагмента в виде исчисления rLP, в котором спецификация констант CS выступает в роли множества аксиом, а правила вывода следующие:

$$\frac{s\colon(F \to G)\; t\colon F}{(s \cdot t)\colon G}, \quad \frac{t\colon F}{!t\colon(t\colon F)}, \quad \frac{s\colon F}{(s+t)\colon F}, \quad \frac{t\colon F}{(s+t)\colon F}.$$

Определим интерпретирующее отображение $*$: положим $t^* := \{F \mid \mathsf{rLP} \vdash t\colon F\}$, зададим истинностные значения p_i^* для $p_i \in P$ произвольно и продолжим отображение $*$ на все формулы согласно определению модели.

Лемма 1. *Отображение $*$ задает базисную модель логики* LP.

Доказательство. Рассмотрим модель Мкртычева $\bullet$, совпадающую с $*$ на всех атомарных высказываниях и на всех термах. Отличие моделей Мкртычева от базисных моделей состоит в другом определении истинности квазиатомарных формул: $(t\colon F)^\bullet = 1 \Leftrightarrow F \in t^\bullet \wedge F^\bullet = 1$, что автоматически обеспечивает выполнение аксиомы **A11**, поэтому условие рефлексивности $F \in t^\bullet \Rightarrow F^\bullet = 1$ для моделей Мкртычева не требуется. Справедливость включений (1), из которых следует истинность остальных аксиом исчисления LP_0, легко проверяется непосредственно. Отсюда следует истинность всех формул, принадлежащих CS. Тем самым $\bullet$ является моделью LP.

Известна конструкция [2, 3], преобразующая произвольную модель Мкртычева в базисную модель с сохранением предиката истинности. Достаточно переопределить значения $t^\bullet$, заменив их на $t^\bullet \cap \{F \mid F^\bullet = 1\}$, и воспользоваться определением истинности для базисных моделей. В нашем случае это преобразование не изменит значений $t^\bullet = t^*$, так как t^* содержит только теоремы LP. Таким образом, результатом преобразования будет в точности отображение $*$. Лемма доказана.

Теорема 1. *Отображение $*$ задает точную модель логики* LP.

Доказательство. Теорема следует из леммы 1 и вида правил исчисления rLP. Теорема доказана.

Та же конструкция позволяет построить и другие примеры точных моделей логики LP. Достаточно применить ее к расширению исчисления rLP дополнительной аксиомой вида $x\colon F$, где формула F истинна в уже построенной модели, а x — "свежая" переменная, не встречающаяся в формуле F. Конструкцию можно итерировать.

Нормализация термов. Пусть точная модель $*$ логики LP фиксирована. Два терма s и t назовем эквивалентными: $s \sim t$, если $s^* = t^*$.

Лемма 2. *Операции $\cdot$ и $+$ согласованы с отношением эквивалентности $\sim$. С точностью до отношения $\sim$ операция $+$ ассоциативна, коммутативна и идемпотентна, а операция $\cdot$ дистрибутивна относительно $+$.*

Доказательство. Утверждение леммы непосредственно следует из определения операций. Например, установим правую дистрибутивность. Ввиду условия точности $G \in ((s_1 + s_2) \cdot t)^*$ равносильно тому, что для некоторой формулы $F \in t^*$ формула $F \to G$ содержится в одном из множеств s_1^* или s_2^*. Тогда G принадлежит одному из множеств $(s_1 \cdot t)^*$ или $(s_2 \cdot t)^*$, откуда $G \in (s_1 \cdot t + s_2 \cdot t)^*$. Обратное включение устанавливается аналогично. Лемма доказана.

Терм называется *мономом*, если в нем нет операции $+$, а операция $!$ применяется только к атомарным подтермам. *Полином доказательств* — это сумма нескольких мономов. С точностью до отношения эквивалентности порядок суммирования мономов несуществен (лемма 2). Порядок выполнения операций внутри мономов оказывается существенным, так как операция $\cdot$ не является ассоциативной и коммутативной.

Лемма 3. *Справедливы следующие эквивалентности:*

$$!(s\cdot t)\sim(\mathbf{o}_{\mathbf{s},\mathbf{t}}\cdot!s)\cdot!t\,,\quad !(s+t)\sim\mathbf{l}_{\mathbf{s},\mathbf{t}}\cdot!s+\mathbf{r}_{\mathbf{s},\mathbf{t}}\cdot!t\,,\quad !!t\sim\mathbf{c}_{\mathbf{t}}\cdot!t\,.$$

Доказательство. 1. Рассмотрим произвольную формулу $X\in(\,!(s\cdot t)\,)^*$. Она имеет вид $(s\cdot t){:}G$, причем $X^*=1$, откуда $G\in(s\cdot t)^*$. По свойству точности модели $(F\to G)\in s^*$ для некоторой формулы $F\in t^*$. Тогда $s{:}(F\to G)\in(!s)^*$, $t{:}F\in(!t)^*$ и

$$X=(s\cdot t){:}G\in(\,(\mathbf{o}_{\mathbf{s},\mathbf{t}})^*\rhd(!s)^*)\rhd(!t)^*=(\,(\mathbf{o}_{\mathbf{s},\mathbf{t}}\cdot!s)\cdot!t\,)^*.$$

Теперь рассмотрим произвольную формулу $X\in(\,(\mathbf{o}_{\mathbf{s},\mathbf{t}}\cdot!s)\cdot!t\,)^*$. По свойству точности модели найдутся формулы $Y\in(!t)^*$ и $Z\in(!s)^*$, для которых $(Z\to(Y\to X))\in(\mathbf{o}_{\mathbf{s},\mathbf{t}})^*$. Но множество $(\mathbf{o}_{\mathbf{s},\mathbf{t}})^*$ содержит только формулы вида **A12** с данными s и t, поэтому $X=(s\cdot t){:}G$ для некоторой формулы G. Кроме того, $X^*=1$, откуда $G\in(s\cdot t)^*$ и $(s\cdot t){:}G\in(\,!(s\cdot t)\,)^*$.

2. Произвольная формула $X\in(\,!(s+t)\,)^*$ имеет вид $(s+t){:}G$ для некоторой формулы $G\in(s+t)^*$. Ввиду точности модели возможны два варианта: $G\in s^*$ или $G\in t^*$. В первом случае $s{:}G\in(!s)^*$ и

$$X=(s+t){:}G\,\in\,(\mathbf{l}_{\mathbf{s},\mathbf{t}})^*\rhd(!s)^*=(\,\mathbf{l}_{\mathbf{s},\mathbf{t}}\cdot!s\,)^*\subseteq(\,\mathbf{l}_{\mathbf{s},\mathbf{t}}\cdot!s+\mathbf{r}_{\mathbf{s},\mathbf{t}}\cdot!t\,)^*.$$

Второй случай разбирается аналогично.

Пусть теперь $X\in(\,\mathbf{l}_{\mathbf{s},\mathbf{t}}\cdot!s+\mathbf{r}_{\mathbf{s},\mathbf{t}}\cdot!t\,)^*$, т.е. X принадлежит одному из множеств $(\,\mathbf{l}_{\mathbf{s},\mathbf{t}}\cdot!s)^*$ или $(\mathbf{r}_{\mathbf{s},\mathbf{t}}\cdot!t\,)^*$. Разберем первый случай. По свойству точности модели найдется формула $Y\in(!s)^*$, для которой $(Y\to X)\in(\mathbf{l}_{\mathbf{s},\mathbf{t}})^*$. Но множество $(\mathbf{l}_{\mathbf{s},\mathbf{t}})^*$ содержит только формулы вида **A13** (левый вариант) с данными s и t, поэтому $X=(s+t):F$ для некоторой формулы F. Так как $X^*=1$, то $F\in(s+t)^*$, откуда $(s+t){:}F\in(\,!(s+t)\,)^*$. Второй случай аналогичен.

3. Произвольная формула $X\in(!!t)^*$ имеет вид $!t:G$ для некоторой формулы G и $X^*=1$. Поэтому $G^*=1$, $G\in(!t)^*$ и имеет вид $t{:}F$ для некоторой формулы $F\in(t)^*$. Но $(t{:}F\to!t{:}t{:}F)\in\mathbf{c}_{\mathbf{t}}{}^*$ и $t{:}F\in(!t)^*$, откуда $X=!t{:}t{:}F\in(\mathbf{c}_{\mathbf{t}}\cdot!t)^*$.

Пусть теперь $X\in(\mathbf{c}_t\cdot!t)^*$. Тогда $X^*=1$ и для некоторой формулы $Y\in(!t)^*$ имеем $(Y\to X)\in\mathbf{c}_{\mathbf{t}}{}^*$. Но $\mathbf{c}_{\mathbf{t}}{}^*$ состоит из формул вида **A13** с данным t, поэтому $X=!t{:}t{:}F$ для некоторой формулы F и $X\in(!!t)^*$. Лемма доказана.

Теорема 2. *В точной модели логики* LP *каждый терм эквивалентен некоторому полиному доказательств.*

Доказательство опирается на леммы 2, 3. Теорема доказана.

Множество всех полиномов доказательств, эквивалентных данному терму, зависит от выбора точной модели. Но существует единый полином доказательств, который эквивалентен исходному терму во всех точных моделях. Его конструкция легко извлекается из подробного доказательства теоремы 1.

СПИСОК ЛИТЕРАТУРЫ

1. *Artemov S.* Explicit provability and constructive semantics // Bull. Symbol. Log. 2001. **7**, N 1. 1–36.
2. *Mkrtychev A.* Models for the logic of proofs // Logical Foundations of Computer Science: Int. Symp. LFCS'97 / Ed. by S. Adyan, A. Nerode. Lect. Notes Comput. Sci. Vol. 1234. Cham: Springer, 1997. 266–275.
3. *Artemov S., Fitting M.* Justification logic: Reasoning with reasons. Cambridge: Cambridge University Press, 2019.
4. *Artemov S.* Justification awareness models // Logical Foundations of Computer Science: Int. Symp. LFCS 2018 / Ed. by S. Artemov, A. Nerode. Lect. Notes Comput. Sci. Vol. 10703. Cham: Springer, 2018. 22–36.
5. *Krupski N.* On the complexity of the reflected logic of proofs // Theor. Comput. Sci. 2006. **357**, N 1–3, 136–142.

Поступила в редакцию
07.04.2023