ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ

УДК 510.52, 510.643

МОДЕЛИРОВАНИЕ АРИФМЕТИКИ В ЯЗЫКЕ ПЕРВОГО ПОРЯДКА, ОБОГАЩЕННОМ ТЕМПОРАЛЬНЫМИ КВАНТОРАМИ[1]

Котикова Е.А.[*], **Рыбаков М.Н.**[*,**,***]
[*]Кафедра функционального анализа и геометрии
[**]ЗАО НИИ ЦПС, г. Тверь
[***]Университет Витватерсранда, г. Йоханнесбург

Поступила в редакцию 29.08.2016, после переработки 07.10.2016.

Рассматривается язык классической логики предикатов с равенством, обогащенный модальностями темпоральной логики **CTL**[*]. В качестве семантики для него предлагаются серийные шкалы Крипке с постоянными предметными областями. Строится погружение множества арифметических формул, истинных в стандартной модели арифметики, во множество всех модальных предикатных формул, истинных в указанном классе шкал Крипке. Извлекается ряд следствий, касающихся алгоритмических, синтаксических и семантических свойств большого класса логик в рассматриваемом языке.

Ключевые слова: логика первого порядка, логика ветвящегося времени, рекурсивная перечислимость, семантика Крипке.

Вестник ТвГУ. Серия: Прикладная математика. 2016. № 4. С. 5–19.

Введение

В данной работе речь пойдет о формальном языке, получающемся за счет «соединения» двух других, каждый из которых сам по себе эффективно используется в математике. Первый из них — это язык классической логики предикатов **QCL**, а второй — это язык логики ветвящегося времени **CTL**[*]. Основная цель, которую мы ставим, — продемонстрировать выразительную силу этого «соединения», показав, в частности, что она существенно превосходит выразительную силу каждого из «соединяемых» языков.

Несмотря на то, что классическая логика предикатов алгоритмически неразрешима (см., например, [1], глава 10), она, тем не менее, имеет эффективные описания в виде исчислений [2, 8, 9], для классического языка первого порядка хорошо развита теория моделей (см., например, [4]), на основе классической логики предикатов определены многие важные математические теории (например, теория множеств, формальная арифметика и др. [8]). С другой стороны, неразрешимость и

[1]Работа выполнена при поддержке РФФИ, гранты 14–06–00298-а и 16–07–01272-а.

невозможность выразить некоторые условия (например, конечность, связность) и операции (например, транзитивное замыкание бинарного отношения) вынуждают для решения многих прикладных задач прибегать к иным формальным языкам.

Язык логики $\mathbf{CTL}^*$ является пропозициональным, но помимо привычных пропозициональных связок конъюнкции, дизъюнкции, импликации, отрицания и им подобных содержит особые темпоральные модальности — так называемые кванторы пути и кванторы состояния, — позволяющие описывать свойства вычислений, или, более общо, свойства цепочек событий, происходящих с течением времени; при этом обычно ограничиваются модальностями, которые описывают только «будущее» (см., например, [3, 5]).

Кванторы пути — это модальности $\boldsymbol{A}$ и $\boldsymbol{E}$, позволяющие строить формулы вида $\boldsymbol{A}\varphi$ и $\boldsymbol{E}\varphi$. Если считать, что путь — это бесконечная последовательность состояний некоторой системы, то $\boldsymbol{A}\varphi$ можно понимать в состоянии s как «в любом пути, выходящем из s, верно φ», а $\boldsymbol{E}\varphi$ — как «в некотором пути, выходящем из s, верно φ».

Кванторы состояния — это модальности $\boldsymbol{X}$, $\boldsymbol{F}$, $\boldsymbol{G}$ и $\boldsymbol{U}$, позволяющие строить формулы вида $\boldsymbol{X}\varphi$, $\boldsymbol{F}\varphi$, $\boldsymbol{G}\varphi$ и $(\varphi\boldsymbol{U}\psi)$. Буквы X, F, G, U, используемые для обозначения кванторов состояний взяты из слов «next», «future», «globally», «until», соответственно. Если имеется путь $s_0, s_1, s_2, \ldots$, то по отношению к этому пути $\boldsymbol{X}\varphi$ означает, что φ верно в s_1, $\boldsymbol{F}\varphi$ — что φ верно хотя бы в одном из его состояний, $\boldsymbol{G}\varphi$ — что φ верно в каждом его состоянии, и, наконец, $(\varphi\boldsymbol{U}\psi)$ — что имеется состояние s_k, в котором верно ψ, при этом в каждом из состояний $s_0, \ldots, s_{k-1}$ верно φ.

Таким образом, язык логики $\mathbf{CTL}^*$ позволяет описывать вычисления и состояния, возникающие в этих вычислениях. Отметим, что эта логика разрешима, хотя сложность проблемы разрешения для нее довольно высока [19].

Мы покажем, что при добавлении кванторов пути и кванторов состояния к языку первого порядка получается язык, позволяющий описывать множества, не являющиеся арифметическими. В частности, мы покажем, что даже при некоторых ограничениях этот язык позволяет описать множество всех утверждений, истинных в стандартной модели арифметики с операциями сложения и умножения.

1. Логика $\mathbf{QCTL}^*$.E.CD

Пусть имеется язык, содержащий счетное множество предметных переменных, счетное множество предметных констант, счетное множество функциональных символов любой местности, счетное множество предикатных букв любой местности, символ $=$, логическиую константу $\bot$, логическую связку $\to$, кванторный символ $\forall$, модальности $\boldsymbol{A}$, $\boldsymbol{X}$, $\boldsymbol{U}$, а также символы скобок и запятую. Понятия терма, формулы пути и формулы состояния определим обычным образом.

Термом считаем каждую предметную переменную x, каждую предметную константу c и любое выражение вида $f(t_1, \ldots, t_n)$, где f — n-местный функциональный символ, а $t_1, \ldots, t_n$ — термы.

Формулой состояния считаем константу $\bot$, все выражения вида $t_1 = t_2$, где t_1 и t_2 — термы, все выражения вида $P(t_1, \ldots, t_n)$, где P — n-местная предикатная буква, а $t_1, \ldots, t_n$ — термы, все выражения вида $(\varphi \to \psi)$ и $\forall x\, \varphi$, где φ и ψ —

формулы состояния, а x — предметная переменная, и все выражение вида $\boldsymbol{A}\varphi$, где φ — формула пути.

Формулой пути считаем каждую формулу состояния, все выражения вида $(\varphi \to \psi)$ и $\forall x\, \varphi$, где φ и ψ — формулы пути, а x — предметная переменная, а также все выражения вида $\boldsymbol{X}\varphi$ и $(\varphi \boldsymbol{U} \psi)$, где φ и ψ — формулы состояния.

Определим константу $\top$, связки $\neg$, $\vee$, $\wedge$, $\leftrightarrow$, кванторы вида $\exists x$, а также модальности $\boldsymbol{E}$, $\boldsymbol{F}$ и $\boldsymbol{G}$ как следующие сокращения: $\neg\varphi = (\varphi \to \bot)$, $\top = \neg\bot$; $(\varphi \vee \psi) = (\neg\varphi \to \psi)$, $(\varphi \wedge \psi) = \neg(\varphi \to \neg\psi)$, $(\varphi \leftrightarrow \psi) = ((\varphi \to \psi) \wedge (\psi \to \varphi))$, $\exists x\, \varphi = \neg\forall x\, \neg\varphi$, $\boldsymbol{E}\varphi = \neg\boldsymbol{A}\neg\varphi$, $\boldsymbol{F}\varphi = (\top \boldsymbol{U} \varphi)$ и $\boldsymbol{G}\varphi = \neg\boldsymbol{F}\neg\varphi$.

При записи формул будем опускать некоторые скобки, определяя силу связывания формул по убыванию: $\neg$, $\forall x$, $\exists x$, $\boldsymbol{X}$, $\boldsymbol{F}$, $\boldsymbol{G}$, $\boldsymbol{U}$, $\wedge$, $\vee$, $\leftrightarrow$, $\to$.

Теперь определим семантику для этого языка. Сделаем это в несколько этапов: нам понадобятся понятия шкалы и модели Крипке, а также понятие интерпретации предметных переменных, используя которые, мы сможем описать, какие формулы языка будем считать истинными.

Шкалой Крипке называется набор $\mathfrak{F} = \langle W, R\rangle$, где W — непустое множество, а R — бинарное отношение на W. Элементы множества W будем называть состояниями, а отношение R — отношением достижимости. Если пара состояний s и t находится в отношении R, то пишем sRt; при этом говорим что из состояния s достижимо состояние t. Отношение R называется серийным, если для всякого $s \in W$ существует $t \in W$ такое, что sRt. Шкала $\mathfrak{F} = \langle W, R\rangle$ называется серийной, если отношение достижимости в ней серийно.

В дальнейшем мы будем рассматривать только серийные шкалы Крипке. Содержательно это означает, что мы считаем время неограниченным в «будущем».

Бесконечную последовательность $\pi = \{s_k\}_{k=0}^{\infty}$ называют путем в шкале $\mathfrak{F} = \langle W, R\rangle$, если элементы этой последовательности являются состояниями из W, причем для каждого $k \in \mathbb{N}$ выполнено условие $s_k R s_{k+1}$. Состояние s_0 называется началом пути $\{s_k\}_{k=0}^{\infty}$. Заметим, что в серийной шкале каждое состояние является началом хотя бы одного пути.

Можно сказать, что шкала Крипке определяется структуру возможных переходов между состояниями некоторой системы. Применительно к вычислениям, пути, начинающиеся в состоянии s шкалы Крипке определяют возможные вычисления, начинающиеся в s.

Предикатной шкалой Крипке будем называть набор $\mathfrak{F}(D) = \langle W, R, D\rangle$, где $\langle W, R\rangle$ — шкала Крипке, а D — непустое множество, называемое предметной областью. Каждому состоянию $s \in W$ поставим в соответствие модель $\mathfrak{M}_s = \langle D, I_s\rangle$ для классического языка первого порядка, где I_s — интерпретация констант, функциональных символов и предикатных букв в D. Пусть I — функция, которая каждому состоянию $s \in W$ ставит в соответствие интерпретацию I_s модели $\mathfrak{M}_s$. Тогда набор $\mathfrak{M} = \langle W, R, D, I\rangle$ будем называть предикатной моделью Крипке на шкале $\mathfrak{F}(D)$.

Пусть α — интерпретация предметных переменных в D, т. е. для $\alpha(x) \in D$ для каждой предметной переменой x. Пусть $s \in W$; расширим α на множество всех термов, определив для каждого терма t его значение $\alpha_s(t)$ в модели $\mathfrak{M}_s$: если x — предметная переменная, то $\alpha_s(x) = \alpha(x)$; если c — константа, то $\alpha_s(c) = I_s(c)$; если же $t = f(t_1, \ldots, t_n)$, то $\alpha_s(t) = I_s(f)(\alpha_s(t_1), \ldots, \alpha_s(t_n))$.

Теперь мы можем определить отношение истинности формул состояния в состояниях, а формул пути — в путях модели $\mathfrak{M}$ при интерпретации предметных

переменных. Пусть s — состояние модели $\mathfrak{M}$. Положим для формул состояния:

- $\mathfrak{M}, s \not\models^{\alpha} \bot$;
- $\mathfrak{M}, s \models^{\alpha} t_1 = t_2$, если $\alpha_s(t_1) = \alpha_s(t_2)$;
- $\mathfrak{M}, s \models^{\alpha} P(t_1, \ldots, t_n)$, если $\langle \alpha_s(t_1), \ldots, \alpha_s(t_n) \rangle \in I_s(P)$;
- $\mathfrak{M}, s \models^{\alpha} \varphi \to \psi$, если $\mathfrak{M}, s \not\models^{\alpha} \varphi$ или $\mathfrak{M}, s \models^{\alpha} \psi$;
- $\mathfrak{M}, s \models^{\alpha} \forall x \varphi$, если для всякой интерпретации β, которая не отличается от α ни на какой переменной, кроме, быть может, x, выполнено отношение $\mathfrak{M}, s \models^{\beta} \varphi$;
- $\mathfrak{M}, s \models^{\alpha} \boldsymbol{A}\varphi$, если для всякого пути π, начинающегося в s, выполнено отношение $\mathfrak{M}, \pi \models^{\alpha} \varphi$.

Пусть $\pi = \{s_k\}_{k=0}^{\infty}$ — путь в модели $\mathfrak{M}$. Если φ — формула состояния, то положим

- $\mathfrak{M}, \pi \models^{\alpha} \varphi$, если $\mathfrak{M}, s_0 \models^{\alpha} \varphi$.

Кроме того, считаем, что

- $\mathfrak{M}, \pi \models^{\alpha} \varphi \to \psi$, если $\mathfrak{M}, \pi \not\models^{\alpha} \varphi$ или $\mathfrak{M}, \pi \models^{\alpha} \psi$;
- $\mathfrak{M}, \pi \models^{\alpha} \forall x \varphi$, если для всякой интерпретации β, которая не отличается от α ни на какой переменной, кроме, быть может, x, выполнено отношение $\mathfrak{M}, \pi \models^{\beta} \varphi$;
- $\mathfrak{M}, \pi \models^{\alpha} \boldsymbol{X}\varphi$, если $\mathfrak{M}, s_1 \models^{\alpha} \varphi$;
- $\mathfrak{M}, \pi \models^{\alpha} \varphi \boldsymbol{U} \psi$, если существует $k \in \mathbb{N}$ такое, что $\mathfrak{M}, s_k \models^{\alpha} \psi$ и при этом для любого $j \in \mathbb{N}$ такого, что $j < k$, выполнено отношение $\mathfrak{M}, s_j \models^{\alpha} \varphi$.

Полагаем также

- $\mathfrak{M}, s \models \varphi$, если для всякой интерпретации α выполнено отношение $\mathfrak{M}, s \models^{\alpha} \varphi$;
- $\mathfrak{M}, \pi \models \varphi$, если для всякой интерпретации α выполнено отношение $\mathfrak{M}, \pi \models^{\alpha} \varphi$.

Если φ — формула состояния, то считаем, что

- $\mathfrak{M} \models \varphi$, если для всякого состояния s модели $\mathfrak{M}$ выполнено отношение $\mathfrak{M}, s \models \varphi$.

Если φ — формула пути, то считаем, что

- $\mathfrak{M} \models \varphi$, если для всякого пути π в модели $\mathfrak{M}$ выполнено отношение $\mathfrak{M}, \pi \models \varphi$.

Заметим, что последнее условие эквивалентно следующему: если φ — формула пути, то

- $\mathfrak{M} \models \varphi$ тогда и только тогда, когда $\mathfrak{M} \models \boldsymbol{A}\varphi$.

Таким образом, в качестве формул языка достаточно рассматривать только формулы состояния; в литературе так и принято поступать. Мы будем следовать этому соглашению, считая далее, что под словом «формула» понимается формула состояния[2].

Пусть φ — формула состояния, $\mathfrak{F} = \langle W, R\rangle$, $\mathfrak{F}(D) = \langle W, R, D\rangle$. Полагаем, что

– $\mathfrak{F}(D) \models \varphi$, если для всякой интерпретации I выполнено отношение $\langle W, R, D, I\rangle \models \varphi$;

– $\mathfrak{F} \models \varphi$, если для всякого непустого множества D выполнено отношение $\langle W, R, D\rangle \models \varphi$.

Определим логику **QCTL*****.E.CD** как множество всех формул, истинных во всех шкалах Крипке.

Поясним используемое обозначение. Аббревиатура CTL означает «computational tree logic» – на русский язык это название переводят как «логика ветвящегося времени». Логика **CTL** является фрагментом **CTL***. Этот фрагмент определяется формулами, в которых модальности используются только парами: за каждым квантором пути сразу же идет квантор состояния, например, $\boldsymbol{AG}$, $\boldsymbol{AF}$, $\boldsymbol{EX}$ и т. п. Буква Q означает «quantified»; имеется в виду, что в языке используются предикатные буквы, предметные переменные и кванторы по предметным переменным. Таким образом, **QCTL*** — это «расширенная **CTL** с кванторами по предметным переменным». Буква E означает «equality» и сигнализирует о том, что в языке используется равенство. Вообще говоря, в модальных предикатных логиках равенство ведет себя несколько иначе, чем в классической логике предикатов, в частности, не всегда можно ограничиться рассмотрением т. н. нормальных моделей, когда равенство понимается как предикат совпадения[3], но целям данной работы такое понимание мешать не будет. Наконец, буквы CD означают «constant domains». Дело в том, что в моделях Крипке допускается, что при переходе по отношению достижимости из одного состояния в другое предметная область может расшириться. Опять же, для целей данной работы не так важно, являются предметные области состояний расширяющимися или нет[4].

2. Моделирование натуральных чисел в QCTL*.E.CD

Пусть **TA** — множество всех формул в языке первого порядка с равенством и дополнительными нелогическими символами $0, ', +, \cdot$, истинных в стандартной модели арифметики, т. е. в алгебре $\langle \mathbb{N}, 0, ', +, \cdot\rangle$. Мы покажем, как построить погружение **TA** в логику **QCTL*****.E.CD**. Для этого воспользуемся идеями, изложенными в [14, 15].

Пусть $\prec$ — бинарная предикатная буква, 0 — константа. Следующая формула утверждает, что $\prec$ является строгим линейным порядком, не имеющем верхней

[2]При этом, конечно же, формулы (т. е., по нашему соглашению, формулы состояния) могут содержать в качестве подформул и формулы пути.

[3]См., например, обсуждение интерпретации равенства в семантике Крипке для неклассических логик в [13] на стр. 195.

[4]Отметим, что постоянство областей можно обеспечить, принимая формулу Баркан, которая в нашем случае будет такой: $\forall x\, \boldsymbol{AG} P(x) \to \boldsymbol{AG} \forall x\, P(x)$.

границы и имеющей 0 в качестве нижней границы:

$$\begin{aligned} A_1 \quad = \quad & \forall x \neg(x \prec x) \wedge \\ & \wedge \forall x \forall y \forall z (x \prec y \wedge y \prec z \to x \prec z) \wedge \\ & \wedge \forall x \forall y (x \prec y \vee x = y \vee y \prec x) \wedge \\ & \wedge \forall x \exists y (x \prec y) \wedge \\ & \wedge \forall x (x = 0 \vee 0 \prec x). \end{aligned}$$

Пусть $'$ — одноместный функциональный символ. Опишем условие, означающее, что $'$ является операцией следования, согласованной с порядком $\prec$:

$$A_2 \quad = \quad \forall x \forall y (y = x' \leftrightarrow x \prec y \wedge \neg \exists z (x \prec z \wedge z \prec y)).$$

Сразу заметим, что если в некотором состоянии s некоторой модели $\mathfrak{M} = \langle W, R, D, I \rangle$ истинны формулы A_1 и A_2, то множество значений термов $T_{\mathbb{N}} = \{0, 0', 0'', 0''', \ldots\}$ образует в модели $\mathfrak{M}_s = \langle D, I_s \rangle$ подмножество, изоморфное множеству натуральных чисел с отношением $<$.

Пусть $+$ и $\cdot$ — бинарные функциональные символы. Опишем условие, которое будет гарантировать, что на множестве элементов, соответствующих термам из $T_{\mathbb{N}}$ эти функциональные символы задают сложение и умножение:

$$\begin{aligned} A_3 \quad &= \quad \forall x \forall y (x + 0 = x \wedge x + y' = (x + y)'); \\ A_4 \quad &= \quad \forall x \forall y (x \cdot 0 = 0 \wedge x \cdot y' = (x \cdot y) + x). \end{aligned}$$

Все, что осталось сделать, — это описать условия, гарантирующие, что интерпретация каждой предметной переменной совпадает с интерпретацией одного из термов из множества $T_{\mathbb{N}}$. Сделаем это.

Прежде всего потребуем, чтобы отношение $\prec$ и функция $'$ сохранялись при переходе к другим состояниям:

$$A_5 \quad = \quad \forall x \forall y (x \prec y \leftrightarrow \boldsymbol{AG}(x \prec y)) \wedge \forall x \forall y (y = x' \leftrightarrow \boldsymbol{AG}(y = x')).$$

Пусть теперь N — одноместная предикатная буква. Мы будем использовать N, чтобы приписывать состояниям путей «номера». Начальному (текущему) состоянию припишем «номер», соответствующий терму 0, следующему за ним — «номер», соответствующий терму $0'$, следующему за ним — «номер», соответствующий терму $0''$, и т. д.:

$$A_6 \quad = \quad N(0) \wedge \boldsymbol{AG} \forall x ((N(x) \wedge N(y) \to x = y) \wedge (N(x) \to \boldsymbol{AX} N(x'))).$$

Осталось сказать, что каждый элемент является «номером» для какого-нибудь состояния, и тогда наша цель будет достигнута, т. к. состояния в пути упорядочены так же, как натуральные числа. Положим

$$A_7 \quad = \quad \forall x \boldsymbol{EF} N(x).$$

Пусть $A = A_1 \wedge \ldots \wedge A_7$. Из описанных построений следует справедливость следующего утверждения.

Лемма 1. *Пусть s — состояние некоторой модели $\mathfrak{M} = \langle W, R, D, I\rangle$ и пусть $\mathfrak{M}, s \models A$. Тогда алгебра $\langle D, I_s(0), I_s(')), I_s(+), I_s(\cdot)\rangle$ изоморфна алгебре $\langle \mathbb{N}, 0, ', +, \cdot\rangle$.*

Теперь несложно построить погружение теории **TA** в логику **QCTL*****.E.CD**: достаточно замкнутой арифметической формуле φ ставить в соответствие формулу $A \to \varphi$.

Теорема 1. *Для всякой замкнутой арифметической формулы φ справедлива следующая эквивалентность:*

$$\varphi \in \mathbf{TA} \iff A \to \varphi \in \mathbf{QCTL}^*\mathbf{.E.CD}.$$

Доказательство. Пусть $\varphi \in \mathbf{TA}$. Предположим, что, вопреки утверждению теоремы, $A \to \varphi \notin \mathbf{QCTL}^*\mathbf{.E.CD}$. Тогда существует модель $\mathfrak{M} = \langle W, R, D, I\rangle$ и состояние $s \in W$ такое, что $M, s \not\models A \to \varphi$, т. е. $M, s \models A$ и $M, s \not\models \varphi$. Тогда, согласно лемме 1, алгебра $\langle D, I_s(0), I_s(')), I_s(+), I_s(\cdot)\rangle$ изоморфна алгебре $\langle \mathbb{N}, 0, ', +, \cdot\rangle$, из чего заключаем, что φ опровергается в $\langle \mathbb{N}, 0, ', +, \cdot\rangle$, т. е. $\varphi \notin \mathbf{TA}$. Получили противоречие. Следовательно, $A \to \varphi \in \mathbf{QCTL}^*\mathbf{.E.CD}$.

Пусть $A \to \varphi \in \mathbf{QCTL}^*\mathbf{.E.CD}$. Предположим, что $\varphi \notin \mathbf{TA}$. Тогда φ опровергается в $\langle \mathbb{N}, 0, ', +, \cdot\rangle$. Покажем, что в этом случае существует модель логики **QCTL*****.E.CD**, в которой опровергается формула $A \to \varphi$.

Положим $\mathfrak{M} = \langle \mathbb{N}, R, \mathbb{N}, I\rangle$, где для любых состояний $s, t \in \mathbb{N}$

$$sRt \leftrightharpoons t = s + 1$$

и для каждого состояния $s \in \mathbb{N}$ интерпретация I_s константе 0 ставит в соответствие число 0, символам $'$, $+$ и $\cdot$ — операции следования, сложения и умножения, соответственно, букве $\prec$ — отношение $<$, а буква N интерпретируется так:

$$\mathfrak{M}, s \models^{\alpha} N(x) \leftrightharpoons \alpha(x) = s;$$

интерпретация остальных констант, функциональных символов и предикатных букв произвольна.

Тогда $\mathfrak{M}, 0 \models A$; мы оставляем проверку этого факта читателю. Кроме того, поскольку для каждого состояния $s \in \mathbb{N}$ в модели $\mathfrak{M}_s = \langle \mathbb{N}, I_s\rangle$ интерпретация для 0, $'$, $+$ и $\cdot$ является такой же, как в стандартной модели арифметики $\langle \mathbb{N}, 0, ', +, \cdot\rangle$, получаем, что для каждого $s \in \mathbb{N}$ имеет место отношение $\mathfrak{M}, s \not\models \varphi$. Отсюда следует, что $\mathfrak{M}, 0 \not\models A \to \varphi$, а это противоречит тому, что $A \to \varphi \in \mathbf{QCTL}^*\mathbf{.E.CD}$.

Следовательно, $\varphi \in \mathbf{TA}$. □

Итак, **TA** погружается в **QCTL*****.E.CD**. Это означает, что все, что можно выразить в теории **TA**, можно выразить и в логике **QCTL*****.E.CD**. Мы покажем, что из теоремы 1 и ее доказательства можно извлечь ряд следствий, относящихся не только к логике **QCTL*****.E.CD**.

3. Некоторые следствия

Прежде всего заметим, что в приведенной выше конструкции можно избавиться от констант, функциональных символов и равенства: константу 0 можно заменить переменной, по которой будет стоять квантор существования, n-местный

функциональный символ — $(n+1)$-местной преридкатной буквой (не забыв сказать, что эта буква определяет функциональное отношение), а равенство — бинарной предикатной буквой, для которой добавить условие, означающее, что она определяет отношение конгруэнтности для всех предикатных букв, используемых в формуле. Кроме того, используя идею С. Крипке [16][5], можно все предикатные буквы промоделировать одноместными предикатными буквами: формулу $P(x_1, \ldots, x_n)$ можно заменить на формулу $\boldsymbol{EF}(P_1(x_1) \wedge \ldots \wedge P_n(x_n))$. После всех этих замен формула $A \to \varphi$ превратится в некоторую формулу $A^\star \to \varphi^\star$.

Множество формул в языке без равенства, констант и функциональных символов, истинных во всех шкалах Крипке, обозначим посредством $\mathbf{QCTL}^*.\mathbf{CD}$. Тогда, с учетом сделанных замечаний, получаем следующее утверждение.

Следствие 1. *Существует алгоритмически вычислимая функция f такая, что для всякой замкнутой арифметической формулы φ имеют место следующие эквивалентности:*

$$\varphi \in \mathbf{TA} \iff f(\varphi) \in \mathbf{QCTL}^*.\mathbf{E.CD} \iff f(\varphi) \in \mathbf{QCTL}^*.\mathbf{CD},$$

причем $f(\varphi)$ содержит только одноместные предикатные буквы.

Теперь заметим, что в формуле A (и в $A^\star$) модальности используются только в сочетаниях $\boldsymbol{AG}$, $\boldsymbol{EF}$ и $\boldsymbol{AX}$. Это означает, что фактически мы использовали модальности логики $\mathbf{CTL}$, являющейся фрагментом $\mathbf{CTL}^*$ (см. стр. 9). Кроме того, в моделях Крипке можно избавиться от требования постоянства областей, приписав каждому состоянию s свою область D_s (т. е. состоянию s ставить в соответствие модель $\mathfrak{M}_s = \langle D_s, I_s \rangle$), потребовав лишь, чтобы выполнялось условие

$$sRt \implies D_s \subseteq D_t.$$

Поскольку для доказательства теоремы 1, по сути, нам важно лишь, чтобы натуральные числа получились хотя бы в одном мире (где опровергается $A \to \varphi$ или — после модификаций — $A^\star \to \varphi^\star$), расширяющиеся области мешать доказательству не будут.

Определим $\mathbf{QCTL}$ как множество формул языка $\mathbf{QCTL}^*.\mathbf{CD}$, в котором из модальностей используются только модальности языка логики $\mathbf{CTL}$ и которые истинны во всех шкалах Крипке с расширяющимися областями.

С учетом сделанных замечаний, в следствии 1 можно заменить $\mathbf{QCTL}^*.\mathbf{CD}$ на $\mathbf{QCTL}$.

Следствие 2. *Существует алгоритмически вычислимая функция f такая, что для всякой замкнутой арифметической формулы φ имеют место следующие эквивалентности:*

$$\varphi \in \mathbf{TA} \iff f(\varphi) \in \mathbf{QCTL}^*.\mathbf{E.CD} \iff f(\varphi) \in \mathbf{QCTL},$$

причем $f(\varphi)$ содержит только одноместные предикатные буквы.

До сих пор мы сужали язык и расширяли семантику, получая все более узкие фрагменты логики $\mathbf{QCTL}^*.\mathbf{E.CD}$, для которых справедлив аналог теоремы 1.

[5] Русский перевод этой работы можно найти в книге [6], с. 247–253.

Теперь сузим семантику, получив тем самым расширение этой логики. Заметим, что для доказательства теоремы 1 достаточно, чтобы в нашем распоряжении была одна-единственная шкала Крипке — это шкала $\mathfrak{F} = \langle \mathbb{N}, R\rangle$, на которой определена модель $\mathfrak{M} = \langle \mathbb{N}, R, \mathbb{N}, I\rangle$, используемая во второй части доказательства теоремы 1. Обозначим множество формул логики **QCTL*****.E.CD**, которые истинны в шкале $\mathfrak{F} = \langle \mathbb{N}, R\rangle$, посредством **QCTL*****.E.CD**$^\omega$.

Следствие 3. *Существует алгоритмически вычислимая функция f такая, что для всякой замкнутой арифметической формулы φ имеют место следующие эквивалентности:*

$$\varphi \in \mathbf{TA} \iff f(\varphi) \in \mathbf{QCTL}^*\mathbf{.E.CD} \iff f(\varphi) \in \mathbf{QCTL}^*\mathbf{.E.CD}^\omega,$$

причем $f(\varphi)$ содержит только одноместные предикатные буквы.

Поскольку для доказательства следствий 1–3 функцию f можно определить одинаково (например, положив $f(\varphi) = A^\star \to \varphi^\star$), эти следствия можно объединить в следующее утверждение.

Теорема 2. *Существует алгоритмически вычислимая функция f такая, что для всякой замкнутой арифметической формулы φ и для всякого множества формул L такого, что* **QCTL** $\subseteq L \subseteq$ **QCTL*****.E.CD**$^\omega$*, справедлива следующая эквивалентность:*

$$\varphi \in \mathbf{TA} \iff f(\varphi) \in L,$$

причем $f(\varphi)$ содержит только одноместные предикатные буквы.

Теперь обратимся к алгоритмическим свойствам логики **QCTL*****.E.CD**.

Напомним, что множество называется разрешимым, если его характеристическая функция вычислима, и рекурсивно перечислимым, если оно пустое или существует алгоритм, последовательно перечисляющий элементы этого множества.

Заметим, что безмодальным фрагментом логики **QCTL*****.E.CD** является классическая логика предикатов (с равенством). Она рекурсивно перечислима, т. к. имеет конечную аксиоматику, но неразрешима в силу теоремы Черча–Тьюринга[6] [1], следовательно, согласно тереме Поста (см., например, [7], глава II, §4, теорема 3), дополнение классической логики предикатов не является рекурсивно перечислимым. Из сказанного заключаем, что логика **QCTL*****.E.CD** неразрешима, а ее дополнение не является рекурсивно перечислимым. Аналогичные рассуждения можно повторить для любого множества L, лежащего между **QCTL** и **QCTL*****.E.CD**$^\omega$ (учитывая, что безмодальным фрагментом логик без равенства будет классическая логика предикатов без равенства, что в данном случае непринципиально).

Принимая во внимание теорему 2, мы можем утверждать большее: любое множество L, лежащее между **QCTL** и **QCTL*****.E.CD**$^\omega$, не является рекурсивно перечислимым. Действительно, в силу теоремы Тарского (см. [8], глава 3, §6), **TA** не является арифметическим множеством[7], а значит, **TA** не является рекурсивно перечислимым. Поскольку **TA** погружается в L, получаем, что L тоже не является рекурсивно перечислимым.

[6] Доказательство А. Черча опубликовано в [11, 12], а доказательство А. Тьюринга — в [17, 18].
[7] Точнее, арифметическим не является множество Геделевых номеров формул из **TA**.

Следствие 4. *Пусть L — некоторое множество формул такое, что* $\mathbf{QCTL} \subseteq L \subseteq \mathbf{QCTL}^*.\mathbf{E}.\mathbf{CD}^\omega$. *Тогда L не является рекурсивно перечислимым.*

Заметим, что любая рекурсивно аксиоматизируемая логика является рекурсивно перечислимой: чтобы перечислить выводимые в ней формулы, достаточно последовательно строить все выводы в ней, а это возможно благодаря рекурсивной перечислимости множества ее аксиом и правил вывода. Значит, имеет место следующее утверждение.

Следствие 5. *Пусть логика L такова, что* $\mathbf{QCTL} \subseteq L \subseteq \mathbf{QCTL}^*.\mathbf{E}.\mathbf{CD}^\omega$. *Тогда L не является рекурсивно аксиоматизируемой.*

Конечно, следствия 4 и 5 останутся справедливыми, если ограничиться только формулами с одноместными предикатными буквами.

Другой «стороной медали» теоремы 1 (или следствия 4) является неполнота по Крипке большого класса исчислений. Напомним, что логика L называется полной по Крипке, если она совпадает со множеством формул, истинных в некотором классе шкал Крипке.

Следствие 6. *Пусть L — рекурсивно перечислимая логика (исчисление) в языке первого порядка, обогащенном модальностями логики* **CTL** *или* $\mathbf{CTL}^*$, *и пусть* $L \subseteq \mathbf{QCTL}^*.\mathbf{E}.\mathbf{CD}^\omega$. *Тогда L не является полной по Крипке.*

Доказательство. Если бы логика L была полной по Крипке, то она содержала бы в себе логику **QCTL** (поскольку формулы, принадлежащие **QCTL** истинны в любой шкале Крипке), и тогда, учитывая, что $L \subseteq \mathbf{QCTL}^*.\mathbf{E}.\mathbf{CD}^\omega$, по следствию 4 мы получили бы, что L не является рекурсивно перечислимой, что не так. □

Отметим, что условие включения логики L в логику $\mathbf{QCTL}^*.\mathbf{E}.\mathbf{CD}^\omega$ является довольно слабым: оно всего лишь означает, что логика L имеет хотя бы одну модель Крипке с бесконечным путем, образованным попарно различными состояниями. Поскольку состояния соответствуют неким «моментам времени», то получаем, что такое условие говорит всего лишь о том, что L допускает «незацикливание» времени. Таким образом, неполнота по Крипке оказывается «естественным» свойством исчислений в первопорядковом языке, обогащенным модальностями логики **CTL** или $\mathbf{CTL}^*$.

Тем не менее, полное по Крипке исчисление в рассматриваемом языке построить несложно: достаточно взять логику любой конечной (разумеется, сериальной) шкалы Крипке. Используя технику из [10], можно построить погружение такой логики в классическую логику предикатов, откуда будет следовать перечислимость, а значит, и рекурсивная аксиоматизируемость.

Последний момент, который рассмотрим, — это вопрос о том, насколько сложно описывается семантика полных по Крипке логик, содержащихся в $\mathbf{QCTL}^*.\mathbf{CD}^\omega$. Можно ли это сделать с помощью классических формул первого порядка?

Несложно понять, что нет, нельзя. В работе [10] показано, что если логика L задается семантически и при этом соответствующая семантика описывается формулами первого порядка, то L погружается в классическую логику предикатов. Существование такого погружения гарантирует, что L рекурсивно перечислима. Согласно теореме 2, полные по Крипке логики, содержащиеся в $\mathbf{QCTL}^*.\mathbf{E}.\mathbf{CD}^\omega$,

не являются рекурсивно перечислимыми, а значит, их семантику невозможно описать классическими формулами первого порядка. Фактически сложность в том, чтобы, имея в языке бинарную предикатную букву для отношения достижимости и равенство, выразить отношение истинности для формул, начинающихся с модальностей, а для этого, согласно семантике Крипке, требуется описать понятие пути, которое, в свою очередь опирается на возможность описать структуру типа ω, что в классическом предикатном языке сделать невозможно.

Заключение

Мы показали, что при «соединении» классического языка первого порядка и языка логики **CTL*** получается язык, позволяющий выразить натуральные числа со следованием, сложением и умножением, при этом мы усилили этот результат, добавив ограничения на использование предикатных букв. Мы предполагаем, что теорему 2 можно усилить.

Гипотеза 1. *Существует алгоритмически вычислимая функция f такая, что для всякой замкнутой арифметической формулы φ и для всякого множества формул L такого, что* **QCTL** $\subseteq L \subseteq$ **QCTL*****.E.CD**, *справедлива следующая эквивалентность:*

$$\varphi \in \mathbf{TA} \iff f(\varphi) \in L,$$

причем $f(\varphi)$ содержит только одну одноместную предикатную букву.

Кроме того, мы предполагаем, что аналогичные результаты можно получить и для случая языков, близких к языкам логик **CTL** и **CTL***, в частности, для **ATL**, **ATL***, **LTL**. Для **ATL**, **ATL*** это почти очевидно, поскольку **CTL** и **CTL*** являются фрагментами этих логик; для **LTL** требуется незначительная модификация использованным нами формул, учитывающая ограничения на использование модальностей.

Список литературы

[1] Булос Дж., Джеффри Р. Вычислимость и логика. М.: Мир, 1994.

[2] Ершов Ю. Л., Палютин Е. А. Математическая логика. Изд. 2-е. М.: Наука, 1987.

[3] Карпов Ю. Г. Model checking. Верификация параллельных и распределенных программных систем. СПб: БХВ-Петербург, 2010.

[4] Кейслер Г., Чэн Ч. Теория моделей. М.: Мир, 1977.

[5] Кларк Э. М., Грамберг О., Пелед Д. Верификация моделей программ: Model checking. М.: МЦНМО, 2002.

[6] Фейс Р. Модальная логика. М.: Наука, 1974.

[7] Мальцев А.И. Алгоритмы и рекурсивные функции. Изд. 2-е. М.: Наука, 1986.

[8] Мендельсон Э. Введение в математическую логику. М.: Наука, 1976.

[9] Новиков П.С. Элементы математической логики. Изд. 2-е. М.: Наука, 1973.

[10] Рыбаков М.Н., Чагров А.В. Стандартные переводы неклассических формул и относительная разрешимость логик // Труды научно-исследовательского семинара Логического центра Института философии РАН. Вып. XIV. М.: Издательство Института философии РАН, 2000. С. 81–98.

[11] Church A. An unsolvable problem of elementary number theory // American Journal of Mathematics. 1936. Vol. 58. Pp. 345–363.

[12] Church A. A note on the Entscheidungsproblem // Journal of Symbolic Logic. 1936. Vol. 1. Pp. 40–41.

[13] Gabbay D.M., Skvortsov D., Shehtman V. Quantification in Nonclassical Logic. Volume 153. Elsevier Science, 2009.

[14] Kotikova E.A., Rybakov M.N. First-Order Logics of Branching Time: On Expressive Power of Temporal Operators // Logical Investigations. 2013. Vol. 19. Pp. 68–99.

[15] Kotikova E.A., Rybakov M.N. Kripke incompleteness of first-order calculi with temporal modalities of CTL and near logics // Logical Investigations. 2015. Vol. 21(1). Pp. 86–99.

[16] Kripke S. The undecidability of monadic modal quantificational theory // Zeitschrift für Mathematische Logik und Grundlagen der Mathematik. 1962. Vol. 8. Pp. 113–116.

[17] Turing A.M. On computable numbers with an application to the Entscheidungsproblem // Proceedings of the London Mathematical Society. 1936. Ser. 2, vol. 42. Pp. 230–265.

[18] Turing A.M. On computable numbers, with an application to the Entscheidungsproblem. A correction // Proceedings of the London Mathematical Society. 1937. Ser. 2, vol. 43. Pp. 544–546.

[19] Vardi M.Y., Stockmeyer L. Improved upper and lower bounds for modal logics of programs // In Proceedings of 17th Symposium on Theory of Computing, STOC'85. Baltimore, USA, May 1985. Pp. 240–251.

Библиографическая ссылка

Котикова Е.А., Рыбаков М.Н. Моделирование арифметики в языке первого порядка, обогащенном темпоральными кванторами // Вестник ТвГУ. Серия: Прикладная математика. 2016. № 4. С. 5–19.

Сведения об авторах

1. **Котикова Екатерина Александровна**
аспирант, ассистент кафедры функционального анализа и геометрии ТвГУ.

Россия, 170100, г. Тверь, ул. Желябова, д. 33, ТвГУ.
E-mail: kotikova.e.a@gmail.com.

2. **Рыбаков Михаил Николаевич**
доцент кафедры функционального анализа и геометрии ТвГУ; инженер-программист ЗАО НИИ ЦПС; научный сотрудник отдела информатики и прикладной математики университета Витватерсранда, Йоханнесбург

Россия, 170100, г. Тверь, ул. Желябова, д. 33, ТвГУ. E-mail: m_rybakov@mail.ru

MODELING ARITHMETIC IN THE FIRST-ORDER LANGUAGE ENRICHED WITH TEMPORAL QUANTIFIERS

Kotikova Ekaterina Aleksandrovna
PhD student, assistant at the Functional Analysis and Geometry department,
Tver State University.
Russia, 170100, Tver, 33 Zhelyabova str., TSU. E-mail: kotikova.e.a@gmail.com

Rybakov Mikhail Nikolaevich
Senior Lecturer at the Functional Analysis and Geometry department,
Tver State University;
Software engineer at CJSC Scientific Research Institute Centerprogramsystem;
Research Fellow at the School of Computer Science and Applied Mathematics,
University of the Witwatersrand, Johannesburg.
Russia, 170100, Tver, 33 Zhelyabova str., TSU. E-mail: m_rybakov@mail.ru

Received 29.08.2016, revised 07.10.2016.

We investigate the classical first-order language with equality enriched by the modalities of the computational tree logic **CTL***. As a semantics for it we consider serial Kripke frames with constant domains. We construct an embedding of the truth arithmetics into the set of all formulas that are valid in the class of such frames. Then, we obtain some corollaries concerned algorithmical, syntactical, and semantical properties for a large class of logic in the language.

Keywords: first-order logic, computational tree logic, recursive enumerability, Kripke semantics.

Bibliographic citation

Kotikova E.A., Rybakov M.N. Modeling arithmetic in the first-order language enriched with temporal quantifiers. *Vestnik TvGU. Seriya: Prikladnaya Matematika* [Herald of Tver State University. Series: Applied Mathematics], 2016, no. 4, pp. 5–19. (in Russian)

References

[1] Boolos G. S., Jeffrey R. C. *Computability and Logic.* Third Edition. Cambrige University Press, 1989.

[2] Ershov Yu.L., Palyutin E.A. *Matematicheskaya Logika* [Mathematical Logic]. Second Edition. Moscow, Nauka, 1987. (in Russian)

[3] Karpov Yu.G. *Model checking: Verifikatsiya Parallel'nykh i Raspredelennykh Sistem* [Model Checking: Verification of Parallel and Distributive Systems]. Sankt-Peterburg, BKHV-Peterburg, 2010. (in Russian)

[4] Chang C.C., Keisler H.J. *Model Theory.* North-Holland Publishing Company, 1973.

[5] Clarke E.M., Grumberg O., Peled D. *Model Checking.* MIT Press, 1999.

[6] Feys R. *Modal'naya Logika* [Modal Logic]. Moscow, Nauka, 1974. (in Russian)

[7] Mal'tsev A.I. *Algoritmy i Rekursivnye Funktsii* [Algorithms and Recursive Functions]. Second Edition. Moscow, Nauka, 1986. (in Russian)

[8] Mendelson E. *Introduction to Mathematical Logic.* D. van Nostrand Company, Inc., 1964.

[9] Novikov P.S. *Elementy Matematicheskoy Logiki* [Elements of Mathematical Logic]. Second Edition. Moscow, Nauka, 1973. (in Russian)

[10] Chagrov A.V., Rybakov M.N. Standard translations of non-classical formulas and relative decidability of logics. *Trudy Nauchno-Issledovatel'skogo Seminara Logicheskogo Tsentra Instituta Filosofii RAN* [Proceedings of the Research Seminar of the Logical Center of the Institute of Philosophy, RAS], 2000, vol. XIV, pp. 81–98. (in Russian)

[11] Church A. An unsolvable problem of elementary number theory. *American Journal of Mathematics*, 1936, vol. 58, pp. 345–363.

[12] Church A. A note on the Entscheidungsproblem. *Journal of Symbolic Logic*, 1936, vol. 1, pp. 40–41.

[13] Gabbay D.M., Shehtman V.B., Skvortsov D.P. *Quantification in Nonclassical Logic.* Volume 1. Elsevier Science, 2009.

[14] Kotikova E.A., Rybakov M.N. First-order logics of branching time: on expressive power of temporal operators. *Logical Investigations*, 2013, vol. 19, pp. 68–99.

[15] Kotikova E.A., Rybakov M.N. Kripke incompleteness of first-order calculi with temporal modalities of CTL and near logics. *Logical Investigations*, 2015, vol. 21(1), pp. 86–99.

[16] Kripke S. The undecidability of monadic modal quantificational theory. *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, 1962, vol. 8, pp. 113–116.

[17] Turing A.M. On computable numbers with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, 1936, ser. 2, vol. 42, pp. 230–265.

[18] Turing A.M. On computable numbers, with an application to the Entscheidungsproblem. A correction. *Proceedings of the London Mathematical Society*, 1937, ser. 2, vol. 43, pp. 544–546.

[19] Vardi M.Y., Stockmeyer L. Improved upper and lower bounds for modal logics of programs. *In Proceedings of 17th Symposium on Theory of Computing, STOC'85.* Baltimore, USA, May 1985. Pp. 240–251.