УДК 510.53, 510.643

DOI: 10.15827/0236-235X.123.591-597

Дата подачи статьи: 21.03.18

2018. Т. 31. № 3. С. 591–597

Алгоритмическая неразрешимость проблемы первопорядковой определимости формул логики ветвящегося времени

М.Н. Рыбаков^{1, 2, 3}, к.ф.-м.н., доцент, научный сотрудник, инженер-программист,
m_rybakov@mail.ru

Л.А. Чагрова¹, к.ф.-м.н., доцент, chagrovay@mail.ru

¹ Тверской государственный университет, г. Тверь, 170100, Россия

² Университет Витватерсранда, г. Йоханнесбург, 2001, Южная Африка

³ НИИ «Центрпрограммистем», г. Тверь, 170024, Россия

В качестве формального средства, описывающего свойства различных структур (в том числе структур вычислений), обычно используют язык логики предикатов. Этот язык, с одной стороны, понятен и удобен, а с другой, многие вопросы, важные с прикладной точки зрения, для него алгоритмически неразрешимы, то есть не могут быть решены программно.

Сейчас существует много альтернативных языков, позволяющих описывать вычисления и их свойства, при этом, в отличие от языка логики предикатов, аналогичные вопросы для них алгоритмически разрешимы. В работе рассматривается один из таких языков – язык логики ветвящегося времени CTL. Он используется для верификации программ, так как содержит средства для описания свойств программных вычислений, в частности, свойств бинарного отношения, возникающего в реляционной семантике Крипке.

В работе исследуется возможность алгоритмического нахождения формул языка первого порядка, которые задают те же классы шкал Крипке, что и формулы языка логики CTL. Известно, что для интуиционистских формул проблема их первопорядковой определимости алгоритмически неразрешима. Показано, как, используя перевод Гёделя интуиционистских формул в модальные, а затем перевод получившихся модальных формул в формулы языка логики CTL, свести проблему первопорядковой определимости интуиционистских формул на шкалах Крипке к проблеме первопорядковой определимости CTL-формул на шкалах Крипке. В качестве следствия такого сведения получена алгоритмическая неразрешимость соответствующей проблемы для CTL.

В заключении обсуждаются возможные модификации приведенной конструкции с целью распространения полученного результата на фрагменты языка логики CTL, а также алгоритмическая разрешимость проблемы CTL-определимости формул первого порядка.

Ключевые слова: модели вычислений, логика ветвящегося времени, первопорядковая определимость.

Язык логики ветвящегося времени CTL (computational tree logic) – удобное и эффективное средство для описания свойств различных сложных вычислительных систем, в том числе с целью их последующей верификации [1, 2]. Его существенным отличием от хорошо известного и широко используемого языка логики предикатов QCL является то, что важные для прикладного аспекта задачи общезначимости и выполнимости CTL-формул разрешимы [3], в то время как для проблем тождественной истинности и выполнимости формул языка логики QCL разрешающей процедуры не существует в принципе [4].

Оба языка позволяют описывать свойства (серийного) бинарного отношения: свойства отношения достижимости в шкалах Крипке для CTL, с одной стороны, могут быть описаны с помощью модальностей языка CTL, а с другой – с помощью формул языка логики предикатов, содержащих предикатную букву R для отношения достижимости, R^* для его рефлексивно-транзитивного замыкания, а также символ равенства. Многие условия, выражаемые на одном из этих языков, могут быть выражены и на другом. Таковыми являются, например, условия рефлексивности, симметричности и транзитивности отношения достижимости, а также многие другие. Но, скажем, условие ирре-

флексивности не может быть выражено средствами языка логики CTL, а в языке логики QCL выражается формулой $\forall x \neg(xRx)$. И наоборот: например, условие, выраженное формулой Маккинси $AX \neg AX \neg p \rightarrow \neg AX \neg AX p$, не может быть выражено никакой формулой языка логики QCL.

В связи с этим возникают, как минимум, два вопроса. Первый: как по формуле одного из этих языков установить, существует ли ее эквивалент во втором языке? Второй: если такой эквивалент существует, то как его найти?

Частично ответы на эти вопросы известны. Так, для мономодального языка имеется класс так называемых формул Салквиста [5–7], а для предикатного – так называемых формул Крахта [8, 9]. Между этими классами установлено соответствие, связывающее каждую формулу одного из них с ее эквивалентом в другом. Но ни формулы Салквиста, ни формулы Крахта не описывают все условия, выражаемые на языках логик CTL и QCL. Отметим, что недавно получены обобщения формул Салквиста и формул Крахта [10–13], а также ряд результатов, касающихся взаимосвязи между определимостью различных условий и запросами [14, 15].

В данной работе рассматривается ситуация без ограничений, то есть для полных языков, а не для специальных их фрагментов типа формул Салквиста.

ста, формул Крахта или их обобщений. При этом показано, что, хотя язык логики QCL алгоритмически более выразителен, чем язык CTL, тем не менее, не существует алгоритма, который по произвольной формуле языка CTL давал бы ответ на вопрос, существует ли эквивалент этой формулы в языке QCL. Чтобы показать это, будем использовать фундаментальные результаты из [16], полученные для интуиционистской логики Int и ее модального напарника S4, который, как будет показано, встроен в CTL. Приводимые здесь результаты не являются неожиданными для специалистов по теории соответствий (Correspondence Theory), но могут оказаться интересными тем, кто не знаком с этой теорией, но пользуется средствами языка логики CTL для верификации программ.

Синтаксис и семантика

Коротко напомним, как устроены языки логик CTL, S4 и Int, а также одна из возможных их семантик (см. более детально [1, 2, 6]).

Каждый из этих языков содержит счетное множество пропозициональных переменных, логические связки $\wedge$ (конъюнкция), $\vee$ (дизъюнкция), $\rightarrow$ (импликация), $\neg$ (отрицание), логические константы $\perp$ (ложь) и $\top$ (истина), а также скобки. При этом язык логики S4 содержит дополнительно модальность $\Box$, а язык CTL – модальности AX , EX , AF , EF , AG , EG , AU , EU . Модальность $\Box$ позволяет строить формулы вида $\Box\varphi$, читаемые как «необходимо φ ». Модальности языка логики CTL являются составными, при этом первые шесть – одноместные, они позволяют строить формулы вида $AX\varphi$, $EX\varphi$, $AF\varphi$, $EF\varphi$, $AG\varphi$ и $EG\varphi$, а две последние – двухместные, они позволяют строить формулы вида $(\varphi AU \psi)$ и $(\varphi EU \psi)$. Каждая из этих модальностей состоит из двух частей: первая – A или E , вторая – X , F , G или U . Части A и E называются кванторами пути и соответствуют выражениям «для каждого пути верно, что...» (A – от all) и «существует такой путь, что...» (E – от exists). Части X , F , G и U называются кванторами состояний и соответствуют выражениям «в следующем состоянии данного пути...» (X – от next), «в некотором состоянии данного пути...» (F – от future), «в каждом состоянии данного пути...» (G – от globally) и «в состояниях данного пути справедливо..., пока не станет справедливо...» (U – от until). Так, $EG\varphi$ означает, что «существует путь, в каждом состоянии которого верно φ », а формула $(\varphi EU \psi)$ – что «существует путь, в состояниях которого верно φ , пока не станет верным ψ ».

Для оценки истинности формул каждого из языков будем использовать семантику С. Крипке. Шкала Крипке – это набор $\mathcal{F} = \langle W, R \rangle$, где W – непустое множество, а R – бинарное отношение на W . Элементы W принято называть *точками*, *состояниями* или *мирами*, а отношение R – *отношением*

достижимости. Если выполнено условие xRy , то говорим, что *из точки x достижима точка y* . В случае CTL дополнительно требуется, чтобы отношение достижимости в шкалах было серийным (серийность R выражается следующей формулой логики предикатов: $\forall x \exists y (xRy)$). В случае S4 отношение достижимости должно быть рефлексивным (то есть $\forall x (xRx)$) и транзитивным (то есть $\forall x \forall y \forall z (xRy \wedge yRz \rightarrow xRz)$), а в случае Int – рефлексивным, транзитивным и антисимметричным (то есть $\forall x \forall y (xRy \wedge yRx \rightarrow x = y)$). *Оценкой* в шкале $\mathcal{F} = \langle W, R \rangle$ называется функция v , которая каждой пропозициональной переменной p сопоставляет некоторое подмножество $v(p)$ множества W . Содержательно условие $x \in v(p)$ означает, что переменная p истинна в точке x . При этом в случае интуиционистской логики дополнительно требуется наследственность оценки, то есть следующее условие: если $x \in v(p)$ и xRy , то $y \in v(p)$. *Модель Крипке* – это набор $\mathcal{M} = \langle W, R, v \rangle$, где $\langle W, R \rangle$ – шкала Крипке, а v – оценка в этой шкале.

Путем в шкале $\mathcal{F} = \langle W, R \rangle$ называется бесконечная последовательность $\pi = (\pi_0, \pi_1, \pi_2, \pi_3, \dots)$ состояний (необязательно различных), в которой для каждого k выполнено условие $\pi_k R \pi_{k+1}$; при этом π_0 называется *началом* пути π . Заметим, что в случае серийности отношения R каждое состояние является началом хотя бы одного пути.

Для модели $\mathcal{M} = \langle W, R, v \rangle$, точки $x \in W$ и CTL-формулы φ определим отношение истинности $\mathcal{M}, x \models \varphi$ (читается: в точке x модели $\mathcal{M}$ истинна формула φ). Оно определяется классически для $\wedge$, $\vee$, $\rightarrow$, $\neg$, $\perp$ и $\top$, а для модальностей – в соответствии с вкладываемым в них смыслом:

- $\mathcal{M}, x \models AX\varphi$, если для каждого пути π , начинающегося в x , верно, что $\mathcal{M}, \pi_1 \models \varphi$;
- $\mathcal{M}, x \models AF\varphi$, если в каждом пути π , начинающемся в x , существует такое состояние π_k , что $\mathcal{M}, \pi_k \models \varphi$;
- $\mathcal{M}, x \models AG\varphi$, если в каждом пути π , начинающемся в x , для каждого состояния π_k верно, что $\mathcal{M}, \pi_k \models \varphi$;
- $\mathcal{M}, x \models \varphi AU \psi$, если в каждом пути π , начинающемся в x , существует состояние π_k , для которого $\mathcal{M}, \pi_k \models \psi$, при этом для каждого t , строго меньшего k , верно, что $\mathcal{M}, \pi_t \models \varphi$;
- $\mathcal{M}, x \models EX\varphi$, если существует такой начинающийся в x путь π , что $\mathcal{M}, \pi_1 \models \varphi$;
- $\mathcal{M}, x \models EF\varphi$, если существует такой начинающийся в x пути π , для некоторого состояния π_k которого верно, что $\mathcal{M}, \pi_k \models \varphi$;
- $\mathcal{M}, x \models EG\varphi$, если существует такой начинающийся в x путь π , для каждого состояния π_k которого верно, что $\mathcal{M}, \pi_k \models \varphi$;
- $\mathcal{M}, x \models \varphi EU \psi$, если в некотором начинающемся в x пути π существует состояние π_k , для которого $\mathcal{M}, \pi_k \models \psi$, при этом для каждого t , строго меньшего k , верно, что $\mathcal{M}, \pi_t \models \varphi$.

Формула φ истинна в модели, если φ истинна в каждом состоянии этой модели. Формула φ истинна в шкале, если φ истинна в каждой модели, определенной на этой шкале.

Для случая S4-формулы аналогичное определение требует следующей корректировки:

– $\mathcal{M}, x \models \Box\varphi$, если для каждого $y \in W$, достижимого из x по R , верно, что $\mathcal{M}, y \models \varphi$.

Для случая интуиционистских формул ситуация иная. Определение истинности для переменных, а также для логических связок $\wedge$, $\vee$, $\perp$ и $\top$ внешне не отличается от классического случая, а истинность связок $\rightarrow$ и $\neg$ определяется иначе:

– $\mathcal{M}, x \models \varphi \rightarrow \psi$, если для каждого $y \in W$, достижимого из x по R , из условия $\mathcal{M}, y \models \varphi$ следует, что $\mathcal{M}, y \models \psi$;

– $\mathcal{M}, x \models \neg\varphi$, если для каждого $y \in W$, достижимого из x по R , неверно, что $\mathcal{M}, y \models \varphi$.

Пусть C_S , C_R , C_T и C_A – классы всех серийных, всех рефлексивных, всех транзитивных и всех антисимметричных шкал. Пусть также $C_{RT} = C_R \cap C_T$ и $C_{RTA} = C_{RT} \cap C_A$. Определим логики CTL, S4 и Int как множества формул в соответствующих языках, истинных во всех шкалах из C_S , C_{RT} и C_{RTA} (при подходящем определении отношения истинности), соответственно. Каждая формула φ задает некоторый класс шкал, в которых она истинна, являющийся подклассом C_S , C_{RT} или C_{RTA} в зависимости от того, в языке какой логики определена φ ; обозначим этот класс посредством $C(\varphi)$.

Погружения S4 в CTL и Int в S4

Опишем некоторые связи между языками логик CTL, S4 и Int, позволяющие в ряде случаев задавать классы шкал Крипке формулами одного из этих языков, если известно, как можно это сделать в другом.

Заметим, что S4-формулы моделируются CTL-формулами. Определение истинности формулы $AX\varphi$ можно переписать в эквивалентном виде следующим образом: $\mathcal{M}, x \models AX\varphi$ тогда и только тогда, когда для каждого $y \in W$, достижимого из x по R , верно, что $\mathcal{M}, y \models \varphi$. Такая формулировка по своей форме в точности соответствует определению истинности формулы вида $\Box\varphi$. Но имеется существенное отличие: в случае шкал для CTL отношение достижимости является серийным, а в случае шкал для S4 – рефлексивным и транзитивным. Из рефлексивности бинарного отношения следует его серийность, но из серийности не следуют ни рефлексивность, ни транзитивность. Тем не менее, можно ввести в рассмотрение отношение R^* , определив его как рефлексивно-транзитивное замыкание отношения R . В случае шкал логики S4 получаем, что $R^* = R$ и определение истинности для формулы $\Box\varphi$ не изменится при замене в нем R на R^* . А в случае CTL при замене R на R^* в приведенном определении истинности формулы $AX\varphi$ полу-

чим определение истинности формулы $AG\varphi$: $\mathcal{M}, x \models AG\varphi$ тогда и только тогда, когда для каждого $y \in W$, достижимого из x по R^* , верно, что $\mathcal{M}, y \models \varphi$. Так происходит из-за того, что достижимость по R^* как раз и дает все точки всех путей, выходящих из данной точки, то есть соответствует модальности AG .

Это наблюдение позволяет сделать следующий вывод. Пусть f – функция, которая заменяет в произвольной S4-формуле φ каждое вхождение символа $\Box$ вхождением модальности AG . Для каждой шкалы $\mathcal{F} = \langle W, R \rangle$ определим шкалу $\mathcal{F}^*$, положив $\mathcal{F}^* = \langle W, R^* \rangle$; тогда, если $\mathcal{F} \in C_S$, то $\mathcal{F}^* \in C_{RT}$. Справедливо следующее утверждение.

Утверждение 1. Пусть φ – S4-формула и $\mathcal{F} \in C_S$. Тогда $\mathcal{F}^* \models \varphi \Leftrightarrow \mathcal{F} \models f(\varphi)$.

Замечание 1. В частности, это означает, что $\varphi \in S4 \Leftrightarrow f(\varphi) \in CTL$.

Следствие 1. Для всякой S4-формулы φ имеет место равенство $C(\varphi) = C(f(\varphi)) \cap C_{RT}$.

Таким образом, если известен класс шкал, задающий $f(\varphi)$ в классе C_S , то известен и класс шкал, задающий φ в классе C_{RT} .

Покажем, как моделировать интуиционистские формулы S4-формулами. Для этих целей можно использовать перевод Гёделя t , который действует так: он ставит модальность $\Box$ перед каждой пропозициональной переменной, логической константой, отрицанием и импликацией [6]. Например, $t(\neg p \wedge q \rightarrow \perp) = \Box(\Box\neg p \wedge \Box q \rightarrow \Box\perp)$.

Для перевода Гёделя верно следующее [6]: $\varphi \in \text{Int} \Leftrightarrow t(\varphi) \in S4$. Рассмотрим, как связаны классы шкал, определяемые формулами φ и $t(\varphi)$. Пусть $\mathcal{F} = \langle W, R \rangle$ – шкала логики S4, то есть $\mathcal{F} \in C_{RT}$. Разобьем множество W на классы эквивалентности по отношению R , где класс $[x]$, порожденный точкой x , определяется обычно: $[x] = \{y \in W : xRy \text{ и } yRx\}$. Класс $[x]$ называют *сгустком*, или *кластером*. Пусть $W^\#$ – множество получившихся сгустков в шкале $\mathcal{F}$, а $R^\#$ – отношение достижимости на $W^\#$, определяемое следующим образом: $[x]R^\#[y]$, если xRy . Пусть $\mathcal{F}^\# = \langle W^\#, R^\# \rangle$. Если $\mathcal{F} \in C_{RTA}$, то шкала $\mathcal{F}^\#$ изоморфна шкале $\mathcal{F}$, поскольку в этом случае $[x] = \{x\}$. В случае, когда $\mathcal{F} \in C_{RT}$ (в частности, и если $\mathcal{F} \in C_{RTA}$), получаем, что $\mathcal{F}^\# \in C_{RTA}$, причем единственным отличием шкалы $\mathcal{F}^\#$ от шкалы $\mathcal{F}$ будет то, что каждый сгусток «схлопнется» в одну точку. Из-за условия наследственности оценки интуиционистские формулы не могут различить точки из одного сгустка, а потому не могут этого сделать и их образы при переводе Гёделя. Таким образом, справедливо следующее утверждение.

Утверждение 2. Пусть φ – интуиционистская формула и $\mathcal{F} \in C_{RT}$. Тогда $\mathcal{F}^\# \models \varphi \Leftrightarrow \mathcal{F} \models t(\varphi)$.

Следствие 2. Для всякой интуиционистской формулы φ имеет место следующее равенство: $C(\varphi) = C(t(\varphi)) \cap C_{RTA}$.

Из следствий 1 и 2 получаем результат, описывающий связь между интуиционистским языком и языком логики CTL.

Следствие 3. Для всякой интуиционистской формулы φ имеет место равенство $C(\varphi) = C(f(t(\varphi))) \cap C_{\text{RTA}}$.

Логика предикатов и шкалы Крипке

Обратимся к языку первого порядка, то есть к языку логики предикатов QCL. Рассмотрим не весь язык логики предикатов, а только ту его часть, которая позволяет описывать свойства отношения достижимости в моделях Крипке. Будем считать, что в языке логики предикатов имеются счетное множество предметных переменных, бинарная предикатная буква R , соответствующая отношению достижимости в шкалах Крипке, символ равенства $=$, а также логические связки, кванторы по предметным переменным и технические символы (скобки). Тогда каждую шкалу Крипке $\mathcal{F} = \langle W, R \rangle$ можно понимать как модель описанного фрагмента языка логики QCL, в результате чего для предикатной формулы Φ получаем естественное определение отношения истинности в шкале $\mathcal{F}$; если Φ истинна в $\mathcal{F}$, то пишем $\mathcal{F} \models \Phi$. Так, например, если $\Phi = \forall x (xRx)$, то $\mathcal{F} \models \Phi$ тогда и только тогда, когда отношение достижимости в $\mathcal{F}$ рефлексивно. Далее под формулами языка логики предикатов будем понимать только замкнутые формулы, то есть не содержащие свободных переменных. Пусть $C(\Phi)$ – класс шкал, в которых истинна формула Φ .

В случае семантики CTL для описания свойств отношения достижимости R наряду с символами R и $=$ целесообразно использовать также символ R^* , соответствующий рефлексивно-транзитивному замыканию отношения R . Тогда выразительные свойства предикатного языка существенно повышаются: проблема истинности формул становится не только алгоритмически неразрешимой, но и рекурсивно неперечислимой. Для предикатной формулы Φ в языке с символами $=$, R и R^* класс шкал, в которых истинна Φ , также будем обозначать $C(\Phi)$.

Здесь будет важным следующее.

Утверждение 3. Пусть Φ – формула в языке с символами $=$, R и R^* , причем $C(\Phi) \subseteq C_{\text{RT}}$. Тогда существует такая формула Ψ в языке с символами R и $=$, что $C(\Phi) = C(\Psi)$.

Доказательство. Поскольку $C(\Phi) \subseteq C_{\text{RT}}$, формула Φ определяет в шкалах отношение R , являющееся рефлексивно-транзитивным. Следовательно, его рефлексивно-транзитивное замыкание совпадает с ним самим, то есть $R^* = R$. Таким образом, в качестве Ψ можно взять формулу, получающуюся из Φ заменой каждого вхождения символа R^* на R .

Утверждение доказано.

Определимость классов шкал формулами

Класс шкал C называется *определимым формулами языка логики L* , если существует такая фор-

мула φ языка логики L , что выполняется равенство $C = C(\varphi)$. Например, $C_S = C(\forall x \exists y (xRy))$, то есть C_S является определимым предикатными формулами, или, как принято говорить, *первопорядково определимым*. Поскольку условия рефлексивности, транзитивности и антисимметричности также описываются предикатными формулами, то классы шкал C_R , C_T и C_A тоже первопорядково определимы. Именно, пусть ref_{QCL} , tr_{QCL} и asym_{QCL} – это формулы $\forall x (xRx)$, $\forall x \forall y \forall z (xRy \wedge yRz \rightarrow xRz)$ и $\forall x \forall y (xRy \wedge yRx \rightarrow x = y)$, соответственно; тогда $C_R = C(\text{ref}_{\text{QCL}})$, $C_T = C(\text{tr}_{\text{QCL}})$, $C_A = C(\text{asym}_{\text{QCL}})$. Условия рефлексивности и транзитивности можно описать и CTL-формулами: взяв $\text{ref}_{\text{CTL}} = AXp \rightarrow p$ и $\text{tr}_{\text{CTL}} = AXp \rightarrow AXAXp$, получим, что $C_R = C(\text{ref}_{\text{CTL}})$ и $C_T = C(\text{tr}_{\text{CTL}})$.

Сделаем следующее наблюдение.

Утверждение 4. Пусть классы C_1 и C_2 определены формулами языка одной из логик Int, S4, CTL или QCL. Тогда класс $C_1 \cap C_2$ тоже является определимым формулами языка этой же логики.

Доказательство. Достаточно заметить: если C_1 определяется формулой φ_1 , а C_2 – формулой φ_2 , то $C_1 \cap C_2$ определяется формулой $\varphi_1 \wedge \varphi_2$.

Утверждение доказано.

Отметим, что для операции объединения аналогичное утверждение тоже выполняется, а для дополнения ситуация иная. В предикатном случае, если Φ задает некоторый класс шкал, $\neg\Phi$ задает его дополнение. В случае же логик Int, S4 и CTL это не так. Например, в CTL условие рефлексивности описывается формулой ref_{CTL} , условие транзитивности – формулой tr_{CTL} , условие симметричности – формулой $\text{sym}_{\text{CTL}} = p \rightarrow AX\neg AX\neg p$, при этом условия нерелексивности, нетранзитивности, несимметричности (и антисимметричности) формулами языка CTL описать невозможно. Так, отрицание формулы $\text{ref}_{\text{CTL}} = AXp \rightarrow p$, задающей условие рефлексивности в шкалах, можно опровергнуть в любой шкале логики CTL, в том числе в нерелексивной: достаточно взять оценку, при которой переменная p истинна в каждой точке шкалы, и тогда формула ref_{CTL} станет истинной в каждой точке получившейся модели, а $\neg\text{ref}_{\text{CTL}}$ – ложной. Таким образом, $\neg\text{ref}_{\text{CTL}}$ не задает условие нерелексивности (формула $\neg\text{ref}_{\text{CTL}}$ вообще определяет пустой класс шкал логики CTL). Ситуация с остальными указанными формулами аналогична.

Точные формулировки вопросов

Теперь можно дать точные формулировки вопросов, о которых шла речь в начале статьи.

Вопрос 1. Существует ли алгоритм, который по произвольной CTL-формуле φ дает ответ на вопрос о том, существует ли такая предикатная формула Φ , что $C(\varphi) = C(\Phi)$?

Вопрос 2. Существует ли алгоритм, который по произвольной CTL-формуле φ строит такую

предикатную формулу Φ , что $C(\varphi) = C(\Phi)$, а в случае ее отсутствия сообщает об этом?

Вопрос 3. Существует ли алгоритм, который по произвольной предикатной формуле Φ дает ответ на вопрос о том, существует ли такая CTL-формула φ , что $C(\varphi) = C(\Phi)$?

Вопрос 4. Существует ли алгоритм, который по произвольной предикатной формуле Φ строит такую CTL-формулу φ , что $C(\varphi) = C(\Phi)$, а в случае ее отсутствия сообщает об этом?

Конечно, вопросы связаны между собой. Если ответ на вопрос 2 положителен, то и ответ на вопрос 1 положителен; соответственно, отрицательный ответ на вопрос 1 приводит к отрицательному ответу на вопрос 2. То же относится и к вопросам 3 и 4. Покажем, как из известных результатов о связи между Int и QCL получить ответ на вопросы 1 и 2; в отношении же вопросов 3 и 4 ограничимся формулировкой гипотезы.

Формулу φ языка логики L будем называть *первопорядково определимой*, если класс $C(\varphi)$ определим с помощью формул языка логики предикатов, то есть если существует такая предикатная формула Φ , что $C(\varphi) = C(\Phi)$. Под *проблемой первопорядковой определимости формул языка логики L* будем понимать следующую задачу: по произвольной L -формуле φ выяснить, является ли φ первопорядково определимой. Для краткости первопорядково определимые формулы будем называть *ППО-формулами*.

Известен следующий результат для Int и QCL, доказанный в [16]: *проблема первопорядковой определимости интуиционистских формул алгоритмически неразрешима*, то есть не существует алгоритма, решающего эту задачу. Покажем, как из этого результата и сделанных выше наблюдений следует аналогичный результат для языков CTL и QCL.

Неразрешимость первопорядковой определимости CTL-формул

Пусть функция g определена для каждой интуиционистской формулы φ следующим образом: $g(\varphi) = f(t(\varphi)) \wedge \text{ref}_{\text{CTL}} \wedge \text{tr}_{\text{CTL}}$.

Утверждение 5. Пусть φ – интуиционистская формула. Тогда $C(\varphi) = C(g(\varphi)) \cap C_A$.

Доказательство. Согласно следствию 3, имеем $C(\varphi) = C(f(t(\varphi))) \cap C_{\text{RTA}}$. По утверждению 4, $C(g(\varphi)) = C(f(t(\varphi))) \cap C(\text{ref}_{\text{CTL}}) \cap C(\text{tr}_{\text{CTL}})$. Поскольку $C_R = C(\text{ref}_{\text{CTL}})$ и $C_T = C(\text{tr}_{\text{CTL}})$, получаем, что $C(g(\varphi)) = C(f(t(\varphi))) \cap C_R \cap C_T$, следовательно, $C(g(\varphi)) \cap C_A = C(f(t(\varphi))) \cap C_R \cap C_T \cap C_A$, то есть $C(g(\varphi)) \cap C_A = C(f(t(\varphi))) \cap C_{\text{RTA}}$. В итоге получаем $C(\varphi) = C(g(\varphi)) \cap C_A$, что и требовалось.

Утверждение доказано.

Следствие 4. Пусть φ – интуиционистская формула. Тогда, если $g(\varphi)$ – ППО-формула, то φ – тоже ППО-формула.

Доказательство. Пусть Φ – формула языка логики предикатов, для которой выполнено равен-

ство $C(g(\varphi)) = C(\Phi)$. Согласно утверждению 5, $C(\varphi) = C(g(\varphi)) \cap C_A$. Класс C_A первопорядково определим, и тогда из утверждения 4 получаем, что класс $C(\Phi) \cap C_A$ тоже первопорядково определим. Поскольку он равен $C(\varphi)$, заключаем, что φ – ППО-формула.

Следствие доказано.

Следствие 5. Пусть φ – интуиционистская формула. Тогда, если φ – ППО-формула, то $g(\varphi)$ – тоже ППО-формула.

Доказательство. Пусть Φ – формула логики предикатов, для которой $C(\varphi) = C(\Phi)$. Тогда, согласно утверждению 5, $C(\varphi) = C(g(\varphi)) \cap C_A$, отсюда получаем $C(\Phi) = C(g(\varphi)) \cap C_A$. Шкалы класса $C(\varphi)$ являются рефлексивными, транзитивными и антисимметричными, поэтому формула Φ должна, в частности, требовать выполнения каждого из этих условий. Формула $g(\varphi)$ требует выполнения рефлексивности и транзитивности, но, вообще говоря, не антисимметричности.

Пусть $\mathcal{F} = \langle W, R \rangle$ – некоторая шкала из класса $C(g(\varphi))$. Поскольку $C(g(\varphi)) = C(f(t(\varphi))) \cap C_{\text{RT}}$, получаем, что $\mathcal{F} \in C(f(t(\varphi)))$ и $\mathcal{F} \in C_{\text{RT}}$. Из условия $\mathcal{F} \in C_{\text{RT}}$ следует, что $R^* = R$, а значит, $\mathcal{F}^* = \mathcal{F}$. Из того, что $\mathcal{F}^* \in C(f(t(\varphi)))$, по утверждению 1 получаем, что $\mathcal{F} \in C(t(\varphi))$. Кроме того, из условия $\mathcal{F} \in C_{\text{RT}}$ следует, что $\mathcal{F}^{\#} \in C_{\text{RTA}}$. Но тогда, по утверждению 2, $\mathcal{F}^{\#} \in C(\varphi)$. Шкала $\mathcal{F}$ отличается от $\mathcal{F}^{\#}$ лишь тем, что каждый сгусток в $\mathcal{F}$ заменяется в $\mathcal{F}^{\#}$ одной точкой. Пусть теперь $\mathcal{F}_1 \in C(\varphi)$. Тогда из сделанного наблюдения вытекает следующее: если $\mathcal{F}$ – такая шкала, что $\mathcal{F}^{\#}$ изоморфна шкале $\mathcal{F}_1$, то $\mathcal{F} \in C(g(\varphi))$. Следовательно, для описания шкал из класса $C(g(\varphi))$ достаточно в формуле Φ понимать переменные не как точки, а как сгустки. Заменяем в Φ каждую подформулу вида xRy на формулу $\forall u \forall v (xRu \wedge uRx \wedge yRv \wedge vRy \rightarrow uRv)$, где u и v – некоторые не входящие в Φ переменные; получившуюся предикатную формулу обозначим $\Phi^{\#}$. Суть сделанной замены в том, что условие достижимости точки y из точки x заменяется на условие достижимости любой точки $v \in [y]$ из любой точки $u \in [x]$. Тогда $C(\Phi^{\#}) = C(g(\varphi))$, а значит, $g(\varphi)$ – ППО-формула.

Следствие доказано.

Следующее утверждение вытекает из следствий 4 и 5.

Следствие 6. Для любой интуиционистской формулы φ справедлива следующая эквивалентность: φ – ППО-формула тогда и только тогда, когда $g(\varphi)$ – ППО-формула.

Теперь можно доказать основной результат работы.

Теорема. Проблема первопорядковой определимости CTL-формул алгоритмически неразрешима.

Доказательство. Предположим, что это не так, то есть существует алгоритм $\mathcal{A}$, который по любой CTL-формуле φ находит ответ на вопрос о том, су-

существует ли такая предикатная формула Φ , для которой выполнено равенство $C(\varphi) = C(\Phi)$. Покажем, что в этом случае проблема первопорядковой определимости интуиционистских формул тоже должна быть алгоритмически разрешима, что противоречит упомянутому выше результату из [16].

Пусть φ – произвольная интуиционистская формула. Применим алгоритм $\mathcal{A}$ к CTL-формуле $g(\varphi)$. Если результат работы $\mathcal{A}$ на φ будет положительным, то, согласно следствию 6, φ является ППО-формулой; если же результат будет отрицательным, то, снова по следствию 6, φ не является ППО-формулой. Таким образом, с помощью преобразования g и алгоритма $\mathcal{A}$ можно решить проблему первопорядковой определимости интуиционистских формул, а это противоречит результату из [16]. Значит, такого алгоритма $\mathcal{A}$ не существует.

Теорема доказана.

Заключение

При формулировке понятия первопорядковой определимости был установлен запрет на использование для описания классов шкал буквы R^* , соответствующей рефлексивно-транзитивному замыканию отношения достижимости в шкалах Крипке. Поэтому выясним, изменится ли что-нибудь, если разрешить использовать R^* для описания классов шкал. Такое расширение языка представляется естественным, поскольку при описании вычислений бывает важно не только то, что происходит на следующем шаге вычисления (этому соответствует R), но и то, что может произойти когда-либо (этому соответствует R^*). Проблема определимости CTL-формул в таком обогащенном языке тоже будет алгоритмически неразрешимой. Достаточно заметить, что преобразование g строит формулу $g(\varphi)$, требующую от отношения достижимости, чтобы оно было рефлексивным и транзитивным. Тогда, согласно утверждению 3, если существует такая формула Φ в языке с R^* , что $C(\Phi) = C(g(\varphi))$, то существует и формула Ψ в языке без R^* , для которой выполняется равенство $C(\Psi) = C(g(\varphi))$.

Следующий уместный вопрос: какова ситуация с первопорядковой определимостью естественных фрагментов языка CTL, в частности, таких, в которых не будет модальности AG ? Во-первых, заметим, что AG можно промоделировать, используя EU : формула $AG\varphi$ эквивалентна в CTL формуле $\neg EF\neg\varphi$, при этом $EF\varphi$ эквивалентна в CTL формуле $TEU\varphi$. Во-вторых, в приведенных выше рассуждениях можно вообще обойтись без модальности AG и использовать только AX . Для этого в определении функции f надо заменить AG на AX . Причем для полученной модификации f уже не будет выполняться аналог утверждения 1; если же добавить конъюнктивные члены ref_{CTL} и tr_{CTL} , то аналог утверждения 1 будет справедлив.

Итак, согласно доказанной теореме, ответ на вопросы 1 и 2 отрицателен, причем даже для до-

вольно простых фрагментов языка логики CTL. Что касается вопросов 3 и 4, то ответ на них не получить так же просто, как это было сделано для решения вопросов 1 и 2 (хотя известно, что проблема определимости предикатных формул интуиционистскими алгоритмически неразрешима): в приведенном доказательстве авторы, по сути, лишь воспользовались тем, что интуиционистские связки можно промоделировать средствами CTL, но как сделать обратное – непонятно, поскольку язык логики CTL является более богатым по своим выразительным возможностям и подходящий перевод CTL-формул в интуиционистские неизвестен (и, видимо, невозможен). Таким образом, вопросы 3 и 4 требуют отдельного исследования и иных методов решения. Тем не менее, сформулируем предположение.

Гипотеза. Проблема CTL-определимости формул логики предикатов алгоритмически неразрешима.

Работа выполнена при поддержке РФФИ, гранты №№ 16-07-01272, 17-03-00818-ОГН и 18-011-00869.

Литература

1. Кларк Э.М., Грамберг О., Пелед Д. Верификация моделей программ: Model checking. М.: Изд-во МЦНМО, 2002, 416 с.
2. Карпов Ю.Г. Model checking: Верификация параллельных и распределенных программных систем. СПб: БХВ-Петербург, 2010, 560 с.
3. Emerson E.A., Halpern J.Y. Decision procedures and expressiveness in the temporal logic of branching time. J. of Comp. and Syst. Sc., 1985, vol. 30, no. 1, pp. 1–24. DOI: [http://dx.doi.org/10.1016/0022-0000\(85\)90001-7](http://dx.doi.org/10.1016/0022-0000(85)90001-7).
4. Булос Дж., Джеффри Р. Вычислимость и логика. М.: Мир, 1994, 396 с.
5. Blackburn P., de Rijke M., Venema Y. Modal logic. Cambridge Univ. Press, 2002.
6. Chagrov A.V., Zakharyashev M.V. Modal logic. Oxford Univ. Press, 1997.
7. Sahlqvist H. Completeness and correspondence in the first and second order semantics for modal logic. Proc. 3rd Scandinavian Logic Symposium, Amsterdam, North-Holland, 1975, pp. 110–143. DOI: [http://dx.doi.org/10.1016/S0049-237X\(08\)70728-6](http://dx.doi.org/10.1016/S0049-237X(08)70728-6).
8. Kracht M. How completeness and correspondence theory got married. In: M. de Rijke (Ed.), Diamonds and Defaults, 1993, pp. 175–214. DOI: http://dx.doi.org/10.1007/978-94-015-8242-1_7.
9. Kracht M. Tools and techniques in modal logic. Studies in Logic and the Foundations of Mathematics, Elsevier, 1999, vol. 142, 559 p.
10. Balbiani P., Kikot S. Sahlqvist theorems for precontact logics. Advances in Modal Logic, 2012, vol. 9, pp. 55–70.
11. Kikot S. A new generalization of Sahlqvist theorem. In: Algebraic and Topological Methods in Non-classical Logics II, Univ. de Barcelona, 2005, pp. 40–41.
12. Kikot S. An extension of Kracht's theorem to generalized Sahlqvist formulas. J. of Applied Non-Classical Logic, 2009, vol. 19, no. 2, pp. 227–251. DOI: <http://dx.doi.org/10.3166/jancl.19.227-251>.
13. Kikot S. Semantic characterization of Kracht's formulas. Advances in Modal Logic, 2010, vol. 8, pp. 218–234.
14. Kikot S., Tsarkov D., Zakharyashev M., Zolin E. Query Answering via Modal Definability with FaCT++. In Proc. of DL, 2013.
15. Kikot S., Zolin E. Modal definability of first-order formulas with free variables and query answering. J. of Applied Logic, 2013, vol. 11, pp. 190–216. DOI: <http://dx.doi.org/10.1016/j.jal.2013.03.007>.
16. Chagrova L.A. An undecidable problem correspondence theory. J. of Symbolic Logic, 1991, vol. 56, iss. 4, pp. 1261–1272. DOI: <http://dx.doi.org/10.2307/2275473>.
17. Мендельсон Э. Введение в математическую логику. М.: Наука, 1976, 320 с.

Software & Systems
DOI: 10.15827/0236-235X.123.591-597

Received 21.03.18
2018, vol. 31, no. 3, pp. 591–597

Algorithmic undecidability of the problem of first-order correspondence of computational tree logic formulas

M.N. Rybakov^{1,2,3}, Ph.D. (Physics and Mathematics), Associate Professor, Research Fellow, Software Engineer,
m_rybakov@mail.ru

L.A. Chagrova¹, Ph.D. (Physics and Mathematics), Associate Professor, chagrov@mail.ru

¹ Tver State University, Tver, 170100, Russian Federation

² University of the Witwatersrand, Johannesburg, 2001, South Africa

³ R&D Institute Centerprograms, Tver, 170024, Russian Federation

Abstract. It is common to use the first-order language as a formal tool for describing properties of various (computational) structures. On the one hand, this language is well understood and easy to use; on the other, many questions that are important from the applications point of view related to this language are algorithmically undecidable, i.e., cannot be answered using a computer program.

These days, there exist various alternative languages that can be used for describing computational processes and their properties, for which the corresponding questions are, in contrast to the first-order language, algorithmically decidable. In this paper, we consider one of such languages, – the language of the Computational Tree Logic (CTL). It is commonly used for program verification as it is capable of describing properties of computational processes, – in particular, properties of the binary relation used in the Kripke semantics.

The authors investigate the possibility of finding algorithmically first-order formulas defining the same classes of Kripke frames as the formulas of the language of CTL. It is well known the problem of finding first-order correspondents of propositional intuitionistic formulas is algorithmically undecidable. The authors reduce – using the Gödel translation of intuitionistic formulas into modal ones, and subsequently a translation of resultant modal formulas into CTL-formulas – the first-order correspondence problem for propositional intuitionistic formulas to the first-order correspondence problem for CTL-formulas on Kripke frames. As a result of this reduction, they prove that the first-order correspondence problem for CTL-formulas is algorithmically undecidable.

In the conclusion, the authors discuss some possible modifications of their construction for fragments of the language of CTL as well as algorithmic decidability of the CTL correspondence problem for first-order formulas.

Keywords: computational models, computational tree logic, first-order definability.

Acknowledgements. The work has been supported by RFBR, projects no. 16-07-01272, 17-03-00818, and 18-011-00869.

References

1. Clarke E.M., Grumberg O., Peled D. *Model Checking*. MIT Press, 1999, 314 p.
2. Karpov Yu.G. *Model Checking: Verification of Parallel and Distributive Software Systems*. St. Petersburg, BHV-Peterburg Publ., 2010, 560 p.
3. Emerson E.A., Halpern J.Y. Decision procedures and expressiveness in the temporal logic of branching time. *J. of Comp. and Syst. Sciences*. 1985, vol. 30, no. 1, pp. 1–24.
4. Boolos G.S., Jeffrey R.C. *Computability and Logic*. 3rd ed. Cambridge Univ. Press, 1989.
5. Blackburn P., de Rijke M., Venema Y. *Modal logic*. Cambridge Univ. Press, 2002.
6. Chagrov A.V., Zakharyashev M.V. *Modal Logic*. Oxford Univ. Press, 1997.
7. Sahlqvist H. Completeness and correspondence in the first and second order semantics for modal logic. *Proc. 3rd Scandinavian Logic Symp.* Amsterdam, North-Holland, 1975, pp. 110–143.
8. Kracht M. How completeness and correspondence theory got married. *Diamonds and Defaults*. M. de Rijke (Ed.). 1993, pp. 175–214.
9. Kracht M. Tools and Techniques in Modal Logic. *Studies in Logic and the Foundations of Mathematics*. Elsevier Publ., 1999, 142 p.
10. Balbiani P., Kikot S. Sahlqvist theorems for precontact logics. *Advances in Modal Logic*. 2012, vol. 9, pp. 55–70.
11. Kikot S. A new generalization of Sahlqvist theorem. *Algebraic and Topological Methods in Non-classical Logics II*. Barcelona, 2005, pp. 40–41.
12. Kikot S. An extension of Kracht's theorem to generalized Sahlqvist formulas. *J. of Applied Non-Classical Logic*. 2009, vol. 19, no. 2, pp. 227–251.
13. Kikot S. Semantic characterization of Kracht's formulas. *Advances in Modal Logic*, 2010, vol. 8, pp. 218–234.
14. Kikot S., Tsarkov D., Zakharyashev M., Zolin E. Query Answering via Modal Definability with FaCT++: First Blood. *Proc. of DL*. 2013.
15. Kikot S., Zolin E. Modal definability of first-order formulas with free variables and query answering. *J. of Applied Logic*. vol. 11, 2013, pp. 190–216.
16. Chagrova L.A. An undecidable problem correspondence theory. *J. of Symbolic Logic*. 1991, vol. 56, iss. 4, pp. 1261–1272.
17. Mendelson E. *Introduction to Mathematical Logic*. Van Nostrand Reinhold Inc. Publ., 1964, 300 p.