УДК 517.11

СЛОЖНОСТЬ КОНСТАНТНОГО ФРАГМЕНТА ПРОПОЗИЦИОНАЛЬНОЙ ДИНАМИЧЕСКОЙ ЛОГИКИ[1]

Рыбаков М.Н.
Кафедра алгебры и математической логики

Поступила в редакцию 15.05.2007, после переработки 14.06.2007.

Основной результат работы состоит в том, что константные фрагменты логик $\mathbf{K}^*$ (с $\mathbf{K}$-модальностью и её «рефлексивно-транзитивным замыканием»), **PDL**, а также некоторых других являются EXPTIME-полными. Доказательство содержит описание довольно общей идеи построения полиномиального погружения логик в их фрагменты от n переменных (и даже в константные фрагменты, как в случае $\mathbf{K}^*$ и **PDL**). В качестве следствия описанной конструкции получена EXPTIME-полнота фрагментов от одной переменной логик знания с оператором всеобщего знания.

The main result of the paper is in that the variable-free fragments of the logics $\mathbf{K}^*$ (with $\mathbf{K}$-modality and its 'reflexive and transitive closure'), **PDL**, and some others are EXPTIME-complete. In the proof some quite general idea how to construct a polynomial reduction of propositional logic to its n-variable (and even variable-free in the case of $\mathbf{K}^*$ and **PDL**) fragment is presented. As a corollary we obtain that the one-variable fragments of logics of knowledge with common knowledge operator are EXPTIME-complete.

Ключевые слова: пропозициональная динамическая логика, сложность, EXPTIME-полнота, проблема разрешения.
Keywords: propositional dynamic logic, complexity, EXPTIME-completeness, decision problem.

Введение. Язык пропозициональной динамической логики **PDL** предоставляет богатые выразительные средства, благодаря чему **PDL** и логики, подобные **PDL**, находят много приложений в различных областях знания, в частности, в различных исследованиях, связанных с компьютерными вычислениями. Своего рода «обратной стороной» выразительности языка является высокая сложность динамической логики: хотя **PDL** и разрешима, проблема разрешения для **PDL** является EXPTIME-полной [7].

Однако заметим, что для приложений, как правило, не требуется вся логика: в приложениях обычно используется лишь некоторая её часть, фрагмент. В частности, для приложений достаточно рассматривать фрагменты логик в языках с

[1]Работа выполнена при поддержке РФФИ, проекты 06–06–80380, 06–01–72555–НЦНИЛ и 07–06–00318.

конечным (и даже заранее ограниченным) множеством переменных. А значит, и многие вопросы — в том числе и проблему разрешения — разумно рассматривать не только для логики в целом, но и для подобных её фрагментов.

Для пропозициональной логики L и натурального числа n посредством $L(n)$ будем обозначать фрагмент логики L, формулы которого строятся из константы $\bot$ и переменных $p_1, \ldots, p_n$ с помощью логических связок языка логики L. В частности, $L(0)$ — это константный фрагмент L.

Отметим следующее. Во-первых, хорошо известны примеры, когда проблема разрешения некоторой логики L достаточно сложна, а фрагменты вида $L(n)$ полиномиально разрешимы. Так, проблема выполнимости булевых формул NP-полна [6], а проблема выполнимости булевых формул от n переменных полиномиально разрешима при любом фиксированном n: в качестве полиномиального алгоритма, решающего эту проблему, можно взять алгоритм, основанный на построении таблиц истинности фиксированного размера — состоящих из 2^n строк. Аналогична ситуация с проблемой выполнимости булевых формул с кванторами: эта проблема PSPACE-полна в случае языка с бесконечным числом переменных [18], но несложно понять, что соответствующая проблема для формул в языке с n переменными полиномиально разрешима для каждого фиксированного n. Примерно то же можно сказать и о проблеме разрешения некоторых неклассических логик: например, проблема **S5**-выполнимости NP-полна [12], а фрагмент $\mathbf{S5}(n)$ полиномиально разрешим (для любого n), проблема разрешения для интуиционистской логики **Int** является PSPACE-полной [17], при этом фрагмент $\mathbf{Int}(1)$ полиномиально разрешим [13], проблема разрешения для логик из интервала $[\mathbf{D}, \mathbf{Grz}]$ является PSPACE-трудной, см. [12, 20], а их константные фрагменты тривиально полиномиально разрешимы (даже если сама логика при этом неразрешима). Во-вторых, оказывается, для многих неклассических логик с NP-трудной[2] или PSPACE-трудной проблемой разрешения сложность проблемы разрешения фрагментов этих логик от n переменных также NP-трудна или, соответственно, PSPACE-трудна. Так, NP-полной является проблема выполнимости для $\mathbf{GLLin}(1)$, $\mathbf{S4.3}(2)$, $\mathbf{Grz.3}(2)$ [4], PSPACE-трудной является проблема выполнимости для всех (фрагментов) логик из интервалов $[\mathbf{K}(0), \mathbf{K4}(0)]$, $[\mathbf{K}(1), \mathbf{GL}(1)]$, $[\mathbf{K}(1), \mathbf{Grz}(1)]$, $[\mathbf{Int}(2), \mathbf{KC}(2)]$ и др. [4, 9, 15, 16, 19].

Какова сложность проблемы разрешения для $\mathbf{PDL}(n)$? Полученные ранее результаты позволяют указать следующие верхние и нижние границы: ввиду [4] эта проблема, как минимум, PSPACE-трудна, а ввиду [7] она находится в классе EXPTIME. Является ли она EXPTIME-полной? Последний вопрос задавался автору на научных семинарах, где обсуждались полученные ранее близкие результаты, которые можно найти в [4, 15].

Известно [16], что во многих случаях для доказательства EXPTIME-трудности проблемы разрешения логики достаточно использовать константные формулы или формулы от одной переменной, а также две независимые модальности и одну «сильную» модальность, вроде универсальной модальности или так называемого оператора всеобщего знания. При этом двух модальностей — одной «обычной» и одной «сильной» — для обоснования EXPTIME-трудности может не хватать (при условии, что PSPACE $\neq$ EXPTIME, см. [16]). Цель данной работы — пред-

[2]Имеется в виду, что проблема выполнимости формул является NP-трудной или coNP-трудной.

ставить решение вопроса о сложности $\mathbf{PDL}(n)$, а также подобных фрагментов некоторых других логик с EXPTIME-полной проблемой разрешения. Именно, ниже будет показано, что при наличии в языке логики константы $\bot$, полного набора булевых связок и двух модальностей — модальности $\Box$, соответствующей в шкалах Крипке произвольному отношению R, и модальности $\Box^*$, соответствующей рефлексивно-транзитивному замыканию R, — проблема разрешения логики является EXPTIME-трудной. Это означает, в частности, что проблема разрешения для константного фрагмента **PDL** является EXPTIME-полной при наличии всего лишь одной элементарной программы и операции итерации программ, а также что фрагмент $\mathbf{PDL}(0)$ не является полиномиально разрешимым.

Отметим, что приводимое ниже доказательство EXPTIME-трудности указанной проблемы содержит описание некоторого достаточно общего способа построения полиномиального погружения пропозициональной логики в её фрагмент от конечного числа переменных.

1. Необходимые определения. Мы будем рассматривать формулы, которые строятся из пропозициональных переменных $p_0, p_1, p_2, p_3, \ldots$ и константы $\bot$ с помощью двухместных связок $\wedge$, $\vee$, $\to$, а также одноместных модальностей $\Box$ и $\Box^*$. Определим $\neg$, $\top$, $\leftrightarrow$, $\Diamond$ и $\Diamond^*$ как обычные сокращения: $(\neg\varphi) = (\varphi \to \bot)$, $\top = (\neg\bot)$, $(\varphi \leftrightarrow \psi) = ((\varphi \to \psi) \wedge (\psi \to \varphi))$, $(\Diamond\varphi) = (\neg(\Box(\neg\varphi)))$, $(\Diamond^*\varphi) = (\neg(\Box^*(\neg\varphi)))$. При записи формул будем опускать некоторые скобки, считая самой сильной связкой $\neg$ и далее по убыванию силы связывания — $\Box$, $\Box^*$, $\Diamond$, $\Diamond^*$, $\wedge$, $\vee$, $\leftrightarrow$, $\to$.

В качестве семантики описанного языка будем использовать семантику Крипке. Под *шкалой Крипке* понимаем пару $\mathfrak{F} = \langle W, R\rangle$, где W — непустое множество, а R — бинарное отношение на W. Элементы множества W будем называть мирами, а отношение R — отношением достижимости. Если для некоторых $x, y \in W$ выполнено xRy, то говорим, что из мира x достижим мир y.

Моделью Крипке называем набор $\mathfrak{M} = \langle \mathfrak{F}, v\rangle$, где $\mathfrak{F}$ — шкала Крипке, а v — функция, сопоставляющая каждой переменной некоторое подмножество множества W. Функцию v будем называть оценкой переменных в мирах шкалы $\mathfrak{F}$.

Пусть $\mathfrak{F} = \langle W, R\rangle$ — шкала Крипке, $\mathfrak{M} = \langle \mathfrak{F}, v\rangle$ — модель, определённая на этой шкале. Обозначим через R^* рефлексивно-транзитивное замыкание отношения R. Для всякой формулы φ и всякого мира $x \in W$ определим индуктивно отношение $(\mathfrak{M}, x) \models \varphi$:

$(\mathfrak{M}, x) \not\models \bot$;

$(\mathfrak{M}, x) \models p_i \quad \leftrightharpoons \quad x \in v(p_i)$, где p_i — пропозициональная переменная;

$(\mathfrak{M}, x) \models \varphi \wedge \psi \quad \leftrightharpoons \quad (\mathfrak{M}, x) \models \varphi$ и $(\mathfrak{M}, x) \models \psi$;

$(\mathfrak{M}, x) \models \varphi \vee \psi \quad \leftrightharpoons \quad (\mathfrak{M}, x) \models \varphi$ или $(\mathfrak{M}, x) \models \psi$;

$(\mathfrak{M}, x) \models \varphi \to \psi \quad \leftrightharpoons \quad (\mathfrak{M}, x) \not\models \varphi$ или $(\mathfrak{M}, x) \models \psi$;

$(\mathfrak{M}, x) \models \Box\varphi \quad \leftrightharpoons \quad$ для всякого $y \in W$ такого, что xRy, выполнено $(\mathfrak{M}, y) \models \varphi$;

$(\mathfrak{M}, x) \models \Box^*\varphi \quad \leftrightharpoons \quad$ для всякого $y \in W$ такого, что xR^*y, выполнено $(\mathfrak{M}, y) \models \varphi$.

Из приведённого определения следует, что для связок, введённых как сокра-

щения, справедливо следующее:

$$(\mathfrak{M}, x) \models \neg\varphi \quad \Longleftrightarrow \quad (\mathfrak{M}, x) \not\models \varphi;$$

$$(\mathfrak{M}, x) \models \top;$$

$$(\mathfrak{M}, x) \models \varphi \leftrightarrow \psi \quad \Longleftrightarrow \quad (\mathfrak{M}, x) \models \varphi \text{ тогда и только тогда, когда } (\mathfrak{M}, x) \models \psi;$$

$$(\mathfrak{M}, x) \models \Diamond\varphi \quad \Longleftrightarrow \quad \text{существует мир } y \in W \text{ такой, что } xRy \text{ и } (\mathfrak{M}, y) \models \varphi;$$

$$(\mathfrak{M}, x) \models \Diamond^*\varphi \quad \Longleftrightarrow \quad \text{существует мир } y \in W \text{ такой, что } xR^*y \text{ и } (\mathfrak{M}, y) \models \varphi.$$

Если $(\mathfrak{M}, x) \models \varphi$, то говорим, что формула φ истинна в мире x модели $\mathfrak{M}$, иначе — что формула φ опровергается в мире x модели $\mathfrak{M}$. Говорим, что формула φ истинна в модели $\mathfrak{M}$, если φ истинна в каждом мире этой модели; в этом случае пишем $\mathfrak{M} \models \varphi$. Говорим, что формула φ истинна в мире x шкалы $\mathfrak{F}$, если для каждой модели $\mathfrak{M} = \langle \mathfrak{F}, v \rangle$, определённой на шкале $\mathfrak{F}$, справедливо утверждение $(\mathfrak{M}, x) \models \varphi$; в этом случае пишем $(\mathfrak{F}, x) \models \varphi$. Говорим, что формула φ истинна в шкале $\mathfrak{F}$, если φ истинна в каждой модели, определённой на этой шкале; пишем $\mathfrak{F} \models \varphi$.

Определим логику $\mathbf{K}^*$ как множество формул в описанном языке, истинных во всех шкалах Крипке.

Напомним определения классов сложности P и EXPTIME, а также некоторые понятия, связанные с ними. Мы ограничимся рассмотрением проблем распознавания множеств, т. е. проблем вида «$x \in X$?», где X — некоторое множество (слов). В этом случае P — это класс проблем, решаемых детерминированными алгоритмами за полиномиальное время от размера входных данных, EXPTIME — класс проблем, решаемых детерминированными алгоритмами за экспоненциальное время от размера входных данных.

Проблема «$x \in X$?» называется EXPTIME-трудной, если к ней полиномиально сводится любая проблема из класса EXPTIME, т. е. если для всякой проблемы «$y \in Y$?» из класса EXPTIME существует полиномиально вычислимая функция f такая, что для всякого y выполняется эквивалентность

$$y \in Y \quad \Longleftrightarrow \quad f(y) \in X.$$

Проблема «$x \in X$?» называется EXPTIME-полной, если она принадлежит классу EXPTIME и является EXPTIME-трудной.

Более детально по вопросам, касающимся теории вычислительной сложности, читатель может проконсультироваться, обратившись к [8, 11, 14, 18] (отметим, что [8] имеет русский перевод [1], а [18] имеет русский перевод [2]).

2. Сложность константного фрагмента $\mathbf{K}^*$. Цель данного раздела состоит в том, чтобы доказать следующую теорему.

Теорема 1. *Проблема разрешения константного фрагмента логики* $\mathbf{K}^*$ *является* EXPTIME*-полной.*

Доказательство. Тот факт, что проблема разрешения для $\mathbf{K}^*(0)$ принадлежит классу EXPTIME, следует из того, что проблема разрешения для логики $\mathbf{K}^*$

является EXPTIME-полной [7] (см. также [3]). Покажем, что проблема разрешения для константного фрагмента логики $\mathbf{K}^*$ является EXPTIME-трудной. Для этого сначала сведём проблему принадлежности логике $\mathbf{K}^*$ к проблеме принадлежности логике $\mathbf{K}^*$ формул специального вида.

Пусть φ — произвольная формула. Пусть n — число пропозициональных переменных, входящих в φ. Без ограничений общности можем считать, что φ является формулой от переменных $p_1, \ldots, p_n$. В этом случае переменная p_{n+1} не входит в φ. Используя p_{n+1}, для каждой подформулы ψ формулы φ определим формулу ψ^* следующим образом:

$$\begin{aligned}
\bot^* &= \bot;\\
p_i^* &= p_i, \text{ где } i \in \{1, \ldots, n\};\\
(\psi_1 \wedge \psi_2)^* &= \psi_1^* \wedge \psi_2^*;\\
(\psi_1 \vee \psi_2)^* &= \psi_1^* \vee \psi_2^*;\\
(\psi_1 \to \psi_2)^* &= \psi_1^* \to \psi_2^*;\\
(\Box\psi_1)^* &= \Box(p_{n+1} \to \psi_1^*);\\
(\Box^*\psi_1)^* &= \Box^*(p_{n+1} \to \psi_1^*).
\end{aligned}$$

Определим формулу $\varphi^\#$, положив

$$\varphi^\# = (p_{n+1} \wedge \Box^*(\neg p_{n+1} \to \Box^* \neg p_{n+1})) \to \varphi^*.$$

Формула $\varphi^\#$ отличается от φ, по сути, лишь тем, что все вхождения модальностей в φ заменяются вхождениями соответствующих «ограниченных» модальностей, где в роли «ограничения» выступает новая переменная p_{n+1}. Снимая это «ограничение», мы получаем формулу, эквивалентную в $\mathbf{K}^*$ исходной формуле φ. Более точно, пусть $\varphi^\#_\top$ — формула, получающаяся из $\varphi^\#$ подстановкой формулы $\top$ вместо переменной p_{n+1}.

Лемма 2. *Для всякой формулы φ справедливо следующее: $\varphi^\#_\top \leftrightarrow \varphi \in \mathbf{K}^*$.*

Доказательство этого утверждения мы оставляем читателю. ❑

В дальнейшем рассмотрение формулы $\varphi^\#$ вместо φ даст нам некоторые «технические» преимущества; эти преимущества станут понятны ниже. Сейчас же покажем, что принадлежность одной из этих формул логике $\mathbf{K}^*$ равносильна принадлежности второй формулы логике $\mathbf{K}^*$.

Лемма 3. *Для всякой формулы φ имеет место следующая эквивалентность:*

$$\varphi \in \mathbf{K}^* \iff \varphi^\# \in \mathbf{K}^*.$$

Доказательство. Пусть φ — некоторая формула, $p_1, \ldots, p_n$ — её переменные. Если $\varphi^\# \in \mathbf{K}^*$, то $\varphi^\#_\top \in \mathbf{K}^*$, откуда, согласно лемме 2, получаем, что $\varphi \in \mathbf{K}^*$.

Пусть теперь $\varphi \in \mathbf{K}^*$. Предположим, что $\varphi^\# \notin \mathbf{K}^*$. Тогда существует шкала $\mathfrak{F} = \langle W, R\rangle$ и модель $\mathfrak{M} = \langle \mathfrak{F}, v\rangle$, определённая на этой шкале, такая, что $(\mathfrak{M}, x_0) \not\models \varphi^\#$ для некоторого $x_0 \in W$. Пусть

$$W_1 = \{x \in W : x_0 R^* x \text{ и } (\mathfrak{M}, x) \models p_{n+1}\}.$$

Заметим, что W_1 — непустое множество, т. к. $x_0 \in W_1$. На множестве W_1 определим отношение R_1, положив для всяких $x, y \in W_1$

$$xR_1y \quad \leftrightharpoons \quad xRy.$$

Пусть $\mathfrak{F}_1 = \langle W_1, R_1 \rangle$. В шкале $\mathfrak{F}_1$ определим оценку v_1, положив для всякой переменной p и всякого $x \in W_1$

$$x \in v_1(p) \quad \leftrightharpoons \quad x \in v(p).$$

Пусть $\mathfrak{M}_1 = \langle \mathfrak{F}_1, v_1 \rangle$.

Индукцией по построению подформулы ψ формулы φ (т. е. по числу связок в ψ) покажем, что для всякого $x \in W_1$ имеет место эквивалентность

$$(\mathfrak{M}_1, x) \models \psi \quad \Longleftrightarrow \quad (\mathfrak{M}, x) \models \psi^*.$$

Случай, когда $\psi = \bot$ тривиален. Если $\psi = p_i$, то указанная эквивалентность выполняется в силу определения оценки v_1.

Пусть формулы ψ_1 и ψ_2 таковы, что для всякого $x \in W_1$ имеют место эквивалентности

$$(\mathfrak{M}_1, x) \models \psi_1 \quad \Longleftrightarrow \quad (\mathfrak{M}, x) \models \psi_1^*;$$
$$(\mathfrak{M}_1, x) \models \psi_2 \quad \Longleftrightarrow \quad (\mathfrak{M}, x) \models \psi_2^*.$$

Если $\psi = \psi_1 \wedge \psi_2$, то для всякого $x \in W_1$ имеем следующую цепочку эквивалентностей:

$$\begin{aligned}(\mathfrak{M}_1, x) \models \psi \quad &\Longleftrightarrow \quad (\mathfrak{M}_1, x) \models \psi_1 \text{ и } (\mathfrak{M}_1, x) \models \psi_2 \\ &\Longleftrightarrow \quad (\mathfrak{M}, x) \models \psi_1^* \text{ и } (\mathfrak{M}, x) \models \psi_2^* \\ &\Longleftrightarrow \quad (\mathfrak{M}, x) \models \psi^*.\end{aligned}$$

Случаи $\psi = \psi_1 \vee \psi_2$ и $\psi = \psi_1 \to \psi_2$ рассматриваются аналогично.

Пусть $\psi = \Box\psi_1$ и пусть $x \in W_1$.

Если $(\mathfrak{M}_1, x) \not\models \psi$, то существует мир $y \in W_1$ такой, что xR_1y и $(\mathfrak{M}_1, y) \not\models \psi_1$, и, согласно индукционному предположению, $(\mathfrak{M}, y) \not\models \psi_1^*$. Но $y \in W_1$, поэтому $(\mathfrak{M}, y) \models p_{n+1}$, а следовательно, $(\mathfrak{M}, y) \not\models p_{n+1} \to \psi_1^*$, а т. к. xRy, получаем, что $(\mathfrak{M}, x) \not\models \Box(p_{n+1} \to \psi_1^*)$, т. е. $(\mathfrak{M}, x) \not\models \psi^*$.

Пусть теперь $(\mathfrak{M}, x) \not\models \psi^*$. Тогда существует мир $y \in W$ такой, что xRy, $(\mathfrak{M}, y) \models p_{n+1}$ и $(\mathfrak{M}, y) \not\models \psi_1^*$. Поскольку $(\mathfrak{M}, y) \models p_{n+1}$, получаем, что $y \in W_1$, и, по индукционному предположению, $(\mathfrak{M}_1, y) \not\models \psi_1$, а т. к. xR_1y, получаем, что $(\mathfrak{M}_1, x) \not\models \psi$.

Пусть $\psi = \Box^*\psi_1$ и пусть $x \in W_1$.

Если $(\mathfrak{M}_1, x) \not\models \psi$, то аналогично предыдущему случаю (просто заменяя в доказательстве R на R^*) получаем, что $(\mathfrak{M}, x) \not\models \psi^*$.

Пусть теперь $(\mathfrak{M}, x) \not\models \psi^*$. Тогда существует мир $y \in W$ такой, что xR^*y, $(\mathfrak{M}, y) \models p_{n+1}$ и $(\mathfrak{M}, y) \not\models \psi_1^*$. Поскольку $(\mathfrak{M}, y) \models p_{n+1}$, получаем, что $y \in W_1$. Покажем, что xR_1^*y. Утверждение xR^*y означает, что выполнено хотя бы одно из следующих условий:

- $x = y$;
- xRy;

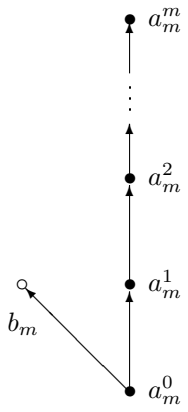

Рис. 1: Шкала $\mathfrak{F}_m$

- существуют $x_1, \ldots, x_k \in W$ такие, что $xRx_1R \ldots Rx_kRy$.

Ясно, что в первом и втором случаях xR_1^*y. Рассмотрим третий случай. Покажем, что $x_1, \ldots, x_k \in W_1$. Предположим, что это не так, т. е. $x_i \notin W_1$ для некоторого $i \in \{1, \ldots, k\}$. Но тогда $(\mathfrak{M}, x_i) \not\models p_{n+1}$. Поскольку $(\mathfrak{M}, x_0) \not\models \varphi^\#$, получаем, что $(\mathfrak{M}, x_0) \models p_{n+1} \wedge \Box^*(\neg p_{n+1} \to \Box^* \neg p_{n+1})$. Последнее, в частности, означает, что $(\mathfrak{M}, x_i) \models \neg p_{n+1} \to \Box^* \neg p_{n+1}$, и из того, что $(\mathfrak{M}, x_i) \models \neg p_{n+1}$ получаем, что $(\mathfrak{M}, x_i) \models \Box^* \neg p_{n+1}$, а следовательно, $(\mathfrak{M}, y) \models \neg p_{n+1}$, что невозможно, т. к. $y \in W_1$. Таким образом, $x_1, \ldots, x_k \in W_1$, а значит, и в третьем случае xR_1^*y. Осталось заметить, что, по индукционному предположению, $(\mathfrak{M}_1, y) \not\models \psi_1$, а значит, $(\mathfrak{M}_1, x) \not\models \psi$.

Из доказанного следует, что $(\mathfrak{M}, x_0) \not\models \varphi$, что невозможно, т. к. $\varphi \in \mathbf{K}^*$. Следовательно, $\varphi^\# \in \mathbf{K}^*$. ❑

Отметим ещё одно свойство формулы $\varphi^\#$.

Лемма 4. *Если* $\varphi^\# \notin \mathbf{K}^*$, *то существует модель* $\mathfrak{M} = \langle \mathfrak{F}, v \rangle$, *определённая на некоторой шкале* $\mathfrak{F} = \langle W, R \rangle$, *такая, что* $\mathfrak{M} \not\models \varphi^\#$ *и* $v(p_{n+1}) = W$.

Доказательство. Если $\varphi^\# \notin \mathbf{K}^*$, то, согласно лемме 3, $\varphi \notin \mathbf{K}^*$, и, согласно лемме 2, $\varphi_\top^\# \notin \mathbf{K}^*$, откуда следует справедливость доказываемого утверждения. ❑

Для всякого положительного натурального числа m определим стандартным образом сокращение $\Diamond^m \psi$: $\Diamond^1 \psi = \Diamond \psi$, $\Diamond^{k+1} \psi = \Diamond \Diamond^k \psi$. Для каждого $m > 0$ определим формулы α_m и β_m следующим образом:

$$\begin{aligned} \alpha_m &= \Diamond^m \Box \bot \wedge \neg \Diamond^{m+1} \Box \bot \wedge \Diamond(\Diamond \top \wedge \Box \Diamond \top); \\ \beta_m &= \Diamond \alpha_m. \end{aligned}$$

Кроме того, для каждого $m > 0$ определим шкалу $\mathfrak{F}_m = \langle W_m, R_m \rangle$, положив

$$\begin{array}{rcl} W_m & = & \{a_m^0, a_m^1, \ldots, a_m^m\} \cup \{b_m\}; \\ xR_m y & \leftrightharpoons & \text{либо } x = a_m^i,\ y = a_m^j \text{ и } i < j, \\ & & \text{либо } x = a_m^0,\ y = b_m, \\ & & \text{либо } x = y = b_m. \end{array}$$

Шкала $\mathfrak{F}_m$ изображена на рис. 1; чёрные кружки́ соответствуют иррефлексивным мирам $a_m^0, \ldots, a_m^m$, светлый — рефлексивному миру b_m, отношение достижимости транзитивно.

Лемма 5. *Для всяких положительных натуральных чисел k и m имеет место следующая эквивалентность:*

$$(\mathfrak{F}_m, x) \models \alpha_k \iff k = m \text{ и } x = a_m^0.$$

Доказательство состоит в тривиальной проверке указанного условия и предоставляется читателю. ❑

Определим $\varphi_\beta^\#$ как формулу, получающуюся подстановкой формул $\beta_1, \ldots, \beta_{n+1}$ в формулу $\varphi^\#$ вместо переменных $p_1, \ldots, p_{n+1}$ соответственно.

Лемма 6. *Имеет место следующая эквивалентность:*

$$\varphi \in \mathbf{K}^* \iff \varphi_\beta^\# \in \mathbf{K}^*.$$

Доказательство Пусть $\varphi \in \mathbf{K}^*$. Тогда, по лемме 3, $\varphi^\# \in \mathbf{K}^*$, а поскольку формула $\varphi_\beta^\#$ является подстановочным примером формулы $\varphi^\#$, получаем, что $\varphi_\beta^\# \in \mathbf{K}^*$.

Пусть $\varphi \notin \mathbf{K}^*$. Тогда, согласно лемме 3, $\varphi^\# \notin \mathbf{K}^*$. Следовательно, существует модель $\mathfrak{M} = \langle \mathfrak{F}, v \rangle$, определённая на некоторой шкале $\mathfrak{F} = \langle W, R \rangle$, такая, что формула $\varphi^\#$ опровергается в некотором мире x_0 этой модели. Согласно лемме 4, можем считать, что $\mathfrak{M} \models p_{n+1}$. Построим шкалу, в некотором мире которой будет опровергаться формула $\varphi_\beta^\#$.

Без ограничений общности можем считать, что множества миров шкал Крипке $\mathfrak{F}, \mathfrak{F}_1, \ldots, \mathfrak{F}_{n+1}$ попарно не пересекаются. Пусть $\mathfrak{F}_\beta = \langle W_\beta, R_\beta \rangle$, где

$$\begin{array}{rcl} W_\beta & = & W \cup W_1 \cup \cdots \cup W_{n+1}; \\ xR_\beta y & \leftrightharpoons & \text{либо } x, y \in W \text{ и } xRy, \\ & & \text{либо } x, y \in W_m \text{ для некоторого } m \in \{1, \ldots, n+1\} \text{ и } xRy, \\ & & \text{либо } x \in W,\ (\mathfrak{M}, x) \models p_k \text{ и } y = a_k^0. \end{array}$$

Для всякой подформулы ψ формулы φ обозначим через ψ_β формулу, получающуюся из ψ^* подстановкой формул $\beta_1, \ldots, \beta_{n+1}$ вместо $p_1, \ldots, p_{n+1}$ соответственно. Индукцией по построению подформулы ψ формулы φ докажем, что для всякого $x \in W$

$$(\mathfrak{F}_\beta, x) \models \psi_\beta \iff (\mathfrak{M}, x) \models \psi^*.$$

Если $\psi = \bot$, то $\psi^* = \bot$ и $\psi_\beta = \bot$, поэтому указанная эквивалентность выполняется тривиально.

Пусть $\psi = p_k$, где $k \in \{1, \ldots, n\}$. В этом случае $\psi^* = p_k$, $\psi_\beta = \beta_k$.

Пусть $x \in W$ и $(\mathfrak{M}, x) \models p_k$. В этом случае $xR_\beta a_k^0$. Тогда, согласно лемме 5, $(\mathfrak{F}_k, a_k^0) \models \alpha_k$; ясно, что также $(\mathfrak{F}_\beta, a_k^0) \models \alpha_k$, а поэтому $(\mathfrak{F}_\beta, x) \models \Diamond\alpha_k$, т. е. $(\mathfrak{F}_\beta, x) \models \beta_k$.

Пусть $x \in W$ и $(\mathfrak{F}_\beta, x) \models \beta_k$. Тогда существует мир $y \in W_\beta$ такой, что $xR_\beta y$ и $(\mathfrak{F}_\beta, y) \models \alpha_k$. Заметим, что $y \notin W$. Действительно, предположим, что $y \in W$. Тогда $yR_\beta a_{n+1}^0$ (поскольку $\mathfrak{M} \models p_{n+1}$), поэтому $(\mathfrak{F}_\beta, y) \not\models \neg\Diamond^{k+1}\Box\bot$, и следовательно, $(\mathfrak{F}_\beta, y) \not\models \alpha_k$. Получаем противоречие, а значит, $y \notin W$. Значит, $y \in W_m$ для некоторого $m \in \{1, \ldots, n+1\}$, и в силу леммы 5, $y = a_k^0$. Осталось заметить, что, по определению отношения R_β, $xR_\beta a_k^0$ только в том случае, когда $(\mathfrak{M}, x) \models p_k$.

Пусть подформулы χ и ξ формулы φ таковы, что для всякого $z \in W$

$$(\mathfrak{F}_\beta, z) \models \chi_\beta \iff (\mathfrak{M}, z) \models \chi^*;$$
$$(\mathfrak{F}_\beta, z) \models \xi_\beta \iff (\mathfrak{M}, z) \models \xi^*.$$

Пусть $\psi = \chi \wedge \xi$, $x \in W$. Тогда имеют место следующие эквивалентности:

$$\begin{aligned}(\mathfrak{F}_\beta, x) \models \psi_\beta &\iff (\mathfrak{F}_\beta, x) \models \chi_\beta \text{ и } (\mathfrak{F}_\beta, x) \models \xi_\beta \\ &\iff (\mathfrak{M}, x) \models \chi^* \text{ и } (\mathfrak{M}, x) \models \xi^* \\ &\iff (\mathfrak{M}, x) \models \psi^*.\end{aligned}$$

Случаи, когда $\psi = \chi \vee \xi$ и $\psi = \chi \to \xi$, рассматриваются аналогично.

Пусть $\psi = \Box\chi$, $x \in W$. Если $(\mathfrak{M}, x) \not\models (\Box\chi)^*$, то существует мир $y \in W$ такой, что xRy, $(\mathfrak{M}, y) \models p_{n+1}$ и $(\mathfrak{M}, y) \not\models \chi^*$. По индукционному предположению, $(\mathfrak{F}_\beta, y) \not\models \chi_\beta$. С другой стороны, т. к. $(\mathfrak{M}, y) \models p_{n+1}$, получаем, что $yR_\beta a_{n+1}^0$, откуда следует, что $(\mathfrak{F}_\beta, y) \models \beta_{n+1}$. Значит, $(\mathfrak{F}_\beta, y) \not\models \beta_{n+1} \to \chi_\beta$, и следовательно, $(\mathfrak{F}_\beta, x) \not\models \Box(\beta_{n+1} \to \chi_\beta)$, т. е. $(\mathfrak{F}_\beta, x) \not\models \psi_\beta$.

Пусть теперь $(\mathfrak{F}_\beta, x) \not\models \psi_\beta$. Тогда существует мир $y \in W_\beta$ такой, что $xR_\beta y$, $(\mathfrak{F}_\beta, y) \models \beta_{n+1}$ и $(\mathfrak{F}_\beta, y) \not\models \chi_\beta$. Нетрудно убедиться, что β_{n+1} опровергается в каждом мире каждой из шкал $\mathfrak{F}_1, \ldots \mathfrak{F}_{n+1}$, откуда несложно заключить, что $y \in W$. Следовательно, по индукционному предположению, $(\mathfrak{M}, y) \not\models \chi^*$. Учитывая, что $\mathfrak{M} \models p_{n+1}$, получаем, что $(\mathfrak{M}, y) \not\models p_{n+1} \to \chi^*$, а значит, $(\mathfrak{M}, y) \not\models \Box(p_{n+1} \to \chi^*)$, т. е. $(\mathfrak{M}, y) \not\models \psi^*$.

Случай, когда $\psi = \Box^*\chi$, рассматривается аналогично.

Теперь вернёмся к формуле $\varphi^\#$. Из того, что $(\mathfrak{M}, x_0) \not\models \varphi^\#$, следует, что $(\mathfrak{M}, x_0) \models p_{n+1} \wedge \Box^*(\neg p_{n+1} \to \Box^*\neg p_{n+1})$ и $(\mathfrak{M}, x_0) \not\models \varphi^*$. Последнее, с учётом доказанного выше, даёт, что $(\mathfrak{F}_\beta, x_0) \not\models \varphi_\beta$. Кроме того, нетрудно видеть, что $(\mathfrak{F}_\beta, x_0) \models \beta_{n+1} \wedge \Box^*(\neg\beta_{n+1} \to \Box^*\neg\beta_{n+1})$, а значит, $(\mathfrak{F}_\beta, x_0) \not\models \varphi_\beta^\#$. Следовательно, $\varphi_\beta^\# \notin \mathbf{K}^*$. ❑

Для завершения доказательства теоремы 1 осталось заметить, что формула $\varphi_\beta^\#$ строится по формуле φ полиномиально. ❑

Некоторые следствия. Приведём несколько следствий теоремы 1, а также конструкции, используемой в доказательстве теоремы 1.

Следствие 7. *Проблема разрешения для* **PDL**(0) *является* EXPTIME*-полной.*

Доказательство. Достаточно проинтерпретировать в языке **PDL** модальность $\Box$ как $[\alpha]$, а модальность $\Box^*$ — как $[\alpha^*]$, где α — некоторая элементарная программа. ❑

Логика $\mathbf{K}^*$ погружается не только в **PDL**, но и в другие логики. В качестве примера рассмотрим логики знания с оператором всеобщего знания. Это логики с n однотипными независимыми модальностями $K_1, \ldots, K_n$ (рассматриваемыми как операторы знания в системе с n агентами знания), а также с модальностью C (оператором всеобщего знания), которой на шкалах Крипке соответствует транзитивное замыкание объединения отношений достижимости, соответствующих модальностям $K_1, \ldots, K_n$; подробнее см., например, [10].

Следствие 8. *Проблема разрешения для* $\mathbf{K}_n^C(0)$ *при* $n \geqslant 1$ *и для* $\mathbf{K4}_n^C(0)$ *при* $n \geqslant 2$ *является* EXPTIME*-полной.*

Отметим, что логика $\mathbf{K4}_1^C$ эквивалентна мономодальной логике **K4** в том смысле, что $K_1\varphi \leftrightarrow C\varphi \in \mathbf{K4}_1^C$. Это, в частности, означает, что проблема разрешения для константного фрагмента $\mathbf{K4}_1^C$ является PSPACE-полной [4].

Что касается модальных логик, содержащих формулу $\Diamond\top$ (для каждой модальности типа $\Diamond$ в случае полимодальных логик), то несложно понять, что их константные фрагменты полиномиально разрешимы, т. к. наличие этой формулы в логике позволяет «стирать» модальности $\Box$ и $\Diamond$ в константных формулах. Тем не менее, для многих логик описанную конструкцию можно провести, используя формулы от одной переменной, например, предложенные в [4] для обоснования PSPACE-трудности проблемы разрешения фрагментов $\mathbf{T}(1)$, $\mathbf{S4}(1)$, $\mathbf{Grz}(1)$ и некоторых других логик (применительно к описанной выше конструкции, нужно взять отрицания соответствующих формул из [4]). В результате получаем ещё одно следствие.

Следствие 9. *Проблема разрешения для* $\mathbf{T}_n^C(1)$ *при* $n \geqslant 1$ *и для* $\mathbf{S4}_n^C(1)$ *при* $n \geqslant 2$ *является* EXPTIME*-полной.*

Отметим, что ситуация с $\mathbf{S4}_1^C$ аналогична ситуации с $\mathbf{K4}_1^C$: логика $\mathbf{S4}_1^C$ эквивалентна логике **S4** в том смысле, что $K_1\varphi \leftrightarrow C\varphi \in \mathbf{S4}_1^C$, откуда следует, что проблема разрешения для $\mathbf{S4}_1^C(1)$ является PSPACE-полной [4].

3. Сложность контрмоделей. Обычно наблюдается связь между сложностью (в смысле трудности в классах сложности типа NP, PSPACE, EXPTIME) неклассических логик и сложностью контрмоделей для непринадлежащих этим логикам формул. Следуя [5], для пропозициональной логики (множества формул) L определим следующую функцию $f_L(n)$:

$$f_L(n) = \max_{\substack{|\varphi| \leqslant n \\ \varphi \notin L}} \min_{\substack{\mathfrak{F} \models L \\ \mathfrak{F} \not\models \varphi}} |\mathfrak{F}|,$$

где $|\mathfrak{F}|$ — мощность множества миров шкалы $\mathfrak{F}$, а $|\varphi|$ — длина формулы φ. Функцию $f_L(n)$ будем называть функцией сложности логики (множества формул) L.

Функция сложности для L позволяет оценить сложность проблемы разрешения L. Так, она даёт возможность получить верхние границы некоторых вычислительных ресурсов (например, временны́х), затрачиваемых алгоритмами, разрешающими L путём поиска контрмоделей для тестируемых формул.

Как правило, функция сложности $f_L(n)$ полиномиальна в случае, когда L имеет NP-полную проблему разрешения, и экспоненциальна в случае, когда проблема разрешения L является PSPACE-полной. Функция сложности остаётся экспоненциальной и для PSPACE-полных фрагментов вида $L(n)$, см. [4, 15]. Поскольку фрагменты $\mathbf{K}^*(0)$, $\mathbf{PDL}(0)$, $\mathbf{K}_n^C(0)$, $\mathbf{K4}_n^C(1)$, $\mathbf{T}_n^C(1)$, $\mathbf{S4}_n^C(1)$ содержат PSPACE-полные фрагменты — в зависимости от логики это $\mathbf{K}(0)$, $\mathbf{K4}(0)$, $\mathbf{T}(1)$ или $\mathbf{S4}(1)$, — то ввиду [4] справедливо следующее утверждение.

Следствие 10. *Функция сложности для* $\mathbf{K}^*(0)$, $\mathbf{PDL}(0)$, $\mathbf{K}_n^C(0)$, $\mathbf{K4}_n^C(1)$, $\mathbf{T}_n^C(1)$, $\mathbf{S4}_n^C(1)$, *где* $n \geqslant 1$, *ограничена снизу экспонентой.*

На самом деле функцию сложности для подобных фрагментов можно ограничить экспонентой не только снизу, но и сверху, см., например, [10]. Тем не менее, даже при, казалось бы, одинаковых ограничениях на функцию сложности проблема разрешения для логик типа **K**, **T**, **K4**, **S4** и др. является PSPACE-полной, а для логик типа $\mathbf{K}^*$, $\mathbf{K}_n^C$ и др. — EXPTIME-полной. Принимая во внимание то, что функция сложности $f_L(n)$ позволяет оценить границы вычислительных ресурсов, затрачиваемых алгоритмами, разрешающими L, мы приходим к вопросу о различии контрмоделей в случае PSPACE-полных и EXPTIME-полных логик. Это различие известно: хотя мощность контрмоделей в обоих случаях может быть «почти одинаковой» — экспоненциальной, — тем не менее, в случае PSPACE-полных логик, вроде **K**, **T**, **K4**, **S4**, высота[3] контрмоделей для формулы φ может быть ограничена сверху линейной функцией от модальной глубины[4] φ, в то время как высота контрмоделей для φ в случае логик, вроде $\mathbf{K}^*$, **PDL**, $\mathbf{K}_n^C$, может быть ограничена снизу экспонентой.

Действительно, рассмотрим следующие формулы от пропозициональных переменных $p_1, \ldots, p_n$, см. [3]:

$$
\begin{aligned}
A_n^0 &= \neg p_1 \to \Big[\Box p_1 \wedge \bigwedge_{i=2}^{n} ((p_i \to \Box p_i) \wedge (\neg p_i \to \Box \neg p_i))\Big];\\
A_n^k &= \neg p_{k+1} \wedge \bigwedge_{i=1}^{k} p_k \to \\
&\qquad \to \Big[\Box(p_{k+1} \wedge \bigwedge_{i=1}^{k} \neg p_k) \wedge \bigwedge_{i=k+2}^{n} ((p_i \to \Box p_i) \wedge (\neg p_i \to \Box \neg p_i))\Big],
\end{aligned}
$$

где $k \in \{1, \ldots, n-1\}$.

Поясним «устройство» формул A_n^i. Если смотреть на набор значений переменных $p_n, \ldots, p_1$ как на двоичное число (где p_i соответствует цифре «1», а $\neg p_i$ — цифре «0»), то каждую формулу A_n^i можно понимать как описание операции прибавления единицы к двоичному числу, заканчивающемуся на i единиц, перед которыми стоит ноль. Результат этой операции будет описываться набором значений переменных $p_n, \ldots, p_1$ в мире, достижимом из мира, в котором истинна форму-

[3] Т. е. максимальная длина цепей, состоящих из попарно различных миров.

[4] Модальная глубина формулы — это максимальное число «вложенных» модальностей. Более точно, модальная глубина безмодальных формул равна 0, модальная глубина для конъюнкции, дизъюнкции и импликации формул определяется как максимум модальной глубины соединяемых формул, а навешивание на формулу модальности увеличивает модальную глубину на 1.

ла A_n^i. Несложно убедиться, что в этом случае формула

$$\varphi_n \;=\; \neg\Big(\bigwedge_{i=1}^{n}\neg p_i \;\wedge\; \Box^*\Diamond\top \;\wedge\; \Box^*\bigwedge_{i=1}^{n-1} A_n^i\Big)$$

требует для своего опровержения модели, число миров в которой не менее, чем 2^n, в то время как длина формул φ_n ограничена сверху полиномом (второй степени) от n.

Возможна ли аналогичная конструкция в случае $\mathbf{K}^*(n)$? Да, причём уже при $n = 0$: достаточно рассмотреть формулы $(\varphi_n)^{\#}_{\beta}$. Несложно понять, что формулы, подобные φ_n, можно построить и для других упомянутых выше EXPTIME-полных логик. В результате получаем ещё одно следствие приведённой конструкции.

Следствие 11. *Пусть L — один из следующих фрагментов: $\mathbf{K}^*(0)$, $\mathbf{PDL}(0)$, $\mathbf{K}_n^C(0)$, $\mathbf{K4}_{n+1}^C(0)$, $\mathbf{T}_n^C(1)$, $\mathbf{S4}_{n+1}^C(1)$, где $n \geqslant 1$. Тогда для всякого натурального числа k в языке фрагмента L существует формула φ_k, не принадлежащая L и требующая для своего опровержения модели Крипке, содержащей цепь из не менее чем 2^k различных миров, при этом длина формул φ_k ограничена сверху некоторым полиномом от k.*

Список литературы

[1] М. Гэри, Д. Джонсон. Вычислительные машины и труднорешаемые задачи. М., Мир, 1982.

[2] Л. Стокмейер. Классификация вычислительной сложности проблем. Кибернетический сборник, вып. 26, 1989, с. 20–83.

[3] P. Blackburn, M. de Rijke, Y. Venema. Modal Logic. Cambridge University Press, 2001.

[4] A. V. Chagrov, M. N. Rybakov. How many variables one needs to prove PSPACE-hardness of modal logics? Advances in Modal Logic, vol. 4, 2003, p. 71–81.

[5] A. V. Chagrov, M. V. Zakharyaschev. Modal Logic. Oxford University Press, 1997.

[6] S. A. Cook. The complexity of theorem-proving procedures. In Proceedings of the Third Annual ACM Symposium on the Theory of Computation, 1971, p. 151–158.

[7] M. J. Fisher, R E. Ladner. Propositional dynamic logic of regular programs. J. Comput. Syst. Sci., vol. 18, No. 2, 1979, p. 194–211.

[8] M. R. Garey, D. S. Johnson. Computers and Intractability, A Guide to the Theory of NP-completeness. San Francisco, 1979.

[9] J. Y. Halpern. The effect of bounding the number of primitive propositions and the depth of nesting on the complexity of modal logic. Artificial Intelligence, vol. 75, No. 2, 1995, p. 361–372.

[10] J. Y. Halpern, Y. Moses. A guide to completeness and complexity for modal logics of knowledge and belief. Artificial Intelligence, vol. 54, 1992, p. 319–379.

[11] N. Immerman. Descriptive Complexity. Springer, 1999.

[12] R. E. Ladner. The computational complexity of provability in systems of modal logic. SIAM Journal on Computing, vol. 6, 1997, p. 467–480.

[13] I. Nishimura. On formulas of the one variable in intuitionistic propositional calculus. The Journal of Symbolic Logic, vol. 25, 1960, p. 327–331.

[14] C. H. Papadimitriou. Computational Complexity. Addison–Wesley Publishing Company, 1995.

[15] M. N. Rybakov. Complexity of intuitionistic and visser's basic and formal logic in finitely many variables. Advances in Modal Logic, vol. 6, 2006, p. 393–411.

[16] E. Spaan. Complexity of Modal Logics. PhD thesis, University of Amsterdam, Department of Mathematics and Computer Science, 1993.

[17] R. Statman. Intuitionistic propositional logic is polynomial-space complete. Theoret. Comput. Sci., vol. 9, No. 1, 1979, p. 67–72.

[18] L. Stockmeyer. Classifying the computational complexity of problems. The Journal of Symbolic Logic, vol. 52, No. 1, 1987, p. 1–43.

[19] V. Švejdar. The decision problem of provability logic with only one atom. Arch. Math. Logic, 2003, p. 1–6.

[20] M. Zakharyaschev, F. Wolter, A. Chagrov. Advanced modal logic. In D. M. Gabbay and F. Guenthner, editors, Handbook of Philosophical Logic, vol. 3, p. 83–266. Kluwer Academic Publishers, 2nd edition, 2001.