УДК 512.572, 510.52, 510.643

СЛОЖНОСТЬ ПРОБЛЕМЫ РАВЕНСТВА СЛОВ В МНОГООБРАЗИЯХ МОДАЛЬНЫХ АЛГЕБР

Рыбаков М.Н.[*,**,***]
[*]ИППИ имени А.А. Харкевича РАН, г. Москва
[**]НИУ ВШЭ, г. Москва
[***]Тверской государственный университет, г. Тверь

Поступила в редакцию 04.08.2021, после переработки 17.08.2021.

Приводится доказательство PSPACE-полноты проблемы равенства слов в классе всех нуль-порождённых модальных алгебр, или, эквивалентно, проблемы равенства константных слов в классе всех модальных алгебр. Также рассматривается вопрос о сложности равенства слов в произвольном многообразии модальных алгебр. Доказывается, что уже проблема равенства константных слов в многообразии модальных алгебр может быть сколь угодно трудной (включая как классы сложности, так и степени неразрешимости). Показано, как построить соответствующие многообразия.

Ключевые слова: модальная алгебра, равенство слов, вычислительная сложность.

Вестник ТвГУ. Серия: Прикладная математика. 2021. № 3. С. 5–17.
https://doi.org/10.26456/vtpmk619

Введение

Проблема равенства слов состоит в следующем: пусть имеется сигнатура Σ, состоящая из конечноместных функциональных знаков, множество свободных образующих V, класс алгебр $\mathscr{C}$ сигнатуры Σ; требуется по любой паре термов, построенных из образующих множества V с помощью функциональных знаков из Σ выяснить, справедливо ли равенство этих термов в каждой алгебре из $\mathscr{C}$. То есть, под словами понимаются термы в некоторой сигнатуре, а под равенством слов — равенство значений этих слов как термов при любой возможной оценке в любой из алгебр некоторого класса.

Известно, что эта проблема может быть очень трудной уже, казалось бы, в простой ситуации. Так, А. Туэ поставил проблему равенства слов в ассоциативных алгебрах [18], которая, как было доказано независимо А. А. Марковым и Э. Л. Постом, оказалась алгоритмически неразрешимой [3, 11]; позже были найдены и другие примеры неразрешимых проблем равенства слов, в частности, в группах и полугруппах [1].

Мы будем рассматривать проблему равенства слов в различных многообразиях модальных алгебр, и акцент будет сделан на равенстве константных слов, или, эквивалентно, на равенстве произвольных слов в нуль-порождённых модальных алгебрах.

Известно, что для многообразия всех модальных алгебр проблема равенства слов разрешима и, как следует из результатов Р. Ладнера [9], является PSPACE-полной (по вопросам вычислительной сложности см. [10]). Фактически Р. Ладнер доказал PSPACE-полноту других проблем — проблем выводимости формул в модальных системах **K**, **T** и **S4**; но проблема выводимости формул в **K** эквивалентна[1] проблеме равенства термов в многообразии всех модальных алгебр. В предложенном доказательстве существенно использовался тот факт, что в языке имеется бесконечно много переменных. Позже было показано [8, 17], что можно обойтись одной переменной, а ещё позже — что только константными формулами [6]. Из последнего результата следует, что проблема равенства константных термов в классе всех модальных алгебр и проблема равенства произвольных термов в классе нуль-порождённых модальных алгебр являются PSPACE-полными, и здесь будет приведено короткое алгебраическое доказательство этого факта.

Другой вопрос, который будет здесь рассмотрен, — это вопрос о том, насколько сложной в принципе может оказаться проблема равенства константных термов в многообразиях модальных алгебр. Используя идеи, изложенные в [5, 15, 17], покажем, что эта проблема может быть сколь угодно сложной, более того, может иметь сколь угодно высокую степень неразрешимости. Этот факт будет справедлив даже при условии, что любое выполнимое (опровержимое) в соответствующем многообразии равенство слов выполнимо (опровержимо) и в некоторой конечной алгебре из этого многообразия, число элементов которой не превосходит экспоненты от суммы длин этих слов.

Работа устроена следующим образом. В разделе 1 приводятся основные понятия, связанные с модальными алгебрами, в разделе 2 описываются реляционные представления модальных алгебр, известные как шкалы Крипке, в разделе 3 описаны основные понятия, связанные с классами сложности и степенями неразрешимости. Раздел 4 содержит техническую конструкцию, которая является ключевой для получения результатов, представленных в работе. В разделе 5 приводится доказательство PSPACE-полноты проблемы равенства константных термов в классе всех модальных алгебр и проблемы равенства произвольных термов в классе нуль-порождённых модальных алгебр. Раздел 6 содержит описание способа построения многообразий модальных алгебр с проблемой равенства константных термов любой заранее заданной сложности. Заключение содержит некоторые комментарии к представленным здесь результатам.

1. Модальные алгебры

Пусть $\boldsymbol{B} = \langle B, \wedge, \vee, \neg, \bot, \top \rangle$ — алгебра с бинарными операциями $\wedge$ и $\vee$, унарной операцией $\neg$, выделенными элементами $\bot$ и $\top$. Алгебра $\boldsymbol{B}$ называется *булевой*,

[1] Причём алгоритмы, сводящие эти проблемы друг к другу, линейны по затратам времени.

если для всяких $a, b, c \in B$

$$\begin{array}{rcl@{\qquad}rcl} a \wedge b & = & b \wedge a; & a \vee b & = & b \vee a; \\ a \wedge (b \wedge c) & = & (a \wedge b) \wedge c; & a \vee (b \vee c) & = & (a \vee b) \vee c; \\ (a \wedge b) \vee b & = & b; & (a \vee b) \wedge b & = & b; \\ a \wedge (b \vee c) & = & (a \vee b) \wedge (a \vee c); & a \vee (b \wedge c) & = & (a \wedge b) \vee (a \wedge c); \\ a \wedge \neg a & = & \bot; & a \vee \neg a & = & \top. \end{array}$$

Алгебра $\boldsymbol{A} = \langle A, \wedge, \vee, \neg, \bot, \top, \Box \rangle$ называется *модальной*, если $\langle A, \wedge, \vee, \neg, \bot, \top \rangle$ — булева алгебра, а $\Box$ — унарная операция на A, причём для всяких $a, b \in A$

$$\begin{array}{rcl} \Box(a \wedge b) & = & \Box a \wedge \Box a; \\ \Box\top & = & \top. \end{array}$$

Пусть V — счётное множество переменных; *термом* называем выражение, построенное стандартным способом из переменных множества V и констант $\bot$ и $\top$ с помощью знаков $\wedge$, $\vee$, $\neg$ и $\Box$.

Пусть v — функция, которая каждой переменной $x \in V$ сопоставляет элемент $v(x) \in A$. Расширим v на множество всех термов:

$$\begin{array}{rcl} v(t \wedge s) & = & v(t) \wedge v(s); \\ v(t \vee s) & = & v(t) \vee v(s); \\ v(\neg t) & = & \neg v(t); \\ v(\bot) & = & \bot; \\ v(\top) & = & \top; \\ v(\Box t) & = & \Box v(t). \end{array}$$

Функцию v будем называть *оценкой* термов в алгебре $\boldsymbol{A} = \langle A, \wedge, \vee, \neg, \bot, \top, \Box \rangle$, а элемент $v(t)$ — *значением терма* t в $\boldsymbol{A}$ при оценке v.

Говорим, что в $\boldsymbol{A}$ истинно равенство термов $t = s$ при оценке v, если $v(t) = v(s)$; этот факт обозначаем как $\boldsymbol{A} \models^v t = s$. Говорим, что в $\boldsymbol{A}$ истинно равенство термов $t = s$, если $\boldsymbol{A} \models^v t = s$ для любой оценки v в $\boldsymbol{A}$; этот факт обозначаем как $\boldsymbol{A} \models t = s$. Говорим, что равенство $t = s$ истинно в классе классе $\mathscr{C}$ алгебр, если оно истинно в каждой алгебре класса $\mathscr{C}$; в этом случае пишем $\mathscr{C} \models t = s$.

Введём сокращения для записи термов: если t, s — термы, то $t \to s = \neg t \vee s$, $t \leftrightarrow s = (t \to s) \wedge (s \to t)$; $\Diamond t = \neg\Box\neg t$. Эти сокращения естественным образом определяют операции $\neg$, $\leftrightarrow$ и $\Diamond$ на A.

2. Реляционные представления модальных алгебр

По техническим причинам нам понадобятся реляционные представления модальных алгебр. Приведём необходимые определения и факты.

Пара $\mathfrak{F} = \langle W, R \rangle$ называется *шкалой Крипке*, если $W \neq \varnothing$ и R — бинарное отношение на W; элементы множества W называют *мирами* шкалы $\mathfrak{F}$, а отношение R — *отношением достижимости*. Если миры w и w' находятся в отношении R, то пишут $\langle w, w' \rangle \in R$ или wRw' и говорят, что w' *достижим* из w. Для каждого $w \in W$ определим множество $R(w)$ миров, достижимых из w, положив $R(w) = \{w' \in W : wRw'\}$.

На шкалу Крипке $\mathfrak{F} = \langle W, R\rangle$ можно смотреть как на ориентированный граф с множеством вершин W и множеством дуг R.

Пусть $\mathfrak{F} = \langle W, R\rangle$ — шкала Крипке; сопоставим шкале $\mathfrak{F}$ модальную алгебру $\mathfrak{F}^+ = \langle \mathscr{P}(W), \cap, \cup, \bar{\cdot}, \varnothing, W, \Box\rangle$, где

$$\begin{array}{lcl} \mathscr{P}(W) & = & \{X : X \subseteq W\}; \\ \Box X & = & \{w \in W : R(w) \subseteq X\}, \end{array}$$

а $\cap$, $\cup$, $\bar{\cdot}$ — обычные теоретико-множественные операции пересечения, объединения и дополнения на $\mathscr{P}(W)$.

Оценкой в шкале Крипке $\mathfrak{F}$ называется оценка в модальной алгебре $\mathfrak{F}^+$.

Равенство термов $t = s$ считаем истинным в шкале Крипке $\mathfrak{F}$, если $\mathfrak{F}^+ \models t = s$; равенство $t = s$ считаем истинным в классе $\mathscr{C}$ шкал Крипке, если $t = s$ истинно в каждой шкале Крипке из класса $\mathscr{C}$.

Если v — оценка в шкале Крипке $\mathfrak{F} = \langle W, R\rangle$, то нетрудно проверить, что для неё справедливы следующие свойства:

$$\begin{array}{lcl} w \in v(\Box s) & \iff & \forall w'\ (w' \in R(w) \Rightarrow w' \in v(s)); \\ w \in v(\Diamond s) & \iff & \exists w'\ (w' \in R(w)\ \&\ w' \in v(s)). \end{array} \qquad (*)$$

Отметим, что для каждой конечной модальной алгебры $\boldsymbol{A}$ существует представляющая её шкала Крипке $\mathfrak{F}$, т.е. такая, что $\mathfrak{F}^+ = \boldsymbol{A}$, см. [7, раздел 7.5], откуда, в частности, следует, что равенство термов истинно в классе всех модальных алгебр тогда и только тогда, когда оно истинно в классе всех шкал Крипке.

3. Классы сложности и степени неразрешимости

Нам понадобятся понятия, связанные со сложностью задач и двумя видами сводимости одних задач к другим.

Под *задачей* понимаем множество слов в некотором конечном алфавите. Пусть X и Y — задачи в алфавитах $\mathcal{A}$ и $\mathcal{B}$ соответственно. Говорим, что функция $f\colon \mathcal{A}^* \to \mathcal{B}^*$ *сводит* задачу X к задаче Y, если для каждого слова $x \in \mathcal{A}^*$

$$x \in X \iff f(x) \in Y;$$

функцию $f\colon \mathcal{A}^* \to \mathcal{B}^*$ в этом случае называем *сводящей*. Задача X называется *полиномиально сводимой* к задаче Y, если существует полиномиально вычислимая (по затратам времени) функция, сводящая X к Y, и задача X называется *m-сводимой*[2] к задаче Y, если существует вычислимая функция, сводящая X к Y; пишем $X \leqslant_{\mathrm{p}} Y$ и $X \leqslant_{\mathrm{m}} Y$, соответственно.

Под *классом сложности* понимаем любой класс S разрешимых задач, замкнутый относительно полиномиальной сводимости[3] (т.е. если $X \in S$ и $Y \leqslant_{\mathrm{p}} X$, то $Y \in S$), а под *степенью неразрешимости* понимаем любой класс S неразрешимых задач, замкнутый относительно m-сводимости (т.е. если $X \in S$ и $Y \leqslant_{\mathrm{m}} X$, то $Y \in S$). Для класса сложности S задачу X называем *S-полной*, если $X \in S$ и

[2] Буква «m» — от английского «many-one reducible».

[3] Вообще говоря, это довольно грубое условие, но для целей работы такое допущение приемлемо.

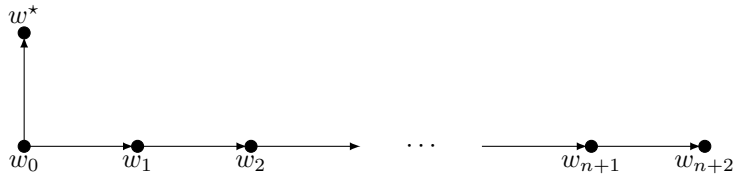

Рис. 1: Шкала Крипке $\mathfrak{F}_n$

любая задача Y из S полиномиально сводима к X; для степени неразрешимости S задачу X называем *S-полной*, если $X \in S$ и любая задача Y из S m-сводима к X.

В контексте задач и классов задач натуральные числа отождествляем с их двоичными записями. Отметим, что символы любого конечно алфавита можно полиномиально закодировать двоичными записями натуральных чисел, поэтому можно, не теряя общности, ограничиться рассмотрением задач, определяемых множествами натуральных чисел.

Более детальную информацию о классах сложности читатель может найти в [10], а по степеням неразрешимости — в [16].

4. Основная техническая конструкция

Введём следующие сокращения: $\Diamond^0 t = t$, $\Diamond^{n+1} t = \Diamond\Diamond^n t$, где $n \in \mathbb{N}$. Пусть для каждого $n \in \mathbb{N}^+$

$$a_n = \Diamond\Box\bot \wedge \Diamond^{n+2}\Box\bot, \quad b_n = \Diamond a_n. \tag{$**$}$$

Заметим, что термы a_n и b_n являются константными, и их значения в модальной алгебре никак не зависят от оценки.

Нам будут важны некоторые свойства этих термов, и чтобы их показать, определим специальные шкалы Крипке. Пусть для каждого $n \in \mathbb{N}^+$

$$\begin{array}{lcl} W_n & = & \{w^\star, w_0, w_1, \ldots, w_{n+2}\}; \\ R_n & = & \{\langle w_i, w_{i+1}\rangle : i \in \{0, 1, \ldots, n+1\}\} \cup \{\langle w_0, w^\star\rangle\}; \\ \mathfrak{F}_n & = & \langle W_n, R_n\rangle. \end{array}$$

Шкала $\mathfrak{F}_n$ представлена в виде графа на рис. 1: миры изображены в виде закрашенных кружков, а отношению достижимости соответствуют стрелки между ними.

Следующее утверждение носит технический характер, но оно будет ключевым для всех дальнейших построений.

Лемма 1. *Пусть $k, m \in \mathbb{N}^+$ и v — произвольная оценка в $\mathfrak{F}_m$. Тогда для всякого мира w шкалы $\mathfrak{F}_m$ справедлива следующая эквивалентность:*

$$w \in v(a_k) \iff w = w_0 \text{ и } k = m.$$

Доказательство. Воспользуемся эквивалентностями $(*)$. Согласно определению оценки в шкалах Крипке, $v(\bot) = \varnothing$, поэтому, по $(*)$, $v(\Box\bot) = \{w^\star, w_{m+2}\}$, откуда, снова по $(*)$, получаем, что $v(\Diamond\Box\bot) = \{w_0, w_{m+1}\}$ и

$$v(\Diamond^{k+2}\Box\bot) = \begin{cases} \{w_{m-k}\}, & \text{если } m \geqslant k; \\ \varnothing, & \text{если } m < k. \end{cases}$$

Но тогда

$$v(a_n) \;=\; v(\Diamond\Box\bot) \cap v(\Diamond^{k+2}\Box\bot) \;=\; \begin{cases} \{w_0\}, & \text{если } m = k; \\ \varnothing, & \text{если } m \neq k, \end{cases}$$

что и даёт справедливость доказываемого утверждения. □

5. Равенство константных слов в классе всех алгебр

Пусть $\boldsymbol{A} = \langle A, \wedge, \vee, \neg, \bot, \top, \Box\rangle$ — модальная алгебра и $X \subseteq A$. Наименьшая подалгебра алгебры $\boldsymbol{A}$, содержащая все элементы множества X, называется *подалгеброй* алгебры $\boldsymbol{A}$, *порождённой множеством* X; в этом случае X называется множеством, *порождающим* эту подалгебру. Алгебра $\boldsymbol{A}$ называется *n-порождённой*, где $n \in \mathbb{N}$, если существует n-элементное множество X, порождающее алгебру $\boldsymbol{A}$; в частности, если $X = \varnothing$, то $\boldsymbol{A}$ называется 0-порождённой алгеброй.

Пусть t — некоторый терм, $x_1, \ldots, x_n$ — список всех переменных, входящих в t, и x — некоторая переменная. Определим рекурсивно *x-релятивизацию* $\rho_x t$ терма t:

$$\begin{array}{lcll} \rho_x s & = & s, & \text{если } s \in \{\bot, \top, x_1, \ldots, x_n\}; \\ \rho_x(s \wedge s') & = & \rho_x s \wedge \rho_x s'; & \\ \rho_x(s \vee s') & = & \rho_x s \vee \rho_x s'; & \\ \rho_x \neg s & = & \neg \rho_x s; & \\ \rho_x \Box s & = & \Box(x \to \rho_x s). & \end{array}$$

Пусть $\mathscr{C}_{all}$ — класс всех модальных алгебр.

Лемма 2. *Пусть x — переменная, не входящая ни в терм t, ни в терм s. Тогда*

$$\mathscr{C}_{all} \models t = s \iff \mathscr{C}_{all} \models \rho_x t = \rho_x s.$$

Доказательство. Пусть $x_1, \ldots, x_n$ — список всех переменных, каждая из которых входит в t или в s.

($\Rightarrow$) Пусть $\mathscr{C}_{all} \not\models \rho_x t = \rho_x s$. Тогда существует шкала Крипке $\mathfrak{F} = \langle W, R\rangle$ и оценка v в этой шкале, для которых $\mathfrak{F}^+ \not\models^v \rho_x t = \rho_x s$. В этом случае существует $u \in (v(\rho_x t) \setminus v(\rho_x s)) \cup (v(\rho_x s) \setminus v(\rho_x t))$.

Пусть $W' = v(x) \cup \{u\}$ и $\boldsymbol{A} = \langle \mathscr{P}(W'), \cap, \cup, \overline{\cdot}, \varnothing, W', \Box\rangle$ — подалгебра алгебры $\mathfrak{F}^+$. Пусть v' — оценка в алгебре $\boldsymbol{A}$, определяемая следующим условием: $v'(x_i) = v(x_i) \cap W'$ для каждого $i \in \{1, \ldots, n\}$. Индукцией по сложности терма r, не содержащего переменных, отличных от $x_1, \ldots, x_n$, несложно показать, что для всякого $w \in W'$

$$w \in v'(r) \iff w \in v(\rho_x r).$$

Но тогда $u \in (v'(t) \setminus v'(s)) \cup (v'(s) \setminus v'(t))$, а значит, $\mathscr{C}_{all} \not\models t = s$.

($\Leftarrow$) Пусть $\mathscr{C}_{all} \not\models t = s$. Тогда существует шкала Крипке $\mathfrak{F} = \langle W, R\rangle$ и оценка v в этой шкале, для которых $\mathfrak{F}^+ \not\models^v t = s$. Рассмотрим оценку v', при которой $v'(x_i) = v(x_i)$ для каждого $i \in \{1, \ldots, n\}$ и $v'(x) = W$; такая оценка существует,

поскольку $x \notin \{x_1, \ldots, x_n\}$. Тогда $\mathfrak{F}^+ \models^{v'} x = \top$. Осталось заметить, что равенство $\top \to r = r$ справедливо в любой модальной алгебре для любого терма r, откуда получаем, что $\mathfrak{F}^+ \models^{v'} r = \rho_x r$, а значит, $\mathfrak{F}^+ \not\models^{v'} \rho_x t = \rho_x s$, и поэтому $\mathscr{C}_{all} \not\models \rho_x t = \rho_x s$. □

Замечание 1. *Из приведённого доказательства следует, что если* $\mathscr{C}_{all} \not\models t = s$, *то существуют такие шкала Крипке* $\mathfrak{F} = \langle W, R\rangle$ *и оценка* v *в* $\mathfrak{F}$, *что* $v(x) = W$ *и* $v(\rho_x t) \neq v(\rho_x s)$.

Для дальнейших построений зафиксируем термы t и s. Пусть $x_1, \ldots, x_n$ — список всех переменных, каждая из которых входит в t или s. Для каждого терма r, не содержащего переменных, отличных от $x_1, \ldots, x_n$, через r^* обозначим терм, получающийся из $\rho_{x_{n+1}} r$ подстановкой термов $b_1, \ldots, b_{n+1}$ (см. (∗∗)) вместо переменных $x_1, \ldots, x_{n+1}$ соответственно.

Лемма 3. $\mathscr{C}_{all} \models \rho_{x_{n+1}} t = \rho_{x_{n+1}} s \iff \mathscr{C}_{all} \models t^* = s^*$.

Доказательство. ($\Rightarrow$) Пусть $\mathscr{C}_{all} \not\models t^* = s^*$. Тогда равенство $t^* = s^*$ опровергается в некоторой модальной алгебре $\boldsymbol{A}$ при некоторой оценке v. Достаточно взять такую оценку v', что $v'(x_i) = v(b_i)$ для каждого $i \in \{1, \ldots, n+1\}$, и тогда должно быть ясно, что $\boldsymbol{A} \not\models^{v'} \rho_{x_{n+1}} t = \rho_{x_{n+1}} s$.

($\Leftarrow$) Пусть $\mathscr{C}_{all} \not\models \rho_{x_{n+1}} t = \rho_{x_{n+1}} s$. Тогда, согласно замечанию 1, существуют такие шкала Крипке $\mathfrak{F} = \langle W, R\rangle$ и оценка v в шкале $\mathfrak{F}$, что $v(x_{n+1}) = W$ и $v(\rho_{x_{n+1}} t) \neq v(\rho_{x_{n+1}} s)$. Последнее условие означает, что существует $u \in (v(\rho_{x_{n+1}} t) \setminus v(\rho_{x_{n+1}} s)) \cup (v(\rho_{x_{n+1}} s) \setminus v(\rho_{x_{n+1}} t))$.

Переобозначим элементы шкал Крипке $\mathfrak{F}_1, \ldots, \mathfrak{F}_{n+1}$ так, чтобы никакой из них не был сразу в двух шкалах из этого списка: вместо элементов $w^\star, w_0, \ldots, w_{k+2}$ множества W_k возьмём элементы $w_k^\star, w_0^k, \ldots, w_{k+2}^k$, соответственно, и вместо шкалы $\mathfrak{F}_k$ будем рассматривать изоморфную ей шкалу $\mathfrak{F}' = \langle W'_k, R'_k\rangle$, где $W'_k = \{w_k^\star, w_0^k, \ldots, w_{k+2}^k\}$, а R'_k получается из R_k с помощью того же переобозначения. Будем также считать, что $W \cap W'_k = \varnothing$ для каждого $k \in \{1, \ldots, n+1\}$.

Пусть теперь

$$\begin{array}{lcl} W^* & = & W \cup W'_1 \cup \ldots \cup W'_{n+1}; \\ R^* & = & R \cup R'_1 \cup \ldots \cup R'_{n+1} \cup \{\langle w, w_0^k, \rangle : k \in \{1, \ldots, n+1\} \ \&\ w \in v(x_k)\}; \\ \mathfrak{F}^* & = & \langle W^*, R^*\rangle. \end{array}$$

По построению шкалы Крипке $\mathfrak{F}^*$, с учётом леммы 1, справедливо следующее: для любого $k \in \{1, \ldots, n+1\}$ и любой оценки v' в $\mathfrak{F}^*$ выполняется равенство $v'(b_k) = v(x_k)$, в частности, $v'(b_{n+1}) = W$. Используя это наблюдение, индукцией по построению терма r, не содержащего переменных, отличных от $x_1, \ldots, x_n$, нетрудно доказать, что для всякого $w \in W$ и любой оценки v' в $\mathfrak{F}^*$

$$w \in v'(r^*) \iff w \in v(\rho_{x_{n+1}} r),$$

откуда сразу же получаем, что $u \notin (v'(t^*) \setminus v'(s^*)) \cup (v'(s^*) \setminus v'(t^*))$, а значит, $\mathfrak{F}^{*+} \not\models^{v'} t^* = s^*$. □

В качестве следствия доказанных лемм получаем две теоремы.

Теорема 1. *Проблема равенства константных термов в классе всех модальных алгебр является* PSPACE*-полной.*

Доказательство. Проблема равенства термов в классе модальных алгебр полиномиально (линейно) эквивалентна проблеме выводимости формул в модальной логике **K**, которая PSPACE-полна [9], поэтому проблема равенства константных термов находится в PSPACE. Как мы показали, проблема равенства произвольных термов полиномиально сводится к проблеме равенства константных термов, поэтому проблема равенства константных термов PSPACE-трудна. □

Теорема 2. *Проблема равенства термов в классе всех нуль-порождённых модальных алгебр является* PSPACE*-полной.*

Доказательство. Следует из теоремы 1. □

6. Равенство константных слов в произвольном классе алгебр

Для произвольного непустого подмножества I множества $\mathbb{N}$ определим класс шкал

$$\mathcal{C}(I) \quad = \quad \{\mathfrak{F}_k : k \in \mathbb{N} \setminus 2 \cdot I\}.$$

Пусть $\mathscr{C}_I$ — многообразие алгебр, в которых истинны все равенства термов, которые истинны в классе $\mathcal{C}(I)$. Нетрудно видеть, что $\mathcal{C}(I) \subset \mathscr{C}_I$, и поэтому в классах $\mathcal{C}(I)$ и $\mathscr{C}_I$ истинны одни и те же равенства термов.

Следующая лемма устанавливает связь между термами $a_1, a_2, a_3, \ldots$ (см. $(**)$), многообразием $\mathscr{C}_I$ и множеством I.

Лемма 4. *Для любого $n \in \mathbb{N}$ справедлива следующая эквивалентность:*

$$\mathscr{C}_I \models \neg a_{2n} = \top \quad \Longleftrightarrow \quad n \in I.$$

Доказательство. Следует из леммы 1. □

Под *длиной* терма r понимаем суммарное число вхождений символов в терм r как в слово в конечном алфавите, при этом длину переменной считаем равной единице[4]; длину терма r будем обозначать $|r|$.

Лемма 5. *Для любых термов t и s справедливо следующее: $\mathscr{C}_I \not\models t = s$ тогда и только тогда, когда существует такое $n \in \mathbb{N}$, что*

- *n не превосходит удвоенной суммарной длины термов t и s;*
- *$\mathfrak{F}_n \in \mathcal{C}(I)$;*
- *$\mathfrak{F}_n^+ \not\models t = s$.*

Доказательство. ($\Rightarrow$) Пусть $\mathscr{C}_I \not\models t = s$. Тогда $\mathfrak{F}_k^+ \not\models^v t = s$ для некоторого $k \in \mathbb{N} \setminus 2 \cdot I$ и некоторой оценки v в $\mathfrak{F}_k$. Тогда существует $u \in (v(t) \setminus (s)) \cup (v(s) \setminus (t))$. Пусть m — наибольшее число вложенных модальностей в термах t и s. Согласно $(*)$, на принадлежность мира u множеству $(v(t) \setminus (s)) \cup (v(s) \setminus (t))$ влияют только

[4]Возможно и другое определение, когда длина переменной считается равной количеству символов в записи этой переменной с учётом числа символов в индексе. Для наших целей такое определение длины тоже подходит.

те миры из W_k, которые достижимы из u по отношению R_k не более чем за m шагов. И если $k > m$, то вместо $\mathfrak{F}_k$ можно взять шкалу $\mathfrak{F}_{2m+1}$: в этом случае несложно убедиться, что $\mathfrak{F}_{2m+1} \not\models t = s$, причём $\mathfrak{F}_{2m+1} \in \mathcal{C}(I)$. Осталось заметить, что число $2m + 1$ не превосходит удвоенной суммарной длины термов t и s.

($\Leftarrow$) Если $\mathscr{C}_I \models t = s$, то равенство $t = s$ истинно, в частности, в любой шкале из $\mathcal{C}(I)$, а значит, указанного в условии n не существует. □

Замечание 2. Таким образом, если некоторое равенство термов опровергается в $\mathscr{C}_I$, то оно опровергается в некоторой нуль-порождённой алгебре из $\mathscr{C}_I$, число элементов которой не превосходит числа подмножеств множества миров шкалы $\mathfrak{F}_n$, т.е. $2^{2(|t|+|s|)}$.

Из этих двух лемм получаем следующую теорему.

Теорема 3. *Пусть S — класс сложности или степень неразрешимости, причём* coNP $\subseteq S$ *и для S существует S-полная задача. Тогда существует многообразие алгебр, для которого проблема равенства термов и проблема равенства константных термов в нём являются S-полными.*

Доказательство. Пусть множество I натуральных чисел — S-полная задача. Из леммы 4 следует S-трудность проблемы равенства константных термов в многообразии $\mathscr{C}_I$. Покажем, что из леммы 5 следует принадлежность этой проблемы классу S.

Нетрудно понять, что существует полиномиальный недетерминированный алгоритм, который по числу n и термам t и s выясняет, опровергается ли равенство $t = s$ в шкале $\mathfrak{F}_n$: соответствующий алгоритм сначала «угадывает» оценку v переменных, входящих в t или s, и мир w в $\mathfrak{F}_n$, а затем, используя $(*)$, выясняет, верно ли, что $w \in (v(t) \setminus v(s)) \cup (v(s) \setminus v(t))$. Запустив этот алгоритм последовательно на числах от 0 до $2(|t| + |s|)$, мы получим конечное множество J номеров шкал, не превосходящих числа $2(|t| + |s|)$, в которых опровергается равенство $t = s$. Но тогда, с учётом леммы 5,

$$\mathscr{C}_I \not\models t = s \iff J \cap (\mathbb{N} \setminus 2 \cdot I) \neq \varnothing,$$

откуда следует, что проблема опровержимости термов в многообразии $\mathscr{C}_I$ принадлежит классу co$S$, а значит, проблема равенства термов в многообразии $\mathscr{C}_I$ принадлежит классу S. □

Заключение

Результаты, касающиеся PSPACE-полноты проблемы равенства константных термов в классе всех модальных алгебр, следуют из [6], но здесь представлено более компактное и менее зависимое[5] доказательство. Кроме того, в [6] строится погружение лишь специального PSPACE-полного фрагмента модальной логики **K** в её константный фрагмент, а здесь мы предлагаем полиномиальный алгоритм, сводящий равенство *любых* двух термов к равенству константных термов; такой

[5] В [6] существенно использовалось построение, возникающее в доказательстве PSPACE-трудности логики **K**, здесь же мы этого избежали.

подход был использован в [4,12–14] для доказательства EXPTIME- и 2EXPTIME-полноты константных фрагментов некоторых логик, а в [14] ещё и для доказательства неразрешимости константного фрагмента некоторой логики. Результаты, касающиеся вопроса существования многообразий модальных алгебр с проблемами равенства термов и константных термов, имеющими любую заранее заданную алгоритмическую сложность, имеют взаимосвязь с работой [5] и представленными недавно результатами [15].

Из кажущихся автору интересных вопросов стоит отметить следующий: верно ли, что любое равенство модальных термов, опровергающееся в некоторой алгебре, опровергается и в некоторой нуль-порождённой алгебре? Если ответ на этот вопрос положителен, то, скорее всего, в приведённых выше доказательствах можно было бы обойтись без построений типа x-релятивизации термов. Кроме того, это означало бы, что класс всех модальных алгебр порождается нуль-порождёнными модальными алгебрами.

Список литературы

[1] Адян С.И., Дурнев В.Г. Алгоритмические проблемы для групп и полугрупп // Успехи математических наук. 2000. Т. 55, № 2(332). С. 3–94.

[2] Левин Л.А. Универсальные задачи перебора // Проблемы передачи информации. 1973. Т. 9, № 3. С. 115–116.

[3] Марков А.А. Невозможность некоторых алгорифмов в теории ассоциативных систем // Доклады Академии наук СССР. 1947. Т. 55, № 7. С. 587–590.

[4] Рыбаков М.Н. Сложность константного фрагмента пропозициональной динамической логики // Вестник ТвГУ. Серия: Прикладная математика. 2007. № 5. С. 5–17.

[5] Рыбаков М.Н. Алгоритмические свойства линейно аппроксимируемых квазинормальных модальных логик // Вестник ТвГУ. Серия: Прикладная математика. 2018. № 4. С. 87–97. https://doi.org/10.26456/vtpmk520

[6] Chagrov A., Rybakov M. How many variables does one need to prove PSPACE-hardness of modal logics? // Advances in Modal Logic. 2003. № 4. Pp. 71–82.

[7] Chagrov A., Zakharyaschev M. Modal Logic. Oxford: Oxford University Press, 1997.

[8] Halpern J.Y. The effect of bounding the number of primitive propositions and the depth of nesting on the complexity of modal logic // Aftificial Intelligence. 1995. Vol. 75, № 2. Pp. 361–372.

[9] Ladner R.E. The computational complexity of provability in systems of modal propositional logic // SIAM Journal on Computing. 1977. Vol. 6, № 3. Pp. 467–480.

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

[11] Post E.L. Recursive unsolvability of a problem of Thue // Journal of Symbolic Logic. 1947. Vol. 12, № 1. Pp. 1–11.

[12] Rybakov M. Complexity of finite-variable fragments of EXPTIME-complete logics // Journal of Applied Non-Classical Logics. 2007. Vol. 17, № 3. Pp. 359–382.

[13] Rybakov M., Shkatov D. Complexity and expressivity of branching- and alternating-time temporal logics with finitely many variables // Theoretical Aspects of Computing. Eds. by B. Fischer, T. Uustalu. Series: Lecture Notes in Computer Science. Springer, 2018. Pp. 396–414.

[14] Rybakov M., Shkatov D. Complexity and expressivity of propositional dynamic logics with finitely many variables // Logic Journal of the IGPL. 2018. Vol. 26, № 5. Pp. 539–547.

[15] Rybakov M., Shkatov D. On relationship between complexity function and complexity of validity in propositional modal logic // Logical Perspectives 2021 (Moscow, June 7 – July 8).

[16] Shoenfield J.R. Degrees of unsolvability. North-Holland Publishing Company, American Elsevier Publishing Company, 1971.

[17] Spaan E. Complexity of modal logics: PhD thesis. Universiteit van Amsterdam, 1993.

[18] Thue A. Problem über Veränderungen von Zeichenreihen nach gegebehen Regeln // Videnskapsselskapets Skrifter. I. Mat.-Naturv. Klasse. 1914. № 10.

Образец цитирования

Рыбаков М.Н. Сложность проблемы равенства слов в многообразиях модальных алгебр // Вестник ТвГУ. Серия: Прикладная математика. 2021. № 3. С. 5–17. https://doi.org/10.26456/vtpmk619

Сведения об авторах

1. **Рыбаков Михаил Николаевич**
ведущий научный сотрудник ИППИ имени А. А. Харкевича РАН; доцент факультета математики НИУ ВШЭ; доцент кафедры функционального анализа и геометрии Тверского государственного университета.

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

COMPUTATIONAL COMPLEXITY OF THE WORD PROBLEM IN MODAL ALGEBRAS

Rybakov Mikhail
Leading Researcher, A.A. Kharkevich IITP of the Russian Academy of Sciences
Associate Professor at Faculty of Mathematics, Higher School of Economics
Associate Professor at Functional Analysis and Geometry department,
Tver State University
Russia, 170100, Tver, 33 Zhelyabova str., TSU.
E-mail: m_rybakov@mail.ru

Received 04.08.2021, revised 17.08.2021.

The paper deals with the word problem for modal algebras. It is proved that, for the variety of all modal algebras, the word problem is PSPACE-complete if only constant modal terms or only 0-generated modal algebras are considered. We also consider the word problem for different varieties of modal algebras. It is proved that the word problem for a variety of modal algebras can be C-hard, for any complexity class or unsolvability degree C containing a C-complete problem. It is shown how to construct such varieties.

Keywords: modal algebra, word equality problem, computational complexity.

Citation

Rybakov M., "Computational complexity of the word problem in modal algebras", *Vestnik TvGU. Seriya: Prikladnaya Matematika [Herald of Tver State University. Series: Applied Mathematics]*, 2021, № 3, 5–17 (in Russian). https://doi.org/10.26456/vtpmk619

References

[1] Adian S.I., Durnev V.G., "Decision problems for groups and semigroups", *Russian Mathematical Surveys*, **55**:2 (2000), 207–296.

[2] Levin L.A., "Universal sequential search problems", *Problems of Information Transmission*, **9**:3 (1973), 265–266.

[3] Markov A.A., "The impossibility of some algorithms in the theory of associative systems", *Soviet Mathematics. Doklady*, **55**:7 (1947), 587–590 (in Russian).

[4] Rybakov M.N., "The complexity of a constant fragment of propositional dynamic logic", *Vestnik TvGU. Seriya: Prikladnaya Matematika [Herald of Tver State University. Series: Applied Mathematics]*, 2007, № 5, 5–17 (in Russian).

[5] Rybakov M.N., "Algorithmical properties of quasinormal modal logics with linear finite model property", *Vestnik TvGU. Seriya: Prikladnaya Matematika [Herald of Tver State University. Series: Applied Mathematics]*, 2018, № 4, 87–97 (in Russian), https://doi.org/10.26456/vtpmk520.

[6] Chagrov A., Rybakov M., "How many variables does one need to prove PSPACE-hardness of modal logics?", *Advances in Modal Logic*, 2003, № 4, 71–82.

[7] Chagrov A., Zakharyaschev M., *Modal Logic*, Oxford University Press, Oxford, 1997.

[8] Halpern J.Y., "The effect of bounding the number of primitive propositions and the depth of nesting on the complexity of modal logic", *Aftificial Intelligence*, **75**:2 (1995), 361–372.

[9] Ladner R.E., "The computational complexity of provability in systems of modal propositional logic", *SIAM Journal on Computing*, **6**:3 (1977), 467–480.

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

[11] Post E.L., "Recursive unsolvability of a problem of Thue", *Journal of Symbolic Logic*, **12**:1 (1947), 1–11.

[12] Rybakov M., "Complexity of finite-variable fragments of EXPTIME-complete logics", *Journal of Applied Non-Classical Logics*, **17**:3 (2007), 359–382.

[13] Rybakov M., Shkatov D., "Complexity and expressivity of branching- and alternating-time temporal logics with finitely many variables", *Theoretical Aspects of Computing*, Lecture Notes in Computer Science, eds. B. Fischer, T. Uustalu, Springer, 2018, 396–414.

[14] Rybakov M., Shkatov D., "Complexity and expressivity of propositional dynamic logics with finitely many variables", *Logic Journal of the IGPL*, **26**:5 (2018), 539–547.

[15] Rybakov M., Shkatov D., "On relationship between complexity function and complexity of validity in propositional modal logic", *Logical Perspectives 2021* (Moscow, June 7 – July 8).

[16] Shoenfield J.R., *Degrees of unsolvability*, North-Holland Publishing Company; American Elsevier Publishing Company, 1971.

[17] Spaan E., *Complexity of modal logics*, PhD thesis, Universiteit van Amsterdam, 1993.

[18] Thue A., "Problem über Veränderungen von Zeichenreihen nach gegebehen Regeln", *Videnskapsselskapets Skrifter. I. Mat.-Naturv. Klasse*, 1914, № 10.