М.Н.Рыбаков

ПОГРУЖЕНИЕ ИНТУИЦИОНИСТСКОЙ ЛОГИКИ В ЕЕ ФРАГМЕНТ ОТ ДВУХ ПЕРЕМЕННЫХ И СЛОЖНОСТЬ ЭТОГО ФРАГМЕНТА*

Abstract. *An embedding of intuitionistic propositional logic into its two-variable fragment is constructed. Using this embedding, we prove that the decision problem for two-variable fragment of intuitionistic propositional logic is* PSPACE-*complete.*

1. Введение

Как следует из названия, речь пойдет, в частности, о построении погружения интуиционистской пропозициональной логики **Int** в ее фрагмент от двух переменных. Здесь под погружением множества формул A во множество формул B мы понимаем полиномиально (по затратам времени) вычислимую функцию (алгоритм, эффективную процедуру) f такую, что для всякой формулы φ имеет место эквивалентность

$$\varphi \in A \iff f(\varphi) \in B.$$

Погружение, которое будет построено, на самом деле обладает и некоторыми дополнительными «хорошими» свойствами, например, оно в определенном смысле сохраняет структуру исходной интуиционистской формулы.

Сразу заметим, что это погружение (или существование такого погружения) навряд ли представляет большой интерес само по себе; оно в первую очередь является лишь средством для решения других задач. Более того, оно и возникло при решении автором вопроса, не связанного напрямую с погружениями, а именно вопроса о сложности проблемы разрешения некоторых фрагментов интуиционистской логики. И хотя в названии работы погружение поставлено на первое место, мы, тем не менее, ставим целью не столько построить его, сколько получить с его помощью некоторые новые факты об **Int**, в частности, касающиеся алгоритмических аспектов этой логики и некоторых ее расширений.

Опишем ситуацию с проблемой разрешения интуиционистской логики подробнее.

* Работа выполнена при поддержке РФФИ, грант 03–06–80115.

2. Сложность разрешения Int

Хорошо известно, что интуиционистская логика **Int**, как и многие другие «естественные» пропозициональные логики, является разрешимой. Это означает, что существует алгоритм (эффективная процедура), который по всякой формуле дает ответ на вопрос о том, принадлежит эта формула интуиционистской логике или нет. Заметим, что существование такого алгоритма говорит лишь о принципиальной разрешимости интуиционистской логики, поскольку алгоритмы, разрешающие **Int**, могут оказаться довольно сложными, например, все они могут требовать для своей работы слишком больших временны́х ресурсов, что сильно затруднит их применение на практике.

В некотором смысле дело именно так и обстоит. В [9] доказано, что проблема разрешения интуиционистской логики является PSPACE-полной (доказательство этого факта можно найти также в [4]). Напомним, что проблема называется PSPACE-полной, если

- она находится в классе PSPACE, т.е. может быть решена некоторым алгоритмом с полиномиальными затратами памяти от длины входных данных;
- она PSPACE-трудна, т.е. всякая проблема из класса PSPACE полиномиально (по времени) сводится к данной проблеме

(о классах сложности см. [5, 10]). Проблемы, являющиеся PSPACE-полными, на данный момент считаются реально не решаемыми – из известных алгоритмов, решающих такие проблемы, самые быстрые требуют для своей работы экспоненту времени (при этом неизвестно, существуют ли более эффективные алгоритмы, решающие такого рода проблемы). Таким образом, хотя интуиционистская логика и разрешима, вряд ли удастся решать на практике проблему принадлежности формул логике **Int** с использованием существующей сегодня вычислительной техники.

Тем не менее, хотя и имеются определенные трудности с разрешением логики **Int**, быть может, некоторые достаточно выразительные фрагменты этой логики удастся разрешать за «реальное время».

Одним из таких фрагментов является позитивный фрагмент логики **Int**, обозначим его через $\mathbf{Int}^{+}$. Заметим, что, отказываясь от использования отрицания, мы практически не теряем выразительности языка: логика **Int** погружается в $\mathbf{Int}^{+}$, см., например, [1]. Но и PSPACE-полноту мы тоже не теряем: на самом деле в [9] для обоснования PSPACE-трудности проблемы разрешения **Int** использовались формулы, которые в качестве связок содержали лишь конъюнкцию и импликацию. Более того, как показано в [3], уже импликативный фрагмент **Int** обладает PSPACE-полной проблемой разрешения. Поскольку безымпликативные интуиционистские фрагменты не столь интересны, то на пути уменьшения набора связок (с сохранением импликации[1]) нельзя получить фрагменты интуиционистской логики, которые были бы разрешимы за «реальное время».

Мы рассмотрим ситуацию, когда язык интуиционистской логики содержит лишь конечное число переменных. Такое ограничение на язык, с одной стороны, вполне оправдано: в реально возникающих формулах (множествах формул) обычно имеется лишь конечное число переменных, причем это число зачастую невелико (например, чтобы аксиоматизировать **Int**, вполне достаточно формул от трех переменных). С другой стороны, известно, что для некоторых логик с достаточно сложной проблемой разрешения в полном языке удается доказать, что проблема разрешения в языке с конечным числом переменных решается с полиномиальными затратами времени. Например, так обстоит дело с проблемой выполнимости булевых формул – она является NP-полной – и с проблемой выполнимости булевых формул с кванторами – эта проблема PSPACE-полна. Если рассматривать булевы формулы (или булевы формулы с кванторами) только от n переменных (число n фиксировано), то соответствующие проблемы решаются с полиномиальными затратами времени, поскольку в этом случае для решения указанных проблем достаточно обозревать таблицы истинности с заранее ограниченным некоторой константой числом наборов возможных значений переменных (например, для булевых формул от n переменных в качестве такой константы можно взять 2^n).

Для удобства дальнейшего изложения введем следующее обозначение. Пусть L – некоторая пропозициональная логика (в языке с бесконечным числом переменных); через $L(n)$ будем обозначать фрагмент логики L, состоящий из формул от не более чем n переменных.

Из сказанного выше следует, что фрагмент **Cl**(n) полиномиально разрешим для любого n. Может, и с **Int**(n) дело обстоит примерно так же?

Известно, что фрагмент **Int**(0) является полиномиально разрешимым. Действительно, любая константная формула эквивалентна в **Int** либо формуле $\perp$, либо формуле $\top$, а из того, что **Int** содер-

[1] Например, проблема разрешения некоторых безымпликативных фрагментов **Int** находится в классе NP.

жится в классической пропозициональной логике **Cl**, получаем, что **Int**(0) = **Cl**(0), т.е. для выяснения принадлежности константной формулы интуиционистской логике достаточно выяснить, является ли эта формула тождественно истинной, а последний вопрос решается для константных формул с квадратичными затратами времени от длины тестируемой формулы: соответствующий алгоритм состоит в нахождении истинностного значения формулы с использованием таблиц истинности для булевых связок. Более того, полиномиально разрешимым является фрагмент **Int**(1), что следует из конструкции Нишимуры [7]: каждая формула от одной переменной, которая не принадлежит **Int**, опровергается в одном из миров «лестницы» Нишимуры. Остается заметить, что для выяснения опровержимости формулы от одной переменной на «лестнице» Нишимуры достаточно проверить, истинна ли эта формула в верхних[2] мирах «лестницы», число которых не превышает длины тестируемой формулы.

Что можно сказать о сложности **Int**(n) для $n \geqslant 2$?

Некоторое время назад А.В. Чагровым была высказана гипотеза о том, что для всякого натурального n фрагмент **Int**(n) полиномиально разрешим. Эта гипотеза отчасти подкреплялась тем, что в доказательстве PSPACE-трудности проблемы разрешения **Int** в [9] (как, впрочем, и в других, более поздних, доказательствах) существенно использовался тот факт, что язык интуиционистской логики содержит бесконечно много переменных. Однако в середине 90-х годов XX века было доказано, что для обоснования PSPACE-полноты проблемы разрешения некоторых модальных пропозициональных логик достаточно, чтобы в языке была лишь одна переменная [6, 8], а чуть позже было установлено, что в ряде случаев достаточно и константных формул [2]. Возникло предположение, что аналогичный результат (только с двумя или более переменными в языке) может быть справедлив и для **Int**. Построив погружение, о котором говорилось во введении, мы докажем, что дело именно так и обстоит: уже фрагмент **Int**(2) обладает PSPACE-полной проблемой разрешения.

3. Построение погружения

Считаем, что интуиционистские формулы строятся из переменных $p_0, p_1, p_2, \ldots$ и константы $\bot$ с помощью $\wedge$, $\vee$ и $\to$. Отрицание вводим как обычное сокращение: $\neg\psi = \psi \to \bot$. При записи формул будем опускать некоторые скобки, считая самой сильной

[2] Имеются в виду, конечно, не самые верхние миры «лестницы» (т.е. из которых достижимы только они сами), а верхняя часть «лестницы».

связкой $\neg$, затем $\wedge$, $\vee$ и $\to$. В рассуждениях будет использоваться семантика Крипке; мы будем придерживаться обозначений [4].

Поскольку имеется погружение **Int** в **Int**$^+$ [1], нам достаточно построить погружение **Int**$^+$ в **Int**(2).

Пусть p и q – две (различные) пропозициональные переменные. Определим следующие формулы:

$$A_1^0 = \neg(p\wedge q);\ A_2^0 = \neg(\neg p\wedge q);\ B_1^0 = \neg(p\wedge\neg q);\ B_2^0 = \neg(\neg p\wedge\neg q);$$

$$\begin{array}{ll} A_1^1 = A_1^0\wedge A_2^0 \to B_1^0\vee B_2^0; & B_1^1 = A_2^0\wedge B_1^0 \to A_1^0\vee B_2^0; \\ A_2^1 = A_1^0\wedge B_1^0 \to A_2^0\vee B_2^0; & B_2^1 = A_2^0\wedge B_2^0 \to A_1^0\vee B_1^0; \\ A_3^1 = A_1^0\wedge B_2^0 \to A_1^0\vee B_1^0; & B_3^1 = B_1^0\wedge B_2^0 \to A_1^0\vee A_2^0. \end{array}$$

Пусть определены формулы $A_1^k, \dots, A_m^k$ и $B_1^k, \dots, B_m^k$, где $k \geqslant 1$. Определим формулы $A_1^{k+1}, \dots, A_n^{k+1}$ и $B_1^{k+1}, \dots, B_n^{k+1}$, где $n = (m-1)^2$:

$$\begin{array}{ll} A_1^{k+1} = A_1^k \to B_1^k\vee A_2^k\vee B_2^k; & B_1^{k+1} = B_1^k \to A_1^k\vee A_2^k\vee B_2^k; \\ A_2^{k+1} = A_1^k \to B_1^k\vee A_2^k\vee B_3^k; & B_2^{k+1} = B_1^k \to A_1^k\vee A_2^k\vee B_3^k; \\ A_3^{k+1} = A_1^k \to B_1^k\vee A_2^k\vee B_4^k; & B_3^{k+1} = B_1^k \to A_1^k\vee A_2^k\vee B_4^k; \\ \dots & \dots \\ A_s^{k+1} = A_1^k \to B_1^k\vee A_i^k\vee B_j^k; & B_s^{k+1} = B_1^k \to A_1^k\vee A_i^k\vee B_j^k; \\ \dots & \dots \\ A_n^{k+1} = A_1^k \to B_1^k\vee A_m^k\vee B_m^k; & B_n^{k+1} = B_1^k \to A_1^k\vee A_m^k\vee B_m^k. \end{array}$$

Формулы A_i^k и B_i^k будем называть формулами уровня k. Обозначим через N_k число формул A_i^k уровня k (ясно, что N_k будет также и числом формул B_i^k уровня k). Нетрудно видеть, что

$$N_0 = 2, \quad N_1 = 3, \quad N_{k+2} = (N_{k+1} - 1)^2.$$

Через $|A|$ обозначим длину формулы A. Пусть

$$l = \max_{1\leqslant i\leqslant 2}\{|A_i^0| + |B_i^0|\}.$$

Считая отрицание за один символ, получаем, что $l = 15$. Понятно, что $|A_i^k| < 5^k\cdot l$ и $|B_i^k| < 5^k\cdot l$ (этот факт легко обосновывается индукцией по k). Кроме того, нетрудно видеть, что существует k_0 такое, что для всякого $k \geqslant k_0$ имеет место отношение $5^k\cdot l < N_k$. Легко убедиться, что в качестве k_0 можно взять любое целое число, большее пяти; пусть для определенности $k_0 = 6$.

Теперь построим модель, в которой будут опровергаться все определенные выше формулы, при этом для каждой формулы будет существовать единственный максимальный мир, в котором она опровергается. Положим

$$W = \{a_i^0, b_i^0 : k \geqslant 0,\ 1 \leqslant i \leqslant N_k\}.$$

Элементы a_i^k и b_i^k будем называть мирами уровня k. На множестве W определим отношение достижимости R. Положим

$R^a_1 = \{\langle a^1_1, b^0_1\rangle, \langle a^1_1, b^0_2\rangle, \langle a^1_2, a^0_1\rangle, \langle a^1_2, b^0_2\rangle, \langle a^1_3, a^0_2\rangle, \langle a^1_3, b^0_1\rangle\}$;
$R^b_1 = \{\langle b^1_1, a^0_1\rangle, \langle b^1_1, b^0_2\rangle, \langle b^1_2, a^0_1\rangle, \langle b^1_2, b^0_1\rangle, \langle b^1_3, a^0_1\rangle, \langle b^1_3, a^0_2\rangle\}$;
$R_1 = R^a_1 \cup R^b_1$.

Для всякого $k \geqslant 1$ положим

$R^a_{k+1} = \{\langle a^{k+1}_m, b^k_1\rangle, \langle a^{k+1}_m, a^k_i\rangle, \langle a^{k+1}_m, b^k_j\rangle : A^{k+1}_m = A^k_1 \to B^k_1 \vee A^k_i \vee B^k_j\}$;
$R^b_{k+1} = \{\langle b^{k+1}_m, a^k_1\rangle, \langle b^{k+1}_m, a^k_i\rangle, \langle b^{k+1}_m, b^k_j\rangle : B^{k+1}_m = B^k_1 \to A^k_1 \vee A^k_i \vee B^k_j\}$;
$R_{k+1} = R^a_{k+1} \cup R^b_{k+1}$.

Теперь положим

$$R' = \bigcup_{k=1}^{\infty} R_k$$

и в качестве отношения достижимости R возьмем рефлексивно-транзитивное замыкание отношения R'.

Положим $\mathcal{F} = \langle W, R\rangle$, $\mathcal{M} = \langle \mathcal{F}, v\rangle$, где оценка v определена следующим образом:

$$(\mathcal{M},w) \vDash p \iff w = a^0_1 \text{ или } w = b^0_1;$$
$$(\mathcal{M},w) \vDash q \iff w = a^0_1 \text{ или } w = b^0_2.$$

Для наглядности модель $\mathcal{M}$ изображена на рис. 1.

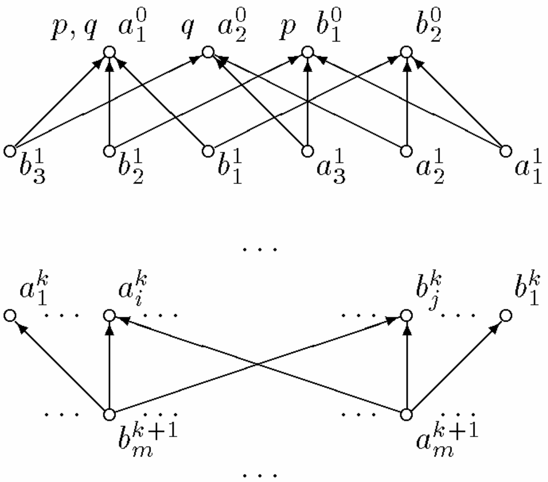

Рис. 1: Модель $\mathcal{M}$

Лемма 1. *Пусть w – мир модели $\mathcal{M}$. Тогда*

$$(\mathcal{M},w) \nvDash A^k_m \iff wRa^k_m;$$
$$(\mathcal{M},w) \nvDash B^k_m \iff wRb^k_m.$$

Доказательство проведем индукцией по k. Пусть $k = 0$. Имеется всего четыре формулы нулевого уровня: A_1^0, A_2^0, B_1^0 и B_2^0.

Поскольку $(\mathcal{M}, a_1^0) \models p \wedge q$, то $(\mathcal{M}, a_1^0) \not\models A_1^0$, а следовательно, для всякого мира w такого, что wRa_1^0, имеет место отношение $(\mathcal{M}, w) \not\models A_1^0$. Пусть теперь для некоторого $w \in W$ выполнено отношение $(\mathcal{M}, w) \not\models A_1^0$. Тогда существует мир w', достижимый из w, такой, что $(\mathcal{M}, w') \models p \wedge q$. Но единственным миром модели $\mathcal{M}$, в котором истинны обе переменные p и q, является мир a_1^0. Следовательно, $w' = a_1^0$, и значит, wRa_1^0.

Поскольку $(\mathcal{M}, a_2^0) \models \neg p \wedge q$, то $(\mathcal{M}, a_2^0) \not\models A_2^0$, а следовательно, для всякого мира w такого, что wRa_2^0, имеет место отношение $(\mathcal{M}, w) \not\models A_2^0$. Пусть теперь для некоторого $w \in W$ выполнено отношение $(\mathcal{M}, w) \not\models A_2^0$. Тогда существует мир w', достижимый из w, такой, что $(\mathcal{M}, w) \models \neg p \wedge q$. Но единственным миром модели $\mathcal{M}$, в котором истинна только переменная q, является мир a_2^0. Следовательно, $w' = a_2^0$, и значит, wRa_2^0.

Поскольку $(\mathcal{M}, b_1^0) \models p \wedge \neg q$, то $(\mathcal{M}, b_1^0) \not\models B_1^0$, а следовательно, для всякого мира w такого, что wRb_1^0, имеет место отношение $(\mathcal{M}, w) \not\models B_1^0$. Пусть теперь для некоторого $w \in W$ выполнено отношение $(\mathcal{M}, w) \not\models B_1^0$. Тогда существует мир w', достижимый из w, такой, что $(\mathcal{M}, w) \models p \wedge \neg q$. Но единственным миром модели $\mathcal{M}$, в котором истинна только переменная p, является мир b_1^0. Следовательно, $w' = b_b^0$, и значит, wRa_2^0.

Поскольку $(\mathcal{M}, b_2^0) \models \neg p \wedge \neg q$, то $(\mathcal{M}, b_2^0) \not\models B_2^0$, а следовательно, для всякого мира w такого, что wRb_2^0, имеет место отношение $(\mathcal{M}, w) \not\models B_2^0$. Пусть теперь для некоторого $w \in W$ выполнено отношение $(\mathcal{M}, w) \not\models B_2^0$. Тогда существует мир w', достижимый из w, такой, что $(\mathcal{M}, w) \models \neg p \wedge \neg q$. Предположим, что $w' \neq b_2^0$. Заметим, что w' в этом случае не может быть миром нулевого уровня, поскольку в каждом мире нулевого уровня, отличном от b_2^0, истинна хотя одна из переменных p и q. Значит, w' является миром уровня k для некоторого $k > 0$. Нетрудно видеть, что в этом случае из w' достижимы как минимум два различных мира уровня 0; хотя бы в одном из них истинна хотя бы одна из переменных p и q, а последнее противоречит справедливости отношения $(\mathcal{M}, w) \models \neg p \wedge \neg q$. Следовательно, $w' = b_2^0$, и значит, wRb_2^0.

Пусть для всякого мира w модели $\mathcal{M}$ и всякого $s \leqslant N_k$ имеют место следующие эквивалентности:

$$(\mathcal{M}, w) \not\models A_s^k \iff wRa_s^k;$$
$$(\mathcal{M}, w) \not\models B_s^k \iff wRb_s^k.$$

Пусть $A_m^{k+1} = A_1^k \to B_1^k \vee A_i^k \vee B_j^k$ и $B_m^{k+1} = B_1^k \to A_1^k \vee A_i^k \vee B_j^k$ для некоторых $i, j \in \{2, \dots, N_k\}$. Покажем, что

$$(\mathcal{M}, w) \nvDash A_m^{k+1} \iff wRa_m^{k+1};$$
$$(\mathcal{M}, w) \nvDash B_m^{k+1} \iff wRb_m^{k+1}.$$

Поскольку $a_m^{k+1}Rb_1^k$, $a_m^{k+1}Ra_i^k$, $a_m^{k+1}Rb_j^k$, то по индукционному предположению $(\mathcal{M}, a_m^{k+1}) \nvDash B_1^k \vee A_i^k \vee B_j^k$, а поскольку неверно, что $a_m^{k+1}Ra_1^k$, то по индукционному предположению $(\mathcal{M}, a_m^{k+1}) \vDash A_1^k$. Следовательно, для всякого w такого, что wRa_m^{k+1}, имеет место отношение $(\mathcal{M}, w) \nvDash A_m^{k+1}$.

Аналогично обосновывается, что для всякого w такого, что wRb_m^{k+1}, имеет место отношение $(\mathcal{M}, w) \nvDash B_m^{k+1}$.

Пусть $(\mathcal{M}, w) \nvDash A_m^{k+1}$ для некоторого мира w модели $\mathcal{M}$. Тогда существует достижимый из w мир w' такой, что $(\mathcal{M}, w') \vDash A_1^k$ и $(\mathcal{M}, w') \nvDash B_1^k \vee A_i^k \vee B_j^k$. По индукционному предположению, из w' должны быть достижимы миры b_1^k, a_i^k, b_j^k, и должен быть недостижим мир a_1^k. Поскольку различные миры одного и того же уровня друг из друга не достижимы, а миры более высокого уровня не достижимы из миров более низкого уровня, то w' является миром уровня не ниже, чем $k + 1$. С другой стороны, для всякого мира w'' более высокого уровня, чем $k + 1$, имеет место отношение $w''Ra_1^k$, и значит, $(\mathcal{M}, w'') \nvDash A_1^k$. Следовательно, w' является миром уровня не выше, чем $k + 1$. Итак, w' – мир уровня $k + 1$, из которого достижимы миры b_1^k, a_i^k, b_j^k и не достижим мир a_1^k. По определению шкалы $\mathcal{F}$ это возможно только в том случае, когда $w' = a_s^{k+1}$, где s таково, что $A_s^{k+1} = A_1^k \to B_1^k \vee A_i^k \vee B_j^k$. Ясно, что в нашем случае $s = m$, т.е. $w' = a_m^{k+1}$. Следовательно, wRa_m^{k+1}.

Аналогично доказывается, что если $(\mathcal{M}, w) \nvDash B_m^{k+1}$, то wRb_m^{k+1}.

Пусть φ – некоторая интуиционистская формула, не содержащая отрицания, $p_1, \dots , p_n$ – все ее переменные. Обозначим через k наименьшее натуральное число, удовлетворяющее отношению $|\varphi| < 5^k \cdot 15$. Заметим, что
$$N_{k+6} > 5^{k+6} \cdot 15 > 5^6 \cdot 15 \cdot |\varphi| > |\varphi| > n,$$
поэтому следующее определение корректно: для всякого $i \in \{1, \dots , n\}$ определим формулу α_i, положив
$$\alpha_i = A_i^{k+6} \vee B_i^{k+6}.$$
Обозначим через φ_α формулу, которая получается из φ подстановкой формул $\alpha_1, \dots , \alpha_n$ вместо переменных $p_1, \dots , p_n$ соответственно.

Лемма 2. *Для некоторого натурального числа c имеет место отношение* $|\varphi_\alpha| < c \cdot |\varphi|^2$.

Доказательство. Пусть k – наименьшее натуральное число, удовлетворяющее отношению $|\varphi| < 5^k \cdot 15$. Тогда $5^{k-1} \cdot 15 \leqslant |\varphi|$, и следовательно,

$$5^{k+6} \cdot 15 \leqslant 5^7 \cdot |\,\varphi\,|.$$

Поскольку $|\,A_i^{k+6}\,| < 5^{k+6} \cdot 15$ и $|\,B_i^{k+6}\,| < 5^{k+6} \cdot 15$, то

$$|\,\alpha_i\,| < 2 \cdot 5^{k+6} \cdot 15 \leqslant 2 \cdot 5^7 \cdot |\,\varphi\,|.$$

Следовательно,

$$|\,\varphi_\alpha\,| \leqslant |\,\varphi\,| \cdot \max_{1 \leqslant i \leqslant n} |\,\alpha_i\,| < 2 \cdot 5^7 \cdot |\,\varphi\,|^2,$$

т.е. в качестве c можно взять число $2 \cdot 5^7$.

Лемма 3. *Для всякой интуиционистской формулы φ, не содержащей отрицания, имеет место следующая эквивалентность:*

$$\varphi \in \mathbf{Int} \iff \varphi_\alpha \in \mathbf{Int}.$$

Доказательство. Если $\varphi \in \mathbf{Int}$, то $\varphi_\alpha \in \mathbf{Int}$, поскольку φ_α является подстановочным примером формулы φ.

Пусть φ – интуиционистская формула, не содержащая отрицания, и пусть $\varphi_\alpha \notin \mathbf{Int}$. Тогда существует интуиционистская модель $\mathcal{M}_\varphi = \langle \mathcal{F}_\varphi, v_\varphi \rangle$, определенная на шкале $\mathcal{F}_\varphi = \langle W_\varphi, R_\varphi \rangle$, такая, что для некоторого $w_0 \in W_\varphi$ имеет место отношение $(\mathcal{M}_\varphi, w_0) \not\models \varphi$.

Построим интуиционистскую модель, в некотором мире которой будет опровергаться формула φ_α. Без ограничений общности можем считать, что $W \cap W_\varphi = \varnothing$. Положим $W^* = W \cup W_\varphi$. На множестве W^* рассмотрим следующее отношение R':

$$R' = \{\langle w, a_i^{k+6}\rangle, \langle w, b_i^{k+6}\rangle : w \in W_\varphi, (\mathcal{M}_\varphi, w) \not\models p_i, 1 \leqslant i \leqslant n\} \cup$$
$$\cup \{\langle w, a_{n+1}^{k+6}\rangle, \langle w, b_{n+1}^{k+6}\rangle : w \in W_\varphi\}.$$

Пусть R^* – рефлексивно-транзитивное замыкание отношения $R \cup R_\varphi \cup R'$ и пусть $\mathcal{F}^* = \langle W^*, R^* \rangle$. На шкале $\mathcal{F}^*$ определим модель $\mathcal{M}^* = \langle \mathcal{F}^*, v^* \rangle$, положив для всякого $w \in W^*$

$$(\mathcal{M}^*, w) \models p \iff w = a_1^0 \text{ или } w = b_1^0;$$
$$(\mathcal{M}^*, w) \models q \iff w = a_1^0 \text{ или } w = b_2^0.$$

Для всякой подформулы ψ формулы φ через ψ_α обозначим формулу, получающуюся из ψ подстановкой формул $\alpha_1, \ldots, \alpha_n$ вместо переменных $p_1, \ldots, p_n$ соответственно. Индукцией по построению ψ докажем, что для всякого $w \in W_\varphi$

$$(\mathcal{M}^*, w) \models \psi_\alpha \iff (\mathcal{M}_\varphi, w) \models \psi.$$

Пусть $\psi = p_m$. Если $(\mathcal{M}_\varphi, w) \not\models p_m$, то в модели $\mathcal{M}^*$ из мира w достижимы миры a_m^{k+6} и b_m^{k+6}. Но $(\mathcal{M}, a_m^{k+6}) \not\models A_m^{k+6}$, $(\mathcal{M}, b_m^{k+6}) \not\models B_m^{k+6}$. Понятно, что в этом случае также имеют место отношения $(\mathcal{M}^*, a_m^{k+6}) \not\models A_m^{k+6}$, $(\mathcal{M}^*, b_m^{k+6}) \not\models B_m^{k+6}$, а следовательно, $(\mathcal{M}^*, w) \not\models \alpha_m$, т.е. $(\mathcal{M}^*, w) \not\models \psi_\alpha$.

Пусть теперь $(\mathcal{M}^*, w) \not\models \alpha_m$ для некоторого мира $w \in W_\varphi$; пусть при этом $A_m^{k+6} = A_1^{k+5} \to B_1^{k+5} \vee A_i^{k+5} \vee B_j^{k+5}$, $B_m^{k+6} = B_1^{k+5} \to A_1^{k+5} \vee A_i^{k+5} \vee B_j^{k+5}$.

Тогда в модели $\mathcal{M}^*$ существуют миры w' и w'' такие, что wR^*w', wR^*w'', и при этом

$$(\mathcal{M}^*, w') \vDash A_1^{k+5}, (\mathcal{M}^*, w') \nvDash B_1^{k+5}, (\mathcal{M}^*, w') \nvDash A_i^{k+5}, (\mathcal{M}^*, w') \nvDash B_j^{k+5};$$
$$(\mathcal{M}^*, w'') \vDash B_1^{k+5}, (\mathcal{M}^*, w'') \nvDash A_1^{k+5}, (\mathcal{M}^*, w'') \nvDash A_i^{k+5}, (\mathcal{M}^*, w'') \nvDash B_j^{k+5}.$$

Заметим, что $w', w'' \notin W_\varphi$. Действительно, для всякого $u \in W_\varphi$ имеют место отношения $uR^*a_{n+1}^{k+6}$ и $uR^*b_{n+1}^{k+6}$; но $(\mathcal{M}^*, a_{n+1}^{k+6}) \nvDash B_1^{k+5}$ и $(\mathcal{M}^*, b_{n+1}^{k+6}) \nvDash A_1^{k+5}$, поэтому $(\mathcal{M}^*, u) \nvDash A_1^{k+5}$ и $(\mathcal{M}^*, u) \nvDash B_1^{k+5}$, и поскольку $(\mathcal{M}^*, w') \vDash A_1^{k+5}$ и $(\mathcal{M}^*, w'') \vDash B_1^{k+5}$, то $w', w'' \notin W_\varphi$.

Так как миры w' и w'' достижимы по R^* из некоторого мира множества W_φ, то они не могут быть мирами более высокого уровня, чем $k+6$. С другой стороны, $(\mathcal{M}^*, w') \nvDash A_m^{k+6}$ и $(\mathcal{M}^*, w'') \nvDash B_m^{k+6}$, поэтому w' и w'' не могут быть мирами уровня ниже, чем $k+6$. Таким образом, w' и w'' – миры уровня $k+6$. Но среди миров уровня $k+6$ формула A_m^{k+6} опровергается только в мире a_m^{k+6}, а формула B_m^{k+6} – только в мире b_m^{k+6}, следовательно, $w' = a_m^{k+6}$, а $w'' = b_m^{k+6}$.

Итак, $wR^*a_m^{k+6}$. Это означает, что при построении шкалы $\mathcal{F}^*$ мы положили $uR'a_m^{k+6}$ для некоторого $u \in W_\varphi$ такого, что $wR_\varphi u$. Но если при построении шкалы $\mathcal{F}^*$ мы положили $uR'a_m^{k+6}$, то мы также должны были положить $uR'b_m^{k+6}$, и сделать это мы могли только в том случае, когда $(\mathcal{M}_\varphi, u) \nvDash p_m$. Поскольку $wR_\varphi u$, то получаем, что $(\mathcal{M}_\varphi, w) \nvDash p_m$, и тем самым базис индукции обоснован.

Пусть теперь ψ' и ψ'' – подформулы формулы φ такие, что для всякого мира $w \in W_\varphi$

$$(\mathcal{M}^*, w) \vDash \psi'_\alpha \iff (\mathcal{M}_\varphi, w) \vDash \psi';$$
$$(\mathcal{M}^*, w) \vDash \psi''_\alpha \iff (\mathcal{M}_\varphi, w) \vDash \psi''.$$

Пусть $\psi = \psi' \wedge \psi''$. Тогда для всякого $w \in W_\varphi$

$$\begin{aligned}(\mathcal{M}^*, w) \vDash \psi_\alpha &\iff (\mathcal{M}^*, w) \vDash \psi'_\alpha \text{ и } (\mathcal{M}^*, w) \vDash \psi''_\alpha \\ &\iff (\mathcal{M}_\varphi, w) \vDash \psi' \text{ и } (\mathcal{M}_\varphi, w) \vDash \psi'' \\ &\iff (\mathcal{M}_\varphi, w) \vDash \psi.\end{aligned}$$

Пусть $\psi = \psi' \vee \psi''$. Тогда для всякого $w \in W_\varphi$

$$\begin{aligned}(\mathcal{M}^*, w) \vDash \psi_\alpha &\iff (\mathcal{M}^*, w) \vDash \psi'_\alpha \text{ или } (\mathcal{M}^*, w) \vDash \psi''_\alpha \\ &\iff (\mathcal{M}_\varphi, w) \vDash \psi' \text{ или } (\mathcal{M}_\varphi, w) \vDash \psi'' \\ &\iff (\mathcal{M}_\varphi, w) \vDash \psi.\end{aligned}$$

Пусть $\psi = \psi' \to \psi''$. Если $(\mathcal{M}_\varphi, w) \nvDash \psi$, то в модели $\mathcal{M}_\varphi$ существует мир w', достижимый из w, такой, что $(\mathcal{M}_\varphi, w') \vDash \psi'$ и $(\mathcal{M}_\varphi, w') \nvDash \psi''$; но тогда $(\mathcal{M}^*, w') \vDash \psi'_\alpha$ и $(\mathcal{M}^*, w') \nvDash \psi''_\alpha$, а следовательно, $(\mathcal{M}^*, w) \nvDash \psi_\alpha$.

Пусть для некоторого $w \in W_\varphi$ имеет место отношение $(\mathcal{M}^*, w) \nvDash \psi_\alpha$. Тогда существует $w' \in W^*$ такой, что wR^*w', $(\mathcal{M}^*, w') \vDash \psi'_\alpha$ и $(\mathcal{M}^*, w') \nvDash \psi''_\alpha$. Заметим, что во всяком мире $u \in W$ уровня не выше $k + 6$ формулы $\alpha_1, \dots, \alpha_n$ истинны. Следовательно, во всяком таком мире будут истинны и все формулы, построенные из $\alpha_1, \dots, \alpha_n$ с помощью конъюнкции, дизъюнкции и импликации, в частности, во всяком таком мире должна быть истинной формула ψ''_α. Поскольку $(\mathcal{M}^*, w') \nvDash \psi''_\alpha$, то w' не может быть миром из множества W, и следовательно, $w' \in W_\varphi$. Тогда, применяя индукционное предположение, получаем, что $(\mathcal{M}_\varphi, w') \vDash \psi'_\alpha$ и $(\mathcal{M}_\varphi, w') \nvDash \psi''_\alpha$, и значит, $(\mathcal{M}_\varphi, w') \nvDash \psi_\alpha$.

Поскольку $(\mathcal{M}_\varphi, w_0) \nvDash \varphi$, то $(\mathcal{M}^*, w_0) \nvDash \varphi_\alpha$, т.е. $\varphi_\alpha \notin$ **Int**.

Определим функцию f, положив для всякой интуиционистской формулы φ

$$f(\varphi) = \varphi_\alpha.$$

Следующая теорема является следствием лемм 2 и 3.

Теорема 1. *Функция f является погружением* $\mathbf{Int}^+$ *в* $\mathbf{Int}(2)$.

Ввиду того, что **Int** погружается в $\mathbf{Int}^+$ [1], то из теоремы 1 следует

Теорема 2. *Существует погружение* **Int** *в* **Int**(2).

4. Некоторые следствия

Имея погружение **Int** в **Int**(2), получаем оценку сложности проблемы разрешения для **Int**(2).

Теорема 3. *Проблема разрешения* **Int**(2) *является* PSPACE-*полной.*

Доказательство. Тот факт, что эта проблема находится в классе PSPACE, следует из того, что в классе PSPACE находится проблема разрешения **Int**, а PSPACE-трудность проблемы разрешения **Int**(2) – из того, что к этой проблеме полиномиально сводится PSPACE-полная проблема, именно проблема разрешения $\mathbf{Int}^+$.

Описанную выше конструкцию можно модифицировать и построить погружение, аналогичное f, для некоторых суперинтуиционистских логик, отличных от **Int**. Мы покажем, как это сделать в случае логики слабого закона исключенного третьего **KC** = **Int** + $\neg p \vee \neg\neg p$. Положим

$$C_0 = \neg(p \wedge q); \qquad D_1 = p \to q \vee C_0;$$
$$D_2 = q \to p \vee C_0; \qquad D_3 = D_1 \vee D_2 \to p \vee q \vee C_0;$$
$$A_1^0 = D_2 \to D_1 \vee D_3; \qquad B_1^0 = D_1 \to D_2 \vee D_3;$$
$$A_2^0 = D_3 \to D_1 \vee D_2; \qquad B_2^0 = A_1^0 \wedge A_2^0 \wedge B_1^0 \to D_1 \vee D_2 \vee D_3;$$

$$A_1^1 = A_1^0 \wedge A_2^0 \to B_1^0 \vee B_2^0; \qquad B_1^1 = A_2^0 \wedge B_1^0 \to A_1^0 \vee B_2^0;$$
$$A_2^1 = A_1^0 \wedge B_1^0 \to A_2^0 \vee B_2^0; \qquad B_2^1 = A_2^0 \wedge B_2^0 \to A_1^0 \vee B_1^0;$$
$$A_3^1 = A_1^0 \wedge B_2^0 \to A_1^0 \vee B_1^0; \qquad B_3^1 = B_1^0 \wedge B_2^0 \to A_1^0 \vee A_2^0.$$

Если формулы $A_1^k, \dots, A_m^k$ и $B_1^k, \dots, B_m^k$, где $k \geqslant 1$, уже определены, то формулы $A_1^{k+1}, \dots, A_n^{k+1}$ и $B_1^{k+1}, \dots, B_n^{k+1}$, где $n = (m-1)^2$, определяются аналогично тому, как это описано выше:

$$A_s^{k+1} = A_1^k \to B_1^k \vee A_i^k \vee B_j^k; \qquad B_s^{k+1} = B_1^k \to A_1^k \vee A_i^k \vee B_j^k,$$

где $i, j \in \{2, \dots, m\}$.

Пусть

$$W^+ = W \cup \{c_0, d_1, d_2, d_3\},$$

а R^+ – рефлексивно-транзитивное замыкание следующего отношения R':

$$R' = \mathrm{R} \cup \{\langle d_1, c_0\rangle, \langle d_2, c_0\rangle, \langle d_3, c_0\rangle, \langle a_1^0, d_1\rangle, \langle a_2^0, d_1\rangle, \langle b_2^0, d_1\rangle,$$
$$\langle a_2^0, d_2\rangle, \langle b_1^0, d_2\rangle, \langle b_2^0, d_2\rangle, \langle a_1^0, d_3\rangle, \langle b_1^0, d_3\rangle, \langle b_2^0, d_3\rangle\}.$$

Положим $\mathcal{F}^+ = \langle W^+, R^+\rangle$, $\mathcal{M}^+ = \langle \mathcal{F}^+, v^+\rangle$, где оценка v определена следующим образом:

$$(\mathcal{M}^+, w) \models p \iff w = c_0 \text{ или } w = d_1;$$
$$(\mathcal{M}^+, w) \models q \iff w = c_0 \text{ или } w = d_2.$$

Для наглядности модель изображена на рис. 2.

Нетрудно убедиться, что имеют место следующие утверждения.

Лемма 4. *Пусть* w – *мир модели* $\mathcal{M}^+$. *Тогда*

$$(\mathcal{M}^+, w) \not\models C_0 \iff wRc_0;$$
$$(\mathcal{M}^+, w) \not\models D_i \iff wRd_i,\ 1 \leqslant i \leqslant 3.$$

Используя лемму 4, несложно доказать следующее утверждение; доказательство проводится аналогично доказательству леммы 1, и мы его опускаем.

Лемма 5. *Пусть* w – *мир модели* $\mathcal{M}^+$. *Тогда*

$$(\mathcal{M}^+, w) \not\models A_m^k \iff wRa_m^k;$$
$$(\mathcal{M}^+, w) \not\models B_m^k \iff wRb_m^k.$$

Обозначим через $\mathbf{KC}^+$ позитивный фрагмент логики $\mathbf{KC}$. Заменяя в рассуждениях выше формулы A_m^k и B_m^k их новыми вариантами, а вместо модели $\mathcal{M}$ рассматривая модель $\mathcal{M}^+$, с помощью леммы 5 несложно доказать справедливость следующего утверждения.

Теорема 4. *Существует погружение* $\mathbf{KC}^+$ *в* $\mathbf{KC}(2)$.

Поскольку проблема разрешения **KC**$^+$ является PSPACE-полной (доказательство аналогично доказательству PSPACE-полноты проблемы разрешения **Int**$^+$, см. [9]), то в качестве следствия получаем, что имеет место

Теорема 5. *Проблема разрешения* **KC**(2) *является* PSPACE-*полной.*

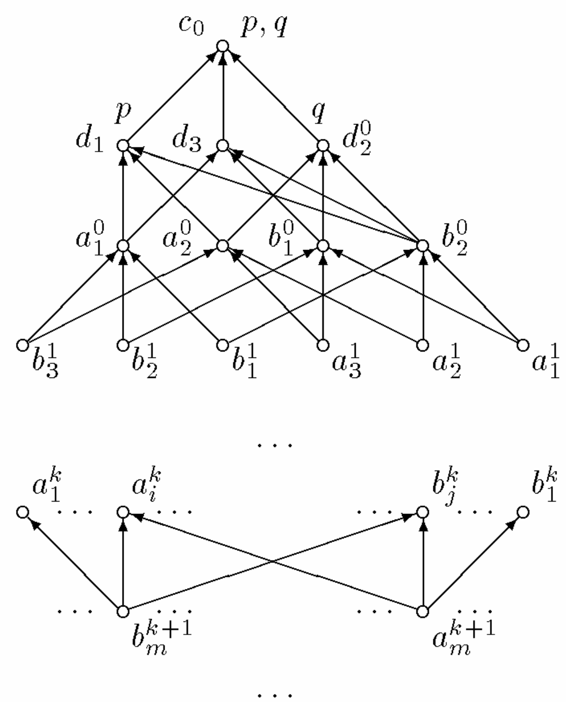

Рис. 2: Модель $\mathcal{M}^+$

Заметим, что новые формулы A_m^k и B_m^k можно бы было использовать и для построения погружения **Int**$^+$ в **Int**(2), поэтому на самом деле мы доказали более сильное утверждение. Для суперинуиционистской логики L обозначим через L^+ ее позитивный фрагмент. Тогда имеет место

Теорема 6. *Пусть* $L \in$ [**Int**, **KC**]. *Тогда существует погружение* L^+ *в* $L(2)$.

В качестве следствия теоремы 6 получаем следующее утверждение.

Теорема 7. *Пусть* $L \in$ [**Int**, **KC**]. *Тогда проблема разрешения для* $L(2)$ *является* PSPACE-*трудной.*

В заключение скажем несколько слов о функции сложности М.В. Захарьящева для $L(2)$, где $L \in$ [**Int**, **KC**]. Пусть L – некоторая логика (множество формул); функция сложности $f_L(n)$ определяется следующим образом (см. [4]):

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

где $|\mathcal{F}|$ – число миров шкалы $\mathcal{F}$.

Функция сложности М.В. Захарьящева – это, в некотором роде, еще одна мера сложности проблемы разрешения логики L. Имеется некоторая связь между функцией сложности и сложностью вычислений в смысле оценки затрат памяти и времени. Так, в известных случаях, когда логика L обладает PSPACE-полной проблемой разрешения, $f_L(n)$ тоже оказывается довольно «сложной», например, экспоненциальной в смысле оценки по порядку.

Используя формулы [9] и приведенную выше конструкцию, несложно показать, что справедлива

Теорема 8. *Пусть* $L \in$ [**Int**, **KC**]. *Тогда функция* $f_{L(2)}(n)$ *не может быть ограничена сверху никаким полиномом от* n.

ЛИТЕРАТУРА

1. *Попов В.М.* Погружение интуиционистского пропозиционального исчисления в его позитивный фрагмент // Логические исследования. Вып.8. М.: Наука, 2003. С. 150–154.
2. *Рыбаков М.Н., Чагров А.В.* Константные формулы в модальных логиках: проблема разрешения // Логические исследования. Вып.9. М.: Наука, 2003. С. 202–220.
3. *Чагров А.В.* О сложности пропозициональных логик // Сложностные проблемы математической логики. Калинин, 1985. С. 80–90.
4. *Chagrov A., Zakharyaschev M.* Modal Logic. Oxford University Press, 1997.
5. *Garey M.R., Johnson D.S.* Computers and Intractability: A Guide to the Theory of NP-completeness. San Francisco, 1979. (Русский перевод: *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982).
6. *Halpern J.Y.* The Effect of Bounding the Number of Primitive Propositions and the Depth of Nesting on the Complexity of Modal Logic // Artificial Intelligence. Vol. 75. 1995. P. 361–372.
7. *Nishimura I.* On formulas of the one variable in intuitionistic propositional calculus // The Journal of Symbolic Logic. Vol. 25. N. 1. 1960. P. 327–331.
8. *Spaan E.* Complexity of Modal Logics // PhD thesis. Department of Mathematics and Computer Science, University of Amsterdam, 1993.

9. *Statman R.* Intuitionistic propositional logic is polynomial-space complete // Theoret. Comput. Sci. Vol. 9. N. 1. 1979. P. 67–72.
10. *Stockmeyer L.* Classifying the Computational complexity of Problems // The Journal of Symbolic Logic. Vol. 52. N.1. 1987. P. 1–43. (Русский перевод: *Стокмейер Л.* Классификация вычислительной сложности проблем // Кибернетический сборник, вып. 26. М.: Мир, 1989. С. 20–83.)