М.Н.Рыбаков

СЛОЖНОСТЬ ПРОБЛЕМЫ РАЗРЕШЕНИЯ БАЗИСНОЙ И ФОРМАЛЬНОЙ ЛОГИК*

Abstract. *The complexity of decision problem for basic proposition logic* **BPL** *and formal proposition logic* **FPL** *is considered. It is proved that decision problem for positive fragments of both* **BPL** *and* **FPL** *is* PSPACE*-complete. The main result is that decision problem for variable-free fragment of* **BPL** *and one-variable fragment of* **FPL** *is PSPACE-complete.*

1. Введение

Базисная пропозициональная логика **BPL** и формальная пропозициональная логика **FPL** введены А. Виссером в [12] в виде секвенциальных исчислений. Формулы логик **BPL** и **FPL** строятся из (счетного множества) пропозициональных переменных и константы «ложь» с помощью конъюнкции, дизъюнкции и импликации. Из [12] следует, что логику **BPL** можно рассматривать как «суперинтуиционистский фрагмент» модальной логики **K4**, а логику **FPL** – как «суперинтуиционистский фрагмент» модальной логики **GL**, где под «суперинтуиционистским фрагментом» модальной логики понимается множество формул этой логики, которые являются результатами следующего T-перевода:

$$\begin{aligned}
\mathsf{T}(\bot) &= \Box\bot;\\
\mathsf{T}(p) &= \Box p;\\
\mathsf{T}(\varphi\wedge\psi) &= \mathsf{T}(\varphi)\wedge\mathsf{T}(\psi);\\
\mathsf{T}(\varphi\vee\psi) &= \mathsf{T}(\varphi)\vee\mathsf{T}(\psi);\\
\mathsf{T}(\varphi\to\psi) &= \Box(\mathsf{T}(\varphi)\to\mathsf{T}(\psi)).
\end{aligned}$$

(Таким образом, посредством T-перевода **BPL** связана с **K4**, а **FPL** с **GL** также же, как интуиционистская логика **Int** с **S4**.) В [12] для **BPL** и **FPL** строится реляционная семантика, близкая семантике Крипке для **Int**: разница состоит лишь в том, что при определении шкал и моделей Крипке нет требования рефлексивности миров (о семантике Крипке см., например, [4], [5]). В такой семантике **BPL** может быть определена как множество формул, истинных во всех шкалах Крипке с транзитивным отношением достижимости, а **FPL** – как множество формул, истинных во всех конечных шкалах

* Работа выполнена при поддержке РФФИ, грант № 03–06–80115.

Крипке с иррефлексивным транзитивным отношением достижимости [12].

Мы рассмотрим алгоритмические аспекты базисной и формальной логик. Прежде всего заметим, что обе эти логики разрешимы. Действительно, для того чтобы выяснить, принадлежит ли формула φ логике **BPL** или логике **FPL**, достаточно проверить, принадлежит ли $\mathsf{T}(\varphi)$ логике **K4** или, соответственно, логике **GL**, а проверка принадлежности логикам **K4** и **GL** может быть осуществлена эффективно в силу их разрешимости, см., например, [5].

Обратим внимание на тот факт, что разрешимость означает лишь принципиальную возможность уметь выяснять по формулам их принадлежность данным логикам, но реальные алгоритмы, решающие этот вопрос, могут оказаться довольно сложными. Так, например, проблема разрешения логик **K4** и **GL** является PSPACE-полной: она решается некоторым алгоритмом, затрачивающим полиномиальный объем памяти от длины тестируемой формулы, и к этой проблеме полиномиально сводится любая проблема из класса PSPACE (что следует, например, из конструкции, описанной в [8][1]), то же относится и к **Int** [10], а PSPACE-полные задачи считаются реально не решаемыми[2] (точные определения класса PSPACE, понятия PSPACE-полноты и т.п. можно найти в [6] и [11]).

Наша задача будет состоять как раз в том, чтобы описать сложность алгоритмов, разрешающих **BPL** и **FPL**. Мы покажем, что (*i*) проблема разрешения логик **BPL** и **FPL** PSPACE-полна (теорема 2), при этом из доказательства этого факта будет следовать, что (*ii*) проблема разрешения позитивных фрагментов **BPL** и **FPL** PSPACE-полна (теорема 3); затем мы построим погружение позитивного фрагмента логики **BPL** в ее фрагмент, состоящий из константных формул, и погружение позитивного фрагмента логики **FPL** в ее фрагмент, состоящий из формул от одной переменной, в результате чего сможем доказать, что (*iii*) проблема разрешения константного фрагмента **BPL** и проблема разрешения фрагмента **FPL**, состоящего из формул от одной переменной, являются PSPACE-полными (теорема 5).

---

[1] В [8] рассматриваются логики **K**, **T** и **S4**, но доказательство PSPACE-полноты проблемы разрешения этих логик легко переносится на случай **K4** и **GL**.

[2] На данный момент известны только так называемые переборные алгоритмы, решающие PSPACE-полные задачи, время работы которых не ограничено ни одним полиномом от длины тестируемой формулы, при этом вопрос о существовании (даже недетерминированных!) алгоритмов, решающих PSPACE-полные задачи за полиномиальное время, открыт.

2. Сложность проблемы разрешения BPL и FPL

Мы будем пользоваться тем фактом, что проблема выполнимости булевых формул с кванторами является PSPACE-полной, при этом без ограничений общности можем рассматривать только формулы вида

$$\varphi \;=\; Q_1 p_1 \ldots Q_n p_n \bigwedge_{k=1}^{m} \Big(\bigvee_{i \in I_k}^{n+1} p_i \;\vee\; \bigvee_{i \in J_k}^{n+1} \neg p_i \Big), \qquad (*)$$

где $Q_1, \ldots, Q_n \in \{\forall, \exists\}$, $I_k, J_k \in \{1, \ldots, n\}$, $I_k \cap J_k = \varnothing$, см. [6], [11]. Опишем, как булевой формуле с кванторами φ сопоставить формулу φ^*, которая эффективно строится по φ за время, ограниченное некоторым полиномом от длины φ, и такую, что

$$\begin{aligned} \varphi \text{ истинна} \quad &\Leftrightarrow \quad \varphi^* \notin \mathbf{BPL} \\ &\Leftrightarrow \quad \varphi^* \notin \mathbf{FPL}. \end{aligned}$$

Формула φ^* в определенном смысле будет описывать условие истинности формулы φ[3].

Начнем построение φ^* с того, что опишем «раскрытие» кванторов; для этого нам понадобятся формулы

$$\begin{aligned} A(s_1,s_2,s_3,s_4,s_5) \;&=\; (s_1 \wedge s_2 \to s_3) \wedge (s_1 \wedge s_2 \to s_4) \wedge (s_1 \to s_5) \wedge (s_2 \to s_5) \to (\top \to s_5), \\ E(s_1,s_2,s_3,s_4,s_5) \;&=\; (s_1 \wedge s_2 \to s_3) \wedge (s_1 \wedge s_2 \to s_4) \wedge (s_1 \wedge s_2 \to s_5) \to (\top \to s_5), \end{aligned}$$

где $\top = p \to p$ для некоторой фиксированной переменной p. Каждую переменную p_i мы промоделируем с помощью двух формул: $t_i = q_i \to r_i$ и $f_i = r_i \to q_i$. Подразумеваемое значение этих формул следующее: если переменная q_i истинна, а r_i опровергается, то переменная p_i принимает значение «истина», а если наоборот, то p_i принимает значение «ложь».

Предположим теперь, что формула $A(t_i, f_i, t_{i+1}, f_{i+1}, s)$ опровергается в некотором мире a модели Крипке логики **BPL** или логики **FPL**. Тогда из a должен быть достижим мир b, из которого должен быть достижим мир c, в котором опровергается s, при этом в мире b должны быть истинны формулы $(t_i \to s)$ и $(f_i \to s)$. Следовательно, из c должны быть достижимы два (различных!) мира, скажем, d_1 и d_2, в первом из которых истинна переменная q_i и опровергается переменная r_i, а во втором – истинна r_i и опровергается q_i, что, согласно подразумеваемому смыслу формул t_i и f_i, вынуждает нас рассматривать обе возможные оценки для переменной p_i. При этом первый и второй конъюнктивные члены формулы $A(t_i, f_i, t_{i+1}, f_{i+1}, s)$ обеспечивают сохранение оценки q_i и r_i в мирах,

[3] Идея построения φ^* взята из [5].

достижимых из d_1 и d_2. Если же в некотором мире a опровергается формула $E(t_i, f_i, t_{i+1}, f_{i+1}, s)$, то возникает аналогичная ситуация с той разницей, что вместо миров d_1 и d_2 должен существовать некоторый мир d, в котором либо q_i истинно и r_i опровергается, либо r_i истинно и q_i опровергается.

Каждой кванторной приставке $Q_1p_1\ldots Q_kp_k$ сопоставим формулу ψ_k следующим образом (ниже s – некоторая пропозициональная переменная, отличная от q_i и r_i):

если $Q_1 = \forall$, то $\psi_1 = A(t_1, f_1, t_2, f_2, s)$;

если $Q_1 = \exists$, то $\psi_1 = E(t_1, f_1, t_2, f_2, s)$;

если $Q_k = \forall$, то

$$\psi_k = [A(t_k, f_k, t_{k+1}, f_{k+1}, t_{k-1}) \to (\top \to t_{k-1})] \wedge \\ \wedge [A(t_k, f_k, t_{k+1}, f_{k+1}, f_{k-1}) \to (\top \to f_{k-1})] \to \psi_{k-1};$$

если $Q_k = \exists$, то

$$\psi_k = [E(t_k, f_k, t_{k+1}, f_{k+1}, t_{k-1}) \to (\top \to t_{k-1})] \wedge \\ \wedge [E(t_k, f_k, t_{k+1}, f_{k+1}, f_{k-1}) \to (\top \to f_{k-1})] \to \psi_{k-1}.$$

Теперь положим

$$\varphi^* = \Big(\bigvee_{k=1}^{m} \Big(\bigwedge_{i \in I_k}^{n+1} t_i \vee \bigwedge_{i \in J_k}^{n+1} f_i\Big) \to t_n \wedge f_n\Big) \to \psi_n.$$

Нетрудно видеть, что длина формулы φ^* может быть ограничена линейной функцией от длины формулы φ, а поэтому и на выписывание формулы φ^* по формуле φ потребуется время, ограниченное полиномом от длины φ, кроме того, опровержимость формулы φ^* в некотором мире некоторой модели логики **BPL** или логики **FPL** означает следующее: если последовательно «раскрыть» кванторы формулы φ, то выражение, стоящее в φ за кванторной приставкой, истинно. Более точно, верно следующее утверждение.

Лемма 1. *Для всякой булевой формулы с кванторами φ вида* (∗) *имеют место следующие эквивалентности:*

$$\varphi \text{ истинна} \quad \Leftrightarrow \quad \varphi^* \notin \mathbf{BPL} \\ \Leftrightarrow \quad \varphi^* \notin \mathbf{FPL},$$

при этом формула φ^* эффективно строится по φ за полиномиальное время от длины φ.

Теорема 2. *Проблема разрешения логик* **BPL** *и* **FPL** *является* PSPACE-*полной.*

Доказательство. Проблема разрешения логик **BPL** и **FPL** находится в классе PSPACE, поскольку с помощью T-перевода она полиномиально сводится к проблеме разрешения логик **K4** и **GL** соответственно, а как отмечалось выше, проблема разрешения **K4**

и **GL** является PSPACE-полной, в частности, находится в классе PSPACE. Кроме того, любая проблема из класса PSPACE полиномиально сводима к проблеме выполнимости булевых формул с кванторами (в силу PSPACE-полноты последней), а проблема выполнимости булевых формул с кванторами в силу леммы 1 полиномиально сводима к проблеме разрешения **BPL** и **FPL**, что и завершает доказательство.

Обозначим через $\mathbf{BPL}^+$ и $\mathbf{FPL}^+$ позитивные фрагменты логик **BPL** и **FPL** соответственно, т.е. множества формул этих логик, построенных без использования константы «ложь». Поскольку при выписывании формулы φ^* константа «ложь» не использовалась, то мы на самом деле доказали более сильное утверждение, чем теорема 2.

Теорема 3. *Проблема разрешения фрагментов* $\mathbf{BPL}^+$ *и* $\mathbf{FPL}^+$ *является* PSPACE*-полной.*

Теперь обратимся к вопросу о сложности разрешения фрагментов **BPL** и **FPL**, состоящим из формул, построенных в языке с конечным числом переменных. В [1] была высказана гипотеза о том, что проблема разрешения фрагмента **BPL** является PSPACE-полной уже в том случае, когда в языке имеются всего две пропозициональные переменные. Как было сказано во введении, мы докажем даже более сильное утверждение. Но для этого нам потребуется некоторый технический факт, который, кстати, представляется интересным сам по себе.

Введем следующее обозначение. Для всякого множества формул L через $L(n)$ обозначим множество тех формул из L, в построении которых помимо связок участвуют только константа «ложь» и переменные $p_1, \ldots, p_n$.

3. Погружение $\mathbf{BPL}^+$ в $\mathbf{BPL}(0)$ и $\mathbf{FPL}^+$ в $\mathbf{FPL}(1)$

Идея погружения, которое будет описано ниже, взята из [7] и уже использовалась автором в совместных работах с А.В. Чагровым при доказательстве близких результатов для модальных логик: см. [1], [2], [3]. При получении аналогичных результатов для **BPL** и **FPL** придется, конечно, учитывать специфику «интуиционистского»[4] случая.

Идея, собственно, состоит в том, чтобы заменить все переменные в рассматриваемой формуле формулами (константными в

[4] С одной стороны, семантика рассматриваемых логик близка к семантике **Int**, но с другой стороны, логика **FPL** не является ни подлогикой, ни расширением **Int** (хотя **BPL** как множество формул включается в **Int**).

случае **BPL** и зависящими от одной переменной в случае **FPL**), которые могут рассматриваться как переменные: каждую из них можно, определенным образом изменив модель, опровергнуть или сделать истинной в рассматриваемом мире независимо от истинности в этом мире остальных построенных формул.

Введем следующее сокращение. Для всякой формулы ψ обозначим через $?\psi$ формулу $\top \to \psi$. Для всякого $n \geqslant 1$ положим

$$\alpha_n = (?^{n+2}\bot \to ?^{n+1}\bot) \to (?^{n+1}\bot \to ?^{n}\bot) \vee ?^{n+2}\bot;$$
$$\beta_n = ?^{2}p \to (?^{n+1}\bot \to ?^{n}\bot \vee p).$$

Пусть φ – произвольная формула, не содержащая константы «ложь», и пусть $p_1, \ldots, p_n$ – все переменные, входящие в φ. Обозначим через φ_α формулу, получающуюся из φ заменой каждого вхождения переменной p_i на α_i, а через φ_β – формулу, получающуюся из φ заменой каждого вхождения переменной p_i на β_i.

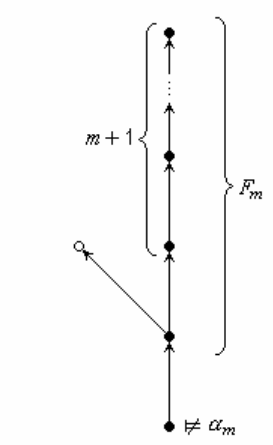

Рис. 1

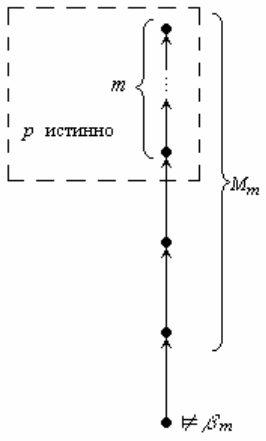

Рис. 2

Заметим, что для того чтобы в некотором мире опровергалась формула α_m, достаточно, чтобы из него была достижима шкала F_m (т.е. нижний мир F_m), изображенная на рис. 1, а для того чтобы в некотором мире опровергалась формула β_m, достаточно, чтобы из него была достижима модель M_m, изображенная на рис. 2 (черные кружки соответствуют иррефлексивным мирам, а светлые – рефлексивным). При этом несложно убедиться, что истинность формул α_k и β_k, где $k \neq m$, не зависит от того, достижимы ли из данного мира модели указанного вида, опровергающие α_m и β_m соот-

ветственно. Это наблюдение позволяет обосновать следующее утверждение.

Лемма 4. *Пусть* φ *– формула, не содержащая константы «ложь». Тогда имеют место следующие эквивалентности:*

$$\varphi \in \mathbf{BPL}^{+} \quad \Leftrightarrow \quad \varphi_{\alpha} \in \mathbf{BPL}(0);$$
$$\varphi \in \mathbf{FPL}^{+} \quad \Leftrightarrow \quad \varphi_{\beta} \in \mathbf{FPL}(1).$$

4. Сложность разрешения BPL(m) и FPL(m)

Заметим, что длина формул α_k и β_k, где $k \geqslant n$, ограничена некоторой линейной функцией от n, а n в свою очередь не превосходит длины φ. Следовательно, длина формул φ_{α} и φ_{β} может быть ограничена квадратичным полиномом от длины φ, из чего легко заключить, что φ_{α} и φ_{β} эффективно строятся по φ с помощью алгоритма, время работы которого ограничено некоторым полиномом от длины φ. Таким образом, проблема разрешения $\mathbf{BPL}^{+}$ и $\mathbf{FPL}^{+}$ полиномиально сводится к проблеме разрешения **BPL**(0) и **FPL**(1) соответственно, и тем самым нами доказана

Теорема 5. *Для всякого* $m \geqslant 0$ *проблема разрешения* **BPL**(m) *и* **FPL**($m + 1$) *является* PSPACE*-полной.*

Остается вопрос о сложности проблемы разрешения **FPL**(0), но ответ на него почти очевиден. В [1] доказано, что фрагмент **GL**(0) разрешим полиномиально по времени, а **FPL**(0) погружается в **GL**(0) с помощью T-перевода, причем $\mathsf{T}(\varphi)$ вычисляется по φ за полиномиальное время от длины φ. Поэтому имеет место

Теорема 6. *Фрагмент* **FPL**(0) *разрешим с помощью алгоритма, время работы которого ограничено полиномом от длины проверяемой формулы.*

5. Сложность разрешения Int(m)

Получив оценки сложности проблемы разрешения **BPL**(m) и **FPL**(m), трудно ничего не сказать о сложности проблемы разрешения **Int**(m). Как уже было сказано выше, проблема разрешения **Int** является PSPACE-полной [10]. Тем не менее, имеется алгоритм, основанный на «лестнице» И. Нишимуры [9], разрешающий **Int**(1) за полиномиальное время. Что касается **Int**(m) для $m > 1$, то имеют место следующие факты.

Лемма 7. *Для всякой булевой формулы с кванторами* φ *вида* (∗) *имеют место следующие эквивалентности:*

$$\varphi \text{ истинна} \quad \Leftrightarrow \quad \varphi^{*} \notin \mathbf{Int}.$$

Обозначим через $\mathbf{Int}^+$ позитивный фрагмент логики **Int**. Из леммы 7 вытекает

Теорема 8 [10]**.** *Проблема разрешения* $\mathbf{Int}^+$ *является* PSPACE-*полной.*

Лемма 9. *Существует погружение* $\mathbf{Int}^+$ *в* **Int**(2)*, которое вычислимо с помощью некоторого алгоритма, время работы которого ограничено полиномом от длины подаваемой на вход формулы.*

Построение такого погружения $\mathbf{Int}^+$ в **Int**(2) основано на той же идее, что и построение погружения $\mathbf{BPL}^+$ в **BPL**(0), а также $\mathbf{FPL}^+$ в **FPL**(1), но требует значительно больше технических выкладок, что, к сожалению, не позволяет привести его в рамках данной работы.

Из леммы 9 и PSPACE-полноты проблемы разрешимости **Int** и $\mathbf{Int}^+$ вытекает

Теорема 10. *Для всякого* $m \geqslant 2$ *проблема разрешения* **Int**(m) *является* PSPACE-*полной.*

ЛИТЕРАТУРА

1. *Рыбаков М.Н., Чагров А.В.* Константные формулы в модальных логиках: проблема разрешения // Логические исследования. Вып.9. М.: Наука, 2003.
2. *Рыбаков М.Н., Чагров А.В.* Модальные формулы без переменных и PSPACE-полнота // Современная логика: Проблемы теории, истории и применения в науке. Материалы VII Международной научной конференции. СПб: Издательство Санкт-Петербургского университета. 2002. С. 498–500.
3. *Рыбаков М.Н., Чагров А.В.* О сложности модальных логик, имеющих доказуемостную интерпретацию, с ограничениями на число переменных // Колмогоров и современная математика. Международная конференция. М.: Издательство МГУ, 2003. С. 707–708.
4. Семантика модальных и интенсиональных логик // Пер. с англ., сост., общ. ред. и вступит. статья В.А. Смирнова. М.: Прогресс, 1981.
5. *Chagrov A., Zakharyaschev M.* Modal Logic. Oxford University Press, 1997.
6. *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).
7. *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.
8. *Ladner R.E.* The computational complexity of provability in systems of modal logic // SIAM Journal on Computing. Vol. 6. 1977. P. 467–480.

9. *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.
10. *Statman R.*. Intuitionistic propositional logic is polynomial-space complete // Theoret. Comput. Sci. Vol. 9. N. 1. 1979. P. 67–72.
11. *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.)
12. *Visser A.* A Propositional Logic with Explicit Fixed Points // Studia Logica. Vol. 40. 1981. P. 155–175.