ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ

УДК 510.675, 510.531

НЕРАЗРЕШИМОСТЬ ПРОБЛЕМЫ ОПРЕДЕЛЕННОСТИ БИНАРНЫХ IFP-ОПЕРАТОРОВ ДЛЯ ТЕОРИИ ОДНОГО СЛЕДОВАНИЯ[1]

Дудаков С.М.
Кафедра информатики

Поступила в редакцию 12.12.2014, после переработки 19.12.2014.

В работе продолжается исследование определенности оператора инфляционной фиксированной точки. Показано, что проблема определенности бинарного IFP-оператора для теории следования алгоритмически неразрешима.

Ключевые слова: инфляционная фиксированная точка, неразрешимость, теория одной функции следования.

Вестник ТвГУ. Серия: Прикладная математика. 2014. № 4. С. 7–15.

Введение

Мы продолжаем исследование проблем, связанных с изучением итеративных операторов (см. [6]). Ранее в [15,16] нами найдены некоторые условия, при которых IFP-оператор гарантированно определен. Некоторые результаты по разрешимости теорий с оператором транзитивного замыкания получены в [17].

Важность изучения подобных задач проистекает из того, что логические языки широко применяются в системах управления базами данных, что восходит к Кодду [4, 5]. Хорошо известно, возможности языков первого порядка ограничены [1, 3, 12]. Обогащение таких языков с помощью внешних отношений [2, 19] универсума – реализованная возможность. Однако, несмотря на значительные усилия по исследованиям в данной области, «положительные» результаты весьма скромны. Известно, что увеличения выразительной силы можно добиться с использованием линейного порядка (Ю.Гуревич, см. [12]), автоматных систем (см. [11]), упорядоченного случайного графа (см. [10, 14]). Расширение выразительных возможностей в первых двух случаях очень специфично, формулы, его иллюстрирующие, весьма искусственны. Вариант со случайным графом более перспективен, но и здесь выразительные возможности довольно ограничены, например, только регулярными языками (см., например, [7–9, 13] и обзор в [12]).

Таким образом, применение операторов, выводящих за пределы логики первого порядка, является весьма естественным приемом, который позволяет выразить

[1]Работа выполнена при финансовой поддержке РФФИ, гранты № 13-01-00382 и № 13-01-00643.

больше. Так, например, в [6] показано, что на упорядоченных конечных системах с помощью IFP-оператора можно выразить в точности свойства, вычислимые за полиномиальное время. В [18] аналогично показывается соответствие логики с оператором транзитивного замыкания с множеством свойств, проверяемых в логарифмической памяти недетерминированными алгоритмами.

В настоящей работе мы рассматриваем саму задачу выяснения определенности IFP-оператора для формулы первого порядка в теории следования. Конечно, при многократном применении IFP-оператора такая задача неразрешима, так как с помощью инфляционной фиксированной точки можно поочередно построить операции сложения и умножения. Возникает вопрос: что можно сказать про однократное применение данного оператора? Мы показываем, что для бинарных IFP-операторов данная задача остается алгоритмически неразрешимой.

1. Инфляционная фиксированная точка

Мы используем обычные определения формулы логики первого порядка и ее значения (см., например, [20]). Строка $\varphi(\bar{x})$ означает, что формула φ не содержит никаких свободных переменных, кроме, может быть, $\bar{x}$. В этом случае строка $\varphi(\bar{t})$ означает результат замены переменных $\bar{x}$ термами $\bar{t}$ соответственно. Если $\mathfrak{A}$ – алгебраическая система, а $\bar{a} \in |\mathfrak{A}|$ – набор элементов ее носителя, то $\varphi(\bar{a})$ – это значение формулы φ, когда значения переменных $\bar{x}$ равны $\bar{a}$ соответственно.

Мы рассматриваем обогащение языка логики первого порядка оператором инфляционной фиксированной точки.

Определение 1 (см. [6]). *Формулой* IFP*-логики называется формула, построенная по правилам логики первого порядка, а также с помощью оператора инфляционной фиксированной точки* IFP*: если $\varphi(\bar{x}, \bar{y})$ – формула со свободными переменными $\bar{x}$ и $\bar{y}$, содержащая несигнатурный предикатный символ Q (местность Q должна совпадать с длиной набора $\bar{y}$, будем называть ее* **местностью** IFP**-оператора***), то* $\mathrm{IFP}_{Q(\bar{y})}(\varphi)$ *– формула исходной сигнатуры со свободными переменными $\bar{x}$ и $\bar{y}$.*

Семантика атомных формул, булевых связок и кванторов определяется как в логике первого порядка.

Определение 2 (см. [6]). *Пусть $\mathfrak{A}$ – это алгебраическая система, $\varphi(\bar{x}, \bar{y})$ – формула, с новым предикатным символом Q. Зафиксируем значение переменных $\bar{x}$ – $\bar{a} \in |\mathfrak{A}|$.* **Инфляционной фиксированной точкой** $\mathrm{IFP}_{Q(\bar{y})}(\varphi)(\bar{a})$ *называется множество $Q_*^{\bar{a}}$, построенное следующим образом. Пусть*

$$Q_0^{\bar{a}} = \varnothing; \quad Q_{i+1}^{\bar{a}} = Q_i^{\bar{a}} \cup \{\bar{y} \in |\mathfrak{A}| : (\mathfrak{A}, Q_i^{\bar{a}}) \models \varphi(\bar{a}, \bar{y})\}, \tag{1}$$

для $i \in \omega$.

Если $Q_n^{\bar{a}} = Q_{n+1}^{\bar{a}}$ для некоторого $n \in \omega$, то полагаем $Q_*^{\bar{a}} = Q_n^{\bar{a}}$. Наименьшее n, удовлетворяющее такому условию, назовем **степенью** *оператора* $\mathrm{IFP}_{Q(\bar{y})}(\varphi)(\bar{a})$. *В этом случае считаем формулу* $\mathrm{IFP}_{Q(\bar{y})}(\varphi)(\bar{a}, \bar{y})$ *истинной, если $\bar{y} \in Q_*^{\bar{a}}$, и ложной, при $\bar{y} \notin Q_*^{\bar{a}}$.*

Если указанного числа n не существует, то считаем, что значение оператора $\mathrm{IFP}_{Q(\bar{y})}(\varphi)(\bar{a})$ *(и формулы* $\mathrm{IFP}_{Q(\bar{y})}(\varphi)(\bar{a}, \bar{y})$*)* **неопределено**.

2. Алгоритмическая неразрешимость проблемы IFP-определенности

Мы рассмотрим задачу IFP-определенности для моделей одной из простейших теорий – теории одной функции следования. Как известно, эта теория разрешима, допускает эффективную элиминацию кванторов в исходной сигнатуре [20]. Тем не менее даже для нее задача IFP-определенности оказывается неразрешимой.

Сама проблема IFP-*определенности* формулируется так: по формуле $\mathrm{IFP}_{Q(\bar{x})}\,\varphi$ и значению переменных $\bar{y}$, отличных от $\bar{x}$, выяснить, определено ли значение этой формулы.

Теорема 1. *В теории одной функции следования задача определенности бинарного* IFP-*оператора для формул первого порядка алгоритмически неразрешима.*

Доказательство. Напомним [21], что машиной Минского называется автомат, конфигурация которого в каждый момент времени является тройкой (q, c_1, c_2), где q – состояние машины, c_1 и c_2 – натуральные числа, значения первого и второго счетчиков соответственно. Машина Минского может выполнять команды двух видов:

$$«q \to \mathrm{inc}_i, p» \quad \text{и} \quad «q \to \mathrm{dec}_i, p : r».$$

Первая из них означает, что машина в состоянии q увеличивает на единицу счетчик номер i, после чего переходит в состояние p. Вторая означает, что машина в состоянии q пытается уменьшить на единицу счетчик номер i. Если значение счетчика i было больше 0, то после уменьшения машина переходит в состояние p, а если значение счетчика уже было равно 0, то оно не меняется, но следующим состоянием будет r. Машина называется детерминированной, если для каждого состояния существует не более одной команды. Если команды для текущего состояния нет, то машина останавливается.

Проблема остановки заключается в том, чтобы по начальному состоянию и значению счетчиков определить, остановится ли машина. Как известно [21], существует детерминированная машина Минского $\mathfrak{M}$ с двумя счетчиками, для которой проблема остановки неразрешима. Мы будем считать, что такая машина $\mathfrak{M}$ зафиксирована, а ее состояния пронумерованы: $q_0, q_1, \ldots, q_N$.

Покажем, что проблема остановки для машины $\mathfrak{M}$ может быть сведена к проблеме определенности некоторого IFP-оператора в теории одной функции следования. Будем считать, что сигнатура включает один символ константы 0, означающий начальный элемент, и один одноместный функциональный символ $+1$, означающий функцию следования, то есть должны выполняться следующие аксиомы:

$$(\forall x)x + 1 \neq 0; \quad (\forall x)(\forall y)(x + 1 = y + 1 \to x = y);$$
$$(\forall x)(\exists y)(x \neq 0 \to y + 1 = x).$$

Для краткости мы будем обозначать с помощью $s + k$ результат k применений функции $+1$ к s:

$$s \underbrace{+1 + 1 + \cdots + 1}_{k \text{ раз}}.$$

Символ 0 в начале терма будем опускать, то есть k – сокращение для $0 + k$.

Основная идея сведения будет заключаться в том, что конфигурация (q_n, c_1, c_2) машины $\mathfrak{M}$ в момент времени t будет соответствовать истинности $Q_T(3t, n)$, $Q_T(3t+1, c_1)$, $Q_T(3t+2, c_2)$ для всех $T > t$.

Сначала для каждого состояния q_n определим формулу $\varphi_n(u', x', u)$, описывающую построение Q_{t+1} по Q_t. Если в программе машины $\mathfrak{M}$ присутствует команда $q_n \to \mathrm{inc}_1, q_m$, то формула $\varphi_n(u', x', u)$ будет иметь вид:

$$u' = u + 3 \wedge x' = m \vee (\exists x)(Q(u+1, x) \wedge u' = u + 3 + 1 \wedge x' = x + 1) \vee \\ \vee (\exists x)(Q(u+2, x) \wedge u' = u + 3 + 2 \wedge x' = x). \qquad (2)$$

Для команды $q_n \to \mathrm{inc}_2, q_m$ формула $\varphi_n(u', x', u)$ строится симметрично:

$$u' = u + 3 \wedge x' = m \vee (\exists x)(Q(u+1, x) \wedge u' = u + 3 + 1 \wedge x' = x) \vee \\ \vee (\exists x)(Q(u+2, x) \wedge u' = u + 3 + 2 \wedge x' = x + 1). \qquad (3)$$

Рассмотрим теперь построение формулы $\varphi_n(u', x', u)$ для команды декремента $q_n \to \mathrm{dec}_1, q_{m_1} : q_{m_2}$:

$$(\exists x)Q(u+1, x+1) \wedge u' = u + 3 \wedge x' = m_1 \vee \\ \vee (\exists x)Q(u+1, 0) \wedge u' = u + 3 \wedge x = m_2 \vee \\ \vee (\exists x)(Q(u+1, x+1) \wedge u' = u + 3 + 1 \wedge x' = x) \vee \\ \vee (\exists x)(Q(u+1, 0) \wedge u' = u + 3 + 1 \wedge x' = 0) \vee \\ \vee (\exists x)(Q(u+2, x) \wedge u' = u + 3 + 2 \wedge x' = x), \qquad (4)$$

и аналогично для $q_n \to \mathrm{dec}_2, q_{m_1} : q_{m_2}$:

$$(\exists x)Q(u+2, x+1) \wedge u' = u + 3 \wedge x' = m_1 \vee \\ \vee (\exists x)Q(u+2, 0) \wedge u' = u + 3 \wedge x' = m_2 \vee \\ \vee (\exists x)(Q(u+1, x) \wedge u' = u + 3 + 1 \wedge x' = x) \vee \\ \vee (\exists x)(Q(u+2, x+1) \wedge u' = u + 3 + 2 \wedge x' = x) \vee \\ \vee (\exists x)(Q(u+2, 0) \wedge u' = u + 3 + 2 \wedge x' = 0). \qquad (5)$$

Теперь построим всю формулу $\varphi(u', x')$ целиком:

$$(\exists u)\Big(\underbrace{(\exists x)Q(u+2, x) \wedge \neg(\exists x)Q(u+3, x)}_{(a)} \wedge \bigvee_{n=0}^{N} \big(Q(u, 0+n) \wedge \varphi_n(u', x', u)\big)\Big). \qquad (6)$$

Наконец, по начальной конфигурации (q_{n_0}, d_1, d_2) машины $\mathfrak{M}$ построим всю формулу:

$$\mathrm{IFP}_{Q(u',x')}\big((u' = 0 \wedge x' = n_0) \vee \\ \vee (u' = 1 \wedge x' = d_1) \vee) u' = 2 \wedge x' = d_2) \vee \varphi(u', x')\big). \qquad (7)$$

Покажем, что значение IFP-оператора (7) определено тогда и только тогда, когда машина $\mathfrak{M}$ останавливается на начальной конфигурации (q_{n_0}, d_1, d_2).

Сначала индукцией по t, $t > 0$, покажем такое утверждение:

для каждого $j < t$ существуют и единственны n, c_1 и c_2, для которых выполнено

$$Q_t(3j, n), \quad Q_t(3j+1, c_1), \quad Q_t(3j+2, c_2),$$

причем конфигурация машины $\mathfrak{M}$ в момент времени j есть в точности (q_n, c_1, c_2). При $j \geq 3t$ формулы вида $Q_t(j, x)$ ложны для всех x.

Прежде всего отметим, что формула $\varphi(u', x', u)$ может быть истинна только при непустом Q, поэтому при построении Q_1 она будет ложной: $Q_0 = \varnothing$. Значит, истинность формул

$$Q_1(0, n), \quad Q_1(1, c_1), \quad Q_1(2, c_2)$$

может означать только то, что соответствующие кортежи получены с помощью формулы

$$(u' = 0 \wedge x' = n_0) \vee (u' = 1 \wedge x' = d_1) \vee (u' = 2 \wedge x' = d_2).$$

Это и означает $n = n_0$, $c_1 = d_1$, $c_2 = d_2$. Обратно, если в момент времени 0 мы имеем конфигурацию (q_{n_0}, d_1, d_2), то для Q_1 обязательно будет выполняться

$$Q_1(0, n_0), \quad Q_1(1, d_1), \quad Q_1(2, d_2).$$

Теперь предположим, что утверждение для t уже доказано. Рассмотрим новые кортежи, которые добавлены в Q_{t+1}. Очевидно, что они могут быть добавлены только с помощью формулы $\varphi(u', x')$. Если выполнено (a) в формуле (6), то это означает, что $u = 3(t-1)$. Чтобы вся формула (6) была истинной, нужно чтобы был выполнен один из элементов дизъюнкции. Заметим, что два одновременно выполнены быть не могут в силу индукционного предположения. Предположим, выполнено $Q(u, 0+n) \wedge \varphi_n(u', x', u)$. По индукционному предположению из $Q_t(3(t-1), n)$ вытекает, что машина $\mathfrak{M}$ в момент $t-1$ находится в состоянии n.

Пусть командой для состояния q_n является $q_n \to \mathrm{inc}_1, q_m$. Тогда следующей за (q_n, c_1, c_2) конфигурацией является (q_m, c_1+1, c_2). Из формулы (2) вытекает, что $\varphi_n(u', x', u)$ может быть истинна в следующих трех случаях: $u' = u+3$ и $x' = m$, $u' = u+3+1$ и $x' = c_1+1$, $u' = u+3+2$ и $x' = c_2$. Это означает, что к Q_{t+1} будут добавлены три новых кортежа:

$$(3t, m), \quad (3t+1, c_1+1), \quad (3t+2, c_2),$$

что соответствует утверждению для $t+1$.

Если команда для состояния q_n была $q_n \to \mathrm{dec}_1, q_{m_1} : q_{m_2}$ и $c_1 > 0$, то следующая конфигурация – (q_{m_1}, c_1-1, c_2). Из формулы (4) получаем, что $\varphi_n(u', x', u)$ может быть истинна в следующих трех случаях: $u' = u+3$ и $x' = m_1$, $u' = u+3+1$ и $x' = c_1-1$, $u' = u+3+2$ и $x' = c_2$, что снова согласуется со следующей конфигурацией.

Наконец, если для той же команды выполнено $c_1 = 0$, то $\varphi_n(u', x', u)$ может быть истинна в следующих трех случаях: $u' = u+3$ и $x' = m_2$, $u' = u+3+1$ и $x' = c_1$, $u' = u+3+2$ и $x' = c_2$, что опять совпадает со следующей конфигурацией – (q_{m_2}, c_1, c_2).

Команды для счетчика 2 рассматриваются аналогично с помощью формул (3) и (5).

Предположим, что машина $\mathfrak{M}$ останавливается при работе на начальной конфигурации (q_{n_0}, d_1, d_2). Тогда существует момент времени t, в котором конфигурация машины $\mathfrak{M}$ примет вид (q_n, c_1, c_2) и команды для состояния q_n не будет. Но тогда при построении $t+2$ ни одного нового кортежа не будет добавлено в Q (дизъюнкция в формуле (6) не будет содержать ни одного истинного элемента), следовательно, $Q_{t+1} = Q_{t+2}$ поэтому значение оператора (7) определено. Если машина $\mathfrak{M}$ не останавливается, то кортежи будут добавляться на каждом шаге, поэтому процесс никогда не остановится и значение оператора (7) неопределено. $\square$

Заключение

В связи с полученными нами результатами естественно возникает несколько вопросов. Во-первых, распространяется ли результат о неразрешимости проблемы определенности в теории одной функции следования на унарные IFP-операторы. Возможно, что как и во многих других задачах логики, ограничение на унарный случай делает задачу проще.

Второй вопрос связан с тем, что полученный в работе результат легко обобщить на произвольные теории, в которых существует формула $\varphi(\bar{x}, \bar{y})$, задающая граф со сколь угодно длинными путями без циклов. Вопрос состоит в том, какую местность в этом случае должен иметь неопределенный IFP-оператор? В другом виде эту задачу можно сформулировать так: вытекает ли из определенности всех n-местных (например, унарных) IFP-операторов в полной теории T определенность всех $n+1$-местных (соответственно, бинарных) IFP-операторов в этой же теории?

Список литературы

[1] Aho A.V., Ullman J.D. Universality of data retrieval languages // Proc. of 6th Symp. on Principles of Programming Languages. 1979. Pp. 110–120.

[2] Benedikt M., Dong G., Libkin L., Wong L. Relational expressive power of constraint query languages // Proc. of 15th ACM Symp. on Principles of Database Systems. 1996. Pp. 5–16.

[3] Chandra A., Harel D. Computable queries for relational databases // Journal of Computer and System Sciences. 1980. Vol. 21, № 2. Pp. 156–178.

[4] Codd E.F. A relational model for large shared data banks // Association for Computing Machinery. Communications of the ACM. 1970. Vol. 13. Pp. 377–387.

[5] Codd E.F. Relational completeness of data base sublanguages // Database Systems / Ed. by Rustin R. Prentice-Hall, 1972. Pp. 33–64.

[6] Gurevich Y., Shelah S. Fixed-point extensions of first-order logic // Annals of Pure and Applied Logic. 1986. № 32. Pp. 265—280.

[7] Дудаков С.М. Трансляционный результат для расширений арифметики Пресбургера одноместной функцией, согласованной со сложением // Математические заметки. 2004. Т. 76, № 3. С. 362–371.

[8] Дудаков С.М. Трансляционная теорема для теорий I-сводимых алгебраических систем // Известия Российской академии наук. Серия математическая. 2004. Т. 68, № 5. С. 67–90.

[9] Дудаков С.М. Выразительная сила языков запросов первого порядка для баз данных на неупорядоченном случайном графе // Вестник Новгородского государственного университета им. Ярослава Мудрого. 2005. № 34. С. 57–62.

[10] Дудаков С.М. Разрешимая теория без трансляционной теоремы // Вестник ТвГУ. Серия: Прикладная математика. 2005. № 2. С. 23–26.

[11] Дудаков С.М. Трансляционная теорема и автоматные структуры // Вестник ТвГУ. Серия: Прикладная математика. 2006. № 3. С. 5–35.

[12] Дудаков С.М., Тайцлин М.А. Трансляционные результаты для языков запросов в теории баз данных // Успехи математических наук. 2006. Т. 61, № 2. С. 3–66.

[13] Дудаков С.М. Псевдоконечная однородность, изолированность и сводимость // Математические заметки. 2007. Т. 81, № 4. С. 515–527.

[14] Дудаков С.М. Монадические состояния над упорядоченным универсальным случайным графом и конечные автоматы // Известия Российской академии наук. Серия математическая. 2011. Т. 75, № 5. С. 47–64.

[15] Дудаков С.М. О безопасности рекурсивных запросов // Вестник ТвГУ. Серия: Прикладная математика. 2012. № 4(27). С. 71–80.

[16] Дудаков С.М. О безопасности IFP-операторов и рекурсивных запросов // Вестник ТвГУ. Серия: Прикладная математика. 2013. № 2(29). С. 5–13.

[17] Золотов А.С. Применение оператора транзитивного замыкания для формул с одной функции следования и предикатами делимости // Вестник ТвГУ. Серия: Прикладная математика. 2013. № 1(28). С. 101–117.

[18] Immerman N. Languages that capture complexity classes // SIAM Journal on Computing. 1987. Vol. 16. Pp. 760–778.

[19] Kanellakis P., Kuper G., Revesz P. Constraint query languages // Journal of Computer and System Sciences. 1995. Vol. 51. Pp. 26–52.

[20] Кейслер Г., Чен Ч.Ч. Теория моделей. М.: Мир, 1977. 616 с.

[21] Минский М. Вычисления и автоматы. М.: Мир, 1971. 268 с.

Библиографическая ссылка

Дудаков С.М. Неразрешимость проблемы определенности бинарных IFP-операторов для теории одного следования // Вестник ТвГУ. Серия: Прикладная математика. 2014. № 4. С. 7–15.

Сведения об авторах

1. **Дудаков Сергей Михайлович**
заведующий кафедрой информатики Тверского госуниверситета.

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

ON UNDECIDABILITY OF DEFINITENESS OF BINARY IFP-OPERATORS FOR ONE SUCCESSOR FUNCTION THEORY

Dudakov Sergey Mikhailovich
Head of Computer Science department, Tver State University
Russia, 170100, Tver, 33 Zhelyabova str., TSU. E-mail: sergeydudakov@yandex.ru

Received 12.12.2014, revised 19.12.2014.

We continue to investigate definiteness of inflationary fix point. We show it is impossible to check algorithmically whether IFP-operator value is defined for one successor function theory.

Keywords: inflationary fix point, undecidability, successor function.

Bibliographic citation

Dudakov S.M. On undecidability of definiteness of binary IFP-operators for one successor function theory. *Vestnik TvGU. Seriya: Prikladnaya matematika* [Herald of Tver State University. Series: Applied Mathematics], 2014, no. 4, pp. 7–15. (in Russian)