ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ

УДК 510.675, 510.531

СИЛЬНАЯ МИНИМАЛЬНОСТЬ И IFP-БЕЗОПАСНОСТЬ[1]

Дудаков С.М.
Кафедра информатики

Поступила в редакцию 10.08.2015, после переработки 15.08.2015.

В работе продолжено исследование IFP-безопасности теорий. Доказано, что среди полных конечно аксиоматизируемых сильно минимальных теорий IFP-безопасных нет.

Ключевые слова: сильная минимальность, конечная аксиоматизируемость, инфляционная фиксированная точка.

Вестник ТвГУ. Серия: Прикладная математика. 2015. № 3. С. 25–32.

Введение

Мы продолжаем исследование, начатое в [6], посвященное безопасному применению оператора инфляционной фиксированной точки [9]. Данный оператор аналогичен понятию рекурсивного запроса в языке SQL, в то время как «обычный» SQL представляет собой аналог логики первого порядка. Традиция использования языка первого порядка восходит к Кодду [4, 5], но его возможности ограничены [1, 3], например, транзитивное замыкание графа невыразимо.

Но SQL позволяет использовать не только элементы базы данных, но и операции и отношения предметной области (универсума), что соответствует вложению конечной алгебраической системы в бесконечный универсум и использованию в формулах логики как отношений базы данных, так и универсума [10]. Однако такая операция если и увеличивает выразительные возможности языка первого порядка, то лишь незначительно [2, 8].

Таким образом, современные реализации языка SQL соответствуют логике с оператором инфляционной фиксированной точки, когда база данных вложена в универсум. Это сочетание часто позволяет промоделировать работу произвольного алгоритма, что приводит к неразрешимости, то есть невозможности в общем случае получить результат за конечное время. Например, простой функции следования достаточно, чтобы построить моделирующую формулу.

В данной работе мы продолжаем поиск условий, когда такая ситуация может возникнуть. Системы и их теории, в которых каждый IFP-запрос выполняется за конечное время, называются IFP-безопасными.

В [6] продемонстрировано, что для IFP-безопасности системы (и ее теории) достаточно потребовать безопасности для формул первого порядка. Там же доказана IFP-безопасность счетно-категоричных теорий.

[1]Работа выполнена при финансовой поддержке РФФИ, гранты 13-01-00382 и 13-01-00643.

В [7] приведен пример теории IFP-безопасной, но не являющейся счетно-категоричной, и получены необходимые и достаточные условия IFP-безопасности. В заключении сформулирован вопрос о конечно аксиоматизируемых полных теориях: является ли для таких теорий счетная категоричность необходимым условием IFP-безопасности.

Результат настоящей работы дает частичный ответ на этот вопрос. Мы показываем, что полные конечно аксиоматизируемые сильно минимальные теории IFP-безопасными не являются. Такие теории категоричны в несчетных мощностях, а как известно из работ Зильбера [12], конечно аксиоматизируемые полные несчетно категоричные теории не могут быть счетно категоричными.

1. Определения

Мы используем обычные определения формулы логики первого порядка и ее значения (см., например, [11]). 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. [9]). *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, то* $\mathrm{IFP}_{Q(\bar{y})}(\varphi)$ *— формула исходной сигнатуры со свободными переменными $\bar{x}$ и $\bar{y}$. При этом местность символа Q должна быть равна длине набора $\bar{y}$.*

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

Определение 2 (см. [9]). *Пусть $\mathfrak{A}$ — это алгебраическая система, $\varphi(\bar{x}, \bar{y})$ — формула, с новым предикатным символом Q, m — количество элементов набора $\bar{y}$. 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*

$$Q^{\bar{a}}_0 = \varnothing; \quad Q^{\bar{a}}_{i+1} = Q^{\bar{a}}_i \cup \{\bar{y} \in \mathfrak{A} : (\mathfrak{A}, Q^{\bar{a}}_i) \models \varphi(\bar{a}, \bar{y})\},$$

для $i \in \omega$.

Если $Q^{\bar{a}}_n = Q^{\bar{a}}_{n+1}$ для некоторого $n \in \omega$, то полагаем $Q^{\bar{a}}_* = Q^{\bar{a}}_n$. 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* $\mathrm{IFP}_{Q(\bar{y})}(\varphi)(\bar{a}, \bar{y})$*)* не определено.

Будем говорить, что алгебраическая система $\mathfrak{A}$ является IFP-безопасной, *если любой* IFP*-оператор в ней определен.*

В [6] показано, что если система $\mathfrak{A}$ является IFP-безопасной, то и любая элементарно эквивалентная ей тоже является IFP-безопасной, то есть безопасность является свойством полных теорий.

Определение 3 (см. [11]). *Теория T называется* сильно минимальной*, если для любой ее модели $\mathfrak{A}$, любой формулы $\varphi(\bar{x}, y)$ и любого набора $\bar{a} \in \mathfrak{A}$ множество*

$$\{b \in \mathfrak{A} : \mathfrak{A} \models \varphi(\bar{a}, b)\}$$

либо конечно, либо кофинитно. Здесь набор $\bar{x}$ может иметь произвольную длину, а y — в точности одна переменная.

Кофинитным называется множество, дополнение которого конечно. Классическим примером сильно минимальной теории является теория алгебраически замкнутых полей фиксированной характеристики.

2. Основные результаты

Лемма 1. *Если определимое расширение теории T IFP-небезопасно, то и теория T IFP-небезопасна.*

Доказательство. В определимом расширении каждый новый символ может быть заменен некоторой формулой старой сигнатуры. □

Теорема 1. *Пусть теория T полна, конечно аксиоматизируема, сильно минимальна и имеет бесконечную модель. Тогда теория T не является IFP-безопасной.*

Доказательство. Объединив аксиомы конъюнкцией, можно считать, что аксиома Φ всего одна. Дальше применим ограниченное морлиевское обогащение, чтобы получить $\forall\exists$-аксиоматизируемую теорию T' — определимое расширение теории T. Для этого на каждом шаге выбираем в Φ экзистенциальную подформулу вида $(\exists u)\theta(u, \bar{v})$, где формула θ — бескванторная, вводим новый предикатный символ $P_\theta(\bar{v})$, заменяем в Φ подформулу $(\exists u)\theta(u, \bar{v})$ на $P_\theta(\bar{v})$ и добавляем к множеству аксиом определяющую $P_\theta(\bar{v})$ эквивалентность:

$$(\forall\bar{v})(P_\theta(\bar{v}) \leftrightarrow (\exists u)\theta(u, \bar{v})).$$

Последняя очевидным образом эквивалентна

$$(\forall\bar{v})((\forall u)(\theta(u, \bar{v}) \to P_\theta(\bar{v})) \wedge (\exists u)(P_\theta(\bar{v}) \to \theta(u, \bar{v}))),$$

то есть $\forall\exists$-формуле с одним квантором существования. Поскольку на каждом шаге количество кванторов в формуле Φ будет уменьшаться, то рано или поздно мы получим конечное множество $\forall\exists$-формул, причем в каждой из них кванторов всеобщности может быть несколько, а квантор существования в точности один.

Итак, можно считать, что теория T' задается конечным множеством $\forall\exists$-аксиом:

$$(\forall\bar{x})(\exists y)\varphi_i(\bar{x}, y), \quad i = 1, \ldots, k.$$

Рассмотрим любую модель $\mathfrak{A}'$ теории T'. Отметим, что определимое расширение сильно минимальной теории снова будет сильно минимальным. Следовательно, для каждого $i = 1, \ldots, k$ и для каждого $\bar{a} \in \mathfrak{A}'$ найдется конечно или кофинитно много $b \in \mathfrak{A}'$, для которых выполнено $\varphi_i(\bar{a}, b)$. Заметим, что это количество (или его дополнение) не просто конечно, а ограничено некоторой натуральной константой N_i, не зависящей от $\mathfrak{A}'$ и $\bar{a}$. В противном случае с помощью теоремы компактности легко построить модель $\mathfrak{B}'$ теории T' и набор $\bar{c} \in \mathfrak{B}'$ такие, что оба множества

$$\{b \in \mathfrak{B}' : \mathfrak{B}' \models \varphi_i(\bar{c}, b)\} \quad \text{и} \quad \{b \in \mathfrak{B}' : \mathfrak{B}' \models \neg\varphi_i(\bar{c}, b)\}$$

будут бесконечными. Пусть

$$N = \max\{N_1, \ldots, N_k\} + 1. \tag{1}$$

В силу полноты и наличия бесконечных моделей у теории T можно сделать вывод, что и теория T' полна и имеет бесконечные модели. Поэтому никакое конечное подмножество $X \subseteq \mathfrak{A}'$ не является носителем модели T', так как конечных моделей у T' быть не может. Следовательно, если некоторая формула $\psi(x)$ с одной свободной переменной выделяет в $\mathfrak{A}'$ конечное множество X_ψ мощности n, то хотя бы одна из X_ψ-релятивизированных формул $(\forall \bar{x} \in X_\psi)(\exists y \in X_\psi)\varphi_i(\bar{x}, y)$, $i = 1, \ldots, k$, будет ложной. Это означает, что найдется такой набор $\bar{a} \in X_\psi$, что никакой $b \in X_\psi$ не делает соответствующую формулу $\varphi_i(\bar{a}, b)$ истинной в $\mathfrak{A}'$. С другой стороны, в силу

$$\mathfrak{A}' \models (\forall \bar{x})(\exists y)\varphi_i(\bar{x}, y)$$

найдется такой $b \in \mathfrak{A}'$, для которого $\mathfrak{A}' \models \varphi_i(\bar{a}, b)$, следовательно, такой b не может быть элементом X_ψ.

Предположим, что $n \geq N$. Рассмотрим множество

$$Y_{\bar{a}} = \{b \in \mathfrak{A}' : \mathfrak{A}' \models \varphi_i(\bar{a}, b)\}.$$

Допустим, что это множество кофинитно. Согласно (1), количество $b \in \mathfrak{A}'$, не попавших в $Y_{\bar{a}}$, будет меньше N. Но X_ψ содержит не меньше N элементов, следовательно, хотя бы один из них попадет в $Y_{\bar{a}}$, то есть $\mathfrak{A}' \models \varphi_i(\bar{a}, b)$ для некоторого $b \in X_\psi$. Это противоречит ранее доказанному. Таким образом, множество $Y_{\bar{a}}$ должно быть конечным. Кроме того, исходя из тех же соображений, это множество должно быть непустым и не должно пересекаться с X_ψ.

Подведем итог этих рассуждений. При $n \geq N$ найдутся такие $i = 1, \ldots, k$ и набор $\bar{a} \in X_\psi$, что не выполнено $(\exists y \in X_\psi)\varphi_i(\bar{a}, y)$, и для любых таких i и $\bar{a} \in X_\psi$ множество $Y_{\bar{a}}$ является непустым, конечным и не пересекающимся с X_ψ.

Исходя из этого, мы можем легко построить неопределенный в системе $\mathfrak{A}'$ IFP-оператор. Выберем в качестве «начального» множества Q произвольные попарно различные элементы $a_1, \ldots, a_N$. Теперь на каждом шаге построения Q будем искать в «старом» Q определенный выше номера i и наборы $\bar{a}$ и добавлять к «новому» Q элементы соответствующих множеств $Y_{\bar{a}}$, которых конечно много:

$$\mathrm{IFP}_{Q(z)}\left(\bigvee_{i=1}^{N} z = a_i \vee \bigvee_{i=1}^{k} (\exists \bar{x} \in Q)\Big(\neg(\exists y \in Q)\varphi_i(\bar{x}, y) \wedge \varphi_i(\bar{x}, z)\Big)\right).$$

Поскольку на каждом шаге множество Q_i будет конечным, содержащим не менее N элементов, то каждый следующий шаг будет расширять Q, то есть $Q_i \neq Q_{i+1}$. Следовательно, указанный IFP-оператор не определен, теория T' не является IFP-безопасной, а, значит, и теория T тоже. □

3. Обобщение

Заметим, что в доказательстве теоремы 1 на самом деле используются более слабые условия, чем полнота и сильная минимальность. Поэтому можно доказать более сильное утверждение:

Теорема 2. *Пусть теория* T

1) *конечно аксиоматизируема с помощью* $\forall\exists$*-формул* $(\forall\bar{x})(\exists\bar{y})\varphi_i(\bar{x},\bar{y})$, $i = 1,\dots,k$;

2) *не имеет конечных моделей;*

3) *в каждой модели* $\mathfrak{A}$ *теории* T *каждая атомная формула вида* $\varphi_i(\bar{a},\bar{y})$, *где* $\bar{a} \in \mathfrak{A}$, $i = 1,\dots,k$, *выделяет конечное или кофинитное множество.*

Тогда любая модель теории T *не является* IFP*-безопасной.*

Доказательство. В основном повторяет доказательство теоремы 1. Единственное изменение — непосредственно при построении IFP-формулы нужно перебирать все элементы наборов $\bar{y}$:

$$\mathrm{IFP}_{Q(z)}\Bigg(\bigvee_{i=1}^{N} z = a_i \vee \bigvee_{i=1}^{k} (\exists \bar{x} \in Q) \\ \Big(\neg(\exists \bar{y} \in Q)\varphi_i(\bar{x}, y) \wedge (\exists \bar{y})(\varphi_i(\bar{x},\bar{y}) \wedge \bigvee_{j=1}^{m} z = y_j)\Big)\Bigg).$$

Здесь мы считаем, что длина набора $\bar{y}$ равна m: $\bar{y} = (y_1,\dots,y_m)$. □

Используя этот, усиленный, вариант теоремы можно доказать IFP-небезопасность некоторых теорий, которые не являются ни полными, ни сильно минимальными.

Пример 1. Рассмотрим сигнатуру, состоящую из одного двухместного предикатного символа E, и произвольное натуральное число N. Пусть теория T на графах задана аксиомами, утверждающими, что

1) степень каждой вершины не превосходит N;

2) степень исхода каждой вершины превосходит степень входа.

Тогда эта теория удовлетворяет условиям теоремы 2, и, следовательно, никакой такой граф не является IFP-безопасным.

Заключение

Результаты данной работы являются частичным ответом на вопрос, сформулированный в [7]:

Вопрос 1. Существуют ли полные, конечно аксиоматизируемые, IFP-безопасные теории, которые не являются счетно категоричными.

Можно утверждать, что среди сильно минимальных теорий таких нет.

Тем не менее, окончательный ответ на вопрос 1 так и не получен, поэтому представляют интерес дальнейшие результаты в этом направлении. Например:

Вопрос 2. Можно ли в теореме 1 ослабить условие сильной минимальности до ω-стабильности или хотя бы до несчетной категоричности?

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. 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, no. 2. Pp. 156–178.

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

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

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

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

[8] 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.

[9] Gurevich Y., Shelah S. Fixed-point extensions of first-order logic // Annals of Pure and Applied Logic. 1986. Vol. 32. Pp. 265–280.

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

[11] Marker D. Model theory: an introduction. New York: Springer-Verlag, 2002. 346 p.

[12] Зильбер Б.И. Решение проблемы конечной аксиоматизируемости для теорий, категоричных во всех бесконечных мощностях // Теория моделей и ее приложения. Алма-Ата: МинВУЗ КазССР и КазГУ, 1980. С. 47–60.

Библиографическая ссылка

Дудаков С.М. Сильная минимальность и IFP-безопасность // Вестник ТвГУ. Серия: Прикладная математика. 2015. № 3. С. 25–32.

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.

STRONG MINIMALITY AND IFP-SAFETY

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

Received 10.08.2015, revised 15.08.2015.

We continue to investigate an IFP-safety of theories. It is proved that complete finitely axiomatizable strongly minimal theories are IFP-unsafe.

Keywords: strong minimality, finite axiomatizability, inflationary fix point.

Bibliographic citation

Dudakov S.M. Strong minimality and IFP-safety. *Vestnik TvGU. Seriya: Prikladnaya matematika* [Herald of Tver State University. Series: Applied Mathematics], 2015, no. 3, pp. 25–32. (in Russian)