S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 13, стр. 882–887 (2016) УДК 510.652
DOI 10.17377/semi.2016.13.070 MSC 11U99

ГЕНЕРИЧЕСКАЯ НЕРАЗРЕШИМОСТЬ ЭКЗИСТЕНЦИАЛЬНОЙ ТЕОРИИ КОЛЬЦА ЦЕЛЫХ ЧИСЕЛ

А.Н. РЫБАЛОВ

Abstract. Famous theorem of Matiyasevich about undecidability of Hilbert's thenth problem implies that existential theory of ring of integer numbers is undecidable. In this paper we prove that this theory remains undecidable if we restrict the set of all existential arithmetic statements by any recursive subsets of almost all statements (so called generic sets).

Keywords: existential theory of ring of integer numbers, generic complexity.

1. Введение

Теория алгоритмов в классической постановке изучает алгоритмические проблемы в худшем случае, рассматривая поведение алгоритмов на всём множестве входов. В Computer Science исследуется также сложность алгоритмов в среднем, при этом алгоритм может хорошо (полиномиально) работать на большинстве входных данных и плохо (экспоненциально) на очень редких входах. Генерический подход в применении к алгоритмическим проблемам был впервые предложен в 2003 году, в статье [2]. В рамках этого подхода изучается поведение алгоритмов на множествах почти всех входов (эти множества называются генерическими), игнорируя поведение алгоритма на остальных входах, на которых алгоритм может работать медленно или вообще не останавливаться. Такой подход имеет приложение в криптографии, где требуется, чтобы алгоритмические проблемы были трудными для почти всех входов. В отличие от сложности в среднем, генерический подход применим и для алгоритмически

Rybalov, A.N., Generic undecidability of existential theory of integer numbers ring.

Работа поддержана грантом РФФИ (проект №14-01-00068).
Поступила 24 марта 2016 г., опубликована 20 октября 2016 г.

неразрешимых проблем. Для многих классических алгоритмически неразрешимых проблем алгебры доказано, что они разрешимы в генерическом случае. Например, в работе [1] установлено, что проблема остановки для машин Тьюринга с полубесконечной лентой, генерически разрешима.

Большой пласт алгоритмических проблем связан с проблемами разрешения элементарных теорий различных алгебраических систем. Как правило, эти проблемы либо неразрешимы (формальная арифметика, теория поля рациональных чисел, теория графов и т.д.), либо разрешимы, но имеют очень высокую вычислительную сложность (арифметика Пресбургера, теория упорядоченного поля действительных чисел и т.д.). Поэтому представляет интерес изучение их генерической разрешимости и сложности. Рыбалов и Мясников в работе [4] доказали, что любая неразрешимая в классическом смысле элементарная теория остается неразрешимой на строго генерических множествах формул. Также представляет интерес изучение в рамках генерического подхода фрагментов элементарных теорий различных алгебраических систем, например, их экзистенциальных теорий. В данной работе изучается экзистенциальная теория кольца целых чисел. Из знаменитой теоремы Дэвиса, Робинсон, Патнема и Матиясевича ([6]) о неразрешимости десятой проблемы Гильберта следует, что эта теория неразрешима. В данной работе доказывается, что эта теория остается неразрешимой на любом рекурсивном генерическом множестве экзистенциальных арифметических формул. При этом используется так называемое нормализованное представление формул, которое подразумевает упорядоченность нумерации переменных в формуле слева направо: вторая переменная не может встретиться раньше (левее) первой, третья — раньше второй и т.д. Это довольно естественное требование, ведь если человека попросить написать случайную формулу, он не станет сразу использовать x_{100}, а начнет с x_1 и будет вводить новые переменные по мере надобности. Полученный результат можно перенести на любую неразрешимую экзистенциальную теорию алгебраической системы с конечной сигнатурой.

2. Генерические алгоритмы

Следуя [2], дадим основные определения теории генерической сложности вычисления. Пусть I – множество всех входов, а I_n – множество входов размера n. Для любого подмножества $S \subseteq I$ определим следующую последовательность

$$\rho_n(S) = \frac{|S \cap I_n|}{|I_n|},\ n = 1, 2, 3, \ldots.$$

Величина $\rho_n(S)$ это вероятность получить вход из множества S при случайной и равномерной генерации входов из I_n. *Асимптотической плотностью* S назовем следующий предел (если он существует)

$$\rho(S) = \lim_{n\to\infty} \rho_n(S).$$

Множество S называется *генерическим*, если $\rho(S) = 1$ и *пренебрежимым*, если $\rho(S) = 0$. Очевидно, что S генерическое тогда и только тогда, когда его дополнение $I \setminus S$ пренебрежимо.

Множество $S \subseteq I$ *генерически разрешимо*, если существует множество $G \subseteq I$ такое, что

(1) G генерическое,

(2) G разрешимо,
(3) $S \cap G$ разрешимо.

Генерический алгоритм $\mathcal{A}$ для S работает на входе $x \in I$ следующим образом. Сначала $\mathcal{A}$ решает принадлежит ли x множеству G. Если $x \in G$, то $\mathcal{A}$ может решить S на G, иначе $\mathcal{A}$ отвечает "Я НЕ ЗНАЮ!". Таким образом, $\mathcal{A}$ корректно решает S на "почти всех"входах (входах из генерического множества).

3. Представление экзистенциальных арифметических формул

В этой главе рассмотрим естественное представление замкнутых экзистенциальных арифметических формул языка $\{+, -, \times, 1, 0\}$ с помощью двоичных деревьев. Это представление, с одной стороны настолько же компактно как и стандартное представление строками символов (с точностью до линейного множителя). С другой стороны, оно удобно для различного рода подсчетов. Кроме того, достаточно просто написать компьютерную программу для случайной генерации формул, заданных с помощью этого представления.

Назовем замкнутую арифметическую формулу Φ *простой атомарной* если она имеет следующий вид:

1) $x_i = x_j + x_k$,
2) $x_i = x_j - x_k$,
3) $x_i = x_j x_k$,
4) $x_i = 0$,
5) $x_i = 1$,

где x_i, x_j, x_k – переменные.

Мы говорим, что замкнутая экзистенциальная арифметическая формула Φ имеет *натуральную пренексную* форму, если она имеет вид:

$$\Phi = \exists x_1 \dots \exists x_t \phi,$$

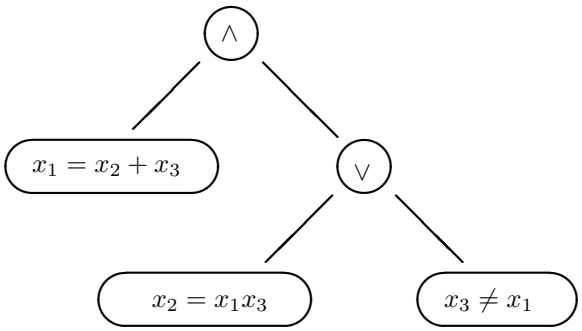
где ϕ – бесквантворная формула, полученная с помощью конъюнкций, дизъюнкций из простых атомарных формул или их отрицаний. Заметим, что любая замкнутая экзистенциальная формула может быть приведена с помощью эквивалентных преобразований к натуральной пренексной форме. При этом размер формулы увеличивается не более чем линейно.

Пусть теперь ϕ – бесквантворная формула, которая является булевой комбинацией простых атомарных формул и их отрицаний. Естественным образом можно сопоставить формуле ϕ бинарное дерево T_ϕ, которое представляет конструкцию ϕ из простых атомарных формул и их отрицаний с помощью конъюнкций и дизъюнкций. Внутренние вершины T_ϕ помечены символами $\vee$ и $\wedge$, а листья T_ϕ помечены простыми атомарными или их отрицаниями. С другой стороны, по любому такому бинарному дереву можно восстановить бесквантворную формулу. Это дает взаимно-однозначное представление бесквантворных частей замкнутых экзистенциальных арифметических формул в натуральной пренексной форме размеченными бинарными деревьями. Если T_ϕ имеет n листьев, то не более $3n$ переменных могут встетиться в T_ϕ, поэтому в дальнейшем будем полагать, что все переменные T_ϕ лежат в множестве $x_1, \dots, x_{3n}$.

Будем называть дерево T_ϕ *нормализованным*, если для любой переменной x_i, $i > 1$, найдется переменная x_{i-1}, расположенная либо в том же листе дерева, либо в более левом. Заметим, что любое дерево T_ϕ можно нормализовать подходящей перестановкой переменных.

Пусть $\Phi = \exists x_1 \dots \exists x_t \phi$ — экзистенциальная формула в натуральной пренексной форме. *Представление* Φ состоит из бинарного нормализованного дерева T_ϕ, которое кодирует бесквантерную часть ϕ. Если T_ϕ имеет n листьев, то длина кванторной приставки не более $3n$. Поэтому число n листьев в дереве T_ϕ дает линейную верхнюю оценку на число нефиктивных переменных и кванторов в Φ. Заметим также, что число булевых операций в бесквантерной части Φ равно $n-1$. Под размером формулы Φ будем понимать число n. Для упрощения подсчетов считается, что формула Φ размера n зависит от всех переменных $\{x_1, \dots, x_{3n}\}$ и кванторы берутся по всем этим переменным.

Например, вот представление формулы $\exists x_1 \exists x_2 \exists x_3 \Big((x_1 = x_2 + x_3) \wedge \big((x_2 = x_1 x_3) \vee (x_3 \neq x_1) \big) \Big)$:



В дальнейшем будем отождествлять замкнутые экзистенциальные арифметические формулы с их представлениями.

Для любой экзистенциальной арифметической формулы $\Phi = \exists x_1 \dots \exists x_t \phi$ рассмотрим множество формул

$$eq(\Phi) = \{\exists x_1 \dots \exists x_{3n} \Big(\phi \vee ((x_1 \neq x_1) \wedge \psi) \Big)\},$$

где $n > t$, ψ – произвольная бесквантерная формула от переменных $x_1, \dots, x_n$. Легко видеть, что все формулы из $eq(\Phi)$ эквивалентны Φ в том смысле, что они истинны или ложны одновременно с Φ.

Лемма 1. *Для любой формулы* Φ *множество* $eq(\Phi)$ *не является пренебрежимым.*

Доказательство. Обозначим через F множество всех формул и через F_n – множество всех формул размера n. Любая формула размера n, состоит из бинарного нормализованного дерева с n листьями и $n-1$ внутренней вершиной. Известно (см., например, [5]), что существует C_{n-1} неразмеченных бинарных деревьев с n листьями, где

$$C_{n-1} = \frac{1}{n} \binom{2(n-1)}{n-1}$$

– $n-1$-е число Каталана. Каждая внутренняя вершина может быть помечена либо $\vee$, либо $\wedge$ (всего $n-1$ таких вершин – 2^{n-1} вариантов разметки). Обозначим через L_i число способов разметки i-го листа (нумерация листов дерева

слева направо). В итоге получается

$$|F_n| = L_1 L_2 \dots L_n 2^{n-1} C_{n-1}.$$

Теперь посчитаем число формул размера n из множества $eq(\Phi)$. Это делается аналогично, с той лишь разницей, что там у формул произвольным может быть лишь поддерево, отвечающее за формулу ψ. Оно имеет $n-t-1$ листьев, листья могут быть размечены $L_{t+2}, \dots, L_n$ способами. Поэтому

$$|eq(\Phi)_n| = L_{t+2} \dots L_n 2^{n-t-2} C_{n-t-2}.$$

Оценим теперь асимптотическую плотность множества $eq(\Phi)$.

$$\mu(eq(\Phi)) = \lim_{n\to\infty} \frac{|eq(\Phi)_n|}{|F_n|} = \lim_{n\to\infty} \frac{L_{t+2} \dots L_n 2^{n-t-2} C_{n-t-2}}{L_1 L_2 \dots L_n 2^{n-1} C_{n-1}} =$$

$$= \lim_{n\to\infty} \frac{C_{n-t-2}}{L_1 L_2 \dots L_{t+1} 2^{t+1} C_{n-1}} =$$

$$= \frac{1}{L_1 L_2 \dots L_{t+1} 2^{t+1}} \lim_{n\to\infty} \frac{4^{n-t-2}(n-1)^{3/2}}{4^{n-1}(n-t-2)^{3/2}} = const > 0.$$

Здесь использована асимптотика чисел Каталана $C_n \sim \frac{4^n}{n^{3/2}\sqrt{\pi}}$ (см. [5]). Также использовано то, что число способов разметить лист $L_i, i \le t$, является константой – это следует из нормализованности представления формул. □

4. Основной результат

Теперь все готово, чтобы доказать основной результат статьи.

Теорема 1. *Экзистенциальная теория кольца целых чисел не является генерически разрешимой.*

Доказательство. Допустим, что экзистенциальная теория кольца целых чисел $Th_\exists(\mathbb{Z})$ генерически разрешима. Это значит, что существует разрешимое генерическое множество формул G такое, что $Th_\exists(\mathbb{Z}) \cap G$ разрешимо. Покажем, что тогда и вся $Th_\exists(\mathbb{Z})$ будет разрешимой. Разрешающий алгоритм для $Th_\exists(\mathbb{Z})$ будет работать на формуле Ψ следующим образом. Перебираем формулы из множества $eq(\Psi)$ в возрастающем порядке до тех пор, пока не получим формулу Ψ_1 из G. Это обязательно произойдет, потому что множество $eq(\Psi)$, по лемме 1, не пренебрежимо, а множество G генерическое. Попав в G, решаем проблему истинности для Ψ_1, а, тем самым, и проблему истинности для Ψ. Полученное противоречие доказывает теорему. □

References

[1] J.D. Hamkins, A. Miasnikov, *The halting problem is decidable on a set of asymptotic probability one*, Notre Dame Journal of Formal Logic, **47**:4 (2006), 515–524. Zbl 1137.03024

[2] I. Kapovich, A. Myasnikov, P. Schupp, V. Shpilrain, *Generic-case complexity, decision problems in group theory and random walks*, Journal of Algebra, **264**:2 (2003), 665–694. Zbl 1041.20021

[3] I. Kapovich, A. Myasnikov, P. Schupp, V. Shpilrain, *Average-case complexity for the word and membership problems in group theory*, Advances in Mathematics, **190** (2005), 343–359. Zbl 1065.20044

[4] A. Myasnikov, A. Rybalov. *Generic complexity of undecidable problems*, Journal of Symbolic Logic, **73**:2 (2008), 656–673. Zbl 1140.03025

[5] D. Knuth, *The Art of Computer Programming*, Addison-Wesley, (2008).

[6] Y. Matiyasevich, *The diophantiness of recursively enumerable sets (in Russian)*, Soviet Math. Dokl, **191**:2 (1970), 2790-—282. Zbl 0212.33401

Alexander Nikolaevich Rybalov
Sobolev Institute of Mathematics,
Pevtsova str. 13,
Omsk 644043, Russia
E-mail address: alexander.rybalov@gmail.com