S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

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

Том 16, стр. 1298–1294 (2019) УДК 510.652
DOI 10.33048/semi.2019.16.089 MSC 11U99

ГЕНЕРИЧЕСКАЯ НЕРАЗРЕШИМОСТЬ УНИВЕРСАЛЬНЫХ ТЕОРИЙ

А.Н. РЫБАЛОВ

Abstract. Generic-case approach to algorithmic problems was suggested by Miasnikov, Kapovich, Schupp and Shpilrain in 2003. This approach studies behavior of an algorithm on typical (almost all) inputs and ignores the rest of inputs. In this paper we study generic complexity of undecidable universal theories. We prove that any undecidable universal theory remains generically undecidable (i.e. for almost all inputs).

Keywords: universal theory, 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 предложен Каповичем, Мясниковым, Шпильрайном и Шуппом в [3]. 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 неразрешимых проблем. Для многих классических алгоритмически неразрешимых проблем алгебры доказано, что они разрешимы в

Rybalov, A.N., Generic undecidability of universal theories.

© 2019 Рыбалов А.Н.

Работа поддержана грантом РНФ № 19-11-00209.

Поступила 30 января 2019 г., опубликована 23 сентября 2019 г.

генерическом случае [4]. Также, в [2] было 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 [5] доказали, что любая неразрешимая в классическом смысле элементарная теория остается неразрешимой на строго генерических множествах формул. В последние 20 лет активно развивается так называемая универсальная алгебраическая геометрия [1], в которой многие понятия и алгоритмы классической алгебраической геометрии переносятся на произвольные алгебраические системы. При этом особую роль играют универсальные теории — от их сложности зависят переспективы построения «хорошей» алгебраической геометрии над той или иной алгебраической системой. Поэтому также представляет интерес изучение в рамках генерического подхода универсальных теорий различных алгебраических систем.

В данной работе изучаются универсальные теории, неразрешимые в классическом смысле. Доказывается, что каждая такая теория остается неразрешимой и генерически, то есть для ее распознавания не существует генерического алгоритма. 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.

2. Генерические алгоритмы

Пусть I — множество всех входов, а I_n — множество входов размера n. Для любого подмножества $S \subseteq I$ определим следующую последовательность

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

где $S_n = S \cap I_n$ – множество входов из S размера n. Здесь $|A|$ — число элементов в множестве A. *Асимптотической плотностью* S назовём предел (если он существует)

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

Множество S называется *генерическим*, если $\rho(S) = 1$, и *пренебрежимым*, если $\rho(S) = 0$.

Алгоритм $\mathcal{A}$ с множеством входов I и множеством выходов $J \cup \{?\}$ $(? \notin J)$ называется *генерическим*, если

(1) $\mathcal{A}$ останавливается на всех входах из I;
(2) множество $\{x \in I : \mathcal{A}(x) = ?\}$ является пренебрежимым.

Здесь через $\mathcal{A}(x)$ обозначается результат работы алгоритма $\mathcal{A}$ на входе x. Генерический алгоритм $\mathcal{A}$ *вычисляет функцию* $f : I \to J$, если для любого $x \in I$

такого, что $\mathcal{A}(x) \neq ?$, имеет место $\mathcal{A}(x) = f(x)$. Ситуация $\mathcal{A}(x) = ?$ означает, что $\mathcal{A}$ не может вычислить функцию f на аргументе x. Но условие 2 гарантирует, что $\mathcal{A}$ корректно вычисляет f на почти всех входах (входах из генерического множества). Множество $S \subseteq I$ называется *генерически разрешимым*, если существует генерический алгоритм, вычисляющий его характеристическую функцию.

3. Представление универсальных формул

Зафиксируем конечную сигнатуру

$$\sigma = \{P_1^{(a_1)}, \dots, P_k^{(a_k)}, f_1^{(b_1)}, \dots, f_m^{(b_m)}, c_1, \dots, c_l\},$$

где P_i предикаты, f_i функции и c_i константы. Положим

$$K = K_\sigma = \max_{i=1,\dots,k, j=1,\dots,m} \{a_i, b_j + 1, 2\}.$$

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

1) $x_j = f_i(x_{i_1}, \dots, x_{i_s})$,
2) $P_i(x_{i_1}, \dots, x_{i_r})$,
3) $x_i = c_j$.

Лемма 1. *Число $a(n)$ простых атомарных формул σ от n переменных и их отрицаний равно*

$$a(n) = \sum_{i=1}^{m} 2n^{b_i+1} + \sum_{j=1}^{k} 2n^{a_j} + 2nl.$$

Доказательство. Прямой подсчет. □

Будем говорить, что замкнутая универсальная формула Φ сигнатуры σ имеет *натуральную пренексную* форму, если она имеет вид:

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

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

Пусть теперь ϕ – бескванторная 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 формулами или их отрицаниями. С другой стороны, по любому такому бинарному дереву можно восстановить бескванторную формулу. Это дает взаимно-однозначное представление бескванторных частей замкнутых формул сигнатуры σ в натуральной пренексной форме размеченными бинарными деревьями. Если T_ϕ имеет n листьев, то не более Kn переменных могут встретиться в T_ϕ, поэтому в дальнейшем будем полагать, что все переменные T_ϕ лежат в множестве $x_1, \dots, x_{Kn}$.

Пусть $\Phi = \forall x_1 \dots \forall x_t \phi$ – универсальная формула в натуральной пренексной форме. *Представление* Φ состоит из бинарного дерева T_ϕ, которое кодирует бескванторную часть ϕ. Если T_ϕ имеет n листьев, то длина кванторной приставки не более Kn. 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 бескванторной части Φ равно $n-1$. Под размером формулы Φ будем понимать число n. Для упрощения подсчетов будем считать, что формула Φ размера n зависит от всех переменных $\{x_1, \dots, x_{Kn}\}$ и кванторы навешаны на все эти переменные (то есть кванторная приставка содержит ровно Kn кванторов). В дальнейшем будем отождествлять замкнутые универсальные формулы сигнатуры σ с их представлениями.

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. Соответствующую формулу будем также называть нормализованной. В дальнейшем все формулы будут предполагаться нормализованными и замкнутыми, поэтому слова «нормализованная» и «замкнутая» будем опускать.

Напомним, что числа Каталана C_n определяются следующим образом

$$C_n = \frac{1}{n+1}\binom{2n}{n},$$

где $\binom{2n}{n}$ – соответствующий биномиальный коэффициент. В дальнейшем нам понадобится следующее утверждение о числах Каталана.

Лемма 2. *Для $n > m$ имеет место*

$$\frac{C_{n-m}}{C_n} > \frac{1}{4^m}.$$

Доказательство. Оценим отношение чисел Каталана:

$$\frac{C_{n-m}}{C_n} = \frac{n+1}{n-m+1} \times \frac{\binom{2(n-m)}{n-m}}{\binom{2n}{n}} > \frac{n+1}{n-m+1} \times \frac{\frac{(2(n-m))!}{(n-m)!(n-m)!}}{\frac{(2n)!}{n!n!}} >$$

$$> \frac{(2(n-m))!n!n!}{(n-m)!(n-m)!(2n)!} = \frac{n!}{(n-m)!} \times \frac{2(n-m)\dots(n-m+1)}{2n\dots(n+1)} =$$

$$= \frac{n(n-1)\dots(n-m+1)2(n-m)\dots(n-m+1)}{2n\dots(n+1)} =$$

$$= \frac{(n\dots(n-m+1))^2}{2n\dots(2(n-m)+1)} > \Big(\frac{(n-1)\dots(n-m)}{2(n-1)\dots(2n-2m)}\Big)^2 > \frac{1}{2^{2m}} = \frac{1}{4^m}.$$

□

4. Основной результат

Пусть $\mathfrak{A} = \langle A, \sigma \rangle$ – алгебраическая система конечной сигнатуры σ. Обозначим через $\mathcal{UF}$ множество всех универсальных формул сигнатуры σ, а через $\mathcal{UF}_n$ множество всех формул в $\mathcal{UF}$ размера n. Для любой универсальной формулы $\Phi = \forall x_1 \dots \forall x_t \phi$ рассмотрим множество формул

$$eq(\Phi) = \{\forall x_1 \dots \forall x_{Kn}\Big(\phi \vee ((x_1 \neq x_1) \wedge \psi)\Big)\},$$

где $n > t$, ψ – произвольная бескванторная формула от переменных $x_1, \ldots, x_n$. Очевидно, что для любой формулы $\Phi' \in eq(\Phi)$ имеет место $\mathfrak{A} \models \Phi \Leftrightarrow \mathfrak{A} \models \Phi'$.

Лемма 3. *Для любой универсальной формулы Φ множество $eq(\Phi)$ не является пренебрежимым.*

Доказательство. Любая формула размера n, состоит из бинарного нормализованного дерева с n листьями и $n-1$ внутренней вершиной. Известно [6], что существует C_{n-1} неразмеченных бинарных деревьев с n листьями. 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

$$|\mathcal{UF}_n| = L_1 L_2 \ldots L_n 2^{n-1} C_{n-1}.$$

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 $L_{t+2}, \ldots, L_n$ способами. Поэтому

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

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

$$\rho(eq(\Phi)) = \lim_{n\to\infty} \frac{|eq(\Phi)_n|}{|\mathcal{UF}_n|} = \lim_{n\to\infty} \frac{L_{t+2} \ldots L_n 2^{n-t-2} C_{n-t-2}}{L_1 L_2 \ldots L_n 2^{n-1} C_{n-1}} =$$

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

$$> \frac{1}{L_1 L_2 \ldots L_{t+1} 2^{t+1}} \lim_{n\to\infty} \frac{1}{4^{t+1}} = const > 0.$$

Здесь использована лемма 2. Также использовано то, что число способов разметить лист $L_i, i \le t$, является константой – это следует из нормализованности представления формул. □

Теперь все готово, чтобы доказать основной результат статьи.

Теорема 1. *Пусть $\mathfrak{A} = \langle A, \sigma \rangle$ – алгебраическая система конечной сигнатуры σ с неразрешимой универсальной теорией $Th_\forall(\mathfrak{A})$. Проблема распознавания $(Th_\forall(\mathfrak{A}), \mathcal{UF})$ не является генерически разрешимой.*

Доказательство. Допустим, что универсальная теория $Th_\forall(\mathfrak{A})$ генерически разрешима. Это значит, что существует генерический алгоритм $\mathcal{A}$, вычисляющий характеристическую функцию множества $Th_\forall(\mathfrak{A})$ на множестве входов $\mathcal{UF}$. Покажем, что тогда теория $Th_\forall(\mathfrak{A})$ будет разрешимой в классическом смысле. Классический алгоритм для $Th_\forall(\mathfrak{A})$ будет работать на формуле Φ следующим образом. Перебирает формулы из множества $eq(\Phi)$ в возрастающем порядке до тех пор, пока не получит такую формулу Φ', что $\mathcal{A}(\Phi') \neq ?$. Это обязательно произойдет, потому что множество $eq(\Phi)$, по лемме 3, не пренебрежимо, а множество $\{\Psi \in \mathcal{UF} : \mathcal{A}(\Psi) = ?\}$ пренебрежимо. Таким образом, $\mathcal{A}(\Phi')$ решает проблему истинности для Φ' и, тем самым, проблему истинности и для Φ. Полученное противоречие доказывает теорему. □

References

[1] E.Y. Daniyarova, A.G. Myasnikov, V.N. Remeslennikov, *Algebraic geometry over algebraic structures*, Novosibirsk: SB RAS, 2016 (in Russian).

[2] 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

[3] 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

[4] 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

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

[6] D.E. Knuth, *The Art of Computer Programming*, Reading, Massachusetts: Addison-Wesley, 1997. Zbl 0895.68055

Alexander Nikolaevich Rybalov
Sobolev Institute of Mathematics,
13, Pevtsova str.,
Omsk, 644043, Russia.
Omsk State Technical University,
11, Mira ave.,
Omsk, 644050, Russia.
E-mail address: alexander.rybalov@gmail.com