МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УДК 510.52

О ГЕНЕРИЧЕСКОЙ НЕРАЗРЕШИМОСТИ ДЕСЯТОЙ ПРОБЛЕМЫ ГИЛЬБЕРТА ДЛЯ ПОЛИНОМИАЛЬНЫХ ДЕРЕВЬЕВ[1]

А. Н. Рыбалов

Институт математики им. С. Л. Соболева СО РАН, г. Омск, Россия

Генерический подход к алгоритмическим проблемам предложен Каповичем, Мясниковым, Шуппом и Шпильрайном в 2003 г. В рамках этого подхода изучается поведение алгоритмов на множестве «почти всех» входов (это множество называется генерическим) и игнорируется его поведение на остальных входах, на которых алгоритм может работать медленно или вообще не останавливаться. В работе изучается генерическая сложность десятой проблемы Гильберта для диофантовых уравнений, представляемых в виде полиномиальных деревьев. Полиномиальное дерево — это бинарное дерево, листья которого помечены переменными или константой 1, а внутренние вершины содержат операции сложения, вычитания или умножения. Любой полином от многих переменных с целыми коэффициентами можно представить в виде такого полиномиального дерева. Доказывается, что проблема разрешимости диофантовых уравнений, представляемых в виде полиномиальных деревьев, является генерически неразрешимой.

Ключевые слова: *генерическая сложность, диофантовы уравнения.*

DOI 10.17223/20710410/44/8

ON GENERIC UNDECIDABILITY OF HILBERT'S TENTH PROBLEM FOR POLYNOMIAL TREES

A. N. Rybalov

Sobolev Institute of Mathematics, Omsk, Russia

E-mail: alexander.rybalov@gmail.com

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. We study generic complexity of the Hilbert's tenth problem for systems of Diophantine equations represented by so-called polynomial trees. Polynomial tree is a binary tree, which leafs are marked by variables or the constant 1, and internal vertices are marked by operations of addition, subtraction and multiplication. Every polynomial with integer coefficients can be represented by a polynomial tree. We prove generic undecidability of the decidability problem for Diophantine equations represented by polynomial trees. To prove

[1]Исследование поддержано программой фундаментальных научных исследований СО РАН I.1.1.4, проект № 0314-2019-0004.

this theorem, we use the method of generic amplification, which allows to construct generically undecidable problems from the problems undecidable in the classical sense. The main ingredient of this method is a technique of cloning, which unites inputs of the problem together in the large enough sets of equivalent inputs. Equivalence is understood in the sense that the problem is solved similarly for them.

Keywords: *generic complexity, Diophantine equations.*

Введение

Генерический подход в применении к алгоритмическим проблемам впервые предложен в 2003 г. в [1]. В рамках этого подхода изучается поведение алгоритма на множестве «почти всех» входов (это множество называется генерическим) и игнорируется его поведение 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 1970 г. Ю. В. Матиясевич [2], основываясь на работах М. Дэвиса, Дж. Робинсон и Х. Патнема, доказал, что проблема определения разрешимости диофантовых уравнений в целых числах, известная как десятая проблема Гильберта, алгоритмически неразрешима. В [3 – 5] показано, что основные функции шифрования многих криптографических систем с открытым ключом, среди которых система RSA и системы, основанные на трудноразрешимости проблемы дискретного логарифма, записываются на языке диофантовых уравнений. Эффективная генерическая разрешимость этих уравнений приводит к взлому соответствующих систем, поэтому актуальной является задача изучения генерической сложности проблемы разрешимости диофантовых уравнений в различных её постановках. Например, в [6, 7] доказано, что десятая проблема Гильберта остаётся неразрешимой на строго генерических подмножествах входов при представлении диофантовых уравнений с помощью так называемых арифметических схем. В [8] изучена генерическая сложность десятой проблемы Гильберта для систем диофантовых уравнений в форме Сколема.

В данной работе изучается генерическая сложность десятой проблемы Гильберта для диофантовых уравнений, представляемых в виде полиномиальных деревьев. Полиномиальное дерево — это бинарное дерево, листья которого помечены переменными или константой 1, а внутренние вершины содержат операции сложения, вычитания или умножения. Любой полином от многих переменных с целыми коэффициентами можно представить в виде такого полиномиального дерева. В работе доказывается, что проблема разрешимости диофантовых уравнений, представляемых в виде полиномиальных деревьев, является генерически неразрешимой.

1. Генерические алгоритмы

Пусть I — множество всех входов, а I_n — множество входов размера n. Для любого подмножества $S \subseteq I$ определим 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 $\rho(S) = 0$. Очевидно, что S генерическое тогда и только тогда, когда его дополнение $I \setminus S$ пренебрежимо.

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 $x \in I$ не выполнено $\mathcal{A}(x) = ?$, то $f(x) = \mathcal{A}(x)$. 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.

2. Представление диофантовых уравнений в виде полиномиальных деревьев

Здесь и далее под размером двоичного дерева понимается число листьев. *Полиномиальным деревом* называется бинарное дерево, листья которого помечены переменными из множества $\{x_1, \ldots, x_n\}$ (n — размер дерева) или константой 1, а внутренние вершины помечены знаками операций сложения, вычитания или умножения. Каждое полиномиальное дерево Φ с n листьями представляет некоторый полином $P_\Phi(x_1, \ldots, x_n)$ с целыми коэффициентами следующим образом:

1) $P_\Phi(x_1, \ldots, x_n) = 1$, если Φ состоит из одного листа, помеченного константой 1;
2) $P_\Phi(x_1, \ldots, x_n) = x_i$, если Φ состоит из одного листа, помеченного переменной x_i;
3) $P_\Phi(x_1, \ldots, x_n) = P_\Psi(x_1, \ldots, x_n) * P_\Sigma(x_1, \ldots, x_n)$, если Φ состоит из левого поддерева Ψ, правого поддерева Σ и корня, помеченного операцией $* \in \{+, -, \times\}$.

С другой стороны, легко видеть, что для любого полинома с целыми коэффициентами $P(x_1, \ldots, x_n)$ найдется полиномиальное дерево Φ (возможно, размера больше n) такое, что $P(x_1, \ldots, x_n) = P_\Phi(x_1, \ldots, x_n)$. Таким образом, будем представлять диофантовы уравнения вида $P(x_1, \ldots, x_n) = 0$ с помощью полиномиальных деревьев.

Будем называть полиномиальное дерево *нормализованным*, если при нумерации листьев дерева слево направо лист L_k может быть помечен переменной x_i, где $i \leqslant k$. Очевидно, что любое полиномиальное дерево можно нормализовать при помощи подходящего перенумерования переменных. В дальнейшем будем рассматривать только нормализованные полиномиальные деревья. Обозначим через $\mathcal{T}$ множество всех нормализованных полиномиальных деревьев.

Напомним, что числа Каталана C_n определяются следующим образом:

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

Здесь $\binom{2n}{n}$ — биномиальный коэффициент.

Лемма 1. Число нормализованных полиномиальных деревьев размера n есть

$$|\mathcal{T}_n| = 3^{n-1}(n+1)!C_{n-1}.$$

Доказательство. Любое дерево из $\mathcal{T}$ размера n есть размеченное бинарное дерево с n листьями и $n-1$ внутренними вершинами. Известно (см., например, [9]), что существует C_{n-1} неразмеченных бинарных деревьев с n листьями. Каждая внутренняя вершина такого дерева может быть помечена тремя символами $\{+,-,\times\}$, поэтому есть всего 3^{n-1} таких разметок. Занумеруем листья дерева слева направо. Из условия нормализованности следует, что лист с номером k может быть помечен одной из k переменных $x_1,\ldots,x_k$ или константой 1, поэтому существует $(n+1)!$ разметок для листьев. Это показывает, что $|\mathcal{T}_n| = 3^{n-1}(n+1)!C_{n-1}$. ■

В дальнейшем 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:

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

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

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

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

Лемма доказана. ■

3. Основной результат

Для произвольного полиномиального дерева Φ рассмотрим множество $\mathrm{eq}(\Phi)$ полиномиальных деревьев вида, представленного на рис. 1, где Ψ — произвольное полиномиальное дерево.

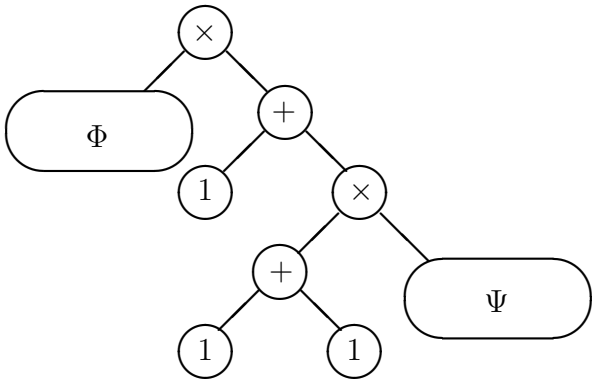

Рис. 1

Пусть m — размер дерева Φ. Заметим, что для любого $\Sigma \in \mathrm{eq}(\Phi)$ размера $n > m$ имеет место

$$P_\Sigma(x_1,\ldots,x_n) = P_\Phi(x_1,\ldots,x_m)(1+2P_\Psi(x_1,\ldots,x_n)).$$

Из этого следует, что диофантово уравнение $P_\Sigma(x_1,\dots,x_m)=0$ разрешимо в целых числах тогда и только тогда, когда разрешимо в целых числах диофантово уравнение $P_\Phi(x_1,\dots,x_k)=0$.

Лемма 3. Для любого полиномиального дерева Φ множество $\mathrm{eq}(\Phi)$ не является пренебрежимым.

Доказательство. Пусть m — размер дерева Φ и $n > m+3$. Любое дерево $\Sigma \in \mathrm{eq}(\Phi)_n$ имеет вид, приведённый на рис. 1. В нём произвольно может выбираться только поддерево Ψ с числом листьев $n-m-3$. Посчитаем, сколькими способами это можно сделать. Есть C_{n-m-4} неразмеченных бинарных деревьев с $n-m-3$ листьями. Внутренние $n-m-4$ вершин можно пометить арифметическими операциями 3^{n-m-4} способами. Занумеруем листья дерева Φ слева направо. Из условия нормализованности следует, что лист поддерева Ψ с номером $k > m+3$ может быть помечен одной из k переменных $x_1,\dots,x_k$ или константой 1, поэтому существует $(m+5)(m+6)\dots(n+1)$ разметок для листьев поддерева Ψ. Итого имеем

$$|\mathrm{eq}(\Phi)_n| = 3^{n-m-4}(m+5)(m+6)\dots(n+1)C_{n-m-4}.$$

По лемме 1 $|\mathcal{T}_n| = 3^{n-1}(n+1)!C_{n-1}$. Следовательно,

$$\rho_n(\mathrm{eq}(\Phi)) = \frac{|\mathrm{eq}(\Phi)_n|}{|\mathcal{T}_n|} = \frac{3^{n-m-4}(m+5)(m+6)\dots(n+1)C_{n-m-4}}{3^{n-1}(n+1)!C_{n-1}} =$$
$$= \frac{1}{3^{m+3}(m+4)!}\,\frac{C_{n-m-4}}{C_{n-1}} > \frac{1}{3^{m+3}(m+4)!}\,\frac{1}{4^{m+3}} = \mathrm{const} > 0.$$

Здесь использована лемма 2 для оценки отношения чисел Каталана. Таким образом, множество $\mathrm{eq}(\Phi)$ не является пренебрежимым. ■

Теперь докажем основной результат статьи.

Теорема 1. Проблема разрешимости диофантовых уравнений, представляемых в виде полиномиальных деревьев, не является генерически разрешимой.

Доказательство. Допустим, что существует генерический алгоритм $\mathcal{A}$, определяющий разрешимость диофантовых уравнений, заданных полиномиальными деревьями, на некотором генерическом множестве полиномиальных деревьев. Используя этот алгоритм, построим алгоритм $\mathcal{B}$, который будет определять разрешимость диофантовых уравнений для всех полиномиальных деревьев. Тем самым получим противоречие с неразрешимостью Десятой проблемы Гильберта.

Алгоритм $\mathcal{B}$ на дереве Φ работает следующим образом: перебирает элементы $\mathrm{eq}(\Phi)$ в порядке возрастания размера до тех пор, пока не получит дерево $\Sigma \in \mathrm{eq}(\Phi)$, такое, что $\mathcal{A}(\Sigma) \neq ?$. Ответ $\mathcal{A}(\Sigma)$ и будет правильным ответом для исходного дерева Φ.

То, что всегда найдётся такое дерево Σ, следует из того, что множество $\{\Psi \in \mathcal{T} : \mathcal{A}(\Psi) = ?\}$ пренебрежимо, а множество $\mathrm{eq}(\Phi)$, по лемме 3, не является пренебрежимым. Теорема доказана. ■

ЛИТЕРАТУРА

1. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks // J. Algebra. 2003. V. 264. No. 2. P. 665–694.
2. *Матиясевич Ю. В.* Диофантовость перечислимых множеств // Доклады АН СССР. 1970. Т. 191. № 2. С. 279–282.
3. *Myasnikov A. and Romankov V.* Diophantine cryptography in free metabelian groups: Theoretical base // Groups, Complexity, Cryptology. 2014. V. 6. No. 2. P. 103–120.

4. *Романьков В. А.* Диофантова криптография на бесконечных группах // Прикладная дискретная математика. 2012. № 2 (16). С. 15–42.
5. *Романьков В. А.* Алгебраическая криптография. Омск: ОмГУ, 2013.
6. *Rybalov A.* Generic complexity of the Diophantine problem // Groups, Complexity, Cryptology. 2013. V. 5. No. 1. P. 25–30.
7. *Рыбалов А.* О генерической неразрешимости Десятой проблемы Гильберта // Вестник Омского университета. 2011. № 4. С. 19–22.
8. *Рыбалов А.* О генерической сложности проблемы разрешимости систем диофантовых уравнений в форме Сколема // Прикладная дискретная математика. 2017. № 37. С. 100–106.
9. *Кнут Д.* Искусство программирования. М.: Вильямс, 2010. 720 с.

REFERENCES

1. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks. J. Algebra, 2003, vol. 264, no. 2, pp. 665–694.
2. *Matiyasevich Yu. V.* Diofantovost' perechislimykh mnozhestv [Diophantineity of enumerable sets]. Doklady Akademii Nauk USSR, 1970, vol. 191, no. 2, pp. 279–282. (in Russian)
3. *Myasnikov A. and Romankov V.* Diophantine cryptography in free metabelian groups: Theoretical base. Groups, Complexity, Cryptology, 2014, vol. 6, no. 2, pp. 103–120.
4. *Roman'kov V. A.* Diofantova kriptografiya na beskonechnykh gruppakh [Diophantine cryptography over infinite groups]. Prikladnaya Diskretnaya Matematika, 2012, no. 2 (16), pp. 15–42. (in Russian)
5. *Roman'kov V. A.* Algebraicheskaya Kriptografiya [Algebraic Cryptography]. Omsk, OmSU Publ., 2013. (in Russian)
6. *Rybalov A.* Generic complexity of the Diophantine problem. Groups, Complexity, Cryptology, 2013, vol. 5, no. 1, pp. 25–30.
7. *Rybalov A.* O genericheskoy nerazreshimosti Desyatoy problemy Gil'berta [On generic undecidability of Hilbert Tenth problem]. Vestnik Omskogo Universiteta, 2011, no. 4, pp. 19–22. (in Russian)
8. *Rybalov A.* O genericheskoy slozhnosti problemy razreshimosti sistem diofantovyh uravneniy v forme Skolema [On generic complexity of decidability problem for diophantine systems in the Skolem's form]. Prikladnaya Diskretnaya Matematika, 2017, no. 37, pp. 100–106. (in Russian)
9. *Knuth D. E.* The Art of Computer Programming. Reading, Massachusetts, Addison-Wesley, 1997.