УДК 510.52

О ГЕНЕРИЧЕСКОЙ СЛОЖНОСТИ ПРОБЛЕМЫ РАЗРЕШИМОСТИ СИСТЕМ ДИОФАНТОВЫХ УРАВНЕНИЙ В ФОРМЕ СКОЛЕМА[1]

А. Н. Рыбалов

Омский государственный университет им. Ф. М. Достоевского, г. Омск, Россия,
Институт математики им. С. Л. Соболева СО РАН, г. Новосибирск, Россия

Изучается генерическая сложность десятой проблемы Гильберта для систем диофантовых уравнений в форме Сколема. Приводится генерический полиномиальный алгоритм, определяющий разрешимость таких систем уравнений над множеством натуральных чисел (без нуля). Доказывается, что проблема разрешимости таких систем уравнений над множеством целых чисел является неразрешимой на любом рекурсивном строго генерическом подмножестве входов. Доказательство этой теоремы проходит также для случая, когда решения ищутся во множестве натуральных чисел с нулём.

Ключевые слова: *генерическая сложность, диофантовы уравнения.*

DOI 10.17223/20710410/37/8

ON GENERIC COMPLEXITY OF DECIDABILITY PROBLEM FOR DIOPHANTINE SYSTEMS IN THE SKOLEM'S FORM

A. N. Rybalov

Omsk State University, Omsk, Russia,
Sobolev Institute of Mathematics, Novosibirsk, 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. This approach has applications in cryptography where it is required that algorithmic problems must be difficult for almost all inputs. Romankov in 2012 shows that the basic encryption functions of many public key cryptographic systems, among which the RSA system and systems, based on the intractability of the discrete logarithm problem, can be written in the language of Diophantine equations. The effective generic decidability of these equations leads to hacking of corresponding systems, therefore it is actual to study the generic complexity of the decidability problem for Diophantine equations in various formulations. For example, Rybalov in 2011 proved that the Hilbert's tenth problem remains undecidable on strongly generic subsets of inputs in the representation of Diophantine equations by so-called arithmetic schemes. In this paper, we study generic complexity of the Hilbert's tenth problem for systems of Diophantine equations in the Skolem's form. We construct generic polynomial algorithm for determination of solvability of such systems over natural numbers (without zero). We prove strongly generic undecidability of this problem for systems over integers and over natural numbers with zero.

[1]Работа поддержана грантом РФФИ № 15-41-04312.

Keywords: *generic complexity, diophantine equations.*

Введение

В 1900 г. Д. Гильберт на II математическом конгрессе сформулировал 23 математические проблемы, которые XIX век оставил в наследство XX веку. Десятая проблема в современной формулировке звучит следующим образом: найти алгоритм, который по любому диофантовому уравнению определяет, разрешимо ли оно в целых числах. В 1970 г. Ю. В. Матиясевич [1], основываясь на работах М. Дэвиса, Дж. Робинсон и Х. Патнема, доказал, что такого алгоритма не существует. В дальнейшем было доказано, что десятая проблема Гильберта алгоритмически неразрешима уже для диофантовых уравнений от тринадцати неизвестных (Матиясевич, Робинсон [2]). Оценка улучшена до девяти неизвестных (Дж. Джонс [3]).

Генерический подход в применении к алгоритмическим проблемам впервые предложен в 2003 г. в [4]. В рамках этого подхода изучается поведение алгоритма на множестве «почти всех» входов (это множество называется генерическим), игнорируя 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 [5 – 7] 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 [8, 9] доказано, что десятая проблема Гильберта остаётся неразрешимой на строго генерических подмножествах входов при представлении диофантовых уравнений с помощью так называемых арифметических схем. В данной работе изучается генерическая сложность десятой проблемы Гильберта для систем диофантовых уравнений в форме Сколема. Приводится генерический полиномиальный алгоритм для проблемы разрешимости таких систем уравнений над множеством натуральных чисел (без нуля). Доказывается, что проблема разрешимости таких систем уравнений над множеством целых чисел является неразрешимой на любом рекурсивном строго генерическом подмножестве входов.

1. Генерические алгоритмы

Пусть I — некоторое множество. Через $\mathbb{N}$ будем обозначать множество натуральных чисел (без нуля), а через $\mathbb{N}_0$ — натуральные числа с нулём. Функция $\mathrm{size} : I \to \mathbb{N}_0$ называется *функцией размера*, если для любого $n \in \mathbb{N}_0$ множество $I_n = \{x \in I : \mathrm{size}(x) = n\}$ конечно. Например, на множестве $I = \Sigma^*$ слов конечного алфавита Σ естественно определяется функция размера (длины) $w \mapsto |w|$, где $|w|$ — длина слова w. На $\mathbb{N}$ также естественно определяется функция размера (длины двоичной записи) $n \mapsto |n|_2$, где $|n|_2$ — длина двоичной записи числа n. Как обычно делается в теории вычислимости, будем под алгоритмическими проблемами понимать проблемы распознавания подмножеств из некоторого множества входов с определённой на нём функцией размера. Зафиксируем некоторое множество входов I и функцию размера на этом множестве. Для 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. Заметим, что $\rho_n(S)$ — это вероятность попасть в S при случайной и равновероятной генерации входов из I_n. *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.

Следуя [4], назовём множество S *строго пренебрежимым*, если последовательность $\rho_n(S)$ экспоненциально быстро сходится к 0, т. е. существуют константы $0 < \sigma < 1$ и $C > 0$, такие, что для любого n

$$\rho_n(S) < C\sigma^n.$$

Теперь S называется *строго генерическим*, если его дополнение $I \setminus S$ строго пренебрежимо.

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

1) $\mathcal{A}$ останавливается на всех входах из I;
2) множество $\{x \in I : \mathcal{A}(x) = ?\}$ является (строго) 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 (*строго*) *генерически разрешимым*, если существует (строго) генерический алгоритм, вычисляющий его характеристическую функцию.

2. Системы диофантовых уравнений в форме Сколема

Система диофантовых уравнений записана в *форме Сколема* [10], если каждое уравнение в ней имеет один из следующих типов:

1) $x_i = x_j x_k$,
2) $x_i = x_j + x_k$,
3) $x_i = 1$.

Нетрудно показать, что для любого диофантова уравнения (системы) можно эффективно построить эквивалентную ему систему диофантовых уравнений в форме Сколема. Например, для уравнения $x^2 - 3y^2 = 1$ эквивалентной системой Сколема является

$$x_1 = x_2x_2,\ x_3 = x_4x_4,\ x_5 = x_3 + x_3,\ x_6 = x_5 + x_3,\ x_7 = 1,\ x_8 = x_6 + x_7,\ x_8 = x_1.$$

Будем называть систему в форме Сколема *нормализованной*, если в k-м уравнении системы могут встречаться только переменные x_i, где $i \leqslant 3k$. Очевидно, что любую систему в форме Сколема можно нормализовать при помощи подходящего перенумерования переменных. В дальнейшем будем рассматривать только нормализованные системы диофантовых уравнений в форме Сколема. Размер такой системы — это число уравнений в ней. Обозначим через $\mathcal{S}$ множество всех нормализованных систем в форме Сколема.

Лемма 1. Число нормализованных систем в форме Сколема размера n есть

$$|\mathcal{S}_n| = \prod_{k=1}^{n}(54k^3 + 3k).$$

Доказательство. Для k-го уравнения в системе $S \in \mathcal{S}_n$ существует $(3k)^3$ вариантов выбрать уравнение вида $x_i = x_j x_k$, также $(3k)^3$ вариантов выбрать уравнение вида $x_i = x_j + x_k$ и только $3k$ вариантов выбрать уравнение вида $x_i = 1$. Итого для k-го уравнения есть $54k^3 + 3k$ вариантов. Отсюда получаем требуемое равенство. ■

3. Системы в форме Сколема над натуральными числами

Приведём полиномиальный генерический алгоритм для проверки разрешимости диофантовых уравнений в форме Сколема над множеством натуральных чисел $\mathbb{N}$.

Теорема 1. Проблема разрешимости диофантовых уравнений в форме Сколема над множеством $\mathbb{N}$ генерически разрешима за полиномиальное время.

Доказательство. Соответствующий генерический полиномиальный алгоритм работает на системе S следующим образом:

1) ищет в системе S уравнение вида $x_i = x_i + x_j$;
2) если такое уравнение найдётся, то система неразрешима над $\mathbb{N}$ и алгоритм выдаёт ответ 0;
3) иначе выдает ответ «?».

Покажем, что этот алгоритм дает неопределённый ответ на пренебрежимом множестве систем Сколема. Обозначим через $\mathcal{L}$ множество систем, в которых отсутствуют уравнения вида $x_i = x_i + x_j$. Число вариантов выбрать k-е уравнение в системе из множества $\mathcal{L}$ есть $54k^3 + 3k - 9k^2$. Поэтому

$$|\mathcal{L}_n| = \prod_{k=1}^{n}(54k^3 + 3k - 9k^2).$$

По лемме 1 $|\mathcal{S}_n| = \prod\limits_{k=1}^{n}(54k^3 + 3k)$, поэтому

$$\rho_n(\mathcal{L}) = \frac{|\mathcal{L}_n|}{|\mathcal{S}_n|} = \frac{\prod\limits_{k=1}^{n}(54k^3 + 3k - 9k^2)}{\prod\limits_{k=1}^{n}(54k^3 + 3k)} = \prod_{k=1}^{n}\frac{18k^3 + k - 3k^2}{18k^3 + k} = \prod_{k=1}^{n}\Big(1 - \frac{3k^2}{18k^3 + k}\Big) <$$

$$< \prod_{k=1}^{n}\Big(1 - \frac{3k^2}{18k^3 + k^3}\Big) = \prod_{k=1}^{n}\Big(1 - \frac{3}{19k}\Big) < \prod_{k=1}^{n}\Big(1 - \frac{1}{7k}\Big).$$

Для того чтобы оценить сверху последнее произведение, возведём его в степень 7:

$$\prod_{k=1}^{n}\Big(1 - \frac{1}{7k}\Big)^7 < \prod_{k=1}^{n}\Big(\big(1 - \frac{1}{7k}\big)\big(1 - \frac{1}{7k+1}\big)\ldots\big(1 - \frac{1}{7k+6}\big)\Big) = \prod_{k=7}^{n}\Big(1 - \frac{1}{k}\Big) =$$

$$= \prod_{k=7}^{n}\frac{k-1}{k} = \frac{6}{7}\cdot\frac{7}{8}\cdot\ldots\cdot\frac{n-2}{n-1}\cdot\frac{n-1}{n} = \frac{6}{n}.$$

В результате получаем

$$\rho(\mathcal{L}) = \lim_{n\to\infty}\frac{|\mathcal{L}_n|}{|\mathcal{S}_n|} \leqslant \lim_{n\to\infty}\sqrt[7]{\frac{6}{n}} = 0.$$

Теорема доказана. ■

4. Системы в форме Сколема над целыми числами

Докажем, что проблема разрешимости нормализованных систем диофантовых уравнений в форме Сколема над множеством целых чисел является неразрешимой на любом рекурсивном строго генерическом подмножестве входов.

Для произвольной нормализованной системы диофантовых уравнений в форме Сколема $S = \{S_1, \ldots, S_m\}$ рассмотрим множество систем $\mathrm{eq}(S)$, которые получаются добавлением к системе S любого количества произвольных уравнений вида $x_i = x_j x_k$ или $x_i = x_j + x_k$, где $i, j, k > 3m$, с сохранением условия нормализации. Очевидно, что любая система из $\mathrm{eq}(S)$ разрешима в целых числах тогда и только тогда, когда разрешима в целых числах система S.

Лемма 2. Для любой системы S множество $\mathrm{eq}(S)$ не является строго пренебрежимым.

Доказательство. Пусть $n > m$. Для t-го добавленного к S уравнения вида $x_i = x_j x_k$ или $x_i = x_j + x_k$, где $i, j, k > 3m$, имеется $2(3t)^3 = 54t^3$ вариантов. Поэтому

$$|\mathrm{eq}(S)_n| = \prod_{t=1}^{n-m} (54t^3).$$

Теперь по лемме 1

$$\rho_n(\mathrm{eq}(S)) = \frac{|\mathrm{eq}(S)_n|}{|\mathcal{S}_n|} = \frac{\prod\limits_{k=1}^{n-m} (54k^3)}{\prod\limits_{k=1}^{n} (54k^3 + k)} = \prod_{k=1}^{n-m} \frac{54k^2}{54k^2 + 1} \prod_{k=n-m+1}^{n} \frac{1}{54k^3 + k}.$$

Оценим снизу первое произведение:

$$\prod_{k=1}^{n-m} \frac{54k^2}{54k^2 + 1} = \prod_{k=1}^{n-m} \Big(1 - \frac{1}{54k^2 + 1}\Big) > \prod_{k=2}^{n-m+1} \Big(1 - \frac{1}{k^2}\Big) = \prod_{k=2}^{n-m+1} \frac{(k-1)(k+1)}{k^2} =$$
$$= \frac{1 \cdot 3}{2^2} \frac{2 \cdot 4}{3^2} \frac{(n-m-1)(n-m+1)}{(n-m)^2} \frac{(n-m)(n-m+2)}{(n-m+1)^2} = \frac{n-m+2}{2(n-m+1)} > \frac{1}{2}.$$

Теперь оценим второе произведение:

$$\prod_{k=n-m+1}^{n} \frac{1}{54k^3 + k} > \frac{1}{(54n^3 + n)^m}.$$

Получаем

$$\rho_n(\mathrm{eq}(S)) = \frac{|\mathrm{eq}(S)_n|}{|\mathcal{S}_n|} > \frac{1}{2(54n^3 + n)^m}.$$

Из этого неравенства следует, что последовательность $\rho_n(\mathrm{eq}(S))$ не может стремиться к нулю экспоненциально быстро. Поэтому множество $\mathrm{eq}(S)$ не является строго пренебрежимым. ■

Теорема 2. Проблема разрешимости нормализованных систем диофантовых уравнений в форме Сколема над множеством целых чисел не является строго генерически разрешимой.

Доказательство. Допустим, что существует строго генерический алгоритм $\mathcal{A}$, определяющий разрешимость диофантовых систем на некотором строго генерическом

множестве входов. Используя этот алгоритм, построим алгоритм $\mathcal{B}$, который будет определять разрешимость диофантовых систем на всём множестве входов. Тем самым получим противоречие с неразрешимостью десятой проблемы Гильберта.

Алгоритм $\mathcal{B}$ на системе S работает следующим образом: перебирает элементы $\mathrm{eq}(S)$ в порядке возрастания размера до тех пор, пока не получит систему $S' \in \mathrm{eq}(S)$, такую, что $\mathcal{A}(S') \neq ?$. Ответ $\mathcal{A}(S')$ и будет правильным ответом для исходной системы S.

То, что всегда найдётся такая система S', следует из того, что множество $\{S \in \mathcal{S} : \mathcal{A}(S) = ?\}$ строго пренебрежимо, а множество $\mathrm{eq}(S)$ не является строго пренебрежимым. ■

Заметим, что доказательство этой теоремы проходит для случая, когда решения ищутся во множестве натуральных чисел с нулём $\mathbb{N}_0$.

Автор выражает искреннюю благодарность рецензенту за полезные замечания и предложения по улучшению текста статьи.

ЛИТЕРАТУРА

1. *Матиясевич Ю. В.* Диофантовость перечислимых множеств // Доклады Академии наук СССР. 1970. Т. 191. № 2. С. 279–282.
2. *Matiyasevich Yu. and Robinson J.* Reduction of an arbitrary Diophantine equation to one in 13 unknowns // Acta Arithmetica. 1975. V. 27. P. 521–553.
3. *Jones J.* Undecidable Diophantine equations // Bull. Amer. Math. Soc. 1980. V. 3. No. 2. P. 859–862.
4. *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.
5. *Myasnikov A. and Romankov V.* Diophantine cryptography in free metabelian groups: Theoretical base // Groups, Complexity, Cryptology. 2014. V. 6. No. 2. P. 103–120.
6. *Романьков В. А.* Диофантова криптография на бесконечных группах // Прикладная дискретная математика. 2012. № 2 (16). С. 15–42.
7. *Романьков В. А.* Алгебраическая криптография. Омск: ОмГУ, 2013.
8. *Rybalov A.* Generic complexity of the Diophantine problem // Groups, Complexity, Cryptology. 2013. V. 5. No. 1. P. 25–30.
9. *Рыбалов А.* О генерической неразрешимости Десятой проблемы Гильберта // Вестник Омского университета. 2011. № 4. С. 19–22.
10. *Skolem T.* Diophantische Gleichungen. Berlin: Springer, 1938.

REFERENCES

1. *Matiyasevich Yu. V.* Diofantovost' perechislimykh mnozhestv [Diophantineity of enumerable sets]. Doklady Akademii Nauk USSR, 1970, vol. 191, no. 2, pp. 279–282. (in Russian)
2. *Matiyasevich Yu. and Robinson J.* Reduction of an arbitrary Diophantine equation to one in 13 unknowns. Acta Arithmetica, 1975, vol. 27, pp. 521–553.
3. *Jones J.* Undecidable Diophantine equations. Bull. Amer. Math. Soc., 1980, vol. 3, no. 2, pp. 859–862.
4. *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.
5. *Myasnikov A. and Romankov V.* Diophantine cryptography in free metabelian groups: Theoretical base. Groups, Complexity, Cryptology, 2014, vol. 6, no. 2, pp. 103–120.
6. *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)

7. *Roman'kov V. A.* Algebraicheskaya Kriptografiya [Algebraic Cryptography]. Omsk, OmSU Publ., 2013. (in Russian)
8. *Rybalov A.* Generic complexity of the Diophantine problem. Groups, Complexity, Cryptology, 2013, vol. 5, no. 1, pp. 25–30.
9. *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)
10. *Skolem T.* Diophantische Gleichungen. Berlin, Springer, 1938.