О генерической сложности диофантовых проблем

Александр Рыбалов

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

19 июля, 2024

Десятая проблема Гильберта

Десятая проблема Гильберта

ВХОД: Многочлен $p(x_1, \ldots, x_n)$ с целыми коэффициентами.
Определить, разрешимо ли диофантово уравнение $p(x_1, \ldots, x_n) = 0$ в целых числах.

Десятая проблема Гильберта

Десятая проблема Гильберта

ВХОД: Многочлен $p(x_1, \ldots, x_n)$ с целыми коэффициентами.
Определить, разрешимо ли диофантово уравнение $p(x_1, \ldots, x_n) = 0$ в целых числах.

Теорема (Дэвис, Патнем, Робинсон, Матиясевич, 1970)

Десятая проблема Гильберта алгоритмически неразрешима.

Вопрос Виталия Анатольевича Романькова

Пусть $p(a, x_1, \ldots, x_n)$ – многочлен с целыми коэффициентами.

Параметрическая десятая проблема Гильберта

ВХОД: натуральное число a. Определить, разрешимо ли диофантово уравнение $p(a, x_1, \ldots, x_n) = 0$ в целых числах.

Вопрос Виталия Анатольевича Романькова

Пусть $p(a, x_1, \ldots, x_n)$ – многочлен с целыми коэффициентами.

Параметрическая десятая проблема Гильберта

ВХОД: натуральное число a. Определить, разрешимо ли диофантово уравнение $p(a, x_1, \ldots, x_n) = 0$ в целых числах.

Теорема (Дэвис, Патнем, Робинсон, Матиясевич, 1970)

Существует такой многочлен $p(a, x_1, \ldots, x_n)$, что параметрическая десятая проблема Гильберта алгоритмически неразрешима.

Вопрос Виталия Анатольевича Романькова

Пусть $p(a, x_1, \ldots, x_n)$ – многочлен с целыми коэффициентами.

Параметрическая десятая проблема Гильберта

ВХОД: натуральное число a. Определить, разрешимо ли диофантово уравнение $p(a, x_1, \ldots, x_n) = 0$ в целых числах.

Теорема (Дэвис, Патнем, Робинсон, Матиясевич, 1970)

Существует такой многочлен $p(a, x_1, \ldots, x_n)$, что параметрическая десятая проблема Гильберта алгоритмически неразрешима.

Вопрос В.А.Романькова

Может ли параметрическая десятая проблема Гильберта быть генерически неразрешимой (трудноразрешимой)?

Генерические множества

Определение

Пусть I – все входы, I_n – все входы размера n.

Асимптотическая плотность множества $S \subseteq I$

$$\rho(S) = \lim_{n\to\infty} \rho_n = \lim_{n\to\infty} \frac{|S \cap I_n|}{|I_n|}.$$

Генерические множества

Определение

Пусть I – все входы, I_n – все входы размера n.

Асимптотическая плотность множества $S \subseteq I$

$$\rho(S) = \lim_{n\to\infty} \rho_n = \lim_{n\to\infty} \frac{|S \cap I_n|}{|I_n|}.$$

Определение

Множество входов $S \subseteq I$ называется

- **генерическим** если $\rho(S) = 1$,

Генерические множества

Определение

Пусть I – все входы, I_n – все входы размера n.

Асимптотическая плотность множества $S \subseteq I$

$$\rho(S) = \lim_{n\to\infty} \rho_n = \lim_{n\to\infty} \frac{|S \cap I_n|}{|I_n|}.$$

Определение

Множество входов $S \subseteq I$ называется

- **генерическим** если $\rho(S) = 1$,
- **пренебрежимым** если $\rho(S) = 0$.

Генерические алгоритмы

Определение

Алгоритм $\mathcal{A} : I \to J$ называется **генерическим**, если множество $\{x \in I : \mathcal{A}(x) \uparrow\}$ пренебрежимо.

Генерические алгоритмы

Определение

Алгоритм $\mathcal{A} : I \to J$ называется **генерическим**, если множество $\{x \in I : \mathcal{A}(x) \uparrow\}$ пренебрежимо.

Определение

Алгоритм $\mathcal{A} : I \to J \cup \{?\}$ называется **эффективно генерическим**, если

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

Генерические алгоритмы

Определение

Алгоритм $\mathcal{A} : I \to J$ называется **генерическим**, если множество $\{x \in I : \mathcal{A}(x) \uparrow\}$ пренебрежимо.

Определение

Алгоритм $\mathcal{A} : I \to J \cup \{?\}$ называется **эффективно генерическим**, если

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

Определение

(Эффективно) генерический алгоритм $\mathcal{A}$ вычисляет функцию $f : I \to J$, если $\mathcal{A}(x) \downarrow (\neq ?) \Rightarrow \mathcal{A}(x) = f(x)$.

Полиномиальные генерические алгоритмы

Определение

Генерический алгоритм $\mathcal{A}$ **полиномиальный**, если существует полином $p(n)$ такой, что

$$\forall x(\mathcal{A}(x)\downarrow) \Rightarrow t_{\mathcal{A}}(x) < p(|x|).$$

Полиномиальные генерические алгоритмы

Определение

Генерический алгоритм $\mathcal{A}$ **полиномиальный**, если существует полином $p(n)$ такой, что

$$\forall x(\mathcal{A}(x)\downarrow) \Rightarrow t_{\mathcal{A}}(x) < p(|x|).$$

- Генерическая разрешимость $\Rightarrow$ Эффективная генерическая разрешимость.

Полиномиальные генерические алгоритмы

Определение

Генерический алгоритм $\mathcal{A}$ **полиномиальный**, если существует полином $p(n)$ такой, что

$$\forall x(\mathcal{A}(x)\downarrow) \Rightarrow t_{\mathcal{A}}(x) < p(|x|).$$

- Генерическая разрешимость $\Rightarrow$ Эффективная генерическая разрешимость.
- Генерическая полиномиальная разрешимость $=$ Эффективная полиномиальная генерическая разрешимость.

Ответ на вопрос В.А.Романькова

Теорема

Существуют такие многочлены $p(a, x_1, \ldots, x_n)$, что параметрическая десятая проблема Гильберта

Ответ на вопрос В.А.Романькова

Теорема

Существуют такие многочлены $p(a, x_1, \ldots, x_n)$, что параметрическая десятая проблема Гильберта

1. неразрешима, но генерически разрешима за полиномиальное время,

Ответ на вопрос В.А.Романькова

Теорема

Существуют такие многочлены $p(a, x_1, \ldots, x_n)$, что параметрическая десятая проблема Гильберта

1. неразрешима, но генерически разрешима за полиномиальное время,
2. генерически неразрешима,

Ответ на вопрос В.А.Романькова

Теорема

Существуют такие многочлены $p(a, x_1, \ldots, x_n)$, что параметрическая десятая проблема Гильберта

1. неразрешима, но генерически разрешима за полиномиальное время,
2. генерически неразрешима,
3. разрешима, но не генерически разрешима за полиномиальное время.

Идеи доказательства

Теорема (Дэвис, Патнем, Робинсон, Матиясевич, 1970)

Для любого рекурсивно перечислимого множества $S \subseteq \mathbb{N}$ существует такой многочлен $p_S(a, x_1, \ldots, x_n)$, что

$$a \in S \Leftrightarrow p_S(a, x_1, \ldots, x_n) = 0.$$

Идеи доказательства

Теорема (Дэвис, Патнем, Робинсон, Матиясевич, 1970)

Для любого рекурсивно перечислимого множества $S \subseteq \mathbb{N}$ существует такой многочлен $p_S(a, x_1, \ldots, x_n)$, что

$$a \in S \Leftrightarrow p_S(a, x_1, \ldots, x_n) = 0.$$

Пусть S – рекурсивно перечислимое неразрешимое множество, тогда $2^S = \{2^a \ : \ a \in S\}$ – неразрешимо, но генерически разрешимо.

Построение генерически неразрешимого множества

Определим функцию $C : \mathbb{N} \to P(\mathbb{N})$ для любого $a \in \mathbb{N}$ следующим образом

$$C(a) = \{2^a(2k+1) : k \in \mathbb{N}\}.$$

Легко подсчитать, что $\rho(C(a)) = \frac{1}{2^{size(a)+1}} > 0$ для любого a. Таким образом, для любого a множество $C(a)$ непренебрежимо.

Построение генерически неразрешимого множества

Определим функцию $C : \mathbb{N} \to P(\mathbb{N})$ для любого $a \in \mathbb{N}$ следующим образом

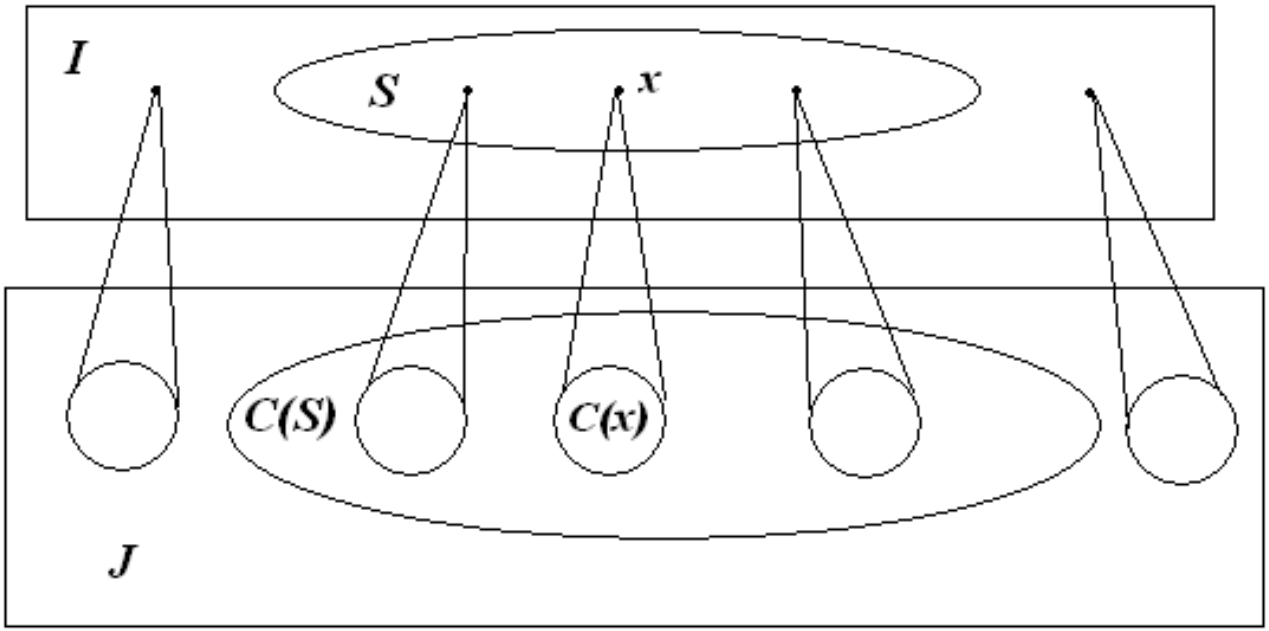
$$C(a) = \{2^a(2k+1) : k \in \mathbb{N}\}.$$

Легко подсчитать, что $\rho(C(a)) = \frac{1}{2^{size(a)+1}} > 0$ для любого a. Таким образом, для любого a множество $C(a)$ непренебрежимо.
Теперь для $S \subseteq \mathbb{N}$ определим

$$C(S) = \bigcup_{a \in S} C(a).$$

Для любого $a \in S$ имеет место $C(a) \subset C(S)$, а для любого $a \notin S$ имеет место $C(a) \subset \overline{C(S)} = \mathbb{N} \setminus C(S)$.

Генерическая амплификация



Построение генерически трудного множества

Пусть есть эффективная нумерация полиномиальных машин Тьюринга $P_1, P_2, P_3, \ldots$. Образуем из них следующую последовательность

$$\{M_i, i = 1, 2, 3, \ldots\} = \{P_1, P_1, P_2, P_1, P_2, P_3, P_1, P_2, P_3, P_4, P_1, P_2, \ldots\}.$$

Построение генерически трудного множества

Стартуя с множества всех натуральных чисел $\mathbb{N}$ на нулевом шаге, мы будем на шаге i вычеркивать или оставлять некоторые числа в завсисимости от поведения машины M_i. Опишем подробно шаг $i > 0$. Запускаем машину M_i на каждом входе размера i и считаем количество ответов ДА и количество ответов НЕТ. Если ответов ДА получилось больше половины, то вычеркиваем все входы размера i, иначе все их оставляем. Предельное множество в этом процессе и есть искомое множество S.

Обзор других результатов

1. Генерическая неразрешимость десятой проблемы Гильберта для арифметических схем (Рыбалов, 2013).

Обзор других результатов

1. Генерическая неразрешимость десятой проблемы Гильберта для арифметических схем (Рыбалов, 2013).
2. Генерическая неразрешимость десятой проблемы Гильберта для систем уравнений в форме Сколема (Рыбалов, 2017).

Обзор других результатов

1. Генерическая неразрешимость десятой проблемы Гильберта для арифметических схем (Рыбалов, 2013).
2. Генерическая неразрешимость десятой проблемы Гильберта для систем уравнений в форме Сколема (Рыбалов, 2017).
3. Генерическая неразрешимость десятой проблемы Гильберта для арифметических деревьев (Рыбалов, 2020).

Обзор других результатов

1. Генерическая неразрешимость десятой проблемы Гильберта для арифметических схем (Рыбалов, 2013).
2. Генерическая неразрешимость десятой проблемы Гильберта для систем уравнений в форме Сколема (Рыбалов, 2017).
3. Генерическая неразрешимость десятой проблемы Гильберта для арифметических деревьев (Рыбалов, 2020).
4. Генерическая трудноразрешимость проблемы двух квадратов (Рыбалов, 2019).

Проблема двух квадратов

Проблема

ВХОД: натуральное число N в двоичном виде. Определить, разрешимо ли в целых числах уравнение $x^2 + y^2 = N$.

Проблема двух квадратов

Проблема

ВХОД: натуральное число N в двоичном виде. Определить, разрешимо ли в целых числах уравнение $x^2 + y^2 = N$.

Рождественская теорема Ферма

Каждое простое число вида $4n + 1$ есть сумма двух квадратов целых чисел.

Проблема двух квадратов

Проблема

ВХОД: натуральное число N в двоичном виде. Определить, разрешимо ли в целых числах уравнение $x^2 + y^2 = N$.

Рождественская теорема Ферма

Каждое простое число вида $4n + 1$ есть сумма двух квадратов целых чисел.

Теорема (Ферма-Эйлер)

Диофантово уравнение $N = x^2 + y^2$ разрешимо в целых числах тогда и только тогда, когда каждый простой делитель N вида $4k + 3$ входит в разложение N в четной степени.

Сложность проблемы двух квадратов

Открытая проблема

Существует ли полиномильный алгоритм для проблемы двух квадратов?

Сложность проблемы двух квадратов

Открытая проблема

Существует ли полиномильный алгоритм для проблемы двух квадратов?

Полиномиальный алгоритм для проблемы факторизации $\Rightarrow$ Полиномиальный алгоритм для проблемы двух квадратов.

Сложность проблемы двух квадратов

Открытая проблема

Существует ли полиномильный алгоритм для проблемы двух квадратов?

Полиномиальный алгоритм для проблемы факторизации $\Rightarrow$ Полиномиальный алгоритм для проблемы двух квадратов.

Теорема (Адлеман, Мандерс)

Обобщение проблемы двух квадратов (для произвольных бинарных квадратичных форм) NP-полно.

Генерическая амплификация проблемы двух квадратов

$N \to N(a^2 + b^2)$ со случайными большими a и b.

Генерическая амплификация проблемы двух квадратов

$N \to N(a^2 + b^2)$ со случайными большими a и b.

Вопрос

Почему клон будет большим?

Генерическая амплификация проблемы двух квадратов

$N \to N(a^2 + b^2)$ со случайными большими a и b.

Вопрос

Почему клон будет большим?

Теорема (Гаусс)

Пусть $N(r)$ есть число решений неравенства $x^2 + y^2 \leq r$ в натуральных числах. Тогда

$$|N(r) - \frac{\pi r}{4}| \leq \frac{\sqrt{2}\pi\sqrt{r}}{2}.$$

Спасибо за внимание!

Спасибо за внимание!