Генерическая NP-полнота проблем разрешимости систем уравнений над конечными группами, полугруппами и полями

Горкун Илья

Омский государственный университет им.Ф.М.Достоевского, Омск

Сентябрь, 2023

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 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 $\rho(S) = 0$,
- **сильно генерическим** если последовательность ρ_n экспоненциально быстро стремится к 1,

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 $\rho(S) = 0$,
- **сильно генерическим** если последовательность ρ_n экспоненциально быстро стремится к 1,
- **сильно пренебрежимым**, если ρ_n экспоненциально быстро стремится к 0.

Генерические алгоритмы

Определение

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

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

Генерические алгоритмы

Определение

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

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

Определение

Генерический алгоритм $\mathcal{A}$ вычисляет функцию $f : I \to J$, если для всех $x \in I$ $\mathcal{A}(x) = y \in J \Rightarrow f(x) = y$.

Полиномиальные генерические сводимости

Множество $A \subseteq I$ **сильно генерически полиномиально сводится** к множеству $B \subseteq J$, если существуют вероятностный полиномиальный алгоритм $\mathcal{R} : I \times \mathbb{N} \to P(J) \cup \{?, !\}$, полином $p(n)$, полином $q(n)$ степени больше 2 и константа $C > 0$ такие, что

1. $\forall x \in I$ либо $\forall n\ \mathcal{R}(x, n) = \{?\}$, либо $\forall n \geq q(k)$, где $k = size(x)$, имеет место
   1. $\forall y \in \mathcal{R}(x, n)\ y \neq !\ \Rightarrow\ size(y) = n$.
   2. Все элементы в $\mathcal{R}(x, n) \setminus \{!\}$, выдаются алгоритмом $\mathcal{R}$ равновероятно.
   3. Вероятность получить ответ "!" в $\mathcal{R}(x, n)$ не больше 2^{-Ck}.
   4. $\frac{|\mathcal{R}(x,n)|}{|J_n|} > \frac{1}{(p(n))^k}$.
   5. $x \in A \Rightarrow \mathcal{R}(x, n) \subseteq B$.
   6. $x \notin A \Rightarrow \mathcal{R}(x, n) \subseteq J \setminus B$.
2. Множество $\{x \in I : \forall n\ \mathcal{R}(x, n) = \{?\}\}$ строго пренебрежимо.

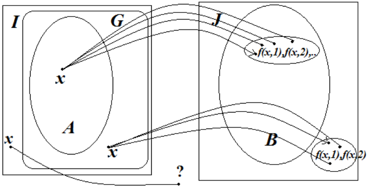

Рис.: Генеричесчкая сводимость

Определим генерический аналог класса NP. Множество $S \subseteq I$ принадлежит классу $\mathrm{sg}\,\mathrm{NP}$, если существует полиномиальное строго генерическое множество $G \subseteq I$, такое, что $S \cap G \in \mathrm{NP}$. Множество $S \in \mathrm{sg}\,\mathrm{NP}$ называется *генерически NP-полным*, если для любого $A \in \mathrm{sg}\,\mathrm{NP}$ имеет место $A \leq_{GenP} S$.

Проблема разрешимости систем уравнений

Многие применения алгебры в информатике требует решения уравнений над различными конечными алгебраическими структурами: поля, группы, полугруппы, графы и другие. Но опять же, обычно эта проблема оказывается вычислительно сложной. NP-полнота этой проблемы над каждым конечным полем – общеизвестный факт. Гольдманн и Расселл в 2002 году доказали, что эта проблема разрешима за полиномиальное время для всех абелевых конечных групп и NP-полно для каждой неабелевой конечной группы. Клима, Тессон и Териен в 2007 году доказали полиномиальную разрешимость для каждого конечного коммутативного моноида, являющегося объединением подгрупп и NP-полно для остальных конечных моноидов. NP-полнота означает, что не существует полиномиального алгоритма, решающее систему уравнений, при условии $P \neq NP$.

Задача решения систем уравнений над конечными группами

Предположим, что G - конечная группа. *Система уравнений* S над G - это набор уравнений $\{e_0, \ldots, e_{n-1}\}$, где e_l, $l = 0, \ldots, n-1$ имеет форму $y_{3l+1}^{\epsilon_1} = y_{3l+2}^{\epsilon_2} y_{3l+3}^{\epsilon_3}$, где y_{3l+i}, $i = 1, 2, 3$, может быть константой из G или переменной x_j, $j = 1, \ldots, 3l+i$, и $\epsilon_{1,2,3} \in \{1, -1\}$. *Размер* системы S – это число уравнений n.

Теорема

Предположим G – конечная неабелевая группа. Проблема разрешимости систем уравнений над G генерически NP-полно.

Задача решения системы уравнений над конечными полугруппами

Пусть M – конечная полугруппа. *Система уравнений* S над M – набор из уравнений $\{e_0, \ldots, e_{n-1}\}$, где каждое уравнение e_l, $l = 0, \ldots, n-1$ имеет форму $y_{3l+1} = y_{3l+2} y_{3l+3}$, где y_{3l+i}, $i = 1, 2, 3$, может быть константой из M или переменной x_j, $j = 1, \ldots, 3l + i$. *Размер* системы S это число уравнений n.

Теорема

Пусть M – конечная полугруппа такая, что задача решения системы уравнений над M – NP-полно. Проблема разрешимости систем уравнений над M генерически NP-полно.

Задача решения системы уравнений над конечными полями

Пусть F – конечное поле. *Система уравнений* S над F – набор из уравнений $\{e_0, \dots, e_{n-1}\}$, где уравнение e_l, $l = 0, \dots, n-1$ имеет форму $y_{3l+1} = y_{3l+2} + y_{3l+3}$ или $y_{3l+1} = y_{3l+2} y_{3l+3}$, где y_{3l+i}, $i = 1, 2, 3$, может быть константой из F или переменной x_j, $j = 1, \dots, 3l + i$. *Размер* системы S – это число уравнений n.

Теорема

Пусть F – конечное поле. Проблема разрешимости систем уравнений над F генерически NP-полно.