Алгебраическая геометрия и алгоритмы в классе частично упорядоченных множеств

Выступающий: А. Ю. Никитин

ООО "Диплей"

Омск, 2023

Классическая алгебраическа геометрия исследует уравнения над полем вещественных чисел.

$$2x^3 + 3x^2 - x + 1.5 = 0.$$

Пусть $L = \mathbb{F} \cup \mathbb{R} \cup \mathbb{C}$, где

- $\mathbb{F}$ – множество функциональных символов;
- $\mathbb{R}$ – множество предикатных символов;
- $\mathbb{C}$ – множество константных символов.

Универсальная алгебраическая геометрия исследует уравнения над произвольными алгебраическими структурами $\mathcal{A} = \langle A; L \rangle$.

Алгебраическая геометрия над конкретными алгебраическими системами. Исследования.

- Свободная неабелева группа: Р.К. Линдон, А.А. Разборов, Г.С. Маканин, В.Н. Ремесленников, А.Г. Мясников и др.
- Абелевы группы: А.Г. Мясников, В.Н. Ремесленников, Э.Ю. Даниярова и др.
- Разрешимые группы: Н.С. Романовский, Е.И. Тимошенко и др.
- Полугруппы: М.В. Волков, Б.М. Верников, Л.Н. Шеврин, А.Н. Шевляков и др.
- Графы: А.В. Ильев, В.П. Ильев, А.В. Трейер, И.М. Бучинский и др.
- Дистрибутивные решетки, полурешетки: Ю.С. Дворжецкий, А.Н. Шевляков и др.

Определение

Частично упорядоченным множеством (частичным порядком) называется алгебраическая система $\mathcal{P} = \langle P; \leqslant^{(2)}, A \rangle$, где $\leqslant$ – предикатный символ отношения порядка и A – множество константных символов, на которой выполнены 3 аксиомы:

1. $\forall p \in P \ \ p \leqslant p$ *(рефлексивность)*;
2. $\forall p_1, p_2 \in P \ \ p_1 \leqslant p_2 \wedge p_2 \leqslant p_1 \rightarrow p_1 = p_2$ *(антисимметричность)*;
3. $\forall p_1, p_2, p_3 \in P \ \ p_1 \leqslant p_2 \wedge p_2 \leqslant p_3 \rightarrow p_1 \leqslant p_3$ *(транзитивность)*.

Определение

Термом в языке L от переменных X называется выражение, определенное рекурсивно следующим образом:

1. любая переменная $x \in X$ есть терм;
2. любая константа языка L есть терм;
3. если $t_1, \ldots, t_n$ – термы и $F^{(n)}$ функциональный символ языка L, то $F(t_1, \ldots, t_n)$ является термом.

Определение

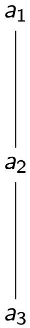
Атомарной формулой языка L от переменных X называется выражение, определенное следующим образом:

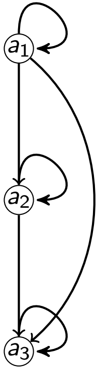
1. $\forall t_i, t_j \in T_L(X)$ $t_i = t_j$ является атомарной формулой;
2. для любого предикатного символа $R^{(n)}$ языка L и для любых термов $t_1, \ldots, t_n \in T_L(X)$ выражение $R(t_1, \ldots, t_n)$ является атомарной формулой.

Уравнения над частично упорядоченными множествами

A – константные символы в языке $\langle P; \leqslant^{(2)}, A\rangle$, X_n – переменные.

1. $a_i = a_j$, где $a_i, a_j \in A$,
2. $a_i \leqslant a_j$, где $a_i, a_j \in A$,
3. $x_i = a_j$, где $x_i \in X_n,\ a_j \in A$,
4. $x_i = x_j$, где $x_i, x_j \in X_n$,
5. $a_i \leqslant x_j$, где $x_j \in X_n,\ a_i \in A$,
6. $x_i \leqslant a_j$, где $x_i \in X_n,\ a_j \in A$,
7. $x_i \leqslant x_j$, где $x_i, x_j \in X_n$.


a_1
a_2
a_3


a_1
a_2
a_3

Сложность проблемы разрешимости системы уравнений над частичными порядками

Зафиксируем диофантов частичный порядок $\mathcal{P}$ в языке $L_A = \{\leqslant, A\}$. Задача разрешимости системы уравнений $S(X_n)$ над частичным порядком $\mathcal{P}$: совместна ли система уравнений $S(X_n)$ над частичным порядком $\mathcal{P}$ в языке L_A. Обозначается данная задача как $Cons(\mathcal{P})$.

Теорема 1

Пусть задан конечный частичный порядок $\mathcal{P}$. Если для соответствующего ему р-графа H в соответствующем неориентированном графе $U(H)$ содержится цикл без хорд длины больше 3, то задача $Cons(\mathcal{P})$ является NP-полной.

Теорема 2

Пусть $\mathcal{P}$ – частичный порядок и H – соответствующий этому частичному порядку р-граф. Тогда, если H – приведенный интервальный орграф, то задача $Cons(\mathcal{P})$ разрешима за полиномиальное время.

Проблема разрешимости систем уравнений над конечными частичными порядками с ограничением

Заданы конечный частичный порядок $\mathcal{P}$ в языке $L = \{\leqslant\}$ без констант и конечная система уравнений $S(X_n)$ над $\mathcal{P}$. Требуется определить, существует ли решение $p = (p_1, \ldots, p_n)$ системы $S(X_n)$ над $\mathcal{P}$ с попарно различными p_i, $i = 1, \ldots, n$.

Теорема 3 (А.Ю.Н., А.Н. Рыбалов)

Проблема разрешимости систем уравнений над конечными частичными порядками с ограничением NP-полна.

Определение

Алгебраическая система $\mathcal{A}$ называется *нётеровой по уравнениям*, если для любого конечного множества переменных X и любой системы уравнений $S \subseteq At_L(X)$ существует такая конечная подсистема $S_0 \subseteq S$, что $V_{\mathcal{A}}(S) = V_{\mathcal{A}}(S_0)$.

Нётеровы по уравнениям алгебраические системы

Диофантов случай.

- Любая конечная алгебраическая система;
- Любая гиперболическая группа без кручения (Z. Sela, А.Г. Мясников);
- Любая жёсткая группа (Н.С. Романовский);
- Любая конечно-порожденная метабелева алгебра Ли (Э.Ю. Даниярова).

Критерии нётеровости по уравнениям. Результат 4.

- Алгебраические и топологические критерии/общий случай (Э.Ю. Даниярова, А.Г. Мясников, В.Н. Ремесленников);
- Критерий для простых графов (А.В. Трейер, И.М. Бучинский);
- Критерий для дистрибутивных $\mathcal{C}$-решеток с произвольным конечным набором предикатных символов (Ю.С. Дворжецкий);
- Критерий для булевых $\mathcal{C}$-алгебр (А.Н. Шевляков).

Критерий нётеровости по уравнениям для частичных порядков

Теорема 4 (А.Ю.Н., И.Д. Кудык)

Частичный порядок $\mathcal{P}$ в языке L_A (диофантов случай) обладает свойством нётеровости по уравнениям тогда и только тогда, когда для любого подмножества B элементов частичного порядка $\mathcal{P}$ можно выбрать конечные подмножества $B', B'' \subseteq B$, что $B^{\uparrow} = B'^{\uparrow}$ и $B^{\downarrow} = B''^{\downarrow}$.

Определение

Теория T алгебры $\mathcal{A}$ языка L называется *разрешимой*, если существует алгоритм, который для любого предложения φ языка L проверяет: принадлежит ли предложение φ теории T.

Известные результаты для элементарной теории

- Неразрешимость элементарной теории графов (И.А. Лавров);
- Разрешимость элементарной теории конечных полей (J. Ax);
- Разрешимость элементарной теории абелевых групп (W. Szmielew);
- Неразрешимость элементарной теории групп (A. Tarski).

- Неразрешимость экзистенциальной теории свободной нильпотентной группы ступени $n \geqslant 9$ счетного ранга (В.А. Романьков);
- Разрешимость $\exists\forall \wedge \vee$-теории для $GL(n, \mathbb{Z})$ для любого $n \geqslant 2$ (Ю.В. Нагребецкая);
- Разрешимость универсальной и экзистенциальной теории графов (А.В. Ильев).

Разрешимость универсальной теории частичных порядков. Результат 5.

Теорема 5

Универсальная теория класса всех частичных порядков в языке $L = \{\leqslant\}$ без констант разрешима.

Для алгебраической системы $\mathcal{A}$ и системы уравнений $S(X_n)$ над этой системой от переменных X_n **координатная алгебра** для этой системы является *общим решением* системы уравнений $S(X_n)$.

Радикалом системы уравнений $S(X_n)$ называется *максимальная система* уравнение $Rad_{\mathcal{L}}(S)$, множество решений которой совпадает с $S(X_n)$.

Способы нахождения координатных алгебр

- Алгоритмы решения системы линейных уравнений над аддитивной группой поля рациональных чисел (координатная группа);
- Построение координатного графа (А.В. Ильев, В.Н. Ремесленников).

Теорема 6

Существует полиномиальный алгоритм построения радикала системы уравнений $S(X_n)$ и её координатного частичного порядка с трудоемкостью $O(n^3)$ в языке $L = \{\leqslant\}$.

Строгое частично упорядоченное множество – это алгебраическая структура $\mathcal{P} = \langle P\ ; < \rangle$ с предикатом строгого порядка в языке, на котором выполнены три аксиомы:

1. $\forall p \in P\ \neg(p < p)$ *(иррефлексивность)*;
2. $\forall p_1, p_2, p_3 \in P\ (p_1 < p_2) \wedge (p_2 < p_3) \rightarrow (p_1 < p_3)$ *(транзитивность)*;
3. $\forall p_1, p_2 \in P\ (p_1 < p_2) \rightarrow \neg(p_2 < p_1)$ *(асимметричность)*.

Пусть система $S(X_n) = S_{x<x}$ в языке строгих линейных порядков $L = \{<\}$ типа дерева. G_S – частичный порядок, соответствующий системе. Операция $[S(X_n)]$ – замыкание системы относительно равенства.
$h(S)$ – высота дерева G_S; $h(x)$ – высота x в G_S; $d(S)$ – множество элементов с глубиной $h(S)$.

Теорема 7 (А.Ю.Н., А.Н. Шевляков)

Пусть дана система уравнений $S(X_n) = S_{x<x}$. Из множества $d(S)$ выбирается любой элемент a. Свойство ($[G_S] = Rad_{\mathcal{L}}(S)$) выполнено тогда и только тогда, когда

$$|\mathcal{L}| \geqslant \begin{cases} h(S) + \max\limits_{x \not< a}\{h(x)\} - 1, & \text{если } \max\limits_{x \not< a}\{h(x)\} > 1, \\ & \text{или } \max\limits_{x \not< a}\{h(x)\} = 1 \text{ и } |d(S)| = 1; \\ h(S) + 1, & \text{иначе.} \end{cases}$$

- Получение теоремы дихотомии о полиномиальной разрешимости и NP-полноте задачи разрешимости систем уравнений над частичными порядками;
- Изучение обобщенных свойств нётеровости по уравнениям (q_ω-, u_ω-компактность) класса частичных порядков;
- Построение радикалов систем уравнений над произвольными строгими порядками.

Спасибо за внимание!