МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УДК 510.52

О СЛОЖНОСТИ ПРОБЛЕМЫ РАЗРЕШИМОСТИ СИСТЕМ УРАВНЕНИЙ НАД КОНЕЧНЫМИ ЧАСТИЧНЫМИ ПОРЯДКАМИ¹

А. Ю. Никитин, А. Н. Рыбалов

Омский государственный технический университет, г. Омск, Россия

Классическая алгебраическая геометрия изучает множества решений алгебраических уравнений над полями вещественных и комплексных чисел. В рамках вычислительной алгебраической геометрии предложены алгоритмы (например, алгоритм Бухбергера) для решения систем полиномиальных уравнений над этими полями. Универсальная алгебраическая геометрия изучает системы уравнений над произвольными алгебраическими системами. Под уравнениями понимаются атомарные формулы языка алгебраической системы. В работе рассматривается проблема распознавания разрешимости систем уравнений над конечными частично упорядоченными множествами. Доказывается, что эта проблема является NP-полной в случае, когда проверяется существование решения, состоящего из попарно различных элементов частично упорядоченного множества.

Ключевые слова: *частично упорядоченное множество, системы уравнений, NP-полнота.*

DOI 10.17223/20710410/39/8

ON COMPLEXITY OF THE SATISFIABILITY PROBLEM OF SYSTEMS OVER FINITE POSETS

A. Y. Nikitin, A. N. Rybalov

*Omsk State Technical University, Omsk, Russia***E-mail:** nikitinlexey@gmail.com, alexander.rybalov@gmail.com

Classical algebraic geometry studies sets of solutions of algebraic equations over the fields of real and complex numbers. In the frameworks of computational algebraic geometry, several algorithms were proposed (for example, the Buchberger algorithm) for solving systems of polynomial equations over these fields. Universal algebraic geometry studies systems of equations over arbitrary algebraic structures. The equations are atomic formulas in the language of an algebraic structure. In this article, we consider the problem of recognizing the solvability of systems of equations over finite partially ordered sets. We prove that this problem is NP-complete in the case when we seek a solution consisting of pairwise distinct elements of a finite partially ordered set.

Keywords: *partially ordered sets, systems of equations, NP-completeness.*

¹Работа поддержана грантом РФФ № 17-11-01117.

Введение

Решение уравнений и систем уравнений над вещественными, комплексными, рациональными, целыми числами является классической темой исследований в различных областях математики в течение уже нескольких тысяч лет. Классическая алгебраическая геометрия изучает множества решений алгебраических уравнений над полями вещественных и комплексных чисел. В рамках диофантовой геометрии и диофантова анализа изучаются решения алгебраических уравнений над целыми и рациональными числами. В XX веке большую роль начали играть вычислительные аспекты этих теорий. Изучение алгоритмических проблем, связанных с определением наличия решения у систем уравнений, а также с нахождением и описанием множества решений, является темой многочисленных теоретических и практических исследований. Как правило, эти алгоритмические проблемы оказываются либо неразрешимыми, либо разрешимыми, но вычислительно трудными. Например, проблема решения полиномиальных уравнений над кольцом целых чисел неразрешима [1]. Известные на сегодняшний день алгоритмы для решения систем полиномиальных уравнений над полями комплексных и вещественных чисел имеют дважды экспоненциальную сложность [2]. Проблема решения систем полиномиальных уравнений над конечными полями, эквивалентная проблеме выполнимости булевых формул, является NP-полной [3].

В последние 20 лет активно развивается так называемая универсальная алгебраическая геометрия (см., например, [4]), в которой изучаются системы уравнений над произвольными алгебраическими системами. Под уравнениями понимаются атомарные формулы языка алгебраической системы. Многие понятия и алгоритмы классической алгебраической геометрии переносятся на произвольные алгебраические системы. При этом возникают новые интересные вопросы. В данной работе в рамках универсальной алгебраической геометрии рассматривается проблема распознавания разрешимости систем уравнений над конечными частично упорядоченными множествами. Доказывается, что эта проблема является NP-полной в случае, когда проверяется существование решения, состоящего из попарно различных элементов частично упорядоченного множества.

1. Предварительные сведения

Напомним, что *частично упорядоченным множеством* (*частичным порядком*) называется алгебраическая система $\mathcal{P} = \langle P \mid \leq^{(2)}, A \rangle$, где $\leq$ — предикатный символ отношения порядка и A — множество константных символов, на которой выполнены следующие аксиомы:

- 1) $\forall p \in P (p \leq p)$;
- 2) $\forall p_1, p_2 \in P ((p_1 \leq p_2 \wedge p_2 \leq p_1) \Rightarrow p_1 = p_2)$;
- 3) $\forall p_1, p_2, p_3 \in P ((p_1 \leq p_2 \wedge p_2 \leq p_3) \Rightarrow p_1 \leq p_3)$.

Уравнение над частичным порядком $\mathcal{P}$ от переменных X — это выражение одного из следующих типов:

- 1) $a_i = a_j$, где $a_i, a_j \in \mathcal{P}$;
- 2) $a_i \leq a_j$, где $a_i, a_j \in \mathcal{P}$;
- 3) $x_i = a_j$, где $x_i \in X, a_j \in \mathcal{P}$;
- 4) $x_i = x_j$, где $x_i, x_j \in X$;
- 5) $a_i \leq x_j$, где $a_i \in \mathcal{P}, x_j \in X$;
- 6) $x_i \leq a_j$, где $x_i \in X, a_j \in \mathcal{P}$;
- 7) $x_i \leq x_j$, где $x_i, x_j \in X$.

Система уравнений $S(X)$ от переменных $X = \{x_1, \dots, x_n\}$ — это любое множество уравнений от переменных X . Точка $p = (p_1, \dots, p_n) \in P^n$ называется *решением* системы уравнений S , если для любого уравнения системы S при подстановке вместо переменных соответствующих значений получается истинное над $\mathcal{P}$ выражение (равенство или неравенство). Две системы уравнений S_1 и S_2 называются *эквивалентными* над $\mathcal{P}$, если их множества решений совпадают. В данной работе будем рассматривать только конечные системы уравнений, то есть системы, состоящие из конечного числа уравнений.

Легко видеть, что любая система уравнений над частичным порядком либо не имеет решения, либо для неё можно построить эквивалентную систему, в которой присутствуют только уравнения типов 5, 6, 7. Действительно, уравнения первых двух типов либо тождественно истинны над данным частичным порядком (тогда от них можно избавиться, упростив систему), либо какое-то из них ложно (тогда система не имеет решения). От уравнений третьего вида можно избавиться, заменяя для каждого такого уравнения $x_i = a_j$ каждое вхождение переменной x_i в системе на константу a_j . После всех таких замен могут возникнуть уравнения первых двух типов — от них нужно избавиться описанным выше способом.

Напомним некоторые сведения из теории графов. Граф G задается парой (V, E) , где V — множество вершин; $E \subseteq V \times V$ — множество рёбер графа G . Для любого конечного множества A через $|A|$ будем обозначать его мощность. Два графа $G = (V_1, E_1)$ и $H = (V_2, E_2)$ называются *изоморфными* (обозначается $G \cong H$), если $|V_1| = |V_2|$, $|E_1| = |E_2|$ и существует взаимно однозначная функция $f : V_1 \rightarrow V_2$, такая, что $(u, v) \in E_1$ тогда и только тогда, когда $(f(u), f(v)) \in E_2$. Проблема изоморфизма подграфу состоит в следующем. Заданы два графа $G = (V, E)$ и $H = (V', E')$. Требуется определить, существует ли подграф $G_0 = (V_0, E_0)$, где $V_0 \subseteq V$ и $E_0 \subseteq E$, такой, что $G_0 \cong H$. Известно [5], что эта проблема является NP-полной. Более того, эта проблема остаётся NP-полной в классе ациклических ориентированных графов [6]. Напомним, что ориентированный граф называется *ациклическим*, если в нём отсутствуют направленные циклы — пути, начинающиеся и заканчивающиеся в одной и той же вершине. Далее нас будет интересовать эта проблема для ещё более узкого класса графов — транзитивно замкнутых. Ориентированный граф называется *транзитивно замкнутым*, если для любых его трёх вершин x, y, z наличие дуг из x в y и из y в z влечёт наличие дуги из x в z .

Лемма 1. Проблема изоморфизма подграфу в классе транзитивно замкнутых графов является NP-полной.

Доказательство. Пусть дан простой граф G . Опишем процедуру трансформации графа G в ориентированный ациклический граф G^t . На первом шаге присвоим каждому ребру (v_1, v_2) графа G уникальную метку $m(v_1, v_2)$. На втором шаге для каждого ребра (v_1, v_2) графа G делаем следующее: ребро (v_1, v_2) удаляем из графа G и вместо него добавляем вершину $m(v_1, v_2)$, затем проводим две дуги (v_1, m) и (v_2, m) . Очевидно, что получившийся граф G^t является ациклическим, так как из всех старых (соответствующих вершинам графа G) вершин дуги выходят, а в новые вершины (соответствующие дугам в графе G) — входят. Кроме того, граф G^t является транзитивно замкнутым. Описанный алгоритм построения графа G^t по графу G является полиномиальным от размера графа G , так как число вершин графа G^t равно сумме числа рёбер и числа вершин графа G .

Пусть есть вход (G, H) проблемы изоморфизма подграфу для простых графов. По описанному алгоритму получим пару транзитивно замкнутых ациклических ориентированных графов (G^t, H^t) . Легко видеть, что в графе G^t найдется подграф, изоморфный H^t , тогда и только тогда, когда в G найдется подграф, изоморфный H . Таким образом, по входу проблемы изоморфизма подграфу для простых графов строится вход для проблемы изоморфизма подграфу в классе ориентированных ациклических графов. Следовательно, и для класса транзитивно замкнутых ациклических ориентированных графов проблема изоморфизма подграфу NP-полна. ■

2. Основной результат

Естественным образом можно перейти от частичного порядка к ациклическому ориентированному графу [7]. Пусть дан частичный порядок $\mathcal{P}$, построим по нему граф $\Gamma_{\mathcal{P}}$. Множеством вершин графа $\Gamma_{\mathcal{P}}$ будет базовое множество частичного порядка $\mathcal{P}$. В графе $\Gamma_{\mathcal{P}}$ присутствует дуга от v_i к v_j , если над $\mathcal{P}$ верно $v_j \leq v_i$. При рассмотрении алгоритмических проблем вместо частичного порядка $\mathcal{P}$ будем подавать на вход алгоритма матрицу смежности графа $\Gamma_{\mathcal{P}}$.

Проблема разрешимости систем уравнений над конечными частичными порядками состоит в следующем. Заданы конечный частичный порядок $\mathcal{P}$ и конечная система уравнений $S(X)$ над $\mathcal{P}$. Требуется определить, существует ли решение $p = (p_1, \dots, p_n)$ системы $S(X)$ над $\mathcal{P}$ с попарно различными $p_i, i = 1, \dots, n$.

Теорема 1. Проблема разрешимости систем уравнений над конечными частичными порядками NP-полна.

Доказательство. Доказательство заключается в сведении проблемы изоморфизма подграфу в классе транзитивно замкнутых ориентированных графов к проблеме разрешимости систем уравнений над конечными частичными порядками.

Пусть заданы два транзитивно замкнутых ориентированных графа G и H и для этих графов нужно определить, существует ли в графе G подграф G_0 , изоморфный графу H . Поскольку граф G транзитивно замкнут и ацикличесок, ему можно сопоставить частичный порядок $\mathcal{P}$ таким образом, что вершины графа G будут элементами базового множества $\mathcal{P}$, а дуги задают отношение порядка $\leq$. Пусть также для каждого элемента $p \in \mathcal{P}$ выполняется $p \leq p$.

По графу H строится система $S(X)$ так, что переменным X соответствуют вершины графа H (положим, что их n штук), а уравнения определяются дугами, т. е. если в графе H есть дуга (x_i, x_j) , то в системе $S(X)$ содержится уравнение $x_j \leq x_i$.

Докажем, что множество изоморфизмов между графом H и всевозможными подграфами G находится во взаимно однозначном соответствии с множеством решений системы уравнений $S(X)$ над $\mathcal{P}$ при условии, что $x_i \neq x_j, i, j \in \{1, \dots, n\}, i \neq j$. Пусть задано вложение графов $\alpha : H \rightarrow G$. Рассмотрим пару вершин $h_1, h_2 \in H$. Тогда $\alpha(h_i) = g_{\alpha_i}, i = 1, 2$. Если в H есть ребро (h_1, h_2) , то в G также есть ребро $(g_{\alpha_1}, g_{\alpha_2})$. При описанном сведении графов к системе уравнений и частичному порядку вершинам h_1 и h_2 соответствуют переменные x_1 и x_2 , вершинам $g_{\alpha_1}, g_{\alpha_2}$ — элементы базового множества частичного порядка p_{α_1} и p_{α_2} . При этом для ребра (h_1, h_2) верно, что в системе $S(X)$ присутствует уравнение $x_2 \leq x_1$, а на частичном порядке $\mathcal{P}$ определено отношение $p_{\alpha_2} \leq p_{\alpha_1}$. Следовательно, для вложения α существует такое решение системы уравнений, что $x_i = p_{\alpha_i}, i = 1, 2$.

Обратно, пусть дано решение системы уравнений $S(X)$ над $\mathcal{P}$. Рассмотрим уравнение $x_1 \leq x_2$ из $S(X)$. Пусть в этом решении $x_i = p_{\alpha_i}, i = 1, 2$. Уравнению $x_1 \leq x_2$ соответствует ребро (h_2, h_1) в графе H для x_1, x_2 и соответствующих вершин h_1, h_2 .

Отношению порядка на элементах базового множества $p_{\alpha_1} \leq p_{\alpha_2}$ соответствует ребро $(g_{\alpha_2}, g_{\alpha_1})$ в графе G .

Итак, проблема изоморфизма графа H подграфу G для класса транзитивно замкнутых ориентированных графов сведена к проблеме разрешимости системы уравнений $S(X)$ над частичным порядком $\mathcal{P}$. Сведение является полиномиальным по размеру матриц смежности графов G и H . Действительно, представление частичного порядка $\Gamma_{\mathcal{P}}$ совпадает с матрицей смежности графа G . Процедура построения системы $S(X)$ по графу H выполняется за линейное время, так как число уравнений в $S(X)$ равно числу рёбер графа H .

Таким образом, проблема разрешимости систем уравнений над конечными частичными порядками является NP-полной. ■

Авторы выражают 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. *Mayr E. W. and Meyer A. R.* The complexity of the word problems for commutative semigroups and polynomial ideals // Adv. Math. 1982. V. 46 (3). P. 305–329.
3. *Cook S. A.* The complexity of theorem proving procedures // Proc. 3d Ann. ACM Symp. Theory of Computing. N.Y., USA, 1971. P. 151–158.
4. *Даниyarова Э. Ю., Мясников А. Г., Ремесленников В. Н.* Алгебраическая геометрия над алгебраическими системами. Новосибирск: СО РАН, 2016. 288 с.
5. *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982. 419 с.
6. *Werth T., Wörlein M., Dreweke A., et al.* DAG mining for code compaction / eds. L. Cao, P. S. Yu, C. Zhang, and H. Zhang. Data Mining for Business Applications. Boston, MA: Springer, 2009. P. 209–223.
7. *Ore O.* Теория графов. М.: Наука, 1980. 336 с.

REFERENCES

1. *Matiyasevich Yu. V.* Diophantovost' perechislimykh mnozhestv [Diophantineity of enumerable sets]. Doklady Akademii Nauk USSR, 1970, vol. 191, no. 2, pp. 279–282. (in Russian)
2. *Mayr E. W. and Meyer A. R.* The complexity of the word problems for commutative semigroups and polynomial ideals. Adv. Math., 1982, vol. 46 (3), pp. 305–329.
3. *Cook S. A.* The complexity of theorem proving procedures. Proc. 3d Ann. ACM Symp. Theory of Computing, N.Y., USA, 1971, pp. 151–158.
4. *Daniyarova E. Yu., Myasnikov A. G., and Remeslennikov V. N.* Algebraicheskaya geometriya nad algebraicheskimi sistemami [Algebraic Geometry over Algebraic Structures]. Novosibirsk, SB RAS, 2016. 288 p (in Russian).
5. *Garey M. and Johnson D.* Computers and Intractability. N. Y., Freeman & Co, 1979. 340 p.
6. *Werth T., Wörlein M., Dreweke A., et al.* DAG mining for code compaction. In: Cao L., Yu P. S., Zhang C., and Zhang H. (eds). Data Mining for Business Applications. Boston, MA, Springer, 2009, pp. 209–223.
7. *Ore O.* Theory of Graphs. Amer. Math. Soc., 1962. 270 p.