ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 510.665

РАЗРЕШИМОСТЬ ОГРАНИЧЕННЫХ ТЕОРИЙ КЛАССА ЧАСТИЧНЫХ ПОРЯДКОВ[1]

А. Ю. Никитин

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

Классическая алгебраическая геометрия изучает множества решений алгебраических уравнений над полями вещественных и комплексных чисел. В последние 20 лет активно развивается так называемая универсальная алгебраическая геометрия, в которой изучаются системы уравнений над произвольными алгебраическими системами. При этом особое значение имеют универсальные и экзистенциальные теории — от их сложности зависят перспективы построения «хорошей» алгебраической геометрии над той или иной алгебраической системой. В работе доказывается, что экзистенциальная и универсальная теории класса всех частичных порядков являются разрешимыми.

Ключевые слова: *частично упорядоченное множество, частичные порядки, разрешимость универсальной теории, разрешимость экзистенциальной теории, классы.*

DOI 10.17223/20710410/45/1

DECIDABILITY OF THE RESTRICTED THEORIES OF A CLASS OF PARTIAL ORDERS

A. Yu. Nikitin

Sobolev Institute of Mathematics, Omsk, Russia

E-mail: nikitinlexey@gmail.com

Classical algebraic geometry studies the solution sets of algebraic equations over the fields of real and complex numbers. In the past 20 years, the so-called universal algebraic geometry, which studies systems of equations over arbitrary algebraic structures, has been actively developed. In this frameworks, universal and existential theories are very important, the prospect for constructing good algebraic geometry over algebraic systems depends on their complexity. In this paper, we prove that the existential and universal theories of the class of all finite orders are decidable.

Keywords: *partially ordered set, poset, decidability of univarsal theory, decidability of existential theory, classes.*

[1]Работа поддержана грантом РНФ № 18-71-10028.

Введение

Решение уравнений и систем уравнений над вещественными, комплексными, рациональными, целыми числами является классической темой исследований в различных областях математики в течение многих сотен 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 последние 20 лет активно развивается так называемая универсальная алгебраическая геометрия [1], 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 особую роль играют универсальные и экзистенциальные теории — от их сложности зависят перспективы построения «хорошей» алгебраической геометрии над той или иной алгебраической системой. Как правило, эти теории оказываются либо неразрешимыми, либо разрешимыми, но вычислительно трудными. Например, экзистенциальная теория кольца целых чисел неразрешима [2]. Вопрос о разрешимости экзистенциальной теории поля рациональных чисел до сих пор открыт. Известные на сегодняшний день алгоритмы для экзистенциальной теории полей комплексных и вещественных чисел имеют дважды экспоненциальную сложность [3]. Экзистенциальная теория любого конечного поля, эквивалентная проблеме выполнимости булевых формул, является NP-полной [4].

В XX веке, в связи с бурным развитием компьютерной техники и прикладной математики, на первый план вышли исследования различных конечных комбинаторных и алгебраических объектов. Прежде всего, это конечные графы, конечные поля, конечные порядки (частично упорядоченные множества). Классическими подходами к изучению конечных алгебраических систем являются алгебраический и комбинаторный. Новый подход к изучению этих объектов — логический и теоретико-модельный — родился в рамках универсальной алгебраической геометрии [1]. Многие практически важные задачи о конечных графах, конечных полях и конечных порядках можно формулировать как задачи, связанные с решением систем уравнений над этими системами, что приводит к необходимости развития алгебраической геометрии. Алгебраическая геометрия над этими объектами тесным образом связана со свойствами экзистенциальных и универсальных теорий. С практической точки зрения важнейшими являются вопросы разрешимости и вычислительной сложности этих теорий, хотя некоторые задачи алгебраической геометрии над данными объектами могут быть алгоритмически сложны [5]. Что касается классических алгебраических структур, то ещё в 1949 г. А. Тарский [6] установил, что элементарная теория класса конечных порядков неразрешима. Дж. Акс в 60-х годах прошлого века получил серьёзный результат о разрешимости элементарной теории класса всех конечных полей [7]. Из этого следует разрешимость экзистенциальной и универсальной теорий класса конечных полей. И. А. Лавров [8] доказал, что элементарная теория класса конечных графов неразрешима. Но экзистенциальная и универсальная теории класса конечных графов уже разрешимы, что показано А. В. Ильевым [9].

В данной работе доказывается, что экзистенциальная и универсальная теории класса всех частичных порядков являются разрешимыми и, как следствие, теории конечных частичных порядков тоже.

1. Предварительные сведения

Напомним базовые определения из теории частичных порядков [10], теории графов [11] и теории моделей [12].

Частично упорядоченным множеством (*частичным порядком*) называется алгебраическая система $\mathcal{P} = \langle P| \leqslant^{(2)}\rangle$, где $\leqslant$ — предикатный символ отношения порядка, на которой выполнены следующие три 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).

Данный частичный порядок определён в языке без констант. Будем обозначать такой язык через L, а множество переменных — через X.

Элементы x и y частичного порядка $\mathcal{P}$ называются *сравнимыми*, если либо $x \leqslant y$, либо $y \leqslant x$ верно в $\mathcal{P}$. Если оба неравенства не верны, то элементы *несравнимы*.

Атомарной формулой языка L от переменных X называется выражение одного из следующих типов:

1) $x_i = x_j$, где $x_i, x_j \in X$;
2) $x_i \leqslant x_j$, где $x_i, x_j \in X$.

Формулой языка L называется выражение, определённое рекурсивно следующим образом:

1) Атомарная формула — это формула.
2) Если φ — формула, то $\neg\varphi$ — тоже формула.
3) Если φ, ψ — формулы, то $\varphi \vee \psi$ и $\varphi \wedge \psi$ — тоже формулы.
4) Если φ — формула, то $\exists x_i\ \varphi$ и $\forall x_i\ \varphi$ — тоже формулы.

Определим следующие типы формул языка L. *Предложением* языка L называется формула без свободных переменных (т. е. все переменные находятся под действием кванторов). Предложение имеет общий вид $Q_1x_1 \ldots Q_nx_n\Psi(x_1, \ldots, x_n)$, где Q_i для $i \in \{1, \ldots, n\}$ — это квантор существования или всеобщности, а Ψ — формула языка L со свободными переменными $x_1, \ldots, x_n$. *Универсальным*, или $\forall$-предложением, называется предложение, где все переменные находятся под действием кванторов всеобщности. Аналогично, *экзистенциальным*, или $\exists$-предложением, называется предложение, в котором все переменные находятся под действием кванторов существования.

Для краткости формулу $\neg(x = y)$ будем обозначать $x \neq y$. Определим формулу строгого порядка следующим образом: $x < y \Leftrightarrow x \leqslant y \wedge x \neq y$. Формула, показывающая, что элементы x и y несравнимы, определяется как $x \not\sim y \Leftrightarrow x \neq y \wedge \neg(x < y) \wedge \wedge \neg(y < x)$. Отрицание неравенства определяется следующим образом: $\neg(x \leqslant y) \Leftrightarrow \Leftrightarrow (y < x) \vee (x \not\sim y)$. При отрицании неравенства между переменными они могут оказаться либо сравнимыми обратным строгим неравенством (первый конъюнкт), либо несравнимыми (второй конъюнкт).

Теорией частичного порядка $\mathcal{P}$ языка L называется всё множество предложений языка L, верное над $\mathcal{P}$. *Универсальной* теорией (или $\forall$-теорией) частичного порядка $\mathcal{P}$ языка L называется подмножество $\forall$-предложений теории частичного порядка $\mathcal{P}$. По аналогии, *экзистенциальной* теорией ($\exists$-теорией) называется подмножество $\exists$-предложений теории частичного порядка $\mathcal{P}$. Строго говоря, здесь дано определение *полной* теории частичного порядка. В данной работе рассматриваются именно такие теории.

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

Определим теории класса частичных порядков. Под классом частичных порядков $\mathbf{P}$ языка L будем понимать семейство частичных порядков языка L, которое вместе с любым частичным порядком содержит все изоморфные ему частичные порядки языка L. *Элементарной* теорий или просто теорией класса $\mathbf{P}$ называется множество $Th(\mathbf{P})$ всех предложений языка L, выполненных на всех частичных порядках из $\mathbf{P}$. Универсальной теорией класса $\mathbf{P}$ называется подмножество $Th_{\forall}(\mathbf{P}) \subseteq Th(\mathbf{P})$ универсальных предложений теории класса $\mathbf{P}$. Аналогично, экзистенциальной теорией класса $\mathbf{P}$ называется подмножество $Th_{\exists}(\mathbf{P}) \subseteq Th(\mathbf{P})$ экзистенциальных предложений теории класса $\mathbf{P}$.

Частичные порядки тесно связаны с графами, а именно: каждому конечному частичному порядку можно сопоставить взаимно однозначно соответствующий конечный граф. Эта связь хорошо известна [11], но для понимания опишем алгоритм перехода от конечного частичного порядка $\mathcal{P} = \langle P | \leqslant \rangle$ к конечному графу $\Gamma = \langle V | E \rangle$. Вершинам графа Γ соответствуют элементы носителя $\mathcal{P}$. В графе Γ есть дуга (p_1, p_2), если в $\mathcal{P}$ верно $p_1 \geqslant p_2$. Полученный граф Γ является транзитивно замкнутым с петлями в каждой вершине. Если убрать все петли из Γ, то получится ациклический ориентированный граф. Назовём такие графы, соответствующие частичным порядкам, *p-графами.*

2. Разрешимость теории

Теорема 1. Универсальная теория класса всех частичных порядков в языке L без констант разрешима.

Доказательство. В качестве доказательства построим алгоритм проверки вхождения произвольного универсального предложения φ в $\forall$-теорию класса частичных порядков $\mathbf{P}$. Заметим, что для того, чтобы предложение φ принадлежало универсальной теории класса, необходимо, чтобы её отрицание $\neg\varphi$ было ложно на всех частичных порядках из $\mathbf{P}$. Если же существует частичный порядок из $\mathbf{P}$, на котором $\neg\varphi$ верно, то само предложение φ не принадлежит универсальной теории класса $\mathbf{P}$.

Краткое описание алгоритма таково. Пусть $Th_{\forall}(\mathbf{P})$ — универсальная теория класса всех частичных порядков. На вход алгоритма подаётся произвольное универсальное предложение φ. От этого предложения берётся его отрицание $\neg\varphi$ и приводится к предварённой дизъюнктивной форме. Далее алгоритм строит графы по конъюнктам из $\neg\varphi$ и определяет наличие циклов в этих графах. Если хотя бы один граф является ациклическим, то предложение φ не принадлежит $Th_{\forall}(\mathbf{P})$. Если не удалось построить ни одного графа либо все построенные графы содержат цикл, то $\varphi \in Th_{\forall}(\mathbf{P})$ (алгоритм 1).

Алгоритм 1.

1: От универсального предложения φ берём его отрицание. Полученное предложение $\neg\varphi = \exists p_1 \ldots \exists p_n \, \psi$ является экзистенциальным, ψ — его бескванторная часть. Далее $\neg\varphi$ преобразуется в эквивалентное предложение $\neg\varphi_1 = \exists p_1 \ldots \exists p_n (\psi_1 \vee \ldots \vee \vee \psi_m)$, находящееся в предварённой дизъюнктивной форме, где ψ_i, $i \in \{1, \ldots, m\}$, — конъюнкты, имеющие вид $\psi_i = \bigwedge\limits_j \xi_j$, ξ_j — либо атомарные формулы, либо их отрицания.

2: Алгоритм последовательно просматривает все конъюнкты ψ_i в предложении $\neg\varphi_1$. Если нашёлся конъюнкт $\psi_i = \xi_i \wedge \neg(x \leqslant y)$, где ξ_i — предложение, то ψ_i заменяется на дизъюнкцию $(\xi_i \wedge y < x) \vee (\xi_i \wedge x \not\sim y)$. В конце процедуры получится новое предложение $\neg\varphi_2$.

3: Алгоритм последовательно просматривает все конъюнкты ψ_i' в предложении $\neg\varphi_2$. Если нашёлся конъюнкт $\psi_i' = \xi_i \wedge x \leqslant y$, где ξ_i — предложение, то ψ_i' заменяется на дизъюнкцию $(\xi_i \wedge x < y) \vee (\xi_i \wedge x = y)$. В конце процедуры получится новое предложение $\neg\varphi_3$.

4: Алгоритм последовательно просматривает все конъюнкты ψ_i'' в предложении $\neg\varphi_3$. Если в каком-то конъюнкте ψ_i'' нет равенства или отрицания равенства между переменными x и y, то ψ_i'' заменяется на дизъюнкцию $(\psi_i'' \wedge x = y) \vee (\psi_i'' \wedge x \neq y)$. В конце процедуры получится новое предложение $\neg\varphi_4$.

5: В каждом конъюнкте ψ_i''' предложения $\neg\varphi_4$, содержащем равенства переменных $x = y$, это равенство удаляется из конъюнкта и вхождение переменной y в ψ_i''' заменяется на переменную x. В конце процедуры получится новое предложение $\neg\varphi_5$.

6: Предложение $\neg\varphi$ истинно над частичным порядком $\mathcal{P}$ из $\mathbf{P}$, если над $\mathcal{P}$ выполнен хотя бы один конъюнкт из предложения $\neg\varphi_5$. Алгоритм последовательно просматривает все конъюнкты $\widehat{\psi}_i$ из $\neg\varphi_5$ и удаляются те из них, которые ложны на всех частичных порядках. Это конъюнкты следующего вида:

1) конъюнкт содержит уравнение типа $x \neq x$;
2) конъюнкт содержит и $x \not\sim y$, и цепь между этими элементами;
3) конъюнкт содержит циклическую цепь типа $x_1 < x_2 < \ldots < x_n < x_1$.

Если в конце процедуры удалены все конъюнкты, то предложение φ истинно для всех частичных порядков и, следовательно, принадлежит универсальной теории $Th_\forall(\mathbf{P})$. Иначе не принадлежит.

Для окончания доказательства остаётся обосновать алгоритм.

Первый шаг алгоритма приводит к предварённой дизъюнктивной форме формулу $\neg\varphi$. Шаги со второго по пятый приводят формулу $\neg\varphi_1$ к такому эквивалентному виду, где в каждом конъюнкте присутствуют только формулы типа $x < y$, $x \neq y$ и $x \not\sim y$. На втором шаге происходит ветвление конъюнкта, содержащего формулу $\neg(x \leqslant y)$. Так как отрицание отношения порядка двух элементов — это либо $y < x$, либо $x \not\sim y$, то этим объясняется ветвление на данном шаге. Аналогично происходит деление на третьем шаге, где $x \leqslant y \Leftrightarrow x < y \vee x = y$. Далее, если в конъюнкте для переменных x и y нет уравнений $x = y$ и $x \neq y$, то опять производится ветвление конъюнкта на пару: конъюнкт с равенством переменных x и y и конъюнкт с отрицанием равенства. Наконец, на пятом шаге происходит замена всех групп равных переменных на представителей. При этом могут получиться противоречивые конъюнкты. Например, конъюнкт $\psi = (x \neq z) \wedge (y = z) \wedge (y = x)$, состоящий из трёх формул, после пятого шага преобразуется в $y \neq y$.

Далее по каждому конъюнкту ψ_i в формуле $\neg\varphi_5$ можно построить граф Γ_i таким образом, что переменные в конъюнкте — это вершины графа Γ_i, а уравнение $x < y$ задаёт дугу (v_y, v_x) в графе Γ. Естественно, в конъюнкте не должно содержаться отрицаний равенств вида $x \neq x$, иначе конъюнкт несовместен и построение графа по нему невозможно. Конъюнкт также несовместен, если в нём содержится $x \not\sim y$ и одновременно с этим есть цепь между x и y. Это означает, что элементы в конъюнкте одновременно сравнимы и несравнимы. Теперь, если граф Γ_i не содержит циклов, то обязательно найдётся частичный порядок $\mathcal{P} \in \mathbf{P}$, p-граф которого содержит граф Γ_i. p-Граф является ациклическим (исключая петли) и транзитивно замкнутым, поэтому в такой граф может вкладываться граф Γ_i. Поэтому, если в конъюнкте содержится цикл $x_1 < x_2 < \dots < x_n < x_1$, то для такого графа Γ_i не существует соответствующего p-графа и, следовательно, конъюнкт не верен для любых значений переменных. Иначе конъюнкт верен.

Если хотя бы один конъюнкт формулы $\neg\varphi_5$ верен, то вся формула $\neg\varphi$ верна и, следовательно, формула φ не принадлежит универсальной теории $Th_\forall(\mathbf{P})$. ■

Поскольку универсальная теория класса всех частичных порядков в языке L разрешима, то и универсальная теория всех *конечных* частичных порядков в языке L также является разрешимой. Сформулируем следствие.

Теорема 2. Экзистенциальная теория класса всех частичных порядков в языке L без констант разрешима.

Доказательство. Класс $\mathbf{P}$ содержит частичный порядок, состоящий ровно из одного элемента. Обозначим такой частичный порядок через ε. Это значит, что для того чтобы предложение φ принадлежало экзистенциальной теории частичных порядков, предложение φ должно быть выполнено над ε. Предваренная дизъюнктивная форма предложения φ — это $\varphi_1 = \exists x_1 \dots \exists x_n \bigvee\limits_j \xi_j$, где ξ_j — конъюнкт. Если φ выполнено над ε, то в φ_1 существует такой конъюнкт ξ_i, что предложение $\omega = \exists x_1 \dots \exists x_n \xi_i$ выполнено над ε. Такое предложение ω будет выполнено над любым частичным порядком из $\mathbf{P}$. Поэтому предложение φ принадлежит теории $Th_\exists(\mathbf{P})$, если его предварённая ДФ содержит такой конъюнкт ξ_i.

Поиск такого конъюнкта можно провести с помощью алгоритма 1 по шагам 1–4. Конъюнкт будет состоять их всех возможных равенств между переменными. Если такой конъюнкт нашёлся, то предложение φ принадлежит экзистенциальной теории класса $\mathbf{P}$, иначе не принадлежит. ■

Аналогично выводу из предыдущей теоремы, экзистенциальная теория класса всех конечных частичных порядков в языке L является разрешимой.

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

ЛИТЕРАТУРА

1. *Даниярова Э. Ю., Мясников А. Г., Ремесленников В. Н.* Алгебраическая геометрия над алгебраическими системами. Новосибирск: Изд-во СО РАН, 2016. 288 с.
2. *Матиясевич Ю. В.* Диофантовость перечислимых множеств // Доклады АН СССР. 1970. Т. 191. № 2. С. 279–282.
3. *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.
4. *Cook S. A.* The complexity of theorem proving procedures // Proc. 3d Ann. ACM Symp. Theory of Computing. N.Y., USA, 1971. P. 151–158.
5. *Никитин А. Ю., Рыбалов А. Н.* О сложности проблемы разрешимости систем уравнений над конечными частичными порядками // Прикладная дискретная математика. 2018. № 39. С. 94–98.
6. *Tarski A.* Undecidability of the theory of lattices and projective geometries // J. Symbolic Logic. 1949. V. 15. P. 77–78.
7. *Ax J.* The elementary theory of finite fields // Ann. Math. 1968. V. 88. No. 2. P. 239–271.
8. *Лавров И.А.* Эффективная неотделимость множества тождественно истинных и конечно опровержимых формул некоторых элементарных теорий // Алгебра и логика. 1963. Т. 2. № 1. С. 5–18.

9. *Ильев А.В.* Разрешимость универсальных теорий и аксиоматизируемость наследственных классов графов // Труды Института математики и механики УрО РАН. 2016. Т. 22. № 1. С. 100–111.
10. *Gratzer G.* General Lattice Theory. Birkhauser, 1998. 663 p.
11. *Оре О.* Теория графов. М.: Наука, 1980. 336 с.
12. *Marker D* Model Theory: An Introduction. N.Y..: Springer, 2002. 342 p.

REFERENCES

1. *Daniyarova E. Y., Myasnikov A. G., and Remeslennikov V. N.* Algebraicheskaya geometria nad algebraicheskimi sistemami [Algebraic Geometry over Algebraic Systems]. Novosibirsk, SB RAS Publ., 2016. 288 p (in Russian).
2. *Matiyasevich Yu. V.* Diofantovost' perechislimykh mnozhestv [Diophantineity of enumerable sets]. Doklady Akademii Nauk USSR, 1970, vol. 191, no. 2, pp. 279–282. (in Russian)
3. *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.
4. *Cook S. A.* The complexity of theorem proving procedures. Proc. 3d Ann. ACM Symp. Theory of Computing, N.Y., USA, 1971, pp. 151–158.
5. *Nikitin A. Yu. and Rybalov A. N.* O slozhnosti problemy razreshimosti sistem uravneniy nad konechnymi chastichnymi poryadkami [On complexity of the satisfiability problem of systems over finite posets]. Prikladnaya Diskretnaya Matematika, 2018, no. 39, pp. 94–98. (in Russian)
6. *Tarski A.* Undecidability of the theory of lattices and projective geometries. J. Symbolic Logic, 1949, vol. 15, pp. 77–78.
7. *Ax J.* The elementary theory of finite fields. Ann. Math., 1968, vol. 88, no. 2, pp. 239–271.
8. *Lavrov I. A.* Effectivnaya neotdelimost' mnojestva tojdestvenno istinnih i conechno oproverjimih formul nekotorih elementarnih teoriy [Effective inseparability of the set of identically true and finitely refutable formulas of some elementary theories]. Algebra i Logica, 1963, vol. 2, no. 1, pp. 5–18. (in Russian)
9. *Il'ev A. V.* Razreshimost' universalnih teoriy i aksiomatiziruemost' nasledstvennih classov grafov [Decidability of universal theories and axiomatizability of hereditary classes of graphs]. Trudi Instituta Matematiki i Mehaniki UrO RAN, 2016, vol. 22, no. 1, pp. 100–111. (in Russian)
10. *Gratzer G.* General Lattice Theory. Birkhauser, 1998. 663 p.
11. *Ore O.* Theory of Graphs. American Mathematical Soc, 1962. 270 p.
12. *Marker D* Model Theory: An Introduction. N.Y., Springer, 2002. 342 p.