МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УДК 510.52

О СЛОЖНОСТИ ЭКЗИСТЕНЦИАЛЬНОЙ И УНИВЕРСАЛЬНОЙ ТЕОРИЙ КОНЕЧНЫХ ПОЛЕЙ[1]

А. Н. Рыбалов

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

Конечные поля являются важнейшими математическими объектами, которые используются при решении многих практически важных задач оптимизации, информатики, передачи информации и криптографии. Многие такие задачи можно формулировать как задачи, связанные с решением систем уравнений над полями, 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. В работе изучается вычислительная сложность экзистенциальной и универсальной теорий конечных полей. Доказывается, что экзистенциальная теория класса всех конечных полей является NP-трудной, а универсальная теория этого класса является co-NP-трудной. Это означает, что, при условии неравенства классов сложности P, NP и co-NP, не существует полиномиальных алгоритмов, распознающих эти теории.

Ключевые слова: *конечные поля, универсальная теория, экзистенциальная теория, NP-трудность.*

DOI 10.17223/20710410/45/9

ON COMPLEXITY OF THE EXISTENTIAL AND UNIVERSAL THEORIES OF FINITE FIELDS

A. N. Rybalov

Sobolev Institute of Mathematics, Omsk, Russia

E-mail: alexander.rybalov@gmail.com

Finite fields are the most important mathematical objects that are used for solving many practical problems of optimization, computer science, information transfer and cryptography. Many such problems can be formulated as problems connected with the solving systems of equations over fields. This leads to the need for the development of algebraic geometry. Algebraic geometry over such objects is closely related to properties of existential and universal theories. From a practical point of view, the most important are questions about decidability and computational complexity of these theories. In this paper, we study the computational complexity of existential and

[1]Работа поддержана грантом РНФ № 19-11-00209.

universal theories of finite fields. We prove that the existential theory of finite fields is NP-hard, and the universal theory of finite fields is co-NP-hard. This means that there are no polynomial algorithms that recognize these theories, provided the inequality of classes P, NP and co-NP.

Keywords: *finite fields, universal theory, existential theory, NP-hardness.*

Введение

Большой пласт алгоритмических проблем связан с проблемами разрешения элементарных теорий различных алгебраических систем. Как правило, эти проблемы либо неразрешимы (формальная арифметика, теория поля рациональных чисел, теория графов и т. д.), либо разрешимы, но имеют очень высокую вычислительную сложность (арифметика Пресбургера, теория упорядоченного поля действительных чисел, теория конечных полей и т. д.). Поэтому большой интерес представляет изучение экзистенциальных и универсальных теорий. Экзистенциальные и универсальные теории тесно связаны с решением уравнений и систем уравнений над различными алгебраическими системами. Для классических алгебраических систем, таких, как поля вещественных, комплексных, рациональных чисел, кольца целых и алгебраических чисел изучение их экзистенциальных и универсальных теорий является классической темой исследований в различных областях математики в течение уже 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 XX веке, в связи с бурным развитием компьютерной техники и прикладной математики, на первый план вышли исследования различных конечных комбинаторных и алгебраических объектов. Одними из важнейших таких объектов являются конечные поля, без которых немыслима теория передачи информации и современная криптография. Классическим подходом к изучению конечных полей является использование алгебраических методов. Новый подход к изучению этих объектов — логический и теоретико-модельный — родился в рамках так называемой универсальной алгебраической геометрии [1]. Многие практически важные задачи о конечных полях можно формулировать как задачи, связанные с решением систем уравнений над полями, 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.

В данной работе изучается вычислительная сложность экзистенциальной и универсальной теорий конечных полей. Доказывается, что экзистенциальная теория класса всех конечных полей является NP-трудной, а универсальная теория этого класса является co-NP-трудной. Это означает, что, при условии неравенства классов сложности P, NP и co-NP, не существует полиномиальных алгоритмов, распознающих эти теории.

1. Предварительные сведения

Напомним некоторые определения из математической логики и теории моделей [1]. *Сигнатурой* называется множество σ, состоящее из предикатных, функциональных и константных символов. *Алгебраическая система* сигнатуры σ есть набор $\mathfrak{A} = \langle A, \sigma \rangle$, где A — непустое множество, причём каждому предикатному символу сигнатуры σ со-

поставлен некоторый предикат на множестве A, каждому функциональному символу из σ сопоставлена функция на множестве A со значениями в множестве A, а каждому константному символу из σ — элемент из A. *Классом* алгебраических систем $\mathcal{K}$ сигнатуры σ называется множество алгебраических систем фиксированной сигнатуры σ.

Формула логики первого порядка сигнатуры σ, в которой на каждую переменную навешан квантор, называется *предложением*. Тот факт, что предложение Φ сигнатуры σ истинно в алгебраической системе $\mathfrak{A} = \langle A, \sigma \rangle$, обозначается $\mathfrak{A} \models \Phi$. Предложение Φ сигнатуры σ называется *экзистенциальным* (или $\exists$-предложением), если оно имеет вид

$$\Phi = \exists x_1 \ldots \exists x_n \varphi(x_1, \ldots, x_n),$$

где φ — бесквантор ная формула сигнатуры σ. Предложение Φ сигнатуры σ называется *универсальным* (или $\forall$-предложением), если оно имеет вид

$$\Phi = \forall x_1 \ldots \forall x_n \varphi(x_1, \ldots, x_n),$$

где φ — бесквантор ная формула сигнатуры σ. *Элементарной теорией* класса $\mathcal{K}$ называется множество $Th(\mathcal{K})$ всех предложений сигнатуры σ, истинных во всех алгебраических системах класса $\mathcal{K}$. Множество всех $\exists$-предложений теории $Th(\mathcal{K})$ называется *экзистенциальной* теорией $Th_\exists(\mathcal{K})$ класса $\mathcal{K}$. Множество всех $\forall$-предложений теории $Th(\mathcal{K})$ называется *универсальной* теорией $Th_\forall(\mathcal{K})$ класса $\mathcal{K}$. Теория (элементарная, экзистенциальная, универсальная) класса $\mathcal{K}$ разрешима, если существует алгоритм, который по произвольному предложению сигнатуры σ позволяет определить, принадлежит ли оно этой теории.

Приведём некоторые сведения из теории сложности вычислений [2]. *Время работы* $t_M(x)$ машины Тьюринга M над алфавитом A на входе $x \in A^*$ — это число шагов машины от начала работы до остановки. Если M на x не останавливается, полагаем $t_M(x) = \infty$. В дальнейших определениях для строки x под $|x|$ понимается длина строки x. Машина Тьюринга M *полиномиальна*, если существует полином $p(n)$, такой, что для любого $x \in A^*$ имеет место $t_M(x) < p(|x|)$. Множество $S \subseteq I$ принадлежит *классу* P, если существует полиномиальная машина Тьюринга, вычисляющая характеристическую функцию множества S. Множество $S \subseteq I$ принадлежит *классу* NP, если существует такое множество $S' \in$ P и такой полином $p(n)$, что

$$x \in S \Leftrightarrow \exists y \in \{0,1\}^* \ (|y| < p(|x|) \text{ и } (x, y) \in S').$$

Здесь строка y называется подсказкой (или сертификатом, или решением), а множество S' — проверятелем. Множество $S \subseteq I$ принадлежит *классу* co-NP, если $I \setminus S \in$ NP.

Множество $A \subseteq I$ *полиномиально сводится* к множеству $B \subseteq J$, если существует функция $f : I \to J$, вычислимая на полиномиальной машине Тьюринга, такая, что

$$\forall x \in I \ (x \in A \Leftrightarrow f(x) \in B).$$

Множество A называется *NP-трудным*, если любое множество $B \in$ NP полиномиально сводится к A. Если при этом $A \in$ NP, то A называется *NP-полным*. Соответствующая проблема распознавания NP-трудного множества также называется *NP-трудной*. NP-трудные проблемы являются самыми сложными проблемами в классе NP в том смысле, что если хотя бы одна из них лежит в классе P, то P = NP, а также, если P $\neq$ NP, то любая NP-трудная проблема не лежит в классе P. Множество A называется *co-NP-трудным*, если любое множество $B \in$ co-NP полиномиально сводится к A. Легко видеть, что $S \subseteq I$ co-NP-трудно тогда и только тогда, когда $I \setminus S$ NP-трудно.

2. Конечные поля

Рассмотрим класс $\mathcal{F}$ всех конечных полей $\mathrm{GF}(q)$ сигнатуры $\sigma_{\mathcal{F}} = \{=, +, -, /, 0, 1\}$. В [3] доказано, что элементарная теория класса всех конечных полей разрешима. Поэтому разрешимы экзистенциальная и универсальная теория класса конечных полей. Изучим вычислительную сложность этих теорий.

Булева формула $\varphi(x_1, \ldots, x_n)$ называется *выполнимой*, если существуют значения булевых переменных $x_1, \ldots, x_n$, при которых $\varphi(x_1, \ldots, x_n)$ является истинной. *Проблема выполнимости булевых формул* — это проблема распознавания множества выполнимых булевых формул на множестве всех булевых формул. Булева формула записана в виде 3-КНФ, если она имеет вид

$$\varphi(x_1, \ldots, x_n) = \bigwedge_{k=1}^{m} \left(x_{k1}^* \vee x_{k2}^* \vee x_{k3}^*\right),$$

где x_i^* есть литерал, то есть либо сама логическая переменная x_i, либо её отрицание $\neg x_i$. Известно [2], что проблема выполнимости 3-КНФ является NP-полной.

Определим отображение t из множества всех литералов от переменных $x_1, \ldots, x_n$ в множество многочленов от переменных $x_1, \ldots, x_n$ следующим образом:

$$t(x_i^*) = \begin{cases} x_i, & \text{если } x_i^* = x_i, \\ (1 - x_i), & \text{если } x_i^* = \neg x_i. \end{cases}$$

Построим по 3-КНФ $\varphi(x_1, \ldots, x_n)$ следующее экзистенциальное предложение сигнатуры $\sigma_{\mathcal{F}}$:

$$\Phi_\varphi = \exists x_1 \ldots \exists x_n \bigwedge_{i=1}^{n} \big((x_i = 0) \vee (x_i = 1)\big) \wedge \bigwedge_{k=1}^{m} \big(t(x_{k1}^*)t(x_{k2}^*)t(x_{k3}^*) = 0\big).$$

Лемма 1. Пусть φ — 3-КНФ. Тогда φ выполнима тогда и только тогда, когда $\Phi_\varphi \in Th_\exists(\mathcal{F})$.

Доказательство. Пусть 3-КНФ $\varphi(x_1, \ldots, x_n)$ выполнима и $a_1, \ldots, a_n$ — набор значений логических переменных, на которых φ истинна. Пусть $\mathfrak{A}_F$ — любое конечное поле. Тогда $\mathfrak{A}_F \models \Phi_\varphi$, при этом значения переменных $x_1, \ldots, x_n$, которые делают бескванторную часть предложения Φ_φ истинной, определяются следующим образом:

$$x_i = \begin{cases} 0, \text{ если } a_i = \text{истина}, \\ 1, \text{ если } a_i = \text{ложь}. \end{cases}$$

Таким образом, $\Phi_\varphi \in Th_\exists(\mathcal{F})$.

Обратно, пусть $\Phi_\varphi \in Th_\exists(\mathcal{F})$, то есть $\mathfrak{A}_F \models \Phi_\varphi$ для любого конечного поля $\mathfrak{A}_F$, в частности для двоичного поля $\mathrm{GF}(2)$. Но тогда 3-КНФ $\varphi(x_1, \ldots, x_n)$ выполнима, а значения логических переменных $a_1, \ldots, a_n$, на которых φ истинна, определяются по значениям переменных $x_1, \ldots, x_n$, которые делают бескванторную часть предложения Φ_φ истинной в $\mathrm{GF}(2)$:

$$a_i = \begin{cases} \text{истина}, & \text{если } x_i = 0, \\ \text{ложь}, & \text{если } x_i = 1. \end{cases}$$

Лемма доказана. ■

Теорема 1. Экзистенциальная теория конечных полей является NP-трудной.

Доказательство. Доказательство заключается в сведении проблемы выполнимости 3-КНФ к проблеме разрешимости экзистенциальной теории конечных полей. Определим сводимость f между двумя этими проблемами следующим образом. Если φ — 3-КНФ, то положим $f(\varphi) = \Phi_\varphi$. По лемме 1 φ выполнима тогда и только тогда, когда $\Phi_\varphi \in Th_\exists(\mathcal{F})$. Полиномиальность сводимости следует из того факта, что размер формулы Φ_φ линейно ограничен от размера 3-КНФ φ. Таким образом, проблема разрешимости экзистенциальной теории конечных полей является NP-трудной. ■

Теорема 2. Универсальная теория конечных полей является co-NP-трудной.

Доказательство. Докажем, что дополнение $Th_\exists(\mathcal{F})$ в множестве всех экзистенциальных предложений сигнатуры $\sigma_\mathcal{F}$ полиномиально сводится к $Th_\forall(\mathcal{F})$. Отсюда по теореме 1 будет следовать, что последняя теория co-NP-трудна. Эта сводимость f действует на предложение

$$\Phi = \exists x_1 \ldots \exists x_n \varphi(x_1, \ldots, x_n)$$

следующим образом:

$$f(\Phi) = \neg\Phi = \neg\big(\exists x_1 \ldots \exists x_n \varphi(x_1, \ldots, x_n)\big) = \forall x_1 \ldots \forall x_n \neg\varphi(x_1, \ldots, x_n).$$

Очевидно, что для любого $\exists$-предложения Φ имеет место $\Phi \notin Th_\exists(\mathcal{F}) \Leftrightarrow \neg\Phi \in Th_\forall(\mathcal{F})$. Полиномиальность сводимости f следует из того, что размер $\neg\varphi$ линейно ограничен от размера φ. ■

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

ЛИТЕРАТУРА

1. *Даниярова Э. Ю., Мясников А. Г., Ремесленников В. Н.* Алгебраическая геометрия над алгебраическими системами. Новосибирск: СО РАН, 2016. 288 с.
2. *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982. 419 с.
3. *Ax J.* The elementary theory of finite fields // Ann. Math. 1968. V. 88. No. 2. P. 239–271.

REFERENCES

1. *Daniyarova E. Y., Myasnikov A. G., and Remeslennikov V. N.* Algebraicheskaya geometriya nad algebraicheskimi sistemami [Algebraic Geometry over Algebraic Structures]. Novosibirsk, SB RAS Publ., 2016. 288 p. (in Russian)
2. *Garey M. and Johnson D.* Computers and Intractability. N. Y., Freeman & Co, 1979. 340 p.
3. *Ax J.* The elementary theory of finite fields. Ann. Math., 1968, vol. 88, no. 2, pp. 239–271.