УДК 512.552
AMS MSC2020: 12K05

О некоторых системах уравнений над конечными почти-полями[1]

Селиверстов А. В.

Институт проблем передачи информации им. А.А. Харкевича Российской академии наук

Аннотация. Мы рассматриваем вычислительную сложность задачи распознавания существования решения для некоторых типов систем уравнений над конечными почти-полями. На примерах показана связь между вычислительной сложностью и определимостью множества из нуля, единицы и минус единицы системой уравнений рассматриваемого вида. Обсуждается применимость полученных результатов к решению некоторых систем нелинейных алгебраических уравнений над конечными полями.

Ключевые слова: почти-поле, левая дистрибутивность, система уравнений, вычислительная сложность.

Введение

Интерес к конечным почти-полям объясняется недавно полученными новыми результатами [1, 2], а также различными приложениями. В частности, конечные почти-поля связаны с кодами, исправляющими ошибки. Это делает актуальным создание быстрых алгоритмов для решения систем уравнений над почти-полями.

1. Предварительные сведения

Определение 1 (Почти-поле). *Алгебраическая система с константой нуль и бинарными операциями сложения и умножения называется левым почти-полем (near-field), если относительно сложения*

[1]Работа выполнена в рамках государственного задания ИППИ РАН, утвержденного Минобрнауки России.

© Селиверстов А. В.

это абелева группа, относительно умножения ненулевые элементы образуют группу, а также выполнены: левый дистрибутивный закон $z(x+y) = zx+zy$, *свойства нуля* $0 \cdot x = x \cdot 0 = 0$ *и для элементов* $\alpha \neq \beta$ *и любого* γ *уравнение* $\alpha x = \beta x + \gamma$ *имеет единственное решение.*

Для конечных почти-полей последнее свойство следует из остальных. Также мы используем обычные обозначения для операций вычитания и возведения в степень.

Первую серию некоммутативных конечных почти-полей построил Леонард Юджин Диксон (Leonard Eugene Dickson, 1874–1954) [3, 4]. Наименьший порядок почти-поля Диксона равен девяти. Рассмотрим двумерное линейное пространство над полем $GF(3)$. Его элементами служат линейные комбинации $a + b\lambda$, где a и b пробегают поле $GF(3)$ из элементов $\{0, 1, 2\}$ с обычными операциями по модулю три, а через λ обозначен новый порождающий элемент. Определим умножение, полагая $\lambda^2 = 2$ и в общем случае

$$(a + b\lambda)(c + d\lambda) = ac - (a^2 + b^2)bd + \big(bc + (a^2 + b^2)ad\big)\,\lambda.$$

Так определено левое почти-поле, в котором выполнено $xy = \pm yx$, но, вообще говоря, $(y + z)x \neq yx + zx$.

Аналогично определяются правые почти-поля Диксона [5]. Центр почти-поля состоит из элементов, коммутирующих со всеми элементами. Центром почти-поля Диксона служит поле Галуа. Почти-поле Диксона с центром $GF(q)$ имеет порядок q^m, где пара (q, m) удовлетворяет дополнительным условиям.

Не все результаты из линейной алгебры переносятся на почти-поля. В частности, свойства правых модулей над левыми почти-полями отличаются от свойств линейных пространств над полем [6].

Ганс Цассенхауз (Hans Julius Zassenhaus, 1912–1991) классифицировал конечные почти-поля [7]. Кроме полей Галуа и почти-полей Диксона, известны семь исключительных конечных почти-полей порядка p^2 для простых чисел p из множества $\{5, 7, 11, 23, 29, 59\}$, из них для $p = 11$ существуют два исключительных почти-поля. Вообще говоря, центр почти-поля не замкнут относительно сложения. Исключительное почти-поле Цассенхауза порядка 29^2 обладает центром из 15 элементов. Три исключительных почти-поля Цассенхауза, порядки которых равны 5^2, 7^2 и 11^2 соответственно, обладают центром, состоящим из нуля, единицы и противоположного элемента [1, 2].

2. Результаты

Предложение 1. *Над левым почти-полем Диксона с центром $GF(q)$ за полиномиальное время разрешима задача о существовании решения у системы уравнений вида $a_{k0} + \sum\limits_{j=1}^{n} (a_{kj}z_j + b_{kj}z_j) = 0$ от переменных $z_1, \ldots, z_n$ с любыми коэффициентами a_{kj} и b_{kj}. Более того, за полиномиальное время* $\mathrm{poly}(n)$ *вычисляется количество решений такой системы уравнений.*

Набросок доказательства. Поскольку почти-поле Диксона служит линейным пространством над полем $GF(q)$, задача сводится к решению системы линейных уравнений над этим полем. □

Предложение 2. *Над конечным левым почти-полем за полиномиальное время разрешима задача о существовании решения у системы уравнений видов $a_{k0} + a_{ki}z_i + b_{ki}z_i + a_{kj}z_j + b_{kj}z_j = 0$, $a_{k0} + a_{ki}z_i + b_{ki}z_i + z_ja_{kj} = 0$, $a_{k0} + z_ia_{ki} + z_ja_{kj} = 0$, каждое из которых зависит от самое большее двух переменных z_i и z_j среди переменных $z_1, \ldots, z_n$, с любыми коэффициентами a_{kj} и b_{kj}. Более того, за полиномиальное время* $\mathrm{poly}(n)$ *вычисляется количество решений такой системы уравнений.*

Набросок доказательства. Поиск решения основан на том, что в каждом отдельно рассматриваемом уравнении этой системы выбор значения одной из входящих в него переменных либо однозначно определяет значение другой переменной, либо приводит к тождеству, либо приводит к ложной формуле. □

Замечание 1. *Предложение 2 справедливо над любым конечным квазиполем, поскольку ассоциативность умножения не используется.*

Предложение 3. *Над левым почти-полем Диксона порядка* 9 *за полиномиальное время разрешима задача о существовании решения у системы двух уравнений вида*

$$\begin{cases} z_1a_1 + \cdots + z_na_n &= 0 \\ z_1b_1 + \cdots + z_nb_n &= b_0 \end{cases}$$

от переменных $z_1, \ldots, z_n$.

Набросок доказательства. Проверка основана на исключении некоторой переменной, от которой зависит уравнение без свободного члена. Трудность в том, что может возникнуть уравнение нового типа, содержащее терм большой глубины. □

© Селиверстов А. В.

Тверской государственный университет

Предложение 4. *Над левым исключительным почти-полем Цассенхауза, центр которого состоит из элементов* $\{0, 1, -1\}$, NP*-полна задача о существовании решения у системы уравнений двух видов: либо* $a_{k0} + \sum_{j=1}^{n} a_{kj} z_j = 0$ *от переменных* $z_1, \ldots, z_n$, *либо* $b_{kj} z_j = z_j b_{kj}$ *от переменной* z_j.

Набросок доказательства. Система уравнений $bz_j = z_j b$ для всех элементов b определяет принадлежность допустимого значения переменной z_j к центру почти-поля. По условию, $z_j \in \{0, 1, -1\}$. Но задача распознавания $\{0, 1, -1\}$-решения системы линейных уравнений над полем характеристики пять или выше NP-трудная. Принадлежность задачи классу NP очевидна. □

Заключение

Над левым почти-полем, отличным от поля, но содержащим максимальное по включению подполе F, терм вида za соответствует нелинейному многочлену над полем Галуа F от двух переменных. Следовательно, предложения 2 и 3 позволяют быстро решать некоторые системы нелинейных алгебраических уравнений над полями Галуа. Однако такие системы должны удовлетворять многим ограничениям. Предложение 4 подтверждает, что такие ограничения неизбежны в предположении различия классов P и NP.

Работа выполнена в рамках государственного задания ИППИ РАН, утвержденного Минобрнауки России.

Список литературы

[1] *Кравцова, О. В.* Вопросы строения конечных почти-полей / О. В. Кравцова, В. М. Левчук // Труды ИММ УрО РАН. — 2019. — Т. 25, № 4. — С. 107–117.

[2] *Яковлева, Т. Н.* Вопросы строения квазиполей с ассоциативными степенями // Известия Иркутского государственного университета. Серия Математика. — 2019. — Т. 29. — С. 107–119.

[3] *Dickson, L. E.* On finite algebras // Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Ph. — 1905. — P. 358–394.

[4] *Dickson, L. E.* Linear algebras in which division is always uniquely possible // Transactions of the American Mathematical Society. — 1906. — V. 7, no. 3. — P. 370–390.

[5] *Djagba, P.* Construction of a finite Dickson nearfield // International Journal of Nonlinear Analysis and Applications. — 2023. — V. 14, no. 10. — P. 155–161.

[6] *Djagba, P.* On linear mappings and seed sets of Beidleman near-vector spaces / P. Djagba, A. L. Prins // Palestine Journal of Mathematics. — 2025. — V. 14, no. 1. — P. 195–212.

[7] *Zassenhaus, H. J.* Über endliche Fastkörper // Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg. — 1935. — V. 11. — P. 187–220.

Библиографическая ссылка

Селиверстов, А. В. О некоторых системах уравнений над конечными почти-полями // Всероссийская конференция «Математические основы информатики и информационно-коммуникационных технологий». Сборник трудов. — Тверь : ТвГУ, 2026. — С. 1–5.

Сведения об авторах

Александр Владиславович Селиверстов
Институт проблем передачи информации им. А.А. Харкевича Российской академии наук. Ведущий научный сотрудник

Россия, 127051, Москва, Большой Каретный переулок, д. 19, с. 1
E-mail: SLVSTV@iitp.ru

© Селиверстов А. В.