Библиотека Чебышевского сборника

Тульский государственный педагогический университет им. Л. Н. Толстого
Московский государственный университет имени М. В. Ломоносова
Санкт-Петербургский государственный университет
Московский педагогический государственный университет
Тульский государственный университет
Математический институт им. В. А. Стеклова РАН
МЦНМУ МЦФПМ
Петербургское отделение Математического института им. В. А. Стеклова РАН
Институт истории естествознания и техники им. С. И. Вавилова РАН

Алгебра, теория чисел, дискретная геометрия и многомасштабное моделирование: современные проблемы, приложения и проблемы истории

Материалы XXV Международной конференции, посвящённой 135-летию со дня рождения академика И. М. Виноградова, член-корреспондента Р. О. Кузьмина, 120-летию со дня рождения член-корреспондента А. О. Гельфонда, член-корреспондента Д. К. Фадеева, 80-летию со дня рождения профессора С. М. Воронина и 75-летию со дня рождения профессора Д. А. Митькина

Тула, 6–10 октября 2026 года

ББК 22.1
УДК 51
А45

Председатель программного комитета — профессор В. Н. Чубариков

Сопредседатели программного комитета:
член-корреспондент В. М. Бухштабер;
академик С. В. Конягин;
академик Ю. В. Матиясевич;
академик В. П. Платонов

Ответственный секретарь — Н. М. Добровольский

Программный комитет:
И. Н. Балаба (Тула), В. А. Быковский (Хабаровск), М. А. Всемирнов (Санкт-Петербург), С. Б. Гашков (Москва), С. А. Гриценко (Москва), Е. И. Деза (Москва), С. С. Демидов (Москва), Н. П. Долбилин (Москва), А. О. Иванов (Москва), М. А. Королёв, В. Н. Кузнецов (Саратов), А. Лауринчикас (Вильнюс, Литва), С. П. Мищенко (Ульяновск), Б. З. Мороз (Москва), Ю. В. Нестеренко (Москва), А. И. Нижников (Москва), А. Ю. Ольшанский (Нашвилл, США), У. М. Пачев (Нальчик), З. Х. Рахмонов (Душанбе, Таджикистан), А. Л. Семёнов (Москва), А. В. Устинов (Хабаровск), А. А. Фомин (Москва), В. Г. Чирский (Москва), A. Mucherino (France), P. Sole (France), M. Dutour (France), A. Jurišić (Slovenia), Y. Wu (China), M. Bounyaev (USA), O. Musin (USA), S. Shpectorov (UK), L. Fukshansky (California, USA), N. Singhi (India), M. Firer (Brasil), Y. Kempner (Israel)

Редакционная коллегия:
доктор физико-математических наук, профессор *В. Н. Чубариков;*
доктор физико-математических наук, профессор *Н. М. Добровольский;*
кандидат физико-математических наук, доцент *И. Ю. Реброва;*
доктор физико-математических наук *Н. Н. Добровольский;*
старший преподаватель *А. В. Родионов*

Алгебра, теория чисел, дискретная геометрия и многомасштабное моделирование: современные проблемы, приложения и проблемы истории: Материалы XXV Международной конференции (Тула, 6–10 октября 2026 года), посвящённой 135-летию со дня рождения академика И. М. Виноградова, член-корреспондента Р. О. Кузьмина, 120-летию со дня рождения член-корреспондента А. О. Гельфонда, член-корреспондента Д. К. Фадеева, 80-летию со дня рождения профессора С. М. Воронина и 75-летию со дня рождения профессора Д. А. Митькина. —

Тула: Тул. гос. пед. ун-т им. Л. Н. Толстого, 2026. – 285 с.
ISBN 5–87954–388–9

ББК 22.1
УДК 51

Список цитированной литературы

1. Байрамгулов А. В, Погорелов Б.А. О подгруппах аффинной группы кольца Галуа четной характеристики // Дискретная математика. 2024. Том 36, №4. С. 13-27.
2. Глухов М. М. О 2-транзитивных произведениях регулярных групп подстановок // Труды по дискретной математике. 2000. Том 3. С. 37-52.
3. Глухов М. М. О матрицах переходов разностей при использовании некоторых модулярных групп // Математические вопросы криптографии. 2013. Том 4, №4. С. 27-47.
4. Погорелов Б. А., Пудовкина М. А. Свойства регулярных представлений неабелевых 2-групп с циклической подгруппой индекса 2 // Математические вопросы криптографии. 2021. Том 12, №4. С. 65-85.
5. Погорелов Б. А., Пудовкина М. А. Простейшие надгруппы регулярных представлений неабелевых 2-групп с циклической подгруппой индекса 2 // Математические вопросы криптографии. 2022. Том 13, №3. С. 107-130.
6. Biham E, Shamir A. Differential cryptanalysis of the Data Encryption Standard — Springer, 1993. 105 p.
7. Keedwell A. On R-Sequenceability and Rh-Sequenceability of Groups // Combinatorics '81 in honour of Beniamino Segre, Proceedings of the International Conference on Combinatorial Geometrics and their Applications. 1983. v.78. P. 535–548.
8. Ollis M., Willmott D. On twizzler, zigzag and graceful terraces // Australasian J. of Combinatorics. 2011. v.51. P. 243–257.

УДК 512.624.3

Применение почти-полей для решения систем алгебраических уравнений над конечным полем[1]

А. В. Селиверстов (Россия, г. Москва)
Институт проблем передачи информации им. А.А. Харкевича Российской академии наук
e-mail: slvstv@iitp.ru

Some application of near-fields to solving systems of algebraic equations over a finite field[1]

A. V. Seliverstov (Russia, Moscow)
Institute for Information Transmission Problems of the Russian Academy of Sciences (Kharkevich Institute)
e-mail: slvstv@iitp.ru

1. Введение

[1]Работа выполнена в рамках государственного задания ИППИ РАН, утвержденного Минобрнауки России.
[1]The research was carried out within the state assignment of Ministry of Science and Higher Education of the Russian Federation for IITP RAS.

Определение 1. *Алгебраическая система с константой нуль и бинарными операциями сложения и умножения называется левым почти-полем, если относительно сложения 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.*

Первые примеры конечных почти-полей нашёл Леонард Юджин Диксон (Leonard Eugene Dickson, 1874–1954) [1, 2]. Позже Ганс Цассенхауз (Hans Julius Zassenhaus, 1912–1991) классифицировал конечные почти-поля (near-field), называя их по-немецки *Fastkörper* [3, 4]. Кроме бесконечного множества почти-полей Диксона существует лишь семь исключительных конечных почти-полей порядка p^2 для простых чисел $p \in \{5, 7, 11, 23, 29, 59\}$, из них для $p = 11$ существуют два почти-поля.

Конечное почти-поле служит линейным пространством над некоторым полем. Поэтому аддитивная группа конечного почти-поля изоморфна аддитивной группе поля Галуа той же мощности. Хотя для некоторых почти-полей элементы этого поля не всегда коммутируют с остальными элементами объемлющего почти-поля [4, 5]. Некоторые линейные уравнения над почти-полем соответствуют нелинейным уравнениям над полем Галуа.

В 1891 году Герман Винер (Hermann Wiener, 1857–1939) сообщил о независимости теоремы Дезарга от некоторых аксиом плоскости [6]. Точнее, такова поздняя интерпретация его результата [7], поскольку Винер использует не аксиомы, но лишь набор допустимых операций. Следующий шаг сделал Давид Гильберт в 1899 году, когда построил пример бесконечной недезарговой плоскости. Позже изящный пример недезарговой плоскости опубликовал американский астроном Форест Рэй Моултон (Forest Ray Moulton, 1872–1952) [7].

Недезарговы проективные плоскости девятого порядка построили Освальд Веблен (Oswald Veblen, 1880–1960) и Джозеф Веддербарн (Joseph Henry Maclagan Wedderburn, 1882–1948) в 1905 году [8]. Они использовали почти-поле Диксона из девяти элементов. Точки проективной плоскости соответствуют классам эквивалентных троек (x, y, z) элементов алгебры, среди которых хотя бы один отличен от нуля. Для ненулевого элемента κ две тройки координат (x, y, z) и $(\kappa x, \kappa y, \kappa z)$ определяют одну точку. Всего 91 точка. Линии определяются линейными уравнениями, но здесь важно место коэффициентов линейных уравнений. Авторы предлагают следующие уравнения: 81 вида $x + y\alpha + z\beta = 0$, девять вида $y + z\beta = 0$ и ещё $z = 0$. Итого, получится 91 линия по 10 точек в каждой. Так определена недезаргова плоскость порядка 9.

2. Результаты и обсуждение

Пусть переменные x_k и y_k принимают значения в поле $GF(3)$ вычетов по модулю три. Обозначим через $z_k = x_k + y_k\lambda$ переменные над левым почти-полем из девяти элементов с порождающим элементом λ и умножением $(a+b\lambda)(c+d\lambda) = ac-(a^2+b^2)bd+\big(bc+(a^2+b^2)ad\big)\,\lambda$. Поле $GF(3)$ изоморфно центру этого почти-поля.

Для a, b, c, d, f и g из $GF(3)$, если оба элемента $a+b\lambda$ и $c+d\lambda$ почти-поля отличны от нуля, то уравнение $z_1(a + b\lambda) = z_2(c + d\lambda) + f + g\lambda$ определяет взаимно однозначное соответствие между переменными z_1 и z_2. Над полем $GF(3)$ это уравнение соответствует системе из двух нелинейных уравнений от четырёх переменных x_1, y_1, x_2 и y_2. Выделяя части без множителя λ и с λ, получим систему двух уравнений:

$$\left\{\begin{array}{rcl} x_1a - (x_1^2 + y_1^2)y_1b & = & x_2c - (x_2^2 + y_2^2)y_2d + f \\ y_1a + (x_1^2 + y_1^2)x_1b & = & y_2c + (x_2^2 + y_2^2)x_2d + g \end{array}\right. .$$

Учитывая тождество $x^3 = x$, эту систему можно переписать так:

$$\left\{\begin{array}{rcl} ax_1 - bx_1^2y_1 - by_1 & = & cx_2 - dx_2^2y_2 - dy_2 + f \\ bx_1 + bx_1y_1^2 + ay_1 & = & dx_2 + dx_2y_2^2 + cy_2 + g \end{array}\right. .$$

Также можно рассматривать и другие уравнения от одной или двух переменных над почти-полем. При этом уравнение от одной переменной может иметь несколько решений. Например, уравнение $z\lambda = \lambda z$ над почти-полем имеет пять решений $\{0, 1, 2, \lambda, 2\lambda\}$, а не девять.

Уравнение $z_1\lambda = \lambda z_2$ от двух переменных над почти-полем соответствует паре уравнений от четырёх уравнений над полем, которые линейны по двум переменным.

Уравнение $\lambda z_1 = \lambda z_2$ от двух переменных над почти-полем соответствует паре линейных уравнений над полем.

Если рассматривать систему из таких пар уравнений от чётного числа переменных x_k и y_k, где уравнения из каждой пары зависят лишь от четырёх переменных, то разрешимость такой системы легко проверяется за полиномиальное время. Если эта система не разбивается на подсистемы от непересекающихся наборов переменных, то число решений не может быть больше девяти. Более того, все решения можно найти за полиномиальное время. Для этого выберем некоторую пару переменных, например, x_1 и y_1. Фиксируем некоторые значения этих двух переменных над $GF(3)$, всего девять вариантов. Это позволяет вычислить значения другой пары или нескольких пар переменных. Продолжая этот процесс, мы либо найдём решение, либо придём к противоречию.

Если же система разбивается на подсистемы от непересекающихся наборов переменных, то эти подсистемы легко найти жадным алгоритмом по аналогии с поиском компонент связности в неориентированном графе. Далее эти подсистемы рассматриваются независимо. В этом случае общее число решений может быть экспоненциально большим. Но число решений вычисляется за полиномиальное время.

Аналогично можно рассматривать другие конечные почти-поля, а также квазиполя, в которых умножение не обязательно ассоциативно [9, 10]. В частности, это позволяет решать некоторые системы нелинейных уравнений над полем Галуа большого порядка.

Геометрический смысл этого подхода в том, что рассматривается конфигурация из недезарговых плоскостей. Некоторые линии из разных плоскостей отождествляются друг с другом, обеспечивая согласование координат между некоторыми плоскостями. Однако эта конфигурация плоскостей и линий не вложена ни в какое объемлющее проективное пространство. Важно, что рассматриваемые уравнения зависят от самое большее двух переменных над почти-полем, хотя они соответствуют нелинейным уравнениям от большего числа переменных над полем. Иными словами, это уравнение определяет линию на недезарговой плоскости. К сожалению, над почти-полем нет быстрого алгоритма для решения линейных уравнений общего вида, зависящих от большого числа переменных. При этом недезаргова плоскость не вкладывается в пространство большей размерности. Поэтому уравнение от многих переменных уже не имеет естественной геометрической интерпретации.

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

Список цитированной литературы

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

2. Dickson L. E. Linear algebras in which division is always uniquely possible // Transactions of the American Mathematical Society. 1906. Vol. 7, № 3. P. 370–390. DOI: 10.2307/1986324

3. Zassenhaus H. J. Über endliche Fastkörper // Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg. 1935. Vol. 11. P. 187–220. DOI: 10.1007/BF02940723

4. Кравцова О. В., Левчук В. М. Вопросы строения конечных почти-полей // Труды ИММ УрО РАН. 2019. Том 25, № 4. С. 107–117. DOI: 10.21538/0134-4889-2019-25-4-107-117

5. Яковлева Т. Н. Вопросы строения квазиполей с ассоциативными степенями // Известия Иркутского государственного университета. Серия Математика. 2019. Том 29. С. 107–119. DOI: 10.26516/1997-7670.2019.29.107

6. Wiener H. Ueber Grundlagen und Aufbau der Geometrie // Jahresbericht der Deutschen Mathematiker-Vereinigung. 1890/91. Vol. 1. P. 45–48.

7. Moulton F. R. A simple non-Desarguesian plane geometry // Transactions of the American Mathematical Society. 1902. Vol. 3. P. 192–195. DOI: 10.1090/S0002-9947-1902-1500595-3

8. Veblen O., Maclagan-Wedderburn J. H. Non-Desarguesian and non-Pascalian geometries // Transactions of the American Mathematical Society. 1907. Vol. 8. P. 379–388. DOI: 10.1090/S0002-9947-1907-1500792-1

9. Кравцова О. В., Логинова В. С. Вопросы строения конечных квазиполей Холла // Труды ИММ УрО РАН. 2024. Том 30, № 1. С. 128–141. DOI: 10.21538/0134-4889-2024-30-1-128-141

10. Kravtsova O. V., Loginova V. S. Finite quasifields with the Hall condition // Journal of Siberian Federal Universit. Mathematics and Physics. 2026. Vol. 19, № 2. P. 231–247. EDN: WTAIQQ

УДК 519.17

Критерии асимметричности графа с малым количеством вершин

В. В. Тензина (РФ, г. Москва)
Московский государственный университет им. М. В. Ломоносова
e-mail: viktoria.tenzina@math.msu.ru

Ways to identify asymmetry in graphs with few vertices

V. V. Tenzina (Russia, Moscow)
Lomonosov Moscow State University
e-mail: viktoria.tenzina@math.msu.ru

Асимметричным графом называется граф, чья группа автоморфизмов состоит из одного элемента - тождественного изоморфизма. Количество всех неизоморфных простых неориентированных графов, то есть без кратных рёбер и петель, с n вершинами, представлено в последовательности A003400 из [1].

Перестановочная матрица — это такая квадратная матрица, у которой в каждом столбце и в каждой строке стоит ровно одна единица, а остальные элементы нули (см. [2]). Напомним, что два графа Γ_1, Γ_2 с соответствующими матрицами смежности A_1 и A_2 изоморфны тогда и только тогда, когда найдётся перестановочная матрица P такая, что $A_2 = P^T A_1 P$ (см. [3]).

Утверждение 1. *Пусть Γ — простой неориентированный граф, A — его матрица смежности. Если найдётся такое натуральное число k, что все элементы на диагонали матрицы A^k различны, то граф Γ асимметричен.*

Как известно (например, из [1]), существует ровно 8 асимметричных графов с 6-ю вершинами.