УДК 512.624

В. Г. Алябьева

Приложения конечных полей

В настоящей статье показаны приложения конечных полей в теории кодирования, конечных геометриях и рекуррентных последовательностях.

Ключевые слова: конечные поля, теория кодирования, конечные геометрии, рекуррентные последовательности.

V. G. Alyabieva

Applications of the Finite Fields

In the present article are shown applications of the finite fields in the coding theory, finite geometries and recurrent sequences.

Keywords: the finite fields, the coding theory, finite geometries, recurrent sequences.

Систематически конечные поля стали изучаться с начала XIX века. Современная теория конечных полей – раздел алгебры, актуальность которого чрезвычайно возросла в связи с разнообразными приложениями в комбинаторике, теории кодирования, в математической теории переключательных схем.

В теории чисел есть раздел, который наиболее естественным образом описывается в теоремах конечных полей. Конечные поля функционально полны. Это значит, что любое отображение конечного поля в себя можно представить в виде некоторого многочлена.

Произвольное конечное поле F_q имеет порядок, равный натуральной степени простого числа:

$q = p^n$, $n \in N$, p – простое число. Для любого простого числа p и любого натурального числа n существует конечное поле F_{p^n}, единственное с точностью до изоморфизма.

Поле порядка p^n можно построить как простое расширение простого поля F_p с помощью корня неприводимого над F_p многочлена степени n, который в поле F_{p^n} содержит все свои корни и поэтому разлагается над F_{p^n} на линейные множители. Простые поля $\boldsymbol{F_p}$ были исследованы Ферма, Эйлером, Лагранжем, Лежандром и Гауссом. Поля F_{p^n} впервые появились в статье Э. Галуа «Из теории чисел» [2] в 1830 году в связи с решением сравнений по модулю p в расширениях поля F_p (в честь Галуа конечные поля F_q стали называть полями Галуа и обозначать GF_q).

Э. Галуа, продолжая исследования Гаусса, рассматривает процедуру расширения поля F_p с помощью корня многочлена $f(x)$ степени n, неприводимого над F_p.

Пусть $f(x) = b_0 + b_1 x + b_2 x^2 + ... + b_n x^n$, $f(x) \in F_p[x]$. Обозначим через α корень $f(x)$. Тогда α принадлежит расширению F_{p^n} поля F_p, и любой элемент из F_{p^n} однозначно представим в виде $a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{n-1}\alpha^{n-1}$ (1), где $a_0, a_1, a_2, ..., a_{n-1} \in F_p$.

Число элементов вида (1) равно p^n. Относительно сложения и умножения элементы вида (1) образуют поле. Заметим, что степени α с показателями, превышающими $n-1$, также представляются в виде (1).

После работ Галуа изучение «высших сравнений», как тогда называли уравнения над конечными полями, было продолжено в работах Шенемана (T. Schönemann, 1846), Серре (J. A. Serre, 1854), Дедекинда (Dedekind R., 1857).

В докладе, прочитанном в 1893 году на Международном математическом конгрессе в Чикаго, американский математик Э. Г. Мур (E. H. Moore) сообщил о доказательстве теоремы: «*Любое конечное поле есть поле Галуа*» [12].

Ученик Мура Л. Диксон (L. E. Dickson) дал первое систематическое изложение теории конечных полей. Совместно с М. Уэддерберном (J. H. M. Wedderburn) Диксон доказал в 1905 году, что, говоря современным языком, *любое конечное тело есть поле*.

В большой статье 1905 года «О конечных алгебрах» [9] Диксон исследовал независимость постулатов конечного поля и построил два типа конечных алгебр, для которых не выполняются некоторые постулаты поля. Одна алгебра – с делением, в ней умножение некоммутативно и выполняется правый дистрибутивный закон умножения относительно сложения. Диксон доказал, что если (p^n-1) и n не взаимно просты (p – простое число), то существует по крайней мере одна некоммутативная алгебра с p^n элементами. Ученый обосновал утверждение, что коммутативность сложения и коммутативность умножения элементов конечной алгебры с делением являются следствиями остальных аксиом поля, но ни один из дистрибутивных законов исключить нельзя, если мы хотим, чтобы алгебра относительно сложения и умножения элементов оставалась полем.

Исследования Диксона некоммутативных алгебр с делением продолжил в 1935 году Ганс Цассенхаус (G. Zassenhaus). Он перечислил все возможные конечные алгебры с делением, в которых выполняется лишь один из дистрибутивных законов, например, левый. Цассенхаус назвал такие алгебры почти-полями и в статье «О конечных почти-полях» [15] дал общий метод их построения.

Подобно тому, как над полями вещественных и комплексных чисел можно построить геометрии разных размерностей, так и над конечными алгебрами можно строить конечные геометрии. Свойства геометрии зависят от свойств алгебр, над которыми они построены.

Ученик Мура Освальд Веблен (O. Veblen) в 1906 году в статье «Конечные проективные геометрии» [13] указал общий метод построения конечных проективных пространств размерностей, превышающих 2, и конечных проективных плоскостей над полями Галуа, сформулировал аксиоматику конечной n–мерной геометрии, исследовал группу коллинеаций геометрии.

Веблен *конечную проективную плоскость* определял следующим образом.

Задано *конечное множество* элементов, называемых *точками*. Некоторые выделенные подмножества точек называются *прямыми*, каждая из которых содержит по крайней мере три точки.

Через любые две различные точки проходит одна и только одна прямая. Если A, B, C – три неколлинеарных точки, а прямая l проходит через точку D прямой AB и через точку E прямой BC, то l содержит точку F прямой AC.

Так, определенная плоскость обладает обычными проективными свойствами. Например, плоскость определяется любыми тремя неколлинеарными точками; прямая, соединяющая две точки плоскости, полностью принадлежит плоскости.

Веблен доказал, что в проективной n-мерной геометрии для $n \geq 3$ теорема Дезарга следует из аксиом этой геометрии и того факта, что порядок поля Галуа, над которым строится геометрия, отличен от 2^n. Используя эту теорему, Веблен построил геометрическую алгебру точек на прямой. Эта алгебра удовлетворяет всем аксиомам поля, кроме коммутативности умножения. Позднее Уэддерберн доказал, что умножение в такой алгебре будет коммутативно всякий раз, когда число точек на прямой конечно. В 1907 году Веблен совместно с Уэддерберном опубликовал статью «Недезарговы и

непаскалевы геометрии» [14], в которой были построены первые конечные недезарговы проективные плоскости над алгебрами Диксона порядка 9.

Столетняя история развития и применения конечных геометрий – это особая тема. Из эпизодов современной математики отметим использование конечных геометрий и групп их коллинеаций в решении проблемы классификации простых конечных групп [3].

Важнейшими приложениями теории конечных полей является теория линейных рекуррентных последовательностей (над конечными полями) и теория кодирования. История исследований линейных рекуррентных последовательностей насчитывает многие века. Основы общей теории рекуррентных последовательностей были разработаны в XVIII веке французским математиком А. Муавром. Он так определяет рекуррентный ряд: «*Если какой-либо ряд так составлен, что если взять произвольно несколько членов, то каждый последующий всегда имеет данную зависимость от такого же числа предыдущих, то такой ряд я называю рекуррентным. Числовые же количества, взятые вместе и соединенные их собственными знаками, составляют индекс отношения».* Если общий член ряда задается равенством $u_{n+k} = a_0 u_{n+k-1} + a_1 u_{n+k-2} + \ldots + a_{k-1} u_n$, то индекс (или *шкала*) отношения состоит из коэффициентов $a_0, a_1, \ldots, a_{k-1}$.

Даниил Бернулли (1732) указал способ приближенного нахождения корней уравнения при помощи рекуррентных рядов.

Развернутую теорию рекуррентных рядов построил крупнейший математик XVIII века Леонард Эйлер во «Введении в анализ бесконечных» [8]. Весь первый том «Введения» посвящен бесконечным рядам и по праву мог быть озаглавлен как «Исчисление рядов». Эйлер считает, что разложение в рекуррентные ряды дробных функций «*совершенно необходимо в интегральном исчислении».* Он пишет: « *Здесь я вывел как их [рядов] суммы, так и их общие члены, а также другие замечательные свойства. И так как к этому привело их разложение на множители, то я разобрал и обратную задачу: каким образом произведения многих, даже бесконечного числа, множителей путем перемножения развертываются в ряды. Это открывает путь к изучению бесчисленного количества рядов. Так как этим способом можно разлагать в ряды произведения из бесчисленного числа сомножителей, то я нашел довольно удобные числовые выражения для логарифмов, синусов и тангенсов. Кроме того, я вывел из того же источника решение многих вопросов, которые могут возникнуть при разбиении чисел; вопросы подобного рода без помощи этих приемов, по-видимому, превышают силы анализа».*

Путем непрерывного деления Эйлер разлагает дробь $\frac{a}{\alpha + \beta z}$ в бесконечный геометрический ряд (2): $\frac{a}{\alpha} - \frac{a\beta}{\alpha^2} z + \frac{a\beta^2}{\alpha^3} z^2 - \frac{a\beta^3}{\alpha^4} z^3 + \ldots$, в котором отношение любого члена к последующему постоянно и равно $\left(-\frac{\alpha}{\beta}\right)$. Заметим, что коэффициенты ряда (2) можно найти, используя равенство $\frac{a}{\alpha + \beta z} = A + Bz + Cz^2 + Dz^3 + \ldots$ и приравнивая коэффициенты при тождественных степенях z. Коэффициент при степени z^n равен $(-1)^n \frac{a\beta^n}{\alpha^{n+1}}$.

Подобным образом путем непрерывного деления Эйлер разлагает в бесконечный ряд дробную функцию $\frac{a + bz}{\alpha + \beta z + \gamma z^2}$.

Если знаменатель дроби линеен относительно z и равен $\alpha + \beta z$, то каждый последующий коэффициент в ряду разложения определяется только по *одному* предыдущему. Если знаменатель дроби представляет собой четырехчлен $\alpha + \beta z + \gamma z^2 + \delta z^3$, то любой коэффициент S ряда разложения определяется по *трем* предыдущим коэффициентам R, Q, P, так как

$$\alpha S + \beta R + \gamma Q + \delta P = 0.$$

Подводя итог, Эйлер пишет: «*Итак, в этих рядах любой член определяется по нескольким предыдущим согласно некоторому постоянному закону, причем этот закон сам собой определяется из знаменателя дроби, производящей этот ряд*».

Новый импульс развития теория рекуррентных рядов получила в исчислении конечных разностей. В этом направлении работали П. Л. Чебышев и А. А. Марков.

Современное направление связано с исследованиями линейных последовательностей над конечными полями. Для случая конечных простых полей порядка p первый весомый вклад был сделан W. Mantel (1894), для случая полей порядка p^n – U. Scarpies (1912).

Во второй половине XX века теория линейных рекуррентных последовательностей развивалась в связи с формированием теории кодов, исправляющих ошибки, криптографии и возможностей элементной базы вычислительной техники. Теория линейных рекуррентных последовательностей преобразовалась в теорию полилинейных рекуррентных последовательностей над модулями и кольцами и продолжает развиваться дальше.

Линейные рекуррентные последовательности над конечными полями с необходимостью периодичны, поэтому центральным вопросом в исследовании их свойств является вычисление минимального периода. Для оценки длины периода рекуррентной последовательности можно использовать сопровождающую матрицу: минимальный период последовательности порядка k над полем F_q делит порядок линейной группы $GL(k, F_q)$, равный

$$q^{\frac{k^2-k}{2}} \cdot (q-1)(q^2-1) \cdot \ldots \cdot (q^k-1).$$

Одним из важнейших инструментов для исследования периодичности последовательности является характеристический многочлен. Если линейная рекуррентная последовательность задана соотношением

$$u_{n+k} = a_{k-1}u_{n+k-1} + a_{k-2}u_{n+k-2} + \ldots + a_0 u_n,\ n = 0,1,\ldots,\ a_i \in F_q,\ 0 \le i \le k-1,$$

то характеристический многочлен последовательности имеет вид

$$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \ldots - a_0.$$

Если характеристический многочлен $f(x)$, где $f(0) \neq 0$, линейной однородной рекуррентной последовательности $\{u_n\}$ (с ненулевым вектором начального состояния) порядка k над полем F_q неприводим, то последовательность является чисто периодической, и ее минимальный период r равен порядку многочлена $f(x)$. *Порядком* $ordf(x)$ многочлена $f(x)$ называется наименьший неотрицательный показатель степени n, для которого выполняется соотношение $(x^n - 1) \vdots f(x)$.

Порядок можно вычислить у любого ненулевого многочлена. Порядки неприводимых многочленов $f(x)$ над F_q (где $f(0) \neq 0$) обладают свойствами, к важнейшим из которых относятся следующие:

1) порядок неприводимого над F_q многочлена совпадает с порядком любого своего корня (как элемента мультипликативной группы поля F_q) и поэтому является делителем $(q-1)$;

2) если многочлен $f(x)$, $f(0) \neq 0$, разлагается на неприводимые множители, то существуют алгоритмы, позволяющие вычислить порядок $f(x)$ по известным порядкам неприводимых сомножителей в каноническом разложении $f(x)$.

Теория конечных полей нашла применение и в теории кодирования.

Началом теории корректирующих кодов считается 1948 год, когда была опубликована статья Клода Шеннона «Математическая теория связи» [7]. Шеннон установил, что по каналу связи информация может передаваться безошибочно в том случае, если скорость передачи не превышает пропускной способности канала. Однако доказательства Шеннона носили неконструктивный характер. Впервые конструктивный метод построения кодов с избыточностью и простым декодированием предложил Ричард Хэмминг в 1950 году. Хэмминг, исследователь с многообразными научными интересами, в своей единственной статье «Коды с обнаружением и исправлением ошибок» [6] предопределил направление большинства работ в этой области. Заметим, что коды, способные корректировать ошибки, были предложены Хэммингом еще до 1948 года, когда была опубликована статья Шеннона. В своей работе Шеннон, ссылаясь на исследования Хэмминга 1947 года, построил в качестве примера простой код длины 7, исправляющий все одиночные ошибки. Если Хэмминг рассматривал коды только над конечным полем F_2 (бинарные коды), то корректирующие коды над произвольными конечными полями, независимо от Хэмминга, построил в 1949 году М. Е. Голей [10]. Поэтому, ради исторической справедливости, уместнее называть коды Хэмминга кодами Хэмминга – Голея. Методы Хэмминга имели фундаментальное значение. Они продемонстрировали инженерам возможность практической реализации приемов кодирования, разработанных в теории информации. Хэмминг ввел в обиход важнейшее понятие теории кодирования – *расстояние Хэмминга* $d(x,y)$ между кодовыми словами, равное числу координат, которыми различаются векторы x и y. Он же нашел соотношение, связывающее длину n корректирующего бинарного кода, содержащего M слов и исправляющего t ошибок

$$\sum_0^t C(n,i) \leq \frac{2^n}{M},$$

где $C(n,i)$ равно числу сочетаний из n по i.

Для случая кода над произвольным конечным полем F_q соотношение имеет вид:

$$\sum_0^t C(n,i) \cdot (q-1)^t \leq \frac{q^n}{M}.$$

Метод Хэмминга основан на добавлении избыточной информации к передаваемому слову. Пусть код строится над произвольным конечным полем F_q. Сообщение $a_1 a_2 \ldots a_k$, $(a_i \in F_q)$ кодируется в кодовое слово $x = a_1 a_2 \ldots a_k x_{k+1} \ldots x_n$, $x_i \in F_q$.

Линейный код, соответствующий описанной процедуре, задается матричным уравнением: $Hx^T = 0$ (3), где H – проверочная матрица размера $(n-k, n)$.

Множество решений уравнения (3) образует k-мерное пространство F_q^k над F_q и задает $(n,k)-$код. Базис пространства F_q^k образуют k линейно независимых кодовых слов. В качестве базисных векторов можно взять строки порождающей матрицы G, которая связана с проверочной матрицей соотношением: $GH^T = 0$. Тогда все кодовые слова могут быть найдены из соотношения: $x = aG$.

Работа Хэмминга сыграла ключевую роль в развитии теории кодирования и стимулировала дальнейшие исследования. В 1956 году Давид Слепян построил [5] общую теорию линейных кодов. Существенное продвижение в теории кодов предопределили работы французского ученого А. Хоквингема (1959, [11]) и американских исследователей Р. К. Боуза и Д. К. Рой-Чоудхури (1960, [1]), построивших большой класс кодов (БЧХ-кодов), исправляющих кратные ошибки. Американцы И. С. Рид и Г. Соломон (1960, [4]) построили код для недвоичных каналов, связанный с БЧХ-кодами.

В 1957–58 годах Прейнджем (E. Prange) были впервые построены циклические коды, являющиеся частным видом линейных кодов.

Циклические коды могут быть построены следующим образом. Между пространством F_q^n всех n-мерных векторов над F_q и фактор-кольцом $F_q[x]/(x^n-1)$ можно установить изоморфизм, позволяющий n-мерный вектор рассматривать как многочлен степени $n-1$. Каждому кодовому слову в циклическом коде сопоставляется кодовый многочлен $w(x)$. Тогда циклический код образует главный идеал в фактор-кольце $F_q[x]/(x^n-1)$ и задается порождающим многочленом $g(x)$. С порождающим многочленом $g(x)$ связан проверочный многочлен $h(x)$. Перечисленные многочлены связаны следующими соотношениями:

- $w(x)\cdot h(x) = 0;$
- $a(x)\cdot g(x) = w(x)$ ($a(x)$ – информационный многочлен);
- $h(x)\cdot g(x) = 0$.

Алгебраические средства позволяют нам эффективно кодировать и декодировать сообщения.

Библиографический список

1. Боуз, Р. К., Рой-Чоудхури, Д. К. Об одном классе двоичных групповых кодов с исправлением ошибок [Текст] / Р. К. Боуз, Д. К. Рой-Чоудхури // Кибернетический сборник. – Вып. 2. – М. : Издательство иностранной литературы, 1961. – С. 83–94.

2. Галуа, Э. Сочинения [Текст] / Э. Галуа. – М.-Л. : ОМТИ,1936. – С. 35–47.

3. Горенстейн, Д. Конечные простые группы. Введение в их классификацию [Текст] / Д. Горенстейн. – М. : Мир, 1985.

4. Рид, И. С., Соломон, Г. Полиномиальные коды над некоторыми конечными полями [Текст] / И. С. Рид, Г. Соломон // Кибернетический сборник. – Вып. 7. – М. : Издательство иностранной литературы, 1963. – С. 74–79.

5. Слепян, Д. Класс двоичных сигнальных алфавитов [Текст] / Д. Слепян // Теория передачи сообщений. – М. : Издательство иностранной литературы, 1957. – С. 82–113.

6. Хэмминг, К. Коды с обнаружением и исправлением ошибок [Текст] / К. Хэмминг // Коды с обнаружением и исправлением ошибок. – М. : Издательство иностранной литературы, 1956. – С. 7–23.

7. Шеннон, К. Математическая теория связи [Текст] / К. Шеннон // Работы по теории информации и кибернетике. – М. : Издательство иностранной литературы, 1963. – С. 243–332.

8. Эйлер, Л. Введение в анализ бесконечных. В 2 т. Т. 1 [Текст] / Л. Эйлер ; пер. Е. Л. Пацановского. – М. : Государственное издательство физико-математической литературы, 1961.

9. Dickson L.E. Of finite algebras// Nachrichten von der Königlichen Gesellschaft der Wissenschaften und der Georg–August – Universität zu Göttingen. 1905. S. 358 – 393.

10. Goley M.J.E. Notes on digital coding // Proceedings IRE. 1949. V. 37, P.657.
11. Hocquenchem A. Codes correcteurs d'erreurs. Chiffres 2. 1959. 147–156.
12. Moore E. H. A double–infinite systems of simple groups / Mathematical Papers Read at the International Mathematical Congress in Chicago 1893, published by MacMillan, 1896. P. 208–242.
13. Veblen O. A system of axioms for geometry // Transactions of the American Mathematical Society. 1904.V.5. P. 343–384.
14. Veblen O., Wedderburn J.H.M. Non–Desarguesian and Non–Pascalian Geometries // Transactions of the American Mathematical Society. 1907. V. 8. P. 379–388.
15. Zassenhaus H. Über endliche Fastkörper // Abhandlungen aus dem mathematischer Seminar der Universität Hamburg. 1935. Bd.11. S. 187–220.