ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
СПбГУТ))) Декабрь 2019 Том 7 № 1 ISSN 2307-1303 http://www.itt.sut.ru
TELECOM IT
December 2019 Vol. 7 Iss. 1 ISSN 2307-1303 http://www.itt.sut.ru

ЗАВИСИМОСТЬ СТРУКТУРНЫХ СВОЙСТВ ДВОЙСТВЕННОГО БАЗИСА ОТ ВИДА ХАРАКТЕРИСТИЧЕСКОГО МНОГОЧЛЕНА

Д. С. Кукунин

Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

Адрес для переписки: coux@yandex.ru

Аннотация
Актуальность темы связана с решением задач обработки рекуррентных последовательностей. Используемый при этом метод определения начальной фазы псевдослучайной последовательности, построенной по характеристическому многочлену, позволяет производить ее обработку непосредственно в процессе приема. Данный подход не требует обязательного накопления всей последовательности целиком, что значительно повышает оперативность работы системы, использующей в качестве метода декодирования рекуррентных последовательностей двойственный базис. Метод декодирования с использованием двойственного базиса поля Галуа представляет собой эффективное средство защиты от ошибок в цифровой системе передачи данных, где в качестве помехоустойчивых кодов могут быть использованы коды БЧХ, Рида-Соломона и другие разновидности рекуррентных последовательностей. Вместе с тем вычисление элементов базиса, двойственного левому степенному базису, порождает ряд задач, связанных с математическими вычислениями над элементами конечного поля. В данной работе рассмотрены способы нахождения элементов двойственного базиса, предложены варианты упрощенных процедур их вычисления, а также поставлена задача провести исследование структурных свойств двойственного базиса, которые зависят от вида характеристического многочлена. **Предмет исследования.** Работа посвящена изучению двоичных полей Галуа, в частности, затрагиваются свойства левого степенного и двойственного ему базиса. **Метод.** На примере М-последовательностей подробно рассмотрена процедура нахождения элементов двойственного базиса через функцию след с использованием математического аппарата, разработанного О. С. Когновицким. **Основные результаты.** Анализ приведенных свойств двойственного базиса позволил выявить новые структурные зависимости между его элементами. **Практическая значимость.** Выявленные структурные зависимости между элементами двойственного базиса поля Галуа позволяют значительно упростить реализацию процедуры формирования его элементов.

Ключевые слова
Поле Галуа, элемент поля, левый степенной базис, двойственный базис, рекуррентные последовательности, функция след.

Информация о статье
УДК 512.623.35
Язык статьи – русский.
Поступила в редакцию 01.07.19, принята к печати 02.09.19.

Ссылка для цитирования: Кукунин Д. С. Зависимость структурных свойств двойственного базиса от вида характеристического многочлена // Информационные технологии и телекоммуникации. 2019. Том 7. № 1. С. 41–51. DOI 10.31854/2307-1303-2019-7-1-41-51

DEPENDENCE OF THE STRUCTURAL PROPERTIES OF THE DUAL BASIS ON THE TYPE OF THE CHARACTERISTIC POLYNOMIAL

D. Kukunin

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Corresponding author: coux@yandex.ru

Abstract—The relevance of the topic is connected with the solution of problems of processing of recurrent sequences. The method used to determine the initial phase of a pseudorandom sequence constructed by the characteristic polynomial allows its processing directly in the receiving process. This approach does not require mandatory accumulation of the entire sequence, which significantly increases the efficiency of the system, which uses a dual basis as a method of decoding recurrent sequences. The method of decoding using the dual basis of the Galois field is an effective means of protection against errors in a digital data transmission system, where the codes of BCH, Reed-Solomon and other varieties of recurrent sequences can be used as noise-resistant codes. At the same time, the calculation of the elements of the basis dual to the left power basis generates a number of problems related to mathematical calculations over the elements of a finite field. In this paper, the methods of finding the elements of the dual basis are considered, the variants of simplified procedures for their calculation are proposed, and the task is to study the structural properties of the dual basis, which depend on the type of the characteristic polynomial. **Research subject.** The work is devoted to the study of binary Galois fields, in particular, the properties of the left power and dual basis are affected. **Method.** On the example of M-sequences, the procedure for finding the elements of the dual basis through the trace function is considered in detail using the mathematical apparatus developed by O. S. Kognovitsky. **Core results.** The analysis of the given properties of the dual basis allowed to reveal new structural dependences between its elements. **Practical relevance.** The revealed structural dependences between the elements of the dual basis of the Galois field make it possible to significantly simplify the implementation of the procedure for the formation of its elements.

Keywords—Galois field, field element, left power basis, dual basis, recurrent sequences, trace function.

Article info
Article in Russian.
Received 01.07.19, accepted 02.09.19.

For citation: Kukunin D.: Dependence of the Structural Properties of the Dual Basis on the Type of the Characteristic Polynomial // Telecom IT. 2019. Vol. 7. Iss. 1. pp. 41–51 (in Russian). DOI 10.31854/2307-1303-2019-7-1-41-51

Полем называется коммутативное кольцо с единичным элементом относительно умножения, в котором каждый ненулевой элемент имеет мультипликативный обратный элемент (обратный по умножению). Поля с конечным числом элементов q называют полями Галуа и обозначают GF(q). Число элементов поля q называют порядком поля. В зависимости от значения q различают простые или расширенные поля. Поле называется простым, если q – простое число. В данной работе из простых полей используется только двоичное поле GF(2), образованное двумя единичными элементами: «0» – относительно операции сложения и «1» – относительно операции умножения. Из расширенных полей GF(p^k), где характеристика p является простым числом, в данной работе рассматриваются конечные поля GF(2^k).

Ненулевые элементы поля GF(2^k) образуют ряд [1]:

$$1, \varepsilon, \varepsilon^2, \varepsilon^3, \ldots, \varepsilon^{2^k-2}. \quad (1)$$

Каждый ненулевой элемент поля Галуа можно представить в виде степени первообразного элемента ε, который, в свою очередь, является корнем характеристического многочлена:

$$P(x) = p_0x^k + p_1x^{k-1} + \ldots + p_{k-1}x + p_k, \quad p_j \in \text{GF}(2). \quad (2)$$

Многочлен (2) является неприводимым примитивным многочленом, входящим в разложение двучлена $x^n - 1$ на неприводимые сомножители, где $n = 2^k-1$.

Любые k последовательных элементов ряда (1) являются линейно-независимыми над GF(2) и могут образовывать базис поля GF(2^k):

$$[\varepsilon^g, \varepsilon^{g+1}, \varepsilon^{g+2}, \ldots, \varepsilon^{g+k-1}]. \quad (3)$$

Любой элемент поля GF(2^k) можно выразить через различные базисы, в том числе левый степенной и двойственный ему базис [2].

Левый степенной базис поля GF(p^k) представляет собой набор из k последовательных элементов ряда (3) при $g = 0$:

$$[1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{k-1}]. \quad (4)$$

Произвольный элемент ε^j поля GF(2^k) выражается через левый степенной базис следующим образом [1]:

$$\varepsilon^j = a_0 + a_1\varepsilon + a_2\varepsilon^2 + \ldots + a_{k-1}\varepsilon^{k-1}, \; a_i \in \text{GF}(2). \quad (5)$$

Последовательность элементов левого степенного базиса (4), через которые выражен элемент ε^j, обозначим в виде индексированного ряда:

$$a_1, a_2, a_3, \ldots, a_k. \quad (6)$$

Переход к базису, двойственного левому степенному (6), проведем через функцию след. Для элемента ε^j из поля GF(2^k) функция след $T(\varepsilon^j)$ определяется по формуле [2]:

$$T(\varepsilon^j) = \varepsilon^j + \left(\varepsilon^j\right)^2 + \left(\varepsilon^j\right)^{2^2} + \ldots + \left(\varepsilon^j\right)^{2^{k-1}}. \quad (7)$$

Для базиса (6) существует двойственный базис:

$$\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_k, \quad (8)$$

который удовлетворяет свойству [2]:

$$T(\lambda_i \alpha_j) = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}. \quad (9)$$

Одной из задач, решаемых при помощи двойственного базиса, является обработка рекуррентных последовательностей с целью определения их начальной фазы [2, 3, 4, 5]. При этом начальный элемент $c \in \mathrm{GF}(2^k)$, порождающий данную последовательность, может быть определен по произвольному k-элементному участку ($S_g\, S_{g+1} \ldots S_{g+k-1}$) следующим образом [2]:

$$c = \varepsilon^{-g} \sum_{i=1}^{k} \lambda_i S_{g+i-1}, \quad (10)$$

где g – определяет расстояние k-элементного участка от начала M-последовательности.

Таким образом, любой элемент ε^j поля $\mathrm{GF}(2^k)$ можно выразить не только через левый степенной (6), а также через двойственный ему базис [2]:

$$\varepsilon^j = b_0\lambda_1 + b_1\lambda_2 + b_2\lambda_3 + \ldots + b_{k-1}\lambda_k, \; b_i \in \mathrm{GF}(2). \quad (11)$$

Для левого степенного базиса поля $\mathrm{GF}(2^k)$ (6) элементы двойственного базиса λ_ρ определяется по формуле [2]:

$$\lambda_\rho = \frac{\sum_{l=0}^{k-\rho} p_{k-\rho-l}\varepsilon^l}{P'(\varepsilon)}, \; \mathrm{GF}(2^k), \; \rho = 1, 2, \ldots, k, \quad (12)$$

где $P'(\varepsilon)$ – значение производной характеристического многочлена $P(x)$ в точке, соответствующей примитивному элементу поля $\mathrm{GF}(2^k)$.

Приведем пример вычисления элементов двойственного базиса [2] по формуле (12) в поле $\mathrm{GF}(2^8)$, $k = 8$, с характеристическим многочленом $P(x) = x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$ (табл. 1).

Таблица 1

ρ	1	2	3	4	5	6	7	8
λ_ρ	λ_1	λ_2	λ_3	λ_4	λ_5	λ_6	λ_7	λ_8
ε^i	ε^{115}	ε^{229}	ε^{208}	ε^{207}	ε^{206}	ε^{211}	ε^{231}	ε^{116}

Вычисление каждого элемента двойственного базиса по формуле (12) производится независимо от остальных и не учитывает корреляционной связи между ними. Поставим задачу обнаружить зависимости между элементами двойственного базиса и вывести общие правила их описания.

Для примера построим первый k-элементный участок канонической M-последовательности $\{S\}$ с тем же характеристическим многочленом $P(x) = x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$ на основании функций след от подряд идущих элементов поля: $\{S\} = [T(1), T(\varepsilon), T(\varepsilon^2), T(\varepsilon^3), T(\varepsilon^4), T(\varepsilon^5), T(\varepsilon^6), T(\varepsilon^7)]$.

$T(1) = 1+1^2+1^4+1^8+1^{16}+1^{32}+1^{64}+1^{128} = 0$
$T(\varepsilon) = \varepsilon+\varepsilon^2+\varepsilon^4+\varepsilon^8+\varepsilon^{16}+\varepsilon^{32}+\varepsilon^{64}+\varepsilon^{128} = 1$
$T(\varepsilon^2) = \varepsilon^2+(\varepsilon^2)^2+(\varepsilon^2)^4+(\varepsilon^2)^8+(\varepsilon^2)^{16}+(\varepsilon^2)^{32}+(\varepsilon^2)^{64}+(\varepsilon^2)^{128} = 1$
$T(\varepsilon^3) = \varepsilon^3+(\varepsilon^3)^2+(\varepsilon^3)^4+(\varepsilon^3)^8+(\varepsilon^3)^{16}+(\varepsilon^3)^{32}+(\varepsilon^3)^{64}+(\varepsilon^3)^{128} = 1$
$T(\varepsilon^4) = \varepsilon^4+(\varepsilon^4)^2+(\varepsilon^4)^4+(\varepsilon^4)^8+(\varepsilon^4)^{16}+(\varepsilon^4)^{32}+(\varepsilon^4)^{64}+(\varepsilon^4)^{128} = 1$
$T(\varepsilon^5) = \varepsilon^5+(\varepsilon^5)^2+(\varepsilon^5)^4+(\varepsilon^5)^8+(\varepsilon^5)^{16}+(\varepsilon^5)^{32}+(\varepsilon^5)^{64}+(\varepsilon^5)^{128} = 1$
$T(\varepsilon^6) = \varepsilon^6+(\varepsilon^6)^2+(\varepsilon^6)^4+(\varepsilon^6)^8+(\varepsilon^6)^{16}+(\varepsilon^6)^{32}+(\varepsilon^6)^{64}+(\varepsilon^6)^{128} = 1$
$T(\varepsilon^7) = \varepsilon^7+(\varepsilon^7)^2+(\varepsilon^7)^4+(\varepsilon^7)^8+(\varepsilon^7)^{16}+(\varepsilon^7)^{32}+(\varepsilon^7)^{64}+(\varepsilon^7)^{128} = 1$

В дальнейшем, используя простейший генератор с обратной связью, построим следующие $k-1$ элементов данной M-последовательности (…1011101).

На основании полученного $(2k-1)$-элементного участка канонической ($c = 1$) M-последовательности (011111111011101) с учетом формулы (10) можно построить систему линейных уравнений:

$$\begin{cases} \lambda_2+\lambda_3+\lambda_4+\lambda_5+\lambda_6+\lambda_7+\lambda_8 = 1 \\ \lambda_1+\lambda_2+\lambda_3+\lambda_4+\lambda_5+\lambda_6+\lambda_7+\lambda_8 = \varepsilon \\ \lambda_1+\lambda_2+\lambda_3+\lambda_4+\lambda_5+\lambda_6+\lambda_7 = \varepsilon^2 \\ \lambda_1+\lambda_2+\lambda_3+\lambda_4+\lambda_5+\lambda_6+\lambda_8 = \varepsilon^3 \\ \lambda_1+\lambda_2+\lambda_3+\lambda_4+\lambda_5+\lambda_7+\lambda_8 = \varepsilon^4 \\ \lambda_1+\lambda_2+\lambda_3+\lambda_4+\lambda_6+\lambda_7+\lambda_8 = \varepsilon^5 \\ \lambda_1+\lambda_2+\lambda_3+\lambda_5+\lambda_6+\lambda_7 = \varepsilon^6 \\ \lambda_1+\lambda_2+\lambda_4+\lambda_5+\lambda_6+\lambda_8 = \varepsilon^7 \end{cases} \quad (13)$$

где λ_i – элементы двойственного базиса, $i = 1, 2, \ldots, k$.

Система уравнений (13) содержит k неизвестных в k уравнениях, что является достаточным условием для ее решения. В данном случае найти значения элементов двойственного базиса и убедиться в их соответствии элементам, полученным при помощи формулы (12), не составляет труда. Однако, с ростом значения параметра k, возрастает сложность решения такой системы уравнений.

Рассмотрим более детально набор элементов двойственного базиса, полученный в результате использования методов (12) и (13). Отметим две важные особенности.

1). Начальный и конечный элементы λ_1 и λ_k являются последовательными для полей GF(2^k), удовлетворяющими условию:

$$\lambda_k = \lambda_1\varepsilon . \quad (14)$$

Не составляет труда подтвердить данное свойство и на других примерах. Например, рассмотрим поле GF(2^{20}) с характеристическим многочленом $P(x) = x^{20} + x^3 + 1$. Набор элементов двойственного базиса в данном случае будет иметь вид: [$\varepsilon^{1048572}$, $\varepsilon^{1048571}$, $\varepsilon^{1048570}$, ε^{14}, …, ε^3, ε^2, ε, 1, $\varepsilon^{1048574}$, $\varepsilon^{1048573}$]. Начальный и конечный элементы двойственного базиса также будут связаны равенством (14). Докажем данное свойство для полей GF(2^k).

Так как элемент поля ε является корнем характеристического многочлена (2), то справедливо утверждение, что $P(\varepsilon) = 0$ и выполняется равенство:

$$p_0\varepsilon^k + p_1\varepsilon^{k-1} + \ldots + p_{k-1}\varepsilon + p_k = 0, \quad p_j \in GF(2). \tag{15}$$

Равенство (15) запишем в виде:

$$p_0\varepsilon^k + p_1\varepsilon^{k-1} + \ldots + p_{k-1}\varepsilon = -p_k, \quad p_j \in GF(2). \tag{16}$$

Запишем формулу (12) для элемента λ_1:

$$\lambda_1 = \frac{p_{k-1} + p_{k-2}\varepsilon + \ldots + p_1\varepsilon^{k-2} + p_0\varepsilon^{k-1}}{P'(\varepsilon)}. \tag{17}$$

Умножим числитель и знаменатель (17) на ε и с учетом (16) получим:

$$\lambda_1 = \frac{p_{k-1}\varepsilon + p_{k-2}\varepsilon^2 + \ldots + p_1\varepsilon^{k-1} + p_0\varepsilon^k}{\varepsilon P'(\varepsilon)} = \frac{-p_k}{\varepsilon P'(\varepsilon)}. \tag{18}$$

Запишем формулу (12) для элемента λ_k:

$$\lambda_k = \frac{p_0}{P'(\varepsilon)}. \tag{19}$$

Умножим числитель и знаменатель (18) на p_0 и с учетом (19) получим:

$$\lambda_1 = \frac{-p_k p_0}{\varepsilon p_0 P'(\varepsilon)} = \left(\frac{-p_k}{p_0}\right)\varepsilon^{-1}\lambda_k. \tag{20}$$

Так как для поля GF(2^k) $p_0 = p_k = 1$ и $-1 = 1$ (mod2), то будет справедливо равенство $\lambda_1 = \varepsilon^{-1}\lambda_k$, которое соответствует равенству (14).

Таким образом, начальный и конечный элементы двойственного базиса поля GF(2^k) являются последовательными. В дальнейшем участки поля Галуа, составленные из последовательно идущих элементов, будем называть линейными фрагментами поля.

2). Элементы двойственного базиса формируют линейные фрагменты поля Галуа. Возникновение таких фрагментов полностью зависит от структуры характеристического многочлена $P(x)$. Таким образом, для всех элементов двойственного базиса будет справедливо условие:

$$\begin{cases} \lambda_j = \lambda_{j-1}\varepsilon^{-1}, & p_{k-j+1} = 0 \\ \lambda_j \neq \lambda_{j-1}\varepsilon^{-1}, & p_{k-j+1} = 1 \end{cases}, \; j = 1..k. \tag{21}$$

Введем обозначение начального и конечного элементов двойственного базиса γ_i и γ_i^* для i-го линейного фрагмента поля:

$$\begin{cases} \gamma_i = \lambda_j, & p_{k-j+1} = 1 \\ \gamma_i^* = \lambda_j, & p_{k-j} = 1 \end{cases}, \; j = 1..k, \; i = 1..r, \tag{22}$$

где r – вес характеристического многочлена $P(x)$ без старшей степени.

Приведем примеры распределения γ_i и γ_i^* с линейными фрагментами поля для различных характеристических многочленов (табл. 2–6).

Таблица 2

$P(x) = 1 + x^5 + x^6$

p_6	p_5	p_4	p_3	p_2	p_1	p_0
1	0	0	0	0	1	1
λ_1	λ_2	λ_3	λ_4	λ_5	λ_6	
ε^{58}	ε^{57}	ε^{56}	ε^{55}	ε^{54}	ε^{59}	
γ_1					γ_2	
				γ_1^*	γ_2^*	

Таблица 3

$P(x) = 1 + x + x^4 + x^5 + x^6$

p_6	p_5	p_4	p_3	p_2	p_1	p_0
1	1	0	0	1	1	1
λ_1	λ_2	λ_3	λ_4	λ_5	λ_6	
ε^{32}	ε^{7}	ε^{6}	ε^{5}	ε^{9}	ε^{33}	
γ_1	γ_2			γ_3	γ_4	
γ_1^*			γ_2^*	γ_3^*	γ_4^*	

Таблица 4

$P(x) = 1 + x^2 + x^3 + x^4 + x^8$

p_8	p_7	p_6	p_5	p_4	p_3	p_2	p_1	p_0
1	0	1	1	1	0	0	0	1
λ_1	λ_2	λ_3	λ_4	λ_5	λ_6	λ_7	λ_8	
ε^{252}	ε^{251}	ε^{45}	ε^{98}	ε	1	ε^{254}	ε^{253}	
γ_1		γ_2	γ_3	γ_4				
	γ_1^*	γ_2^*	γ_3^*				γ_4^*	

Таблица 5

$P(x) = 1 + x + x^6 + x^9 + x^{10}$

p_{10}	p_9	p_8	p_7	p_6	p_5	p_4	p_3	p_2	p_1	p_0
1	1	0	0	0	0	1	0	0	1	1
λ_1	λ_2	λ_3	λ_4	λ_5	λ_6	λ_7	λ_8	λ_9	λ_{10}	
ε^{785}	ε^{430}	ε^{429}	ε^{428}	ε^{427}	ε^{426}	ε^{434}	ε^{433}	ε^{432}	ε^{786}	
γ_1	γ_2					γ_3			γ_4	
γ_1^*					γ_2^*			γ_3^*	γ_4^*	

Таблица 6.1

$P(x) = 1 + x^5 + x^6 + x^{10} + x^{11} + x^{12} + x^{16}$

p_{16}	p_{15}	p_{14}	p_{13}	p_{12}	p_{11}	p_{10}	p_9	p_8
1	0	0	0	0	1	1	0	0
λ_1	λ_2	λ_3	λ_4	λ_5	λ_6	λ_7	λ_8	λ_9
ε^{38861}	ε^{38860}	ε^{38859}	ε^{38858}	ε^{38857}	ε^{965}	ε^{10073}	ε^{10072}	ε^{10071}
γ_1					γ_2	γ_3		
				γ_1^*	γ_2^*			

Таблица 6.2

$P(x) = 1 + x^5 + x^6 + x^{10} + x^{11} + x^{12} + x^{16}$

p_7	p_6	p_5	p_4	p_3	p_2	p_1	p_0
0	1	1	1	0	0	0	1
λ_{10}	λ_{11}	λ_{12}	λ_{13}	λ_{14}	λ_{15}	λ_{16}	
ε^{10}_{070}	ε^{12}_{188}	ε^{37}_{112}	ε^{38}_{865}	ε^{38}_{864}	ε^{38}_{863}	ε^{38}_{862}	
	γ_4	γ_5	γ_6				
γ_3^*	γ_4^*	γ_5^*				γ_6^*	

Как видно из примеров, элементы γ_i и γ_i^* определяют границы линейных фрагментов поля, при этом полностью удовлетворяя условиям (21) и (22).

На основании (21) и (22) сделаем следующие выводы:

- первый элемент λ_1 всегда принимает значение γ_1, так как $p_k = 1$;
- последний элемент λ_k всегда принимает значение γ_r^*;
- λ_j одновременно принимает значения γ_i и γ_i^*, если $p_j = p_{j+1} = 1$, при этом линейный фрагмент поля состоит из одного элемента.

Анализ распределения границ линейных фрагментов для большого количества известных многочленов $P(x)$, проведенный в рамках данной работы, позволил установить следующие взаимосвязи между элементами двойственного базиса:

$$y_i + y_{i-1}^* \varepsilon^{-1} = y_1, \quad i = 2..r\,, \tag{23}$$

$$y_i^* + y_{i+1} \varepsilon = y_r^*, \quad i = 1..(r-1)\,, \tag{24}$$

где r – вес характеристического многочлена $P(x)$ без старшей степени.

Выражения (23) и (24) определяют взаимосвязь между соседними линейными фрагментами поля, опираясь на начальный ($\gamma_1 = \lambda_1$) и конечный ($\gamma_r^* = \lambda_k$) элементы двойственного базиса. Учитывая при этом свойство (14), изобразим данные связи в цепочке элементов поля Галуа (рис.).

Схема, представленная на рис. и базирующаяся на утверждениях (14), (23) и (24), справедлива для любых характеристических многочленов, используемых при построении поля Галуа $GF(2^k)$. При этом равенство (14) позволяет перейти от равенства (23) к равенству (24) путем умножения левой и правой части на ε. Обратный переход от (24) к (23) осуществляется соответственно при делении обеих частей на ε. Поэтому выражения (23) и (24) можно считать равнозначными равенствами, которые описывают одно структурное свойство двойственного базиса.

Рассмотрим пример выполнения свойства (23) в случае с полем $GF(2^{16})$, построенным по $P(x) = 1 + x^5 + x^6 + x^{10} + x^{11} + x^{12} + x^{16}$, для которого ранее были вычислены элементы двойственного базиса (табл. 6).

Выпишем элементы двойственного базиса, определяющие начальные и конечные точки линейных фрагментов поля, а также отметим длины r_i этих фрагментов.

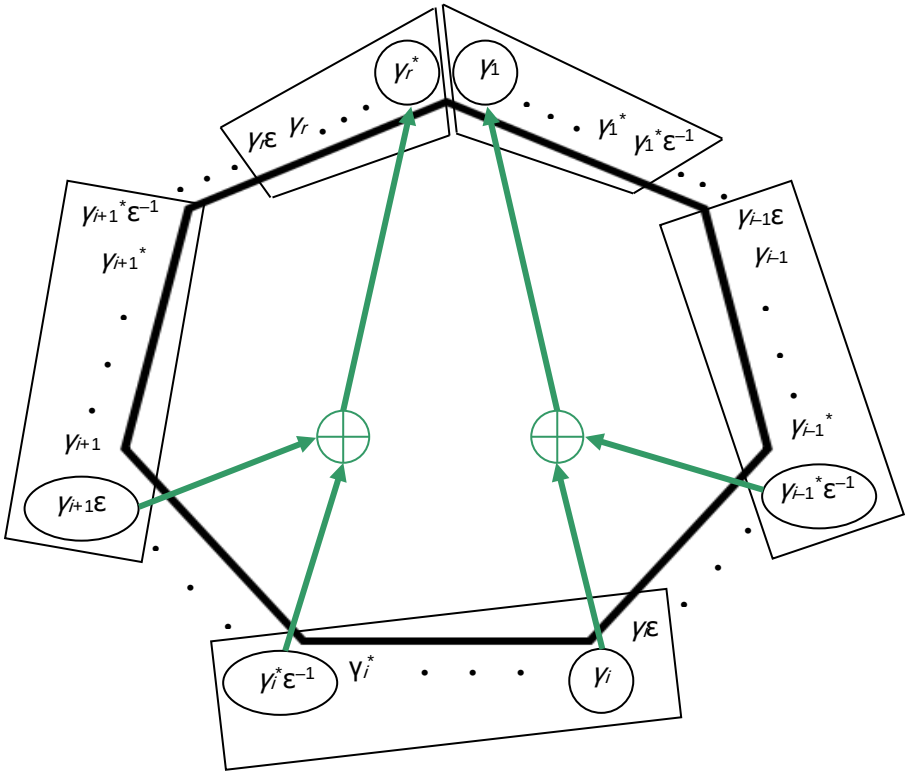

Рис. Структурные связи между линейными фрагментами поля

$\gamma_1=\lambda_1=\varepsilon^{38861}$	$\gamma_1^*=\lambda_5=\varepsilon^{38857}$	$r_1=5$
$\gamma_2=\lambda_6=\varepsilon^{965}$	$\gamma_2^*=\lambda_6=\varepsilon^{965}$	$r_2=1$
$\gamma_3=\lambda_7=\varepsilon^{10073}$	$\gamma_3^*=\lambda_{10}=\varepsilon^{10070}$	$r_3=4$
$\gamma_4=\lambda_{11}=\varepsilon^{12188}$	$\gamma_4^*=\lambda_{11}=\varepsilon^{12188}$	$r_4=1$
$\gamma_5=\lambda_{12}=\varepsilon^{37112}$	$\gamma_5^*=\lambda_{12}=\varepsilon^{37112}$	$r_5=1$
$\gamma_6=\lambda_{13}=\varepsilon^{38865}$	$\gamma_6^*=\lambda_{16}=\varepsilon^{38862}$	$r_6=4$

Видно, что первый линейный фрагмент поля состоит из пяти элементов ($r_1 = 5$), второй, четвертый и пятый – из одного ($r_2 = r_4 = r_5 = 1$), третий и шестой – из четырех ($r_3 = r_6 = 4$). При этом шестой фрагмент, как и положено, сразу переходит в первый, но для выполнения свойства (23) должен рассматриваться как самостоятельный линейный фрагмент поля.

Проверим выполнение (23) для всех линейных фрагментов:

$$\gamma_1^*\varepsilon^{-1} + \gamma_2 = \varepsilon^{38856} + \varepsilon^{965} = \varepsilon^{38861} = \gamma_1 = \lambda_1$$
$$\gamma_2^*\varepsilon^{-1} + \gamma_3 = \varepsilon^{964} + \varepsilon^{10073} = \varepsilon^{38861} = \gamma_1 = \lambda_1$$
$$\gamma_3^*\varepsilon^{-1} + \gamma_4 = \varepsilon^{10069} + \varepsilon^{12188} = \varepsilon^{38861} = \gamma_1 = \lambda_1$$
$$\gamma_4^*\varepsilon^{-1} + \gamma_5 = \varepsilon^{12187} + \varepsilon^{37112} = \varepsilon^{38861} = \gamma_1 = \lambda_1$$
$$\gamma_5^*\varepsilon^{-1} + \gamma_6 = \varepsilon^{37111} + \varepsilon^{38865} = \varepsilon^{38861} = \gamma_1 = \lambda_1$$

Аналогичным образом можно проверить выполнение свойства (24):

$$\gamma_1^* + \gamma_2\varepsilon = \varepsilon^{38857} + \varepsilon^{966} = \varepsilon^{38862} = \gamma_6^* = \lambda_{16}$$
$$\gamma_2^* + \gamma_3\varepsilon = \varepsilon^{965} + \varepsilon^{10074} = \varepsilon^{38862} = \gamma_6^* = \lambda_{16}$$
$$\gamma_3^* + \gamma_4\varepsilon = \varepsilon^{10070} + \varepsilon^{12189} = \varepsilon^{38862} = \gamma_6^* = \lambda_{16}$$
$$\gamma_4^* + \gamma_5\varepsilon = \varepsilon^{12188} + \varepsilon^{37113} = \varepsilon^{38862} = \gamma_6^* = \lambda_{16}$$
$$\gamma_5^* + \gamma_6\varepsilon = \varepsilon^{37112} + \varepsilon^{38866} = \varepsilon^{38862} = \gamma_6^* = \lambda_{16}$$

Данный пример показывает линейную зависимость элементов, которые лежат на границах нескольких линейных фрагментов поля. Отметим при этом важную особенность. Сами линейные фрагменты, формируемые элементами двойственного базиса, не всегда являются последовательными. Например, после первого фрагмента [ε^{38861} ... ε^{38857}] следует второй [ε^{965}], показатель степени элемента которого меньше показателей степеней первого линейного фрагмента. Таким образом, общая схема (рис.) является условной и не учитывает возможное непоследовательное расположение линейных фрагментов в поле Галуа.

Подводя итоги данной работы, отметим рассмотренные способы вычисления элементов двойственного базиса, а также выдвинутые утверждения (23) и (24), которые определяют важные структурные связи между фрагментами поля. Очевидно, что описанные в работе свойства двойственного базиса могут быть использованы при оперативном определении его элементов по заданному характеристическому многочлену, образующему поле.

Вместе с тем, выявленная линейная зависимость между граничными элементами соседних фрагментов поля в дальнейшем может найти широкое практическое применение в задачах обработки длинных псевдослучайных (рекуррентных) последовательностей, в том числе составных.

Литература

1. Когновицкий О. С. Основы циклических кодов: учеб. пособие. Л., 1972.

2. Когновицкий О. С. Двойственный базис и его применение в телекоммуникациях. СПб.: Линк, 2009.

3. Владимиров С. С. Исследование алгоритма мажоритарного декодирования кода Рида-Соломона на основе двойственного базиса // Вестник Поволжского государственного технологического университета. Серия «Радиотехнические и инфокоммуникационные системы». 2012. № 1 (15). С. 60–66.

4. Кукунин Д. С. Анализ эффективности декодирования циклических кодов с использованием двойственного базиса : дис. … канд. техн. наук : 05.13.01 / Кукунин Дмитрий Сергеевич; Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. СПб., 2009. 197 с.

5. Владимиров С. С. Анализ эффективности декодирования циклических кодов Рида-Соломона с использованием двойственного базиса : дис. … канд. техн. наук 05.12.13 / Владимиров Сергей Сергеевич. СПб., 2013. 159 с.

References

1. Kognovitsky, O. S. Basics of Cyclic Codes. L.: LEIC, 1972. (in Russian).

2. Kognovitsky, O. S. Dual Basis and its Application in Telecommunications. SPb.: Link, 2009. (in Russian).

3. Vladimirov, S. S. Investigation of the Algorithm of Majority-Logic Decoding of a Reed-Solomon Code on the Dual Basis // Vestnik of Volga State University of Technology. Series: Radio Engineering and Infocommunication Systems. 2012. No. 1 (15). pp. 60–66. (in Russian).

4. Kukunin, D. S. Analysis of the Efficiency of Decoding Cyclic Codes Using a Dual Basis. Ph.D Thesis in Engineering Science. SPb.: SPbSUT, 2009. 197 p. (in Russian).

5. Vladimirov, S. A. Analysis of the Decoding Efficiency of Reed-Solomon Cyclic Codes Using a Dual Basis. Ph.D Thesis in Engineering Science. SPb.: SPbSUT, 2013. 159 p. (in Russian).

Кукунин Дмитрий Сергеевич – кандидат технических наук, доцент, СПбГУТ, Санкт-Петербург, 193232, Российская Федерация, coux@yandex.ru

Kukunin Dmitry – Candidate of Engineering Sciences, Associate Professor, SUT, St. Petersburg, 193232, Russian Federation, coux@yandex.ru