УДК 621.394.147.3: 621.391

О СВОЙСТВЕ СИММЕТРИЧНОСТИ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГАЛУА

А.А. Борисенко, *д-р техн. наук, профессор;*
Л.Б. Петришин*, *д-р техн. наук, профессор*
Сумский государственный университет, г. Сумы;
**Технический университет* «AGH», *г. Краков*

В материалах статьи произведен анализ свойств многомерной симметричности кодовых упорядочений Галуа, определен их класс как матриц Ганкеля и Теплица, на базе чего предложен метод помехоустойчивого приема и быстрой обработки сообщений в распределенных инфосистемах.

У матеріалах статті проведений аналіз властивостей багатомірної симетричності кодових упорядкувань Галуа, визначений їх клас як Ганкеля і Тепліца, на основі чого був заданий метод завадостійкого прийому і швидкої обробки повідомлень в інфосистемах.

В условиях стремительного внедрения информационных технологий разработка и применение перспективных методов кодирования цифровых сообщений есть решающим фактором повышения эффективности и помехозащищенности преобразования формы и цифровой обработки информации, а также информационного обмена [1-3]. Результаты анализа свойств и специфики применения кодов и кодовых систем позволили определить перспективным направление внедрения методов циклического кодирования [4-9] на базе кодовых систем Галуа [8-11], имеющих рекурсивное упорядочение кодовых элементов согласно выражению

$$a_{i+1} = \sum_{i=1}^{n-1} a_i q_i \bmod p,$$

где p - основание системы счисления; q_i - вектор обратных связей.

Следует обратить внимание, что кодовые последовательности Галуа с соответствующим упорядочением задаются вектором q_i, формируются как последовательности максимальной длины или, собственно, как последовательности Галуа поля $GF(2^n)$ с правым или левым сдвигом рекурсии кодовых элементов (рис. 1).

Ошибка!

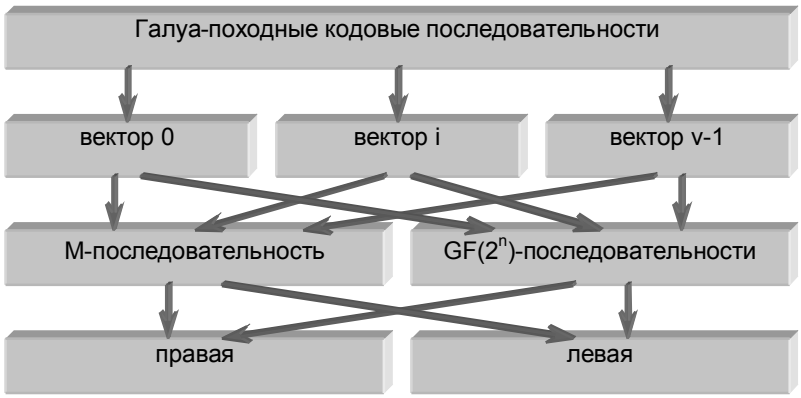

Рисунок 1 – Классификация Галуа-походных систем кодирования

Основой повышения помехозащищенности при кодировании на базе систем Галуа и информационном обмене есть не многоразовое повторение или выборочное вкрапление проверочных элементов, а расширение n-разрядного сообщения $A_i = \{a_i, a_{i+1}, \ldots, a_{i+n-1}\}$ путем введения дополнительных l символов $\{a_{i+n}, \ldots, a_{i+n+l-1}\}$, которые определяются как контрольные и связаны с информационными символами $\{A_i\}$ рекурсивной функцией взаимозависимости (1). Диагональные упорядочения кодовых элементов образуют матрицы с диагональной симметрией, приведенные в таблицах 1 и 2, что позволяет рассматривать их как Теплицевые или Ганкелевы матрицы [12-16], обработка которых не требует выполнения процедуры транспонирования и позволяет значительно повысить быстродействие цифровой обработки сообщений, кодированных в системах Галуа.

Замечательным свойством кодовых систем Галуа есть пространственная многомерная симметрия кодовых элементов по одной из метрик - для зеркально отображенных векторов обратных связей. Как пример, в таблицах 1 и 2 даны векторы обратной связи соответственно 10011 и 11001, а также 1001**1** и 1100**1**. По второй из метрик даны векторы для правых и левых сдвигов рекурсии кодовых элементов, а также по третьей – симметрия инверсии (в таблицах 1 и 2 – 10011, 1001**1**, а также 11001, 1100**1**). Такая симметрия позволяет осуществлять цифровые манипуляции фактически над одним и тем самым полем кодовых элементов для различных зеркально отображенных векторов обратных связей, их инверсий, а также правых и левых сдвигов рекурсий, в результате чего упрощается алгоритм цифровой обработки и операционные ресурсы, привлекаемые к процессу обработки.

Основанием быстрых алгоритмов цифровой обработки сообщений есть алгоритмы дискретного преобразования Фурье (ДПФ), введенные не только над полем комплексных чисел, но и над произвольным алгебраическим полем при условии, что полином порядка n имеет ДПФ только тогда, когда в данном поле существует элемент порядка n. Для поля Галуа ДПФ существует, если n есть делителем числа $z=2^n-1$, где z - размерность поля $GF(2^n)$ [4-6]. В поле Галуа определено ДПФ Меттсона-Соломона (ДПМС) [17], служащее основанием для вычисления циклических сверток. Приведенный случай кратности порядка n и размерности поля z есть в большинстве случаев исключением, чем типовым для полей Галуа, что значительно усложняет прикладное применение метода ДПМС. Но для проведения эффективной цифровой обработки в поле Галуа перспективными оказываются алгоритмы вычисления полевой свертки, которые базируются на дискретных преобразованиях Ганкелевых и Теплицевых матриц [12-16], которые, как было указано выше, полным образом характеризуют векторные упорядочения в поле Галуа. В матрице Ганкеля элементы одинаковые по диагоналях, параллельных главной диагонали и зеркально симметричны относительно побочной диагонали

$$\Gamma = \begin{bmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 2 & 3 & 4 & \ldots & n & n+1 \\ 3 & 4 & 5 & \ldots & n+1 & n+2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ n-1 & n & n+1 & \ldots & 2n-3 & 2n-2 \\ n & n+1 & n+2 & \ldots & 2n-2 & 2n-1 \end{bmatrix}.$$

В матрицах Теплица одинаковые элементы размещены по диагоналям,

параллельным побочной

$$T=\begin{bmatrix} n & n-1 & \dots & 3 & 2 & 1 \\ n+1 & n & \dots & 4 & 3 & 2 \\ n+2 & n+1 & \dots & 5 & 4 & 3 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 2n-2 & 2n-3 & \dots & n+1 & n & n-1 \\ 2n-1 & 2n-2 & \dots & n+2 & n+1 & n \end{bmatrix}.$$

Процедура транспонирования не изменяет характер матрицы, что значительно упрощает процесс цифровой обработки. Если ДПМС порядка n существует только в поле Галуа с кратными n и 2^n-1, то дискретное преобразование Ганкеля-Теплица (ДПГТ) задано в произвольном поле Галуа, а ядро $n \times n$ этого преобразования есть примитивным элементом поля $GF(2^n)$. Поскольку в поле Галуа $GF(2^n)$ определены модульные операции согласно порядка n, то преобразование ДПГТ будет осуществляться на основе циркулянтных матриц $\Gamma_ц$ и $T_ц$:

$$\Gamma_ц=\begin{bmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 2 & 3 & 4 & \dots & n & 1 \\ 3 & 4 & 5 & \dots & 1 & 2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ n-1 & n & 1 & \dots & n-3 & n-2 \\ n & 1 & 2 & \dots & n-2 & n-1 \end{bmatrix},$$

$$T_ц=\begin{bmatrix} n & n-1 & \dots & 3 & 2 & 1 \\ 1 & n & \dots & 4 & 3 & 2 \\ 2 & 1 & \dots & 5 & 4 & 3 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ n-2 & n-3 & \dots & 1 & n & n-1 \\ n-1 & n-2 & \dots & 2 & 1 & n \end{bmatrix}.$$

Всякая порождающая матрица кодовых упорядочений Галуа есть Ганкелевым или Теплицевым циркулянтом, в котором каждая соседняя линейка есть результатом рекурсивного сдвига элементов других соседних линеек. Порождающая матрица-циркулянт размерности $N \times (N+n)$ в полной векторной развертке представляется в следующем виде:

$$G=\begin{bmatrix} g_0 & g_1 & \dots & g_{N-1} & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{N-1} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & g_0 & g_1 & \dots & g_{N-1} \end{bmatrix}.$$

Такая форма представления сообщений в информационных системах позволяет осуществить помехоустойчивый прием и быструю обработку сообщений, при этом с целью аналитической проверки векторов принимаемых сообщений строится проверочная матрица H, ортогональная порождающей G, для которых

$$G\,H^t = 0; \qquad H\,G^t = 0.$$

Таблица 1 – Последовательности максимальной длины $M=2^4-1$

N	Вектор 10011				Вектор 11001			
	неинвертированная 10011		инвертированная 10011		неинвертированная 11001		инвертированная 11001	
	правая	левая	правая	левая	правая	левая	правая	левая
0	111101011001000	111101011001000	000010100110111	000010100110111	111100010011010	111100010011010	000011101100101	000011101100101
1	111010110010001	011110101100100	000101001101110	100001010011011	111000100110101	011110001001101	000111011001010	100001110110010
2	110101100100011	001111010110010	001010011011100	110000101001101	110001001101011	101111000100110	001110110010100	010000111011001
3	101011001000111	000111101011001	010100110111000	111000010100110	100010011010111	010111100010011	011101100101000	101000011101100
4	010110010001111	100011110101100	101001101110000	011100001010011	000100110101111	101011110001001	111011001010000	010100001110110
5	101100100011110	010001111010110	010011011100001	101110000101001	001001101011110	110101111000100	110110010100001	001010000111011
6	011001000111101	001000111101011	100110111000010	110111000010100	010011010111100	011010111100010	101100101000011	100101000011101
7	110010001111010	100100011110101	001101110000101	011011100001010	100110101111000	001101011110001	011001010000111	110010100001110
8	100100011110101	110010001111010	011011100001010	001101110000101	001101011110001	100110101111000	110010100001110	011001010000111
9	001000111101011	011001000111101	110111000010100	100110111000010	011010111100010	010011010111100	100101000011101	101100101000011
A	010001111010110	101100100011110	101110000101001	010011011100001	110101111000100	001001101011110	001010000111011	110110010100001
B	100011110101100	010110010001111	011100001010011	101001101110000	101011110001001	000100110101111	010100001110110	111011001010000
C	000111101011001	101011001000111	111000010100110	010100110111000	010111100010011	100010011010111	101000011101100	011101100101000
D	001111010110010	110101100100011	110000101001101	001010011011100	101111000100110	110001001101011	010000111011001	001110110010100
E	011110101100100	111010110010001	100001010011011	000101001101110	011110001001101	111000100110101	100001110110010	000111011001010
0	111101011001000	111101011001000	000010100110111	000010100110111	111100010011010	111100010011010	000011101100101	000011101100101

Таблица 2 – Рекурсивные последовательности поля Галуа $GF(2^4)$

N	Вектор 10011				Вектор 11001			
	неинвертированная 10011		инвертированная 10011		неинвертированная 11001		инвертированная 11001	
	правая	левая	правая	левая	правая	левая	правая	левая
0	1111010110010000	1111010110010000	0000101001101111	0000101001101111	1111000010011010	1111000010011010	0000111101100101	0000111101100101
1	1110101100100001	0111101011001000	0001010011011110	1000010100110111	1110000100110101	0111100001001101	0001111011001010	1000011110110010
2	1101011001000011	0011110101100100	0010100110111100	1100001010011011	1100001001101011	1011110000100110	0011110110010100	0100001111011001
3	1010110010000111	0001111010110010	0101001101111000	1110000101001101	1000010011010111	0101111000010011	0111101100101000	1010000111101100
4	0101100100001111	0000111101011001	1010011011110000	1111000010100110	0000100110101111	1010111100001001	1111011001010000	0101000011110110
5	1011001000011110	1000011110101100	0100110111100001	0111100001010011	0001001101011110	1101011110000100	1110110010100001	0010100001111011
6	0110010000111101	0100001111010110	1001101111000010	1011110000101001	0010011010111100	0110101111000010	1101100101000011	1001010000111101
7	1100100001111010	0010000111101011	0011011110000101	1101111000010100	0100110101111000	0011010111100001	1011001010000111	1100101000011110
8	1001000011110101	1001000011110101	0110111100001010	0110111100001010	1001101011110000	1001101011110000	0110010100001111	0110010100001111
9	0010000111101011	1100100001111010	1101111000010100	0011011110000101	0011010111100001	0100110101111000	1100101000011110	1011001010000111
A	0100001111010110	0110010000111101	1011110000101001	1001101111000010	0110101111000010	0010011010111100	1001010000111101	1101100101000011
B	1000011110101100	1011001000011110	0111100001010011	0100110111100001	1101011110000100	0001001101011110	0010100001111011	1110110010100001
C	0000111101011001	0101100100001111	1111000010100110	1010011011110000	1010111100001001	0000100110101111	0101000011110110	1111011001010000
D	0001111010110010	1010110010000111	1110000101001101	0101001101111000	0101111000010011	1000010011010111	1010000111101100	0111101100101000
E	0011110101100100	1101011001000011	1100001010011011	0010100110111100	1011110000100110	1100001001101011	0100001111011001	0011110110010100
F	0111101011001000	1110101100100001	1000010100110111	0001010011011110	0111100001001101	1110000100110101	1000011110110010	0001111011001010
0	1111010110010000	1111010110010000	0000101001101111	0000101001101111	1111000010011010	1111000010011010	0000111101100101	0000111101100101

Пускай Q - входной вектор информационных сообщений. Перемножая первое выражение на вектор Q:

$$Q\ G\ H^t = 0$$

или другое на вектор Q^t:

$$Q^t\ G^t\ H = 0,$$

получаем матричные зависимости определения ошибок в векторе сообщения. Контрольная матрица H имеет вид

$$H = \begin{bmatrix} 0 & \dots & 0 & 0 & h_0 & h_1 & \dots & h_{N-1} \\ 0 & \dots & 0 & h_0 & h_1 & \dots & h_{N-1} & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ h_0 & h_1 & \dots & h_{N-1} & 0 & 0 & \dots & 0 \end{bmatrix}.$$

Для определения ошибок достаточной есть проверка на равность нулю $Q\ G\ H^t = 0$.

Определим кодовые слова D из множества информационных векторов как

$$D = Q\ G.$$

При наличии ошибок в кодовом слове D' контрольная процедура не равна нулю: $D'H^t \neq 0$. Пускай результат произведения равен $D'H^t = P$, а причинивший его вектор ошибок – $p = p_{n-1}, p_{n-2}, \dots, p_1, p_0$, в котором количество ошибок не должно превышать половины кодового расстояния [5, 6]. Вектор P есть синдромом матрицы преобразования и характеризует вектор ошибок p, - локатор, который определяет место ошибки и ее вес

$$D'H^t = (D+p)H^t = DH^t + pH^t = pH^t = P.$$

Если синдром P представить в виде

$$P(z) = P_{n-1}\ z^{n-1} + \dots + P_2\ z^2 + P_1\ z + P_0,$$

то полином $l(z)$ имеет корни, противоположные локатору ошибок, а полином $m(z)$ будет характеризовать вес ошибок. Процедура декодирования заключается в определении соотношения

$$P(z)\ l(z) = m(z)\ mod\ z^n.$$

В случае обработки бинарных сообщений процедура упрощается вследствие ненужности вычисления веса ошибки, поскольку по определенному вектору локатора ошибок производится непосредственная коррекция бинарных кодовых знаков в полиноме сообщения на противоположные.

ДПГТ позволяет производить преобразования непосредственно в поле Галуа без традиционных методов логарифмирования и строить обычные и быстрые средства цифровой обработки.

Таким образом, раскрыты свойства многомерной симметрии рекурсивных кодовых последовательностей Галуа и их подкласса – последовательностей максимальной длины. Их применение в системах информационного обмена, преобразования формы и цифровой обработки

информации позволяет не выполнять операций транспонирования, произвести обработку фактически в едином трансформированном поле $GF(2^n)$, осуществляя только его зеркальные отображения или инверсию. При этом сохраняется логика теоретико-числовых преобразований, в результате чего повышается эффективность и защищенность от ошибок информационных систем.

SUMMARY

ON PROPERTY OF SYMMETRY OF GALUA'S CODE SEQUENCES

A.A. Borysenko, L.B. Petrishin*
Sumy State University
**Krakov Technikal University*

In the paper the analysis of the properties of multivariate symmetry of Galua's code rankings is carried out. Their class is determined as Genkle's and Toeplitz' matrices, on the basis of which the method of antinoise receive and fast data processing in distributed information systems is offered.

СПИСОК ЛИТЕРАТУРЫ

1. Касами Т. и др. Теория кодирования: Пер. с япон. - М.: Мир, 1987. - 576 с.
2. Берлекэмп Э. Алгебраическая теория кодирования: Пер. с англ. - М.: Мир, 1971. - 478 с.
3. Вивальнюк Л.М., Григоренко В.К., Левіщенко С.С. Числові системи. - К.: Вища шк., 1988. - 272 с.
4. Вариченко Л.В., Лабунец В.Г., Раков М.А. Абстрактные алгебраические системы и цифровая обработка сигналов. - Киев: Наук. думка, 1986. - 248 с.
5. Кларк Дж., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи: Пер. с англ. - М.: Радио и связь, 1987. - 392 с.
6. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки: Пер. с англ. - М.: Мир, 1976. - 594 с.
7. Хармут Х.Ф. Передача информации ортогональными функциями: Пер. с англ. - М.: Связь, 1975. - 272 с.
8. Петришин Л.Б. Теоретичні основи перетворення форми та цифрової обробки інформації в базисі Галуа. -Київ: ІЗіМН МОУ, 1997. - 237 с.
9. Петришин Л.Б. Теоретико-числові основи кодових систем Галуа /Івано-Франк. держ. техн. ун-т нафти і газу. -Івано-Франківськ, 1995. - 101 с. Моногр. деп. в ДНТБ України 20.12.95 № 57 - Ук 96.
10. Постников М.М. Теория Галуа. - М.: Физматгиз, 1963. - 220 с.
11. Чеботарев Н.Г. Основы теории Галуа. - М.: ОНТИ, 1934. - 283 с.
12. Бабенко К.И. О теплицевых и ганкелевых матрицах // Успехи математических наук. - 1986. - Т. 41, Вып. 1 (247). - С. 171-177.
13. Воеводин В.В., Тартышников Е.Е. Вычисления с теплицевыми матрицами // Вычислительные процессы и системы / Под ред. Г.И. Марчука - М.: Наука, 1983. - Вып. 1 - С. 124-266.
14. Иохвидов И.С. Ганкелевы и теплицевы матрицы и формы. - М.: Наука, 1974. - 263 с.
15. Пустыльников Л.Д. Теплицевы и ганкелевы матрицы и их применение // Успехи метематических наук. - 1984. - Т. 39, Вып. 4(238). - С. 53-84.
16. Brent R.P., Gustavson F.G., Jun D.Y. Fast solution Toeplitz systems of equations and computation of page approximants // Journal of the algorithmus. - 1980. - N 1. - P. 259-295.
17. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки: Пер. с англ. - М.: Связь, 1979. - 744 с.

Поступила в редакцию 14 мая 2009 г.