УДК 621.391.14

М.И. Мазурков, канд. техн. наук, проф.,
В.С. Дмитренко, канд. техн. наук, ст. преп.,
С.Н. Кропачев, магистр,
Одес. нац. политехн. ун-т

КОМПОЗИЦИОННЫЕ ЦИКЛИЧЕСКИЕ ПО ЧАСТОТЕ СИСТЕМЫ ДИСКРЕТНЫХ ЧАСТОТНЫХ СИГНАЛОВ НАД ИЗОМОРФНЫМИ ПОЛЯМИ ГАЛУА

М.І. Мазурков, В.С . Дмитренко, С.М . Кропачов. **Циклічні за частотою композиційні системи дискретних частотних сигналів над ізоморфними полями Галуа.** Запропоновано регулярне правило побудови повних класів композиційних систем дискретних частотних сигналів (КДЧ-сигналів) над розширеними полями Галуа. Проведено моделювання та дослідження кореляційних властивостей запропонованого повного класу систем КДЧ-сигналів і встановлена їхня практична привабливість.

M.I. Mazurkov, V.S. Dmitrenko, S.N. Kropachev. **Frequency-cyclic discrete frequency signals composition systems applied over isomorphic Galois fields.** A regular rule of forming full classes of discrete frequency signals composition systems over augmented Galois fields is proposed. Simulation and research of correlation properties of the given full class of composition discrete frequency signals systems are conducted and their practical attraction is established.

Регулярные правила построения композиционных систем дискретных частотных сигналов (КДЧ-сигналов) со свойством не более трех совпадений ($\lambda \le 3$) над простыми полями Галуа $GF(p)$ [1, 2] имеют ограничения на ассортимент (набор) допустимых длин N ДЧ-сигналов: $N = p-1$, либо $N = p$, где p — произвольное, но простое число. Вместе с тем ясно, что расширенные поля Галуа, например, $GF(p^k)$, и все их автоморфные и изоморфные представления имеют существенно больший ассортимент порядков и, следовательно, набор допустимых длин N сигналов. Однако вопросы построения полных классов систем КДЧ-сигналов над расширенными (изоморфными) полями Галуа исследованы недостаточно полно.

Представляется целесообразным разработка регулярного правила построения циклических по частоте систем КДЧ-сигналов над изоморфными полями Галуа, исследование их структурных и корреляционных свойств.

Для построения (упорядочения) элементов поля $GF(q)$, где $q = p^k$ — порядок основного поля, p — характеристика простого подполя $GF(p)$, необходимо задать первообразный полином $f(x)$ степени $\deg f(x) = k$, неприводимый над подполем $GF(p)$ [3,4]. Методика построения (упорядочения) элементов поля $GF(q)$, представленных в десятичной форме, известна [5]. Пример построения (упорядочения) элементов поля $GF(8) = GF(2^3)$, для случая, когда первообразный полином $f(x) = x^3 + x + 1$ (неприводимый над простым подполем $GF(2)$), при этом первообразный корень поля , приведен (табл. 1). Из анализа данных видно, что каждый элемент основного поля $GF(q)$ может быть представлен в нескольких различных формах: в виде степеней первообразного корня θ^i; в виде полиномов (вычетов) $R_i(x)$; в виде p-ичных векторов $\mathbf{B_i} = [\beta_{i,2}, \beta_{i,1}, \beta_{i,0}]$ и, наконец, в виде натуральных десятичных чисел N_i — нумераторов элементов поля, определяемых правилом

$$N_i = \sum_{\varepsilon=0}^{k-1} p^{\varepsilon} \beta_{i,\varepsilon}, \; i = \overline{0, p^k - 2}. \qquad (1)$$

Таблица1

Формы представления элементов расширенного поля $GF(2^3)$

Форма представления							
1	2	3	4	1	2	3	4
θ^i	$R_i(x)$	B_i	N_i	θ^i	$R_i(x)$	B_i	N_i
θ^0	1	001	1	θ^4	$x^2 + x$	110	6
θ^1	x	010	2	θ^5	$x^2 + x + 1$	111	7
θ^2	x^2	100	4	θ^6	$x^2 + 1$	101	5
θ^3	$x + 1$	011	3	θ^7	1	период	

На основании приведенных данных составленны арифметические таблицы сложения — A и умножения — M элементов поля $GF(2^3)$ с десятичным их представлением:

$A =$

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

$M =$

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	3	1	7	5
3	0	3	6	5	7	4	1	2
4	0	4	3	7	6	2	5	1
5	0	5	1	4	2	7	3	6
6	0	6	7	1	5	3	2	4
7	0	7	5	2	1	6	4	3

.

Все арифметические операции над элементами расширенного поля в десятичной форме. Например, элементами N_i в колонке 4, выполняются по двойному модулю — $\mathrm{modd}[f(x), p]$, или, что то же, в соответствии с арифметическими таблицами сложения A и умножения M элементов каждого алгебраического поля.

Определение. Композиционным циклическим по частоте $S(q)$-кодом над расширенным полем Галуа $GF(q)$, $q = p^k$, будет пользоваться множество кодовых слов, каждое из которых определяется правилом

$$S_k^{r,\nu} = (ki^r + \nu)\mathrm{modd}[f(x),p],\ i = \overline{0,q-1}, \tag{2}$$

для всех $k = \overline{1,q-1}$, $\nu = \overline{0,q-1}$, для каждого значения показателя степенных вычетов $r = \overline{1,q-1}$ и фиксированного полинома $f(x)$.

Из определения (2) следует, что мощность (объем) произвольного композиционного $S(q)$-кода над полем $GF(q)$, $q = p^k$,

$$J = q(q-1). \tag{3}$$

Каждое кодовое слово $S(q)$-кода рассматривается как частотно-кодирующую последовательность (ЧКП) для построения системы КДЧ-сигналов первого порядка [1, 2]. В этом случае показатель степенных вычетов r необходимо выбирать из условия, что наибольший общий делитель $(r, q-1) = 1$, при этом число различных частотных скачков, необходимых для формирования каждого ДЧ-сигнала, $F = q$.

Для исследования и оптимизации корреляционных свойств $S(q)$-кодов, или, что то же, различных систем КДЧ-сигналов, в рамках изоморфных полей каждого заданного порядка,

обозначим максимальный лепесток апериодической взаимокорреляционной функции (АВКФ) между всеми парами кодовых слов $S(q)$-кода, с заданным первообразным полиномом $f(x)$, через λ_{max}. Параметр λ_{max} определяет собой фактически максимальное число совпадений частотных скачков между каждой парой ДЧ-сигналов из соответствующей системы КДЧ-сигналов, сдвинутых между собой на некоторый соответствующий временной интервал τ. Неформально изоморфизм означает, что любые два поля с одинаковым числом элементов являются различными представлениями одного и того же поля. Однако, с точки зрения корреляционных свойств систем КДЧ-сигналов, выбор различных сочетаний пар алгебраических конструкций $[f(x),\theta]$ существенно влияет на порядок следования элементов в кодовых словах и, следовательно, на величину параметра λ_{max} системы КДЧ-сигналов. Таким образом, задача оптимизации корреляционных свойств систем КДЧ-сигналов в рамках изоморфных полей сводится к нахождению таких алгебраических конструкций $[f(x),\theta,r]$, для которых этот параметр имеет минимальное значение — $\lambda_{min\,max}$.

В качестве примера построен по правилу (2) $S(8)$-код над полем $GF(2^3)$ (см. таблицу 1) для значения показателя степенного вычета $r = q - 2 = 6$ (табл. 2).

Таблица 2

Полное множество кодовых слов $S(8)$-кода

№ п/п	Кодовые слова $S(8)$-кода								№ п/п	Кодовые слова $S(8)$-кода							
1	0	1	5	6	7	2	3	4	29	4	0	6	1	5	7	3	2
2	1	0	4	7	6	3	2	5	30	5	1	7	0	4	6	2	3
3	2	3	7	4	5	0	1	6	31	6	2	4	3	7	5	1	0
4	3	2	6	5	4	1	0	7	32	7	3	5	2	6	4	0	1
5	4	5	1	2	3	6	7	0	33	0	5	7	3	6	1	4	2
6	5	4	0	3	2	7	6	1	34	1	4	6	2	7	0	5	3
7	6	7	3	0	1	4	5	2	35	2	7	5	1	4	3	6	0
8	7	6	2	1	0	5	4	3	36	3	6	4	0	5	2	7	1
9	0	2	1	7	5	4	6	3	37	4	1	3	7	2	5	0	6
10	1	3	0	6	4	5	7	2	38	5	0	2	6	3	4	1	7
11	2	0	3	5	7	6	4	1	39	6	3	1	5	0	7	2	4
12	3	1	2	4	6	7	5	0	40	7	2	0	4	1	6	3	5
13	4	6	5	3	1	0	2	7	41	0	6	3	2	4	7	1	5
14	5	7	4	2	0	1	3	6	42	1	7	2	3	5	6	0	4
15	6	4	7	1	3	2	0	5	43	2	4	1	0	6	5	3	7
16	7	5	6	0	2	3	1	4	44	3	5	0	1	7	4	2	6
17	0	3	4	1	2	6	5	7	45	4	2	7	6	0	3	5	1
18	1	2	5	0	3	7	4	6	46	5	3	6	7	1	2	4	0
19	2	1	6	3	0	4	7	5	47	6	0	5	4	2	1	7	3
20	3	0	7	2	1	5	6	4	48	7	1	4	5	3	0	6	2
21	4	7	0	5	6	2	1	3	49	0	7	6	4	3	5	2	1
22	5	6	1	4	7	3	0	2	50	1	6	7	5	2	4	3	0
23	6	5	2	7	4	0	3	1	51	2	5	4	6	1	7	0	3
24	7	4	3	6	5	1	2	0	52	3	4	5	7	0	6	1	2
25	0	4	2	5	1	3	7	6	53	4	3	2	0	7	1	6	5
26	1	5	3	4	0	2	6	7	54	5	2	3	1	6	0	7	4
27	2	6	0	7	3	1	5	4	55	6	1	0	2	5	3	4	7
28	3	7	1	6	2	0	4	5	56	7	0	1	3	4	2	5	6

Исследования показали, что система КДЧ-сигналов на основе $S(8)$-кода мощности $J = 56$ с характеристиками поля $[f(x) = x^3 + x + 1; \theta = x; r = 6]$ имеет минимаксное значение параметра взаимной корреляции $\lambda_{\min\max} = 4$. Если найдена хотя бы одна минимаксная система КДЧ-сигналов, то на ее основе можно построить полный класс различных между собой минимаксных систем КДЧ-сигналов. Для этого достаточно однозначно перекодировать элементы всех кодовых слов исходного $S(q)$-кода по одному и тому же правилу преобразования (подстановки) q-й степени

$$\begin{pmatrix} 0 & 1 & 2 & \cdots & m & \cdots & q-1 \\ 0 & i_1 & i_2 & \cdots & i_m & \cdots & i_{q-1} \end{pmatrix}, \tag{4}$$

где i_m — это образ элемента m при данной подстановке.

Всего таких подстановок (4) может быть

$$W = (q-1)! \tag{5}$$

По правилу (2) были построены и исследованы корреляционные свойства ряда композиционных систем ДЧ-сигналов с различными характеристиками расширенных полей Галуа. Результаты исследований приведены (табл. 3).

Таблица 3

Сводная таблица параметров минимаксных систем КДЧ-сигналов различных длин N

Параметры					Виды полиномов	Параметр r
p	k	$N = q$	$J = q(q-1)$	$\lambda_{\min\max}$		
1	2	3	4	5	6	7
2	2	4	12	2	$f(x) = x^2 + x + 1$	(1,2)
2	3	8	56	4	$f(x) = x^3 + x + 1$ $f(x) = x^3 + x^2 + 1$	(1,2,3,4,5,6) (1,2,3,4,5,6)
2	4	16	240	5	$f(x) = x^4 + x + 1$ $f(x) = x^4 + x^3 + 1$	(7,11,13,14) (7,11,13,14)
2	5	32	992	5	$f(x) = x^5 + x^2 + 1$ $f(x) = x^5 + x^3 + 1$	(7,14,15,19,23,25,27,28,29,30) (11,13,21,22,26)
2	6	64	4032	6	$f(x) = x^6 + x^5 + 1$	(5,10,17,20,34,40)
3	2	9	72	3	$f(x) = x^2 + x + 2$	(5,7)
3	3	27	702	5	$f(x) = x^3 + 2x + 1$ $f(x) = x^3 + x^2 + 2x + 1$	(17,23,25) (5,15,17,19,23,25)
3	4	81	6480	7	$f(x) = x^4 + x + 2$ $f(x) = x^4 + 2x + 2$ $f(x) = x^4 + x^3 + 2$ $f(x) = x^4 + x^3 + x^2 + 2x + 2$ $f(x) = x^4 + 2x^3 + 2$ $f(x) = x^4 + 2x^3 + 2x^2 + x + 2$	(7,13,17,21,29,31, 37,39,51,59,63,73) (11,13,17,19,31,33,37,39, 51,53,57,59,71,73,77,79) (7,11,13,17,19,21,29,31, 33,37,39,51,57,59,63,73) (13,31,37,39,53,71,77,79) (11,13,17,19,23,31,33,37,39,47, 51,53,57,59,61,69,71,73,77,79) (53,71,77,79)
5	2	25	600	4	$f(x) = x^2 + 4x + 2$	(19,23)

5	3	125	15500	6	$f(x) = x^3 + 4x^3 + 3$	(99,119,123)

Из анализа данных следует, что параметр $\lambda_{\min\max}$ зависит от характеристики простого поля p и степени расширения k, а также от вида первообразного полинома $f(x)$, неприводимого над полем $GF(p)$. Приведены оптимальные первообразные полиномы, т.е. полиномы, обеспечивающие минимальное значение параметра $\lambda_{\min\max}$. Приведены множества оптимальных значений вычетов r, для заданного первообразного полинома $f(x)$, таких, что наибольший общий делитель $(r, q-1) = 1$.

По результатам проведенных исследований можно сделать основные выводы:

— системы КДЧ-сигналов, построенные над расширенными полями Галуа $GF(q)$, $q = p^k$ позволяют существенно расширить набор допустимых длин $N = q$ ДЧ-сигналов;

— с ростом характеристики поля q максимальный относительный лепесток АВКФ между всеми парами ДЧ-сигналов из системы КДЧ-сигналов стремится к нулю, т.е. $\rho = \lambda_{\min\max} / q \to 0$, что свидетельствует об асимптотической оптимальности корреляционных свойств рассмотренных систем КДЧ-сигналов с ростом их длины $N = q$;

— предложенные полные классы минимаксных систем КДЧ-сигналов могут служить основой для построения больших систем ДЧ-сигналов с хорошими корреляционными свойствами, объем которых $J \square B$, где B — база каждого ДЧ-сигнала.

Литература

1. Варакин Л.Е. Системы связи с шумоподобными сигналами.— М.: Радио и связь, 1985. — 384 с.
2. Варакин Л.Е. Теория систем сигналов. — М.: Сов. радио, 1978. — 304 с.
3. Мазурков М.И. Конструктивный способ построения первообразных полиномов над простыми полями Галуа // Радиоэлектроника, 1999. — № 2. — С. 41 — 45. (Изв. вузов).
4. Мазурков М.И. Семейства линейных рекуррентных последовательностей на основе полных множеств изоморфных полей Галуа / Мазурков М.И., Конопака Е.А // Радиоэлектроника. — 2005. — № 11. — С. 58 — 65. (Изв. вузов).
5. Мазурков М.І. Основи теорії передавання інформації: Навч. посіб. для вищ. навч. закладів / Одес.нац.політехн.ун-т. — Одеса:Наука і техніка, 2005. — 168с.

Поступила в редакцию 2007 г.