УДК 621.391

А.А. ЗАМУЛА, канд. техн. наук

МЕТОД ПОСТРОЕНИЯ МНОГОФАЗНЫХ ХАРАКТЕРИСТИЧЕСКИХ ДИСКРЕТНЫХ СИГНАЛОВ

Введение

Исследования показывают, что обеспечение требуемых показателей помехоустойчивости, скрытности функционирования системы передачи информации (СПИ), оперативности ввода СПИ в синхронизм может быть достигнуто на основе использования принципов широкополосной связи. При этом указанные показатели могут быть улучшены за счет реализации в СПИ динамического режима функционирования [1] в сочетании с применением классов сигналов, удовлетворяющих определенным требованиям, с точки зрения функций корреляции, ансамблевых, структурных и других свойств.

В [2] приведен метод формирования двоичных характеристических дискретных сигналов в простом поле Галуа GF(p). Более предпочтительными, с точки зрения свойств и приложений, являются многопозиционные характеристические дискретные сигналы. Проведенный анализ показал, что к настоящему времени отсутствует эффективный алгоритм построения многопозиционных сигналов, не изучены в полной мере их свойства и практические приложения в системах связи.

В статье сформулирована и доказана теорема, с использованием которой предлагается метод построения многопозиционных характеристических дискретных сигналов в расширенном поле Галуа GF(p^n), обладающий по сравнению с известным методом [2], существенно меньшей вычислительной сложностью.

Основные результаты исследований

Метод синтеза (формирования) базового изоморфизма многопозиционного характеристического дискретного сигнала (МХДС), обладающий по сравнению с известным алгоритмом [1] меньшей вычислительной сложностью, задается теоремой 1. При этом под базовым изоморфизмом понимается изоморфизм МХДС, построенный при использовании минимального первообразного элемента $\theta_v(x)$ поля Галуа GF(p^n), где n – степень расширения поля.

Теорема 1. Пусть $v_i = \overline{0, p^n - 2}$ есть множество индексов элементов поля GF(p^n), упорядоченных в порядке возрастания, а k-значный характер элементов поля $a_1, a_2, ..., a_{p^{n-1}}$ фиксируется функцией с ограничениями на значность

$$\psi(a_i) = \exp\,(j\frac{2\pi}{k}v_i)\,, \tag{1}$$

причем

$$\begin{cases} p^n - 1 = 0 \bmod k, \\ 2 \le k \le p^n - 1 \end{cases}, \tag{2}$$

где p – простое число, n – степень расширения поля.

Тогда алгоритм построения МХДС может быть описан следующими шагами:

1. Формируется массив сдвинутых по значению индексов $v_i = i+1, i = \overline{0, p^n - 2}$, упорядоченный по возрастанию и массив элементов – чисел $a_j(i = 1, \overline{p^n - 1})$ расширенного поля GF(p^n):

$$a_i = МП\,(i) = \theta_v^i(x) mod\; d(f(x),p)\,, \tag{3}$$

где f(x) – неприводимый над полем многочлен.

2. Формируется массив MC(i) элементов поля GF(p^n), значения которого определяются правилом

$$\text{МС}(i) = \text{МП}(i) + 1 \text{ при } \theta_v^i(x) + 1 \equiv 0 \bmod d(f(x), p) \quad (4)$$

$$\text{МС}(i) = 1 \text{ при } \theta_v^i(x) \equiv 1 \bmod d(f(x), p), \quad (5)$$

где $i = \overline{0,\ p^n - 2}$.

3. Массив индексов V_i или массив $V_i - 1$ преобразуется (записывается) в массив МК(j) по адресу МП(i) так, что

$$\text{МК}(j) = MK(\text{МП}(i)) = MK(\theta_v^i \bmod d(f(x), p) = j - 1, \quad (6)$$

$$j = \overline{1,\ p^n - 1}.$$

4. Формируется массив индексов элементов поля $MU(i)$, $i = \overline{0, p^n - 2}$, значениями которого являются индексы $\mathbf{V_i}$, считанные из массива МК(j) по адресу МС(i), т. е.

$$MU(i) = MK[MC(I)]. \quad (7)$$

5. В соответствии с выражением для всех $p^n - 1$ элементов a_i, вычисляется k-значный характер поля

$$\psi(a_i) = \psi(\theta_v^i + 1) = -\psi[MU(i)] = -\psi\{MK[MC(i)]\} = 1, \text{ если } MU(i) \equiv 0 (\bmod k); \quad (8)$$

$$\exp j\frac{2\pi}{k}, \text{ если } MU(i) \equiv 1 (\bmod k); \quad (9)$$

$$\exp(j\frac{2\pi}{k}(k-1)),\ MU(i) \equiv k - 1 (\bmod k). \quad (10)$$

Для доказательства теоремы 1 покажем, что последовательность шагов, определенная в ней, эквивалентна шагам, представленным для метода в [1]. По существу покажем, что на шагах 1 – 4 обеспечивается решение L^2 сравнений вида $v_i = IND(\theta^i + 1)$.

Действительно, на шаге L обеспечивается формирование всех элементов $a_i = \theta_v^i(x) \equiv 1 \bmod d(f(x), p)$, и сдвинутых на единицу индексов $v_i' = i + 1\ (i = \overline{0, L-1}, L = p^n - 1)$ или индексов $v_i' = i$, упорядоченных по возрастанию. На этом шаге формируются номера элементов поля, расположенных в порядке возрастания.

В таком порядке они представляют собой натуральный ряд чисел, ограниченный числом $p^2 - 1$ или $p^2 - 2$.

Таким образом, на первом этапе алгоритм, определенный теоремой 1, и известный, приведенный в [2], совпадают.

На шаге 2 формируется массив элементов поля a, сдвинутый по значению на единицу, т.е.

$$a_i = (a_i' + 1) \bmod d(f(x), p) = (\theta_v^i + 1) \bmod d(f(x), p). \quad (11)$$

На шагах 1 и 2 формируются массив элементов поля $a_i' = \theta_v^i \bmod d(f(x), p)$ и массив $a_i = (\theta_v^i + 1) \bmod d(f(x), p)$, сдвинутый на единицу по значению, а также натуральный ряд чисел, представляющий собой сдвинутый на единицу, упорядоченный по возрастанию массив индексов. В целом первый и второй шаги алгоритма совпадают с шагами известного алгоритма. На шагах 3 и 4, в результате записи сдвинутых индексов $v_i' = i + 1, i = \overline{0, p^n - 2}$ по адресу МП(i), в массиве МК(i), оказываются записанными по отношению к соответствующим элементам поля $GF(p^n)$ сдвинутое на единицу в сторону возрастания числа индексом. При считывании из массива МК(i) чисел индексов с адресом МС(i) в массиве МИ(i) оказываются записанными индексы v_i', которые также на единицу сдвинуты относительно индексов v_i. Эти операции записи индексов v_i по адресу θ_v^i и считывание по адресам $\theta_v^i + 1$ по существу составляют способ решения $p^2 - 1$ сравнений вида

$$\theta_v^i + 1 = \theta_v^{vi} \bmod d(f(x), p). \quad (12)$$

Таким образом, метод построения многопозиционных характеристических дискретных сигналов для случая *k*-значного характера поля GF(p^n), определяемый теоремой 1, является по отношению к известному методу [1] более общим и совпадает с ним для частного случая, а именно – для случая простого поля и двоичного характера поля.

Рассмотрим примеры построения МХДС.

Пример 1. Пусть необходимо построить МХДС для простого поля Галуа с параметрами

$$\mathrm{n}=1,$$
$$\mathrm{p}=13, \theta=2, \mathrm{k}=2,$$
$$\mathrm{p}=13, \theta=2, \mathrm{k}=3,$$
$$\mathrm{p}=13, \theta=2, \mathrm{k}=4.$$

Запишем ряд сдвинутых индексов (номеров) $\mathrm{v}_\mathrm{i}'=\mathrm{i}+1=1,2,3,4,5,6,7,8,9,10,11,12,$ по адресам

$$\text{МП (i)}=\theta_\mathrm{v}^\mathrm{i}(\mathrm{x})\mathrm{mod}13=\{2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8,..., 2^{11}\}=$$
$$=\{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\};\ i=\overline{0,11}.$$

В результате сформируем массив сдвинутых индексов

$$\text{МК (j)}=\{1, 2, 5, 3, 10, 6, 12, 4, 9, 11, 8, 7\}.$$

Далее произведем считывание сдвинутых индексов из массива МК(j) по адресам $\text{МС(i)}=\theta_\mathrm{v}^\mathrm{i}+1\,\mathrm{mod}\,13=2,3,5,9,4,7,1,12,10,6,11,8$. В соответствии с (3) получим массив сдвинутых на единицу индексов

МИ (i) = {2,5,10,9,3,12,1,7,11,6,8,4}.

Используя выражение (5), получим элементы дискретных сигналов для К= 2:

$$D_{k=2}=\{0,1,0,1,1,0,1,1,1,0,0,0\};$$

для К = 3

$$D_{k=3}=\{2,2,l,0,0,0,1,1,2,0,2,l\};$$

для К = 4

$$D_{k=4}=\{2,1,2,l,3,0,1,3,3,2,0,0\}.$$

Пример 2. Рассмотрим пример построения МХДС для расширенного поля. Пусть OF(p^n) поле с параметрами p = 3, n = 2, f(x) = $x^2 - x - 1$**,** К = 2, К = 4. В этом случае L = 3^2 — $1=8$**.** Запишем ряд сдвинутых индексов U_i в массив МК(i)

$U_i'=U_i+1=1,2,3,4,5,6,7,8$ по адресам, определяемым коэффициентами при элементах-полиномах

$$\text{МП (i)}=\theta^\mathrm{i}\,\mathrm{mod}\,d(x^2-\mathrm{x}-1{,}3)=\{1, \theta, \theta+1, 2\theta+1, 2, 2\theta, 2\theta+2, \theta+2\},$$

учитывая, что Р=3, т. е. подставим вместо θ число Р. Ряд коэффициентов имеет вид $K_1'=\{1,2,4,7,2,6,8,5\}$. Далее сформируем массив МС(i)

$$\text{МС(i)}=\text{МП (i)}+1=\{2, \theta+1, \theta+2, 2\theta+2, \theta, 2\theta+1, 2\theta, \theta\},$$

и соответствующий массив коэффициентов

$$K_2'=\{2,4,5,8,0,7,6,3\}.$$

При этом массив коэффициентов формируется, например, для $2\theta+2$ по правилу

$$K_{2,4}'=2P+2\,\mathrm{mod}\,P^2=2\cdot3+2=8.$$

Считывая из массива МК(i) индексы по адресу K_2', получаем

МИ(i) = {5,3,0,7,1,4,6,2}.

Элементы дискретного сигнала

$$D_{k=2}=\{1,1,0,1,1,0,0,0\};$$

$$D_{k=4} = \{1,3,0,3,1,0,2,2\}.$$

Для получения МХДС в комплексном виде необходимо умножить D_k на $\exp j\frac{2\pi}{k}$, тогда получим:

W_2={-1,-1,1,-1,-1,1,1,1}-двоичный случай;

$$W_4 = \{\exp j\frac{\pi}{2}; \exp j\frac{3\pi}{2}; \exp j\frac{\pi}{2}0; \exp j\frac{\pi}{2}3; \exp j\frac{2x}{2}; 1; \exp j\frac{\pi}{2}2; \exp j\pi\} = \{j,-j,l,-j\ j,1,-1,-1\}$$

– четырехфазный случай.

Покажем, что МХДС обладают оптимальной периодической функцией автокорреляции, т. е. что данное семейство сигналов является плотно упакованным по автокорреляционной функции. Действительно,

$$R(m) = \begin{cases} L,\ \textit{если}\ m \equiv 0 \bmod L, \\ \sum\limits_{i=0}^{p^n-2} \psi(\theta_\nu^i + 1)\psi^*(\theta_\nu^{i+m} + 1) + \psi(-\theta^m + 1) + \psi^*(-\theta^m + 1),\ \textit{если}\ m \neq 0 \bmod L, \end{cases} \tag{13}$$

где символ * – означает комплексное сопряжение.

Выражение (7), как показано в [2], может быть заменено другим, ему эквивалентным, а именно

$$R(m) = -1 - \psi^*(\theta^m) + \psi(\theta^m - 1)[+\psi(\theta^m)]. \tag{14}$$

Так как функция ψ при любом аргументе принимает значения не больше 1, то для граничных значений можно принять, что $\psi(x)$ =-1 или $\psi(x) =$ 1. Тогда выражение (7) примет вид: $R(m) = -1 - 1 - 1[1+1]$.

Выводы

Таким образом, МХДС обладают периодической функцией автокорреляции, для которой $|R_{\max}(m)| \leq 4$ при $m \neq 0 \bmod L$. При этом, периодическая функция автокорреляции является К-уровневой. Предложенный метод построения многопозиционных характеристических дискретных сигналов в расширенном поле Галуа GF(p^n), обладает, по сравнению с известным методом [2], существенно меньшей вычислительной сложностью.

Список литературы: 1. *Помехозащищенность* радиосистем со сложными сигналами / Г. И. Тузова, В. А. Сивов и др. ; под ред. Г. И. Тузова. – М. : Радиосвязь, 1985. – 264 с. 2. *Горбенко И.Д., Замула А.А., Киянчук Р.И.* Методы построения и исследования свойств производных нелинейных рекуррентных последовательностей // Радиотехника: – 2011. – Вып. 166. – С. 125 – 133.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 12.11.2012