УДК 621. 391

СИНТЕЗ ОДНОГО КЛАССА ДИСКРЕТНЫХ СИГНАЛОВ В ПОЛЯХ ГАЛУА

А.А. ЗАМУЛА, Р.И. КИЯНЧУК, Т.Е. ЯРЫГИНА, Е.П. КОЛОВАНОВА

В статье предлагаются методы синтеза одного класса сложных сигналов, основанные на использовании свойств полей Галуа. Кроме того, приводится теорема, на основании которой устанавливаются связи характеров элементов мультипликативной группы поля Галуа и зависимость символов дискретных кодов, построенных на использовании характеров мультипликативной группы поля.

Ключевые слова: характеристические дискретные сигналы, характер мультипликативной группы, функция корреляции.

Системы передачи информации являются одним из основных видов радиотехнических систем и быстро развиваются во многих отношениях. К таким системам предъявляются все более жесткие требования по обеспечению их работы в условиях сложных внешних воздействий, а так же естественных и преднамеренных помех и помех от других радиотехнических систем, работающих на близких частотах или в общем участке диапазона частот. Важной характеристикой некоторых систем передачи информации является скрытность функционирования. Под скрытностью функционирования понимают способность системы функционировать в режиме, затрудняющим обнаружение передаваемых сообщений и оценку их параметров специальной разведывательной аппаратурой злоумышленника. Одним из видов скрытности является информационная скрытность. Такой вид скрытности предполагает целый комплекс мер, методов и средств для затруднения определения злоумышленником: самого факта передачи сообщений по каналам связи, содержания передаваемых сообщений и другое. Большое значение при решении задач обеспечения заданной информационной скрытности имеют исследования, связанные с использованием новых видов сигналов, получивших название: сложных, широкополосных, многомерных и шумоподобных. Разработка методов синтеза сложных сигналов с хорошими корреляционными, ансамблевыми, статистическими, структурными и другими свойствами является актуальной задачей.

В статье предлагаются методы синтеза одного класса сложных сигналов, основанные на использовании свойств полей Галуа. Кроме того, приводится теорема, на основании которой устанавливаются связи характеров элементов мультипликативной группы поля Галуа и зависимость символов дискретных кодов, построенных на использовании характеров мультипликативной группы поля.

В [1] рассмотрены так называемые характеристические дискретные сигналы (ХДС) с числом позиций (символов) $L = 4x + 2$ и $L = 4x$, синтез которых базируется на использовании характера ψ мультипликативной группы поля $GF(P)$.

Правило кодирования таких кодов для $L = 4x + 2$ имеет вид:

$$\mu = \{\mu_i : i = 0, 1, ..., P-2\}$$

$$\mu_i = \psi(\Theta^i + 1), \text{ если } \Theta^i + 1 \not\equiv 0 (\text{mod } P),$$

$$\mu_i = 1, \text{ если } \Theta^i + 1 \equiv 0 (\text{mod } P), \quad (1)$$

$$\mu_i = \psi(\Theta^i + 1), \text{ если } \Theta^i + 1 \not\equiv 0 (\text{mod } P),$$

$$\mu_i = -1, \text{ если } \Theta^i + 1 \equiv 0 (\text{mod } P), \quad (2)$$

где Θ — первообразный элемент поля $GF(P)$.

Для $L = 4x$ правило кодирования имеет вид:

$$\mu = \{\mu_i : i = 0, 1, ..., P-2\}$$

$$\mu_i = \psi(\Theta^i + 1), \text{ если } \Theta^i + 1 \not\equiv 0 (\text{mod } P),$$

$$\mu_i = 1, \text{ если } \Theta^i + 1 \equiv 0 (\text{mod } P), \quad (3)$$

$$\mu_i = \psi(\Theta^i + 1), \text{ если } \Theta^i + 1 \not\equiv 0 (\text{mod } P),$$

$$\mu_i = -1, \text{ если } \Theta^i + 1 \equiv 0 (\text{mod } P). \quad (4)$$

В [1] показано, что мощность метода данного класса сигналов (М) равна числу классов неинверсно-изоморфных коэффициентов, которые могут быть получены разложением мультипликативной группы на смежные классы по классу автоморфных коэффициентов, и определяется как $M = \phi(L)/2 \cdot$.

Известно так же [1], что правила кодирования (1) и (2) приводят к коду с двухуровневой периодической функцией автокорреляции $R_\mu = \{-2, 2\}$, а правила кодирования (3) и (4) — к $R_\mu = \{0, -4\}$ и $R_\mu = \{0, 4\}$ соответственно.

Максимальные по модулю значения боковых лепестков функции автокорреляции импульсного бинарного фазоманипулированного сигнала, построенного на базе кода μ:

$$r_\mu(m) = \sum_{i=0}^{L-m-1} \mu_i \, \mu_{i+m} \quad (5)$$

для правил (1) и (2) находятся в пределах $(0{,}47 \div 0{,}82)/\sqrt{L}$, для правила (3) — $(0{,}57 \div 0{,}82)/\sqrt{L}$, а для правила (4) в пределах — $(0{,}50 \div 0{,}82)/\sqrt{L}$.

Способ формирования ХДС длительностью L, приведеный в работе [1], сводится к составлению таблицы соответствия i-й элемент поля ($a_i = \theta_j^i + 1$ (θ_j^i — первообразный элемент поля)) —

i-й индекс. Для составления таблицы необходимо решить L сравнений вида:

$$a_i \equiv \Theta_j^{U_i} (\mathrm{mod}\ P), i = \overline{0, P-1}. \quad (6)$$

Здесь U_i – индекс элемента поля GF(P), определяемый из решения сравнения (6). Данный способ из-за отсутствия алгоритмизируемых процедур трудно реализуем. В работе [2] предложены способ и устройство формирования ХДС. Способ основан на рекуррентной зависимости между элементами и индексами элементов поля Галуа, при этом становится возможным алгоритмизировать процедуры формирования символов ХДС. Однако вычислительная сложность, (время формирования ХДС) остается значительной:

$$t_{\sum} = L(t_{\text{у}} + t_{\text{сл}} + 3t_{\text{з}} + (L-2)t_{\text{сч}} + (L+1)t_{\text{ср}}), \quad (7)$$

где $t_{\text{у}}$, $t_{\text{сл}}$, $t_{\text{з}}$, $t_{\text{сч}}$, $t_{\text{ср}}$ — время выполнения операций умножения, сложения, записи, считывания и сравнения соответственно. Анализ выражения (7) показывает, что основные временные затраты при построении ХДС связаны с квадратичными членами $L(L+2)t_{\text{сч}}$, $L(L+1)t_{\text{ср}}$.

Изложим подход к синтезу ХДС, обладающий значительно меньшей вычислительной сложностью по сравнению со способами, рассмотренными в [1, 2]. Синтез ХДС базируется на использовании наименьшего по значению первообразного элемента θ_j поля GF(P)) и задается теоремой 1.

Теорема 1. Пусть характер мультипликативной группы поля фиксируется функцией

$$\psi(a_i) = e^{j\pi U_i}, \quad (8)$$

тогда алгоритм построения характеристического сигнала описывается следующими шагами.

1. Формируется массив элементов-чисел $A_i, i = \overline{0, P-2}$ поля GF(P):

$$A(i) = \Theta_j^i (\mathrm{mod}\ P). \quad (9)$$

2. Формируется группа чисел поля GF(P), сдвинутая по значениям на единицу, в соответствии с правилом:

$$H(i) = A(i) + 1, \text{ если } \Theta_j^i + 1 \not\equiv 0 (\mathrm{mod}\ P);$$

$$H(i) = 1, \text{ если } \Theta_j^i + 1 \equiv 0 (\mathrm{mod}\ P). \quad (10)$$

3. Формируется массив индексов $X(i), i = \overline{0, P-2}$, значениями которого являются соответствующие элементу поля индексы i+1, упорядоченные по содержимому с адресом:

$$A(i)\colon X(i) = X[A(i)]. \quad (11)$$

4. Строится массив индексов $J(i)$, значениями которого являются индексы массива $X(i)$, выбранные по адресу $H(i) : J(i) = X[H(i)], i = \overline{0, P-2}$.

5. Вычисляется характер поля по правилу [1]:

$$\psi(a_i) = \psi[J(i)] = \begin{cases} 1, \text{если } J(i) \equiv 0 (\mathrm{mod}\ 2); \\ -1, \text{если } J(i) \equiv 0 (\mathrm{mod}\ 2); \end{cases} \quad (12)$$

Пример. Построим ХДС.

Пусть $P = 13, L = 12, \Theta_j = 2$, Тогда

$$A(i) = \Theta_j^i (\mathrm{mod}\ P) = \{1,2,4,8,3,6,12,11,9,5,10,7\};$$

$i = \{0,1,2,3,4,5,6,7,8,9,5,10,11\}$. Упорядочим ряд $i+1 = \{1,2,3,4,5,6,7,8,9,5,10,11,12\}$ по закону (адресу) $\Theta_j^i = A(i)$. В соответствии с (9) – (11) получим массив индексов $X(i)$={1,2,5,3,10,6,12,4,9,11, 8,7}. Произведем выборку элементов-чисел из поля $X(i)$ по адресу $H(i) = \Theta_j^i + 1 (\mathrm{mod}\ P)$ = {2,3,5,9, 4,7,1,12,10,6,11,8}.

В результате имеем поле чисел $J(i)$={2,5,10,9 ,3,12,1,7,11,6,8,4}. Вычисляя характер по правилу (12), получаем инверсию характеристического сигнала $W_{12} = \{1,-1,1,-1,-1,1,-1,-1,-1,1,1,1\}$. Инвертируя W_{12}, получаем базовый изоморфизм.

Доказательство теоремы 1. С выполнением шагов 1, 2 теоремы 1 обеспечивается формирование мультипликативной группы поля GF(P) $A(i) = \Theta_j^i + 1 (\mathrm{mod}\ P), i = \overline{0, P-2}$ и группы чисел $H(i)$, сдвинутой по отношению к $A(i)$ на единицу, т. е. $H(i) = \Theta_j^i + 1$. Рассмотрим шаги 3, 4 теоремы 1. В результате записи последовательность чисел i+1, сдвинутых на единицу индексов поля $A(i), i = \overline{0, P-2}$, по адресу Θ_j^i в массиве $X(i)$ оказываются записанными по сравнению с соответствующими элементами поля GF(P) сдвинутые по значению на единицу числа-индексы. При считывании с массива $X(i)$ в качестве индексов элементов-чисел с адресом $\Theta_j^i + 1$, индексы U_i, соответствующие элементам $A(i) = \Theta_j^i + 1$, также оказываются сдвинутыми на единицу [1; 3], т.е. считываются индексы со значением U_i+1. Для получения же индексов U_i их нужно сдвинуть по значению на единицу, выполняя, как и ранее, все операции по модулю простого числа P. Однако сдвиг не выполняют, т. к. характер поля $\psi(a_k) = e^{j\pi(U_i+1)} = e^{j\pi} \cdot e^{j\pi U_i} = (\cos\pi + j\sin\pi)e^{j\pi U_i} = -e^{j\pi U_i}$, т.е. сдвиг на единицу индексов приводит к инверсной форме изоморфизма ХДС. Изложенное подтверждает справедливость шага 5. Таким образом, теорема доказана.

Непосредственно из теоремы 1 следует, что время формирования ХДС определяется из выражения:

$$t_{\sum} = L(t_{\text{у}} + t_{\text{сл}} + t_{\text{ср}} + 7t_{\text{з}}). \quad (13)$$

В выражении (13) учтено, что $t_{\text{з}} = t_{\text{сч}}$. Анализ (13) показывает, что время формирования ХДС линейно (в отличии от (7)) зависит от операций, используемых при формировании сигналов.

Приведем теорему о свойствах поля Галуа, определяющих связи элементов a_i поля GF(P^n).

Теорема 2. Пусть $a_1, a_2, \ldots, a_{(P-1)/2}$ — элементы поля GF(P), тогда элементы поля $a_{(P-1)/2+1}, a_{(P-1)/2+2}, \ldots, a_{P-1}$ зависят от (P-1)/2 первых элементов и определяются из выражения:

$$a_{(P-1)/2+i} = P - a_i, \quad (14)$$

где $i = \overline{1, (P-1)/2}$.

Доказательство. Известно, что i-й элемент поля может быть представлен как

$$a_i = \Theta^{i-1} \bmod (P),$$

а $((P\text{-}1)/2+ i)$-й элемент имеет вид:

$$a_{(P-1)/2+i} = \Theta^{(P-1)/2+i-1}.$$

Тогда (14) можно записать следующим образом:

$$\Theta^{i-1} + \Theta^{(P-1)/2+i-1} = P \equiv 0 \,(\text{mod } P).$$

Вынеся за скобки Θ^{i-1}, получим:

$$\Theta^{i-1}(1 + \Theta^{(P-1)/2}) = P \equiv 0 \,(\text{mod } P). \qquad (15)$$

В соответствии с теоремой Ферма:

$$\Theta^{P-1} \equiv 1 \,(\text{mod } P);$$

$$(\Theta^{(P-1)/2} - 1)(\Theta^{(P-1)/2} + 1) \equiv 0 \,(\text{mod } P). \qquad (16)$$

В (16) только один из сомножителей левой части делится на P. В противном случае их разность, равная 2, должна делиться на P. Поэтому имеет место одно и только одно из сравнений

$$\Theta^{(P-1)/2} \equiv 1 \,(\text{mod } P), \qquad (17)$$

$$\Theta^{(P-1)/2} \equiv -1 \,(\text{mod } P). \qquad (18)$$

Сравнение (17) не может выполняться, так как в поле Галуа лишь $\Theta^{P-1} \equiv 1 \,(\text{mod } P)$ и $\Theta^0 \equiv 1 \,(\text{mod } P)$. Поэтому выполняется сравнение (18). В этом случае справедливо и (15). Тогда $((P\text{-}1)/2 + i)$-й элемент поля может быть найден из соотношения $a_{(P-1)/2+i} = P - a_i$. Теорема доказана.

Проиллюстрируем на примере возможность построения $((P\text{-}1)/2+i)$-х элементов поля по известным первым $(P\text{-}1)/2$ элементам.

Пусть характеристика поля GF(P) P = 13, первообразный элемент поля $\Theta = 2$.

Запишем элементы данного поля:

$$\begin{array}{l} a_1=2^0 \bmod 13=1;\ a_2=2^1 \bmod 13=2; \\ a_3=2^2 \bmod 13=4;\ a_4=2^3 \bmod 13=8; \\ a_5=2^4 \bmod 13=3;\ a_6=2^5 \bmod 13=6; \\ a_7=2^6 \bmod 13=12;\ a_8=2^7 \bmod 13=11; \\ a_9=2^8 \bmod 13=9;\ a_{10}=2^9 \bmod 13=5; \\ a_{11}=2^{10} \bmod 13=10; \\ a_{12}=2^{11} \bmod 13=7. \end{array} \qquad (19)$$

Воспользуемся выражением (14) для получения $((P\text{-}1)/2+ i)$-х.элементов поля ($i = \overline{1,(P-1)}$):

$$\begin{array}{l} a_7= a_{(P\text{-}1)/2+1}=P- a_1=12; \\ a_8= a_{(P\text{-}1)/2+2}=P- a_2=11; \\ a_9= a_{(P\text{-}1)/2+3}=P- a_3=9; \\ a_{10}= a_{(P\text{-}1)/2+4}=P- a_4=5; \\ a_{11}= a_{(P\text{-}1)/2+5}=P- a_5=10; \\ a_{12}= a_{(P\text{-}1)/2+6}=P- a_6=7. \end{array} \qquad (20)$$

Сравнение соответствующих элементов поля, приведенных в (19), с элементами поля (20) показывает, что они идентичны.

Рассмотрим более подробно, чем это сделано в теореме 2, конструкцию поля Галуа.

Для произвольно выбранного первообразного элемента Θ_l поля произведение

$$(\Theta_l^i \Theta_l^{P-1-i}) \bmod P \equiv 1 \,(\text{mod } P). \qquad (21)$$

Справедливость (21) вытекает из того, что для простого P $\varphi(P) = P - 1$. Из теоремы Эйлера следует, что $\Theta^{\varphi(P)} = \Theta^{P-1} \equiv 1 \,(\text{mod } P)$, поэтому $(\Theta_l^i \Theta_l^{P-i-1}) \bmod P = \Theta^{P-1} \equiv 1 \,(\text{mod } P)$. Ввиду того что сравнение (21) выполняется при любом Θ_l и P, при i =1 элемент поля a_2 однозначно связан с элементом $a_{P\text{-}1}$, при i=2 элемент поля a_3 связан с элементом $a_{P\text{-}2}$ и т.д. Анализ (21) показывает, что элементы поля a_1 и $a_{P\text{-}2}$, a_2 и $a_{P\text{-}2}$ являются мультипликативно обратными.

В связи с указанным свойством поля Галуа зависимыми оказываются, очевидно, и характеры элементов поля или символы ХДС, построенные в поле. Эта зависимость определяется теоремой 3.

Теорема 3. Пусть характер элементов $\psi(a_i)$ поля (символы ХДС в поле GF(P)) определяются из соотношения

$$W_i = \psi(a_i) = \exp(j\pi u_i), \qquad (22)$$

а индексы элементов поля U_i находят из решения сравнения:

$$a_i = \Theta_l^i + 1 = \Theta_l^{U_i} \,(\text{mod } P),$$

тогда характеры $(P\text{-}1)/2+1+i$ ($i = \overline{1,(P-1)/2-1}$) элементов поля (символы сигнала) зависят от характеров $(P\text{-}1)/2\text{-}i$ первых элементов поля, причем

$$W_{P-i} = (-1)^i W_{i+1}. \qquad (23)$$

Доказательство. Рассмотрим произвольный элемент поля $a_i = \Theta^i + 1$. По теореме Ферма $\Theta^{P-1} \equiv 1 \,(\text{mod } P)$. Тогда элемент поля

$$\Theta^i + 1 = \Theta^i + \Theta^{P-1} = \Theta^i (1 + \Theta^{P-i-1}). \qquad (24)$$

Найдем индексы элементов поля (24):

$$ind(\Theta^i + 1) = ind(\Theta^i (1 + \Theta^{P-i-1})). \qquad (25)$$

Учитывая свойства индексов, $ind(a \cdot b) = ind\, a + ind\, b$ [1] (25) можно представить в виде:

$$ind(\Theta^i + 1) = ind\Theta^i + ind(1 + \Theta^{P-i-1}). \qquad (26)$$

Так как основание индекса (логарифма) Θ_l, то $ind\,\Theta^i (\text{mod}\,(P-1)) = \log_\Theta \Theta^i (\text{mod}\,(P-1)) = i$ и соотношение (26) имеет вид:

$$ind(\Theta^i + 1)(\text{mod}\,(P-1)) =$$
$$= u_i = i + ind(1 + \Theta^{P-i-1}) \bmod (P-1).$$

Символы ХДС (характеры элементов поля) могут быть найдены из (22) и (26):

$$\begin{array}{c} W_i = \exp(j\pi u_i) = \\ = \exp(j\pi(i + ind(1 + \Theta^{P-i-1})) \bmod (P-1) = \\ = \exp j\pi i \,(\text{mod}(P-1)) \exp j\pi(1 + \Theta^{P-i-1})) \bmod (P-1). \end{array} \qquad (27)$$

Анализ (27) показывает, что при i четном ($i = 2k$) характер индексов не изменяется. Действительно в этом случае:

$$W_i = \exp(j\pi\, ind(1+\Theta^{P-i-1}))\,, \qquad (28)$$

т.е. символы совпадают по знаку.

При i нечетном ($i = 2k+1$):

$$W_i = -\exp(ind(1+\Theta^{P-i-1}))\bmod(P-1)\,. \qquad (29)$$

В этом случае символы W_i и W_{P-i-1} противоположны по знаку. Приведеное выше подтверждает справедливость (23).

Теорема доказана.

Проилллюстрируем справедливость теоремы 2 на примере.

Пусть характеристика поля GF(P) P =13, а первообразный элемент поля $\Theta = 2$. Изоморфизм НС в данном поле $W = \{-11-111-1111-1-1-1\}$.

Установим зависимость характеров (символов ХДС) в поле GF(13). При $i=1$ $W_2 = -W_2$, $i=2$ $W_{11} = W_3$, $i=3$ $W_{10} = -W_4$, $i=4$ $W_9 = W_5$, $i=5$ $W_8 = -W_6$. Результат будет таким же, если для установления зависимости символов НС применить (23).

Использование теоремы 3 позволяет определить $(P\text{-}1)/2+i$ символы ХДС ($i = \overline{1,(P-1)/2}$) по известным первым $(P\text{-}1)/2\text{-}i$ символам. В этом случае не определены лишь первый и $((P\text{-}1)/2+i)$-й символы ХДС. Но $((P\text{-}1)/2+i)$-й символ ХДС определяется правилом кодирования (1). Действительно, известно, что элемент поля $\Theta^{(P-1)/2} = L$, тогда $\Theta^{(P-1)/2}+1 = L+1(\text{mod}\ P) \equiv 0(\text{mod}\ P)$. В соответствии с правилом кодирования (1), если $\Theta^i + 1 \equiv 0(\text{mod}\ P)$, то символ сигнала равен 1. Для ХДС число символов K, принимающих значение «1», равно $K=L/2$. Это означает, что первый символ ХДС может быть доопределен, если известны P-2 символов сигнала.

Нетрудно убедиться в том, что теоремы 2 и 3 справедливы и для расширенного поля Галуа, т.е. для случая $n>1$.

Выявленные и описанные в теоремах 2 и 3 связи элементов и характеров элементов поля, позволяют в два раза повысить быстродействие устройств формирования ХДС. Достигается указанное формированием согласно правилу (22) лишь половины символов сигнала, остальные символы могут быть получены путем реализации правила (23).

Литература:

[1] *Свердлик М.Б.* Оптимальные дискретные сигналы. М., 1975. 200 с.

[2] *Горбенко И.Д., Замула А.А., Бессарабенко К.В.* Ускоренные алгоритмы построения систем характеристических дискретных сигналов //Радиотехника. 1988. Вып. 84. с.69-72. 2. А.с. СССР Устройство для формирования псевдослучайных сигналов / В.И. Долгов, И.Д. Горбенко – 1983.- № 5. – с. 63.

[3] *Альберт А.А.* Конечные поля // Кибернет. сб. – с. 7 – 43.

Поступила в редколлегию 26.05.2011

Замула Александр Андреевич, профессор кафедры БИТ ХНУРЭ, канд. техн. наук, доцент. Область научных интересов: технологии защиты информации в информационно-телекоммуникационных системах.

Колованова Евгения Павловна, ассистент кафедры БИТ ХНУРЭ. Область научных интересов: информационные технологи, защита информации, методы и средства аутентификации данных, широкополосные системы связи, распознавание изображений.

Киянчук Руслан Игоревич, студент кафедры БИТ ХНУРЭ. Область научных интересов: блочные симметричные шифры, облегченная криптография (Lightweight Cryptography), стеганография.

Ярыгина Татьяна Евгеньевна, студентка кафедры БИТ ХНУРЭ. Область научных интересов: криптография, блочные симметричные шифры, широкополосные системы связи.

УДК 621. 391

Синтез одного класу дискретних сигналів в полях Галуа / Замула О.А. , Кіянчук Р.І., Яригіна Т.Є., Колованова Є.П. // Прикладна радіоелектроніка: наук.-техн. журнал. – 2011. Том 10. № 2. – С. 240–243.

У статті пропонуються методи синтезу одного класу складних сигналів, що засновані на використанні властивостей полів Галуа. Крім того, наводиться теорема, з використанням якої встановлюються зв'язки характерів елементів мультиплікативної групи поля Галуа та залежність символів дискретних кодів, які построєні з використанням характерів мультиплікативної групи поля.

Ключові слова: характеристичні дискретні сигнали, характер мультиплікативної групи, функція кореляції.

Бібліогр. 3 найм.

UDC 621.391

Synthesis of a class of discrete signals in Galois fields / Zamula A.A., Kiyanchuk R.I., Yarygina T.E., Kolovanova E.P. // Applied Radio Electronics: Sci. Journ. – 2011. Vol. 10. № 2. – P. 233–239.

The paper suggests methods for synthesis of a class of complex signals based on the properties of Galois fields. In addition, a theorem is provided on the basis of which links of characters of Galois field multiplicative group elements and a dependence of characters of discrete codes built on the use of multiplicative field group characters are established.

Keywords: characteristic discrete signals, nature of a multiplicative group, correlation function.

Ref.: 3 items.