УДК 621.396

И. Д. ГОРБЕНКО, д-р техн. наук, *Ю. В. СТАСЕВ*,
канд. техн. наук, *А. А. ЗАМУЛА*, канд. техн. наук

АЛГЕБРАИЧЕСКИЙ МЕТОД ПОСТРОЕНИЯ НЕЛИНЕЙНЫХ СИГНАЛОВ ХАРАКТЕРИСТИЧЕСКОГО ТИПА

Основная тенденция развития современных систем связи — повышение эффективности передачи информации. С этой целью внедряются новые методы, обеспечивающие повышение скорости передачи, снижение влияния помех в канале и экономное расходование полосы частот. Решению этих задач способствует рациональный выбор сигналов, используемых для передачи информации по каналам, методов их формирования и обработки на приеме.

В современных системах связи широко используют сложные сигналы с фазовой модуляцией. Возрастает интерес к нелинейным (с точки зрения закона построения) сигналам.

Нелинейные сигналы (НС) существуют для значений длительностей, определяемых из условия $L = 4x + 2 = P^n - 1$ или $L = 4x = P^n - 1$. Здесь P — характеристика поля Галуа; n — степень расширения поля, $x = 1, 2, \ldots$. НС принадлежат к оптимальным по минимаксному критерию системам сигналов. Объем системы, составленной из НС, определяется из выражения $M = \varphi(L)/n$, где $\varphi(\cdot)$ — функция Эйлера. Правило построения НС описывается уравнением [1]:

$$\begin{aligned} W &= \Psi(\Theta^l + 1), \text{ если } \Theta^l + 1 \not\equiv 0 \pmod P; \\ W &= 1, \text{ если } \Theta^l + 1 \equiv 0 \pmod P. \end{aligned} \tag{1}$$

Метод построения НС подробно описан в работе [2].

Одной из операций, выполняемых при построении НС, является формирование поля Галуа $GF(P^n)$. Элементы поля a_i могут быть вычислены с использованием соотношения

$$a_i = \Theta_l^i \bmod d(f(x), P), \tag{2}$$

где Θ_l — l-й первообразный элемент поля Галуа; $i = \overline{0, P^n - 2}$; $f(x)$ — первообразный неприводимый над полем $GF(P)$ полином.

Операции в (2) выполняются по двойному модулю (modd) — модулю $f(x)$ и P.

Как следует из (2), для построения всех элементов поля необходимо выполнить $P^n - 2 = L$ операций возведения θ_l в степени i.

Приведем теорему о свойстве поля Галуа, определяющем связи элементов a_i поля $GF(P^n)$.

Теорема 1. *Пусть* $a_1, a_2, \ldots, a_{(P-1)/2}$ — *элементы поля* $GF(P)$, *тогда элементы поля* $a_{(P-1)/2+1}$, $a_{(P-1)/2+2}$, a_{P-1} *зависят от* $(P-1)/2$ *первых элементов и определяются из выражения* $a_{(P-1)/2+i} = P - a_i$ (3), *где* $i = \overline{1, (P-1)/2}$.

Доказательство. Известно, что i-й элемент поля может быть представлен как $a_i = \Theta^{i-1} (\bmod P)$ ($(P-1)/2 + n$)-й. Элемент имеет вид $a_{(P-1)/2+i} = \Theta^{(P-1)/2+i-1}$.

Тогда (3) можно переписать следующим образом:

$$\Theta^{n-1} + \Theta^{(P-1)/2+i-1} = P \equiv 0 (\bmod P).$$

Вынеся за скобки Θ^{n-1}, получим

$$\Theta^{n-1}(1 + \Theta^{(P-1)/2}) = P \equiv 0 (\bmod P). \tag{4}$$

По теореме Ферма $\Theta^{P-1} \equiv 1 (\bmod P)$;

$$(\Theta^{(P-1)/2} - 1)(\Theta^{(P-1)/2} + 1) \equiv 0 (\bmod P). \tag{5}$$

В (5) 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

$$\Theta^{(P-1)/2} \equiv 1 (\bmod P); \tag{6}$$

$$\Theta^{(P-1)/2} \equiv -1 (\bmod P). \tag{7}$$

Сравнение (6) не может выполняться, так как в поле Галуа лишь $\Theta^{P-1} \equiv 1 (\bmod P)$ и $\Theta^0 \equiv 1 (\bmod P)$. Поэтому выполняется сравнение (7). В этом случае справедливо и (4). Тогда $((P-1)/2 + i)$-й элемент поля может быть найден из соотношения $a_{(P-1)/2+i} = P - a_i$. Теорема доказана.

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

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

Запишем элементы данного поля:

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

Воспользуемся выражением (3) для получения $((P-1)/2+i)$-х элементов поля $(i = 1, \overline{(P-1)}$ (2):

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

Сравнение элементов поля, приведенных в (8), с элементами поля (9) показывает, что они идентичны.

Рассмотрим более подробно, чем это сделано в теореме 1, конструкцию поля Галуа.

Для произвольно выбранного первообразного элемента Θ_l поля произведение

$$(\Theta_l^i \Theta_l^{P-1-i}) \bmod P \equiv 1 \pmod P. \quad (10)$$

Справедливость (10) вытекает из того, что для простого P $\varphi(P) = P - 1$ [1]. Из теоремы Эйлера следует, что $\Theta^{\varphi(P)} = \Theta^{P-1} \equiv 1 \pmod P$, поэтому $(\Theta_l^i \Theta^{P-i-1}) \bmod P = \Theta^{P-1} \equiv 1 \pmod P$. Ввиду того что сравнение (10) выполняется при любом Θ_l и P, при $i = 1$ элемент поля a_1 однозначно связан с элементом a_{P-2}, при $i = 2$ a_2 связан с элементом a_{P-3} и т. д. Анализ (10) показывает, что элементы поля a_1 и a_{P-2}, a_2 и a_{P-3} являются мультипликативно обратными.

В связи с указанным свойством поля Галуа зависимыми оказываются, очевидно, и характеры элементов поля или символы НС, построенные в поле. Эта зависимость описывается теоремой 2.

Теорема 2. *Пусть характер элементов* $\psi(a_i)$ *поля (символы* НС *в поле* GF (P)) *определяются из соотношения*

$$W_i = \psi(a_i) = \exp(j\pi u_i), \quad (11)$$

а индексы элементов поля u_i *находят из решения сравнения*

$$a_i = \Theta_l^i + 1 = \Theta_l^{u_i} \pmod P,$$

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

$$W_{P-1} = (-1)^i W_{i+1}. \quad (12)$$

Доказательство. Рассмотрим произвольный элемент поля $a_i = \Theta_i + 1$. По теореме Ферма $\Theta^{P-1} \equiv 1 \pmod P$. Тогда элемент поля

$$\Theta^i + 1 = \Theta^i + \Theta^{P-1} = \Theta^i (1 + \Theta^{P-i-1}). \quad (13)$$

Найдем индексы элементов поля (13):

$$\operatorname{ind}(\Theta^i + 1) = \operatorname{ind}(\Theta^i(1 + \Theta^{P-i-1})). \qquad (14)$$

Учитывая свойство индексов, $\operatorname{ind}(a \cdot b) = \operatorname{ind} a + \operatorname{ind} b$ [1] (14) можно представить в виде

$$\operatorname{ind}(\Theta^i + 1) = \operatorname{ind}\Theta^i + \operatorname{ind}(1 + \Theta^{P-i-1}). \qquad (15)$$

Так как основание индекса (логарифма) Θ_i, то

$$\operatorname{ind}\Theta^i \pmod{(P-1)} = \log_\theta \Theta^i \pmod{(P-1)} = i$$

и соотношение (15) имеет вид

$$\operatorname{ind}(\Theta^i + 1) \pmod{(P-1)} = u_i = i + \operatorname{ind}(1 + \Theta^{P-i-1}) \bmod (P-1).$$

Символы НС (характеры элементов поля) могут быть найдены из (11) и (15):

$$W_i = \exp(j\pi u_i) = \exp(j\pi(i + \operatorname{ind}(1 + \Theta^{P-i-1})) \bmod (P-1) =$$
$$= \exp j\pi i \pmod{(P-1)} \exp j\pi(\operatorname{ind}(1 + \Theta^{P-i-1})) \bmod (P-1). \qquad (16)$$

Анализ (16) показывает, что при i четном ($i = 2k$) характер индексов не изменяется. Действительно, в этом случае

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

т. е. символы W_i и W_{P-i-1} совпадают по знаку.

При i нечетном ($i = 2k + 1$)

$$W_i = -\exp(\operatorname{ind}(1 + \Theta^{P-i-1})) \bmod (P-1). \qquad (17)$$

В этом случае символы W_i и W_{P-i-1} противоположны. Приведенное выше подтверждает справедливость (12).

Теорема доказана.

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

Проиллюстрируем справедливость теоремы 2 на примере.

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

Установим зависимость характеров (символов НС) в поле GF (17). 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 (12).

Использование теоремы 2 позволяет определить $(P-1)/2 + 1 + i$ символы НС ($i = \overline{1, (P-1)/2}$) по известным первым $(P-1)/2 - 1$ символам. Не определены первый и $((P-1)/2 + 1)$-й символы НС; $((P-1)/2 + 1)$-й символ НС определяется правилом кодирования (1). Действительно, известно, что элемент поля $\Theta^{(P-1)/2} = L$ [1], тогда $\Theta^{(P-1)/2} + 1 = L + 1 \pmod P \equiv 0 \pmod P$. Но в соответствии с правилом кодирования (1), если $\Theta^i + 1 \equiv 0 \pmod P$, то символ сигнала равен 1.

Для НС характеристического типа число символов, принимающих значение «1», равно $K = L/2$. Это означает, что первый символ НС может быть доопределен, если известны $P - 2$ символов сигнала.

Выявленные и описанные в теоремах 1 и 2 связи элементов и характеров элементов поля позволяют в два раза повысить быстродействие устройств формирования НС. Достигается указанное формированием согласно правилу (2) лишь половины элементов поля. Оставшиеся элементы могут быть получены путем реализации правила (3).

Полученное аналитическое выражение (12) дает возможность в два раза уменьшить число операций вида (11) при построении символов НС.

Список литературы: 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.

Поступила в редколлегию 07.07.88