УДК 621.391

И. Д. ГОРБЕНКО, д-р техн. наук,
А. А. ЗАМУЛА, канд. техн. наук

БЫСТРЫЙ АЛГОРИТМ ПОСТРОЕНИЯ НЕЛИНЕЙНЫХ СИГНАЛОВ ХАРАКТЕРИСТИЧЕСКОГО ТИПА В РАСШИРЕННЫХ ПОЛЯХ ГАЛУА

Поиск псевдослучайных последовательностей, используемых для расширения спектра в широкополосных системах, в значительной мере связан с мощными структурами современной алгебры. Многие последовательности основаны на структурах полей Галуа. В работе [1] изложены теоретические основы построения нелинейных сигналов характеристического типа (НСХТ) в простых полях Галуа — $GF(P)$. В тоже время известно, что такие сигналы могут быть построены и в расширенных полях Галуа, т. е. для значений длительностей L, определяемых из условий: $L=4x=P^n-1$ и $L=4x+2=P^n-1$, где $x=1, 2, 3\ldots$; n — степень расширения поля $GF(P)$.

В настоящее время существуют только табличные методы построения НСХТ в расширенных полях, что ограничивает возможности синтеза (формирования) и анализа данных сигналов для больших значений n.

Элементы расширенного поля Галуа представляют собой полиномы степени не выше n, а коэффициенты при неопределенных переменных принимают значения над полем $GF(P)$. Все операции в расширенных полях выполняются по двойному модулю $\mathrm{mod\,d}(f(x), P)$. Если P — простое число, а $f(x)$ — первообразный неприводимый над полем $GF(P)$ полином, то с использованием $\varphi(P^n-1)/n$ первообразных элементов поля может быть построена вся система сигналов.

Ниже приводится теорема, определяющая алгоритм построения НСХТ в расширенных полях Галуа.

Теорема. *Пусть $GF(P^n)$ — расширение n-й степени поля $GF(P)$, а элементы-полиномы, степени которых не превышают n, вычисляются над полем $GF(P)$; $f(x)$ и H_l — соответственно первообразный неприводимый над полем $GF(P)$ полином и l-й первообразный элемент поля $GF(P)$, функция характеров гомоморфного отображения элементов поля $GF(P^n)$ на поле $GF(2)$ зафиксирована*

функцией $\psi(a_i)=\exp(j\pi U_i)$, *причем* a_i *определяется из решения сравнения* $a_i \equiv H_l^{ui} \times (\mathrm{mod}\, df(x), P)$, *а* $U_i=0, \overline{P^n-2}$ *есть множество чисел-индексов, упорядоченных по возрастанию, тогда формирование нелинейных сигналов в поле* $GF(P^n)$ *описывается следующими шагами.*

1. Формируется массив номеров (индексов) $U'=U_i+1$, $i=\overline{0, P^n-2}$, упорядоченных по возрастанию и массив элементов-полиномов a_i по правилу

$$\text{МП}(i) = H_i^l (\mathrm{modd}\, f(x), P).$$

2. Строится масив МС(i) элементов-полиномов, элементы которого сдвинуты по значению на единицу относительно значений элементов массива МП(i):

$$\text{МС}(i) = \text{МП}(i+1), \text{ если } H_i^l + 1 \not\equiv 0 (\mathrm{modd}\, f(x), P);$$

$$\text{МС}(i) = 1, \text{ если } H_i^l + 1 \equiv 0 (\mathrm{modd}\, f(x), P).$$

3. Массив индексов U' записывается в массив МК(i) по адресам A_i, которые определяются десятичным представлением элементов-полиномов, массива МП(i).

4. Формируется массив МН(i), $i=\overline{0, P^n-2}$ — массив индексов путем считывания из массива МК(i) индексов, выбираемых по адресам, которые представляет собой десятичное представление B_i полиномов. Записываются выбранные значения индексов по соответствующим адресам десятичного представления полиномов.

5. Вычисляется для всех значений массива индексов МН(i) двухзначный характер мультипликативной группы поля (символы НСХТ) в соответствии с правилом

$$\psi(a_l) = \psi(H_l^l + 1) = -\psi(\text{МН}(i)) = \begin{cases} 1, \text{ если МН}(i) \equiv 0 (\mathrm{mod}\, 2); \\ -1, \text{ если МН}(i) \not\equiv 0 (\mathrm{mod}\, 2). \end{cases} \quad (1)$$

Доказательство теоремы. Покажем, что алгоритм синтеза НДСХТ в расширенном поле Галуа является эквивалентным алгоритму, изложенному в работе [2]. Приведем этот алгоритм.

1. Осуществляется построение расширенного поля путем возведения в степени $i=0, 1, 2, \ldots, P^n-2$ $\varphi(P^n-1)/n$ первообразных элементов поля. Вычисление элементов поля $GF(P^n)$ производится по двойному модулю — модулю первообразного неприводимого над полем $GF(P)$ полиному $f(x)$ и модулю простого числа P. Таким образом, расширенное поле представляет собой совокупность полиномов степени не выше n с коэффициентами, принимающими значения над полем $GF(P)$.

2. Строится поле $GF(P^n)$, элементы-полиномы которого сдвинуты на 1 в сторону увеличения их значения относительно элементов исходного поля, т. е.

$$a_1' = H^0 + 1 (\mathrm{modd}\, f(x), P); \; a_2' = H^1 + 1 (\mathrm{modd}\, f(x), P);$$

$$a_i' = H^{i-1} + 1 (\mathrm{modd}\, f(x), P); \; a'_{P^n-1} = H^{P^n-2} + 1 (\mathrm{modd}\, f(x), P),$$

3 Вычисляется характер элементов поля $a'_1, a'_2, \ldots a'_i, \ldots a^{P_n-1}$ с использованием соотношения $\psi(H^l+1)=\psi(a'_l)=\exp(j\pi U_l)$

где U_i — индекс некоторого элемента a_j, для которого выполняется сравнение

$$H^l+1\,(\mathrm{modd}\,f(x),\ P)\equiv H^{U_i}\,\mathrm{modd}\,(f(x),\ P). \qquad (2)$$

Сравнение (2) решается путем перебора, т. е. для каждого элемента поля $a'_l=H^l+1$ среди всех элементов поля отыскивается элемент a_j, равный (совпадающий) с a'_l. Значение индекса, при котором выполняется сравнение (2), и будет решением сравнения.

Сопоставление алгоритма, сформулированного в теореме, с приведенным в работе [2] и описанным выше, показывает, что в обоих случаях строится расширенное поле Галуа в естественном виде. Поэтому эти этапы эквивалентны. На втором этапе в обоих случаях строится поле, элементами которого являются элементы-полиномы, сдвинутые на 1. Поэтому и вторые этапы алгоритмов совпадают.

Покажем, что на этапах 3, 4 и 5 нового алгоритма производится решение P^n-1 сравнений вида (2), т. е., что в указанном в теореме шаге 3 запись индексов по адресам, определенных десятичным представлением элементов-полиномов, и чтение с указанного массива значений индексов по адресам, задаваемым десятичным представлением элементов a'_l, приводит к получению массива индексов, сдвинутых относительно истинных на 1, и является по существу этапом известного алгоритма перебора. При этом если i— номер элемента-полинома $F_k(x)$ поля $GF(P^n)$, а $f(x)$ — первообразный неприводимый над полем $GF(P)$ полином, то с точностью до изоморфизма элементы полинома $F_k(x)$, их индексы $\mathrm{Ind}\,F_{k,i}(x)$ и номера позиций i связаны рекуррентных соотношением [3]

$$F_{k,i}=\mathrm{Ind}\,(F_{k,i}(x)+1)(x)=F_{k,i-1}=\mathrm{Ind}\,(F_{k,1}(x))(x)\times$$
$$\times\,(\mathrm{modd}\,f(x),\ P). \qquad (3)$$

Действительно, если левую часть выражения (3) представить в виде $H^{i-1}=F_{k,1}(H)\,\mathrm{mod}\,d\,(f(H,P))$, а правую часть как

$$F_{k,i-1}(H)=H^{i-2}\cdot H\,(\mathrm{modd}\,f(H),\ P)=H^{i-1}\,(\mathrm{modd}\,f(x),\ P).$$

Далее убедимся, что индекс i—1 является индексом-элементом поля $F_{k,i}(x)$. Действительно, если $x=H$ — первообразный элемент, то из свойства цикличности мультипликативной группы следует, что все степени H^{i-1}, $i=\overline{0,\ P^n-2}$ принимают значения всех ненулевых элементов поля. Поэтому $x^{i-1}=H^{i-1}$ также принимают значения всех ненулевых элементов поля.

В результате записи номеров (индексов) по адресам, определяемым коэффициентами при элементах-полиномах (шаг 3), номера (индексы) оказываются записанными каждый соответственно

определенному элементу поля. Номера (индексы) элементов H^l+1 оказываются сдвинутыми по закону коэффициентов при элементах поля $H^l+1=a_i+1$. Для определения индексов этих элементов необходимо считать номера (индексы), записанные по адресам, задаваемым коэффициентами при полиномах $H^l+1 \pmod{d(f(x), P)}$. Выполнение всех P^n-1 операций считывания номеров (индексов), записанных предварительно по адресам $H^l \pmod{df(x), P}$, приводит к решению всей совокупности сравнений вида (2). Однако номера отличаются от индексов сдвигом на 1, поэтому для получения истинных индексов после считывания номеров их значения необходимо уменьшить на 1. Для случая двухзначного характера мультипликативной группы поля Галуа эту операцию можно не выполнять, так как сдвиг на 1 эквивалентен инверсии характеров. Действительно

$$\psi(a_i) = e^{j\pi(U_l+1)} = e^{j\pi}e^{j\pi U_l}(\cos\pi + j\sin\pi)\,e^{j\pi U_l} = -e^{j\pi U_l}.$$

Поэтому на 5-м этапе характер поля можно вычислять для сдвинутых на 1 индексов, учитывая этот сдвиг знаком «минус» в (1). Теорема доказана.

Покажем на примере возможность построения НСХТ с использованием алгоритма, задаваемого теоремой.

Пример. Построить НСХТ длительностью $L=8$. В этом случае $P=3$, $n=2$. В качестве первообразного неприводимого над $GF(3)$ полинома выберем полином вида $f(x)=x^2-x-1$.

Массив элементов поля запишем, реализуя (шаг 1) теоремы

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

Модифицированное поле в соответствии с шагом 2 теоремы примет вид

$$\text{МС}(i) = \{2,\ \text{H}+1,\ \text{H}+2,\ 2\text{H}+2,\ 1,\ 2\text{H}+1,\ 2\text{H},\ \text{H}\}.$$

Сформируем десятичное представление элементов-полиномом исходного поля в соответствии с шагом 3 теоремы

$$A_l = \{1, 3, 4, 7, 2, 6, 8, 5\}.$$

Запишем массив МК(i) путем записи номеров элементов поля по адресам, задаваемым массивом A_i, МК(i)={1, 5, 2, 3, 8, 6, 4 7}. Десятичное представление массива МС(i) имеет вид B_i={2, 4, 5, 8, 1, 7, 6, 3}. В соответствии с шагом 4 формируем массив индексов МН(i)={5, 3, 8, 7, 1, 4, 6, 2}. Вычислим для всех значений МН(i) двухзначный характер мультипликативной группы поля в соответствии с шагом 5 теоремы $\psi(a_i)$= {1, 1, — 1, 1, 1, —1, —1, —1}.

Последовательность выполнения операций по формированию НДСХТ для данного примера приведена в таблице.

U_i	1	2	3	4	5	6	7	8
МП(i)	1	H	H+1	2H+1	2	2H	2H+2	H+2
МС(i)	2	H+1	H+2	2H+2	1	2H+1	2H	H
A_i	1	3	4	7	2	6	8	5
МК(i)	1	5	2	3	8	6	4	7
B_i	2	4	5	8	3	7	1	6
МН(i)	5	3	8	7	2	4	1	6
$\psi(a_i)$	1	1	—1	1	—1	—1	1	—1

Вычислительная сложность известного алгоритма [2] формирования НСХТ может быть оценена с использованием соотношения

$$T_{\text{ф}} = (P^n - 1)(ty + t_{\text{сл}} + t_{\text{дел}}(P^n - 1)/2 + t_{\text{ср}} \times \\ \times (P^n - 1)/2 + 6t_{\text{зап}}), \quad (4)$$

где $t_{\text{у}}$, $t_{\text{сл}}$, $t_{\text{дел}}$, $t_{\text{ср}}$, $t_{\text{зап}}$. — время выполнения операций умножения, сложения, деления, сравнения, записи соответственно.

Вычислительная сложность разработанного алгоритма оценивается с помощью соотношения

$$T_{\text{ф}} = (P^n - 1)(t_{\text{у}} + t_{\text{сл}} + t_{\text{дел}} + 6t_{\text{зап}} + t_{\text{ср}}). \quad (5)$$

Анализ соотношений (4), (5) показывает, что для известного алгоритма время формирования сигналов находится в квадратичной зависимости от $t_{\text{ср}}$ и $t_{\text{дел}}$, для полученного алгоритма эта зависимость линейная.

Список литературы: 1. *Горбенко И. Д., Замула А. А., Бессарабенко К. В.* Ускоренные алгоритмы формирования систем характеристических дискретных сигналов//Радиотехника. 1988. Вып. 84. С. 69—72. 2. *Свердлик М. В.* Оптимальные дискретные сигналы. М., 1975. 200. с. 3. *Лидл Р., Нидеррайтер Г.* Конечные поля. В 2-х т.: Пер. с англ. М., 1988. 822 с.

Поступила в редколлегию 27.12.88