УДК 621.391

И. Д. ГОРБЕНКО, д-р техн. наук, *А. А. ЗАМУЛА*, *К. В. БЕССАРАБЕНКО*

УСКОРЕННЫЕ АЛГОРИТМЫ ФОРМИРОВАНИЯ СИСТЕМ ХАРАКТЕРИСТИЧЕСКИХ ДИСКРЕТНЫХ СИГНАЛОВ

Характеристические дискретные сигналы (ХДС) с двухуровневой периодической функцией автокорреляции (ПФАК), построение которых базируется на использовании характера мультипликативной группы поля Галуа $GF(P)$, рассмотрены ранее [1]. Число символов (длительность) таких сигналов $L = P - 1$ (1), где P — простое число. Объем системы ХДС больше объема системы линейных последовательностей максимального периода [1]. Известно также, что ХДС существуют для значений $L = 4x$, $L = 4x + 2$, при $x = 1, 2, \ldots$. Линейные последовательности максимального периода существуют лишь для значений $L = 2^n - 1$, где n — количество ячеек памяти линейного регистра.

Еще не разработаны способы формирования системы ХДС, которые бы позволяли синтезировать указанную систему в реальном масштабе времени путем применения программных и аппаратных средств при допустимой сложности последних.

Способ формирования ХДС длительностью L, приведенный 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 $\sigma_i \equiv \equiv \Theta_j^{U_i} \pmod P$, $i = \overline{0, P-1}$ (2). Здесь U_i — индекс элемента поля $GF(P)$, определяемый из решения сравнения (2). Данный способ из-за отсутствия алгоритмизуемых процедур трудно реализуем. В работе [2] предложены метод и устройство формирования ХДС. Метод основан на рекуррентной зависимости между элементами и индексами элементов поля Галуа, при этом можно алгоритмизировать процедуры формирования символов ХДС. Однако вычислительная сложность (время формирования ХДС) остается значительной. Время формирования ХДС $t_\Sigma = L(t_у + t_{сл} + 3t_з + (L+2)t_{сч} + (L+1)t_{ср})$ (3), где $t_у$, $t_{сл}$, $t_з$, $t_{сч}$, $t_{ср}$ — время выполнения операций умножения, сложения, записи, считывания и сравнения соответственно. Анализ выражения (3) показывает, что основные временные затраты при построении ХДС связаны с квадратичными членами $L(L+2)t_{сч}$, $L(L+1)t_{ср}$.

Изложим способ формирования базового и всей системы изоморфизмов ХДС, обладающий значительно меньшей вычислительной сложностью по сравнению со способами, рассмотренными выше.

Ускоренный алгоритм построения базового ХДС (синтез ХДС базируется на использовании наименьшего по значению первообразного элемента θ_j поля $GF(P)$) задается теоремой 1.

Теорема 1. *Пусть характер поля фиксируется функцией* $\psi(a_i) = e^{j\pi U_i}$ *(4), тогда алгоритм построения характеристического сигнала описывается следующими шагами.*

1. *Формируется массив элементов-чисел* a_i, $i = \overline{0, P-2}$ *поля* $GF(P)$: $МП(i) = \Theta_j^i \pmod P$ (5).

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

$$МС(i) = МП(i) + 1, \text{ если } \Theta_j^i + 1 \not\equiv 0 \pmod P;$$

$$МС(i) = 1, \text{ если } \Theta_j^i + 1 \equiv 0 \pmod P.$$

3. *Формируется массив индексов* $МК(i)$, $i = \overline{0, P-2}$, *значениями которого являются соответствующие элементу поля индексы* $i+1$, *упорядоченные по содержимому с адресом* $МП(i)$: $МК(i) = МК[МП(i)]$ (7).

4. *Строится массив индексов* $XI(i)$, *значениями которого являются индексы массива* $МК(i)$, *выбранные по адресу* $МС(i)$: $XI(i) = МК[МС(i)]$, $i = \overline{1, P-2}$.

5. *Вычисляется характер поля по правилу* [1]

$$\psi(a_i) = \psi[XI(i)] = \begin{cases} 1, & \text{если } XI(i) \equiv 0 \pmod 2; \\ -1, & \text{если } XI(i) \not\equiv 0 \pmod 2. \end{cases} \quad (8)$$

Пример. Построим ХДС. Пусть $P = 13$, $L = 12$, $\Theta_j = 2$. Тогда $МП(i) = \Theta_j^i \pmod P = \{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\}$; $i = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 1, 11\}$. Упорядочим ряд $i+1 = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ по закону (адресу) $\Theta_j^i = МП(i)$. В соответствии с (5) — (7) получим массив индексов МК

$(i) = \{1, 2, 5, 3, 10, 6, 12, 4, 9, 11, 8, 7\}$. Произведем выборку элементов чисел из поля МК (i) по адресу МС $(i) = \Theta_j^i + 1 \pmod P = \{2, 3, 5, 9, 4, 7, 11, 12, 10, 6, 11, 8\}$. В результате имеем поле чисел $XI\,(i) = \{2, 5, 10, 9, 3, 12, 1, 7, 11, 6, 8, 4\}$. Вычисляя характер по правилу (8), 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 $GF(P)$ $\text{МП}(i) = \Theta_j^i + 1 \pmod P$, $i = \overline{0, P-2}$ и группы чисел МС(i), сдвинутой по отношению к МП(i) на единицу, т. е. $\text{МС}(i) = \Theta_j^i + 1$. Рассмотрим шаги 3,4 теоремы 1. В результате записи последовательности чисел $i + 1$, сдвинутых на единицу индексов поля МП(i), $i = \overline{0, P-2}$, по адресу Θ_j^i в массиве МК(i) оказываются записанными по сравнению с соответствующими элементами поля $GF(P)$ сдвинутые по значению на единицу числа-индексы. При считывании же с массива МК(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 $t'_\Sigma = L(t_у + t_{сл} + t_{ср} + 7t_з)$ **(9).** В выражении (9) учтено, что $t_з = t_{сч}$.

Приведенный ускоренный алгоритм был реализован на мини- и микро-ЭВМ на языке низкого уровня Ассемблер.

В таблице даны значения выигрыша $K = \dfrac{t_\Sigma}{t'_\Sigma}$, достигаемого при использовании предложенного алгоритма по сравнению с известным [2], в зависимости от числа элементов ХДС. Вычисление выигрыша производилось для различных типов ЭВМ. По данным таблицы предпочтительность предлагаемого способа построения ХДС очевидна.

Способ формирования всей системы изоморфизмов для фиксированной длины ХДС задается теоремой 2.

Тип ЭВМ	L					
	40	100	256	1018	4000	9972
Электроника-60	5,1	11,3	25,5	106,9	417,6	1039,6
Электроника-81	4,5	9,8	23,7	91,4	361,3	899,8

Теорема 2. *Пусть $R = \{r\}$ — множество изоморфных коэффициентов разностного множества, а W_1 — ХДС, синтезированный с исполь-*

зованием минимального первообразного элемента θ_1 *поля* $GF(P)$. *Тогда последовательность* V, *образованная посредством децимации* W_1 *по любому из* r_i *изоморфных коэффициентов,* $i = \overline{1,\varphi(P-1)/2-1}$, *есть* i-*й* $V_i = W(r_i)$ *изоморфизм* ХДС W_1.

Доказательство теоремы основывается на показе того, что метод децимации эквивалентен замене сигнала разностным множеством, сбалансированным на два уровня [1], умножению на изоморфный коэффициент всех членов разностного множества и обратному отображению разностного множества в последовательности характеристического типа.

Пример. Децимация ХДС $W_{12} = \{0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0\}$ по изоморфному коэффициенту (коэффициенту децимации) $r = 5$. Децимируя W_{12} по коэффициенту $r = 5$, т.е. выбирая каждый пятый символ W_{12} по модулю L, найдем V_{12}, обладающий двухуровневой ПФАК и являющийся изоморфизмом сигнала W_{12}, $V = \{1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1\}$.

Применение операции децимации позволяет получить выигрыш в вычислительной сложности формирования ХДС по сравнению с методом разностных множеств: $C = \frac{t_р}{t_д} = \frac{2t_{сч} + t_{ср} + 0{,}5t_у}{t_{сч} + t_{сл}}$ **(10)**, где $t_р$ — время формирования ХДС методом разностных множеств; $t_д$ — время формирования ХДС по алгоритму, задаваемому теоремой 2. При $t_{сч} = 0{,}5 \cdot 10^{-6}$ с, $t_{ср} = 10^{-6}$ с, $t_у = 30 \cdot 10^{-6}$ с и $t_{сл} = 3 \cdot 10^{-6}$ с выигрыш $C \approx 4{,}9$.

Список литературы: 1. *Свердлик М. Б.* Оптимальные дискретные сигналы.— М.: Сов. радио, 1975.— 200 с. 2. *А. с. 9995292 СССР.* Устройство для формирования псевдослучайных сигналов / В. И. Долгов, И. Д. Горбенко, И. И. Сныткин// Открытия. Изобретения.— 1983.— № 5.— С. 6. 3. *Альберт А. А.* Конечные поля // Кибернет. сб.— 1966.— Вып. 3.— С. 7 — 43.

Поступила в редколлегию 23.09.86