УДК 621.391

*И. Д. ГОРБЕНКО*, д-р техн. наук, *А. А. ЗАМУЛА*, канд. техн. наук,
*С. В. РОДИОНОВ*

# ПОСТРОЕНИЕ СИСТЕМ ХАРАКТЕРИСТИЧЕСКИХ ДИСКРЕТНЫХ СИГНАЛОВ С УЛУЧШЕННЫМИ СВОЙСТВАМИ

В работе [1] приведены новые алгоритмы синтеза характеристических дискретных сигналов (ХДС), отличающиеся от известных существенно меньшей вычислительной сложностью. В [2] приведены корреляционные, ансамблевые и структурные свойства ХДС. Анализ указанных свойств показывает, что по ансамблевым и структурным свойствам ХДС значительно превосходят широко применяемые линейные рекуррентные последовательности максимального периода (ЛРПМ). В то же время ХДС обладают близкими к потенциально-возможным корреляционными свойствами [2], т. е. относятся к дискретным сигналам с оптимальными корреляционными свойствами. Приведенные в [1] алгоритмы позволяют синтезировать любой авто- или изоморфизм ХДС в общем случае в расширенном поле $GF\ (p^n)$. Однако для практической реализации алгоритма и средств формирования ХДС необходимо рассчитывать множество первообразных элементов $\{\Theta\}$ простого $GF\ (p)$ или расширенного $GF\ (p^n)$ полей Галуа. Кроме того, для синтеза ХДС в расширенных полях Галуа необходимо знать множество первообразных неприводимых над полем $GF\ (p)$ полиномов. В [2] показано, что наиболее продпочтительным методом построения всего ансамбля авто- и изоморфизмов является метод децимации. По сравнению с методами разностных множеств [3] метод децимации характеризуется меньшей вычислительной сложностью. Однако для реализации этого метода необходимо предварительно рассчитать требуемый коэффициент (или все множество коэффициентов децимации $(C_i)$) для заданного $L=p^n-1$. В известных источниках не приводятся алгоритмы расчета множества первообразных элементов $\{\Theta\}$ поля и множества коэффициентов децимации $\{C_i\}$. Последнее существенно затрудняет вычисление значений множества $\{\Theta\}$ и $\{C_i\}$ при заданном $L=p^n-1$. Цель статьи — разработка алгоритмов расчета параметров, необходимых для построения ХДС: для простого поля — алгоритмы расчета множества $\{\Theta\}$ и $\{C\}$, а для расширенного поля $GF\ (p^n)$ — множество первообразных неприводимых над полем полиномов.

*Алгоритм расчета первообразных элементов*

Множество первообразных элементов $\{\Theta\}$ характеризуется тем, что каждый изоморфный коэффициент дает максимальный период, равный $L=p^n-1$. С использованием этого свойства в [3] предложен алгоритм нахождения $\Theta_{min}$ элемента, т. е. первообразного элемента, наименьшего среди всего множества $\{\Theta\}$. Используя это свойство, выбирая в качестве первообразных числа $\Theta=2, 3, \ldots$ и, возводя их

в степени 0, 1, 2, ... $p-2$, проверяют, являются ли числа $a_i$ полем Галуа соответствующего периода $L=p^n-1$. Если период $L=p^n-1$, то это является необходимым условием определения $\Theta_{\min}$. Достаточное условие формируется в следующем виде.

Утверждение 1. Если $\Theta_{\min}$ есть первообразный элемент поля, то $((p-1)/2+1)$ элемент мультипликативной группы поля равен $p-1$.

Для доказательства утверждения найдем $((p-1)/2+1)$ элемент мультипликативной группы поля $GF(p)$

$$a_{(p-1)/2+1} = \Theta^{(p-1)/2} \pmod p. \qquad (1)$$

Необходимым и достаточным условием выполнения сравнения $(p-1)/q$ вида $x^q = A$ (2) есть $A \equiv 1 \pmod p$ [4]. Если наибольший общий делитель (НОД) $(A, p) = 1$, а $q > 1$ и является делителем $p-1$, то соотношение (2) при $n=(p-1)/2$, $A=p-1$, $x=\Theta$ будет иметь вид $\Theta_v^{(p-1)/2} = p-1 \pmod p$ (3). С тем, чтобы показать справедливость соотношения (3), необходимо доказать, что $(p-1)^{(p-1)/(p-1)/2} \equiv 1 \pmod p$. Преобразуем последнее выражение, при этом все действия будем выполнять по модулю числа $p$:

$$(p-1)^{\overline{(p-1)/2}} = (p-1)^2 = (p^2 - 2p + 1) \bmod p \equiv 1 \pmod p.$$

Отсюда следует, что $a_{(p-1)/2+1} = (p-1) \bmod p$. Утверждение 1 доказано.

Анализ утверждения 1 показывает, что для расчета $\Theta_{\min}$ (любого $\Theta$) необходимо выполнять не $p-1$ операций возведения в степени $\Theta_i$, $i=2, 3$ ..., а только $(p-1)/2$ операций возведения в степень, так как $a_{(p-1)/2+1}$ элемент равен $L=p^n-1$.

В табл. 1 в качестве справочных данных приведены значения $\Theta_{\min}$ для ряда $L=p-1$, причем $L \leqslant 4000$, а также для $L > 4000$ (выборочные значения).

Известно, что НДС могут быть сформированы для значений $L=p^n-1$, где $n \geqslant 1$ — степень расширения поля Галуа, $p$ — простое число. Построение ХДС в расширенных полях Галуа позволяет увеличить число значений $L$ (по сравнению с использованием для формирования ХДС только простых полей Галуа), для которых существуют ХДС ($L=4x=p^n-1$; $L=4x+2=p^n-1$). Так, в интервале длительностей $\Delta L = 8 \div 10^4$, дополнительно к числу значений $L$, для которых могут быть построены ХДС в простых полях, добавляется еще 32 значения длительностей $L$ ХДС. Суммарный объем системы сигналов, составленной из ХДС, построенных в расширенных полях, составляет $M = 2152943$.

Элементы расширенного поля $GF(p^n)$ представляют собой полиномы степени не выше $n$, а коэффициенты в полиномах принимают значения над полем $GF(p)$. Все операции над элементами поля выполняются по двойному модулю (mod$d(f(x), p)$). Если $p$ — простое, а $f(x)$ — первообразный неприводимый над полем $GF(p)$ полином, то с использованием $\varphi(p^n-1)/n$ первообразных элементов можно построить систему ХДС (множество инверсно-изоморфных сигналов).

*Таблица 1*

| Значение $\theta_{min}$ | Значение $L$, для которых $\theta_{min}$ — первообразный элемент |
|---|---|
| 2 | 4, 10, 12, 18, 28, 36, 52, 58, 60, 66, 82, 100, 106, 130, 138, 148, 162, 172, 178, 180, 196, 210, 226, 268, 292, 316, 346, 348, 372, 378, 388, 418, 420, 442, 460, 466, 490, 508, 522, 540, 546, 556, 562, 586, 612, 618, 652, 658, 660, 676, 700, 708, 756, 772, 786, 796, 820, 826, 828, 852, 858, 876, 882, 908, 940, 946, 1018, 1060, 1090, 1108, 1116, 1122, 1170, 1186, 1212, 1228, 1236, 1258, 1276, 1282, 1290, 1300, 1306, 1372, 1380, 1426, 1450, 1452, 1482, 1492, 1498, 1422, 1530, 1548, 1570, 1618, 1620, 1636, 1666, 1668, 1692, 1732, 1740, 1746, 1786, 1860, 1866, 1876, 1900, 1906, 1930, 1948, 1972, 1978, 1986, 1996, 2026, 2028, 2052, 2068, 2082, 2098, 2130, 2140, 2212, 2220, 2236, 2242, 2266, 2268, 2292, 2308, 2332, 2338, 2356, 2370, 2388, 2436, 2458, 2466, 2476, 2530, 2538, 2548, 2556, 2578, 2620, 2658, 2676, 2682, 2692, 2698, 2706, 2740, 2788, 2796, 2802, 2818, 2836, 2842, 2850, 2860, 2908, 2938, 2956, 2962, 3010, 3018, 3036, 3066, 3082, 3186, 3202, 3252, 3298, 3306, 3322, 3346, 3370, 3412, 3460, 3466, 3468, 3490, 3498, 3516, 3532, 3538, 3546, 3556, 3570, 3580, 3612, 3636, 3642, 3658, 3676, 3690, 3700, 3708, 3732, 3778, 3796, 3802, 3850, 3852, 3876, 3906, 3916, 3922, 3930, 3946, 3988, 5002 |
| 3 | 6, 16, 30, 42, 78, 88, 112, 126, 136, 198, 222, 232, 256, 280, 282, 330, 352, 400, 448, 462, 486, 520, 568, 570, 592, 606, 616, 630, 640, 690, 738, 750, 808, 810, 822, 856, 880, 928, 952, 976, 1012, 1038, 1048, 1062, 1086, 1096, 1192, 1216, 1230, 1278, 1326, 1360, 1408, 1422, 1432, 1446, 1458, 1480, 1552, 1566, 1578, 1600, 1612, 1626, 1662, 1696, 1698, 1708, 1720, 1722, 1830, 1888, 1912, 1950, 1998, 2010, 2080, 2128, 2142, 2152, 2238, 2272, 2310, 2346, 2380, 2392, 2416, 2502, 2608, 2632, 2646, 2656, 2718, 2728, 2730, 2752, 2766, 2776, 2800, 2896, 2968, 3040, 3088, 3136, 3162, 3208, 3256, 3258, 3270, 3328, 3330, 3388, 3390, 3448, 3462, 3558, 3582, 3592, 3616, 3726, 3760, 3820, 3822, 3832, 3918, 3928, 3942, 4000, 6006, 7007, 8008, 14008 |
| 5 | 22, 46, 72, 96, 102, 156, 166, 192, 262, 276, 306, 382, 396, 432, 502, 576, 646, 672, 682, 726, 742, 862, 886, 936, 966, 982, 1032, 1092, 1102, 1152, 1162, 1222, 1366, 1486, 1548, 1582, 1606, 1776, 1822, 1846, 1932, 1992, 2002, 2016, 2062, 2086, 2112, 2202, 2206, 2296, 2376, 2382, 2422, 2446, 2472, 2542, 2616, 2662, 2686, 2712, 2832, 2886, 2902, 2916, 2926, 3022, 3166, 3216, 3342, 3372, 3406, 3432, 3526, 3606, 3622, 3672, 3696, 3766, 3792, 3846, 3862, 10006 |
| 6 | 40, 108, 150, 228, 250, 270, 366, 732, 760, 970, 990, 1068, 1288, 1302, 1428, 1470, 1758, 1788, 1810, 1878, 2410, 2440, 2550, 2748, 2790, 3060, 3078, 3108, 3228, 3250, 3300, 3318, 3966 |
| 7 | 70, 238, 240, 358, 430, 498, 598, 600, 918, 996, 1050, 1180, 1248, 1438, 1608, 1752, 2038, 2088, 2110, 2178, 2250, 2280, 2340, 2590, 2592, 2670, 2710, 2878, 3118, 3120, 3168, 3180, 3456, 3510, 3540, 3718, 3738, 3768, |
| 10 | 312, 336, 1020, 1296, 1782, 2136, 2970, 3220, 3312 |
| 11 | 642, 718, 768, 838, 1008, 1128, 1200, 1510, 1596, 1656, 1800, 2398, 2856, 3048, 3190, 3358, 3888 |
| 13 | 456, 478, 1318, 1320, 1398, 2350, 2952, 3670, 3880, 3910, 12006 |
| 14 | 1030, 1488, 1870, 3000 |
| 15 | 438, 3630 |
| 17 | 310, 910, 1150, 2520, 2998, 3528 |
| 19 | 190, 1558, 2286, 2688 |
| 21 | 408 |
| 22 | 3360 |
| 23 | 2160 |

В [1] приведен алгоритм формирования ХДС в расширенных полях Галуа. Из него следует, что элементы-полиномы поля $GF(p^n)$ заменяются $p$-ичным представлением по правилу

$$\beta = \sum_{i=0}^{L-1} a_i p^i, \tag{4}$$

где $a_i$ — элементы поля $GF(p)$ и являются коэффициентами при степенях x полиномов-элементов $GF(p^n)$. Пусть для поля $GF(3^2)$ элемент поля имеет вид $2x+2$, тогда принимая $x=p=3$, получаем $\beta=2\times3+2=8$, для элемента поля $2x$ $\beta=6$ и т. д..

Докажем, что $p$-ичное представление элементов поля $GF(p^n)$ справедливо или другими словами соответствие (4) — единственное.

Утверждение 2. Если известен полином $F(x)$ $\{GF(p^n)$ и $F(x)=a_0x^0+a_1x^1+a_2x^2+\cdots+a_{n-1}x^{n-1}$, то ему можно поставить в соответствие число $\beta \leqslant p^n-1$ и это соответствие будет единственное, единственным будет и обратное соответствие.

Доказательство. Из определения расширенного поля следует, что коэффициенты полинома $F(x)$ принимают значения над полем $GF(p)$, тогда полином, имеющий максимальное представление в p-ичной системе, может быть записан в виде.

$$F_{\max}(x) = p-1+(p-1)x+(p-1)x^2+\cdots+(p-1)x^{n-1}. \tag{5}$$

Согласно (4)

$$\beta = (p-1)+(p-1)p+(p-1)p^2+\ldots+(p-1)p^{n-1} = \\ = p-1+p^2-p+p^3-p^2+\ldots+p^n-p^{n-1}=p^n-1. \tag{6}$$

Из (6) следует, что представление $\beta$ полинома не превышает порядка поля $GF(p^n)$. Покажем, что $\beta \leqslant p^n-1$ можно представить в виде полинома $a_0+a_1p+a_2p^2+a_3p^3+\ldots+a_{n-1}p^{n-1}$, причем единственным образом. Предположим обратное. Пусть число $\beta$ может быть представлено в виде двух различных полиномов с коэффициентами $a_i$, $i=\overline{0,\ n-1}$; $b_i$, $i=\overline{0,\ n-1}$.

Тогда можно записать равенство

$$a_0+a_1p+a_2p^2+\ldots+a_{n-1}p^{n-1}=b_0+b_1p+\ldots+b_{n-1}p^{n-1}. \tag{7}$$

Преобразуем выражение (7) к виду

$$(b_0-a_0)+(b_1-a_1)p+(b_2-a_2)p^2+\ldots+(b_{n-1}-a_{n-1})p^{n-1}=0 \tag{8}$$

(при неравных нулю коэффициентах).

Так как множество классов вычетов по модулю примитивного неприводимого полинома степени $n$ является множеством линейно-независимых классов вычетов [4], равенство (8) выполняется тогда и только тогда, когда $b_0=a_0$, $b_1=a_1$, $b_2=a_2$... . Утверждение доказано.

Все операции в расширенном поле выполняются по двойному модулю — модулю простого числа $p$ и модулю первообразного неприводимого над полем $GF(p)$ полинома $f(x)$ степени не выше $n$. Остатки от деления любого ненулевого полинома в поле $GF(p^n)$ на полином $f(x)$ образуют поле относительно операции покоэффициентного сложения и операции умножения по модулю $f(x)$. В совре-

менной алгебре доказывается [4], что в поле $GF(p^n)$ существуют первообразные неприводимые полиномы любой степени. Это означает, что можно получать любые расширения поля $GF(p)$, которые называются гиперкомплексными полями. Тем не менее на практике известно лишь ограниченное число неприводимых полиномов. Для практических приложений требуются сигналы с значительно большим числом символов. Разработан алгоритм определения первообразных неприводимых над полем $GF(p)$ полиномов степени $n$. С учетом полученных результатов появляется возможность строить ХДС в расширенных полях порядка $L=p^n-1\leqslant 139^2-1=19320$. В табл. 2 приведены значения $f(x)$ для ряда значений $L=p^n-1$. С использованием приведенных значений $\Theta_{\min}$ синтез ХДС поля $GF(p)$ проводится в соответствии с алгоритмом, задаваемым теоремой 1 [1]. При синтезе ХДС в расширенном поле, выбрав для соответствующего значения $L$ $\Theta_{\min}$ и $f(x)$ из табл. 2,

*Таблица 2*

| Характеристика поля ($p$) | Первообразный над полем $GF(p)$ полином | $p$ | Первообразный неприводимый над $GF(p)$ полином | $p$ | Первообразный неприводимый над $GF(p)$ полином |
|---|---|---|---|---|---|
| 3 | $x+x+2$;<br>$x+x+2x+1$;<br>$x+x+2x+2$; | 37 | $x+x+5$ | 97 | $x+x+5$ |
| | $x+x+1$;<br>$x+x+2x+x+2$ | 41 | $x+x+12$ | 101 | $x+x+3$ |
| 5 | $x+x+2$;<br>$x+x+2$;<br>$x+x+2x+2$; | 43 | $x+x+3$ | 103 | $x+x+5$ |
| | $x+x+2$;<br>$x+x+x+3$ | 47 | $x+x+13$ | 107 | $x+x+5$ |
| 7 | $x+x+3$;<br>$x+x+x+2$;<br>$x+x+3x+5$; | 53 | $x+x+5$ | 109 | $x+x+6$ |
| | $x+2x+2x+4$ | 59 | $x+x+2$ | 113 | $x+x+10$ |
| 11 | $x+x+7$; $x+x+3$<br>$x+x+2x+2$ | 61 | $x+x+2$ | 131 | $x+x+14$ |
| 13 | $x+x+2$;<br>$x+x+2$;<br>$x+x+x+2$ | 67 | $x+x+12$ | 137 | $x+x+6$ |
| 17 | $x+x+3$;<br>$x+x+7$ | 71 | $x+x+11$ | 139 | $x+x+2$ |
| 19 | $x+x+2$; $x+x+6$ | 73 | $x+x+11$ | | |
| 23 | $x+x+7$; $x+x+6$ | 79 | $x+x+3$ | | |
| 29 | $x+x+3$; $x+x+3$ | 83 | $x+x+2$ | | |
| 31 | $x+x+12$;<br>$x+x+9$ | 89 | $x+x+6$ | | |

и воспользовавшись теоремой 2 из работы [1], получим один (исходный) изоморфизм ХДС), причем в дальнейшем ХДС, построенный с использованием $\Theta_{\min}$, будем называть базовым изоморфизмом.

Построим ХДС с числом символов $L=80$. Виберем из табл. 1 $\Theta_{min}=2$. Воспользовавшись теоремой 1 в работе [1] и, учитывая, что $L=p-1$, строим ХДС. Полученный ХДС ($L=80$, $p=81$, $\Theta=2$) приведен в табл. 3.

*Таблица 3*

Последовательность: $L=80$, $p=81$, $\Theta=2$ в поле GF ($p$)

1 1 0 1 0 1 0 0 0 1 1 0 0 0 1 1 1 1 0 0 1 0 1 1 0 0 0 1 0 0 1 0 1
0 1 0 0 0 1 0 0 1 1 1 0 1 1 1 1 1 1 1 1 0 0 0 1 0 0 1 1 1 1 0 0 1 0
1 1 0 1 1 0 0 1 0 0 0 0 0 0

Пример синтеза ХДС для $L=124$ в расширенном поле GF($5^3$) в соответствии с теоремой 2 [1] приведен в табл. 4.

*Таблица 4*

Последовательность: $L=124$, $p=5$, $\Theta=3$ в поле GF ($5^3$)

0 0 0 1 1 0 0 0 0 1 0 0 0 1 1 1 1 0 0 0 1 1 1 0 1 0 0 0 1 1 0 1 1
0 0 0 1 0 1 1 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 0 1 0 1 0 0 0 0 1 0 1
1 1 1 1 1 1 0 1 0 1 0 1 0 0 1 0 1 1 0 0 1 1 1 1 0 1 1 0 0 0 1 1 0
1 1 1 1 0 1 1 0 1 1 0 1 0 0 1 0 0 0 0 1 0 1 1 1 0 0 1

Согласно работе [3] весь ансамбль $\varphi(p^n-1)/2n$ изоморфизмов ХДС может быть построен с использованием теоремы 1 или 2 [1], если известно все множество первообразных элементов поля. Однако, следует из работы [1], вычислительная сложность или время формирования каждого из изоморфизмов остаются еще значительными и требуют применения быстродействующих микропроцессорных устройств. Однако и в этом случае весьма проблематичным является формирование ХДС в реальном масштабе времени. Некоторое уменьшение вычислительной сложности (времени формирования) достигается за счет применения метода разностных множеств [3]. В работе [2] показано, что метод децимации обладает меньшей вычислительной сложностью, чем метод разностных множеств. В частности, время формирования ХДС методом децимации примерно в пять раз меньше времени формирования ХДС метода с применением разностных множеств. Под операцией децимации (разрядки) понимается такое преобразование исходного изоморфизма, при котором элементы изоморфизма оказываются упорядоченными по другому закону, соответствующему другому $\Theta_v$ первообразному элементу, $\Theta_v \neq \Theta_{min}$. Так, если последовательность элементов $W=\{W_0, W_1, W_2\}$ из поля $GF(p)$ является изоморфизмом, а $C \{ GF(p)$ — коэффициент децимации (натуральное число), то изоморфизмом $W^{(C)}$ формируется из элементов поля $W_0$, $W_{0+C}$, $W_{0+2C}$, ..., причем операция сложения в индексе выполняется по mod $p$. Коэффициентами децимации являются такие $C$, для которых выполняется условие $(C, p-1)=1$, т. е. числа $C$ и $P-1$ взаимнопростые. Для нахождения всего множества $\{C\}$, для которых наибольший общий делитель (НОД) $(C, p-1)=1$, может быть применен алгоритм Эвклида [4].

В табл. 5 приведены значения коэффициентов децимации для ряда значений $L=80$ и $L=256$.

*Таблица 5*

| Массив коэффициентов децимации для $L=80$ | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 3 | 7 | 9 | 11 | 13 | 17 | 19 | 21 | 23 | 27 | 29 | 31 | 33 | 37 | 39 | 41 | 43 | 47 | 49 | 51 |
| 53 | 57 | 59 | 61 | 63 | 67 | 69 | 71 | 73 | 77 | 79 | | | | | | | | | | |

| Массив коэффициентов децимации для $L=256$ | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 | 21 | 23 | 25 |
| 31 | 33 | 35 | 37 | 39 | 41 | 43 | 45 | 47 | 49 | 51 | 53 | 55 |
| 61 | 63 | 65 | 67 | 69 | 71 | 73 | 75 | 77 | 79 | 81 | 83 | 85 |
| 91 | 93 | 95 | 97 | 99 | 101 | 103 | 105 | 107 | 109 | 111 | 113 | 115 |
| 121 | 123 | 125 | 127 | 129 | 131 | 133 | 135 | 137 | 139 | 141 | 143 | 145 |
| 151 | 153 | 155 | 157 | 159 | 161 | 163 | 165 | 167 | 169 | 171 | 173 | 175 |
| 181 | 183 | 185 | 187 | 189 | 191 | 193 | 195 | 197 | 199 | 201 | 203 | 205 |
| 211 | 213 | 215 | 217 | 219 | 221 | 223 | 225 | 227 | 229 | 231 | 233 | 235 |
| 241 | 243 | 245 | 247 | 249 | 253 | 253 | 255 | 27 | 29 | 57 | 59 | 87 |
| 89 | 117 | 119 | 147 | 149 | 177 | 179 | 207 | 209 | 237 | 239 | | |

Построим изоморфизм ХДС с числом элементов $L=80$.

Выбирая из табл. 5 соответствующий коэффициент децимации ($C=3$), преобразуем базовый изоморфизм $W_0$.

Базовый ХДС с числом символов $L=80$ и ХДС, полученный путем децимации базового коэффициента децимации 3, представлены в табл. 6.

*Таблица 6*

| Базовый ХДС с $L=80$ |
|---|
| 1 1 0 1 0 1 0 0 0 1 1 0 0 0 1 1 1 1 0 0 1 0 1 1 0 0 0 1 0 0 1 0 1 |
| 0 1 0 0 0 1 0 0 1 1 1 0 1 1 1 1 1 1 1 0 0 0 1 0 0 1 1 1 1 0 0 1 0 |
| 1 1 0 1 1 0 0 1 0 0 0 0 0 0 |

| ХДС, полученный путем децимации базового изоморфизма, $C=3$ |
|---|
| 0 1 0 0 1 1 1 1 0 0 1 0 1 1 0 1 1 0 0 1 0 0 0 0 0 0 1 1 0 1 0 1 0 |
| 0 0 1 1 0 0 0 1 1 1 1 0 0 1 0 1 1 0 0 0 1 0 0 1 0 1 0 1 0 0 0 1 0 |
| 0 1 1 1 0 1 1 1 1 1 1 1 0 0 |

На рисунке в качестве примера приведены реализации периодической функции автокорреляции изоморфизма ХДС.

В случае синтеза системы ХДС непосредственно с использованием множества первообразных элементов поля последние рассчитываются на основе применения теоремы о периоде элемента поля [4]. Суть ее заключается в следующем. Если имеется период элемента $a^{\beta}$ поля $GF(p)$, причем $E=E_{\max}$, а НОД $(\beta, E)=d$, то период элемента $a=E/d$. Максимальный период $E$ элемента поля $GF(p)$ $E=p-1=L$. Но тогда, если НОД $(\beta, E)=1$, период элемента $a^{\beta}=E$, а это значит, что элемент поля $a^{\beta}$ — первообразный. Таким образом осуществляется поиск чисел взаимно простых $C$ и $p-1$.

Находя степени числа $a^{\beta}$ можно рассчитать все множество $\{\theta\}$, а следовательно, построить в соответствии с алгоритмом [1] все изоморфизмы.

Разработанные алгоритмы и приведенные в таблицах значения длительности $L$, для которых существует ХДС, значения $\theta_{min}$ (минимальных первообразных элементов), коэффициентов децимации $C$ и первообразных неприводимых над полем GF($P$) полиномов $f(x)$, позволяют реализовать средства формирования ХДС программно и программно-аппаратно. Кроме того, они могут быть использованы для синтеза ансамбля ХДС с целью моделирования и исследования свойств данных систем сигналов.

**Список литературы:** 1. *Горбенко И. Д.* Новые алгоритмы синтеза оптимальных дискретных сигналов характеристического типа // Радиотехника и электроника. 1989. № 11. С. 2352—2357. 2. *Горбенко И. Д.* Свойства характеристических дискретных сигналов. Радиотехника и электроника. 1990. № 2. С. 421—427. 3. *Свердлик Б. М.* Оптимальные дискретные сигналы. М., 1975. 200 с. 4. *Виноградов И. М.* Основы теории чисел. М., 1981. 175 с.

*Поступила в редколлегию 16.01.90*

УДК 621.391

*И. Д. ГОРБЕНКО*, д-р техн. наук, *А. А. ЗАМУЛА*, канд. техн. наук, *В. Л. КУЛЕШОВ*

## ПРОГРАММНЫЕ СРЕДСТВА ФОРМИРОВАНИЯ НЕЛИНЕЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НАД КОНЕЧНЫМИ ПОЛЯМИ

В теории кодирования в различных областях электроники широко используются последовательности над конечными полями, каждый член которых, будучи элементом основного поля, некоторым простым образом зависит от предшествующих ему членов. Такие последовательности легко получить с помощью рекурсивных процедур. Кроме того, такие последовательности обладают полезными статистическими свойствами. Для большинства приложений в качестве основного поля выбирается поле $GF(2)$. Если $l$ — натуральное число, $a$ $b$, $b_0$, $b_1$, ... $b_{l-1}$ — заданные элементы конечного поля GF($P$) (где $P$ — характеристика поля), то последовательность $S_0$, $S_1$, ... элементов поля $GF(P)$, удовлетворяющая соотношению

$$S_{n+l} = b_{l-1}S_{n+l-1} + b_{l-1}S_{n+l-2} + \ldots + b_0 S_n + b, \quad n = 0, 1, \ldots,$$

называется линейной рекуррентной последовательностью ($l$-го порядка) над полем GF($P$).

В ряде практических приложений интерес представляют нелинейные последовательности (НП) характеристического типа [1], построение которых базируется на вычислении двухзначного харак-