УДК 519.725
DOI: 10.17586/0021-3454-2017-60-4-318-330

ПОСЛЕДОВАТЕЛЬНОСТИ ГОРДОНА—МИЛЛСА—ВЕЛЧА С ПЕРИОДОМ N=1023

В. Г. Стародубцев, А. М. Попов

Военно-космическая академия им. А. Ф. Можайского, 197198, Санкт-Петербург, Россия
E-mail: vgstarod@mail.ru

На основе разработанного алгоритма формирования последовательностей Гордона—Миллса—Велча (ГМВП) получены проверочные полиномы для полного перечня ГМВП с периодом N=1023. Качественным отличием от последовательностей с меньшим периодом является возможность формирования нескольких ГМВП с различной эквивалентной линейной сложностью, определяемой степенью проверочного полинома $h_{\text{ГМВ}}(x)$, для каждой базисной М-последовательности (МП) с примитивным проверочным полиномом $h_{\text{МП}}(x)$ и с аналогичным периодом, на основе которой формируются ГМВП. Данное положение является следствием того, что в конечном поле GF(2^5) существует шесть примитивных полиномов, а не по два, как в полях GF(2^3) и GF(2^4). Для каждой из шести МП с периодом N=31, выступающих в качестве характеристической при матричном представлении МП с периодом N=1023, можно использовать остальные пять МП для формирования различных ГМВП. Показано, что на основе каждой базисной МП с периодом N=1023 можно построить по пять ГМВП, одна из которых будет иметь проверочный полином восьмидесятой степени, две — полиномы сороковой и две — двадцатой степени.

Ключевые слова: *последовательности с составным периодом, конечные поля, неприводимые и примитивные полиномы, эквивалентная линейная сложность*

Псевдослучайные последовательности (ПСП) с хорошими авто- и взаимокорреляционными свойствами получили широкое распространение как в системах связи и управления [1—5], так и в системах навигации [6, 7]. К ним относятся МП, последовательности Голда, малого и большого множеств Касами, последовательности Баркера, Уолша, ГМВП [8—11].

В современных системах связи, к которым предъявляются жесткие требования по конфиденциальности, большое значение приобретает такая характеристика ПСП, как структурная скрытность, которая численно характеризуется эквивалентной линейной сложностью (ЭЛС) [12, 13].

ЭЛС псевдослучайной последовательности ПСП численно равна длине регистра сдвига с линейными обратными связями (РС ЛОС), генерирующего данную последовательность, и соответственно степени проверочного полинома, по которому строится этот регистр сдвига.

Среди перечисленных последовательностей наибольшей структурной скрытностью (при одинаковом периоде) обладают ГМВП [14—17], что особенно наглядно проявляется при увеличении периода ПСП. Значения ЭЛС (степеней проверочных полиномов) перечисленных ПСП с хорошими периодическими корреляционными свойствами приведены в табл. 1.

Таблица 1

Период ПСП	ЭЛС последовательностей				
	МП	Голда	Малого множества Касами	Большого множества Касами	ГМВП
31	5	10	—	—	—
63	6	12	9	15	12
127	7	14	—	—	—
255	8	16	12	20	32
511	9	18	—	—	27
1023	10	20	15	25	20, 40, 80
2047	11	22	—	—	—
4095	12	24	18	30	192

Настоящая статья продолжает цикл публикаций, посвященных разработке алгоритмов синтеза ГМВП и анализу их структурных свойств [17—20]. В этих работах на основе представленных алгоритмов формирования последовательностей и определения начальных состояний регистров сдвига получены перечни проверочных полиномов для двоичных ГМВ-последовательностей с периодами N=63, 255 и для троичных с периодом N=80. Основой представленных алгоритмов является то, что корни полиномов $h_{ci}(x)$ — сомножителей проверочного полинома $h_{\text{ГМВ}}(x)$ — являются степенями корней проверочного полинома $h_{\text{МП}}(x)$ базисной М-последовательности, с помощью которой формируется ГМВ-последовательность.

Целью статьи является определение перечня проверочных полиномов двоичных ГМВП с периодом N =1023 и нахождение ЭЛС этих последовательностей.

Двоичные ГМВП формируются над конечными полями с двойным расширением вида $\mathrm{GF}[(2^m)^n]$, вследствие чего их период является составным числом, т.е. $N = 2^{mn} - 1$, где m и n — натуральные числа.

Символы d_i ГМВП с периодом $N = 2^m$–1 определяются выражением [12, 17]:

$$d_i = \mathrm{tr}_{m1}[(\mathrm{tr}_{mn,m}(\alpha^i))^r],\ 1 \le r < 2^m - 1,\ (r, 2^m - 1) = 1, \tag{1}$$

где $\mathrm{tr}_{mn,\,m}(\cdot)$ — след элемента из поля с двойным расширением $\mathrm{GF}[(2^m)^n]$ в расширенном поле $\mathrm{GF}(2^m)$; $\mathrm{tr}_{m1}(\cdot)$ — след элемента из расширенного поля $\mathrm{GF}(2^m)$ в простом поле GF(2); $\alpha \in \mathrm{GF}[(2^m)^n]$ — примитивный элемент поля с двойным расширением; r — взаимно простое число с порядком мультипликативной группы расширенного поля $\mathrm{GF}(2^m)$, равным $2^m - 1$.

ЭЛС двоичных ГМВП определяется выражением [14, 15, 17]:

$$l_s = mn^{g(r)}, \tag{2}$$

где $g(r)$ — число единиц в двоичном представлении r в (1).

Перечень проверочных полиномов ГМВП с периодом N =1023 определяется в поле с двойным расширением $\mathrm{GF}[(2^m)^n] = \mathrm{GF}[(2^5)^2]$.

Количество различных ГМВП (не считая МП) определяется как произведение числа примитивных полиномов в расширенном поле $\mathrm{GF}(2^5)$ и числа примитивных полиномов в поле с двойным расширением $\mathrm{GF}[(2^5)^2]$ [14]:

$$M_{\text{г}} = \left(\frac{\varphi(2^m - 1)}{m} - 1\right)\frac{\varphi(2^{mn} - 1)}{mn} = ((\varphi(31)/5) - 1)(\varphi(1023)/10) = 300, \tag{3}$$

где $\varphi(a)$ — функция Эйлера, равная числу чисел, взаимно простых с числом a, в ряду от 1 до $(a - 1)$.

В качестве базисной, необходимой для формирования ГМВП, берется МП с периодом N =1023 и проверочным полиномом $h_{\text{МП}}(x) = x^{10} + x^3 + 1$, корнями которого являются элемент α и его p-сопряженные элементы.

Предварительное формирование МП проводится для произвольного начального состояния, например, 0000000001. Затем согласно методике, изложенной в [19], определяется начало МП в соответствии с выражением $d_i = \mathrm{tr}_{10,1}(\alpha^i)$, $i = 0, 1, \ldots, 1022$, т.е. находятся символы d_0, d_1, d_2, …, необходимые для вычисления начального состояния регистров сдвига. Полученная МП с начальным состоянием 0000000100 записывается в виде матрицы размерности $[J \times S] = [31 \times 33]$:

$$F_{\text{МП}} = \begin{bmatrix}
000000010000001001000100000110010 \\
011010000100101010000111101011101 \\
011011011000000001100000110110011 \\
000010101101011100011011111100010 \\
001111001111011011010000000101000 \\
010110101010001111101111001001011 \\
000001001100100010100011011011100 \\
000011110001110111111100100001100 \\
010110111010000110101011001111001 \\
011011001000001000100100110000001 \\
011000101001110110011100010111111 \\
010100010111011010110000110011011 \\
010100000111010011110100110101001 \\
001110000011111001110011011110100 \\
010101011011111000010011101000111 \\
010111110110100100001000010100101 \\
011000111001111111011000010001101 \\
001110010011110000110111011000110 \\
001111011111010010010100000011010 \\
001100101110100101101000100010110 \\
011010010100100011000011101101111 \\
000001011100101011100111011101110 \\
011001110101011101111011001010001 \\
001101100010000111001011111001010 \\
011001100101010100111111001100011 \\
010111100110101101001100010010111 \\
000010111101010101011111111010000 \\
010101001011110001010111101110101 \\
001101110010001110001111111111000 \\
000011100000111111011100010011110 \\
001100111110101100101100100100100
\end{bmatrix}. \qquad (4)$$

Каждый столбец матрицы $F_{\text{МП}}$ (кроме нулевого) соответствует одному из циклических сдвигов „короткой“ МП, называемой характеристической последовательностью (ХП) с периодом J=31 и проверочным полиномом $h_2(x) = x^5 + x^4 + x^3 + x^2 + 1$, корнями которого в соответствии с таблицей неприводимых полиномов над полем GF(2^5) (табл. 2) [21] являются элемент α^3 и его p-сопряженные элементы (период корней 31).

Таблица 2

№ пп	Полиномы $h_i(x)$	Корни полиномов (показатели степеней)
1	$h_1(x) = x^5 + x^2 + 1$	$\alpha^1, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}$
2	$h_2(x) = x^5 + x^4 + x^3 + x^2 + 1$	$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{17}$
3	$h_3(x) = x^5 + x^4 + x^2 + x + 1$	5, 10, 20, 9, 18
4	$h_4(x) = x^5 + x^3 + x^2 + x + 1$	7, 14, 28, 25, 19
5	$h_5(x) = x^5 + x^4 + x^3 + x + 1$	11, 22, 13, 26, 21
6	$h_6(x) = x^5 + x^3 + 1$	15, 30, 29, 27, 23

Последовательность циклических сдвигов образует правило формирования (ПФ) МП с периодом N=1023 в виде вектора из S = 33 компонентов:

$$I_{\text{МП}} = \{-\ 0\ 8\ 3\ 24\ 13\ 14\ 6\ 25\ 10\ 3\ 2\ 5\ 2\ 20\ 14\ 27\ 11\ 28\ 2\ 14\ 16\ 12\ 12\ 18\ 1\ 12\ 19\ 17\ 27\ 5\ 9\ 0\}, \qquad (5)$$

где „–“ обозначает нулевую последовательность (НП).

На основе полученного ПФ можно синтезировать ГМВП. С этой целью в качестве ХП необходимо выбрать другие МП с периодом J = 31. Для этого периода существует еще пять МП с проверочными полиномами $h_1(x)$, $h_3(x)$—$h_6(x)$ из табл. 2. В качестве номера ХП будем использовать номер проверочного полинома.

Для получения других ХП необходимо выполнить децимацию символов $ХП_2$ по индексам децимации $i_{d1} = 3$, $i_{d2} = 5$, $i_{d3} = 7$, $i_{d4} = 11$, $i_{d5} = 15$. Это удобно сделать для нулевого сдвига $ХП_2$, соответствующего первому ненулевому столбцу в матрице (3), получив при этом нулевые сдвиги $ХП_1$, $ХП_3$—$ХП_6$.

Корнем проверочного полинома $ХП_2$ является элемент α^3, тогда при индексе децимации $i_{d1} = 3$ корнем проверочного полинома новой последовательности будет элемент $(\alpha^3)^3 = \alpha^9$, а проверочным полиномом $h_3(x) = x^5 + x^4 + x^2 + x + 1$, соответствующий $ХП_3$.

При индексе децимации $i_{d2} = 5$ получаем $ХП_6$ с проверочным полиномом $h_6(x)$, одним из корней которого является элемент $(\alpha^3)^5 = \alpha^{15}$. При $i_{d3} = 7$ получаем $ХП_5$ с $h_5(x)$, одним из корней которого является элемент $(\alpha^3)^7 = \alpha^{21}$. При $i_{d4} = 11$ получаем $ХП_1$ с $h_1(x)$, одним из корней которого является $(\alpha^3)^{11} = \alpha^{33\mathrm{mod}31} = \alpha^2$. При $i_{d5} = 15$ получаем $ХП_4$ с $h_4(x)$, одним из корней которого является $(\alpha^3)^{15} = \alpha^{45\mathrm{mod}31} = \alpha^{14}$.

Рассмотренные индексы децимации определяют параметр r в выражении (1), тогда в соответствии с (2) можно найти ЭЛС формируемых ГМВП, с учетом того, что $g(r{=}3) = 2$, $g(r{=}5) = 2$, $g(r{=}7) = 3$, $g(r{=}11) = 3$, $g(r{=}15) = 4$:

$$l_{s3} = 20,\ l_{s5} = 20,\ l_{s7} = 40,\ l_{s11} = 40,\ l_{s15} = 80. \qquad (6)$$

Таким образом, ЭЛС синтезируемых ГМВП с периодом N=1023 зависит от индекса децимации для ХП и принимает значения 20, 40 и 80.

ГМВП представляются в виде матрицы, аналогичной (3), при подстановке сдвигов $ХП_1$, $ХП_3$—$ХП_6$ в соответствии с правилом формирования (4). Ниже приведены матричные формы записи ГМВП $F_{г3}$ и $F_{г5}$ для индексов $i_{d1} = 3$, $i_{d2} = 5$:

$$F_{г3} = \begin{bmatrix}
000100100111111110111100100111100\\
001110010010001011100000100111000\\
000010001000101000100111101100110\\
011001011100101000000000000110101\\
010010110000000111100100011000101 1\\
011010001101010010110011011101001\\
001111001011011001110100010000010\\
000110101111010110011011001011010\\
010111001110100011100000100001101\\
010000111000100111101111011101101\\
000011010001111010110011011011100\\
011101111011010110111100100001001\\
011100100010000100101000010110011\\
011000000101111010010100110001111\\
010110010111110001110100010110111\\
010100011111011001010011111010001\\
001101000011110001010011111100100\\
011111110011111110011011001101111\\
000101111110101100101000010000110\\
001010110101110101011100000000100\\
001100011010100011000111001011110\\
011011010100000000100111101010011\\
001011101100100111001000110111110\\
001000111101011101111011101100010\\
010101000110001011000111001101011\\
001001100100000111110111101101100 0\\
010001100000111010111101110101011 1\\
000111110110000100000111111100000\\
010011101001011101011100000110001\\
011110101010101100001111111010101\\
000000101100101001001010011011101 0
\end{bmatrix}, \qquad (7)$$

$$F_{г5} = \begin{bmatrix}
001100010110001010100011001011000 \\
0110110000000100011100000100001111 \\
011010111100100100101011011100111 \\
010001011101011001010000010000011 \\
011110100111010111011111011001001 \\
011101001011010011110011011011011 \\
000101100111110100111111111000110 \\
000111110111110111011000000111100 \\
010100111010101101101111101000101 \\
011001010000100000000111011110101 \\
001001110001111110011100110011110 \\
011100110111010100111000100110011 \\
001110000110001001000100110100010 \\
0010000001101111001010111001110110 \\
010111010110101001000011101010111 \\
0000011111000000111001011111101000 \\
001011100001111101111011001100100 \\
001111111010001110001111001001010 \\
000011101100000100101100000010010 \\
011000101100100111001100100011101 \\
000010010000000011100111111111010 \\
010011001101011010110111101111001 \\
001101101010001101101000110110000 \\
0100001000001011110011011101101011 \\
010101000110101010100100010101101 \\
010010110001011101111100010010001 \\
000110001011110000010011111010100 \\
011111011011010000010100100100001 \\
010110101010101110001000010111111 \\
001010011101111010110000110001100 \\
000100011011110011110100000101110
\end{bmatrix}. \quad (8)$$

Проверочные полиномы полученных ГМВП определяются с помощью итеративного алгоритма Берлекемпа—Месси

$$h_{г3}(x) = x^{20} + x^{19} + x^{18} + x^{16} + x^{12} + x^{11} + x^{9} + x^{7} + x^{3} + x + 1; \quad (9)$$

$$h_{г5}(x) = x^{20} + x^{18} + x^{17} + x^{13} + x^{6} + x^{5} + x^{3} + x + 1. \quad (10)$$

Более компактна запись коэффициентов полиномов в двоичном или двоично-восьмеричном коде [21]:

$$h_{г3} = 111010001101010001011_2 = 7215213_8, \quad (11)$$

$$h_{г5} = 101100010000001101011_2 = 5420153_8. \quad (12)$$

Полиномы (9) и (10) являются произведением неприводимых над полем GF(2) полиномов степени 10 (табл. 3).

Таблица 3

№	Корень α^i	Код полинома	Полином	Корень сопряженного полинома	Период корней	Корни полинома (показатели степеней)
1	α^1	2011E	10000001001	511	1023	α^1, α^2, α^4, α^8, α^{16}, 32, 64, 128, 256, 512
2	α^3	2017B	10000001111	255	341	3, 6, 12, 24, 48, 96, 192, 384, 768, 513
3	α^5	2415E	10100001101	383	1023	5, 10, 20, 40, 80, 160, 320, 640, 257, 514
4	7	3771G	11111111001	127	1023	7, 14, 28, 56, 112, 224, 448, 896, 769, 515
5	9	2257B	10010101111	447	341	9, 18, 36, 72, 144, 288, 576, 129, 258, 516
6	11	2065A	10000110101	253	93	11, 22, 44, 88, 176, 352, 704, 385, 770, 517
7	13	2157F	10001101111	191	1023	13, 26, 52, 104, 208, 416, 832, 641, 259, 518
8	15	2653B	10110101011	63	341	15, 30, 60, 120, 240, 480, 960, 897, 771, 519
9	17	3515G	11101001101	479	1023	17, 34, 68, 136, 272, 544, 65, 130, 260, 520
10	19	2773F	10111111011	251	1023	19, 38, 76, 152, 304, 608, 193, 386, 772, 521

Продолжение таблицы 3

№	Корень α^i	Код полинома	Полином	Корень сопряженного полинома	Период корней	Корни полинома (показатели степеней)
11	21	3753D	11111101011	351	341	21, 42, 84, 168, 336, 672, 321, 642, 261, 522
12	23	2033F	10000011011	125	1023	23, 46, 92, 184, 368, 736, 449, 898, 773, 523
13	25	2443F	10100100011	223	1023	25, 50, 100, 200, 400, 800, 577, 131, 262, 524
14	27	3573D	11101111011	159	341	27, 54, 108, 216, 432, 864, 705, 387, 774, 525
15	29	2461E	10100110001	95	1023	29, 58, 116, 232, 464, 928, 833, 643, 263, 526
16	31	3043D	11000100011	31	33	31, 62, 124, 248, 496, 992, 961, 899, 775, 527
17	33	0075C	111101	495	31	33, 66, 132, 264, 528
18	35	3023H	11000010011	247	1023	35, 70, 140, 280, 560, 97, 194, 388, 776, 529
19	37	3543F	11101100011	379	1023	37, 74, 148, 296, 592, 161, 322, 644, 265, 530
20	39	2107B	10001000111	123	341	39, 78, 156, 312, 624, 225, 450, 900, 777, 531
21	41	2745E	10111100101	367	1023	41, 82, 164, 328, 656, 289, 578, 133, 266, 532
22	43	2431E	10100011001	245	1023	43, 86, 172, 344, 688, 353, 706, 389, 778, 533
23	45	3061C	11000110001	189	341	45, 90, 180, 360, 720, 417, 834, 645, 267, 534
24	47	3177H	11001111111	61	1023	47, 94, 188, 376, 752, 481, 962, 901, 779, 535
25	49	3525G	11101010101	239	1023	49, 98, 196, 392, 784, 545, 67, 134, 268, 536
26	51	2547B	10101100111	207	341	51, 102, 204, 408, 816, 609, 195, 390, 780, 537
27	53	2617F	10110001111	175	1023	53, 106, 212, 424, 848, 673, 323, 646, 269, 538
28	55	3453D	11100101011	121	93	55, 110, 220, 440, 880, 737, 451, 902, 781, 539
29	57	3121C	11001010001	111	341	57, 114, 228, 456, 912, 801, 579, 135, 270, 540
30	59	3471G	11100111001	79	1023	59, 118, 236, 472, 944, 865, 707, 391, 782, 541
31	61	3763	11111110011	47	1023	61, 122, 244, 488, 976, 929, 835, 647, 271, 542
32	63	3255	11010101101	15	341	63, 126, 252, 504, 1008, 993, 963, 903, 783, 543
33	69	2701A	10111000001	375	341	69, 138, 276, 552, 81, 162, 324, 648, 273, 546
34	71	3323H	11011010011	119	1023	71, 142, 284, 568, 113, 226, 452, 904, 785, 547
35	73	3507H	11101000111	439	1023	73, 146, 292, 584, 145, 290, 580, 137, 274, 548
36	75	2437B	10100011111	237	341	75, 150, 300, 600, 177, 354, 708, 393, 786, 549
37	77	2413B	10100001011	187	93	77, 154, 308, 616, 209, 418, 836, 649, 275, 550
38	79	2347	10011100111	59	1023	79, 158, 316, 632, 241, 482, 964, 905, 787, 551
39	83	3623H	11110010011	235	1023	83, 166, 332, 664, 305, 610, 197, 394, 788, 553
40	85	2707E	10111000111	343	1023	85, 170, 340, 680, 337, 674, 325, 650, 277, 554
41	87	2311A	10011001001	117	341	87, 174, 348, 696, 369, 738, 453, 906, 789, 555
42	89	2327F	10011010111	221	1023	89, 178, 356, 712, 401, 802, 581, 139, 278, 556
43	91	3265G	11010110101	157	1023	91, 182, 364, 728, 433, 866, 709, 395, 790, 557
44	93	3777D	11111111111	93	11	93, 186, 372, 744, 465, 930, 837, 651, 279, 558
45	95	2145	10001100101	29	1023	95, 190, 380, 760, 497, 994, 965, 907, 791, 559
46	99	0067	110111	231	31	99, 198, 396, 792, 561, 99, 198, 396, 792, 561
47	101	2055E	10000101101	215	1023	101, 202, 404, 808, 593, 163, 326, 652, 281, 562
48	103	3575G	11101111101	115	1023	103, 206, 412, 824, 625, 227, 454, 908, 793, 563
49	105	3607C	11110000111	183	341	105, 210, 420, 840, 657, 291, 582, 141, 282, 564
50	107	3171G	11001111001	167	1023	107, 214, 428, 856, 689, 355, 710, 397, 794, 565
51	109	2047F	10000100111	151	1023	109, 218, 436, 872, 721, 419, 838, 653, 283, 566
52	111	2123	10001010011	57	341	111,222, 444, 888, 753, 483, 966, 909, 795, 567
53	115	2767	10111110111	103	1023	115, 230, 460, 920, 817, 611, 199, 398, 796, 569

Продолжение таблицы 3

№	Корень α^i	Код полинома	Полином	Корень сопряженного полинома	Период корней	Корни полинома (показатели степеней)
54	117	2231	10010011001	87	341	117, 234, 468, 936, 849, 675, 327, 654, 285, 570
55	119	3133	11001011011	71	1023	119, 238, 476, 952, 881, 739, 455, 910, 797, 571
56	121	3247	11010100111	55	93	121, 242, 484, 968, 913, 803, 583, 143, 286, 572
57	123	3421	11100010001	39	341	123, 246, 492, 984, 945, 867, 711, 399, 798, 573
58	125	3301	11011000001	23	1023	125, 250, 500, 1000, 977, 931, 839, 655,287,574
59	127	2377	10011111111	7	1023	127, 254, 508, 1016, 1009, 995, 967,911,799,575
60	147	2355A	10011101101	219	341	147, 294, 588, 153, 306, 612, 201, 402, 804, 585
61	149	3025G	11000010101	347	1023	149, 298, 596, 169, 338, 676, 329, 658, 293, 586
62	151	3441	11100100001	109	1023	151, 302, 604, 185, 370, 740, 457, 914, 805, 587
63	155	2251A	10010101001	155	33	155, 310, 620, 217, 434, 868, 713, 403, 806, 589
64	157	2553	10101101011	91	1023	157, 314, 628, 233, 466, 932, 841, 659, 295, 590
65	159	3367	11011110111	27	341	159, 318, 636, 249, 498, 996, 969, 915, 807, 591
66	165	0051	101001	363	31	165, 330, 660, 297, 594
67	167	2363	10011110011	107	1023	167, 334, 668, 313, 626, 229, 458, 916, 809, 595
68	171	3315C	11011001101	213	341	171, 342, 684, 345, 690, 357, 714, 405, 810, 597
69	173	3337H	11011011111	181	1023	173, 346, 692, 361, 722, 421, 842, 661, 299, 598
70	175	3615	11110001101	53	1023	175, 350, 700, 377, 754, 485, 970, 917, 811, 599
71	179	3211G	11010001001	205	1023	179, 358, 716, 409, 818, 613, 203, 406, 812, 601
72	181	3733	11111011011	173	1023	181, 362, 724, 425, 850, 677, 331, 662, 301, 602
73	183	3417	11100001111	105	341	183, 366, 732, 441, 882, 741, 459, 918, 813, 603
74	187	3205	11010000101	77	93	187, 374, 748, 473, 946, 869, 715, 407, 814, 605
75	189	2143	10001100011	45	341	189, 378, 756, 489, 978, 933, 843, 663, 303, 606
76	191	3661	11110110001	13	1023	191, 382, 764, 505, 1010, 997, 971,919,815,607
77	205	2213	10010001011	179	1023	205, 410, 820, 617, 211, 422, 844, 665, 307, 614
78	207	3465	11100110101	51	341	207, 414, 828, 633, 243, 486, 972, 921, 819, 615
79	213	2633	10110011011	171	341	213, 426, 852, 681, 339, 678, 333, 666, 309, 618
80	215	2641	10110100001	101	1023	215, 430, 860, 697, 371, 742, 461, 922, 821, 619
81	219	2671	10110111001	147	341	219, 438, 876, 729, 435, 870, 717, 411, 822, 621
82	221	3531	11101011001	89	1023	221, 442, 884, 745, 467, 934, 845, 667, 311, 622
83	223	3045	11000100101	25	1023	223, 446, 892, 761, 499, 998, 973, 923, 823, 623
84	231	73	111011	99	31	231, 462, 924, 825, 627
85	235	3117	11001001111	83	1023	235, 470, 940, 857, 691, 359, 718, 413, 826, 629
86	237	3705	11111000101	75	341	237, 474, 948, 873, 723, 423, 846, 669, 315, 630
87	239	2527	10101010111	49	1023	239, 478, 956, 889, 755, 487, 974, 925, 827, 631
88	245	2305	10011000101	43	1023	245, 490, 980, 937, 851, 679, 335, 670, 317, 634
89	247	3103	11001000011	35	1023	247, 494, 988, 953, 883, 743, 463, 926, 829, 635
90	251	3375	11011111101	19	1023	251, 502, 1004, 985, 947, 871, 719, 415,830,637
91	253	2541	10101100001	11	93	253, 506, 1012, 1001, 979, 935,847,671,319,638
92	255	3601	11110000001	3	341	255,510,1020,1017,1011, 999, 975,927,831,639
93	341	0007	111	341	3	341, 682
94	343	3435	11100011101	85	1023	343, 686, 349, 698, 373, 746, 469, 938, 853, 683
95	347	2503	10101000011	149	1023	347, 694, 365, 730, 437, 874, 725, 427, 854, 685
96	351	3277	11010111111	21	341	351, 702, 381, 762, 501, 1002, 981, 939,855,687

Продолжение таблицы 3

№	Корень α^i	Код полинома	Полином	Корень сопряженного полинома	Период корней	Корни полинома (показатели степеней)
97	363	45	100101	165	31	363, 726, 429, 858, 693, 726, 429, 858, 693
98	367	2475	10100111101	41	1023	367, 734, 445, 890, 757, 491, 982, 941, 859, 695
99	375	2035	10000011101	69	341	375, 750, 477, 954, 885, 747, 471, 942, 861, 699
100	379	3067	11000110111	37	1023	379, 758, 493, 986, 949, 875, 727, 431, 862, 701
101	383	2605	10110000101	5	1023	383, 766, 509, 1018,1013,1003,983,943,863,703
102	439	3427	11100010111	73	1023	439, 878, 733, 443, 886, 749, 475, 950, 877, 731
103	447	3651	11110101001	9	341	447, 894, 765, 507, 1014,1005,987,951,879,735
104	479	2627	10110010111	17	1023	479, 958, 893, 763, 503, 1006,989,955,887,751
105	495	57	101111	33	31	495, 990, 957, 891, 759
106	511	2201	10010000001	1	1023	511,1022,1021,1019,1015,1007,991,959,895,767

Полиномы $h_{г3}(x)$ и $h_{г5}(x)$ вида (9), (10) представляются произведением двух полиномов-сомножителей $h_{ci}(x)$ десятой степени (см. табл. 3):

$$h_{г3}(x) = h_{c1}(x)\, h_{c2}(x) = h_2(x)\, h_9(x) = (x^{10}+x^3+x^2+x+1)\,(x^{10}+x^9+x^8+x^6+x^3+x^2+1), \quad (13)$$

$$h_{г5}(x) = h_{c1}(x)\, h_{c2}(x) = h_3(x)\, h_5(x) = (x^{10}+x^8+x^3+x^2+1)\,(x^{10}+x^7+x^5+x^3+x^2+x+1). \quad (14)$$

Проанализируем полином $h_{г3}(x)$. Для поля GF(2^{10}) корни полинома $h_2(x)$ являются 3-ми степенями корней полинома $h_{МП}(x) = x^{10}+x^3+1$ базисной МП, а корни $h_3(x)$ — 17-ми степенями его корней.

Алгоритм формирования полного перечня проверочных полиномов ГМВП основан на свойстве повторяемости соотношений между корнями проверочного полинома $h_{МП}(x)$ базисной МП и корнями полиномов-сомножителей $h_{ci}(x)$ проверочного полинома $h_г(x)$ [18].

В соответствии с (3) в поле GF(2^{10}) существует шестьдесят различных примитивных полиномов, которые могут выступать в качестве проверочных для базисных МП. Таким образом, для $i_{d1} = 3$ можно получить шестьдесят ГМВП с проверочными полиномами двадцатой степени, корни двух сомножителей которых являются 3-ми и 17-ми степенями корней полинома базисной МП.

В качестве примера сформируем проверочный полином ГМВП, основанной на МП с $h_{МП}(x) = h_{71}(x) = x^{10}+x^9+x^7+x^3+1$, корнем которого (с минимальной степенью) является элемент α^{179} (см. табл. 3).

Полиномы-сомножители для $h_г(x) = h_{c1}(x)\, h_{c2}(x)$ определяются следующим образом. Исходный полином $h_{МП}(x)$ имеет корень α^{179}. Тогда одним из корней $h_{c1}(x)$ должен быть элемент $(\alpha^{179})^3 = \alpha^{537}$, что соответствует полиному $h_{c1}(x) = h_{26}(x) = x^{10}+x^8+x^6+x^5+x^2+x+1$ с минимальным корнем α^{51}.

Полином $h_{c2}(x)$ должен иметь корень $(\alpha^{179})^{17} = \alpha^{3043 \bmod 1023} = \alpha^{997}$, что соответствует полиному $h_{c2}(x) = h_{76}(x) = x^{10}+x^9+x^8+x^7+x^5+x^4+1$ с корнем α^{191}.

Искомый проверочный полином для ГМВП

$$h_г(x) = h_{26}(x) h_{76}(x) = (x^{10}+x^8+x^6+x^5+x^2+x+1)(x^{10}+x^9+x^8+x^7+x^5+x^4+1). \quad (15)$$

При анализе полинома $h_{г5}(x)$ необходимо учитывать, что корни $h_{c1}(x)=h_3(x)$ являются 5-ми степенями корней $h_{МП}(x) = x^{10}+x^3+1$ базисной МП, а корни $h_{c2}(x) = h_5(x)$ — 9-ми степенями его корней. Таким образом, при индексе децимации ХП $i_{d2} = 5$ также можно сформировать 60 ГМВП с ЭЛС l_s=20.

Результаты вычислений для остальных примитивных полиномов поля GF(2^{10}) при индексах децимации $i_{d1} = 3$ и $i_{d2} = 5$ представлены в табл. 4.

Для получения ГМВП с ЭЛС l_s=40 необходимо выполнить децимацию ХП по индексам $i_{d3} = 7$ и $i_{d4} = 11$. Не приводя матричную форму записи ГМВП, представим только полученные проверочные полиномы 40-й степени в компактной записи (по убыванию степени):

$$h_{г7}=1100110111010010111001110100001100111010 1_2=31564563503165_8, \qquad (16)$$

$$h_{г11}=1011101101100101110111100011110100011001 1_2=31564563503165_8. \qquad (17)$$

Полиномы $h_{г7}(x)$, $h_{г11}(x)$ вида (16), (17) представляются произведением четырех полиномов-сомножителей $h_{ci}(x)$ десятой степени (см. табл. 3)

$$h_{г7}(x) = h_{c1}(x)\ldots h_{c4}(x) = h_4(x)h_{10}(x)h_{13}(x)\, h_{33}(x) = (x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+1)\times$$
$$\times(x^{10}+x^8+x^7+x^6+x^5+x^4+x^3+x+1)(x^{10}+x^8+x^5+x+1)(x^{10}+x^8+x^7+x^6+1), \qquad (18)$$

$$h_{г11}(x) = h_{c1}(x)\ldots h_{c4}(x) = h_6(x)h_7(x)h_{11}(x)\, h_{35}(x) = (x^{10}+x^5+x^4+x^2+1)\times$$
$$\times(x^{10}+x^6+x^5+x^3+x^2+x+1)(x^{10}+x^9+x^8+x^7+x^6+x^5+x^3+x+1)(x^{10}+x^9+x^8+x^6+x^2+x+1). \qquad (19)$$

Анализ полинома $h_{г7}(x)$ показал, что корни $h_{c1}(x) = h_4(x)$, $h_{c2}(x) = h_{10}(x)$, $h_{c3}(x) = h_{13}(x)$ и $h_{c4}(x) = h_{33}(x)$ являются соответственно 7, 19, 25 и 69-ми степенями корней полинома $h_{МП}(x) = x^{10}+x^3+1$ базисной МП.

Для полинома $h_{г11}(x)$ корни полиномов-сомножителей $h_{c1}(x) = h_6(x)$, $h_{c2}(x) = h_7(x)$, $h_{c3}(x) = h_{11}(x)$, $h_{c4}(x) = h_{35}(x)$ являются соответственно 11, 13, 21 и 73-ми степенями корней полинома $h_{МП}(x) = x^{10}+x^3+1$ базисной МП.

Всего можно получить 120 ГМВП с периодом N=1023 и проверочными полиномами 40-й степени. Результаты вычислений для остальных полиномов поля GF(2^{10}) при $i_{d3} = 7$ и $i_{d4} = 11$ приведены в табл. 4.

Для получения ГМВП с ЭЛС l_s=80 необходимо выполнить децимацию ХП по индексу $i_{d5} = 15$. Не приводя матричную форму записи ГМВП, представим компактную запись проверочного полинома 80-й степени:

$$h_{г15}=111001111111101001011110000000100001111000000000001000110001000 0$$
$$11001010011101100 1_2=717764570041700021420624731_8. \qquad (20)$$

Полином $h_{г15}(x)$ вида (20) представляется произведением восьми полиномов-сомножителей $h_{ci}(x)$ десятой степени (см. табл. 3):

$$h_{г15}(x) = h_{c1}(x)\ldots h_{c8}(x) = h_8(x)h_{12}(x)h_{14}(x)\, h_{15}(x)\, h_{37}(x)h_{40}(x)h_{42}(x)\, h_{60}(x) =$$
$$= (x^{10}+x^8+x^7+x^5+x^3+x+1)(x^{10}+x^4+x^3+x+1)(x^{10}+x^9+x^8+x^6+x^5+x^4+x^3+x+1)\times$$
$$\times(x^{10}+x^8+x^5+x^4+1)(x^{10}+x^8+x^3+x+1)(x^{10}+x^8+x^7+x^6+x^2+x+1)\times$$
$$\times(x^{10}+x^7+x^6+x^4+x^2+x+1)(x^{10}+x^7+x^6+x^5+x^3+x^2+1). \qquad (21)$$

Анализ $h_{г15}(x)$ показал, что корни полиномов $h_{c1}(x) = h_8(x)$, $h_{c2}(x) = h_{12}(x)$, $h_{c3}(x) = h_{14}(x)$, $h_{c4}(x) = h_{15}(x)$, $h_{c5}(x) = h_{37}(x)$, $h_{c6}(x) = h_{40}(x)$, $h_{c7}(x) = h_{42}(x)$ и $h_{c8}(x) = h_{60}(x)$ являются соответственно 15, 23, 27, 29, 77, 85, 89 и 147-ми степенями корней полинома $h_{МП}(x) = x^{10}+x^3+1$ базисной МП.

Всего можно получить 60 ГМВП с периодом N=1023 и проверочными полиномами 80-й степени. Результаты вычислений для остальных полиномов поля $GF(2^{10})$ при индексе децимации $i_{d5} = 15$ приведены в табл. 4.

Таблица 4

№	Корни $h_{МП}(x)$	i_{d1}=3, l_s=20		i_{d2}=5, l_s=20		i_{d3}=7, l_s=40				i_{d4}=11, l_s=40				i_{d5}=15, l_s=80							
		h_{c1}: α^3	h_{c2}: α^{17}	h_{c1}: α^5	h_{c2}: α^9	h_{c1}: α^7	h_{c2}: α^{19}	h_{c3}: α^{25}	h_{c4}: α^{69}	h_{c1}: α^{11}	h_{c2}: α^{13}	h_{c3}: α^{21}	h_{c4}: α^{73}	h_{c1}: α^{15}	h_{c2}: α^{23}	h_{c3}: α^{27}	h_{c4}: α^{29}	h_{c5}: α^{77}	h_{c6}: α^{85}	h_{c7}: α^{89}	h_{c8}: α^{147}
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1	α^1	α^3	α^{17}	α^1	α^9	α^7	α^{19}	α^{25}	α^{69}	α^{11}	α^{13}	α^{21}	α^{73}	α^{15}	α^{23}	α^{27}	α^{29}	α^{77}	α^{85}	α^{89}	α^{147}
2	α^5	α^{15}	α^{85}	α^{25}	α^{45}	α^{35}	α^{95}	125	171	55	17	105	347	75	115	57	73	11	181	367	447
3	α^7	21	119	35	63	49	41	175	111	77	91	147	511	105	37	189	179	55	167	223	3
4	13	39	221	17	117	91	247	85	15	121	149	69	379	51	173	351	175	253	41	49	111
5	17	51	41	85	147	119	53	181	75	187	221	171	109	255	59	183	379	121	205	245	87
6	19	57	53	95	171	41	173	439	9	77	247	123	91	117	347	3	79	55	37	167	375

Продолжение таблицы 4

№	Корни $h_{МП}(x)$	$i_{d1}=3$, $l_s=20$		$i_{d2}=5$, $l_s=20$		$i_{d3}=7$, $l_s=40$				$i_{d4}=11$, $l_s=40$				$i_{d5}=15$, $l_s=80$							
		h_{c1}: α^{3}	h_{c2}: α^{17}	h_{c1}: α^{5}	h_{c2}: α^{9}	h_{c1}: α^{7}	h_{c2}: α^{19}	h_{c3}: α^{25}	h_{c4}: α^{69}	h_{c1}: α^{11}	h_{c2}: α^{13}	h_{c3}: α^{21}	h_{c4}: α^{73}	h_{c1}: α^{15}	h_{c2}: α^{23}	h_{c3}: α^{27}	h_{c4}: α^{29}	h_{c5}: α^{77}	h_{c6}: α^{85}	h_{c7}: α^{89}	h_{c8}: α^{147}
7	23	69	59	115	207	37	347	127	105	253	173	111	41	171	35	219	221	187	157	1	39
8	25	75	181	125	39	175	439	103	351	77	85	27	89	375	127	117	347	55	79	179	189
9	29	87	379	73	21	179	79	347	189	253	175	51	71	219	221	63	157	187	109	47	171
10	35	105	167	175	237	245	205	379	87	11	119	447	383	27	151	123	511	77	61	23	15
11	37	111	235	151	213	13	383	239	447	187	47	39	125	87	245	255	25	121	19	7	69
12	41	123	215	205	87	125	47	1	63	55	43	375	251	207	383	21	83	11	13	73	57
13	43	9	439	215	27	181	115	13	207	187	95	63	35	45	479	69	7	121	149	379	183
14	47	105	127	235	237	149	479	19	87	11	115	447	181	27	29	123	85	77	247	91	15
15	49	147	29	245	183	343	125	101	39	55	251	3	127	447	13	75	115	11	73	53	21
16	53	159	47	37	375	215	511	151	147	121	107	45	25	111	49	51	5	253	235	103	237
17	59	75	383	157	39	235	49	71	351	77	511	27	215	375	167	117	43	55	223	17	189
18	61	183	7	83	75	347	17	251	117	253	103	9	173	159	95	39	343	187	35	157	63
19	71	213	23	107	255	95	101	47	159	55	223	117	17	21	83	447	13	11	115	181	207
20	73	219	109	347	105	511	91	89	123	121	379	255	107	9	41	237	71	253	49	235	351
21	79	237	5	91	123	83	239	119	21	187	1	159	101	69	107	87	245	121	25	479	45
22	83	159	35	251	375	89	85	29	147	121	7	45	59	111	439	51	173	253	175	71	237
23	85	255	205	181	447	167	37	79	375	253	41	351	49	63	157	159	109	187	1	101	219
24	89	45	245	367	57	223	167	179	3	253	49	237	235	39	1	171	47	187	101	95	159
25	91	69	25	119	207	251	43	167	105	253	5	111	191	171	47	219	101	187	125	343	39
26	95	117	37	439	351	205	59	149	45	11	53	207	119	147	89	15	91	77	151	61	213
27	101	189	347	191	111	59	7	479	255	11	73	75	53	123	85	213	247	77	89	151	27
28	103	213	91	7	255	109	221	35	159	55	79	117	179	21	53	447	367	11	119	383	207
29	107	21	115	47	63	439	191	235	111	77	23	147	85	105	251	189	17	55	127	79	3
30	109	117	251	49	351	479	25	245	45	11	83	207	115	147	215	15	23	77	29	247	213
31	115	171	157	127	3	151	89	247	27	121	59	87	205	351	175	9	41	253	71	5	51
32	119	171	125	167	3	29	215	61	27	121	25	87	479	351	235	9	191	253	103	173	51
33	125	375	79	103	51	379	149	7	183	11	181	57	367	213	247	147	89	77	91	511	123
34	127	351	71	247	15	239	367	53	57	187	157	219	1	183	379	45	205	121	107	25	255
35	149	447	239	221	159	5	71	41	51	77	151	15	61	189	179	375	167	55	43	251	105
36	151	87	19	239	21	17	223	43	189	253	235	51	103	219	101	63	125	187	95	35	171
37	157	375	223	71	51	19	245	107	183	11	383	57	13	213	61	147	215	77	23	85	123
38	167	351	103	61	15	73	13	83	57	187	125	219	343	183	19	45	479	121	7	59	255
39	173	15	511	59	45	47	109	157	171	55	179	105	43	75	119	57	239	11	383	13	447
40	175	27	61	379	69	101	1	109	219	55	167	189	223	57	239	207	383	11	83	115	75
41	179	51	191	511	147	115	83	383	75	187	101	171	95	255	25	183	19	121	479	149	87
42	181	63	1	79	189	61	151	91	213	121	205	183	245	237	71	111	49	253	5	191	9
43	191	123	89	479	87	157	35	343	63	55	347	375	37	207	181	21	53	11	367	239	57
44	205	207	13	1	219	103	235	5	237	77	215	213	29	3	223	105	251	55	17	347	117
45	215	45	149	13	57	79	127	17	3	253	439	237	175	39	343	171	35	187	221	109	159
46	221	189	43	41	111	25	107	205	255	11	239	75	83	123	511	213	61	77	215	29	27
47	223	237	173	23	123	53	73	115	21	187	343	159	221	69	7	87	149	121	59	205	45
48	235	27	247	19	69	221	343	95	219	55	127	189	79	57	73	207	181	11	53	119	75
49	239	219	95	43	105	85	23	215	123	121	19	255	7	9	191	237	103	253	439	175	351
50	245	447	73	101	159	173	103	191	51	77	29	15	247	189	17	375	127	55	347	37	105
51	247	183	107	53	75	43	179	37	117	253	71	9	5	159	109	39	1	187	47	125	63
52	251	111	175	29	213	367	181	73	447	187	35	39	157	87	149	255	59	121	379	107	69
53	343	3	179	173	9	107	379	59	69	11	367	21	239	15	91	27	151	77	511	215	147
54	347	9	49	89	27	383	119	367	207	187	109	63	47	45	205	69	107	121	245	19	183
55	367	39	101	179	117	23	61	511	15	121	245	69	19	51	5	351	235	253	191	439	111
56	379	57	83	109	171	191	5	49	9	77	61	123	23	117	43	3	223	55	251	127	375
57	383	63	343	223	189	247	29	23	213	121	479	183	149	237	103	111	439	253	173	41	9

Продолжение таблицы 4

№	Корни $h_{МП}(x)$	i_{d1}=3, l_s=20		i_{d2}=5, l_s=20		i_{d3}=7, l_s=40				i_{d4}=11, l_s=40				i_{d5}=15, l_s=80							
		h_{c1}: α^3	h_{c2}: α^{17}	h_{c1}: α^5	h_{c2}: α^9	h_{c1}: α^7	h_{c2}: α^{19}	h_{c3}: α^{25}	h_{c4}: α^{69}	h_{c1}: α^{11}	h_{c2}: α^{13}	h_{c3}: α^{21}	h_{c4}: α^{73}	h_{c1}: α^{15}	h_{c2}: α^{23}	h_{c3}: α^{27}	h_{c4}: α^{29}	h_{c5}: α^{77}	h_{c6}: α^{85}	h_{c7}: α^{89}	h_{c8}: α^{147}
58	439	147	151	149	183	1	157	221	39	55	37	3	167	447	367	75	119	11	239	83	21
59	479	207	367	343	219	71	175	173	237	77	89	213	151	3	79	105	37	55	179	43	117
60	511	255	479	383	447	127	251	223	375	253	191	351	439	63	125	159	95	187	343	221	219

В табл. 4 использованы следующие обозначения: во втором столбце — корни (далее показатели степени корней) примитивных полиномов $h_{МП}(x)$ базовых МП, в которых осуществляется децимация ХП по индексам i_{d1}—i_{d5}. В столбцах приведены корни (показатели степени корней) полиномов-сомножителей $h_{ci}(x)$ для каждого типа ГМВП, характеризующегося индексом децимации ХП и значением ЭЛС.

Например, требуется определить проверочный полином ГМВП с ЭЛС l_s=40 при индексе децимации i_{d4}=11, если в качестве базисной используется МП с полиномом, одним из корней которого является элемент α^{235}.

В табл. 4 базисная МП с α^{235} соответствует строке 48, в столбцах 11—14 которой для i_{d4}=11 приведены корни полиномов-сомножителей с наименьшими показателями степеней: α^{55}, α^{127}, α^{189}, α^{79}. Данным корням в табл. 3 соответствуют полиномы в двоичной записи h_{28}=11101101011, h_{59}=10011111111, h_{75}=10001100011, h_{38}=10011100111. Тогда проверочный полином ГМВП равен

$$h_{г11}(x) = h_{c1}(x)\ldots h_{c4}(x) = h_{28}(x)h_{59}(x)h_{75}(x)\,h_{38}(x) = (x^{10}+x^9+x^8+x^5+x^3+x+1)\times$$
$$\times(x^{10}+x^7+x^6+x^5+x^4+x^3+x^2+x+1)(x^{10}+x^6+x^5+x+1)\cdot(x^{10}+x^7+x^6+x^5+x^2+x+1). \quad (22)$$

В табл. 5 представлены данные, необходимые для формирования 60 ГМВП с заданной структурной скрытностью.

Таблица 5

Индекс i_{di} децимации ХП	ЭЛС ГМВП l_s	Число сомножителей $h_{ci}(x)$	Показатели степени корней $h_{ci}(x)$
3	20	2	3, 17
5	20	2	5, 9
7	40	4	7, 19, 25, 69
11	40	4	11, 13, 21, 73
15	80	8	15, 23, 27, 29, 77, 85, 89, 147

Таким образом, в статье получен полный перечень проверочных полиномов ГМВП с периодом N=1023, состоящий из 120 ГМВП с ЭЛС l_s=20, 120 с l_s=40 и 60 с l_s=80.

СПИСОК ЛИТЕРАТУРЫ

1. *Варакин Л. Е.* Системы связи с шумоподобными сигналами. М.: Радио и связь, 1985. 384 с.
2. *Ипатов В. П.* Широкополосные системы и кодовое разделение сигналов. Принципы и приложения. М.: Техносфера, 2007. 488 с.
3. *Alasmary W., Zhuang W.* Mobility impact in IEEE 802.11p infrastructureless vehicular networks // Ad Hoc Netw. 2010. DOI:10.1016/j.adhoc.2010.06.006.
4. *Калмыков В. В., Федоров И. Б., Юдачев С. С.* Системы сотовой и спутниковой связи. М.: Рудомино, 2010. 280 с.
5. CDMA: прошлое, настоящее, будущее / Под ред. *Л. Е. Варакина и Ю. С. Шинакова*. М.: МАС, 2003. 608 с.
6. *Levanon N., Mozeson E.* Radar signals. Chichester: John Wiley& Sons, 2005. 411p.
7. *Прозоров Д. Е.* Быстрый поиск дальномерных кодов, сформированных на М-последовательностях // Электросвязь. 2008. № 8. С. 48—51.

8. *Ипатов В. П.* Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992. 152 с.
9. *Golomb S. W.* Two-valued sequences with perfect periodic autocorrelation // IEEE Transact. on Aerospace and Electronic Systems. 1992. Vol. 28, N 2. March. P. 383—386.
10. *Golomb S. W., Gong G.* Signal Design for Good Correlation for Wireless Communication, Criptography and Radar. Cambridge University Press, 2005. 438 p.
11. *Lie-Liang Yang, Hanzo L.* Acquisition of m-sequences using recursive soft sequential estimation // Wireless Communications and Networking. 2003. Vol. 1. P. 683—687.
12. *Стельмашенко Б. Г., Тараненко П. Г.* Нелинейные псевдослучайные последовательности в широкополосных системах передачи информации // Зарубежная радиоэлектроника. 1988. № 9. С. 76—82.
13. *Прозоров Д. Е., Смирнов А. В., Баланов М. Ю.* Алгоритм быстрой кодовой синхронизации шумоподобных сигналов, построенных на последовательностях повышенной структурной сложности // Вестн. РГРТУ (Рязань). Сер. Радиотехника, радиолокация и системы связи. 2015. № 1(51). С. 3—9.
14. *Кренгель Е. И.* О числе псевдослучайных последовательностей Гордона, Милза, Велча // Техника средств связи. Сер. ТРС. 1979. Вып. 3. С. 17—30.
15. *Мешковский К. А., Кренгель Е. И.* Генерация псевдослучайных последовательностей Гордона, Милза, Велча // Радиотехника. 1998. № 5. С. 25—28.
16. *Юдачев С. С., Калмыков В. В.* Ансамбли последовательностей GMW для систем с кодовым разделением каналов // Наука и образование: электронное научно-техническое издание. 2012. № 1.
17. *Стародубцев В. Г.* Алгоритм формирования последовательностей Гордона—Миллса—Велча // Изв. вузов. Приборостроение. 2012. Т. 55, № 7. С. 5—9.
18. *Стародубцев В. Г.* Проверочные полиномы последовательностей Гордона—Миллса—Велча // Изв. вузов. Приборостроение. 2013. Т. 56, № 12. С. 7—14.
19. *Стародубцев В. Г.* Формирование последовательностей Гордона—Миллса—Велча на основе регистров сдвига // Изв. вузов. Приборостроение. 2015. Т. 58, № 6. С. 451—457.
20. *Стародубцев В. Г., Чернявских А. Е.* Формирование троичных последовательностей Гордона—Миллса—Велча на основе регистров сдвига // Изв. вузов. Приборостроение. 2016. Т. 59, № 3. С. 202—210.
21. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. М.: Мир, 1976. 594 с.

Сведения об авторах

Виктор Геннадьевич Стародубцев — канд. техн. наук, доцент; ВКА им. А. Ф. Можайского, кафедра технологий и средств комплексной обработки и передачи информации в АСУ; Университет ИТМО, кафедрой беспроводных телекоммуникаций; E-mail: vgstarod@mail.ru

Антон Михайлович Попов — ВКА им. А. Ф. Можайского, кафедра технологий и средств комплексной обработки и передачи информации в АСУ; слушатель; E-mail: antony57rus@gmail.com

Рекомендована кафедрой беспроводных телекоммуникаций НИУ ИТМО

Поступила в редакцию 14.10.16 г.

Ссылка для цитирования: *Стародубцев В. Г., Попов А. М.* Последовательности Гордона—Миллса—Велча с периодом N=1023 // Изв. вузов. Приборостроение. 2017. Т. 60, № 4. С. 318—330.

GORDON—MILLS—WELCH SEQUENCES OF PERIOD *N* = 1023

V. G. Starodubtsev, A. M. Popov

A. F. Mozhaisky Military State Academy, 197198, St. Petersburg, Russia
E-mail: vgstarod@mail.ru

A full list of testing polynomials for Gordon—Mills—Welch sequences of period *N* = 1023 are derived on the basis of a developed algorithm of forming data sequences. The principle dissimilarity from sequences with a smaller period is the possibility to create several GMW-sequences with different equivalent linear complexity (ELC) determined as the degree of testing polynomial $h_{GMW}(x)$ for each basic M-sequence (MS) with the primitive testing polynomial $h_{MS}(x)$. This is a consequence of existence of six primitive polynomials in the finite field of GF(2^5), in contrast to the fields of GF(2^3) and GF(2^4) with two primitive polynomials in each. For each of the six MS of period N=31 acting as a characteristic sequence for MS matrix representation of period N=1023, it is possible to use the other five different MS to form five different GMW-sequences. It is shown that on the base of every MS with the period N=1023 it is possible to build five GMW-sequences. One of the GMW-sequences has a testing polynomial of the eightieth degree, two sequences — polynomials of fortieth degree, and two sequences — polynomials of the twentieth degree.

Keywords: sequence of composite period, finite fields, indivisible and primitive polynomials, equivalent linear complexity

Data on authors

Victor G. Starodubtsev — PhD, Associate Professor; A. F. Mozhaisky Military State Academy, Department of Technologies and Means of Complex Processing and Transmission of Information in ACS; ITMO University, Department of Wireless Telecommunications; E-mail: vgstarod@mail.ru

Anton M. Popov — A. F. Mozhaisky Military State Academy, Department of Technologies and Means of Complex Processing and Transmission of Information in ACS; Student; E-mail: antony57rus@gmail.com

For citation: *Starodubtsev V. G., Popov A. M.* Gordon—Mills—Welch sequences of period N = 1023 // Journal of Instrument Engineering. 2017. Vol. 60, N 4. P. 318—330 (in Russian).

DOI: 10.17586/0021-3454-2017-60-4-318-330