УДК 519.725
DOI: 10.17586/0021-3454-2021-64-1-32-39

ФОРМИРОВАНИЕ ПРЕДПОЧТИТЕЛЬНЫХ ПАР ГМВ-ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ПЕРИОДОМ N=511 ДЛЯ СИСТЕМ ПЕРЕДАЧИ ЦИФРОВОЙ ИНФОРМАЦИИ

В. Г. СТАРОДУБЦЕВ

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

На основании анализа периодических взаимно корреляционных функций М-последовательностей (МП) и последовательностей Гордона — Миллса — Велча (ГМВП) с периодом N=511 определен порядок формирования предпочтительных пар ГМВП. М- и ГМВ-последовательности с периодом N=511 строятся в конечных полях GF(2^S) при S = 9. Применение предпочтительных пар ГМВП в системах передачи цифровой информации определяется их более высокой по сравнению с МП структурной скрытностью, характеризуемой эквивалентной линейной сложностью, численно равной степени проверочных полиномов, на основании которых формируются данные последовательности. Показано, что предпочтительные пары ГМВП формируются на основе предпочтительных пар МП, при этом каждая МП выступает в качестве базисной последовательности при синтезе соответствующей ГМВП. Результаты по формированию предпочтительных пар ГМВП с периодом N=511 могут найти применение в помехозащищенных системах передачи цифровой информации, к которым предъявляются повышенные требования по конфиденциальности и скрытности, а также при синтезе производных систем псевдослучайных последовательностей, которые могут быть сформированы в расширенных конечных полях.

Ключевые слова: *М-последовательности, ГМВ-последовательности, предпочтительные пары, корреляционная функция, структурная скрытность, примитивные полиномы, конечные поля*

Широкое применение псевдослучайных последовательностей (ПСП) с заданными корреляционными и структурными свойствами при формировании сигналов с расширенным спектром (СРС) в современных системах передачи цифровой информации (СПЦИ) обусловлено постоянно возрастающими требованиями по обеспечению достоверности передачи информации в системах управления, связи и навигации [1—4].

В силу простоты формирования в качестве ПСП часто используются М-последовательности (МП), предпочтительные пары (ПП) МП, а также формируемые на основе ПП МП последовательности Голда, последовательности малого и большого множеств Касами, а также ГМВ-последовательности [5—7]. При этом ГМВ-последовательности, так же как и МП, обладают двухуровневой периодической автокорреляционной функцией (ПАКФ), но характеризуются более высокой структурной скрытностью. С увеличением периода последовательности выигрыш по данному показателю возрастает [8, 9].

Вопросам синтеза ПСП и пар ПСП, которые могут быть использованы для формирования производных множеств последовательностей с хорошими взаимно корреляционными и структурными свойствами, посвящено множество публикаций как в России, так и за рубежом [10—14]. Так, в работе [10] предложен новый класс пары дискретных последовательностей, который можно рассматривать как особый класс несогласованных фильтрующих последовательностей. В [11, 12] основное внимание уделено повышению структурной скрытности формируемых последовательностей как за счет использования манипулирующих кодов, так и за счет применения специальных нелинейных функций. В [13] проведен анализ последовательностей

с локально оптимальными корреляционными свойствами, так называемых последовательностей с нулевой зоной корреляции, которым в последнее время уделяется большое внимание. Алгоритм формирования ПП ГМВП для периодов N=63 и N=255 разработан в [14]. Показано, что ПП ГМВП формируются на основе ПП МП и характеризуются более высокой эквивалентной линейной сложностью (ЭЛС), что определяет предпочтительность их применения в СПЦИ, к которым предъявляются повышенные требования по конфиденциальности. Данный алгоритм может быть использован для формирования ПП ГМВП с более длинным периодом.

Цель настоящей статьи — определение предпочтительных пар ГМВП с периодом N=511.

Двоичные ГМВП формируются в конечных полях с двойным расширением $GF(2^S)$= $= GF[(2^m)^n]$ на основе М-последовательностей, которые выступают в качестве базисных [2, 7, 15].

ЭЛС двоичных ГМВП определяется выражением [2, 8]

$$l_s = mn^{g(r)}, \tag{1}$$

где r — натуральное число, взаимно простое с порядком мультипликативной группы поля $GF(2^m)$, равным $2^m - 1$; $g(r)$ — количество единиц в двоичном представлении числа r.

Предпочтительные пары МП характеризуются тем, что максимальное значение модуля периодической взаимно корреляционной функции (ПВКФ) не превышает величины

$$p(S) = 1+2^{](S+2)/2[}, \tag{2}$$

где $]x[$ — целая часть вещественного числа x [2, 5, 14].

Для двоичных МП ПВКФ $R_{jk}(\tau)$ определяется выражением [6, 16, 17]

$$R_{jk}(\tau) = N - 2B(\tau), \tag{3}$$

где $B(\tau)$ — число несовпадающих позиций в $МП_j$ и $МП_k$ при различных циклических сдвигах τ.

Коэффициент корреляции $b_{jk}(\tau)$ определяется путем нормировки функции корреляции:

$$b_{jk}(\tau) = R_{jk}(\tau) / N. \tag{4}$$

ПВКФ ПП МП с периодом N=511 является трехуровневой и принимает следующие ненормированные значения [2, 5]:

$$R_{jk}(\tau) = \{-p(S), -1, p(S) -2\}. \tag{5}$$

Значения ПВКФ ПП МП представлены в табл. 1, где также указано количество ее значений n_i для каждого уровня. Для сравнения в таблице приведены аналогичные значения параметров для периода N=1023.

Таблица 1

Период МП	R_1 / b_1	n_1	R_2 / b_2	n_2	R_3 / b_3	n_3	$\lvert R_{\max}\rvert$ / $\lvert b_{\max}\rvert$
511	–33	120	–1	255	31	136	33
	–0,06		–0,002		0,06		0,06
1023	–65	120	–1	767	63	136	65
	–0,06		–0,001		0,06		0,06

Определение ПП МП для периода N=511 производится в конечном поле $GF(2^9)$ с неприводимым полиномом $h_1(x) = x^9+x^4+1$.

Формирование МП с периодом N=511 выполняется в соответствии с проверочными полиномами, представленными в табл. 2. Данные полиномы являются неприводимыми в конечном поле $GF(2^9)$ [18]. В графах 1, 4, 7 таблицы приведены корни (минимальные показатели степени корней) прямого и сопряженного полиномов; в графах 2, 5, 8 — коэффициенты полиномов по убыванию степени формальной переменной x. Например, полиному $h_5(x)=x^9+x^8+x^5+x^4+1$ соответствует запись 1100110001. В остальных графах указаны периоды последовательностей, формируемых с помощью данных полиномов. Здесь и в дальнейшем нижний индекс в обозначении неприводимого полинома $h_i(x)$ соответствует показателю степени корня α^i данного полинома.

Таблица 2

α^i в $h(x)$/ α^j в $h^*(x)$	Полином $h_i(x)=x^9+\ldots+1$	Период	α^i в $h(x)$/ α^j в $h^*(x)$	Полином $h_i(x)=x^9+\ldots+1$	Период	α^i в $h(x)$/ α^j в $h^*(x)$	Полином $h_i(x)=x^9+\ldots+1$	Период
1	2	3	4	5	6	7	8	9
α^1 /α^{255}	1000010001	511	43/117	1111001011	511	103/51	1010101111	511
α^3 /α^{127}	1001011001	511	45/93	1001111101	511	107/83	1010100011	511
5/191	1100110001	511	47/29	1101011011	511	109/75	1101111111	511
7/63	1010011001	73	51/103	1111010101	511	111/25	1100011111	511
9/223	1100010011	511	53/87	1010010101	511	117/43	1101001111	511
11/125	1000101101	511	55/57	1010111101	511	119/35	1000000011	73
13/95	1001110111	511	57/55	1011110101	511	123/19	1010000111	511
15/31	1101100001	511	59/39	1011001111	511	125/11	1011010001	511
17/239	1011011011	511	61/23	1001011111	511	127/3	1001101001	511
19/123	1110000101	511	63/7	1001100101	73	171/85	1110110101	511
21/175	1000010111	73	73/219	1011	7	175/21	1110100001	73
23/61	1111101001	511	75/109	1111111011	511	183/41	1100111011	511
25/111	1111100011	511	77/91	1101001001	73	187/37	1111011001	511
27/79	1110001111	511	79/27	1111000111	511	191/5	1000110011	511
29/47	1101101011	511	83/107	1100010101	511	219/73	1101	7
31/15	1000011011	511	85/171	1010110111	511	223/9	1100100011	511
35/119	1100000001	73	87/53	1010100101	511	239/17	1101101101	511
37/187	1001101111	511	91/77	1001001011	73	255/1	1000100001	511
39/59	1111001101	511	93/45	1011111001	511			
41/183	1101110011	511	95/13	1110111001	511			

В поле GF(2^9) имеется 48 примитивных полиномов, с помощью которых можно сформировать 48 различных МП. Анализ ПВКФ различных пар МП показал, что можно выделить 16 типов ПВКФ, характеристики которых приведены в табл. 3. Вычисления проводились для $МП_1$ с полиномом $h_1(x)=x^9+x^4+1$ и $МП_i$, которые задавались остальными примитивными полиномами $h_i(x)$.

Таблица 3

Тип ПВКФ	Полиномы $h_i(x)$ при i, равном	Значения (число значений на периоде) ПВКФ $МП_1$ и $МП_i$
1	3, 5, 13, 17, 19, 27, 31, 47, 59, 87, 103, 171	–33(120), –1(255), 31(136)
2	9, 57,	–65(28), –1(447), 63(36)
3	11, 23, 25, 43, 93, 107, 109	–65(1), –33(108), –1(285), 31(108), 63(9)
4	15, 239	–49(3), –41(27), –33(36), –25(18), –17(63), –9(54), –1(72), 7(100), 15(45), 23(39), 31(18), 39(18), 47(9), 63(9)
5	29, 53, 79, 83, 123	–49(12), –33(54), –17(117), –1(147), 15(99), 31(54), 47(27), 79(1)
6	37, 183	–33(54), –17(135), –1(162), 15(99), 31(27), 47(21), 63(9), 79(1), 95(3)
7	39, 95	–65(1), –49(3), –33(72), –17(108), –1(144), 15(99), 31(54), 47(30)
8	41, 187	–113(1), –49(9), –33(63), –17(99), –1(138), 15(138), 31(45), 47(9), 63(9)
9	45, 125	–49(12), –33(81), –17(63), –1(153), 15(138), 31(37), 47(27)
10	51, 191	–73(3), –41(9), –33(45), –25(27), –17(54), –9(81), –1(81), 7(82), 15(36), 23(27), 31(9), 39(27), 47(30)
11	55, 223	–41(18), –33(27), –25(36), –17(63), –9(72), –1(99), 7(72), 15(36), 23(27), 31(9), 39(27), 47(21), 87(3), 103(1)
12	61, 111,	–113(1), –49(9), –33(54), –17(117), –1(147), 15(102), 31(54), 47(27)
13	75	–33(54), –17(162), –1(108), 15(108), 31(55), 47(18), 63(3), 95(3)
14	85, 127	–49(18), –33(27), –25(48), –17(45), –9(90), –1(57), 7(64), 15(72), 23(36), 31(27), 47(9), 55(18)
15	117	–113(1), –49(3), –33(63), –17(135), –1(108), 15(108), 31(81), 47(9), 63(3)
16	255	–45(3), –41(9), –37(18), –33(36), –29(18), –25(9), –21(27), –17(27), –13(27), –9(36), –5(19), –1(18), 3(45), 7(27), 11(18), 15(45), 19(18), 23(21), 27(45), 31(9), 35(9), 39(18), 43(9)

При выборе произвольной МП с полиномом $h_i(x)$ для нахождения полиномов, задающих МП с определенным типом ПВКФ, необходимо индексы соответствующих полиномов умножить на индекс i по mod 511. Например, МП с полиномом $h_{29}(x)$ будет иметь ПВКФ 8-го типа с двумя МП, задаваемыми полиномами $h_{\text{МП1}}(x) = h_{29\times41\text{mod}511}(x)=h_{117}(x)$ и $h_{\text{МП2}}(x) = h_{29\times187\text{mod}511}(x) = h_{103}(x)$. При вычислениях выбирался наименьший показатель степени p-сопряженных корней полиномов.

Анализ корреляционных свойств МП показал, что выражению (5) удовлетворяет только ПВКФ 1-го типа. Таким образом, в конечном поле $GF(2^9)$ существует 12 ПП МП для $МП_1$, задаваемой полиномом $h_1(x)$. Соответственно для каждой из 48 МП может быть сформировано по 12 предпочтительных пар. Вид ПВКФ ПП МП на примере МП с полиномами $h_1(x)$ и $h_{13}(x)$ показан на рис. 1.

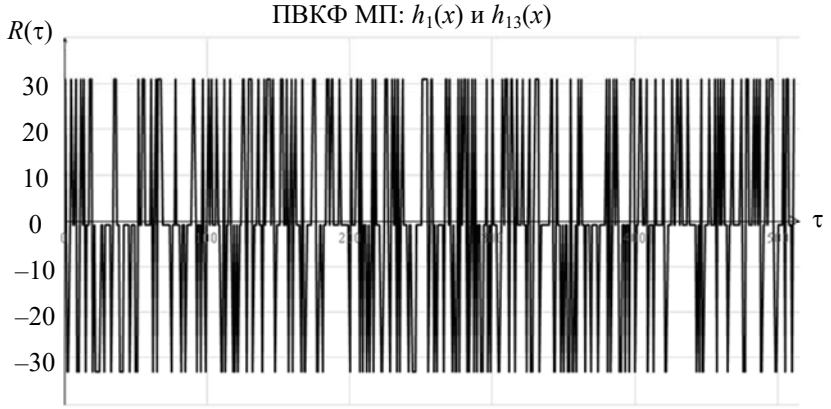

Рис. 1

В работе [14] показано, что ПП ГМВП формируются на основе ПП МП. При этом МП выступают в качестве базисных последовательностей при формировании соответствующих ГМВП.

Если в качестве базисной МП с периодом N=511 выступает МП с проверочным полиномом $h_1(x)=x^9+x^4+1$, то проверочный полином $h_{\Gamma1}(x)$ ГМВП равен произведению трех сомножителей — примитивных полиномов [7]:

$$h_{\Gamma1}(x) = h_{c1}(x)h_{c2}(x)h_{c3}(x) = h_3(x)h_5(x)h_{17}(x). \quad (6)$$

При этом ЭЛС ГМВП будет в три раза больше и равна l_s=27.

В общем случае проверочный полином $h_{\Gamma i}(x)$ ГМВП с периодом N=511 определяется выражением [7]

$$h_{\Gamma i}(x) = h_{3i}(x)h_{5i}(x)h_{17i}(x), \quad (7)$$

где индексы вычисляются по mod 511.

Например, если базисная МП задается проверочным полиномом $h_{19}(x)=x^9+x^8+x^7+x^2+1$ (см. табл. 2), то проверочный полином ГМВП будет иметь вид

$$h_{\Gamma19}(x) = h_{57}(x)h_{95}(x)h_{323}(x) = h_{57}(x)h_{95}(x)h_{29}(x) =$$
$$= (x^9+x^7+x^6+x^5+x^4+x^2+1)(x^9+x^8+x^7+x^5+x^4+x^3+1)(x^9+x^8+x^6+x^5+x^3+x+1). \quad (8)$$

Полином $h_{323}(x)$ из выражения (8) отсутствует в табл. 2, поэтому он заменяется на равный ему полином с индексом, соответствующим наименьшему значению показателя степени среди всех p-сопряженных элементов, являющихся корнями данного полинома.

При определении ПП ГМВП в качестве базисных МП будем рассматривать последовательности, образующие ПП с $МП_1$, т.е. характеризующиеся ПВКФ 1-го типа (табл. 3). Вычисления ПВКФ производятся для $ГМВП_1$ и $ГМВП_i$ с полиномами $h_{\Gamma1}(x)$ и $h_{\Gamma i}(x)$, определяемыми аналогично (8). Вид полиномов-сомножителей $h_{cj}(x)$ полинома $h_{\Gamma i}(x)$ для ПП МП представлен в табл. 4. Индекс i в $h_{\Gamma i}(x)$ соответствует индексу полинома, задающего базисную МП для данной ГМВП. Результаты вычислений ПВКФ $ГМВП_1$ и $ГМВП_i$ приведены в табл. 5.

Таблица 4

$h_{\Gamma i}(x)$	$h_{c1}(x)$	$h_{c2}(x)$	$h_{c3}(x)$	$h_{\Gamma i}(x)$	$h_{c1}(x)$	$h_{c2}(x)$	$h_{c3}(x)$	$h_{\Gamma i}(x)$	$h_{c1}(x)$	$h_{c2}(x)$	$h_{c3}(x)$
$h_{\Gamma 1}(x)$	$h_3(x)$	$h_5(x)$	$h_{17}(x)$	$h_{\Gamma 19}(x)$	57	95	29	$h_{\Gamma 87}(x)$	11	123	79
$h_{\Gamma 3}(x)$	9	15	51	$h_{\Gamma 27}(x)$	37	29	95	$h_{\Gamma 103}(x)$	107	1	109
$h_{\Gamma 5}(x)$	15	25	85	$h_{\Gamma 31}(x)$	93	109	1	$h_{\Gamma 171}(x)$	1	43	11
$h_{\Gamma 13}(x)$	39	9	183	$h_{\Gamma 47}(x)$	53	183	9				
$h_{\Gamma 17}(x)$	51	85	25	$h_{\Gamma 59}(x)$	43	79	123				

Таблица 5

$h_{\Gamma i}(x)$	Тип ПВКФ	Число n значений ПВКФ ГМВП$_1$ и ГМВП$_i$ при $h_{\Gamma 1}(x)= h_3(x)h_5(x)h_{17}(x)$, при $R(\tau)$; $b(\tau)$													
		55; 0,11	47; 0,09	39; 0,08	31; 0,06	23; 0,05	15; 0,03	7; 0,01	–1; 0,00	–9; –0,02	–17; –0,03	–25; –0,05	–33; –0,06	–41; –0,08	–49; –0,1
$h_{\Gamma 3}(x)$	1		27		46		108		174		90		39		27
$h_{\Gamma 5}(x)$	1		27		46		108		174		90		39		27
13	4	9	18	9	28	36	54	63	57	99	45	54	12	18	9
17	1		27		46		108		174		90		39		27
19	3		18	9	37	27	90	63	57	54	54	54	21	9	18
27	3		18	9	37	27	90	63	57	54	54	54	21	9	18
31	1		27		46		108		174		90		39		27
47	2		18	9	19	63	72	63	84	18	45	54	48	9	9
59	4	9	18	9	28	36	54	63	57	99	45	54	12	18	9
87	2		18	9	19	63	72	63	84	18	45	54	48	9	9
103	1		27		46		108		174		90		39		27
171	1		27		46		108		174		90		39		27

Анализ ПВКФ пар ГМВП, сформированных на основе ПП МП, показал, что можно выделить четыре типа корреляционных функций, для трех из них максимальное значение модуля не превышает

$$p_{\Gamma}(S) = 1+3\cdot 2^{(S-1)/2}. \quad (9)$$

Значения ПВКФ первых трех типов лежат в интервале от –49 до +47. Значения ПВКФ 4-го типа выходят за рамки данного интервала.

Для примера на рис. 2 показана ПВКФ 1-го типа, которая является 7-уровневой и принимает следующие значения:

$$R(\tau) \in \{-49(27), -33(39), -17(90), -1(174), +15(108), +31(46), +47(27)\}. \quad (10)$$

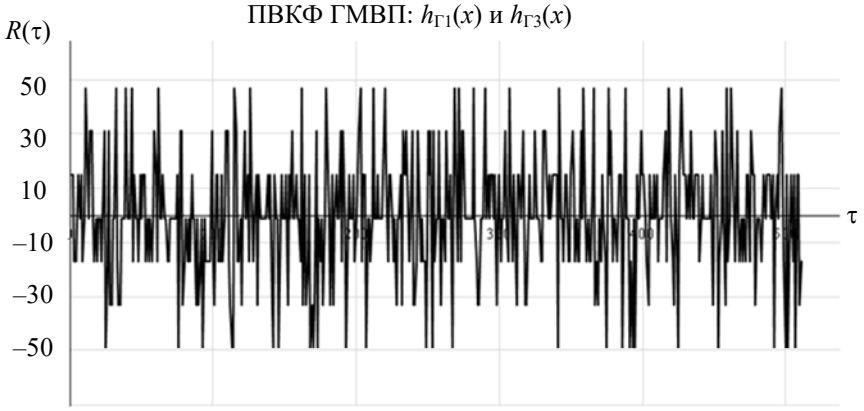

Рис. 2

ПВКФ 2-го типа является 13-уровневой и принимает следующие значения:

$$R(\tau) \in \{-49(9), -41(9), -33(48), -25(54), -17(45), -9(18), -1(84), 7(63), 15(72), 23(63), +31(19), 39(9), +47(18)\}. \quad (11)$$

ПВКФ 3-го типа также является 13-уровневой, но имеет другое распределение числа значений:

$$R(\tau) \in \{-49(18), -41(9), -33(21), -25(54), -17(54), -9(54), -1(57), 7(63),$$
$$15(90), 23(27), +31(37), 39(9), +47(18)\}. \quad (12)$$

Таким образом, для каждого из 48 примитивных полиномов в конечном поле $GF(2^9)$ и соответственно для каждой из 48 ГМВП с периодом N=511 может быть сформировано по десять предпочтительных пар, удовлетворяющих выражению (9) и включающих шесть ПП с ПВКФ 1-го типа вида (10), две ПП с ПВКФ 2-го типа (11) и две ПП с ПВКФ 3-го типа (12).

Все ПП ГМВП формируются на основе ПП МП, ПВКФ которых является 3-уровневой. В отличие от периода N=255, отдельные ПП МП не образуют ПП ГМВП (см. ПВКФ 4-го типа в табл. 5).

ПВКФ всех ПП ГМВП удовлетворяет выражению (9) и может быть как 7-уровневой, так и 13-уровневой. При этом максимальное значение модуля ПВКФ не превышает величины $|R(\tau)| \le 49$.

Структурная скрытность ПП ГМВП в три раза выше, чем у ПП МП.

Полученные результаты могут быть использованы при формировании СРС в СПЦИ, к которым предъявляются повышенные требования по конфиденциальности и помехозащищенности. Также на основе ПП ГМВП возможно формирование производных множеств последовательностей с хорошими корреляционными и структурными свойствами.

СПИСОК ЛИТЕРАТУРЫ

1. *Ипатов В. П.* Широкополосные системы и кодовое разделение сигналов. Принципы и приложения / Пер. с англ.; Под ред. *В. П. Ипатова*. М.: Техносфера. 2007. 488 с.
2. *Golomb S.W., Gong G.* Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar. Cambridge Univ. Press, 2005. 438 p.
3. CDMA: прошлое, настоящее, будущее / Под ред. *Л. Е. Варакина* и *Ю. С. Шинакова*. М.: МАС, 2003. 608 с.
4. *Вишневский В. М., Ляхов А. И., Портной С. Л., Шахнович И. В.* Широкополосные беспроводные сети передачи информации. М.: Техносфера, 2005. 592 с.
5. *Ипатов В.П.* Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992. 152 с.
6. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение: Пер. с англ. М.: Изд. дом „Вильямс“, 2003. 1104 с.
7. *Стародубцев В. Г.* Метод синтеза последовательностей Гордона — Миллса — Велча для систем передачи дискретной информации // Радиотехника и электроника. 2020. Т. 65, № 2. С. 169—173.
8. *Chung H. B., No J. S.* Linear span of extended sequences and cascaded GMW sequences // IEEE Trans. on Information Theory. 1999. Vol. 45, N 6. P. 2060—2065.
9. *Rizomiliotis P., Kalouptsidis N.* Results on the nonlinear span of binary sequences // IEEE Trans. on Information Theory. 2005. Vol. IT—51. P. 1555—1563.
10. *Xiumin Shen, Yanguo Jia, Xiaofei Song.* Constructions of binary sequence pairs of period 3 p with optimal three-level correlation // IEEE Communications Letters. 2017. Vol. 21, N 10. P. 2150—2153.
11. *Tsankov T., Trifonov T., Staneva L.* An algorithm for synthesis of phase manipulated signals with high structural complexity // J. Scientific & Applied Research. 2013. Vol. 4. P. 80—87.
12. *Coulter R. S., Mesnager S.* Bent functions from involutions over $F(2^n)$ // IEEE Trans. on Information Theory. 2018. Vol. 64, N 4. P. 2979—2986.
13. *Popović B. M.* Optimum sets of interference–free sequences with zero autocorrelation zones // IEEE Trans. on Information Theory. 2018. Vol. 64, N 4. P. 2876—2882.
14. *Стародубцев В. Г., Осадчая Я. В.* Предпочтительные пары ГМВ-последовательностей для систем передачи цифровой информации // Изв. вузов. Приборостроение. 2019. Т. 62, № 7. С. 610—620.

15. *No Jong–Seon.* Generalization of GMW sequences and No sequences // IEEE Trans. on Information Theory. 1996. Vol. 42, N 1. P. 260—262.

16. *Tao Zhang, Shuxing Li, Tao Feng, Gennian Ge.* Some new results on the cross correlation of m–sequences// IEEE Trans. on Information Theory. 2014. Vol. 60, N 5. P. 3062—3068.

17. *Zhengchun Zhou, Tor Helleseth, Udaya Parampalli.* A family of polyphase sequences with asymptotically optimal correlation // IEEE Trans. on Information Theory. 2018. Vol. 64, N 4. P. 2896—2900.

18. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки / Пер. с англ.; Под ред. *Р. Л. Добрушина* и *С. И. Самойленко*. М.: Мир, 1976. 594 с.

Сведения об авторе

Виктор Геннадьевич Стародубцев — канд. техн. наук, доцент; ВКА им. А. Ф. Можайского, кафедра технологий и средств автоматизации обработки и анализа информации космических средств; Университет ИТМО; E-mail: vgstarod@mail.ru

Поступила в редакцию
26.08. 2020 г.

Ссылка для цитирования: *Стародубцев В. Г.* Формирование предпочтительных пар ГМВ-последовательностей с периодом N=511 для систем передачи цифровой информации // Изв. вузов. Приборостроение. 2021. Т. 64, № 1. С. 32—39.

FORMATION OF PREFERRED PAIRS OF GMB-SEQUENCES WITH THE PERIOD *N*=511 FOR DIGITAL INFORMATION TRANSFER SYSTEMS

V. G. Starodubtsev

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

The order of formation of preferred pairs of Gordon–Mills–Welch sequences (GMWS) is determined based on the analysis of periodic cross-correlation functions (PCCF) of M-sequences (MS) and GMWS with the period *N*=511. MS and GMWS with the period *N*=511 are constructed in the finite fields GF(2S) at *S* = 9. Application of preferred pairs of GMWS in digital information transmission systems (DITS) is determined by their higher structural secrecy as compared to MS, characterized by an equivalent linear complexity (ELC), numerically equal to the degree of verification polynomials used as the base for sequence data formation. The preferred pairs of GMWS are shown to be formed on the basis of preferred pairs of MS, and each MS acts as a basic sequence in the synthesis of the corresponding GMWS. It is supposed that the results on formation of preferred pairs of GMWS with the period of *N*=511 can be used in noise protected digital information transmission systems with increased requirements for confidentiality and secrecy, as well as in the synthesis of derived systems of pseudorandom sequences that can be formed in extended finite fields.

Keywords: M-sequences, GMW-sequences, preferred pairs, correlation function, structural secrecy, primitive polynomials, finite fields

REFERENCES

1. Ipatov V.P. *Spread Spectrum and CDMA. Principles and Applications*, Wiley, 2005, 400 p.
2. Golomb S.W., Gong G. *Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar*, Cambridge University Press, 2005, 438 p.
3. Varakin L.E. and Shinakov Yu.S., ed., *CDMA: proshloe, nastoyashchee, budushchee* (CDMA: Past, Present, Future), Moscow, 2003, 608 p. (in Russ.)
4. Vishnevskij V.M., Lyahov A.I., Portnoj S.L., Shahnovich I.V. *Shirokopolosnye besprovodnye seti peredachi informacii* (Broadband Wireless Data Transmission Network), Moscow, 2005, 592 p. (in Russ.)
5. Ipatov V.P. *Periodicheskie diskretnye signaly s optimal'nymi korrelyacionnymi svojstvami* (Periodic Discrete Signals with Optimum Correlation Properties), Moscow, 1992, 152 p. (In Russ.).
6. Sklar B. *Digital Communications: Fundamentals and Applications*, Prentice Hall, 2001, 1079 p.
7. Starodubtsev V.G. *Journal of Communications Technology and Electronics*, 2020, no. 2(65), pp. 155–159.
8. Chung H.B., No J.S. *IEEE Trans. on Information Theory*, 1999, no. 6(45), pp. 2060–2065.
9. Rizomiliotis P., Kalouptsidis N. *IEEE Trans. on Information Theory*, 2005, vol. IT–51, pp. 1555–1563.
10. Xiumin Shen, Yanguo Jia, Xiaofei Song. *IEEE Communications Letters*, 2017, no. 10(21), pp. 2150–2153.

11. Tsankov T., Trifonov T., Staneva L. *Journal Scientific & Applied Research*, 2013, vol. 4, pp. 80–87.
12. Coulter R.S., Mesnager S. *IEEE Trans. on Information Theory*, 2018, no. 4(64), pp. 2979–2986.
13. Popović B.M. *IEEE Trans. on Information Theory*, 2018, no. 4(64), pp. 2876–2882.
14. Starodubtsev V.G., Osadchaya Ya.V. *Journal of Instrument Engineering*, 2019, no. 7(62), pp. 610–620. (in Russ.)
15. No Jong-Seon. *IEEE Trans. on Information Theory*, 1996, no. 1(42), pp. 260–262.
16. Tao Zhang, Shuxing Li, Tao Feng, Gennian Ge. I*EEE Trans. on Information Theory*, 2014, no. 5(60), pp. 3062–3068.
17. Zhengchun Zhou, Tor Helleseth, Udaya Parampalli. *IEEE Trans. on Information Theory*, 2018, no. 4(64), pp. 2896–2900.
18. Peterson W.W. & Weldon E.J. *Error-Correcting Codes, Second Edition*, MIT Press, 1972, 560 p.

Data on author

Victor G. Starodubtsev — PhD, Associate Professor; A. F. Mozhaisky Military Space Academy, Department of Technologies and Automation Tools for Processing and Analyzing Information from Space Vehicles; ITMO University; E-mail: vgstarod@mail.ru

For citation: Starodubtsev V. G. Formation of preferred pairs of GMB-sequences with the period *N*=511 for digital information transfer systems. *Journal of Instrument Engineering*. 2021. Vol. 64, N 1. P. 32—39 (in Russian).

DOI: 10.17586/0021-3454-2021-64-1-32-39