УДК 519.725
DOI: 10.17586/0021-3454-2022-65-1-28-35

ПРЕДПОЧТИТЕЛЬНЫЕ ПАРЫ ГМВ-ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ПЕРИОДОМ *N*=1023 ДЛЯ СИСТЕМ ПЕРЕДАЧИ ЦИФРОВОЙ ИНФОРМАЦИИ

В. Г. СТАРОДУБЦЕВ[1,2*], Е. Ю. ПОДОЛИНА[1], А. Х. КЕЛОГЛЯН[1]

[1] *Военно-космическая академия им. А. Ф. Можайского, Санкт-Петербург, Россия,*
[*] *vgstarod@mail.ru*
[2] *Университет ИТМО, Санкт-Петербург, Россия*

Аннотация. На основе алгоритма формирования предпочтительных пар (ПП) последовательностей Гордона — Миллса — Велча (ГМВП) получен полный перечень ПП ГМВП с периодом *N*=1023, обладающих пятиуровневой периодической взаимно корреляционной функцией и различными значениями эквивалентной линейной сложности, выступающей в качестве показателя структурной скрытности псевдослучайных последовательностей. Особенность формирования ГМВП с периодом *N*=1023 заключается в том, что для каждой базисной М-последовательности (МП) можно синтезировать по пять ГМВП, тогда как для периодов *N*=63, *N*=255, *N*=511 для каждой МП можно построить только по одной ГМВП. В поле GF(2^{10}) существует 60 примитивных полиномов, с каждым из которых можно сформировать по десять ПП МП. Структурная скрытность ГМВП с периодом *N*=1023 в 2, 4, 8 раз превышает аналогичную характеристику МП, что определяет предпочтительность применения ГМВП в системах передачи цифровой информации, к которым предъявляются повышенные требования по помехозащищенности, конфиденциальности и скрытности.

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

Ссылка для цитирования: *Стародубцев В. Г., Подолина Е. Ю., Келоглян А. Х.* Предпочтительные пары ГМВ-последовательностей с периодом *N*=1023 для систем передачи цифровой информации // Изв. вузов. Приборостроение. 2022. Т. 65, № 1. С. 28—35. DOI: 10.17586/0021-3454-2022-65-1-28-35.

PREFERRED PAIRS OF GMW SEQUENCES WITH PERIOD *N*=1023 FOR DIGITAL INFORMATION TRANSMISSION SYSTEMS

V. G. Starodubtsev[1,2*], E. Yu. Podolina[1], A. K. Keloglyan[1]

[1] *A. F. Mozhaisky Military Space Academy, St. Petersburg, Russia,*
**vgstarod@mail.ru*
[2] *ITMO University, St. Petersburg, Russia*

Abstract. Based on an algorithm for the formation of preferred pairs (PP) of Gordon — Mills — Welch (GMWP) sequences, a complete list is obtained of PP GMWP with a period *N*=1023, which have a five-level periodic cross-correlation function and different values of equivalent linear complexity, which acts as an indicator of structural secrecy pseudo-random sequences. The peculiarity of HMWR formation with period *N*=1023 is that for each basic M-sequences (MS), five HMWRs can be synthesized, while for periods *N*=63, *N*=255, *N*=511, only one HMWR can be constructed for each MS. There are 60 primitive polynomials in the GF(210) field, each of which can form ten PP MS. Structural secrecy of the GMWP with a period *N*=1023 is 2, 4, 8 times higher than the similar characteristic of the MS, which determines the preference for the use of the GMWP in digital information transmission systems, which are subject to increased requirements for noise immunity, confidentiality and secrecy.

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

For citation: Starodubtsev V. G., Podolina E. Yu., Keloglyan A. K. Preferred pairs of GMW sequences with period *N*=1023 for digital information transmission systems. *Journal of Instrument Engineering*. 2022. Vol. 65, N 1. P. 28—35 (in Russian). DOI: 10.17586/0021-3454-2022-65-1-28-35.

В современных системах передачи цифровой информации (СПЦИ), включающих в том числе системы передачи измерительной информации космических средств, широкое применение получили сигналы с расширенным спектром (СРС), которые формируются на основе псевдослучайных последовательностей (ПСП) с заданными корреляционными и структурными свойствами. В качестве псевдослучайных используются М-последовательности (МП), а также последовательности Голда и Касами, которые формируются на основе предпочтительных пар (ПП) МП [1—4].

Спутниковые каналы связи являются наиболее уязвимыми в плане применения вероятным противником преднамеренных узкополосных, широкополосных и имитационных помех, что может привести к существенному снижению помехозащищенности СПЦИ. Под помехозащищенностью понимается устойчивость по отношению к естественным помехам и скрытность, включающая энергетическую, структурную и информационную составляющие [3]. В частности, структурная скрытность определяется возможностью и требуемым временем выявления структуры ПСП, на основе которой формируется СРС, а также возможностью внесения имитационной помехи.

В условиях радиоэлектронного противодействия используемые в настоящее время СРС, формируемые на основе М-последовательностей и их ПП, обеспечивают требуемую помехозащищенность по отношению как к узкополосным, так и к широкополосным преднамеренным помехам. Однако по отношению к имитационным помехам, вносимым противником после вскрытия структуры полезного сигнала, основанного на МП или производных последовательностях, требуемая помехозащищенность не всегда может быть обеспечена [2, 4—6].

Вопросам определения последовательностей с требуемыми взаимно корреляционными свойствами и высокой структурной скрытностью посвящено множество публикаций [7—11]. Новый класс последовательностей с малыми уровнями периодической взаимно корреляционной функции (ПВКФ) предложен в работе [7]. В [8] проведен анализ последовательностей с локально оптимальными корреляционными свойствами, а в [9] — анализ двоичных последовательностей с высокой структурной скрытностью.

В [10, 11] разработан алгоритм формирования ПП ГМВ-последовательностей (ГМВП) и получены проверочные полиномы для периодов N=63, N=255 и N=511. Показано, что ПП ГМВП формируются на основе ПП МП и характеризуются более высокой эквивалентной линейной сложностью (ЭЛС).

Предпочтительность применения ГМВП определяется тем, что данные последовательности, так же как и МП, имеют двухуровневую периодическую автокорреляционную функцию (ПАКФ), но обладают более высокой структурной скрытностью. Для вскрытия структуры ПСП, т.е. определения ее проверочного полинома, в соответствии с алгоритмом Берлекэмпа — Месси необходимо число символов анализируемой последовательности, равное удвоенной степени проверочного полинома [2, 12]. Тогда выигрыш в структурной скрытности может быть определен как отношение ЭЛС или степеней проверочных полиномов сравниваемых последовательностей.

Применению ПП ГМВП в СПЦИ препятствует отсутствие проверочных полиномов для их формирования для периодов N> 511.

Цель настоящей статьи — определение проверочных полиномов предпочтительных пар ГМВП для периода N=1023. При проведении исследований использован математический аппарат теории конечных полей, линейной алгебры и корреляционного анализа.

Предпочтительной парой называются две МП с периодом $N = 2^S–1$, модуль максимального значения ПВКФ которых не превышает

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

где $[x]$ — целая часть вещественного числа x [2, 11].

Данные свойства ПВКФ могут наследоваться в производных системах сигналов, например в множествах последовательностей Голда и Касами.

Формирование МП производится в соответствии с примитивными проверочными полиномами $h_i(x)$, где индекс „i“ (здесь и далее) соответствует минимальному показателю степени корней данного полинома степени S в конечном поле $GF(2^S)$. Устройство формирования МП реализуется на основе регистров сдвига с линейными обратными связями [3, 4].

ГМВП формируются на основе М-последовательностей с аналогичным периодом путем их матричного представления и замены столбцов матрицы, которые также являются МП, но с более коротким периодом [2, 13].

Для формирования ПП ГМВП необходимо определить пары последовательностей, ПВКФ которых удовлетворяет (1). При выполнении данного условия такие пары ГМВП также можно называть предпочтительными.

ГМВП формируются над полями с двойным расширением $GF(2^S) = GF[(2^m)^n]$, в которых степень расширения поля $S = m \cdot n$ — составное число. Символы d_i ГМВП с периодом $N = 2^{mn}–1$ определяются выражением [2, 6, 13]

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

где $\mathrm{tr}_{u,v}(\cdot)$ — след элемента, принадлежащего полю $GF(2^u)$, в поле $GF(2^v)$; $\alpha \in GF(2^{mn})$ — примитивный элемент; r — натуральное число, взаимно простое с порядком мультипликативной группы поля $GF(2^m)$, равным $2^m - 1$.

Алгоритм формирования ГМВП с периодом $N = 2^{mn}–1 = 2^S–1$ основан на использовании МП с аналогичным периодом и проверочным полиномом $h_{\text{МП}}(x)$ степени S. Одним из корней базисной МП является примитивный элемент α, принадлежащий расширенному полю $GF(2^S)$. Проверочный полином формируемой ГМВП $h_{\text{г}}(x)$ может быть представлен в виде произведения двух и более неприводимых полиномов-сомножителей $h_{\text{с}i}(x)$ степени S, корни которых являются фиксированными степенями корней полинома $h_{\text{МП}}(x)$, т.е. степенями примитивного элемента α и его p-сопряженных элементов. Число полиномов-сомножителей определяет ЭЛС ГМВП и для заданного периода зависит только от значений параметров m, n и r.

ЭЛС двоичных ГМВП определяется выражением [2, 6]

$$l_S = mn^{g(r)}, \qquad (3)$$

где $g(r)$ — количество единиц в двоичном представлении числа r в (2).

Для периодов $N = 31$, $N = 63$, $N = 127$, $N = 511$, $N = 1023$ ПВКФ ПП МП является трехуровневой и принимает следующие ненормированные значения в соответствии с (1):

$$\{–p(S), –1, p(S) –2\}. \qquad (4)$$

Для каждого примитивного полинома $h_i(x)$ в поле $GF(2^S)$ количество ПП равно их числу для полинома $h_1(x)$. Для периода $N = 1023$ для каждого примитивного полинома можно сформировать по десять ПП МП [13].

Особенность формирования ГМВП с периодом N=1023 заключается в том, что для каждой базисной МП можно синтезировать по пять ГМВП, тогда как для периодов N=63, N=255 для каждой МП можно построить только по одной ГМВП. Это определяется тем, что в подполях $GF(2^{S/2})$ при $S = 6$, $S = 8$ существует по два примитивных полинома, а при $S = 10$ в подполе $GF(2^5)$ имеется уже 6 примитивных полиномов. Один полином может быть использован для формирования МП с периодом N=1023, а пять полиномов — для формирования пяти ГМВП.

В зависимости от значения параметра r в выражении (2) и функции $g(r)$ в (3) можно выделить пять типов ГМВП, которые характеризуются различными значениями ЭЛС:

— 1-й тип: $r = 3_{10} = 00011_2$, $g(r) = 2$, $l_{S1} = 20$;
— 2-й тип: $r = 5_{10} = 00101_2$, $g(r) = 2$, $l_{S2} = 20$;
— 3-й тип: $r = 7_{10} = 00111_2$, $g(r) = 3$, $l_{S3} = 40$;
— 4-й тип: $r = 11_{10} = 01011_2$, $g(r) = 3$, $l_{S4} = 40$;
— 5-й тип: $r = 15_{10} = 01111_2$, $g(r) = 4$, $l_{S5} = 80$.

В соответствии с алгоритмом, разработанным в [10, 11], определим ПП ГМВП для каждого из пяти типов. Первые два шага алгоритма являются общими для всех типов ГМВП.

Шаг 1. Выбор конечного поля $GF(2^{10})$ с неприводимым полиномом $f(x) = h_1(x) = x^{10}+x^3+1$, для которого существуют ГМВП с периодом $N=2^{10}-1=1023$.

Шаг 2. Выбор неприводимых полиномов в поле $GF(2^{10})$, выбор производится в соответствии с табл. 1 [14].

Таблица 1

α^t в $h_i(x)$	Полином $h_i(x)$ $x^{10}+\ldots+1$	Период корней	α^t в $h_i(x)$	Полином $h_i(x)$ $x^{10}+\ldots+1$	Период корней	α^t в $h_i(x)$	Полином $h_i(x)$ $x^{10}+\ldots+1$	Период корней
α^1	10000001001	1023	77	10100001011	93	183	11100001111	341
α^3	10000001111	341	79	10011100111	1023	187	11010000101	93
5	10100001101	1023	83	11110010011	1023	189	10001100011	341
7	11111111001	1023	85	10111000111	1023	191	11110110001	1023
9	10010101111	341	87	10011001001	341	205	10010001011	1023
11	10000110101	93	89	10011010111	1023	207	11100110101	341
13	10001101111	1023	91	11010110101	1023	213	10110011011	341
15	10110101011	341	93	11111111111	11	215	10110100001	1023
17	11101001101	1023	95	10001100101	1023	219	10110111001	341
19	10111111011	1023	99	110111	31	221	11101011001	1023
21	11111101011	341	101	10000101101	1023	223	11000100101	1023
23	10000011011	1023	103	11101111101	1023	231	111011	31
25	10100100011	1023	105	11110000111	341	235	11001001111	1023
27	11101111011	341	107	11001111001	1023	237	11111000101	341
29	10100110001	1023	109	10000100111	1023	239	10101010111	1023
31	11000100011	33	111	10001010011	341	245	10011000101	1023
33	111101	31	115	10111110111	1023	247	11001000011	1023
35	11000010011	1023	117	10010011001	341	251	11011111101	1023
37	11101100011	1023	119	11001011011	1023	253	10101100001	93
39	10001000111	341	121	11010100111	93	255	11110000001	341
41	10111100101	1023	123	11100010001	341	341	111	3
43	10100011001	1023	125	11011000001	1023	343	11100011101	1023
45	11000110001	341	127	10011111111	1023	347	10101000011	1023
47	11001111111	1023	147	10011101101	341	351	11010111111	341
49	11101010101	1023	149	11000010101	1023	363	100101	31
51	10101100111	341	151	11100100001	1023	367	10100111101	1023
53	10110001111	1023	155	10010101001	33	375	10000011101	341
55	11100101011	93	157	10101101011	1023	379	11000110111	1023
57	11001010001	341	159	11011110111	341	383	10110000101	1023
59	11100111001	1023	165	101001	31	439	11100010111	1023
61	11111110011	1023	167	10011110011	1023	447	11110101001	341
63	11010101101	341	171	11011001101	341	479	10110010111	1023
69	10111000001	341	173	11011011111	1023	495	101111	31
71	11011010011	1023	175	11110001101	1023	511	10010000001	1023
73	11101000111	1023	179	11010001001	1023			
75	10100011111	341	181	11111011011	1023			

Шаг 3. Вычисление ПВКФ ГМВП первого и второго типов с ЭЛС $l_S = 20$.

Формирование ГМВП с периодом $N=1023$ выполняется на основе базисных МП [13]. Всего в поле $GF(2^{10})$ существует 60 примитивных полиномов десятой степени. Для каждой базисной МП можно сформировать по пять ГМВП с различными значениями ЭЛС. Проверочные полиномы пяти типов ГМВП определяются следующими выражениями [13, 14]:

$$h_{1г1}(x) = h_3(x)h_{17}(x);$$
$$h_{2г1}(x) = h_5(x)h_9(x);$$
$$h_{3г1}(x) = h_7(x)h_{19}(x)h_{25}(x)h_{69}(x);$$
$$h_{4г1}(x) = h_{11}(x)h_{13}(x)h_{21}(x)h_{73}(x);$$

$$h_{5г1}(x) = h_{15}(x)h_{23}(x)h_{27}(x)h_{29}(x)h_{77}(x)h_{85}(x)h_{89}(x)h_{147}(x),$$

где первая слева цифра индекса обозначает принадлежность к одному из пяти типов ГМВП, а третья цифра соответствует индексу примитивного полинома (минимальному показателю степени его корней), с помощью которого образуется базисная МП при формировании ГМВП. Например, если для базисной МП используется примитивный полином $h_{49}(x) = x^{10}+x^9+x^8+x^6+x^4+x^2+1$ (см. табл. 1), то полином для ГМВП четвертого типа имеет вид

$$h_{4г49}(x) = h_{11\cdot49}(x)h_{13\cdot49}(x)h_{21\cdot49}(x)h_{73\cdot49}(x) = h_{55}(x)h_{251}(x)h_{3}(x)h_{127}(x).$$

В табл. 2, 3 показаны отдельные результаты вычисления ПВКФ, т.е. значений функции $R(\tau)$ и количества n этих значений, для ГМВП с проверочными полиномами $h_{1г1}(x)=h_3(x)h_{17}(x)$ и $h_{2г1}(x)=h_5(x)h_9(x)$, образованными на основе МП с полиномом $h_1(x)$, и ГМВП, образованными на основе МП с другими 59 примитивными полиномами $h_i(x)$.

Таблица 2

Тип ПВКФ	Индекс i в $h_{1гi}(x)$	Минимум ПВКФ		Максимум ПВКФ		Число уровней
		$R_{min}(\tau)$	n	$R_{max}(\tau)$	n	
1	5, 205	–97	1	79	10	12
2	13, 79	–97	10	111	10	20
3	17, 181	–73	10	95	5	19
4	25, 41	–97	1	79	10	12
5	49, 107	–97	1	79	20	11
6	511	–85	10	143	1	34
7	43, 119	–73	20	87	20	20
8	223, 367	–65	70	63	86	5

Таблица 3

Тип ПВКФ	Индекс i в $h_{2гi}(x)$	Минимум ПВКФ		Максимум ПВКФ		Число уровней
		$R_{min}(\tau)$	n	$R_{max}(\tau)$	n	
1	5, 205	–73	20	143	1	20
2	13, 79	–97	11	95	10	13
3	17, 181	–97	1	79	10	11
4	25, 41	–121	2	143	1	19
5	49, 107	–89	10	143	1	19
6	511	–77	20	95	5	34
7	43, 119	–65	50	63	86	5
8	223, 367	–65	70	63	86	5

В соответствии с табл. 2 условию (1) для предпочтительных пар удовлетворяют только две пары ГМВП первого типа с проверочными полиномами $h_{1г1}(x)$—$h_{1г223}(x)$ и $h_{1г1}(x)$—$h_{1г367}(x)$. ПВКФ данных ПП ГМВП (рис. 1) принимает пять значений, лежащих в интервале от –65 до +63:

$$R(\tau) \in \{-65(70), -33(200), -1(467), 31(200), 63(86)\}.$$

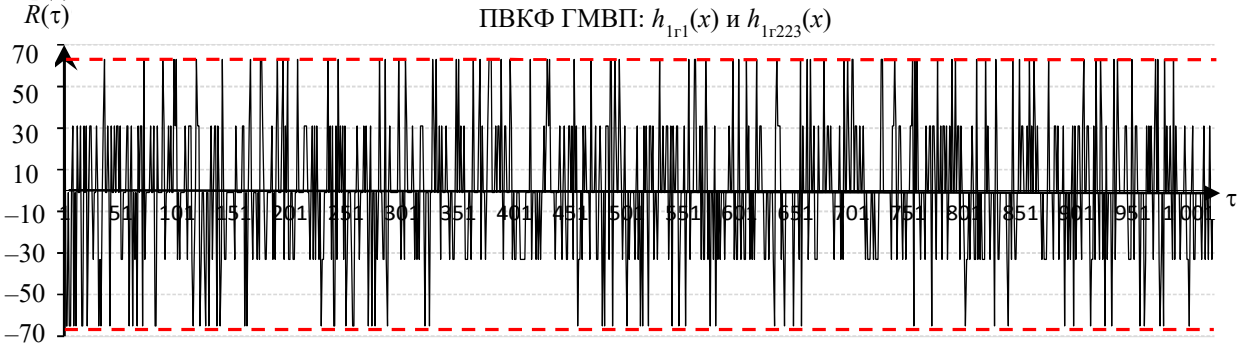

Рис. 1

В соответствии с табл. 3 при $h_{2г1}(x)=h_5(x)h_9(x)$ условию (1) удовлетворяют четыре пары с проверочными полиномами $h_{2г1}(x)$—$h_{2г43}(x)$, $h_{2г1}(x)$—$h_{2г119}(x)$, $h_{2г1}(x)$—$h_{2г223}(x)$, $h_{2г1}(x)$—$h_{2г367}(x)$. ПВКФ ПП ГМВП двух первых пар принимает пять значений, лежащих в интервале от –65 до +63:

$$R(\tau) \in \{-65(50), -33(260), -1(407), 31(220), 63(86)\}.$$

ПВКФ ПП ГМВП двух вторых пар также принимает пять значений, лежащих в интервале от –65 до +63, но с другим распределением числа значений:

$$R(\tau) \in \{-65(70), -33(200), -1(467), 31(200), 63(86)\}.$$

Шаг 4. Вычисление ПВКФ ГМВП третьего и четвертого типов с ЭЛС $l_S = 40$.

Данные ГМВП имеют проверочные полиномы $h_{3г1}(x) = h_7(x)h_{19}(x)h_{25}(x)h_{69}(x)$ и $h_{4г1}(x) = h_{11}(x)h_{13}(x)h_{21}(x)h_{73}(x)$.

В результате вычисления ПВКФ пар ГМВП третьего типа получены две предпочтительные пары с полиномами $h_{3г1}(x)$—$h_{3г17}(x)$ и $h_{3г1}(x)$—$h_{3г181}(x)$. ПВКФ данных ПП ГМВП (рис. 2) принимает пять значений, лежащих в интервале от –65 до +63:

$$R(\tau) \in \{-65(70), -33(210), -1(437), 31(230), 63(76)\}.$$

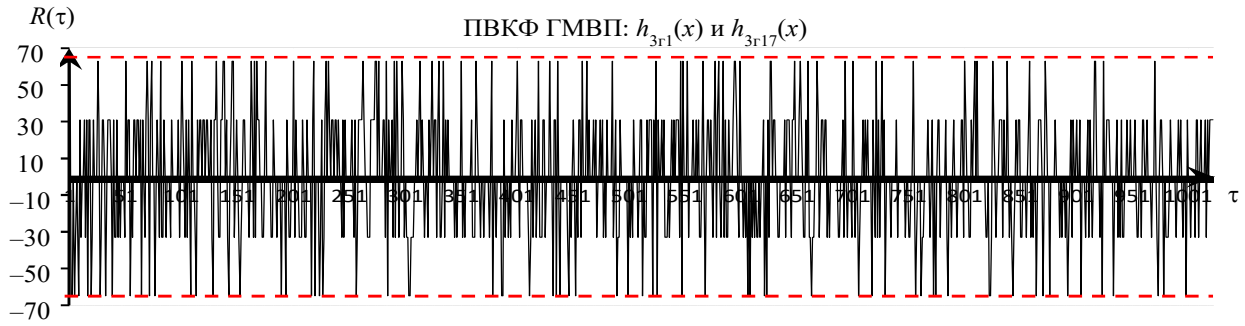

Рис. 2

В результате вычисления ПВКФ пар ГМВП четвертого типа также получены две предпочтительные пары с полиномами $h_{4г1}(x)$—$h_{4г5}(x)$ и $h_{4г1}(x)$—$h_{4г205}(x)$. ПВКФ данных ПП ГМВП также принимает пять значений, лежащих в интервале от –65 до +63:

$$R(\tau) \in \{-65(80), -33(200), -1(407), 31(280), 63(56)\}.$$

Отметим, что ПВКФ предпочтительных пар ГМВП четырех типов являются пятиуровневыми. Отличие заключается в распределении числа значений каждого уровня.

Шаг 5. Вычисление ПВКФ ГМВП пятого типа с ЭЛС $l_S = 80$.

В результате вычислений ПВКФ пар ГМВП пятого типа с полиномом $h_{5г1}(x)=h_{15}(x)h_{23}(x)h_{27}(x)h_{29}(x)h_{77}(x)h_{85}(x)h_{89}(x)h_{147}(x)$ условию (1) соответствуют три пары с проверочными полиномами $h_{5г1}(x)$—$h_{5г25}(x)$, $h_{5г1}(x)$—$h_{5г41}(x)$ и $h_{5г1}(x)$—$h_{5г511}(x)$. Однако ПВКФ данных пар не являются пятиуровневыми. Две первые пары имеют 17 значений корреляционной функции в интервале от –65 до +63, при этом значения от минимального до максимального изменяются через 8 единиц. Третья пара характеризуется 32 уровнями в интервале от –61 до +63, которые изменяются через 4 единицы. Тем не менее данные пары ГМВП также могут быть отнесены к предпочтительным парам именно в силу удовлетворения условию (1).

Вид 32-уровневой ПВКФ предпочтительной пары ГМВП пятого типа с полиномами $h_{5г1}(x) – h_{5г511}(x)$ приведен на рис. 3.

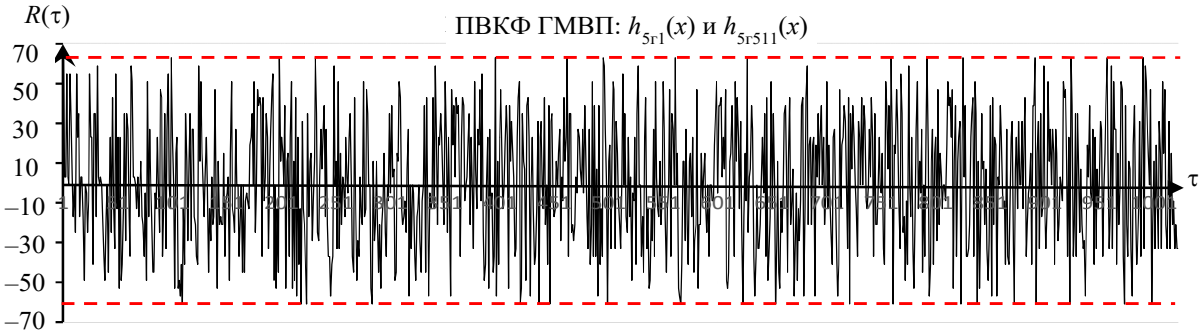

Рис. 3

Таким образом, определены проверочные полиномы для предпочтительных пар ГМВП всех пяти типов с периодом $N = 1023$. Для каждого из 60 примитивных полиномов в конечном поле $GF(2^{10})$ может быть сформировано по две предпочтительные пары ГМВП первого, третьего и четвертого типов и по четыре ПП ГМВП второго типа, обладающие пятиуровневой ПВКФ, удовлетворяющей условию (1). Кроме того, для каждого примитивного полинома может быть сформировано три предпочтительные пары ГМВП пятого типа с многоуровневой ПВКФ, но также удовлетворяющей условию (1).

ПП ГМВП первого и второго типов имеют ЭЛС $l_S = 20$, ПП ГМВП третьего и четвертого типов — ЭЛС $l_S = 40$, ПП ГМВП пятого типа — ЭЛС $l_S = 80$, тогда как ПП МП имеют ЭЛС $l_S = 10$. Применение ПП ГМВП позволяет обеспечить выигрыш в структурной скрытности по сравнению с ПП МП. При этом интервал времени, необходимый средствам радиоэлектронного противодействия для вскрытия структуры сигнала и внесения имитационной помехи, увеличивается в 2, 4 или 8 раз.

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 удовлетворительными корреляционными и структурными свойствами.

СПИСОК ЛИТЕРАТУРЫ

1. *Вишневский В. М., Ляхов А. И., Портной С. Л., Шахнович И. В.* Широкополосные беспроводные сети передачи информации. М.: Техносфера, 2005. 592 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. *Ипатов В. П.* Широкополосные системы и кодовое разделение сигналов. Принципы и приложения. М.: Техносфера, 2007. 488 с.
4. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение: Пер. с англ. М.: Вильямс, 2003. 1104 с.
5. CDMA: прошлое, настоящее, будущее / Под ред. *Л. Е. Варакина и Ю. С. Шинакова*. М.: МАС, 2003. 608 с.
6. *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.
7. *Tang X. H., Pingzhi Z. F.* A class of pseudonoise sequences over GF(p) with low correlation zone // IEEE Trans. on Information Theory. 2001. Vol. 47, N 4. P. 1644—1649.
8. *Popović M. B.* Optimum Sets of Interference-Free Sequences with Zero Autocorrelation Zones // IEEE Trans. on Information Theory. 2018. Vol. 64, N 4. P. 2876—2882.
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. *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.
11. *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.
12. *No J. S.* Generalization of GMW sequences and No sequences // IEEE Trans. on Information Theory. 1996. Vol. 42, N 1. P. 260—262.
13. *Стародубцев В. Г., Попов А. М.* Последовательности Гордона — Миллса — Велча с периодом N=1023 // Изв. вузов. Приборостроение. 2017. Т. 60, № 4. С. 318—330.
14. *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 авторах

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

Екатерина Юрьевна Подолина — ВКА им. А. Ф. Можайского; слушатель; E-mail: vka@mil.ru

Артем Хоренович Келоглян — ВКА им. А. Ф. Можайского; слушатель; E-mail: vka@mil.ru

Поступила в редакцию 25.06.2021; одобрена после рецензирования 09.07.2021; принята к публикации 02.12.2021.

REFERENCES

1. 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.)
2. Golomb S.W., Gong G. *Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar,* Cambridge University Press, 2005, 438 p.
3. Ipatov V.P. *Spread Spectrum and CDMA. Principles and Applications*, NY, John Wiley and Sons Ltd., 2005, 488 p.
4. Sklar B. *Digital Communications: Fundamentals and Applications, Prentice Hall*, 2001, 1079 p.
5. Varakin L.E. and Shinakov Yu.S., ed., *CDMA: proshloe, nastoyashchee, budushchee* (CDMA: Past, Present, Future), Moscow, 2003. 608 p. (in Russ.)
6. Chung H.B., No J.S. *IEEE Transactions on Information Theory*, 1999, no. 6(45), pp. 2060–2065.
7. Tang X.H., Pingzhi Z.F. *IEEE Transactions on Information Theory*, 2001, no. 4(47), pp. 1644–1649.
8. Popović B. M. *IEEE Transactions on Information Theory*, 2018, no. 4(64), pp. 2876–2882.
9. Rizomiliotis P., Kalouptsidis N. *IEEE Transactions on Information Theory*, 2005, vol. IT–51, pp. 1555–1563.
10. Starodubtsev V.G., Osadchaya Ya.V. *Journal of Instrument Engineering*, 2019, no. 7(62), pp. 610–620. (in Russ.)
11. Starodubtsev V.G. *Journal of Instrument Engineering*, 2021, no. 1(64), pp. 32–39. (in Russ.)
12. No Jong-Seon. *IEEE Transactions on Information Theory*, 1996, no. 1(42), pp. 260–262.
13. Starodubtsev V.G., Popov A.M. *Journal of Instrument Engineering*, 2017, no. 4(60), pp. 318–330. (in Russ.)
14. Peterson W.W., Weldon E.J. *Error-correcting Codes*, The MIT PRESS, Cambridge, Massachusetts and London, England, 1972, 588 p.

Data on authors

Victor G. Starodubtsev — PhD, Associate Professor; A. F. Mozhaisky Military Space Academy, Department of Technologies and Automation Means for processing and Analysis of Space Facilities Information; ITMO University, E-mail: vgstarod@mail.ru

Ekaterina Yu. Podolina — Student; A. F. Mozhaisky Military Space Academy; E-mail: vka@mil.ru

Artem K. Keloglyan — Student; A. F. Mozhaisky i Military Space Academy; E-mail: vka@mil.ru

Received 25.06.2021; approved after reviewing 09.07.2021; accepted for publication 02.12.2021.