ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

УДК 519.725
DOI: 10.17586/0021-3454-2019-62-7-610-620

ПРЕДПОЧТИТЕЛЬНЫЕ ПАРЫ ГМВ-ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ СИСТЕМ ПЕРЕДАЧИ ЦИФРОВОЙ ИНФОРМАЦИИ

В. Г. СТАРОДУБЦЕВ[1,2], Я. В. ОСАДЧАЯ[1]

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

[2]*Университет ИТМО, 197101, Санкт-Петербург, Россия*

Представлен анализ периодических взаимно корреляционных функций М-последовательностей (МП) и последовательностей Гордона—Миллса—Велча (ГМВП), обладающих двухуровневой автокорреляционной функцией. ГМВ-последовательности имеют более высокую структурную скрытность по сравнению с МП, что определяет предпочтительность их использования в системах передачи цифровой информации. Разработан алгоритм формирования предпочтительных пар ГМВП и их определения для периодов N=63 и N=255. При проведении исследований использован математический аппарат теории конечных полей, линейной алгебры и корреляционного анализа. Получены значения периодических взаимно корреляционных функций всевозможных пар М- и ГМВ-последовательностей для периодов N=63 и N=255. Показано, что ГМВП, образующие предпочтительные пары, формируются на основе базисных МП, также образующих предпочтительные пары. Полученные результаты могут найти применение при формировании сигналов с расширенным спектром в помехозащищенных системах передачи цифровой информации, а также при синтезе систем сигналов, допускающих аналитическое представление в конечных полях.

Ключевые слова: *псевдослучайные последовательности, предпочтительные пары, корреляционная функция, структурная скрытность, неприводимые и примитивные полиномы, конечные поля*

В современных системах передачи цифровой информации (СПЦИ) широкое распространение получили сигналы с расширенным спектром, одним из направлений формирования которых является использование псевдослучайных последовательностей (ПСП) [1, 2]. Данные последовательности применяются в системах связи с кодовым доступом, в системах радионавигации и радиолокации для расширения спектра дискретных сигналов, а также при формировании сигналов синхронизации и скремблирования [3—6].

Среди ПСП, широко используемых в системах передачи цифровой информации, можно выделить М-последовательности (МП), последовательности Голда, последовательности малого и большого множеств Касами, последовательности бент-функций, последовательности Гордона—Миллса—Велча (ГМВП). При этом М-последовательности вследствие своих корреляционных и структурных свойств применяются как непосредственно в качестве псевдослучайных, так и в виде „кирпичиков“ при формировании других ПСП и их множеств [2, 7—12].

Одна из причин широкого применения МП с периодом $N=2^s-1$ — наличие двухуровневой периодической автокорреляционной функции (ПАКФ) при произвольном сдвиге τ [5, 13]:

$$R(\tau)=\begin{cases} N & \text{при } \tau = kN,\ k = 0,1,2,..., \\ -1 & \text{при } \tau \neq kN. \end{cases} \quad (1)$$

При синтезе последовательностей Голда и Касами (малого множества) используются так называемые предпочтительные пары (ПП) МП, обладающие достаточно небольшими значениями периодической взаимно корреляционной функции (ПВКФ) [5, 6].

Предпочтительной парой называются две М-последовательности с периодом $N = 2^s–1$, модуль максимального значения ПВКФ которых не превышает

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

где $[x]$ — целая часть вещественного числа x [5, 14, 15].

Определение, свойства и алгоритмы формирования ПП МП приведены в известных работах [2—5]. М-последовательности формируются в соответствии с примитивными проверочными полиномами $h_i(x)$; здесь и далее нижний индекс соответствует минимальному показателю степени корней данного полинома в конечном расширенном поле $GF(2^s)$. Аппаратная реализация М-последовательности осуществляется на основе регистров сдвига с линейными обратными связями [2, 3].

Наряду с М-последовательностями двухуровневой ПАКФ вида (1) обладают ГМВП, при этом они имеют более высокую структурную скрытность, характеризуемую эквивалентной линейной сложностью (ЭЛС), что определяет приоритетность их использования в системах передачи цифровой информации, к которым предъявляются повышенные требования по конфиденциальности [7, 16, 17].

ГМВП формируются на основе МП с аналогичным периодом путем матричного представления МП и замены столбцов матрицы, представляющих собой различные сдвиги М-последовательности с более коротким периодом, на соответствующие сдвиги другой МП с коротким периодом [8].

Так как ГМВП аналогично МП обладают двухуровневой ПАКФ и строятся на основе базисных М-последовательностей [17, 18], целесообразно определить пары ГМВП, значения ПВКФ которых удовлетворяют условию (2). При выполнении данного условия такие пары ГМВ-последовательностей также можно называть предпочтительными.

Цель настоящей статьи — разработка алгоритма формирования предпочтительных пар ГМВП и их определение для периодов N=63, N=255.

ГМВП формируются над полями с двойным расширением $GF(2^s) = GF[(2^m)^n]$, в которых степень расширения поля $s = mn$ является составным числом. Символы d_i ГМВП с периодом $N = 2^{mn}–1$ определяются выражением [5, 8]

$$d_i = \mathrm{tr}_{m1}[(\mathrm{tr}_{mn,m}(\alpha^i))^\rho],\ 1 \le \rho < 2^m - 1,\ (\rho, 2^m - 1) = 1, \quad (3)$$

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; ρ — 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. Такая М-последовательность называется базисной [18]. Одним из корней полинома базисной МП является примитивный элемент α, принадлежащий расширенному полю $GF(2^s)$. Проверочный полином $h_{\text{ГМВ}}(x)$ формируемой ГМВП может быть представлен в виде произведения двух и более неприводимых полиномов-сомножителей $h_{ci}(x)$ степени s, корни которых являются фиксированными степенями корней полинома $h_{\text{МП}}(x)$, т.е. степенями примитивного элемента α и его p-сопряженных элементов. Эквивалентная линейная сложность ГМВП определяется числом полиномов-сомножителей и для заданного периода зависит только от значений параметров m, n и r.

ЭЛС двоичных ГМВП определяется выражением [7, 16]

$$l_s = mn^{g(\rho)} \tag{4}$$

где $g(\rho)$ — количество единиц в двоичном представлении числа ρ в выражении (3).

Для сравнения в табл. 1 приведены показатели ЭЛС (степеней проверочных полиномов) широко используемых ПСП с удовлетворительными периодическими корреляционными свойствами.

Таблица 1

Период ПСП	ЭЛС последовательности				
	МП	Голда	Касами (малого множества)	Касами (большого множества)	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	80
2047	11	22	—	—	—
4095	12	24	18	30	192

Отметим, что в табл. 1 для периода N=4095 приведено максимальное значение показателя ЭЛС ГМВП l_s=192, получаемое при m=6, n=2 и r=31. Для других допустимых значений данных параметров показатель ЭЛС может принимать значения 24, 48, 96, 108.

Для разработки алгоритма формирования ПП ГМВП предварительно рассмотрим значения ПВКФ ПП М-последовательностей для периодов N = 31, 63, 127, 255, 511.

Если элементы $a_{j\,i}$ МП_1 и $a_{k\,i}$ МП_2 принадлежат простому полю GF(2), то значение ПВКФ $R_{jk}(\tau)$ определяется выражением [2, 3—5]

$$R_{jk}(\tau) = N - 2B(\tau) = N - 2\sum_{l=0}^{N-1} d(a_{jl}, a_{k,l+\tau}), \tag{5}$$

где $B(\tau)$ — число несовпадающих позиций в МП_1 и МП_2 при различных сдвигах τ; τ — циклический сдвиг, принимающий дискретные значения, сдвиг $(l+\tau)$ вычисляется по $\bmod N$; $d\ (i, j) = (i + j) \bmod 2 = i \oplus j$ — расстояние между элементами i и j в метрике Хемминга.

Коэффициент корреляции $r_{jk}(\tau)$ определяется путем нормирования функции корреляции:

$$r_{jk}(\tau) = R_{jk}(\tau) / N. \tag{6}$$

Значения ПВКФ (R_i) и коэффициента корреляции (r_i) предпочтительной пары МП для рассматриваемых периодов приведены в табл. 2, где также показано количество этих значений для одного периода. В крайней правой графе приведены примитивные полиномы $h_i(x)$ или их нижние индексы в соответствующих полях $\text{GF}(2^s)$, с помощью которых формируются МП, образующие предпочтительные пары с МП, полученной на основе полинома $h_1(x)$.

Таблица 2

Период МП	R_1	n_1	R_2	n_2	R_3	n_3	R_4	n_4	$\lvert R_{\max}\rvert$	Полиномы $h_i(x)$ в паре с $h_1(x)$
	r_1		r_2		r_3		r_4		$\lvert r_{\max}\rvert$	
31	–9	6	–1	15	7	10	–	–	9	$h_3(x)$, $h_5(x)$, $h_7(x)$, $h_{11}(x)$
	–0,29		–0,03		0,23		–		0,29	
63	–17	6	–1	47	15	10	–	–	17	$h_5(x)$, $h_{13}(x)$
	–0,27		–0,02		0,24		–		0,27	
127	–17	28	–1	63	15	36	–	–	17	3, 5, 9, 11, 13, 15, 23, 27, 29, 43
	–0,13		–0,01		0,12		–		0,13	
255	–17	80	–1	119	15	16	31	40	31	$h_{31}(x)$, $h_{91}(x)$
	–0,07		–0,00		0,06		0,12		0,12	
511	–33	120	–1	255	31	136	–	–	33	13,17,19,27,31,59, 87,103,171
	–0,06		–0,00		0,06		–		0,06	

Для периодов $N = 31, 63, 127, 511$ ПВКФ ПП МП является трехуровневой и принимает следующие ненормированные значения в соответствии с выражением (2):

$$\{-p(s), -1, p(s) - 2\}. \quad (7)$$

Для периода $N = 255$ ПВКФ ПП МП является четырехуровневой и принимает следующие ненормированные значения:

$$\{-p(s-1), -1, p(s-1) - 2, p(s) - 2\} = \{-17, -1, 15, 31\}. \quad (8)$$

Для каждого примитивного полинома $h_i(x)$ в поле $GF(2^s)$ количество ПП равно числу ПП для полинома $h_1(x)$. Для их определения необходимо индекс данного полинома умножить по mod N на соответствующие индексы полиномов из табл. 2 и затем для каждого полученного индекса, являющегося степенью примитивного элемента поля $GF(2^s)$, вычислить наименьший показатель степени среди его p-сопряженных элементов.

Например, в поле $GF(2^8)$ существует 16 примитивных полиномов. Для МП, задаваемой полиномом $h_1(x)=x^8+x^4+x^3+x^2+1$, существует всего две предпочтительные пары с М-последовательностями, задаваемыми полиномами $h_{31}(x)=x^8+x^5+x^3+x^2+1$ и $h_{91}(x)=x^8+x^7+x^6+x^5+x^4+x^2+1$ (см. табл. 2). Определим полиномы, на основании которых формируются МП, составляющие ПП с МП, задаваемой примитивным полиномом $h_{59}(x) = x^8+x^6+x^3+x^2+1$. Вычислим произведения: $59 \cdot 31 = 44 \bmod 255$, $59 \cdot 91 = 14 \bmod 255$. Полученные числа равны показателям степени примитивного элемента α, т.е. элементы α^{44} и α^{14} являются корнями полиномов $h_{11}(x) = x^8+x^7+x^6+x^5+x^2+x+1$ и $h_7(x) = x^8+x^6+x^5+x^3+1$. Легко показать, что значения ПВКФ ПП МП, задаваемых полиномами $h_{59}(x)$ и $h_{11}(x)$, а также $h_{59}(x)$ и $h_7(x)$, удовлетворяют выражению (8).

Рассмотрим формирование ПП ГМВП для периодов $N = 63, 255$, являющихся составными числами. Для каждой МП с такими периодами можно сформировать только по одной ГМВП. Это определяется тем, что для полей с двойным расширением $GF[(2^3)^2]$ и $GF[(2^4)^2]$ в подполях $GF(2^3)$ и $GF(2^4)$ существует всего по два примитивных полинома. Заметим, что для периода $N = 1023$ для каждой МП можно сформировать уже по пять ГМВП с различными ЭЛС, так как в подполе $GF(2^5)$ расширенного поля $GF[(2^5)^2]$ имеется шесть примитивных полиномов [19].

Сначала проведем более подробный корреляционный анализ для М- и ГМВ-последовательностей с периодом $N = 63$ в конечном поле $GF(2^6) = GF[(2^3)^2]$. Неприводимые полиномы степени s=6 данного поля приведены в табл. 3 [19].

Таблица 3

Полином	Период корней	Полином	Период корней
$h_1(x) = x^6 + x + 1$	63	$h_{13}(x) = x^6 + x^4 + x^3 + x + 1$	63
$h_3(x) = x^6 + x^4 + x^2 + x + 1$	21	$h_{15}(x) = x^6 + x^5 + x^4 + x^2 + 1$	21
$h_5(x) = x^6 + x^5 + x^2 + x + 1$	63	$h_{23}(x) = x^6 + x^5 + x^4 + x + 1$	63
$h_7(x) = x^6 + x^3 + 1$	9	$h_{31}(x) = x^6 + x^5 + 1$	63
$h_{11}(x) = x^6 + x^5 + x^3 + x^2 + 1$	63		

Для получения ПП ГМВП определим значения ПВКФ $R(\tau)$ и $r(\tau)$ различных пар $МП_1$ и $МП_2$. Результаты вычислений приведены в табл. 4.

Таблица 4

Полиномы для $МП_1$ и $МП_2$	Тип КФ	Число n значений ПВКФ $МП_1$ и $МП_2$ при $R(\tau)$; $r(\tau)$											
		23; 0,37	19; 0,30	15; 0,24	11; 0,17	7; 0,11	3; 0,05	–1; –0,02	–5; –0,08	–9; –0,14	–13; –0,21	–17; –0,27	–21; –0,33
$h_1(x)$ *и* $h_5(x)$	1			10				47				6	
$h_1(x)$ и $h_{11}(x)$	2	2		4		12		27		18			
$h_1(x)$ и $h_{13}(x)$	1			10				47				6	
$h_1(x)$ и $h_{23}(x)$	2	2		4		12		27		18			
$h_1(x)$ и $h_{31}(x)$	3			3	8	9	6	12	12	7	6		

Анализ результатов вычисления ПВКФ МП с периодом N=63 показал, что можно выделить три типа корреляционных функций. При этом все типы ПВКФ представлены для полинома $h_1(x)$. Для остальных пар МП значения корреляционных функций аналогичны. К первому типу относится ПВКФ пар МП, которая принимает три значения, лежащие в интервале от –17 до +15 (рис. 1):

$$R(\tau) \in \{-17(6), -1(47), 15(10)\},$$

где в круглых скобках указано число значений ПВКФ на одном периоде.

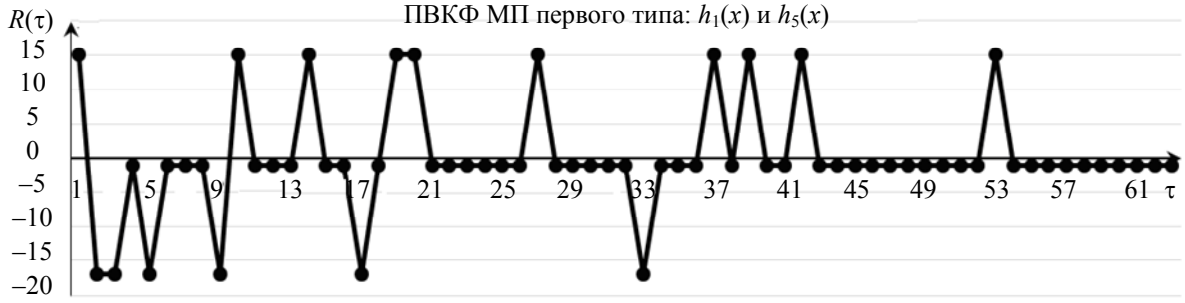

Рис. 1

Данные пары называются предпочтительными парами МП [3, 9]. Для периода N=63 существует шесть предпочтительных пар МП, проверочные полиномы которых имеют следующий вид: $h_1(x)$ и $h_5(x)$, $h_1(x)$ и $h_{13}(x)$, $h_5(x)$ и $h_{11}(x)$, $h_{11}(x)$ и $h_{31}(x)$, $h_{13}(x)$ и $h_{23}(x)$, $h_{23}(x)$ и $h_{31}(x)$.

Ко второму типу относится ПВКФ пар МП, которая принимает пять ненормированных значений, лежащих в интервале от –9 до +23:

$$R(\tau) \in \{-9(18), -1(27), 7(12), 15(4), 23(2)\}.$$

К третьему типу относится ПВКФ пар МП, которая принимает восемь ненормированных значений, лежащих в интервале от –13 до +15:

$$R(\tau) \in \{-13(6), -9(7), -5(12), -1(12), 3(6), 7(9), 11(8), 15(3)\}.$$

Третий тип характеризуется большим числом уровней, но при этом все значения ПВКФ удовлетворяют выражению (2). Проверочные полиномы пар МП являются взаимно сопряженными, т.е. это пары $h_1(x)$ и $h_{31}(x)$, $h_5(x)$ и $h_{23}(x)$, $h_{11}(x)$ и $h_{13}(x)$. Данные пары наряду с ПП МП могут быть использованы при формировании множеств ПСП с удовлетворительными корреляционными свойствами.

Проведем аналогичный анализ ПВКФ для всевозможных пар ГМВП. Проверочный полином ГМВП с периодом N=63 представляет собой произведение двух полиномов, корни которых являются соответственно 3-ми и 5-ми степенями корней примитивного полинома базисной МП [18].

Значения ПВКФ ГМВП сведены в табл. 5. Пары полиномов $h_i(x)$ и $h_j(x)$, являющиеся проверочными полиномами для базисных МП, выступают в качестве полиномов для формирования ГМВП. Например, во второй строке табл. 5 базисными полиномами для ГМВП_1 и ГМВП_2 являются полиномы $h_1(x)$ и $h_{11}(x)$, тогда проверочными полиномами для ГМВП будут $h_{г1}(x) = h_3(x)\cdot h_5(x)$ и $h_{г2}(x) = h_{33}(x)\cdot h_{55}(x) = h_3(x)\cdot h_{31}(x)$. Индексы „33“ и „55“ являются показателями степени для p-сопряженных корней полиномов $h_3(x)$ и $h_{31}(x)$.

Таблица 5

Базисные полиномы для ГМВП_1 и ГМВП_2	Тип КФ	Число n значений ПВКФ ГМВП_1 и ГМВП_2 при $R(\tau)$; $r(\tau)$											
		23; 0,37	19; 0,30	15; 0,24	11; 0,17	7; 0,11	3; 0,05	–1; –0,02	–5; –0,08	–9; –0,14	–13; –0,21	–17; –0,27	–21; –0,33
$h_1(x)$ *и* $h_5(x)$	1			3	12	3		26	6	7	6		
$h_1(x)$ и $h_{11}(x)$	2	2		4		12		27		18			
$h_1(x)$ и $h_{13}(x)$	1			3	12	3		26	6	7	6		
$h_1(x)$ и $h_{23}(x)$	2	2		4		12		27		18			
$h_1(x)$ и $h_{31}(x)$	3			4	6	6	12	15	6	6	8		

Анализ результатов показал, что трем типам ПВКФ МП соответствует также три типа ПВКФ ГМВП. Функция корреляции первого типа принимает семь значений в интервале от –13 до +15:

$$R(\tau) \in \{-13(6), -9(7), -5(6), -1(26), 7(3), 11(12), 15(3)\}.$$

Например, ПВКФ ГМВП с $h_{г1}(x) = h_3(x)\cdot h_5(x)$ и $h_{г2}(x) = h_{15}(x)\cdot h_{11}(x)$ показана на рис. 2.

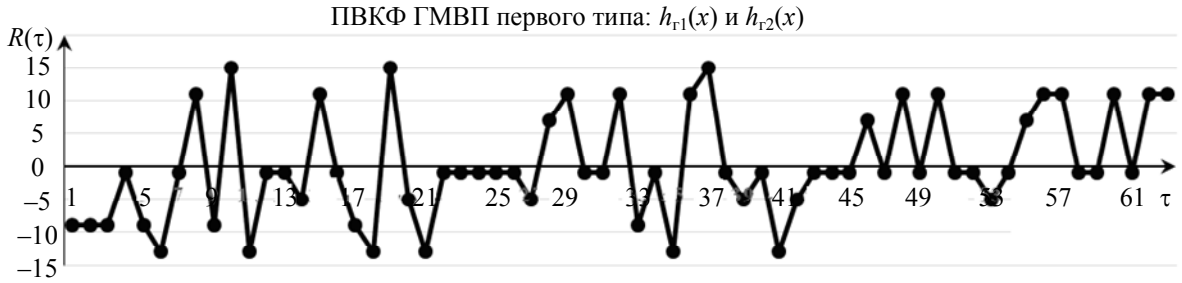

Рис. 2

В отличие от МП, у ПВКФ ГМВП отсутствует уровень „–17“, что является положительным фактором при использовании данных последовательностей. Модуль максимального значения ПВКФ равен 15.

По аналогии с парами МП, которые являются предпочтительными, полученные на их основе пары ГМВП также можно назвать предпочтительными.

ПВКФ ГМВП второго типа принимает пять значений от –9 до +23:

$$R(\tau) \in \{-9(18), -1(27), +7(12), +15(4), +23(2)\},$$

что полностью совпадает как по значениям, так и по числу этих значений с ПВКФ МП второго типа.

ПВКФ ГМВП третьего типа аналогична ПВКФ первого типа и принимает значения, лежащие в интервале от –15 до +13, но с добавлением уровня „+3“:

$$R(\tau) \in \{-13(8), -9(6), -5(6), -1(15), +3(12), +7(6), +11(6), +15(4)\}.$$

Пары ГМВП с ПВКФ третьего типа также могут быть отнесены к предпочтительным, так как максимальное значение модуля ПВКФ удовлетворяет условию (2).

В результате проведенных исследований можно сформулировать алгоритм формирования предпочтительных пар ГМВП.

Шаг 1. Выбор конечного поля с двойным расширением вида $GF[(2^m)^n]$, для которого существуют ГМВП с периодом $N=2^{mn}-1$.

Шаг 2. Определение для поля $GF[(2^m)^n]$ перечня неприводимых полиномов, включающего все примитивные полиномы $h_i(x)$ степени mn, на основании которых формируются базисные МП.

Шаг 3. Вычисление ПВКФ для всевозможных пар МП.

Шаг 4. Выбор пар полиномов, на основании которых формируются предпочтительные пары МП с требуемой ПВКФ.

Шаг 5. Вычисление ПВКФ ГМВП.

Шаг 6. Формирование предпочтительных пар ГМВП на основе полученных ПП М-последовательностей.

В соответствии с алгоритмом определим ПП ГМВП для периода $N=255$.

Шаг 1. Выбор конечного поля с двойным расширением вида $GF[(2^4)^2]$, для которого существуют ГМВП с периодом $N=2^8-1=255$.

Шаг 2. Формирование перечня неприводимых полиномов в поле $GF[(2^4)^2]$ — приведен в табл. 6 [19], периоды корней полиномов обозначены как ε.

Таблица 6

Полином	ε	Полином	ε	Полином	ε
$h_1(x)=x^8+x^4+x^3+x^2+1$	255	$h_{25}(x)=x^8+x^4+x^3+x+1$	51	$h_{59}(x)= x^8+x^6+x^3+x^2+1$	255
$h_3(x)=x^8+x^6+x^5+x^4+x^2+x+1$	85	$h_{27}(x)=x^8+x^5+x^4+x^3+x^2+ x+1$	85	$h_{61}(x)=x^8+x^7+x^6+x^3+x^2+x+1$	255
$h_5(x)=x^8+x^7+x^6+x^5+x^4+x+1$	51	$h_{29}(x)=x^8+x^7+x^3+x^2+1$	255	$h_{63}(x)=x^8+x^7+x^6+x^4+x^3+x^2+1$	85
$h_7(x)=x^8+x^6+x^5+x^3+1$	255	$h_{31}(x)=x^8+x^5+x^3+x^2+1$	255	$h_{85}(x)=x^2+x+1$	3
$h_9(x)=x^8+x^7+x^5+x^4+x^3+x^2+1$	85	$h_{37}(x)=x^8+x^6+x^4+x^3+x^2+x+1$	255	$h_{87}(x)=x^8+x^7+x^5+x+1$	85
$h_{11}(x)=x^8+x^7+x^6+x^5+x^2+x+1$	255	$h_{39}(x)=x^8+x^7+x^6+x^5+x^4+x^3+1$	85	$h_{91}(x)=x^8+x^7+x^6+x^5+x^4+x^2+1$	255
$h_{13}(x)=x^8+x^5+x^3+x+1$	255	$h_{43}(x)= x^8+x^7+x^6+x+1$	255	$h_{95}(x)=x^8+x^7+x^4+x^3+x^2+x+1$	51
$h_{15}(x)=x^8+x^7+x^6+x^4+x^2+x+1$	17	$h_{45}(x)=x^8+x^5+x^4+x^3+1$	17	$h_{111}(x)=x^8+x^6+x^5+x^4+x^3+x+1$	85
$h_{17}(x)=x^4+x+1$	15	$h_{47}(x)=x^8+x^7+x^5+x^3+1$	255	$h_{119}(x)=x^4+x^3+1$	15
$h_{19}(x)=x^8+x^6+x^5+x^2+1$	255	$h_{51}(x)=x^4+x^3+x^2+x+1$	5	$h_{127}(x)=x^8+x^6+x^5+x^4+1$	255
$h_{21}(x)=x^8+x^7+x^3+x+1$	85	$h_{53}(x)=x^8+x^7+x^2+x+1$	255		
$h_{23}(x)= x^8+x^6+x^5+x+1$	255	$h_{55}(x)=x^8+x^7+x^5+x^4+1$	51		

Шаг 3. Вычисление ПВКФ для всевозможных пар МП. Значения ПВКФ $R(\tau)$ и коэффициента корреляции $r(\tau)$ для $МП_1$ с проверочным полиномом $h_1(x)=x^8+x^4+x^3+x^2+1$ и остальных МП с примитивными полиномами $h_i(x)$ приведены в табл. 7. Всего получено 15 вариантов ПВКФ МП, среди которых можно выделить 9 типов корреляционных функций. Типы ПВКФ с первого по шестой встречаются по два раза, а типы с седьмого по девятый — по одному разу.

Таблица 7

$h_i(x)$	Тип КФ	Число n значений ПВКФ $МП_1$ и $МП_2$ при $R(\tau)$; $r(\tau)$																				
		95; 0,37	63; 0,25	47; 0,18	31; 0,12	27; 0,11	23; 0,09	19; 0,07	15; 0,06	11; 0,04	7; 0,03	3; 0,01	–1; 0,00	–5; –0,02	–9; –0,04	–13; –0,05	–17; –0,07	–21; –0,08	–25; –0,10	–29; –0,11	–33; –0,13	–65; –0,25
1—7	5		1		14				68				104				52				16	
11	2			4	10				68				100				64				8	1
13	4		1	4					84				100				48				18	
19	3			8	8				64				87				88					
23	6		2		20				56				89				88					
29_0	2			4	10				68				100				64				8	1
31	1				40				16				119				80					
37	5		1		14				68				104				52				16	
43	7	2	1						76				108				60				8	
47	3			8	8				64				87				88					
53	8		4						96				59				96					
59	4		1	4					84				100				48				18	
61	6		2		20				56				89				88					
91	1				40				16				119				80					
127	9				5	8	20	16	16	16	20	16	16	32	16	24	18	8	16	8		

Шаг 4. Выбор пар полиномов, на основании которых формируются предпочтительные пары МП с требуемой ПВКФ. Условию (2) удовлетворяют только ПВКФ первого и девятого типов. Для первого типа это пары МП с проверочными полиномами $h_1(x)$—$h_{31}(x)$ и $h_1(x)$—$h_{91}(x)$; для девятого типа — пары МП с полиномами $h_1(x)$—$h_{127}(x)$.

ПВКФ первого типа предпочтительных пар МП с периодом N=255 принимает четыре значения, лежащие в интервале от –17 до +31.

$$R(\tau) \in \{-17(80), -1(119), +15(16), +31(40)\}.$$

Для каждого примитивного полинома в поле $GF(2^8)$ можно сформировать по две предпочтительные пары. Для этого необходимо индекс данного полинома умножить на 31 и 91 по mod 255 и привести к наименьшему показателю. Например, МП с примитивным полиномом

$h_{47}(x)$ будет составлять предпочтительную пару с МП, проверочными полиномами которых являются $h_{91}(x)$ и $h_{23}(x)$.

Всего можно сформировать 16 ПП МП, сгруппированных в два множества по 8 МП:

$$h_1(x) - h_{31}(x) - h_{19}(x) - h_{61}(x) - h_{53}(x) - h_{23}(x) - h_{47}(x) - h_{91}(x) - h_1(x),$$
$$h_7(x) - h_{59}(x) - h_{11}(x) - h_{43}(x) - h_{29}(x) - h_{13}(x) - h_{37}(x) - h_{127}(x) - h_7(x).$$

ПВКФ МП девятого типа принимает шестнадцать значений, лежащих в интервале от –29 до +31:

$$R(\tau) \in \{-29(8), -25(16), -21(8), -17(18), -13(24), -9(16), -5(32),$$
$$-1(16), 3(16), 7(20), 11(16), 15(16), 19(16), 23(20), 27(8), 31(5)\}.$$

ПВКФ девятого типа обладают пары МП, проверочными полиномами которых являются сопряженные полиномы. Например, для полинома $h_{47}(x)$ сопряженным будет полином $h_{13}(x)$.

Шаг 5. Вычисление ПВКФ ГМВП. Формирование ГМВП с периодом N=255 также выполняется на основе базисных МП в соответствии с разработанным в работах [17, 18] алгоритмом. Проверочный полином ГМВП вычисляется как произведение четырех полиномов, корни которых являются соответственно 7, 11, 13 и 37-ми степенями корней исходного примитивного полинома базисной МП. ЭЛС ГМВП равна l_s=32, т.е. в четыре раза превышает ЭЛС МП с таким же периодом. Всего в поле GF(2^8) существует шестнадцать примитивных полиномов 8-й степени и соответственно шестнадцать ГМВП с периодом N=255.

Значения ПВКФ ГМВП показаны в табл. 8. Функция корреляции вычисляется для ГМВП с проверочным полиномом $h_{г1}(x)=h_7(x)\cdot h_{11}(x)\cdot h_{13}(x)\cdot h_{37}(x)$, образованной на основе МП с полиномом $h_1(x)$, и ГМВП, образованных на основе МП с другими пятнадцатью примитивными полиномами $h_i(x)$. Для сокращения записи в первой графе табл. 8 вместо четырех сомножителей полинома ГМВП приводится только полином базисной МП. Например, для полинома $h_{МП}(x)=h_{11}(x)$ полиномом для ГМВП будет

$$h_{г11}(x) = h_{77}(x)\cdot h_{121}(x)\cdot h_{143}(x)\cdot h_{152}(x) = h_{53}(x)\cdot h_{47}(x)\cdot h_{31}(x)\cdot h_{19}(x).$$

Индексы „77“, „121“, „143“, „152“ являются показателями степени для p-сопряженных корней полиномов $h_{53}(x)$, $h_{47}(x)$, $h_{31}(x)$ и $h_{19}(x)$. Выражение $h_{г11}(x)$ здесь и далее используется для обозначения проверочного полинома ГМВП, построенного на основе базисной МП с полиномом $h_{МП}(x)=h_{11}(x)$.

Таблица 8

$h_i(x)$	Тип КФ	Число n значений ПВКФ ГМВП$_1$ и ГМВП$_2$ при $R(\tau)$																				
		95	63	47	39	35	31	27	23	19	15	11	7	3	–1	–5	–9	–13	–17	–21	–25	–29	–33
1—7	5			2	4		9	16			16	8	24	40	28	24	28		16	32		8	
11	2		4			8			16	8		8	40	24	43	24	8	40		16	16		
13	4		1	4					32		4	48		16	44	16	8	48	8		24		2
19	3			8			8				64				87				88				
23	6		2				20				56				89				88				
29_0	2		4			8			16	8		8	40	24	43	24	8	40		16	16		
31	1						40				16				119				80				
37	5			2	4		9	16			16	8	24	40	28	24	28		16	32		8	
43	7	2	1						8	16	4	48	24	16	36		24	32	20	16	8		
47	3			8			8				64				87				88				
53	8		4								96				59				96				
59	4		1	4					32		4	48		16	44	16	8	48	8		24		2
61	6		2				20				56				89				88				
91	1						40				16				119				80				
127	9						8	8	16	8	16	24	16	32	23	16	16	16	16	16	16	8	

Шаг 6. Формирование предпочтительных пар ГМВП на основе полученных ПП М-последовательностей. Условию (2) удовлетворяют только первый и девятый типы ПВКФ

ГМВП. Для первого типа это пары ГМВП с проверочными полиномами $h_{г1}(x)$—$h_{г31}(x)$ и $h_{г1}(x)$—$h_{г91}(x)$; для девятого типа — пары ГМВП с полиномами $h_{г1}(x)$ — $h_{г127}(x)$.

ПВКФ первого типа ПП ГМВП полностью соответствует первому типу ПВКФ ПП МП и принимает четыре значения, лежащие в интервале от –17 до +31:

$$R(\tau) \in \{-17(80), -1(119), +15(16), +31(40)\}.$$

Всего в поле $GF(2^8)$ можно сформировать 16 ПП ГМВП, сгруппированных в два множества по 8 ГМВП, как и в случае с ПП МП:

$$h_{г1}(x)–h_{г31}(x)–h_{г19}(x)–h_{г61}(x)–h_{г53}(x)–h_{г23}(x)–h_{г47}(x)–h_{г91}(x)–h_{г1}(x),$$
$$h_{г7}(x)–h_{г59}(x)–h_{г11}(x)–h_{г43}(x)–h_{г29}(x)–h_{г13}(x)–h_{г37}(x)–h_{г127}(x)–h_{г7}(x).$$

ПВКФ ГМВП девятого типа также принимает шестнадцать значений, лежащих в интервале от –29 до +31, но с другим распределением:

$$R(\tau) \in \{-29(8), -25(16), -21(16), -17(16), -13(16), -9(16), -5(16),$$
$$-1(23), 3(32), 7(16), 11(24), 15(16), 19(8), 23(16), 27(8), 31(8)\}.$$

ГМВП с ПВКФ девятого типа формируются на основе базисных МП с сопряженными полиномами. Данные пары ГМВП вследствие удовлетворения ПВКФ условию (2) также можно отнести к предпочтительным. Всего имеется восемь таких пар:

$$h_{г7}(x)–h_{г127}(x),\ h_{г7}(x)–h_{г31}(x),\ h_{г11}(x)–h_{г61}(x),\ h_{г13}(x)–h_{г47}(x),$$
$$h_{г19}(x)–h_{г59}(x),\ h_{г23}(x)–h_{г29}(x),\ h_{г37}(x)–h_{г91}(x),\ h_{г43}(x)–h_{г53}(x).$$

Таким образом, в результате проведенных исследований разработан алгоритм формирования предпочтительных пар ГМВП и определены ПП ГМВП для периодов N=63 и N=255.

На основании анализа корреляционных и структурных свойств М- и ГМВ-последовательностей можно сделать следующие выводы.

1. Для МП и ГМВП с периодом N=63 существует три типа ПВКФ, для последовательностей с периодом N=255 — девять типов ПВКФ.

2. Типы ПВКФ МП с проверочными полиномами $h_i(x)$ и $h_j(x)$ соответствуют типам ПВКФ ГМВП, сформированных на основе базисных МП с этими же полиномами.

3. Предпочтительными являются пары ГМВП, которые формируются на основе базисных ПП МП.

4. Для периода N=63 существует 6 ПП ГМВП с ПВКФ первого типа и 3 ПП ГМВП с ПВКФ третьего типа.

5. Для периода N=255 существует 16 ПП ГМВП с ПВКФ первого типа и 8 ПП ГМВП с ПВКФ девятого типа.

6. Структурная скрытность ГМВП с периодом N=63 в 2 раза больше, чем у МП, а с периодом N=255 — в 4 раза больше.

Результаты могут быть использованы при построении сигналов с расширенным спектром и систем сигналов с высокой структурной скрытностью для систем передачи цифровой информации.

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. *Ипатов В. П.* Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992. 152 с.

3. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение: Пер. с англ. М.: Изд. дом „Вильямс“, 2003. 1104 с.

4. *Ипатов В. П.* Широкополосные системы и кодовое разделение сигналов. Принципы и приложения: Пер. с англ. М.: Техносфера. 2007. 488 с.

5. *Golomb S. W., Gong G.* Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar. Cambridge Univ. Press, 2005. 438 p.

6. *Tsankov T., Trifonov T., Staneva L.* An algorithm for synthesis of phase manipulated signals with high structural complexity // J. Scientific & Appl. Research. 2013. Vol. 4. P. 80—87.

7. *Chung H. B., No J. S.* Linear span of extended sequences and cascaded GMW sequences // IEEE Transact. on Information Theory. 1999. Vol. 45, N 6. P. 2060—2065.

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

9. *Coulter R. S., Mesnager S.* Bent functions from involutions over $F(2^n)$ // IEEE Transact. on Information Theory. 2018. Vol. 64, N 4. P. 2979—2986.

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

11. *Popović B. M.* Optimum sets of interference-free sequences with zero autocorrelation zones // IEEE Transact. on Information Theory. 2018. Vol. 64, N 4. P. 2876—2882.

12. *Min Kyu Song, Hong-Yeop Song.* A construction of odd length generators for optimal families of perfect sequences // IEEE Transact. on Information Theory. 2018. Vol. 64, N 4. P. 2901—2909.

13. CDMA: прошлое, настоящее, будущее / Под ред. *Л. Е. Варакина* и *Ю. С. Шинакова*. М.: Международная акад. связи, 2003. 608 с.

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

15. *Liang H., Tang Y.* The cross correlation distribution of a p-ary m-sequence of period $p^m–1$ and its decimated sequences by $(p^k+1)(p^m+1)/4$ // Finite Fields and their Applications. 2015. Vol. 31. P. 137—161.

16. *Rizomiliotis P., Kalouptsidis N.* Results on the nonlinear span of binary sequences // IEEE Transact. on Information Theory. 2005. Vol. IT–51. P. 1555—1563.

17. *Стародубцев В. Г., Бородько Д. Н., Мышко В. В.* Алгоритм формирования ГМВ-последовательностей с периодом N=4095 в системах передачи телеметрической информации // Авиакосмическое приборостроение. 2018. № 5. С. 3—15.

18. *Стародубцев В. Г., Мышко В. В., Ткаченко В. В.* Аппаратная и программная реализация алгоритма формирования последовательностей Гордона—Миллса—Велча // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10, № 3. С. 13—20.

19. *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

Яна Вячеславовна Осадчая — слушатель; ВКА им. А. Ф. Можайского; E-mail: yana_osadchaya@mail.ru

Поступила в редакцию
03.04.19 г.

Ссылка для цитирования: *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.

PREFERRED PAIRS OF GMW–SEQUENCES FOR DIGITAL INFORMATION TRANSFER SYSTEMS

V. G. Starodubtsev[1,2], Ya. V. Osadchaya[1]

[1]*A. F. Mozhaysky Military Space Academy, 197198, St. Petersburg, Russia*
E-mail: vgstarod@mail.ru

[2]*ITMO University, 197101, St. Petersburg, Russia*

An analysis of periodic cross-correlation functions (PCCF) of M-sequences (MS) and Gordon-Mills-Welch sequences (GMWS), which have a two-level autocorrelation function, is presented. A higher structural secrecy of GMWS as compared with the MS determines the preference for the use of GMWS in digital information transmission systems (DITS) subject to increased confidentiality requirements. An algorithm for formation of preferred pairs of GMWS and their definitions for periods $N = 63$ and $N = 255$ are developed. Mathematical apparatus of the theory of finite fields, linear algebra and correlation analysis are used in the research. Values of PCCF of various pairs of MS and GMWS are obtained for periods $N = 63$ and $N = 255$. It is shown that GMWS, forming preferred pairs, are formed based on MS, also forming preferred pairs. The obtained results can be used in the formation of spread-spectrum signals in the noise-proof DITS, as well as in the synthesis of signal systems that allow an analytical representation in finite fields.

Keywords: pseudorandom sequences, preferred pairs, correlation function, structural secrecy, indivisible and primitive polynomials, finite fields

REFERENCES

1. Vishnevskiy V.M., Lyakhov A.I., Portnoy S.L., Shakhnovich I.V. *Shirokopolosnye besprovodnye seti peredachi informatsii* (Broadband Wireless Networks of Information Transfer), Moscow, 592 p. (in Russ.)
2. Ipatov V.P. *Periodicheskie diskretnye signaly s optimal'nymi korrelyatsionnymi svoystvami* (Periodic Discrete Signals with Optimum Correlation Properties), Moscow, 1992, 152 p. (in Russ.)
3. Sklar B. *Digital Communications: Fundamentals and Applications*, Prentice-Hall, 2001.
4. Ipatov V.P. *Spread Spectrum and CDMA. Principles and Applications*, Wiley, 2005, 400 p.
5. Golomb S.W., Gong G. *Signal Design for Good Correlation for Wireless Communication, Criptography and Radar*, Cambridge University Press, 2005, 438 p.
6. Tsankov T., Trifonov T., Staneva L. *Journal Scientific & Applied Research*, 2013, vol. 4, pp. 80–87.
7. Chung H.B., No J.S. *IEEE Trans. on Information Theory*, 1999, no. 6(45), pp. 2060–2065.
8. No Jong-Seon. *IEEE Trans. on Information Theory*, 1996, no. 1(42), pp. 260–262.
9. Coulter R.S., Mesnager S. *IEEE Trans. on Information Theory*, 2018, no. 4(64), pp. 2979–2986.
10. Zhengchun Zhou, Tor Helleseth, Udaya Parampalli. *IEEE Trans. on Information Theo*ry, 2018, no. 4(64), pp. 2896–2900.
11. Popović B.M. *IEEE Trans. on Information Theory*, 2018, no. 4(64), pp. 2876–2882.
12. Min Kyu Song, Hong-Yeop Song. *IEEE Trans. on Information Theory*, 2018, no. 4(64), pp. 2901–2909.
13. Varakin L.E., Shinakov Yu.S., ed., *CDMA: proshloe, nastoyashchee, budushchee* (CDMA: Last, Real, Future), Moscow, 2003, 608 p. (in Russ.)
14. Tao Zhang, Shuxing Li, Tao Feng, Gennian Ge. *IEEE Trans. on Information Theory*, 2014, no. 5(60), pp. 3062–3068.
15. Liang H., Tang Y. *Finite Fields and Their Applications*, 2015, vol. 31, pp. 137–161.
16. Rizomiliotis P., Kalouptsidis N. *IEEE Trans. on Information Theory*, 2005, vol. IT–51, pp. 1555–1563.
17. Starodubtsev V.G., Borodko D.N., Myshko V.V. *Aerospace Instrument-Making*, 2018, no. 5, pp. 3–15. (in Russ.)
18. Starodubtsev V.G., Myshko V.V., Tkachenko V.V. *H&ES Research,* 2018, no. 3(10), pp. 13–20. (in Russ.)
19. Peterson W.W. & Weldon E.J. *Error-Correcting Codes*, Second Edition, MIT Press, 1972, 560 p.

Data on authors

Victor G. Starodubtsev	—	PhD, Associate Professor; A. F. Mozhaysky Military Space Academy, Department of Technology and Means for Automation of Processing and Analysis of Space Facilities Information; ITMO University; E-mail: vgstarod@mail.ru
Yana V. Osadchaya	—	Student; A. F. Mozhaysky Military Space Academy; E-mail: yana_osadchaya@mail.ru

For citation: Starodubtsev V. G., Osadchaya Ya. V. Preferred pairs of GMW–sequences for digital information transfer systems. *Journal of Instrument Engineering*. 2019. Vol. 62, N 7. P. 610—620 (in Russian).

DOI: 10.17586/0021-3454-2019-62-7-610-620