УДК 519.725
DOI: 10.17586/0021-3454-2022-65-6-383-393

МНОЖЕСТВА ГМВ-ПОДОБНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ СИСТЕМ ПЕРЕДАЧИ И ОБРАБОТКИ ЦИФРОВОЙ ИНФОРМАЦИИ

В. Г. Стародубцев

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

Аннотация. Представлены два множества FF_{G1} и FF_{G2} последовательностей, подобных последовательностям Гордона—Миллса—Велча (ГМВ) в конечных полях GF(2^S) для значений S=2mod4. Множества ГМВ-подобных последовательностей (ГМВ ПП) характеризуются пятиуровневой периодической автокорреляционной и четырехуровневой взаимной корреляционными функциями. Максимальное значение модуля взаимной корреляционной функции $|R_{\max}| = (2^{S/2+1}-1)$ данных множеств меньше аналогичного значения для последовательностей Голда — $(2^{S/2+1}+1)$. Мощность множества ГМВ ПП FF_{G1} равна половине периода последовательностей $M_1 = (N+1)/2 = 2^{S/2}$. Все последовательности этого множества сбалансированы, т.е. их вес равен $V = 2^{S/2}$. Мощность множества ГМВ ПП FF_{G2} примерно равна периоду последовательностей $M_2 = (N+1) = 2^{S/2}$. Последовательности множества FF_{G2} являются несбалансированными, т.е. их вес может принимать четыре значения: $V = [2^{S/2-1}(2^{S/2}+1);\ 2^{S-1};\ 2^{S/2-1}(2^{S/2}-1);\ 2^{S/2}(2^{S/2-1}-1)]$. Показано, что формирование множеств ГМВ ПП с этими характеристиками мощности и корреляции возможно только для периодов N = 63, 1023, 16 383, 262 143, для которых существуют ГМВ-последовательности с проверочными полиномами степени 2^S.

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

Ссылка для цитирования: *Стародубцев В. Г.* Множества ГМВ-подобных последовательностей для систем передачи и обработки цифровой информации // Изв. вузов. Приборостроение. 2022. Т. 65, № 6. С. 383—393. DOI: 10.17586/0021-3454-2022-65-6-383-393.

SETS OF GMW-LIKE SEQUENCES FOR DIGITAL INFORMATION TRANSMISSION AND PROCESSING SYSTEMS

V. G. Starodubtsev

A. F. Mozhaisky Military Space Academy, St. Petersburg, Russia
vgstarod@mail.ru

Abstract. Two sets of sequences similar to Gordon-Mills-Welch (GMW) sequences in finite fields GF(2^S) for values S=2 mod 4 are presented. Sets of GMW-like sequences are characterized by a five-level periodic autocorrelation and a four-level cross-correlation function. For these sets, the maximum value of the modulus of the mutual correlation function $|R_{\max}| = (2^{S/2+1}-1)$ is less than the same value for Gold sequences equal to $(2^{S/2+1}+1)$. The power of one of the sets, FF_{G1}, is equal to half of the sequence period $M_1 = (N+1)/2 = 2^{S/2}$. All sequences of this set are balanced, that is, their weight is equal to $V = 2^{S/2}$. The power of the other set of GMW- like sequences, FF_{G2}, is approximately equal to the period of the sequences $M_2 = (N+1) = 2^{S/2}$. The sequences of FF_{G2} set are unbalanced, that is, their weight can take four values $V = [2^{S/2-1}(2^{S/2}+1);\ 2^{S-1};\ 2^{S/2-1}(2^{S/2}-1);\ 2^{S/2}\ (2^{S/2-1}-1)]$. It is shown that formation of sets of GMW-like sequences with these power and correlation characteristics is possible only for periods N = 63, 1023, 16383, 262143, for which there exist GMW sequences with verification polynomials of degree 2^S.

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

For citation: Starodubtsev V. G. Sets of GMW-like sequences for digital information transmission and processing systems. *Journal of Instrument Engineering.* 2022. Vol. 65, N 6. P. 383—393 (in Russian). DOI: 10.17586/0021-3454-2022-65-6-383-393.

Повысить помехозащищенность систем передачи цифровой информации (СПЦИ), в которых предусматривается корреляционная обработка фазоманипулированных сигналов с расширенным спектром (СРС), позволяет, в частности, применение псевдослучайных последовательностей (ПСП) с низким уровнем взаимной корреляции [1, 2]. При использовании в СПЦИ режима с кодовым многостанционным доступом для разделения каналов связи различных абонентов применяются фазоманипулированные сигналы на основе последовательностей Голда, Касами и др. [3—5].

Разработке методов и алгоритмов формирования ПСП и их множеств с низким уровнем взаимной корреляции посвящено большое количество научных работ [6—18]. В [6] рассмотрен метод построения бинарных последовательностей с асимптотически оптимальным ростом уровня боковых лепестков автокорреляционной и взаимной корреляционной функций из наборов последовательностей с хорошими корреляционными свойствами. В [7] представлен обобщенный циклотомический метод формирования новых семейств двоичных последовательностей, основанный на китайской теореме об остатках.

В последнее время внимание исследователей уделяется методам генерации совершенных целочисленных гауссовых последовательностей произвольной длины с нулевой автокорреляцией, которые находят применение в современных системах связи, таких как CDMA и OFDM [8—10]. Данные последовательности могут быть сформированы на основе следовых представлений последовательностей Лежандра, шестеричных последовательностей вычетов Холла, М-последовательностей (МП) и ГМВ-последовательностей над конечным полем GF(2^S) [11]. При этом шестеричная последовательность вычетов Холла обладает признаками псевдослучайности, имеет идеальную двухуровневую автокорреляцию и линейную сложность порядка величины ее периода [12].

В работах [13—15] исследуются алгоритмы построения последовательностей с непосредственной минимизацией интегрального уровня боковых лепестков корреляционной функции на основе общей структуры алгоритмов максимизации-минимизации. В некоторых телекоммуникационных приложениях используются последовательности с апериодической корреляцией [16]. В [17] проанализировано формирование пар конечных комплекснозначных последовательностей, основанных на различных последовательностях Чу и имеющих низкий уровень апериодических автокорреляционной и взаимной корреляционной функций по критерию Сарвате—Персли.

В [18] предложен эффективный метод формирования аффинных подсемейств, входящих в семейство последовательностей, формируемых с помощью нелинейного регистра сдвига с обратной связью. Эти последовательности обладают высокой структурной скрытностью, характеризующейся эквивалентной линейной сложностью.

Впервые термин „ГМВ-подобная последовательность“ (ГМВ ПП) применен в статье [19]. Данные последовательности формируются на основе тех же проверочных полиномов, что и ГМВ-последовательности, но при этом характеризуются пятиуровневой периодической автокорреляционной функцией (ПАКФ) и использованием в качестве базисной последовательности не только канонической МП, но и МП с произвольным начальным состоянием.

Цель настоящей статьи — разработка процедур формирования множеств ГМВ-подобных последовательностей с низким уровнем взаимной корреляции в конечных полях GF(2^S).

ГМВ ПП формируются на основе ГМВ-последовательностей в конечных полях $GF(2^S)$, для которых степень расширения является четным числом $S = 2m = 2\bmod 4$ и которые могут быть представлены в виде полей с двойным расширением $GF[(2^m)^2]$. Проверочные полиномы формируемых последовательностей должны иметь степень $2S$ и являться произведением только двух неприводимых полиномов, один из которых примитивный.

С учетом этих ограничений множества ГМВ ПП могут быть получены для периодов $N = 2^6–1 = 63$, $N = 2^{10}–1 = 1023$, $N = 2^{14}–1 = 16\,383$, $N = 2^{18}–1 = 262\,143$.

Символы g_i ГМВ-последовательности F_G с периодом $N = 2^{2m}–1$, которые используются для формирования ГМВ ПП, определяются выражением [4, 20]:

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

где $\mathrm{tr}_{a,b}(\cdot)$ — функция следа элемента поля $GF(2^a)$ в поле $GF(2^b)$; $\alpha \in GF(2^{2m})$ — примитивный элемент; r — натуральное число, взаимно простое с порядком мультипликативной группы поля $GF(2^m)$, равным $2^m - 1$.

Структурная скрытность ПСП определяется эквивалентной линейной сложностью (ЭЛС), которая для ГМВ-последовательностей имеет вид [4]:

$$l_s = m \cdot n^{\varphi(r)}, \qquad (2)$$

где $\varphi(r)$ — количество единиц в двоичном представлении числа r в (1).

Разработку процедур проведем на примере формирования множеств ГМВ ПП с периодом $N = 63$ в конечном поле $GF(2^6)$ при $S = 2\bmod 4$. Неприводимые полиномы шестой степени этого поля приведены в табл. 1 [21] (здесь и далее нижние индексы в обозначении полиномов соответствуют минимальным показателям степени их корней).

Таблица 1

Неприводимые полиномы в GF(2^6)

Полином	Корни полинома (показатели степеней)	Период корней
$h_1(x) = x^6 + x + 1$	$\alpha^1, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}$	63
$h_3(x) = x^6 + x^4 + x^2 + x + 1$	$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{48}, \alpha^{33}$	21
$h_5(x) = x^6 + x^5 + x^2 + x + 1$	$\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{40}, \alpha^{17}, \alpha^{34}$	63
$h_{11}(x) = x^6 + x^5 + x^3 + x^2 + 1$	11, 22, 44, 25, 50, 37	63
$h_{13}(x) = x^6 + x^4 + x^3 + x + 1$	13, 26, 52, 41, 19, 38	63
$h_{15}(x) = x^6 + x^5 + x^4 + x^2 + 1$	15, 30, 60, 57, 51, 39	21
$h_{23}(x) = x^6 + x^5 + x^4 + x + 1$	23, 46, 29, 58, 53, 43	63
$h_{31}(x) = x^6 + x^5 + 1$	31, 62, 61, 59, 55, 47	63

В рамках исследований будут рассмотрены процедуры формирования двух множеств ГМВ ПП: FF_{G1} и FF_{G2}.

Процедура формирования множества FF_{G1} основана на использовании канонической формы записи базисной МП $F_{\text{МП}}$ и различных циклических сдвигов сформированной на ее основе ГМВ-последовательности F_G.

В конечном поле $GF(2^S) = GF(2^6)$ с неприводимым полиномом $f(x) = x^6+x+1$ и примитивным элементом $\alpha = a$ символы c_i базисной МП $F_{\text{МП}}$ в канонической форме записываются с учетом (1) при $r = 1$ в виде

$$c_i = \mathrm{tr}_{S1}\alpha^i = \mathrm{tr}_{61}\alpha^i,\quad 0 \le i < 2^S–2 = 2^6–2 = 62. \qquad (3)$$

Начальные и конечные символы c_i канонической формы записи МП $F_{\text{МП}}$ с проверочным полиномом $h_{\text{МП}}(x)=x^6+x+1$ в соответствии с (3) приведены в табл. 2.

Таблица 2

Формирование ГМВ-последовательности F_G

i	0	1	2	3	4	5	6	7	8	9	10	11	…	53	54	55	56	57	58	59	60	61	62
c_i	0	0	0	0	0	1	0	0	0	0	1	1	…	1	0	1	0	1	1	1	1	1	1
c_{3i}	0	0	0	0	0	1	0	1	0	0	1	0	…	0	0	1	1	0	0	1	0	1	1
c_{5i}	0	1	1	1	1	1	1	0	1	0	1	1	…	0	0	1	0	0	0	1	0	1	1
g_i	0	1	1	1	1	0	1	1	1	0	0	1	…	0	0	0	1	0	0	0	0	0	0

На основании символов базисной МП вида (3) может быть сформирована ГМВ-последовательность F_G с проверочным полиномом $h_G(x)$, равным произведению двух неприводимых полиномов $h_{ci}(x)$, один из которых $h_5(x)$ является примитивным, а другой $h_3(x)$ — неприводимым, с корнями, имеющими период $N = 21$ [20, 21]:

$$h_G(x) = h_{c1}(x)h_{c2}(x) = h_3(x)h_5(x) = (x^6+x^4+x^2+x+1)(x^6+x^5+x^2+x+1). \tag{4}$$

Полиномы $h_{ci}(x)$ определены для случая $r = 3$ в (1). Так как $\varphi(r=3) = 2$, то ЭЛС ГМВ-последовательности, в соответствии с (2), равна $l_S = 12$.

ГМВ-последовательность F_G входит в множество FF_{G1}, а ее символы g_i, в соответствии с (4), могут быть получены путем суммирования по mod2 символов c_{3i} и c_{5i} двух последовательностей (см. табл. 2 — 3-я и 4-я строки), полученных путем децимации символов c_i базисной МП $F_{\text{МП}}$ по индексам децимации $i_{d1} = 3$ и $i_{d2} = 5$, соответствующих минимальным показателям степени корней полиномов $h_3(x)$ и $h_5(x)$:

$$g_i = c_{3i} \oplus c_{5i}, \quad 0 \le i < 2^S–2 = 62, \tag{5}$$

где вычисление индексов выполняется по mod63.

Множество ГМВ ПП FF_{G1} образуется из последовательностей $F_{G1,k}$, получаемых путем сложения по mod2 последовательности F_G и ее различных циклических сдвигов. С вычислительной точки зрения эта процедура соответствует определению ПАКФ полученной ГМВ-последовательности.

Для двоичных последовательностей ПАКФ определяется выражением [2, 4]:

$$R(\tau) = N–2D(\tau), \tag{6}$$

где $D(\tau)$ — расстояние по Хэммингу между циклическими сдвигами последовательностей для различных значений τ.

Для двоичных последовательностей расстояние $D(\tau)$ равно числу несовпадающих позиций в двух циклических сдвигах, что эквивалентно весу V последовательности, получаемой при суммировании по mod2 этих сдвигов.

Так как ПАКФ ГМВ-последовательности является четной функцией, то при первом способе формирования мощность множества ГМВП ПП FF_{G1} равна

$$M_1 = 2^{S–1} = (N+1)/2 = 32. \tag{7}$$

Множество FF_{G1} включает $(N–1)/2$ последовательность $F_{G1,k}$, получаемую при сложении двух циклических сдвигов ГМВ-последовательности F_G для $1 \le \tau \le 2^{S-1}–1 = 31$, и непосредственно исходную F_G. Вес каждой последовательности будет равен $V_1 = 2^{S–1} = 32$, так как ПАКФ ГМВ-последовательности является двухуровневой. При значениях сдвига $32 = 2^{S–1} \le \tau \le 2^S–2 = 62$ формируются циклические сдвиги уже рассмотренных последовательностей. В этом случае значения сдвигов τ определяются из условия равенства суммы значений $2^S–1 = 63$. Например, циклическими сдвигами являются последовательности при $\tau_1 = 5$ и $\tau_2 = 58$, а также при $\tau_1 = 17$ и $\tau_2 = 46$.

Определим периодическую взаимную корреляционную функцию (ПВКФ) некоторых пар последовательностей $F_{G1,k}$, как входящих в множество ГМВ ПП FF_{G1}, так и являющихся циклическими сдвигами. Номер последовательности k соответствует циклическому сдвигу τ. Начальные и конечные сегменты некоторых последовательностей $F_{G1,k}$ приведены в табл. 3. Вес всех последовательностей равен $V_k = 32$.

Таблица 3

Сегменты последовательностей $F_{G1,k}$ множества ГМВ ПП FF_{G1}

$F_{G1,k}$	Символы последовательностей для k																				
	0	1	2	3	4	5	6	7	8	9	10	…	53	54	55	56	57	58	59	60	61	62
$F_{G1,0}$	0	1	1	1	1	0	1	1	1	0	0	…	0	0	0	1	0	0	0	0	0	0
$F_{G1,1}$	0	1	0	0	0	1	1	0	0	1	0	…	1	0	0	1	1	0	0	0	0	0
$F_{G1,2}$	0	1	1	0	0	1	0	1	0	1	1	…	0	1	0	1	0	1	0	0	0	0
$F_{G1,5}$	0	1	1	1	1	0	0	0	0	1	0	…	1	1	1	1	1	0	0	0	1	0
$F_{G1,17}$	0	1	0	0	0	0	0	1	1	0	1	…	0	1	1	1	0	1	1	0	1	0
$F_{G1,46}$	0	1	0	1	0	1	1	0	0	1	0	…	1	1	0	1	1	1	1	1	0	1
$F_{G1,58}$	0	0	0	0	1	0	0	0	0	1	0	…	0	0	0	1	0	0	1	1	1	1

Проверочные полиномы для рассмотренных последовательностей могут быть получены из выражения (4).

Значения ПВКФ последовательностей $F_{G1,1}$ и $F_{G1,2}$, входящих в множество ГМВ ПП FF_{G1}, для произвольного сдвига $\tau = 21i+j$ приведены в табл. 4.

Таблица 4

Значения $R_{1,2}(\tau)$ ПВКФ последовательностей $F_{G1,1}$ и $F_{G1,2}$

	j																				
i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	–1	–1	15	–9	7	15	–1	–9	–9	7	15	–1	–1	–1	15	–9	–1	–9	15	–9	–9
1	–9	–1	–1	–9	–1	15	–9	–9	–1	7	–9	–1	–1	15	–9	–1	–9	–1	–1	–9	15
2	7	–9	7	–9	15	–9	–9	7	7	–1	–1	–1	–9	–9	–1	15	–1	7	7	–1	–1

Анализ показывает, что ПВКФ является четырехуровневой и принимает следующие значения (в скобках приведено число соответствующих значений для одного периода):

$$R_{1,2}(\tau) = [-9(21), -1(23), 7(9), 15(10)]. \tag{8}$$

Особенностью первого множества ГМВ ПП FF_{G1} является то, что для каждой корреляционной функции сумма значений ПВКФ равна

$$W_{G1} = \sum_{\tau=0}^{\tau=2^S-2=62} R(\tau) = 1. \tag{9}$$

Например, для выражения (8) $W_{G1} = (-9)\times21+(-1)\times23+7\times9+15\times10 = 1$.

Значения ПВКФ последовательностей $F_{G1,5}$ и $F_{G1,17}$, также входящих в множество ГМВ ПП, приведены в табл. 5.

Таблица 5

Значения $R_{5,17}(\tau)$ ПВКФ последовательностей $F_{G1,5}$ и $F_{G1,17}$

	j																				
i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	–1	–9	–1	–9	–9	–1	–1	–1	–1	15	–1	15	–1	–1	–9	–9	–1	15	15	–1	–1
1	15	7	–9	7	–9	–9	–1	–9	–1	7	–9	7	7	15	7	15	7	–9	–9	–1	–9
2	–1	–1	–9	7	–1	–9	–1	7	–1	–1	–9	–9	7	7	–1	–9	–1	15	–9	–1	–1

ПВКФ данных последовательностей также является четырехуровневой и удовлетворяет выражению (9), но с другим распределением числа значений

$$R_{5,17}(\tau) = [-9(19), -1(25), 7(11), 15(8)].$$

Значения ПАКФ последовательностей $F_{G1,5}$ и $F_{G1,58}$, а также $F_{G1,17}$ и $F_{G1,46}$, являющихся циклическими сдвигами, приведены в табл. 6 и 7.

Таблица 6

Значения $R_{5,58}(\tau)$ ПАКФ последовательностей $F_{G1,5}$ и $F_{G1,58}$

	j																				
i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	–1	–1	7	–1	7	**63**	7	–1	7	–1	–1	–9	–9	–1	–1	–1	7	–1	15	–1	–1
1	–1	–9	–1	–9	–9	–1	–9	–1	7	7	15	–1	–9	–1	–9	–9	–9	–9	–1	–9	–1
2	15	7	7	–1	–9	–1	–9	–9	–1	–9	–1	–1	–1	15	–1	7	–1	–1	–1	–9	–9

Таблица 7

Значения $R_{17,46}(\tau)$ ПАКФ последовательностей $F_{G1,17}$ и $F_{G1,46}$

i	j																				
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	–1	7	7	–9	7	–1	–9	–1	–1	–9	–9	7	–9	–1	–1	–1	–1	**63**	–1	–1	–1
1	–1	–9	7	–9	–9	–1	–1	–9	–1	7	–9	7	7	–1	–1	15	–9	–1	7	–1	–9
2	15	–9	–1	–1	–1	–9	–1	–1	–9	–1	–1	–1	–9	15	–9	–1	7	–1	–9	15	–1

ПАКФ данных последовательностей является пятиуровневой

$$R_{5,58}(\tau) = R_{17,46}(\tau) = [-9(18), -1(30), 7(10), 15(4), 63(1)]$$

и также удовлетворяет выражению (9):

$$W_{G1} = (-9)\times18+(-1)\times30+7\times10+15\times4+63\times1 = 1.$$

Максимальное значение ПАКФ $R(\tau) = 63$ для циклических сдвигов (выделено полужирным шрифтом) достигается при сдвигах τ, равных номерам первых последовательностей.

Таким образом, при формировании первого множества ГМВ ПП FF_{G1} его мощность определяется выражением (7) и равна $M_1 = 32$, ПВКФ является четырехуровневой и принимает следующие значения:

$$R_{ij}(\tau) = [-(2^{S/2}+1), -1, (2^{S/2}-1), (2^{S/2+1}-1)] = (-9, -1, 7, 15). \tag{10}$$

Для сравнения приведем значения трехуровневой ПВКФ последовательностей Голда для периода $N = 2^S-1 = 63$ ($S = 2\text{mod}4$) [4, 5]:

$$R_{ij}(\tau) = [-(2^{S/2+1}+1), -1, (2^{S/2+1}-1)] = (-17, -1, 15). \tag{11}$$

Отметим, что максимальное значение модуля ПВКФ последовательностей Голда на 12 % превышает аналогичное значение для множества ГМВ ПП.

Процедура формирования множества ГМВ ПП FF_{G2} основана на использовании произвольного k-го циклического сдвига базисной МП $F_{\text{МП},k}$. В этом случае при сложении последовательностей, децимированных по индексам 3 и 5, в соответствии с полиномами $h_{ci}(x)$, вместо F_G формируется ГМВ-подобная последовательность $F_{G2,k}$, ПАКФ которой является пятиуровневой [19].

В соответствии с (3) символы c_i МП, представленные в канонической форме, при циклическом сдвиге на τ определяются выражением

$$c_i = \text{tr}_{S1}\alpha^{i+\tau} = \text{tr}_{61}\alpha^{i+\tau}, \quad 0 \le i < 2^S-2 = 62. \tag{12}$$

Начальные и конечные символы МП $F_{\text{МП},k}$ в соответствии с (12) при $\tau = 5$ (сдвиг МП влево) приведены в табл. 8 (вторая строка).

Таблица 8

Символы c_i МП $F_{\text{МП},k}$ при сдвиге $\tau = 5$ и символы q_i ГМВ ПП $F_{G2,k}$

i	0	1	2	3	4	5	6	7	8	9	10	…	53	54	55	56	57	58	59	60	61	62
c_i	1	0	0	0	0	1	1	0	0	0	1	…	1	1	1	1	1	0	0	0	0	0
c_{3i}	1	0	1	0	1	1	1	0	1	0	0	…	0	0	1	1	1	1	0	1	1	0
c_{5i}	1	1	1	1	1	1	0	1	0	1	1	…	0	1	0	0	0	1	0	1	1	0
q_i	0	1	0	1	0	0	1	1	1	1	1	…	0	1	1	1	1	0	0	0	0	0

На основании символов базисной МП $F_{\text{МП},k}$ вида (12) формируется ГМВ-подобная последовательность с проверочным полиномом $h_G(x)$ вида (4) и ЭЛС $l_S = 12$. Символы q_i ГМВ ПП $F_{G2,k}$ могут быть получены аналогично символам g_i ГМВ-последовательности F_G путем суммирования по mod2 новых значений символов c_{3i} и c_{5i} двух последовательностей (табл. 8).

Полный набор последовательностей $F_{G2,k}$ этого множества формируется для всех возможных циклических сдвигов базисной МП. Соответственно мощность множества ГМВ ПП FF_{G2} в этом случае равна

$$M_2 = 2^S – 1 = N = 63 \qquad (13)$$

с учетом исходной ГМВ-последовательности для базисной МП в канонической форме.

Последовательность $F_{G2,k}$ (k = 1—63) множества FF_{G2} удобно нумеровать в соответствии с начальным состоянием циклического сдвига базисной МП, представленным в десятичной форме. Для периода $N = 63$ при начальном состоянии $c_0 = 1$, $c_i = 0$ (i = 1—5) базисной МП в каноническом виде формируется ГМВ-последовательность $F_G = F_{G2,1}$. При остальных начальных состояниях формируются ГМВ ПП $F_{G2,k}$. В табл. 9 приведены некоторые последовательности $F_{G2,k}$ с различным весом V_k.

Таблица 9

Сегменты последовательностей $F_{G2,k}$ множества ГМВ ПП FF_{G2}

$F_{G2,k}$	V_k	Символы последовательностей для k																				
		0	1	2	3	4	5	6	7	8	9	10	…	53	54	55	56	57	58	59	60	61	62
$F_{G3,1}$	32	0	1	1	1	1	0	1	1	1	0	0	…	0	0	0	1	0	0	0	0	0	0
$F_{G3,7}$	32	0	0	0	0	1	1	1	0	1	1	0	…	0	0	0	1	1	1	0	0	1	0
$F_{G3,2}$	36	0	0	1	1	1	0	1	1	1	1	0	…	1	1	1	0	0	1	1	1	1	0
$F_{G3,5}$	36	0	0	1	1	0	1	0	1	0	0	0	…	1	1	1	1	1	0	1	1	0	0
$F_{G3,11}$	28	0	1	0	0	0	0	1	0	1	0	1	…	1	1	0	0	0	0	0	1	0	1
$F_{G3,26}$	28	0	0	0	1	1	1	0	1	1	1	0	…	1	1	1	0	1	1	0	0	0	0
$F_{G3,48}$	24	0	0	0	0	1	1	0	0	1	0	0	…	0	1	0	1	0	1	0	1	0	1
$F_{G3,60}$	24	0	1	0	0	0	0	0	0	1	1	1	…	1	0	0	0	1	0	0	0	1	0

Множество ГМВ ПП FF_{G2} с $N = 63$ и базисной МП с проверочным полиномом $h(x) = x^6 + x + 1$ характеризуется следующим распределением весов последовательностей (в скобках указано число последовательностей):

$$V_k = [36(18), 32(28), 28(8), 24(9)]. \qquad (14)$$

В табл. 10 приведено распределение числа различных значений ПВКФ последовательности $F_{G2,1}$ с последовательностями $F_{G2,k}$. Также показана сумма значений ПВКФ $W_{1,k}$ последовательности $F_{G2,1}$ с $F_{G2,k}$.

Таблица 10

Распределение значений ПВКФ последовательностей $F_{G2,1}$ и $F_{G2,k}$

k	2	3	4	5	6	7	8	9		56	57	58	59	60	61	62	63
V_k	36	36	36	36	28	32	36	36		32	32	28	28	24	36	32	32
$R_1 = –9$	18	18	18	18	21	18	18	18		18	18	21	21	18	18	18	18
$R_2 = –1$	27	27	27	27	21	29	27	27		29	29	21	21	30	27	29	29
$R_3 = 7$	9	9	9	9	14	6	9	9		6	6	14	14	6	9	6	6
$R_4 = 15$	9	9	9	9	7	10	9	9		10	10	7	7	9	9	10	10
$W_{1,k}$	9	9	9	9	–7	1	9	9		1	1	–7	–7	–15	9	1	1

В соответствии с (6) каждому значению веса V_k последовательности $F_{G2,k}$ можно формально сопоставить корреляционную функцию $R_{G2,k} = N – 2V_k$. Тогда выражение (9) для суммарной величины ПВКФ определяется произведением значений корреляционных функций:

$$W_{k,l} = \sum_{\tau=0}^{\tau=2^S-2=62} R(\tau) = R_{G2,k} \times R_{G2,l} = (N - 2V_k)(N - 2V_l). \qquad (15)$$

Так как вес последовательности $F_{G2,1}$ равен $V_1 = 32$, а веса V_l остальных последовательностей множества ГМВ ПП FF_{G2} могут принимать четыре значения (24, 28, 32 и 36), то сумма значений ПВКФ $W_{1,k} = 2V_k – N$ также может принимать четыре значения: –15, –7, 1, 9.

В табл. 11 приведены значения ПВКФ последовательности $F_{G2,2}$, вес которой составляет $V_2 = 36$, с последовательностями $F_{G2,k}$. В этом случае сумма значений ПВКФ будет равна $W_{2,k} = 9(2V_k – N)$ и также может принимать четыре значения: –135, –63, 9, 81.

Таблица 11

Распределение значений ПВКФ ГМВ ПП $F_{G2,2}$ с ГМВ ПП $F_{G2,k}$

k	3	4	5	6	7	8	9	10		56	57	58	59	60	61	62	63
V_k	36	36	36	28	32	36	36	32		32	32	28	28	24	36	32	32
$R_1 = -9$	15	15	18	17	22	14	15	15		15	19	19	20	26	11	22	16
$R_2 = -1$	27	28	20	34	20	28	28	32		32	28	31	29	24	32	22	31
$R_3 = 7$	9	7	14	7	11	10	7	8		8	4	7	8	9	11	7	7
$R_4 = 15$	12	13	11	5	10	11	13	8		8	12	6	6	4	9	12	9
$W_{2,k}$	81	81	81	–63	9	81	81	9		9	9	–63	–63	–135	81	9	9

Аналогично можно показать, что сумма значений ПВКФ последовательности $F_{G2,k}$ с весом 28 с остальными последовательностями равна $W_k = 7(N - 2V_k)$ и также принимает четыре значения: –63, –7, 49, 105.

Сумма значений ПВКФ последовательности $F_{G2,k}$ с весом 24 равна $W_k = 15(N - 2V_k)$ и принимает четыре значения: –135, –15, 105, 225.

Для проверки отсутствия циклических сдвигов среди последовательностей множества ГМВ ПП FF_{G2} с весом 24 и 28 в табл. 12 приведены значения ПВКФ последовательностей с одинаковыми весами. Для вычислений взяты последовательности $F_{G2,15}$ с весом $V_{15} = 24$ и $F_{G2,6}$ с весом $V_6 = 28$.

Таблица 12

Распределение значений ПВКФ ГМВ ПП $F_{G2,k}$ с V_k = 24, 28

Параметр	ПВКФ $F_{G2,15}$ с $F_{G2,k}$ с $V_k = 24$									ПВКФ $F_{G2,6}$ с $F_{G2,k}$ с $V_k = 28$							
K	22	24	32	36	38	47	48	60		k	11	20	26	28	31	58	59
V_k	24	24	24	24	24	24	24	24		V_k	28	28	28	28	28	28	28
$R_1 = -9$	8	8	10	4	12	10	12	4		$R_1 = -9$	14	14	16	16	20	12	18
$R_2 = -1$	27	27	23	33	21	23	21	33		$R_2 = -1$	29	29	26	26	20	32	23
$R_3 = 7$	12	12	14	12	12	14	12	12		$R_3 = 7$	12	12	12	12	12	12	12
$R_4 = 15$	16	16	16	14	18	16	18	14		$R_4 = 15$	8	8	9	9	11	7	10
W_{15}	225	225	225	225	225	225	225	225		W_6	49	49	49	49	49	49	49

Таким образом, определяемая выражением (13) мощность второго множества ГМВ ПП FF_{G2} с периодом $N = 63$ равна $M_2 = 63$, ПВКФ является четырехуровневой и принимает значения в соответствии с (10). Суммарная величина ПВКФ последовательностей множества удовлетворяет (15).

Для формирования множеств ГМВ ПП с периодами $N = 2^{10}–1= 1023$; $2^{14}– 1= 16\,383$ и $2^{18}–1= 262\,143$ необходимо определить проверочные полиномы $h_{МП}(x)$ для базисных МП, а также пары полиномов $h_{ci}(x)$ для получения проверочных полиномов $h_G(x)$ вида (4) ГМВ-последовательностей.

В табл. 13 приведены основные характеристики множеств ГМВ ПП.

Таблица 13

Характеристика множеств ГМВ ПП с периодами $N = 2^S–1$

S	N	$h_{МП}(x)$	$h_{c1}(x)$	$h_{c2}(x)$	$M_1=2^{S–1}$	$M_2=2^S–1$	$R(\tau)$	$\lvert r_{max}\rvert$
6	63	x^6+x+1	$h_3(x)$	$h_5(x)$	32	63	–9, –1, 7, 15	0,24
10	1023	$x^{10}+x^3+1$	$h_3(x)$	$h_{17}(x)$	512	1023	–33, –1, 31, 63	0,06
			$h_5(x)$	$h_9(x)$	512	1023	–33, –1, 31, 63	0,06
14	16383	$x^{14}+x^{10}+x^6+x+1$	$h_3(x)$	$h_{65}(x)$	8192	16383	–129, –1, 127, 255	0,016
			$h_5(x)$	$h_{33}(x)$	8192	16383	–129, –1, 127, 255	0,016
			$h_9(x)$	$h_{17}(x)$	8192	16383	–129, –1, 127, 255	0,016
18	262143	$x^{18}+x^7+1$	$h_3(x)$	$h_{257}(x)$	131072	262143	–513, –1, 511, 1023	0,004
			$h_5(x)$	$h_{129}(x)$	131072	262143	–513, –1, 511, 1023	0,004
			$h_9(x)$	$h_{65}(x)$	131072	262143	–513, –1, 511, 1023	0,004
			$h_{17}(x)$	$h_{33}(x)$	131072	262143	–513, –1, 511, 1023	0,004

При допустимых значениях S показаны полиномы $h_{МП}(x)$ для базисных МП [21], пары полиномов-сомножителей $h_{ci}(x)$ с целью получения проверочных полиномов $h_G(x)$ [20], мощности множеств M_1 и M_2, а также значения функции корреляции и коэффициента корреляции. С увеличением периода последовательностей происходит уменьшение максимально возможного значения модуля коэффициента корреляции $|r_{\max}|= |R_{\max}|/N$.

При периоде $N = 63$ для каждого из шести примитивных полиномов можно сформировать по одному множеству ГМВ ПП; при $N = 1023$ для каждого из 60 примитивных полиномов — по два множества ГМВ ПП. При периоде $N = 16\,383$ для каждого из 756 примитивных полиномов — по три множества ГМВ ПП, а при $N = 262\,143$ для каждого из 7776 примитивных полиномов — по четыре множества ГМВ ПП.

Таким образом, в статье разработаны процедуры формирования двух множеств ГМВ ПП FF_{G1} и FF_{G2}. Мощности множеств FF_{G1} и FF_{G2} определяются выражениями (7) и (13) и равны половине периода и периоду последовательностей соответственно. При этом последовательности множества FF_{G1} являются сбалансированными, их вес равен $V_1 = 2^{S-1}$.

Вес последовательностей $F_{G2,k}$ ($k = 0$—2^{S-1}–1) множества FF_{G2} может принимать четыре значения

$$V_2 = [2^{S/2-1}(2^{S/2}+1);\ 2^{S-1};\ 2^{S/2-1}\,(2^{S/2}-1);\ 2^{S/2}(2^{S/2-1}-1)]. \qquad (16)$$

ПВКФ всех последовательностей множеств FF_{G1} и FF_{G2} является четырехуровневой:

$$R_{ij}(\tau) = [-(2^{S/2}+1),\ -1,\ (2^{S/2}-1),\ (2^{S/2+1}-1)]. \qquad (17)$$

Суммарная величина ПВКФ, определяемая выражением (15), может принимать десять значений в интервале

$$W_{kl} = [-\,(2^{S/2}+1)\,(2^{S/2+1}-1)\ldots\,(2^{S/2+1}-1)^2].$$

Полученные результаты по формированию множеств ГМВ-подобных последовательностей могут быть использованы в СПЦИ в режиме кодового многостанционного доступа для разделения каналов связи различных абонентов наряду с фазоманипулированными сигналами на основе последовательностей Голда, Касами и др. Достоинствами предлагаемых множеств могут служить сбалансированность последовательностей $F_{G1,k}$ и более низкий, по сравнению с последовательностями Голда, уровень взаимной корреляции.

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. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. М.: Вильямс, 2003. 1104 с.
3. *Gold R.* Maximal recursive sequences with 3-valued recursive cross-correlation functions // IEEE Trans. Inf. Theory. 1968. Vol. 14, N 1. P. 154.
4. *Golomb S. W., Gong G.* Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar. Cambridge University Press, 2005. 438 p.
5. CDMA: прошлое, настоящее, будущее / Под ред. Л. *Е. Варакина и Ю. С. Шинакова*. М.: МАС, 2003. 608 с.
6. *Bose A., Soltanalian M.* Constructing Binary Sequences with Good Correlation Properties: An Efficient Analytical-Computational Interplay // IEEE Trans. Signal Process. 2018. Vol. 66, N 11. P. 2998.
7. *Shen X., Jia Y., Song X.* Constructions of binary sequence pairs of period 3p with optimal three-level correlation // IEEE Commun. Lett. 12017. Vol. 21, N 10. P. 12150.
8. *Chang H. H., Li C. P., Lee C. D., Wang S. H., Wu T. C.* Perfect Gaussian integer sequences of arbitrary composite length // IEEE Trans. Inf. Theory. 2015. Vol. 61, N 7. P. 4107.
9. *Pei S. C., Chang K. W.* Arbitrary Length Perfect Integer Sequences Using All-Pass Polynomial // IEEE Signal Processing Letters. 2019. Vol. 26, N 8. P. 1112.
10. *Pei S. C., Chang K. W.* Perfect Gaussian integer sequences of arbitrary length // IEEE Signal Processing Letters. 2015. Vol. 22, N 8. P. 1040.

11. *Lee C. D., Huang Y. P., Chang Y., Chang H. H.* Perfect Gaussian Integer Sequences of Odd Period $2^m - 1$ // IEEE Signal Processing Letters IEEE. 2015. Vol. 22, N 7. P. 881.

12. *Aly H., Winterhof A.* A Note on Hall's Sextic Residue Sequence: Correlation Measure of Order // IEEE Trans. Inf. Theory. 2020. Vol. 66, N 3. P. 1944.

13. *Song J., Babu P., Palomar D. P.* Optimization Methods for Designing Sequences with Low Autocorrelation Sidelobes // IEEE Trans. Signal Process. 2015. Vol. 63, N 5. P. 3998.

14. *Song J., Babu P., Palomar D. P.* Sequence Set Design with Good Correlation Properties Via Majorization-Minimization // IEEE Trans. Signal Process. 2016. Vol. 64, N 11. P. 2866.

15. *Yang Y., Tang X.* Generic Construction of Binary Sequences of Period 2 N with Optimal Odd Correlation Magnitude Based on Quaternary Sequences of Odd Period N // IEEE Trans. Inf. Theory. 2018. Vol. 64, N 1. P. 384.

16. *Katz D. J.* Aperiodic Crosscorrelation of Sequences Derived from Characters // IEEE Trans. Inf. Theory. 2016. Vol. 62, N 9. P. 5237.

17. *Günther C., Schmidt K. U.* Sequence Pairs with Asymptotically Optimal Aperiodic Correlation // IEEE Trans. Inf. Theory. 2019. Vol. 65, N 8. P. 5233.

18. *Zhang J. M., Tian T. T., Qi W. F., Zheng Q. X.* A New Method for Finding Affine Sub-Families of NFSR Sequences // IEEE Trans. Inf. Theory. 2019. Vol. 65, N 2. P. 1249.

19. *Владимиров С. С., Когновицкий О. С., Стародубцев В. Г.* Формирование и обработка ГМВ-подобных последовательностей на основе двойственного базиса // Труды учебных заведений связи. 2019. Т. 5, № 4. С. 16—27.

20. *Стародубцев В. Г.* Метод синтеза последовательностей Гордона—Миллса—Велча для систем передачи дискретной информации // Радиотехника и электроника. 2020. № 2. С. 15.

21. *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; Военно-космическая академия им. А. Ф. Можайского, кафедра технологий и средств автоматизации обработки и анализа информации космических средств; E-mail: vgstarod@mail.ru

Поступила в редакцию 18.03.22; одобрена после рецензирования 05.04.22; принята к публикации 25.04.22.

REFERENCES

1. Ipatov V.P. *Spread Spectrum and CDMA. Principles and Applications,* NY, John Wiley and Sons Ltd., 2005, 488 p.
2. Sklar B. *Digital Communications: Fundamentals and Applications*, Prentice Hall, 2001, 1079 p.
3. Gold R. *IEEE Trans. Inf. Theory*, 1968, no. 1(14), pp. 154.
4. Golomb S.W., Gong G. *Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar*, Cambridge University Press, 2005, 438 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. Bose A., Soltanalian M. *IEEE Trans. Signal Process*, 2018, no. 11(66), pp. 2998.
7. Shen X., Jia Y., Song X. *IEEE Commun. Lett*., 2017, no. 10(21), pp. 12150.
8. Chang H.H., Li C.P., Lee C.D., Wang S.H., Wu T.C. *IEEE Trans. Inf. Theory*, 2015, no. 7(61), pp. 4107.
9. Pei S.C., Chang K.W. *IEEE Signal Processing Letters*, 2019, no. 8(26), pp. 1112.
10. Pei S.C., Chang K.W. *IEEE Signal Processing Letters*, 2015, no. 8(22), pp. 1040.
11. Lee C.D., Huang Y.P., Chang Y., Chang H.H. *IEEE Signal Processing Letters IEEE*, 2015, no. 7(22), pp. 881.
12. Aly H., Winterhof A. *IEEE Trans. Inf. Theory*, 2020, no. 3(66), pp. 1944.
13. Song J., Babu P., Palomar D.P. *IEEE Trans. Signal Process*, 2015, no. 15(63), pp. 3998.
14. Song J., Babu P., Palomar D.P. *IEEE Trans. Signal Process*, 2016, no. 11(64), pp. 2866.
15. Yang Y., Tang X. *IEEE Trans. Inf. Theory*, 2018, no. 1(64), pp. 384.
16. Katz D.J. *IEEE Trans. Inf. Theory*, 2016, no. 9(62), pp. 5237.
17. Günther C., Schmidt K.U. *IEEE Trans. Inf. Theory*, 2019, no. 8(65), pp. 5233.
18. Zhang J.M., Tian T.T., Qi W.F., Zheng Q.X. *IEEE Trans. Inf. Theory*, 2019, no. 2(65), pp. 1249.
19. Vladimirov S.S., Kognovitsky O.S., Starodubtsev V.G. *Trudy uchebnykh zavedeniy svyazi*, 2019, no. 4(5), pp. 16–27. (in Russ.)

20. Starodubtsev V.G. *Journal of Communications Technology and Electronics*, 2020, no. 2(65), pp. 155–159.
21. Peterson W.W., Weldon E.J. *Error-correcting Codes*, The MIT PRESS, Cambridge, Massachusetts and London, England, 1972, 588 p.

Data on author

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

Received 18.03.22; approved after reviewing 05.04.22; accepted for publication 25.04.22.