РАДИОТЕХНИКА И ЭЛЕКТРОНИКА, 2021, том 66, № 8, с. 810–814

ТЕОРИЯ И МЕТОДЫ ОБРАБОТКИ СИГНАЛОВ

УДК 519.725;512.62

ЛИНЕЙНАЯ СЛОЖНОСТЬ НЕДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОРДОНА–МИЛЛСА–ВЕЛЧА

© 2021 г. В. Г. Стародубцев[a, b, *]

[a] *Военно-космическая академия им. А.Ф. Можайского, ул. Ждановская, 13, Санкт-Петербург, 197198 Российская Федерация*

[b] *Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Кронверкский просп., 49, Санкт-Петербург, 197101 Российская Федерация*

**E-mail: vgstarod@mail.ru*

Поступила в редакцию 29.03.2020 г.
После доработки 22.11.2020 г.
Принята к публикации 23.11.2020 г.

Представлено выражение для определения эквивалентной линейной сложности (ЭЛС) l_S p-ичных ($p > 2$) последовательностей Гордона–Миллса–Велча (ГМВП) с периодом $N = p^S - 1$, формируемых в конечных полях $GF(p^S) = GF[(p^m)^n]$, для значения параметра $n = 2$. Выражение получено на основе анализа ЭЛС известных троичных с периодами $N = 80$, 728 и пятеричных ГМВП с периодами $N = 24$, 124, 624, а также с учетом особенностей вычисления ЭЛС для двоичных последовательностей. Определены значения ЭЛС для троичных, пятеричных, семеричных, одиннадцатеричных и тринадцатеричных ГМВП, алгоритмы формирования которых в известной литературе отсутствуют.

DOI: 10.31857/S003384942107010X

Существующие системы передачи цифровой информации (СПЦИ), включающие системы управления, связи, навигации и радиолокации, характеризуются широким применением сигналов с расширенным спектром (СРС), которые формируются на основе псевдослучайных последовательностей (ПСП) [1–4]. В настоящее время в основном используются двоичные ПСП, обладающие как хорошими периодическими автокорреляционными (ПАКФ) и взаимно корреляционными функциями (ПВКФ), так и структурной скрытностью, в качестве показателя которой выступает эквивалентная линейная сложность (ЭЛС), численно равная степени проверочного полинома, на основании которого формируется данная последовательность [5–7].

В качестве ПСП часто используются как М-последовательности (МП), так и последовательности, формируемые на их основе, такие как последовательности Голда, малого и большого множеств Касами [3, 6]. Основной причиной широкого применения МП является то, что данная последовательность является минимаксной, т.е. имеющей минимально возможный для бинарных кодов боковой лепесток ПАКФ. При этом ЭЛС как двоичных, так и недвоичных МП, формируемых в конечных полях $GF(p^S) = GF[(p^m)^n]$, равна $l_S = S$ [2, 6–8].

Наряду с МП к классу минимаксных последовательностей относятся последовательности Гордона–Миллса–Велча (ГМВП). Однако ЭЛС ГМВП существенно превышает ЭЛС МП, причем в зависимости от периода выигрыш может составлять от 2 до 50 и более раз [8–10]. Данное обстоятельство определяет целесообразность применения ГМВП вместо МП в СПЦИ, в которых требуются минимаксные ПСП с повышенной структурной скрытностью.

Одним из направлений повышения эффективности функционирования СПЦИ является переход к многопозиционным сигналам, которые формируются на основе недвоичных ПСП. Вопросам разработки алгоритмов формирования и анализа корреляционных и структурных свойств недвоичных ПСП посвящено большое количество работ как в нашей стране, так и за рубежом [11–20]. В [11] разработан алгоритм формирования и проведен анализ корреляционных свойств семейства p-ичных последовательностей с небольшими значениями взаимной корреляционной функции. В [12] проведен достаточно подробный анализ состояния вопроса формирования недвоичных ПСП и систем ПСП с заданными корреляционными и структурными свойствами. В работах [13, 14] выполнен анализ свойств недвоичных последовательностей, формируемых путем децимации недвоичных МП. В [15] проведен анализ применения недво-

ичных последовательностей для контроля функционирования устройств декодирования помехоустойчивых кодов. В [16] разработан алгоритм формирования и выполнена оценка линейной сложности пятеричных ГМВП с периодом $N = 624$. В [17, 18] приведены результаты по формированию семейств недвоичных последовательностей с низкими уровнями взаимно корреляционных функций. В работах [19, 20] рассмотрены вопросы формирования и оценки корреляционных и структурных свойств ГМВП.

Для формирования недвоичных СРС с заданными характеристиками предварительно требуется определить корреляционные и структурные свойства ПСП. Для двоичных ГМВП известны выражения для ЭЛС данных последовательностей [5, 8–10]. Для недвоичных ГМВП выражения для ЭЛС в известной литературе отсутствуют.

Алгоритмы формирования троичных и пятеричных ГМВП с периодами $N = 80$, 728 и $N = 24$, 124, 624 рассмотрены в [16, 21], где приведены величины ЭЛС данных последовательностей для различных значений параметра r.

Цель статьи – получение выражений для ЭЛС недвоичных ГМВП.

Формирование недвоичных ГМВП с периодом $N = p^{mn} - 1$ осуществляется над конечными полями

$$GF[(p^m)^n] = GF(p^S), \quad S = mn.$$

Символы d_i ($i = 0...N - 1$) ГМВП определяются выражением [5, 9, 10]

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

где $\mathrm{tr}_{a,b}(\alpha)$ – след элемента α из поля $GF(p^a)$ в поле $GF(p^b)$; $\alpha \in GF[(p^m)^n]$ – примитивный элемент; параметр r – натуральное число, взаимно простое с порядком мультипликативной группы подполя $GF(p^m)$, равным $p^m - 1$.

ЭЛС двоичных ГМВП определяется выражением [5, 8, 9]

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

где $g(r)$ – количество единиц в двоичном представлении числа r в (1).

Известно, что любая двоичная ГМВП может быть представлена в виде суммы по mod 2 нескольких ПСП, формируемых на основе неприводимых проверочных полиномов $h(x)$ степени $S = mn$ [9, 10]. В качестве ПСП могут выступать как МП с периодом $N = 2^S - 1$, так и последовательности с периодами, являющимися делителями периода N. Тогда выражение (2) может быть представлено в виде

$$l_S = mnM, \tag{3}$$

где $M = n^{g(r)-1}$ – число суммируемых двоичных последовательностей.

Важным следствием выражения (3) является то, что число суммируемых последовательностей при формировании ГМВП определяется только параметрами n и r и не зависит от параметра m.

При формировании МП функция $g(r) = 1$, поэтому в суммировании участвует только одна последовательность, образуемая на основании примитивного полинома степени $S = mn$. Параметр r в этом случае может принимать значения 1, 2, 4, ..., 2^{m-1}, для которых $g(r) = 1$.

При формировании ГМВП функция $g(r) > 1$. Добавление каждой единицы в двоичном представлении параметра r приводит к увеличению числа суммируемых последовательностей и линейной сложности формируемой ГМВП в n раз. С точки зрения структурных свойств конечных полей увеличение числа единиц при вычислении p-сопряженных элементов для элемента α соответствует аналогичному увеличению числа переходов через границу, равную порядку мультипликативной группы подполя $GF(2^m)$. Например, в подполе $GF(2^4)$ при вычислении p-сопряженных элементов для примитивного элемента α^{11}, т.е. при $r = 11_{10} = 1011_2$ и $g(r) - 1 = 2$, наблюдается два перехода через α^{15}:

$$\alpha^{11}, \alpha^{22 \bmod 15} = \alpha^7, \alpha^{14}, \alpha^{28 \bmod 15} = \alpha^{13}.$$

А в подполе $GF(2^5)$ для примитивного элемента α^{15}, т.е. при $r = 15_{10} = 1111_2$ и $g(r) - 1 = 3$, наблюдается три перехода через α^{31}:

$$\alpha^{15}, \alpha^{30}, \alpha^{60 \bmod 31} = \alpha^{29}, \alpha^{58 \bmod 31} = \alpha^{27}, \alpha^{54 \bmod 31} = \alpha^{23}.$$

Соответственно, ЭЛС ГМВП увеличивается в n^2 или в n^3 раз по сравнению с ЭЛС МП.

Можно дать следующую интерпретацию изменения ЭЛС в зависимости от параметра r при синтезе МП и ГМВП. В силу свойства цикличности расширенное поле $GF[(2^m)^n]$, его подполе $GF(2^m)$ и простое поле $GF(2)$ можно представить в виде вложенных окружностей различных радиусов, пропорциональных числу элементов полей, с распределением данных элементов по окружностям. Тогда функции следа $\mathrm{tr}_{a,b}(\alpha)$ отображаются в виде ребер, соединяющих элементы расширенного поля $GF[(2^m)^n]$ с элементами подполя $GF(2^m)$ и далее с элементами простого поля $GF(2)$. При

формировании МП функция $g(r) = 1$ и ребра проходят напрямую через подполе $GF(2^m)$, т.е.

$$\mathrm{tr}_{m,1}[\mathrm{tr}_{mn,m}(\alpha^i)] = \mathrm{tr}_{mn,1}(\alpha^i).$$

При формировании ГМВП увеличение функции $g(r)$ соответствует изменению значения функции следа $[\mathrm{tr}_{mn,m}(\alpha^i)]^r$ элемента α^i в подполе $GF(2^m)$ и вычислению функции следа в поле $GF(2)$ для элемента, отличного от элемента $\mathrm{tr}_{mn,m}(\alpha^i)$. Данное преобразование можно рассматривать как сдвиг подполя $GF(2^m)$ относительно поля $GF[(2^m)^n]$. Величина сдвига пропорциональна значению $g(r) - 1$, что приводит к соответственному увеличению линейной сложности ГМВП.

В общем случае функциональная зависимость ЭЛС от параметров конечного поля имеет вид $l_S = f(p, m, n, r)$, где параметр r принимает значения, являющиеся взаимно простыми с порядком мультипликативной группы подполя $GF(p^m)$, равным $(p^m - 1)$. В отличие от выражения (2) для ЭЛС двоичных ГМВП, в котором применяется функция $g(r)$, при решении задачи определения ЭЛС недвоичных ГМВП над конечными полями $GF[(p^m)^n] = GF(p^S)$ используются непосредственно значения и кратности разрядов p-ичного представления параметра r.

При выводе выражения для ЭЛС недвоичных ГМВП использован подход, аналогичный двоичному случаю. Данный подход связан с определением числа переходов через границу, равную порядку мультипликативной группы подполя $GF(p^m)$, в зависимости от структуры p-ичного представления параметра r, а именно от значений p-ичных разрядов и их кратности. Анализ проведен на основании результатов определения ЭЛС троичных и пятеричных ГМВП, полученных в [16, 21].

Формирование недвоичных ГМВП, как и в случае двоичных ГМВП, осуществляется путем суммирования нескольких ПСП с проверочными полиномами степени $S = mn$. В качестве ПСП могут выступать как недвоичные МП с периодом $N = p^{mn} - 1$, так и недвоичные ПСП с периодами, являющимися делителями периода N. Для заданных значений m и n величина ЭЛС двоичных и недвоичных ГМВП отличается только значением числа суммируемых последовательностей. Поэтому выражение (3) для недвоичных ГМВП принимает вид

$$l_S = mnM_p, \qquad (4)$$

где M_p – число суммируемых p-ичных последовательностей.

Таким образом, задача определения ЭЛС недвоичных ГМВП сводится к вычислению параметра M_p, т.е. числа суммируемых последовательностей.

При выводе выражения для ЭЛС недвоичных ГМВП анализ проведен для троичных и пятеричных последовательностей, построенных в конечных полях

$$GF[(p^m)^n] = GF[(p^m)^2],$$

т.е. для значения $n = 2$. Данные последовательности обладают максимальным значением ЭЛС при фиксированном значении параметра $S = mn$ и могут быть представлены в виде матрицы размерности $[(p^m - 1) \times (p^m + 1)]$, ненулевые столбцы которой являются различными циклическими сдвигами короткой МП с периодом $J = p^m - 1$ [9, 10].

Сводные исходные данные для анализа ЭЛС представлены в табл. 1. Анализ показал, что число суммируемых последовательностей M_p при фиксированном значении параметра $n = 2$ зависит только от p-ичного представления параметра r, а именно от значений p-ичных разрядов этого представления и их кратности, и не зависит от значений параметров p и m. Например, в строках 1–3, 5, 6, 11 число $M_p = 3$, так как разложение параметра r содержит одну единицу и одну двойку, хотя параметры p и m, а также ЭЛС l_S ГМВП имеют различные значения. Аналогичная картина наблюдается для строк 4, 8, 9, в которых число $M_p = 9$, а разложение параметра r содержит одну единицу и две двойки.

Рассмотрение p-сопряженных элементов для элемента α в степени r показало, что значение каждого разряда p-ичного представления параметра r определяет число переходов через границу, равную порядку мультипликативной группы подполя $GF(p^m)$, при вычислении очередного p-сопряженного значения.

Например, в подполе $GF(5^m) = GF(5^2)$ при вычислении p-сопряженных элементов для элемента α^{13}, т.е. при $r = 13_{10} = 23_5$, наблюдаются два перехода через порядок мультипликативной группы от элемента α^{13} к элементу $\alpha^{13 \times 5 \bmod 24} = \alpha^{65 \bmod 24} = \alpha^{17}$ и три перехода от элемента α^{17} обратно к элементу $\alpha^{17 \times 5 \bmod 24} = \alpha^{85 \bmod 24} = \alpha^{13}$. А при $r = 19_{10} = 34_5$ – три и четыре перехода соответственно (табл. 1, строки 14, 15).

Для двоичных ГМВП, построенных над $GF[(2^m)^2]$, т.е. при $n = 2$, добавление единицы в двоичном представлении параметра r приводит к увеличению ЭЛС в два раза. Для p-ичных ГМВП, построенных над $GF[(p^m)^2]$, наличие разряда со значением $1 < i < p$ приводит к увеличению параметра M_p и ЭЛС l_S в $(i + 1)$ раз. При наличии двух одинаковых разрядов увеличение будет в $(i + 1)^2$ раз, т.е. увеличение кратности разряда p-ичного представления параметра r приводит к росту ЭЛС в степенной зависимости. При отсутствии разряда, равного единице, ЭЛС уменьшается в два раза.

Таблица 1. Значения ЭЛС недвоичных ГМВП с периодами $N < 6561$ при $n = 2$

№	Период N	p	m	r_{10}	r_p	M_p	ЭЛС l_S
1	$3^4 - 1 = 80$	3	2	5	12	3	12
2	$3^6 - 1 = 728$	3	3	5	12	3	18
3		3	3	7	21	3	18
4		3	3	17	122	9	54
5	$3^8 - 1 = 6560$	3	4	7	21	3	24
6		3	4	11	102	3	24
7		3	4	13	111	4	32
8		3	4	17	122	9	72
9		3	4	23	212	9	72
10		3	4	41	1112	12	96
11		3	4	53	1222	27	216
12	$5^2 - 1 = 24$	5	1	3	3	2	4
13	$5^4 - 1 = 624$	5	2	7	12	3	12
14		5	2	13	23	6	24
15		5	2	19	34	10	40

Таким образом, выражение для числа суммируемых последовательностей при формировании p-ичных ГМВП, построенных в конечных полях $GF[(p^m)^2]$, может быть представлено в виде произведения множителей, пропорциональных значениям и кратности разрядов p-ичного разложения параметра r

$$M_p = 0.5\prod_{i=1}^{p-1}(i+1)^{t_i}, \qquad (5)$$

где t_i – кратность разрядов, равных i, в p-ичном представлении параметра r.

Тогда ЭЛС недвоичных ГМВП при значении параметра $n = 2$ определяется выражением (4) при подстановке числа суммируемых последовательностей из (5)

$$l_S = m\prod_{i=1}^{p-1}(i+1)^{t_i}. \qquad (6)$$

В качестве примера определим число суммируемых последовательностей M_p при формировании троичных ГМВП с периодом $N = 3^8 - 1 = 6560$ для значений параметра $r = 41_{10} = 1112_3$ и $r = 53_{10} = 1222_3$:

$$M_p(r_{10} = 41) = 2^{3-1} \times 3^1 = 12;$$
$$M_p(r_{10} = 53) = 2^{1-1} \times 3^3 = 27.$$

Число M_p при формировании пятеричных ГМВП с периодом $N = 5^4 - 1 = 624$ для значений параметра $r = 7_{10} = 12_5$ и $r = 19_{10} = 34_5$:

$$M_p(r_{10} = 7) = 2^{1-1} \times 3^1 = 3;$$
$$M_p(r_{10} = 19) = 0.5 \times 4^1 \times 5^1 = 10,$$

где отсутствие единичных разрядов в p-ичном представлении соответствует делению на два.

Полученные результаты совпадают с приведенными в табл. 1, что подтверждает справедливость выражений (5) и (6).

Кроме того, при $p = 2$ и $n = 2$ выражение (6) переходит в (2) для ЭЛС ГМВП, так как $t_1 = g(r)$, а выражение под знаком произведения становится равным $n^{g(r)}$. Таким образом, выражение (2) для ЭЛС двоичных последовательностей является частным случаем для ЭЛС недвоичных ГМВП при $n = 2$.

В соответствии с выражениями (5) и (6) были получены значения числа суммируемых последовательностей M_p и, соответственно, ЭЛС l_S для троичных, пятеричных, семеричных, одиннадцатеричных и тринадцатеричных ГМВП с периодами $N = 3^{10} - 1$, $N = 5^6 - 1$, $N = 7^4 - 1$, $N = 11^4 - 1$, $N = 11^6 - 1$, $N = 13^6 - 1$ для некоторых значений параметра r. Результаты вычислений представлены в табл. 2.

Таким образом, в статье получено выражение для числа суммируемых последовательностей и

Таблица 2. Значения ЭЛС недвоичных ГМВП при различных N, p, m и $n = 2$

r_{10}	r_p	M_p	l_S
$N = 3^{10} - 1 = 59048$, $p = 3$, $m = 5$			
61	2021	9	90
67	2111	12	120
79	2221	27	270
131	11212	36	360
161	12222	81	810
$N = 5^6 - 1 = 15624$, $p = 5$, $m = 3$			
3	3	2	12
7	12	3	18
47	142	15	90
63	223	18	108
99	344	50	300
$N = 7^2 - 1 = 48$, $p = 7$, $m = 1$			
5	5	3	6
$N = 7^4 - 1 = 2400$, $p = 7$, $m = 2$			
5	5	3	12
19	25	9	36
25	34	10	40
41	56	21	84
$N = 11^2 - 1 = 120$, $p = 11$, $m = 1$			
3	3	2	4
9	9	5	10
$N = 11^4 - 1 = 14640$, $p = 11$, $m = 2$			
7	7	4	16
13	12	3	12
43	3A	22	88
109	9A	55	220
$N = 11^6 - 1 = 1771560$, $p = 11$, $m = 3$			
1209	9AA	605	3630
$N = 13^6 - 1 = 4826808$, $p = 13$, $m = 3$			
1507	8BC	702	4212
2027	BCC	1014	6084

ЭЛС недвоичных ГМВП, формируемых в конечных полях $GF[(p^m)^2]$.

Недвоичные ГМВП могут быть использованы вместо МП при формировании недвоичных сигналов с расширенным спектром с повышенной структурной скрытностью в системах передачи цифровой информации, системах навигации и радиолокации, функционирующих в условиях радиоэлектронного противодействия.

СПИСОК ЛИТЕРАТУРЫ

1. *Ипатов В.П.* Широкополосные системы и кодовое разделение сигналов. Принципы и приложения / Пер. с англ. М.: Техносфера, 2007.
2. *Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В.* Широкополосные беспроводные сети передачи информации. М.: Техносфера, 2005.
3. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. 2-е изд. / Пер. с англ. М.: Вильямс, 2003.
4. *CDMA*: прошлое, настоящее, будущее. М.: МАС, 2003.
5. *Golomb S.W., Gong G.* Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar. Cambridge: Cambridge Univ. Press, 2005.
6. *Ипатов В.П.* Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992.
7. *Rizomiliotis P., Kalouptsidis N.* // IEEE Trans. 2005. V. IT-51. № 4. P. 1555.
8. *Wang Q.* // IEEE Trans. 2010. V. IT-56. № 8. P. 4046.
9. *Chung H.B., No J.S.* // IEEE Trans. 1999. V. IT-45. № 6. P. 2060.
10. *Стародубцев В.Г.* // РЭ. 2020. Т. 65. № 2. С. 169.
11. *Lee Wijik, Kim Ji-Youp, No J.S.* // IEICE Trans. on Commun. 2014. V. E97-B. № 1. P. 2311.
12. *Tasheva Z.* // J. Scientific Appl. Research. 2014. V. 2. P. 17.
13. *Cho Chang-Min, Kim Ji-Youp, No J.S.* // IEICE Trans. Commun. 2015. V. E98. № 7. P. 1268.
14. *Liang H., Tang Y.* // Finite Fields and Their Appl. 2015. V. 31. P. 137.
15. *Самойленко Д.В., Еремеев М.А., Финько О.А., Диченко С.А.* // Труды СПИИРАН. 2018. Вып. 4. С. 31.
16. *Стародубцев В.Г.* // Труды СПИИРАН. 2019. Т. 18. № 4. С. 912.
17. *Liang H., Chen W., Luo J., Tang Y.* // Adv. Mathem. Commun. 2017. V. 11. P. 671.
18. *Shi X., Zhu X., Huang X., Yue Q.* // IEEE Commun. Lett. 2019. V. 23. № 7. P. 1132.
19. *No J.S.* // IEEE Trans. 1996. V. IT-42. № 1. P. 260.
20. *Zhu J., Cheng F., Tong L, Zhou S., Hua J.* // 2nd Intern. Conf. Inform. Science and Engineering. 4-6 Dec. 2010, Hangzhou, China. 2010. P. 716.
21. *Стародубцев В.Г., Ткаченко В.В., Боброва Е.А.* // Изв. вузов. Приборостроение. 2020. Т. 63. № 5. С. 405.