ТЕОРИЯ И МЕТОДЫ ОБРАБОТКИ СИГНАЛОВ

УДК 519.725;512.62

ФОРМИРОВАНИЕ СЕМЕРИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОРДОНА–МИЛЛСА–ВЕЛЧА ДЛЯ СИСТЕМ ПЕРЕДАЧИ ЦИФРОВОЙ ИНФОРМАЦИИ

© 2022 г. **В. Г. Стародубцев***

Военно-космическая академия им. А.Ф. Можайского,
ул. Ждановская, 13, Санкт-Петербург, 197198 Российская Федерация
**E-mail: vgstarod@mail.ru*

Поступила в редакцию 16.11.2021 г.
После доработки 26.11.2021 г.
Принята к публикации 15.01.2022 г.

Представлены семеричные последовательности Гордона–Миллса–Велча (ГМВП) с периодом $N = 2400$, формируемые в конечных полях $GF[(7^m)]^n = GF(7^S)$. Получены проверочные полиномы $h_{ГМВП}(x)$ в виде произведения как примитивных, так и неприводимых полиномов $h_{ci}(x)$ степени $S = 4$. Показано, что для формирования ГМВП путем суммирования последовательностей с полиномами $h_{ci}(x)$ требуется знание символов М-последовательности (МП) с полиномом $h_{МП}(x)$ и индексов децимации, определяемых показателями степени корней полиномов $h_{ci}(x)$. Определено, что по сравнению с двоичным случаем семеричные суммируемые последовательности могут иметь начальный сдвиг, кратный величине $N/(p - 1) = 400$. Показано, что для каждого из 160 примитивных полиномов степени $S = 4$ в поле $GF(7^4)$ можно сформировать по семь ГМВП с эквивалентной линейной сложностью l_s от 12 до 84. Максимальный выигрыш в структурной скрытности по сравнению с семеричными МП составляет 21 раз.

DOI: 10.31857/S0033849422080149

ВВЕДЕНИЕ

В существующих системах передачи цифровой информации (СПЦИ) при формировании фазоманипулированных сигналов с расширенным спектром (СРС) в основном применяются двоичные псевдослучайные последовательности (ПСП), такие как М-последовательности (МП), последовательности Голда, Касами, а также последовательности Гордона–Миллса–Велча (ГМВП) [1–7].

Одним из направлений развития СПЦИ является переход от двоичных к многопозиционным сигналам, в частности к многофазным. Многофазные СРС формируются на основе недвоичных ПСП и обеспечивают повышение помехозащищенности СПЦИ в условиях радиоэлектронного противодействия, особенно по отношению к структурным помехам. Таким образом, в СПЦИ, к которым предъявляются повышенные требования по конфиденциальности, должны применяться ПСП, обладающие как хорошими корреляционными свойствами, так и высокой структурной скрытностью [8–10].

Вопросы разработки алгоритмов формирования недвоичных ПСП нашли отражение в большом количестве публикаций как в нашей стране, так и за рубежом [11–20]. В указанных работах представлены результаты исследований по синтезу ПСП, имеющих различные характеристики, как корреляционные, так и структурные. При этом в большинстве случаев увеличение структурной скрытности ПСП ведет к росту боковых лепестков ее периодической автокорреляционной функции (ПАКФ) и, соответственно, к снижению помехозащищенности СПЦИ.

Среди представителей минимаксных последовательностей, обладающих минимальным значением бокового лепестка ПАКФ, в первую очередь можно выделить МП и ГМВП. При этом ГМВП отличается более высокой структурной скрытностью, которая характеризуется ЭЛС l_s и численно равна степени проверочного полинома $\deg h_{ГМВП}(x)$ [11, 12]. Это определяет приоритетность применения ГМВП в СПЦИ, функционирующих в условиях радиоэлектронного противодействия, особенно при наличии имитационных помех, повторяющих по структуре полезный сигнал. С точки зрения практического применения ГМВП и обеспечения требуемого выигрыша в структурной скрытности периоды формируемых последовательностей должны составлять не менее единиц тысяч.

Цель данной статьи – определить проверочные полиномы $h_{ГМВП}(x)$ семеричных ГМВП с периодом $N = 2400$, а также начальные сдвиги суммируемых последовательностей.

1. ПРОЦЕДУРА ФОРМИРОВАНИЯ НЕДВОИЧНЫХ ГМВП

Недвоичные ГМВП с периодом $N = p^{mn} - 1$ формируются над конечными полями

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

Символы d_i ($i = 0, ..., N - 1$) ГМВП определяются выражением [3, 6, 11, 19]

$$\begin{gathered} d_i = \mathrm{tr}_{m1}[(\mathrm{tr}_{mn,m}(\alpha^i))^r], \\ 1 \le r < p^m - 1, \quad (r, p^m - 1) = 1, \end{gathered} \tag{1}$$

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 $p^m - 1$.

Формирование недвоичных ГМВП над полями $GF[(p^m)^n]$ осуществляется на основе базисной МП с аналогичным периодом $N = p^{mn} - 1$ и примитивным проверочным полиномом $h_{МП}(x)$ степени $S = mn$. Базисная МП представляется в каноническом виде, т.е. ее символы определяются выражением (1) при $r = 1$

$$d_i = \mathrm{tr}_{mn,1}(\alpha^i). \tag{2}$$

Базисная МП при значении параметра $n = 2$ представляется в виде матрицы $\mathbf{F}_{МП}$ с размерностью $[J \times L] = [(p^m - 1) \times (p^m + 1)]$. Столбцы этой матрицы являются различными циклическими сдвигами МП с более коротким периодом $J = p^m–1$, Данная МП называется характеристической последовательностью (ХП).

Последовательность номеров циклических сдвигов $ХП_1$ в матрице $\mathbf{F}_{МП}$ образует правило формирования (ПФ) I_p, в соответствии с которым строится матрица ГМВП $\mathbf{F}_{ГВМП}$. Формирование матрицы $\mathbf{F}_{ГВМП}$ производится путем замены по правилу I_p столбцов матрицы $\mathbf{F}_{МП}$, являющихся циклическими сдвигами $ХП_1$, на соответствующие циклические сдвиги $ХП_2$, которая является другой МП с периодом $J = p^m–1$. Определяется проверочный полином ГМВП $h_{ГМВП}(x)$, который представляется в виде произведения неприводимых полиномов $h_{ci}(x)$ степени S. Вычисляются начальные символы суммируемых последовательностей с учетом их сдвига на величину $N/(p - 1)$ [19].

2. ФОРМИРОВАНИЕ СЕМЕРИЧНЫХ ГМВП С ПЕРИОДОМ $N = 2400$

Особенностью формирования семеричных ГМВП является необходимость определения периодов суммируемых ПСП и числа примитивных полиномов в подполях $GF(7^m)$. При этом формирование ГМВП с периодом $N = 7^4 - 1 = 2400$ характеризуется тем, что для каждой из 160 базисных МП можно сформировать по семь ГМВП с ЭЛС от $l_s = 12$ до $l_s = 84$. Это определяется наличием восьми примитивных полиномов в поле $GF(7^2)$ и, соответственно, семи значений параметра $r > 1$ в (1).

Ниже приведены значения ЭЛС l_s формируемых ГМВП в зависимости от параметра r [20]:

r	5	11	13	17	19	25	41
l_s	12	20	28	24	36	40	84

При формировании семеричных ГМВП с периодом $N = 7^4 - 1 = 2400$ в поле $GF[(7^2)^2]$ используется базисная МП с полиномом $h_{МП}(x) = h_1(x) = x^4 + x^2 + 3x + 5$, которая представляется в виде матрицы размерности $[J \times L] = [48 \times 50]$. Нижний цифровой индекс здесь и в дальнейшем соответствует минимальному показателю степени корней данного полинома. В поле $GF(7^2)$ существует восемь примитивных полиномов, по которым могут формироваться $ХП_i$:

$$h_1(x) = x^2 + x + 3$$

с корнем α^1 (по которому построено поле),

$$h_5(x) = x^2 + 3x + 5,$$

$$h_{11}(x) = x^2 + 4x + 5,$$

$$h_{13}(x) = x^2 + 2x + 3,$$

$$h_{17}(x) = x^2 + 2x + 5,$$

$$h_{19}(x) = x^2 + 5x + 3,$$

$$h_{25}(x) = x^2 + 6x + 3,$$

$$h_{41}(x) = x^2 + 5x + 5.$$

Столбцы матрицы являются циклическими сдвигами МП с периодом $N = 48$ и выступают в качестве $ХП_1$ с примитивным полиномом $h_{ХП1}(x) = h_5(x) = x^2 + 3x + 5$ (с корнем α^5) поля $GF(7^2)$, которое построено по полиному $f(x) = h_1(x) = x^2 + x + 3$, $\alpha = a$.

Таблица 1. Сдвиги суммируемых ПСП при $r = 17$ и $h_{\text{МП}}(x) = h_1(x)$

МП (ПСП)	Сдвиг	Значения начальных символов ПСП			
		c_0	c_1	c_2	c_3
F_{17}	0	$d_0 = 4$	$d_{17} = 4$	$d_{34} = 0$	$d_{51} = 3$
F_{23}	0	$d_0 = 4$	$d_{23} = 1$	$d_{46} = 5$	$d_{69} = 6$
F_{65}	2000	$d_{2000} = 5$	$d_{2065} = 5$	$d_{2130} = 2$	$d_{2195} = 5$
F_{71}	1600	$d_{1600} = 1$	$d_{1671} = 3$	$d_{1742} = 2$	$d_{1813} = 1$
F_{113}	2000	$d_{2000} = 5$	$d_{2113} = 1$	$d_{2226} = 3$	$d_{2339} = 0$
F_{401}	1200	$d_{1200} = 3$	$d_{1601} = 0$	$d_{2002} = 1$	$d_3 = 5$
ГМВП$_1$		1	0	6	6

В результате построения базисной МП получено следующее правило формирования:

$$\mathbf{I_p} = (26,14,15,24,31,25,8,38,37,24,20,26,47,13,45,5,15,37,39,9,33,12,40,5,0,-,\\ 23,27,13,32,4,27,8,5,30,19,10,25,10,36,29,32,44,44,13,29,34,26,16,14). \tag{3}$$

Увеличение номера сдвига соответствует сдвигу последовательности вправо. Прочерк в ПФ обозначает нулевую последовательность.

Рассмотрим формирование ГМВП при $r = 17$ и $r = 41$. В первом случае в соответствии с (3) ХП$_1$ заменяем на ХП$_2$ с $h_{\text{ХП2}}(x) = h_{17}(x) = x^2 + 2x + 5$ и определяем проверочный полином ГМВП$_1$:

$$h_{\text{ГМВП1}}(x) = x^{24} + 2x^{23} + x^{22} + 3x^{20} + 3x^{19} + 3x^{18} + 6x^{17} + 6x^{16} + 4x^{15} + 4x^{14} + x^{13} + 4x^{12} +\\ + 5x^{11} + 5x^{10} + 5x^9 + 4x^8 + 5x^7 + 5x^6 + 2x^5 + 2x^4 + 4x^3 + 1. \tag{4}$$

Таким образом, ЭЛС полученной ГМВП$_1$ равна $l_s = 24$, что соответствует значению, полученному в [20]. Разложение на неприводимые полиномы в поле $GF(7^4)$ имеет следующий вид:

$$h_{\text{ГМВП1}}(x) = h_{c1}(x)h_{c2}(x)h_{c3}(x)h_{c4}(x)h_{c5}(x)h_{c6}(x) = h_{17}(x)h_{23}(x)h_{65}(x)h_{71}(x)h_{113}(x)h_{401}(x) =\\ = (x^4 + 3x^3 + x^2 + 3)(x^4 + 6x^3 + 5x^2 + 5x + 3)(x^4 + 3x^3 + 3x^2 + x + 3)\times\\ \times(x^4 + 2x^3 + 5x^2 + 6x + 3)\left(x^4 + 2x^3 + 5x^2 + 5x + 3\right)\left(x^4 + 4x^2 + 4x + 3\right). \tag{5}$$

Все полиномы в (5) являются примитивными, кроме полинома $h_{65}(x) = x^4 + 3x^3 + 3x^2 + x + 3$, у которого корни имеют период, равный 480, что соответствует периоду формируемой последовательности.

Сдвиги суммируемых ПСП (табл. 1) определены на основе сравнения решений системы из 24-х уравнений со значениями символов, полученными путем децимации базисной МП по индексам $i_{d1} = 17$, $i_{d2} = 23$, $i_{d3} = 65$, $i_{d4} = 71$, $i_{d5} = 113$ и $i_{d6} = 401$.

Последовательность ГМВП$_1$ с ЭЛС $l_s = 24$ формируется в результате сложения по mod7 ПСП F_{17}, F_{23}, ..., F_{401} с циклическими сдвигами в соответствии с табл. 1. В последней строке таблицы приведены начальные символы ГМВП$_1$. Формирование последовательности выполняется продолжением таблицы вправо с учетом того, что все символы d_i определяются из базисной МП.

Во втором случае при $r = 41$ в соответствии с (3) ХП$_1$ заменяем на ХП$_3$ с полиномом $h_{\text{ХП3}}(x) = h_{41}(x) = x^2 + 5x + 5$ и определяем проверочный полином ГМВП$_2$:

$$h_{\text{ГМВП2}}(x) = x^{84} + 6x^{83} + 3x^{81} + 4x^{80} + 4x^{79} + 4x^{78} + 6x^{77} + x^{76} + \ldots + 4x^4 + 5x^3 + 4x + 6 =\\ = h_{41}(x)h_{47}(x)h_{89}(x)h_{95}(x)h_{137}(x)h_{143}(x)h_{185}(x)h_{191}(x)h_{233}(x)h_{239}(x)h_{281}(x)\times\\ \times h_{425}(x)h_{431}(x)h_{473}(x)h_{479}(x)h_{521}(x)h_{527}(x)h_{569}(x)h_{809}(x)h_{815}(x)h_{857}(x). \tag{6}$$

Таблица 2. Сдвиги суммируемых ПСП при $r = 41$ и $h_{МП}(x) = h_1(x)$

МП (ПСП)	Сдвиг	МП (ПСП)	Сдвиг	МП (ПСП)	Сдвиг
F_{41}	0	F_{191}	2000	F_{479}	800
F_{47}	0	F_{233}	0	F_{521}	1600
F_{89}	1200	F_{239}	400	F_{527}	800
F_{95}	400	F_{281}	1200	F_{569}	400
F_{137}	0	F_{425}	1600	F_{809}	2000
F_{143}	2000	F_{431}	1600	F_{815}	2000
F_{185}	1200	F_{473}	400	F_{857}	800

Таблица 3. Сдвиги суммируемых ПСП при $r = 17$ и $h_{МП}(x) = h_{481}(x)$

МП (ПСП)	Сдвиг	Значения начальных символов ПСП			
		c_0	c_1	c_2	c_3
F_{977}	0	$d_0 = 4$	$d_{977} = 6$	$d_{1954} = 3$	$d_{531} = 5$
F_{209}	0	$d_0 = 4$	$d_{209} = 1$	$d_{418} = 3$	$d_{627} = 5$
F_{65}	2000	$d_{2000} = 5$	$d_{2065} = 5$	$d_{2130} = 2$	$d_{2195} = 5$
F_{551}	1600	$d_{1600} = 1$	$d_{2151} = 1$	$d_{302} = 4$	$d_{853} = 4$
F_{1271}	2000	$d_{2000} = 5$	$d_{871} = 6$	$d_{2142} = 3$	$d_{1013} = 2$
F_{881}	1200	$d_{1200} = 3$	$d_{2081} = 5$	$d_{562} = 2$	$d_{1443} = 4$
ГМВП$_3$		1	3	3	4

При $r = 41$ достигается максимальное значение ЭЛС ГМВП $l_s = 84$, что в 21 раз превышает ЭЛС МП. В результате сравнения решений системы из 84-х уравнений со значениями символов, полученными путем децимации по индексам полиномов из (6), определены значения сдвигов ПСП (табл. 2).

Значения сдвигов, которые кратны величине $N/(p-1) = 400$, остаются неизменными при формировании ГМВП для произвольной базисной МП при соблюдении очередности суммируемых последовательностей.

В качестве примера выполним формирование ГМВП$_3$ с ЭЛС $l_s = 24$, если базисная МП задается полиномом $h_{МП}(x) = h_{481}(x) = x^4 + x^3 + 6x^2 + 2x + 5$. Проверочный полином ГМВП определяется выражением

$$\begin{aligned} h_{ГМВП3}(x) &= h_{17\times481 \bmod 2400}(x)h_{23\times481 \bmod 2400}(x)h_{65\times481 \bmod 2400}(x)h_{71\times481 \bmod 2400}(x)h_{113\times481 \bmod 2400}(x) \\ & h_{401\times481 \bmod 2400}(x) = h_{977}(x)h_{209}(x)h_{65}(x)h_{551}(x)h_{1271}(x)h_{881}(x), \end{aligned} \tag{7}$$

в котором в качестве индексов полиномов выбраны минимальные показатели степени их корней. При этом табл. 1 преобразуется в табл. 3. Изменяются только номера символов базисной МП, а начальные сдвиги соответствующих последовательностей остаются без изменения.

ЗАКЛЮЧЕНИЕ

Таким образом, в данной работе получены проверочные полиномы для семеричных ГМВП с периодом $N = 2400$, которые представлены в виде произведения неприводимых полиномов степени S. ГМВП образуется путем суммирования нескольких ПСП, для которых определены сдвиги, кратные величине $N/(p-1)$. Для формирования ГМВП требуется только знание значений символов одной базисной МП с $h_{МП}(x) = h_1(x)$, параметра r, индексов полиномов суммируемых ПСП и их циклических сдвигов.

Показано, что для периода $N = 2400$ для каждого из 160 примитивных полиномов степени $S = 4$ в поле $GF(7^4)$ можно сформировать по семь ГМВП с ЭЛС l_s от 12 до 84. Максимальный выигрыш в структурной скрытности по сравнению с семеричными МП составляет 21 раз.

Полученные результаты могут быть использованы при формировании многофазных СРС в СПЦИ, к которым предъявляются повышенные требования по помехозащищенности и скрытности при выполнении условия минимального значения боковых лепестков ПАКФ.

КОНФЛИКТ ИНТЕРЕСОВ

Автор заявляет об отсутствии конфликта интересов.

СПИСОК ЛИТЕРАТУРЫ

1. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. М.: Вильямс, 2003.
2. *Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В.* Широкополосные беспроводные сети передачи информации. М.: Техносфера, 2005.
3. *Golomb S.W., Gong G.* Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar. Cambridge: Cambridge Univ. Press, 2005.
4. *Ипатов В.П.* Широкополосные системы и кодовое разделение сигналов. Принципы и приложения. М.: Техносфера, 2007.
5. *CDMA*: прошлое, настоящее, будущее. М.: МАС, 2003.
6. *No J.S.* // IEEE Trans. 1996. V. IT-42. № 1. P. 260.
7. *Ипатов В.П.* Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992.
8. *Lee W., Kim J.-Y., No J.S.* // IEICE Trans. Commun. 2014. V. E97-B. № 1. P. 2311.
9. *Shi X., Zhu X., Huang X., Yue Q.* // IEEE Commun. Lett. 2019. V. 23. № 7. P. 1132.
10. *Chen X., Zhang H.* // J. Theoretical Appl. Inform. Technol. 2013. V. 52. № 1. P. 51.
11. *Chung H.B., No J.S.* // IEEE Trans. 1999. V. IT-45. № 6. P. 2060.
12. *Cho C.-M., Kim J.-Y., No J.S.* // IEICE Trans. Commun. 2015. V. E98. № 7. P. 1268.
13. *Kim Y.S., Chung J.S., No J.S., Chung H.* // IEEE Trans. 2008. V. IT-54. № 8. P. 3768.
14. *Liang H., Tang Y.* // Finite Fields and Their Appl. 2015. V. 31. P. 137.
15. *Kim J.Y., Choi S.T., No J.S., Chung H.* // IEEE Trans. 2011. V. IT-57. № 6. P. 3825.
16. *Zhou Z., Helleseth T., Parampalli U.* // IEEE Trans. 2018. V. IT- 64. № 4. P. 2896.
17. *Самойленко Д.В., Еремеев М.А., Финько О.А., Диченко С.А.* // Труды СПИИРАН. 2018. Вып. 4. С. 31.
18. *Luo G., Cao X., Shi M., Helleseth T.* // IEEE Trans. 2021. V. IT- 67. № 8. P. 5168.
19. *Стародубцев В.Г.* // Труды СПИИРАН. 2019. Т. 18. № 4. С. 912.
20. *Стародубцев В.Г.* // РЭ. 2021. Т. 66. № 8. С. 810.