УДК 519.725
DOI: 10.17586/0021-3454-2020-63-5-405-416

ФОРМИРОВАНИЕ ТРОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ВЫСОКОЙ СТРУКТУРНОЙ СКРЫТНОСТЬЮ В СИСТЕМАХ ПЕРЕДАЧИ ЦИФРОВОЙ ИНФОРМАЦИИ

В. Г. СТАРОДУБЦЕВ, В. В. ТКАЧЕНКО, Е. А. БОБРОВА

Военно-космическая академия им. А. Ф. Можайского, 197198, Санкт-Петербург, Россия
E-mail: vka@mil.ru

Представлен алгоритм определения начальных состояний регистров сдвига, входящих в устройство формирования троичных последовательностей Гордона — Миллса — Велча (ГМВ) с периодом N=728. Алгоритм основан на сравнении начальных состояний, полученных в результате решения в конечных полях системы линейных уравнений, и состояний, определенных путем децимации символов базисной М-последовательности. Троичные М-последовательности и ГМВ-последовательности обладают одинаковой двухуровневой периодической автокорреляционной функцией, но различной структурной скрытностью, характеризуемой эквивалентной линейной сложностью. ГМВ-последовательность формируется на основе базисной М-последовательности с аналогичным периодом при ее представлении в виде квазиквадратной матрицы. Показано, что для каждого из 48 примитивных полиномов в конечном поле GF(3^6) может быть сформировано по три ГМВ-последовательности. Для двоичных ГМВ-последовательностей начальные состояния регистров сдвига образуются путем децимации символов базисной М-последовательности, представленной в каноническом виде; для троичных ГМВ-последовательностей отдельные суммируемые составляющие имеют дополнительный сдвиг на полпериода базисной М-последовательности. Полученные результаты могут найти применение при формировании широкополосных недвоичных сигналов в системах передачи цифровой информации.

Ключевые слова: *псевдослучайные последовательности, конечные поля, неприводимые и примитивные полиномы, структурная скрытность, децимация, регистры сдвига*

Современные системы передачи цифровой информации (СПЦИ) характеризуются сложной иерархической структурой, территориальной распределенностью, наличием как проводных, так и радиоканалов связи, включающих, в том числе, каналы спутниковой связи, которые могут функционировать в условиях радиоэлектронного противодействия [1, 2]. В таких радиоканалах широкое применение получили сигналы с расширенным спектром (СРС) [3, 4], позволяющие минимизировать воздействие узкополосных и широкополосных преднамеренных помех.

Одним из показателей, характеризующих помехозащищенность систем передачи цифровой информации, является структурная скрытность. В настоящее время в качестве псевдослучайных последовательностей (ПСП), используемых для расширения спектра сигналов, в основном применяются двоичные М-последовательности, последовательности Голда, последовательности малого и большого множеств Касами, а также последовательности Гордона — Миллса — Велча (ГМВ) [5, 6].

Перспективным направлением развития СПЦИ является переход к недвоичным сигналам, формируемым на основе недвоичных ПСП. Среди последовательностей, обладающих двухуровневой периодической автокорреляционной функцией (ПАКФ), можно выделить p-ичные М-последовательности (МП) и ГМВ-последовательности (ГМВП). При этом

в помехозащищенных СПЦИ целесообразно применять ГМВП, структурная скрытность которых, характеризуемая эквивалентной линейной сложностью (ЭЛС), существенно превышает данный показатель в МП [7].

Вопросам формирования и анализа корреляционных и структурных свойств двоичных и недвоичных ПСП посвящено большое количество публикаций [8—18]. Так, в работе [8] проанализированы корреляционные и структурные свойства как двоичных, так и троичных ПСП над полями нечетных характеристик, а также составных троичных последовательностей. Формированию и оценке структурных свойств двоичных ГМВП посвящена работа [9], а в [10] проведен анализ синтеза троичных ГМВП с периодом N=80 с учетом определения начальных состояний регистров сдвига. Процедура формирования фазоманипулированных сигналов с высокой структурной скрытностью рассмотрена в работе [11]. В [12] разработан алгоритм формирования пятеричных ГМВП с периодом N=624 и произведена оценка их линейной сложности. Подробный анализ вопросов формирования недвоичных ПСП и семейств ПСП с заданными корреляционными и структурными свойствами представлен в работах [13—15]. В работах [16—18] приведены результаты по синтезу семейств троичных и p-ичных последовательностей с низким уровнем взаимно корреляционных функций.

Алгоритм формирования троичных ГМВП с периодом N=728 в конечном поле GF(3^6) рассмотрен в работе [19], где получены проверочные полиномы $h_{\text{г}}(x)$ для трех типов ГМВ-последовательностей с различной ЭЛС, которые представлены в виде произведения трех и девяти неприводимых полиномов-сомножителей $h_{ci}(x)$. Приведена также структурная схема ГМВП с ЭЛС l_s=18, состоящая из трех регистров сдвига с линейными обратными связями. Однако в данной работе не определены начальные состояния регистров сдвига для всех трех типов ГМВП, что не позволяет осуществить их непосредственное формирование.

Цель настоящей статьи — разработка алгоритма определения начальных состояний регистров сдвига, входящих в устройство формирования троичных ГМВП с периодом N=728.

Для двоичных ГМВП начальные состояния регистров сдвига, входящих в устройство формирования, определяются путем децимации символов, начиная с символа d_0, базисной М-последовательности, представленной в каноническом виде, по индексам децимации, равным показателям степени корней неприводимых полиномов-сомножителей $h_{ci}(x)$ проверочного полинома $h_{\text{г}}(x)$ [20]. Данные корни являются элементами конечного поля GF(3^6). Канонический вид МП определяется через функцию следа из расширенного поля GF(3^6) в простом поле GF(3) $d_i = \text{tr}_{6,1}\alpha^i$, $i = 0, 1, 2,\ldots, N-1$, т.е. $d_0 = \text{tr}_{6,1}\alpha^0$, $d_1 = \text{tr}_{6,1}\alpha^1,\ldots$, где α — примитивный элемент поля GF(3^6) [5, 12].

Например, если корнями некоторого полинома $h_{ci}(x)$ являются элемент α^{13} и его различные p-сопряженные элементы, то начальное состояние регистра определяется символами базисной МП d_0, d_{13}, d_{26}, d_{39}, d_{52}, d_{65}.

Умножители и сумматоры по $\bmod p$ (p=2, 3) в цепи обратной связи регистров сдвига расставляются в соответствии с коэффициентами полиномов $h_{\text{c}i}(x)$ как для двоичных, так и троичных последовательностей. Искомая ГМВП формируется путем суммирования последовательностей с выходов всех регистров сдвига. Если полином $h_{ci}(x)$ является примитивным, то на выходе данного регистра формируется МП. Если же полином $h_{ci}(x)$ является только неприводимым, корни которого имеют период меньше максимального, то на выходе регистра формируется ПСП с данным периодом.

Особенность формирования троичных ГМВП с периодом N=728 заключается в том, что некоторые из суммируемых последовательностей начинаются не с символа d_0, а имеют сдвиг на полпериода и начинаются с символа d_{364}. В общем случае при формировании p-ичных ГМВ-последовательностей сдвиг начального состояния может принимать значения, кратные величине $N/(p-1)$ [12]. Тогда для рассмотренного выше примера начальное состояние регист-

ра при наличии сдвига на полпериода определялось бы шестью символами базисной МП d_{364}, d_{377}, d_{390}, d_{403}, d_{416} и d_{429}. Отметим, что номера символов вычисляются по mod 728.

Для разработки алгоритма определения начальных состояний регистров сдвига воспользуемся подходом, изложенным в работах [10, 12] применительно к трем типам ГМВП с периодом N=728, полученным в [19]. Данный подход основан на сравнении начальных состояний, определенных путем децимации символов базисной МП, и состояний, полученных в результате решения в конечных полях системы линейных уравнений.

В работе [19] все три типа ГМВП формируются на основе одной базисной МП с проверочным полиномом $h_{\text{МП}}(x)=x^6+x+2$, представляемой в виде матрицы размером $[J\times L] = [26\times 28]$, столбцы которой являются различными циклическими сдвигами МП с более коротким периодом $J=3^3-1=26$; такой тип называется характеристической последовательностью (ХП).

В поле GF(3^3) существует четыре примитивных полинома, на основе которых можно сформировать четыре М-последовательности с периодом J=26, являющиеся одновременно характеристическими последовательностями для МП с периодом N=728. Последовательность циклических сдвигов ХП в матрице МП образует правило формирования. Один столбец матрицы состоит из нулей и называется нулевой последовательностью (НП).

Для получения трех различных ГМВП необходимо в матрице вместо ХП_1 поставить в соответствии с правилом формирования другие ХП_i, i = 2, 3, 4, проверочные полиномы которых являются примитивными полиномами в поле GF(3^3), построенном по полиному $f(x)=x^3+2x+1$. Данные полиномы вместе с их корнями представлены в табл. 1 (здесь $\alpha^1 = a$). В качестве индексов для полиномов $h_i(x)$ в поле GF(3^3), а также в поле GF(3^6) используются минимальные показатели степени p-сопряженных корней данных полиномов. Значения показателей степени характеризуются также параметром r, используемым при построении ГМВП [12].

Таблица 1

Элементы поля		Параметр r	ХП_i	Минимальные полиномы	Корни
α^t	$a^2a^1a^0$				
α^1	010	r_4=17	ХП_4	$h_1(x) = x^3 + 2x + 1$	$\alpha^1\alpha^3\alpha^9$
α^5	212	r_3=7	ХП_3	$h_5(x) = x^3 + 2x^2 + x + 1$	5,15,19
α^7	122	r_2=5	ХП_2	$h_7(x) = x^3 + x^2 + 2x + 1$	7,21,11
α^{17}	210	r_1=1	ХП_1	$h_{17}(x) = x^3 + 2x^2 + 1$	17,25,23

Проверочный полином для ХП_1 определяется по алгоритму Берлекэмпа — Месси [5] и в соответствии с табл. 1 имеет вид

$$h_{\text{ХП1}}(x) = h_{17}(x) = x^3+2x^2+1.$$

Этому полиному соответствует параметр r_1=1 [10, 19].

Для значений параметров $r_2 = 5$, $r_3 = 7$ и $r_4 = 17$ ХП_i будут формироваться с помощью примитивных полиномов, подстрочный индекс в обозначении которых определяется как $17\cdot r_i$ mod 26:

$$h_{\text{ХП2}}(x) = h_{17\times 5 \bmod 26}(x) = h_7(x) = x^3+x^2+2x+1;$$

$$h_{\text{ХП3}}(x) = h_{17\times 7 \bmod 26}(x) = h_5(x) = x^3+2x^2+x+1,$$

$$h_{\text{ХП4}}(x) = h_{17\times 17 \bmod 26}(x) = h_1(x) = x^3+2x+1.$$

Алгоритм определения начальных состояний рассмотрим на примере ГМВП_1 с параметром r_2=5.

Проверочный полином $h_{\text{г1}}(x)$ и сегмент из 18 символов ГМВП_1, необходимый для составления и решения системы из 18 линейных уравнений, имеют следующий вид [19]:

$$h_{\text{г1}}(x) = h_{\text{с1}}(x)\cdot h_{\text{с2}}(x)\cdot h_{\text{с3}}(x) = h_5(x)\cdot h_{19}(x)\cdot h_{31}(x) =$$

$$=(x^6+2x^5+x^4+x^3+2x^2+x+2)\,(x^6+x^4+2x^3+x^2+x+2)\,(x^6+x^5+x^4+2x^2+2), \quad (1)$$

$$F_{\text{г1}} = c_0c_1c_2\ldots c_{17} = 100112200011110102. \quad (2)$$

Эквивалентная линейная сложность ГМВП$_1$ равна степени проверочного полинома: $l_{s1} = 18$. Полиномы $h_{ci}(x)$ являются неприводимыми полиномами 6-й степени поля GF(3^6), построенного по примитивному полиному $f(x)=x^6+x+2$, $\alpha^1=a$.

Начальные состояния регистров, получаемые путем децимации символов d_i базисной МП по индексам децимации $i_{d1}=5$, $i_{d2}=19$, $i_{d3}=31$, характеризуются выражениями

$$\begin{aligned} h_5(x):&\quad d_0=0,\ d_5=1,\ d_{10}=2,\ d_{15}=1,\ d_{20}=2,\ d_{25}=1;\\ h_{19}(x):&\quad d_0=0,\ d_{19}=0,\ d_{38}=1,\ d_{57}=0,\ d_{76}=1,\ d_{95}=2;\\ h_{31}(x):&\quad d_0=0,\ d_{31}=2,\ d_{62}=2,\ d_{93}=2,\ d_{124}=0,\ d_{155}=0. \end{aligned} \tag{3}$$

Для нахождения сдвигов ПСП, суммируемых по mod 2, необходимо определить значения начальных состояний регистров сдвига путем решения системы линейных уравнений при заданном сегменте троичной ГМВП$_1$ вида (2) длиной 18 символов, т.е. $c_0 = 1$, $c_1 = 0$, $c_2 = 0$, $c_3 = 1$ и т.д. Затем определить сдвиги суммируемых ПСП исходя из условия совпадения начальных состояний регистров, полученных путем децимации символов базисной МП и с помощью решения системы линейных уравнений.

Символы на выходах регистров сдвига определяются коэффициентами полиномов $h_5(x)$, $h_{19}(x)$ и $h_{31}(x)$ с помощью рекуррентных выражений

$$h_5(x):\quad c_{6+i} = c_{0+i} + 2c_{1+i} + c_{2+i} + 2c_{3+i} + 2c_{4+i} + c_{5+i},\ i = 0, 1,\ldots, 721; \tag{4}$$

$$h_{19}(x):\quad c_{6+i} = c_{0+i} + 2c_{1+i} + 2c_{2+i} + c_{3+i} + 2c_{4+i},\ i = 0, 1,\ldots, 721; \tag{5}$$

$$h_{31}(x):\quad c_{6+i} = c_{0+i} + c_{2+i} + 2c_{4+i} + 2c_{5+i},\ i = 0, 1,\ldots, 721. \tag{6}$$

Составим систему из 18 линейных уравнений вида $\sum x_{ij} = c_m$, где $i = 0, 1,\ldots, 5$ — номер ячейки в регистре; $j = 0, 1, 2$ — номер регистра сдвига; $m = 0, 1, 2,\ldots 17$ — номер символа в сегменте ГМВП$_1$. Каждое из уравнений определяется с помощью выражений (4)—(6). Для начальных состояний трех регистров 000001, равных начальным символам МП в каноническом виде, первые два уравнения имеют вид

$$x_{00}+x_{01}+x_{02}=1,\quad x_{10}+x_{11}+x_{12}=0.$$

Полностью система из 18 линейных уравнений в виде коэффициентов при формальных переменных представлена в табл. 2 (для r_2=5). Результаты решения этой системы, т.е. начальные состояния c_{ij} трех регистров сдвига, приведены в конце таблицы.

Таблица 2

x_{00}	x_{10}	x_{20}	x_{30}	x_{40}	x_{50}	x_{01}	x_{11}	x_{21}	x_{31}	x_{41}	x_{51}	x_{02}	x_{12}	x_{22}	x_{32}	x_{42}	x_{52}	c_m
1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1
0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0
0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0
0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	1
0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	1
0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	2
1	2	1	2	2	1	1	2	2	1	2	0	1	0	1	0	2	2	2
1	0	0	0	1	0	0	1	2	2	1	2	2	1	2	1	1	0	0
0	1	0	0	0	1	2	1	2	1	0	1	0	2	1	2	1	1	0
1	2	2	2	2	1	1	1	0	0	0	0	1	0	0	1	1	0	0
1	0	0	1	1	0	0	1	1	0	0	0	0	1	0	0	1	1	1
0	1	0	0	1	1	0	0	1	1	0	0	1	0	2	0	2	0	1
1	2	2	2	2	2	0	0	0	1	1	0	0	1	0	2	0	2	1
2	2	1	0	0	1	0	0	0	0	1	1	2	0	0	0	0	1	1
1	1	0	0	2	1	1	2	2	1	2	1	1	2	1	0	2	2	0
1	0	2	2	2	0	1	0	1	0	0	2	2	1	1	1	1	0	1
0	1	0	2	2	2	2	2	1	0	1	0	0	2	1	1	1	1	0
2	1	0	1	0	1	0	2	2	1	0	1	1	0	0	1	0	0	2
Решение системы уравнений																		
c_{00}	c_{10}	c_{20}	c_{30}	c_{40}	c_{50}	c_{01}	c_{11}	c_{21}	c_{31}	c_{41}	c_{51}	c_{02}	c_{12}	c_{22}	c_{32}	c_{42}	c_{52}	
1	1	0	1	2	0	1	1	2	0	0	2	2	1	1	0	2	0	

Для удобства сравнения представим полученные начальные состояния аналогично выражениям (3)—(6), опуская номера регистров сдвига:

$$\begin{aligned} h_5(x)&: \quad c_0=1,\ c_1=1,\ c_2=0,\ c_3=1,\ c_4=2,\ c_5=0;\\ h_{19}(x)&: \quad c_0=1,\ c_1=1,\ c_2=2,\ c_3=0,\ c_4=0,\ c_5=2;\\ h_{31}(x)&: \quad c_0=2,\ c_1=1,\ c_2=1,\ c_3=0,\ c_4=2,\ c_5=0. \end{aligned} \qquad (7)$$

Можно показать, что при таких начальных состояниях трех регистров сдвига на выходе устройства будет формироваться троичная ГМВП.

Для определения сдвигов последовательностей с начальными состояниями, полученными путем децимации символов базисной МП и определяемыми согласно выражениям (3)—(6), составим таблицу (табл. 3), в которой представлены сегменты базисной МП в каноническом виде и суммируемые последовательности, являющиеся МП с проверочными полиномами $h_5(x)$, $h_{19}(x)$ и $h_{31}(x)$. При этом каждая из суммируемых последовательностей F_i формируется для начальных состояний как вида (3), так и вида (7).

Таблица 3

	Символы базисной МП с $h_1(x)$ и МП с $h_5(x)$, $h_{19}(x)$ и $h_{31}(x)$																
h_1: d_i	d_0	d_1	d_2	3	4	5		642	643	644	645	646	647	648	649	650	651
МП: F_1	0	0	0	0	0	1		1	1	0	1	2	1	0	1	2	2
h_5: d_i	d_0	d_5	d_{10}	15	20	25		298	303	308	313	318	323	328	333	338	343
F_5: (3)	**0**	**1**	**2**	**1**	**2**	**1**		1	0	2	0	2	1	2	0	1	1
F_5: (7)	1	1	0	1	2	0		2	1	**0**	**1**	**2**	**1**	**2**	**1**	2	2
h_{19}: d_i	d_0	d_{19}	d_{38}	57	76	95		550	569	588	607	626	645	664	683	702	721
F_{19}: (3)	**0**	**0**	**1**	**0**	**1**	**2**		1	1	2	0	0	1	1	1	2	2
F_{19}: (7)	1	1	2	0	0	2		0	1	**0**	**0**	**1**	**0**	**1**	**2**	1	1
h_1: d_i	d_0	d_1	d_2	3	4	5		278	279	280	281	282	283	284	285	286	287
МП: F_1	0	0	0	0	0	1		2	2	0	2	1	2	0	2	1	1
h_{31}: d_i	d_0	d_{31}	d_{62}	93	124	155		610	641	672	703	6	37	68	99	130	161
F_{31}: (3)	**0**	**2**	**2**	**2**	**0**	**0**		1	2	1	1	0	0	2	1	1	2
F_{31}: (7)	2	1	1	0	2	0		1	0	**0**	**2**	**2**	**2**	**0**	**0**	2	2

В строке „F_5: (7)“ находим соответствующее строке „F_5: (3)“ начальное состояние 012121, которое начинается с символа 644 базисной МП. Также с данного символа начинается состояние 001012 в строке „F_{19}: (7)“. Иными словами, последовательности F_5 и F_{19} суммируются без сдвига относительно друг друга. (Искомые начальные состояния выделены полужирным шрифтом с подчеркиванием.) В строке „F_{31}: (7)“ находим соответствующее строке „F_{31}: (3)“ начальное состояние 022200, которое начинается с символа 280 базисной МП. Тогда для формирования ГМВП последовательность F_{31} должна быть сдвинута относительно F_5 и F_{19} на 644–280=364 символа, т.е. на полпериода.

Таким образом, для формирования ГМВП с периодом N=728 и параметром $r_2 = 5$ начальные состояния регистров сдвига с учетом (3) определяются через символы базисной МП следующими выражениями:

$$\begin{aligned} h_5(x)&: \quad d_0=0,\ d_5=1,\ d_{10}=2,\ d_{15}=1,\ d_{20}=2,\ d_{25}=1;\\ h_{19}(x)&: \quad d_0=0,\ d_{19}=0,\ d_{38}=1,\ d_{57}=0,\ d_{76}=1,\ d_{95}=2;\\ h_{31}(x)&: \quad d_{364}=0,\ d_{395}=1,\ d_{426}=1,\ d_{457}=1,\ d_{488}=0,\ d_{519}=0. \end{aligned} \qquad (8)$$

Представим формализованную запись алгоритма определения начальных состояний регистров сдвига для формирования троичных ГМВП с периодом N=728.

Шаг 1. Ввод исходных данных:

— неприводимые полиномы в поле GF(3^6), $f(x)=x^6+x+2$;

— проверочные полиномы ХП$_i$ в поле GF(3^3), $f(x)=x^3+2x+1$;

— параметры r_i для трех типов ГМВП: $r_2 = 5$, $r_3 = 7$ и $r_4 = 17$;

— проверочные полиномы ГМВП $h_{\text{г}i}(x)=h_{\text{с}1}(x)\cdot h_{\text{с}2}(x)\ldots\cdot h_{\text{с}k}(x)$ [19]:

$$\begin{aligned} h_{\text{г}1}(x) &= h_{\text{с}1}(x)\cdot h_{\text{с}2}(x)\cdot h_{\text{с}3}(x) = h_5(x)\cdot h_{19}(x)\cdot h_{31}(x) = \\ &=(x^6+2x^5+x^4+x^3+2x^2+x+2)\ (x^6+x^4+2x^3+x^2+x+2)\ (x^6+x^5+x^4+2x^2+2); \end{aligned} \qquad (9)$$

$$h_{г2}(x) = h_{с1}(x)\cdot h_{с2}(x)\cdot h_{с3}(x) = h_7(x)\cdot h_{11}(x)\cdot h_{37}(x) =$$
$$= (x^6+x^3+x^2+2x+2)\,(x^6+2x^5+2x^4+2x^3+x^2+2)\,(x^6+x^4+2x^2+x+2); \quad (10)$$
$$h_{г3}(x) = h_{с1}(x)\cdot h_{с2}(x)\cdot h_{с3}(x)\cdot h_{с4}(x)\cdot h_{с5}(x)\cdot h_{с6}(x)\cdot h_{с7}(x)\cdot h_{с8}(x)\cdot h_{с9}(x) =$$
$$= h_{17}(x)\cdot h_{23}(x)\cdot h_{25}(x)\cdot h_{43}(x)\cdot h_{49}(x)\cdot h_{95}(x)\cdot h_{101}(x)\cdot h_{103}(x)\cdot h_{121}(x) =$$
$$= (x^6+2x^5+2x^3+2)\cdot(x^6+2x^5+2x^4+2x^3+2x+2)\cdot(x^6+2x^5+2x^4+2x^2+x+2)\times$$
$$\times(x^6+x^5+2x^4+x^3+x+2)\cdot(x^6+2x^5+2x^4+x^3+x^2+x+2)\cdot(x^6+x^5+x^3+2)\times$$
$$\times(x^6+2x^4+x^2+x+2)\cdot(x^6+2x^5+x^4+2x^3+x^2+2x+2)\cdot(x^6+x^5+2); \quad (11)$$

— наборы индексов децимации для трех типов ГМВП:

$$h_{г1}(x)\text{: } i_{d1}=5,\ i_{d2}=19,\ i_{d3}=31; \quad (12)$$
$$h_{г2}(x)\text{: } i_{d1}=7,\ i_{d2}=11,\ i_{d3}=37; \quad (13)$$
$$h_{г3}(x)\text{: } i_{d1}=17,\ i_{d2}=23,\ i_{d3}=25,\ i_{d4}=43,\ i_{d5}=49,\ i_{d6}=95,\ i_{d7}=101,\ i_{d8}=103,\ i_{d9}=121; \quad (14)$$

— сегменты ГМВП$_i$ соответствующей длины (определяется числом уравнений):

$$h_{г1}(x)\text{: } F_{г1} = c_0c_1\ldots c_{17} = 100112200011110102; \quad (15)$$
$$h_{г2}(x)\text{: } F_{г2} = c_0c_1\ldots c_{17} = 200120200011210112; \quad (16)$$
$$h_{г3}(x)\text{: } F_{г3} = c_0c_1\ldots c_{53} = 10011220002111002101020202002120222021100200122202012120 1. \quad (17)$$

Шаг 2. Составление предварительных наборов начальных состояний вида (3) на основе децимации символов базисной МП по индексам i_{di} в соответствии с (12) – (14).

Шаг 3. Составление системы линейных уравнений с учетом рекуррентных выражений (4)—(6) и сегментов ГМВП$_i$ (15)—(17).

Шаг 4. Формирование начальных состояний регистров сдвига вида (7) на основе решения системы линейных уравнений.

Шаг 5. Определение сдвигов отдельных суммируемых последовательностей на основе их сравнения для начальных состояний, полученных как путем децимации, так и на основе решения системы уравнений.

Шаг 6. Формирование результирующего набора начальных состояний регистров сдвига вида (8).

Начальные состояния регистров сдвига в устройствах формирования ГМВП$_2$ с ЭЛС l_s =18 и ГМВП$_3$ с ЭЛС l_s =54 определяются для параметров r_3=7 и r_4=17 аналогично процедуре для ГМВП$_1$. В результате выполнения алгоритма с учетом того, что проверочный полином для ХП$_3$ равен $h_5(x) = x^3+2x^2+x+1$, а для ХП$_4$ — $h_1(x) = x^3+2x+1$, а также с учетом выражений (10)—(17) получены решения систем из 18 и 54 линейных уравнений, приведенные в табл. 4.

Таблица 4

Решение системы уравнений для ГМВП$_2$																	
c_{00}	c_{10}	c_{20}	c_{30}	c_{40}	c_{50}	c_{01}	c_{11}	c_{21}	c_{31}	c_{41}	c_{51}	c_{02}	c_{12}	c_{22}	c_{32}	c_{42}	c_{52}
2	0	0	2	1	2	2	2	0	1	2	2	1	1	0	1	2	2
Решение системы уравнений для ГМВП$_3$																	
c_{00}	c_{10}	c_{20}	c_{30}	c_{40}	c_{50}	c_{01}	c_{11}	c_{21}	c_{31}	c_{41}	c_{51}	c_{02}	c_{12}	c_{22}	c_{32}	c_{42}	c_{52}
1	0	2	2	2	1	1	2	2	2	1	2	1	2	1	1	1	0
c_{03}	c_{13}	c_{20}	c_{33}	c_{43}	c_{53}	c_{04}	c_{14}	c_{24}	c_{34}	c_{44}	c_{54}	c_{05}	c_{15}	c_{25}	c_{35}	c_{45}	c_{55}
2	2	1	2	2	2	2	2	0	1	1	0	2	0	1	2	1	1
c_{06}	c_{16}	c_{26}	c_{36}	c_{46}	c_{56}	c_{07}	c_{17}	c_{27}	c_{37}	c_{47}	c_{57}	c_{08}	c_{18}	c_{28}	c_{38}	c_{48}	c_{58}
1	1	0	0	2	2	2	2	2	0	1	0	1	1	0	0	2	0

В результате сравнения начальных состояний, вычисленных путем децимации символов базисной МП по индексам (13), (14) и полученных на основе решения систем уравнений (см. табл. 4), определены сдвиги суммируемых последовательностей и сформированы результирующие наборы начальных состояний ячеек регистров сдвига (Я$_i$), входящих в устройства синтеза ГМВП$_2$ и ГМВП$_3$: см. табл. 5, где также приведены наборы для ГМВП$_1$.

С помощью приведенных в табл. 5 данных можно сформировать две ГМВП с ЭЛС $l_{s1}= l_{s2}$ =18 и одну ГМВП с ЭЛС l_{s3}=54 на основе базисной МП с полиномом $h_{МП}(x) =$ $=h_1(x) = x^6+x+2$. Так как в поле GF(3^6) существует 48 примитивных полиномов

[19, табл. 2], то аналогичные распределения можно получить для любой из 48 МП, рассматриваемых в качестве базисных.

Таблица 5

ЭЛС l_s	$h_{ci}(x)$	Начальные состояния ячеек регистра сдвига					
		Я$_0$	Я$_1$	Я$_2$	Я$_3$	Я$_4$	Я$_5$
18	$h_5(x)$	d_0=0	d_5=1	d_{10}=2	d_{15}=1	d_{20}=2	d_{25}=1
	$h_{19}(x)$	d_0=0	d_{19}=0	d_{38}=1	d_{57}=0	d_{76}=1	d_{95}=2
	$h_{31}(x)$	d_{364}=0	d_{395}=1	d_{426}=1	d_{457}=1	d_{488}=0	d_{519}=0
18	$h_7(x)$	d_0=0	d_7=0	d_{14}=0	d_{21}=0	d_{28}=2	d_{35}=2
	$h_{11}(x)$	d_0=0	d_{11}=1	d_{22}=0	d_{33}=1	d_{44}=1	d_{55}=1
	$h_{37}(x)$	d_{364}=0	d_{401}=0	d_{438}=2	d_{457}=0	d_{512}=0	d_{549}=2
54	$h_{17}(x)$	d_0=0	d_{17}=1	d_{34}=1	d_{51}=1	d_{68}=2	d_{85}=0
	$h_{23}(x)$	d_0=0	d_{23}=1	d_{46}=0	d_{69}=1	d_{92}=2	d_{115}=2
	$h_{25}(x)$	d_0=0	d_{25}=1	d_{50}=0	d_{75}=1	d_{100}=2	d_{125}=2
	$h_{43}(x)$	d_{364}=0	d_{407}=1	d_{450}=0	d_{493}=1	d_{563}=1	d_{579}=2
	$h_{49}(x)$	d_{364}=0	d_{413}=2	d_{462}=0	d_{511}=2	d_{560}=1	d_{609}=0
	$h_{95}(x)$	d_{364}=0	d_{459}=1	d_{554}=2	d_{649}=1	d_{16}=1	d_{111}=0
	$h_{101}(x)$	d_0=0	d_{101}=0	d_{202}=2	d_{303}=0	d_{404}=1	d_{505}=1
	$h_{103}(x)$	d_{364}=0	d_{467}=2	d_{570}=1	d_{673}=2	d_{48}=1	d_{151}=2
	$h_{121}(x)$	d_0=0	d_{121}=2	d_{242}=1	d_{363}=2	d_{484}=1	d_{605}=2

При произвольной базисной МП с примитивным полиномом $h_g(x)$ для получения новой совокупности полиномов-сомножителей $h_{ci}(x)$ необходимо индексы полиномов прежней совокупности умножить по mod 728 на параметр g, являющийся показателем степени корня полинома $h_g(x)$. Набор индексов совокупности полиномов-сомножителей $h_{ci}(x)$ в работе [19] определен как вектор сомножителей.

Пример. Определим проверочные полиномы и начальные состояния ячеек регистров сдвига для трех типов ГМВП с ЭЛС $l_{s1} = l_{s2}$ =18 и l_{s3} = 54, если в качестве базисной используется МП с примитивным полиномом $h_{\text{МП}}(x) = h_{47}(x) = x^6+x^5+2x^3+2x^2+2$.

В работе [19] для $h_{\text{МП}}(x) = h_{47}(x)$ определены векторы сомножителей для проверочных полиномов ГМВП:

$$A_5 = (107,29,1),\ A_7 = (49,95,121),\ A_{17} = (71,67,149,239,119,97,41,395,197).$$

Например, проверочный полином $h_{\text{г}3}(x)$ ГМВП$_3$ при r_4=17 имеет вид

$$\begin{aligned} h_{\text{г}3}(x) &= h_{\text{с}1}(x)\cdot h_{\text{с}2}(x)\cdot h_{\text{с}3}(x)\cdot h_{\text{с}4}(x)\cdot h_{\text{с}5}(x)\cdot h_{\text{с}6}(x)\cdot h_{\text{с}7}(x)\cdot h_{\text{с}8}(x)\cdot h_{\text{с}9}(x) = \\ &= h_{71}(x)\cdot h_{67}(x)\cdot h_{149}(x)\cdot h_{239}(x)\cdot h_{119}(x)\cdot h_{97}(x)\cdot h_{41}(x)\cdot h_{395}(x)\cdot h_{197}(x) = \\ &= (x^6+x^5+x^3+2x^2+x+2)\cdot(x^6+2x^4+2x^3+x^2+2x+2)\cdot(x^6+x^4+x^3+x^2+2x+2)\times \\ &\times(x^6+2x^4+x^3+x^2+x+2)\cdot(x^6+2x^5+2x^4+x^3+2)\cdot(x^6+2x^5+2x^3+2x^2+2x+2)\times \\ &\times(x^6+x^5+x^4+2x^3+2x^2+2x+2)\cdot(x^6+2x^5+x^4+2x^2+2)\cdot(x^6+x^4+2x^3+x+2). \end{aligned} \quad (18)$$

При определении начальных состояний ячеек регистров сдвига обязательно соблюдение последовательности полиномов-сомножителей, так как начальные сдвиги определены для конкретных $h_{ci}(x)$.

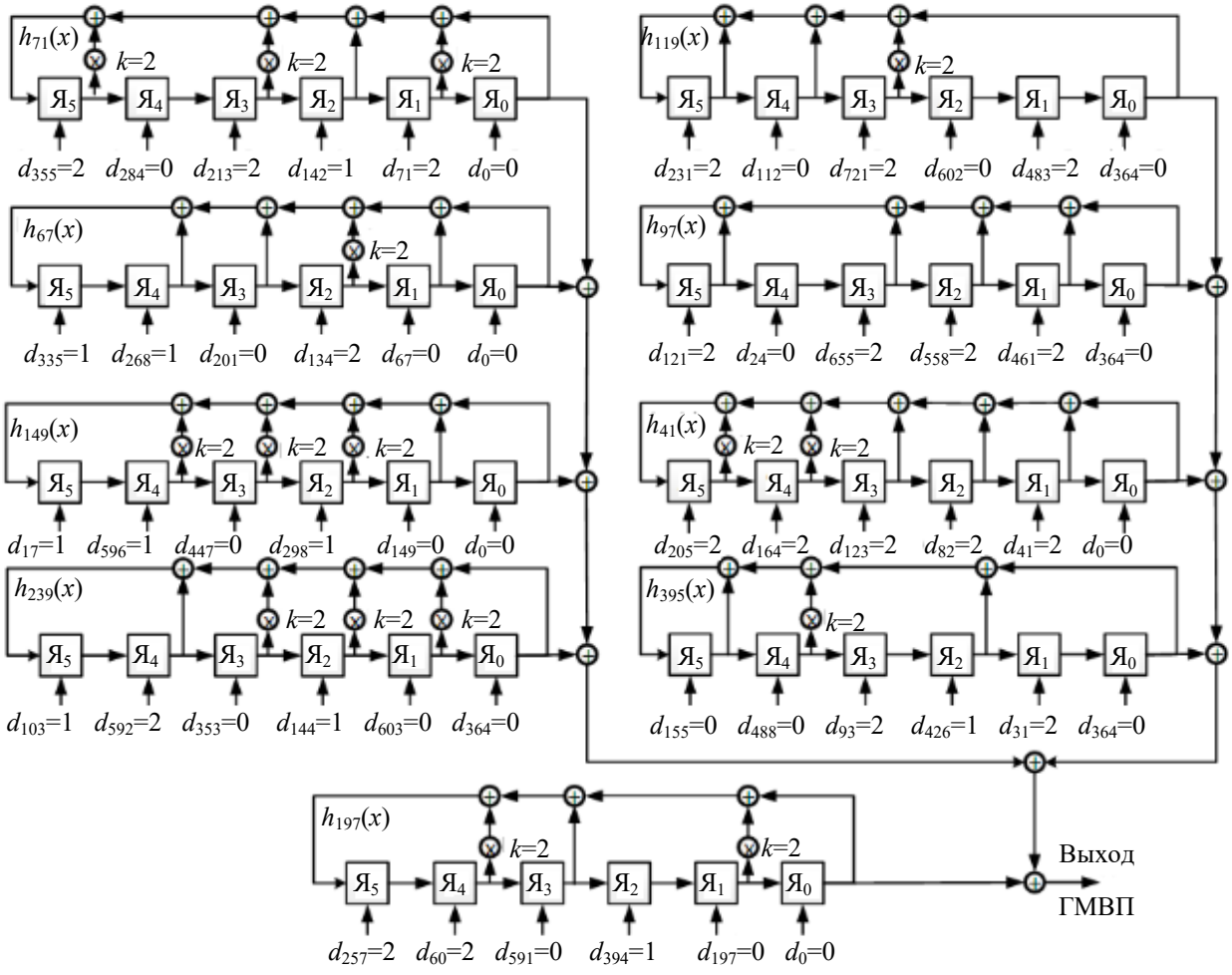
С учетом того, что начальные состояния всех ячеек Я$_0$ остаются без изменений, значения остальных ячеек определяются путем децимации символов исходной базисной МП по индексам новых векторов состояний. Например, для ГМВП с ЭЛС l_{s3} =54 на основе исходной базисной МП с полиномом $h_{\text{МП}}(x) = h_1(x) = x^6+x+2$ начальные состояния четвертого регистра с полиномом $h_{\text{с}4}(x) = h_{43}(x)$ равны d_{364}=0, d_{407}=1, d_{450}=0, d_{493}=1, d_{563}=1, d_{579}=2. При замене на базисную МП с полиномом $h_{\text{МП}}(x) = h_{47}(x) = x^6+x^5+2x^3+2x^2+2$ начальные состояния четвертого регистра с новым полиномом $h_{\text{с}4}(x) = h_{239}(x)$ равны d_{364}=0, d_{603}=0, d_{114}=1, d_{353}=0, d_{592}=2, d_{103}=1.

Результаты расчета начальных состояний ячеек регистров сдвига при данной базисной МП для трех типов ГМВП приведены в табл. 6.

Таблица 6

ЭЛС l_s	$h_{ci}(x)$	Начальные состояния ячеек регистра сдвига					
		$Я_0$	$Я_1$	$Я_2$	$Я_3$	$Я_4$	$Я_5$
18	$h_{107}(x)$	d_0=0	d_{107}=2	d_{214}=1	d_{321}=2	d_{428}=1	d_{535}=0
	$h_{29}(x)$	d_0=0	d_{29}=1	d_{58}=0	d_{87}=1	d_{116}=0	d_{145}=1
	$h_1(x)$	d_{364}=0	d_{365}=0	d_{366}=0	d_{367}=0	d_{368}=0	d_{369}=2
18	$h_{49}(x)$	d_0=0	d_{49}=1	d_{98}=0	d_{147}=1	d_{196}=2	d_{245}=0
	$h_{95}(x)$	d_0=0	d_{95}=2	d_{190}=1	d_{285}=2	d_{380}=2	d_{475}=0
	$h_{121}(x)$	d_{364}=0	d_{485}=1	d_{606}=2	d_{727}=1	d_{120}=2	d_{241}=2
54	$h_{71}(x)$	d_0=0	d_{71}=2	d_{142}=1	d_{213}=2	d_{284}=0	d_{355}=2
	$h_{67}(x)$	d_0=0	d_{67}=0	d_{134}=2	d_{201}=0	d_{268}=1	d_{335}=1
	$h_{149}(x)$	d_0=0	d_{149}=0	d_{298}=1	d_{447}=0	d_{596}=1	d_{17}=1
	$h_{239}(x)$	d_{364}=0	d_{603}=0	d_{114}=1	d_{353}=0	d_{592}=2	d_{103}=1
	$h_{119}(x)$	d_{364}=0	d_{483}=2	d_{602}=0	d_{721}=2	d_{112}=0	d_{231}=2
	$h_{97}(x)$	d_{364}=0	d_{461}=2	d_{558}=2	d_{655}=2	d_{24}=0	d_{121}=2
	$h_{41}(x)$	d_0=0	d_{41}=2	d_{82}=2	d_{123}=2	d_{164}=2	d_{205}=2
	$h_{395}(x)$	d_{364}=0	d_{31}=2	d_{426}=1	d_{93}=2	d_{488}=0	d_{155}=0
	$h_{197}(x)$	d_0=0	d_{197}=0	d_{394}=1	d_{591}=0	d_{60}=2	d_{257}=2

На рисунке показана структурная схема устройства формирования ГМВП$_3$ на основе базисной МП с полиномом $h_{МП}(x)=h_{47}(x)=x^6+x^5+2x^3+2x^2+2$, параметром $r_2=17$ и ЭЛС $l_{s3}=54$, состоящая из девяти регистров сдвига. Умножители и сумматоры по mod 3 в цепи обратной связи регистров расставляются в соответствии с коэффициентами неприводимых полиномов (18). Начальные состояния ячеек регистров сдвига соответствуют нижней части табл. 6.



На выходе устройства формируется ГМВП$_3$ с периодом N=728 и двухуровневой ПАКФ (приведено по 112 начальных и конечных символов):

$$F_{г3}=\begin{vmatrix}
0&1&2&1&2&1&2&2&0&1&2&0&2&1&0&1&2&1&2&2&0&2&2&0&0&1&0&1\\
1&0&2&2&2&0&2&1&2&0&1&1&2&2&0&0&1&1&0&2&2&0&0&1&2&1&2&0\\
0&2&0&1&0&0&1&2&0&0&2&2&1&0&0&2&0&2&2&1&1&0&0&0&0&1&2&2\\
1&0&0&0&0&2&2&0&2&2&0&2&2&1&0&0&2&1&2&2&1&1&1&1&2&2&0&0\\
\multicolumn{6}{c}{.\ .\ .}&\multicolumn{6}{c}{}&\multicolumn{3}{c}{.\ .\ .}&\multicolumn{12}{c}{}&\multicolumn{3}{c}{.\ .\ .}&\multicolumn{1}{c}{}\\
2&1&1&0&1&0&0&0&1&0&0&0&0&1&0&1&2&0&1&0&0&0&0&2&1&1&2&1\\
2&1&0&2&0&1&0&1&1&1&1&2&0&2&0&1&1&0&2&0&1&2&2&2&1&0&1&1\\
1&1&2&1&2&0&1&2&2&0&2&2&1&2&0&1&1&2&1&1&1&0&0&1&2&0&0&1\\
2&2&0&1&0&1&2&2&1&1&2&0&2&2&0&2&1&1&0&2&0&2&2&2&1&2&2&2
\end{vmatrix}. \qquad (19)$$

В соответствии с алгоритмом Берлекэмпа — Месси определяется проверочный полином, который для компактности представлен в виде коэффициентов при формальной переменной x по убыванию степени от x^{54} до x^0:

$$h_г=122001101112012021022220111102000001121200010221111222 2. \qquad (20)$$

ЭЛС ГМВП$_3$ l_{s3}=54, что в девять раз превышает ЭЛС МП $l_{мп}$=6.

Легко проверить, что неприводимые полиномы (18) являются делителями полинома (20).

Таким образом, разработан алгоритм определения начальных состояний ячеек регистров сдвига, входящих в устройство формирования троичных ГМВ-последовательностей с периодом N=728, основанный на сравнении начальных состояний, полученных в результате решения в конечных полях системы линейных уравнений, и состояний, определенных путем децимации символов базисной М-последовательности.

В соответствии с алгоритмом определены начальные состояния при формировании трех типов ГМВП для двух базисных МП (с полиномами $h_1(x)$ и $h_{47}(x)$). Всего можно сформировать 144 ГМВП с периодом N=728.

Максимальный выигрыш в структурной скрытности ГМВП составляет 9 раз по сравнению с МП.

Достоинство алгоритма заключается в том, что при любой базисной МП для определения начальных состояний ячеек регистров сдвига, входящих в устройство формирования ГМВП, используются символы только одной базисной МП с полиномом $h_{МП}(x) = h_1(x) = x^6+x+2$.

Разработанный алгоритм может найти применение при синтезе устройств формирования ГМВП с основанием p=3, а также при формировании широкополосных недвоичных сигналов в системах передачи цифровой информации, к которым предъявляются повышенные требования по конфиденциальности и помехозащищенности.

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. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение: Пер. с англ. М.: Изд. дом „Вильямс“, 2003. 1104 с.
3. *Ипатов В. П.* Широкополосные системы и кодовое разделение сигналов. Принципы и приложения: Пер. с англ. М.: Техносфера, 2007. 488 с.
4. CDMA: прошлое, настоящее, будущее / Под ред. *Л. Е. Варакина и Ю. С. Шинакова*. М.: Международная академия связи, 2003. 608 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. *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.

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

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

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

10. *Стародубцев В. Г., Чернявских А. Е.* Формирование троичных последовательностей Гордона — Миллса — Велча на основе регистров сдвига // Изв. вузов. Приборостроение. 2016. Т. 59, № 3. С. 202—210.

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

12. *Стародубцев В. Г.* Формирование пятеричных последовательностей Гордона — Миллса — Велча для систем передачи дискретной информации // Тр. СПИИРАН. 2019. Т. 18, № 4. С. 912—948.

13. *Lee Wijik, Kim Ji-Youp, No J.S.* New families of p-ary sequence of period (p↑n–1)/2 with low maximum correlation magnitude // IEICE Transact. on Communications. 2014. Vol. E97-B, N 1. P. 2311—2315.

14. *Cho Chang-Min, Kim Ji-Youp, No J. S.* New p-ary sequence families of period $(p^n-1)/2$ with good correlation property using two decimated m-sequences // IEICE Transact. on Communications. 2015. Vol. E98, N 7. P. 1268—1275.

15. *Tasheva Z.* A short survey of p-ary pseudo-random sequences // J. Scientific & Applied Research. 2014. Vol. 2. P. 17—26.

16. *Xia Y., Chen S.* A new family of p-ary sequences with low correlation constructed from decimated sequences // IEEE Transact. on Information Theory. 2012. Vol. 58, N 9. P. 6037—6046.

17. *Helleseth T., Kumar P. V., Martinsen H.* A new family of ternary sequences with ideal two-level autocorrelation function // Designs, Codes and Cryptography. 2001. Vol. 23, N 2. P. 157—166.

18. *Tang X. H., Pingzhi Z. F.* A class of pseudonoise sequences over GF(p) with low correlation zone // IEEE Transact. on Information Theory. 2001. Vol. 47, N 4. Pp. 1644—1649.

19. *Стародубцев В. Г., Ткаченко В. В., Малышева Е. А.* Формирование троичных ГМВ-последовательностей с периодом N=728 в системах передачи измерительной информации // Изв. Тульск. гос. ун-та. Технические науки. 2019. Вып. 6. С. 192—203.

20. *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.

Сведения об авторах

Виктор Геннадьевич Стародубцев — канд. техн. наук, доцент; ВКА им. А. Ф. Можайского, преподаватель; E-mail: vgstarod@mail.ru

Владимир Викторович Ткаченко — канд. техн. наук; ВКА им. А. Ф. Можайского, ст. преподаватель; E-mail: vik_hohol@mail.ru

Елизавета Алексеевна Боброва — слушатель; ВКА им. А. Ф. Можайского, E-mail: m_ea98@mail.ru

Поступила в редакцию
23.01.2020 г.

Ссылка для цитирования: *Стародубцев В. П., Ткаченко В. В., Боброва Е. А.* Формирование троичных последовательностей с высокой структурной скрытностью в системах передачи цифровой информации // Изв. вузов. Приборостроение. 2020. Т. 63, № 5. С. 405—416.

FORMATION OF TERNARY SEQUENCES WITH HIGH STRUCTURAL SECRECY IN DIGITAL INFORMATION TRANSFER SYSTEMS

V. G. Starodubtsev, V. V. Tkachenko, E. A. Bobrova

A. F. Mozhaisky Military Space Academy, 197198, St. Petersburg, Russia
E-mail: vka@mil.ru

An algorithm for determining initial states of shift registers included in the Gordon-Mills-Welch (GMW) ternary sequence generation device with the period of N = 728 is presented. The algorithm is based on comparison of the initial states obtained by solving the system of linear equations in the finite fields and the states determined by decimation of characters of the basic M-sequence. Ternary M-sequences and GMW-sequences have the same two-level periodic autocorrelation function, but different structural secrecy, characterized by equivalent linear complexity. The GMW-sequence is formed using a basic M-sequence with a similar period when it is presented in the form of quasi-square matrix. It is shown that for each of the 48 primitive polynomials in the finite field GF (36), three GMW-sequences can be formed. For binary GMW sequences, the initial states of the shift registers are formed by decimating the symbols of the basic M-sequence, presented in canonical form, by decimation indices corresponding to the roots of indivisible polynomial factor factors. For ternary GMW sequences, the individual summable components have an additional half-period shift of the base M-sequence. It is argued that the obtained results can be used for generating broadband non-binary signals in digital information transmission systems.

Keywords: pseudorandom sequences, finite fields, indivisible and primitive polynomials, structural secrecy, decimation, shift registers

REFERENCES

1. Vishnevskij V.M., Lyahov A.I., Portnoj S.L., Shahnovich I.V. *Shirokopolosnye besprovodnye seti peredachi informacii* (Broadband Wireless Data Transmission Network), Moscow, 2005, 592 p. (in Russ.)
2. Sklar B. *Digital Communications: Fundamentals and Applications*, Prentice Hall, 2001, 1079 p.
3. Ipatov V.P. *Spread Spectrum and CDMA. Principles and Applications*, NY, John Wiley and Sons Ltd., 2005, 488 p.
4. Varakin L.E. and Shinakov Yu.S., ed., *CDMA: proshloe, nastoyashchee, budushchee* (CDMA: Past, Present, Future), Moscow, 2003, 608 p. (in Russ.)
5. Golomb S.W., Gong G. *Signal Design for Good Correlation for Wireless Communication*, *Cryptography and Radar*, Cambridge University Press, 2005, 438 p.
6. Chung H.B., No J.S. *IEEE Transactions on Information Theory*, 1999, no. 6(45), pp. 2060–2065.
7. Rizomiliotis P., Kalouptsidis N. *IEEE Transactions on Information Theory*, 2005, vol. IT–51, pp. 1555–1563.
8. Ipatov V.P. *Periodicheskie diskretnye signaly s optimal'nymi korrelyacionnymi svojstvami* (Periodic Discrete Signals with Optimum Correlation Properties), Moscow, 1992, 152 p. (In Russ.).
9. No Jong-Seon. *IEEE Transactions on Information Theory*, 1996, no. 1(42), pp. 260–262.
10. Starodubtsev V.G., Chernjavskih A.E. *Journal of Instrument Engineering*, 2016, no. 3(59), pp. 201–210. (in Russ.)
11. Tsankov T., Trifonov T., Staneva L. *Journal Scientific & Applied Research*, 2013, vol. 4, pp. 80–87.
12. Starodubtsev V.G. *Trudy SPIIRAN* (SPIIRAS Proceedings), 2019, no. 4(18), pp. 912–948. (in Russ.)
13. Lee Wijik, Kim Ji-Youp, No J.S. *IEICE Transactions on Communications*, 2014, no. 1(E97-B), pp. 2311–2315.
14. Cho Chang-Min, Kim Ji-Youp, No J.S. *IEICE Transactions on Communications*, 2015, no. 7(E98), pp. 1268–1275.
15. Tasheva Z. *Journal Scientific & Applied Research*, 2014, vol. 2, pp. 17–26.
16. Xia Y., Chen S. *IEEE Transactions on Information Theory*, 2012, no. 9(58), pp. 6037–6046.
17. Helleseth T., Kumar P.V., Martinsen H. *Designs, Codes and Cryptography*, 2001, no. 2(23), pp. 157–166.
18. Tang X.H., Pingzhi Z.F. *IEEE Transactions on Information Theory*, 2001, no. 4(47), pp. 1644–1649.
19. Starodubtsev V.G., Tkachenko V.V., Malysheva E.A. *Izvestiya Tulskogo gosudarstvennogo universiteta. Tekhnicheskie nauki* (Proceedings of Tula State University. Technical science), 2019, no. 6, pp. 192–203 (in Russ.)
20. Starodubtsev V.G., Borod'ko D.N., Myshko V.V. *Aviakosmicheskoe priborostroenie* (Aerospace Instrumentation), 2018, no. 5, pp. 3–15 (in Russ.)

Data on authors

Victor G. Starodubtsev — PhD, Associate Professor; A. F. Mozhaisky Military Space Academy, Lecturer; E-mail: vgstarod@mail.ru

Vladimir V. Tkachenko — PhD; A. F. Mozhaisky Military Space Academy, Senior Lecturer; E-mail: vik_hohol@mail.ru

Elizaveta A. Bobrova — Student; A. F. Mozhaisky Military Space Academy,
E-mail: m_ea98@mail.ru

For citation: Starodubtsev V. G., Tkachenko V. V., Bobrova E. A. Formation of ternary sequences with high structural secrecy in digital Information transfer systems. *Journal of Instrument Engineering*. 2020. Vol. 63, N 5. P. 405—416 (in Russian).

DOI: 10.17586/0021-3454-2020-63-5-405-416