УДК 519.725
DOI: 10.17586/0021-3454-2018-61-3-240-248

ФОРМИРОВАНИЕ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОРДОНА — МИЛЛСА — ВЕЛЧА С ПЕРИОДОМ N=511

В. Г. СТАРОДУБЦЕВ, В. М. КУЗНЕЦОВА

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

В соответствии с разработанным алгоритмом формирования последовательностей Гордона — Миллса — Велча (ГМВ) получены проверочные полиномы для полного перечня данных последовательностей с периодом N=511. Двоичные ГМВ-последовательности строятся на основе М-последовательностей, выступающих в качестве базисных последовательностей над конечными полями с двойным расширением вида $GF[(2^m)^n]$ и могут быть представлены в виде матрицы размером $[J\times L]=[(2^m-1)\times(2^m+1)]$. Качественным отличием последовательностей с периодом N=511, формируемых над конечным полем $GF[(2^3)^3]$, является возможность их представления не в виде квазиквадратной матрицы размером $[(2^m-1)\times(2^m+1)]$, а в виде матрицы размером $[J\times L]=[7\times 73]$. Эквивалентная линейная сложность данных последовательностей соответствует степени проверочного полинома, который может быть представлен в виде произведения трех неприводимых полиномов девятой степени. ГМВ-последовательности с периодом N=511 формируются на основе базисных М-последовательностей с аналогичным периодом. Так как в поле $GF(2^9)$ существует 48 примитивных полиномов девятой степени, то полученный полный перечень также содержит 48 проверочных полиномов для ГМВ-последовательностей.

Ключевые слова: *последовательности с составным периодом, конечные поля, неприводимые и примитивные полиномы, эквивалентная линейная сложность*

В современных системах передачи измерительной информации космических средств широко применяются широкополосные сигналы на основе псевдослучайных последовательностей (ПСП) [1—3]. Уникальные свойства сложных сигналов обусловили их использование в системах спутниковой связи, системах навигационного обеспечения, радиолокационных системах [4—6], а также в системах связи и управления военной и специальной техникой ракетно-космической обороны.

В качестве ПСП применяются М-последовательности (МП), последовательности Гордона — Миллса — Велча (ГМВ), последовательности Голда, Касами и др. [7]. Их использование позволяет повысить как структурную скрытность передаваемых сигналов, что является важным условием при проектировании систем передачи информации с повышенными требованиями по конфиденциальности, так и достоверность полученной измерительной информации на этапе предварительной обработки. Повышение достоверности обеспечивается за счет устранения аномальных ошибок, появляющихся вследствие воздействия на передаваемый сигнал помех различного вида в канале связи.

Основной причиной применения МП с периодом N является наличие двухуровневой $(N, -1/N)$ периодической автокорреляционной функции (ПАКФ) при достаточно простой аппаратной реализации в виде регистра сдвига с линейными обратными связями (РС ЛОС). Однако МП обладают низкой структурной скрытностью, которая численно характеризуется эквивалентной линейной сложностью (ЭЛС). ЭЛС определяется степенью проверочного полинома, задающего ПСП, и соответственно количеством символов последовательности, которые необходимо принять для определения проверочного полинома.

Решению задачи повышения ЭЛС ПСП при условии сохранения авто- и взаимнокорреляционных свойств посвящено большое количество работ [8—11]. Среди циклических последовательностей, обладающих наряду с МП двухуровневой ПАКФ, можно выделить ГМВ-последовательности (ГМВП), которые характеризуются более высокой ЭЛС и соответственно более высокой структурной скрытностью [12—15], что определяет приоритетность их применения в системах передачи информации космических средств. Широкому применению ГМВП, однако, препятствует отсутствие практически реализуемых алгоритмов их формирования, включающих определение проверочных полиномов и начальных состояний РС ЛОС, входящих в устройства генерации.

В настоящее время получены полные перечни проверочных полиномов, представляющих собой произведение нескольких неприводимых полиномов, для двоичных ГМВП с периодами N=63 [16], N=255 [17] и N=1023 [18]. Основой алгоритмов формирования этих перечней является положение о том, что корни полиномов $h_{\text{сl}i}(x)$ — сомножителей проверочного полинома $h_{\text{ГМВ}}(x)$ — являются определенными степенями корней проверочного полинома $h_{\text{МП}}(x)$ базисной М-последовательности, с помощью которой формируется ГМВ-последовательность.

Цель настоящей статьи — определение перечня проверочных полиномов двоичных ГМВП с периодом N =511.

Напомним принцип формирования двоичных ГМВП. Двоичные ГМВП формируются над полями с двойным расширением вида GF[$(2^m)^n$], вследствие чего их период является составным числом, т.е. $N = 2^{mn} - 1 = 2^s - 1$, где m, n — натуральные числа. Символы d_i (i=0, 1,…, N–1) ГМВП с периодом $N = 2^{mn}$–1 определяются выражением [7, 13]

$$d_i = \text{tr}_{m1}[(\text{tr}_{mn,m}(\alpha^i))^r], \; 1 \le r < 2^m - 1, \; (r, 2^m - 1) = 1, \tag{1}$$

где $\text{tr}_{mn,\,m}(\cdot)$ — след элемента из поля с двойным расширением GF[$(2^m)^n$] в расширенном поле GF(2^m); $\text{tr}_{m1}(\cdot)$ — след элемента из расширенного поля GF(2^m) в простом поле GF(2); $\alpha \in$ GF[$(2^m)^n$] — примитивный элемент поля с двойным расширением; r — число, взаимно простое с порядком мультипликативной группы расширенного поля GF(2^m), равное $2^m - 1$.

ЭЛС двоичных ГМВП определяется выражением [13]

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

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

Перечень проверочных полиномов ГМВП с периодом N =511 определяется в поле с двойным расширением GF[$(2^m)^n$] = GF[$(2^3)^3$].

Количество различных ГМВП (не считая МП) определяется как произведение числа примитивных полиномов в расширенном поле GF(2^3) и числа примитивных полиномов в поле с двойным расширением GF[$(2^3)^3$] [13]:

$$M_{\text{ГМВ}} = \left(\frac{\varphi(2^m - 1)}{m} - 1 \right) \frac{\varphi(2^{mn} - 1)}{mn} = ((\varphi(7)/3) - 1)(\varphi(511)/9) = 48, \tag{3}$$

где $\varphi(a)$ — функция Эйлера, равная количеству чисел, взаимно простых с числом a, в ряду от 1 до (a – 1).

При n=2 М- и ГМВ-последовательности могут быть представлены в виде матрицы размером $[J \times L]$=[$(2^m$–1)×(2^m+1)], в которой число строк J=2^m–1 равно периоду более короткой МП, называемой характеристической последовательностью (ХП), а количество столбцов L=2^m+1 равно числу различных сдвигов ХП в правиле формирования ГМВП [13].

Качественное отличие последовательностей с периодом N=511, формируемых над конечным полем GF[$(2^3)^3$], заключается в том, что они представляются не в виде квазиквадратной матрицы, а в виде матрицы размером $[J \times L]$=[7×73], что определяется разложением периода N=511 на множители 7 и 73.

В качестве базисной МП, необходимой для формирования ГМВП, берется М-последовательность с периодом N=511 и проверочным полиномом $h_{\text{МП}}(x) = x^9 + x^4 + 1$, корнями которого являются элемент α и его p-сопряженные элементы [19].

Предварительное формирование МП осуществляется для произвольного начального состояния, например 0000000001. Затем согласно методике, изложенной в работе [17], определяется начало МП в соответствии с выражением $d_i = \text{tr}_{9,1}(\alpha^i)$, $i = 0, 1, \ldots, 510$, т.е. находятся символы d_0=1, d_1=0, d_2=0, … d_5=1,…, d_{510}=1, необходимые для вычисления начального состояния регистров сдвига. Полученная МП с начальным состоянием 100001000 записывается в виде матрицы размером $[J \times L] = [7 \times 73]$:

$$F_{\text{МП}} = \begin{vmatrix} 1000010001100001001110010101011000011011110100110111001000101000010101101 \\ 0011111101100100100101101111110010011010100110011000000011000110010100011 \\ 0100101111111010001011000111010110010110011110001111101110100000110101101 \\ 1011101100000101101011111010101010000001010010101111001011101110000001110 \\ 0111010010011110101110101000100100001100111000010111101101100110100001110 \\ 1111000011111111100000111101111000101110011001000001001010011101101000011 \\ 1100111110011011000101010010001110001101101010111000100110001000100000000 \end{vmatrix}. \quad (4)$$

Каждый столбец матрицы $F_{\text{МП}}$ (кроме нулевых) соответствует одному из циклических сдвигов ХП_1, т.е. МП с периодом J=7 и проверочным полиномом $h_1(x) = x^3 + x + 1$, корнями которого в соответствии с таблицей неприводимых полиномов над полем GF(2^3) [19] являются элемент α и его p-сопряженные элементы α^2 и α^4.

Последовательность номеров циклических сдвигов образует правило формирования МП с периодом N=511 в виде вектора из L = 73 компонент:

$$\boldsymbol{I}_{\text{МП}} = \{0\ 6\ 5\ 5\ 3\ 1\ 3\ 3\ 6\ 2\ 2\ 6\ 6\ 5\ 6\ 0\ 5 - 4\ 1\ 4\ 3\ 5\ 0\ 5\ 2\ 3\ 2\ 5\ 2\ 0\ 6\ 3 — 2\ 1\ 6$$
$$2\ 0\ 1\ 4\ 6\ 2\ 3 — 0\ 1\ 3\ 4\ 4\ 4\ 6 — 4\ 6\ 3\ 5\ 4 — 0\ 5\ 5 — 6\ 2 — 2 — 4\ 4\ 5\ 2\}, \quad (5)$$

где „—“ обозначает нулевую последовательность.

На основе полученного правила можно синтезировать ГМВП. Для этого в качестве ХП_2 необходимо выбрать другую МП с периодом J = 7. Для данного периода существует еще только одна М-последовательность с проверочным полиномом $h_3(x) = x^3 + x^2 + 1$, корнями которого являются элементы α^3, α^6 и α^5. (Для удобства записи здесь и далее в качестве подстрочного индекса, являющегося идентификатором полинома, используется минимальный показатель степени корней данного полинома.) Для формирования ХП_2 необходимо выполнить децимацию символов ХП_1 по индексу децимации i_{d1} = 3, соответствующему минимальному показателю степени корней полинома $h_3(x)$. Это удобно сделать для нулевого сдвига ХП_1, соответствующего первому ненулевому столбцу в матрице (4), получив при этом нулевой сдвиг ХП_2.

ГМВП представляется в виде матрицы, аналогичной (4), при подстановке сдвигов ХП_2 в соответствии с правилом формирования (5). Ниже приведена матричная форма записи ГМВП $F_{\text{ГМВ}}$ для индекса i_{d1} = 3, т.е. для ХП_2:

$$F_{\text{ГМВ}} = \begin{vmatrix} 1111101110011111100001111010101110000101001010101000100111001110100000010 \\ 1100010010011011001110010000001100001101111000110111101100101000100001100 \\ 1011010001100101100100111101111000011011100100110000000001001110010100011 \\ 0100111111111010000101000111010110011111010111001100010011000000011010000 1 \\ 1000101101100001001011010111011010010011010110101111001010101000010101101 \\ 0011111100000100101111101010100010001000110010011111001011100110000001110 \\ 0111000011111110101010101101110100010110011100000111101101100110110101111 \end{vmatrix}. \quad (6)$$

Проверочный полином полученной ГМВП определяется с помощью итеративного алгоритма Берлекемпа — Месси:

$$h_{\text{ГМВ}}(x) = x^{27}+x^{26}+x^{25}+x^{24}+x^{23}+x^{21}+x^{20}+x^{19}+x^{17}+x^{12}+x^{10}+x^{8}+x^{5}+x+1. \quad (7)$$

Более компактной записью проверочного полинома является запись коэффициентов полинома в двоичном или двоично-восьмеричном коде [19]:

$$h_{\text{ГМВ}} = 11111011101000010101001000011_2 = 1756412443_8. \quad (8)$$

Полином (7) степени 27 является произведением трех примитивных полиномов степени 9. Данные примитивные полиномы представлены в табл. 1; всего в таблице 48 примитивных полиномов. Далее вместо термина „корень полинома с минимальным показателем степени“ будем использовать термин „минимальный корень“.

Таблица 1

Полином	Полином	Полином
$h_1(x)=x^9+x^4+1$	$h_{41}(x)=x^9+x^8+x^6+x^5+x^4+x+1$	$h_{95}(x)=x^9+x^8+x^7+x^5+x^4+x^3+1$
$h_3(x)=x^9+x^6+x^4+x^3+1$	$h_{43}(x)=x^9+x^8+x^7+x^6+x^3+x+1$	$h_{103}(x)=x^9+x^7+x^5+x^3+x^2+x+1$
$h_5(x)=x^9+x^8+x^5+x^4+1$	$h_{45}(x)=x^9+x^6+x^5+x^4+x^3+x^2+1$	$h_{107}(x)=x^9+x^7+x^5+x+1$
$h_9(x)=x^9+x^8+x^4+x+1$	$h_{47}(x)=x^9+x^8+x^6+x^4+x^3+x+1$	$h_{109}(x)=x^9+x^8+x^6+x^5+x^4+x^3+x^2+x+1$
$h_{11}(x)=x^9+x^5+x^3+x^2+1$	$h_{51}(x)=x^9+x^8+x^7+x^6+x^4+x^2+1$	$h_{111}(x)=x^9+x^8+x^4+x^3+x^2+x+1$
$h_{13}(x)=x^9+x^6+x^5+x^4+x^2+x+1$	$h_{53}(x)=x^9+x^7+x^4+x^2+1$	$h_{117}(x)=x^9+x^8+x^6+x^3+x^2+x+1$
$h_{15}(x)=x^9+x^8+x^6+x^5+1$	$h_{55}(x)=x^9+x^7+x^5+x^4+x^3+x^2+1$	$h_{123}(x)=x^9+x^7+x^2+x+1$
$h_{17}(x)=x^9+x^7+x^6+x^4+x^3+x+1$	$h_{57}(x)=x^9+x^7+x^6+x^5+x^4+x^2+1$	$h_{125}(x)=x^9+x^7+x^6+x^4+1$
$h_{19}(x)=x^9+x^8+x^7+x^2+1$	$h_{59}(x)=x^9+x^7+x^6+x^3+x^2+x+1$	$h_{127}(x)=x^9+x^6+x^5+x^3+1$
$h_{23}(x)=x^9+x^8+x^7+x^6+x^5+x^3+1$	$h_{61}(x)=x^9+x^6+x^4+x^3+x^2+x+1$	$h_{171}(x)=x^9+x^8+x^7+x^5+x^4+x^2+1$
$h_{25}(x)=x^9+x^8+x^7+x^6+x^5+x+1$	$h_{75}(x)=x^9+x^8+x^7+x^6+x^5+x^4+x^3+x+1$	$h_{183}(x)=x^9+x^8+x^5+x^4+x^3+x+1$
$h_{27}(x)=x^9+x^8+x^7+x^3+x^2+x+1$	$h_{79}(x)=x^9+x^8+x^7+x^6+x^2+x+1$	$h_{187}(x)=x^9+x^8+x^7+x^6+x^4+x^3+1$
$h_{29}(x)=x^9+x^8+x^6+x^5+x^3+x+1$	$h_{83}(x)=x^9+x^8+x^4+x^2+1$	$h_{191}(x)=x^9+x^5+x^4+x+1$
$h_{31}(x)=x^9+x^4+x^3+x+1$	$h_{85}(x)=x^9+x^7+x^5+x^4+x^2+x+1$	$h_{223}(x)=x^9+x^8+x^5+x+1$
$h_{37}(x)=x^9+x^6+x^5+x^3+x^2+x+1$	$h_{87}(x)=x^9+x^7+x^5+x^2+1$	$h_{239}(x)=x^9+x^8+x^6+x^5+x^3+x^2+1$
$h_{39}(x)=x^9+x^8+x^7+x^6+x^3+x^2+1$	$h_{93}(x)=x^9+x^7+x^6+x^5+x^4+x^3+1$	$h_{255}(x)=x^9+x^5+1$

Полином $h_{\text{ГМВ}}(x)$ вида (7) может быть представлен в виде произведения трех примитивных полиномов-сомножителей $h_{ci}(x)$ девятой степени из табл. 1:

$$h_{\text{ГМВ}}(x) = h_{\text{c1}}(x)\, h_{\text{c2}}(x)\, h_{\text{c3}}(x) = h_3(x)\, h_5(x)\, h_{17}(x) =$$
$$= (x^9+x^6+x^4+x^3+1)\,(x^9+x^8+x^5+x^4+1)\,(x^9+x^7+x^6+x^4+x^3+x+1). \quad (9)$$

Анализ полинома $h_{\text{ГМВ}}(x)$ показывает, что корни полинома $h_{\text{c1}}(x) = h_3(x)$ являются 3-ми степенями корней полинома $h_{\text{МП}}(x) = x^9+x^4+1$ базисной МП, корни полинома $h_{\text{c2}}(x) = h_5(x)$ — 5-ми степенями, а корни полинома $h_{\text{c3}}(x) = h_{17}(x)$ — 17-ми степенями его корней. Все три полинома являются примитивными.

Алгоритм формирования полного перечня проверочных полиномов ГМВП основан на свойстве повторяемости соотношений между корнями проверочного полинома $h_{\text{МП}}(x)$ базисной МП и корнями полиномов-сомножителей $h_{\text{ci}}(x)$ проверочного полинома $h_{\text{ГМВ}}(x)$ [16].

В соответствии с выражением (3) в поле $GF(2^9)$ существует 48 различных примитивных полиномов, которые могут выступать в качестве проверочных полиномов для базисных МП. Таким образом, можно получить 48 ГМВП с проверочными полиномами 27-й степени, корни трех сомножителей которых являются 3, 5 и 17-ми степенями корней соответствующего полинома базисной МП.

Для примера сформируем проверочный полином ГМВП, основанный на базисной МП с $h_{\text{МП}}(x) = h_{53}(x) = x^9+x^7+x^4+x^2+1$, минимальным корнем которого является элемент α^{53} (см. табл. 1).

Сомножители для $h_{\text{ГМВ}}(x) = h_{\text{c1}}(x)\, h_{\text{c2}}(x)\, h_{\text{c3}}(x)$ определяются следующим образом. Полином $h_{\text{МП}}(x)$ базисной МП имеет корень α^{53}. Тогда одним из корней полинома $h_{\text{c1}}(x)$ должен быть элемент $(\alpha^{53})^3 = \alpha^{159}$, что соответствует полиному $h_{\text{c1}}(x) = h_{125}(x) = x^9+x^7+x^6+x^4+1$ с минимальным корнем α^{125}. Полином $h_{\text{c2}}(x)$ должен иметь корень $(\alpha^{53})^5=\alpha^{265}$, что соответствует

полиному $h_{c2}(x) = h_{19}(x) = x^9+x^8+x^7+x^2+1$ с минимальным корнем α^{19}. Полином $h_{c3}(x)$ должен иметь корень $(\alpha^{53})^{17} = \alpha^{901 \bmod 511} = \alpha^{390}$, что соответствует полиному $h_{c3}(x) = h_{27}(x) = x^9+x^8+x^7+x^3+x^2+x+1$ с минимальным корнем α^{27}. Таким образом, искомый проверочный полином для ГМВП имеет следующий вид:

$$h_{ГМВ}(x) = h_{c1}(x)\, h_{c2}(x)\, h_{c3}(x) = h_{125}(x)\, h_{19}(x)\, h_{27}(x) =$$
$$= (x^9+x^7+x^6+x^4+1)\,(x^9+x^8+x^7+x^2+1)\,(x^9+x^8+x^7+x^3+x^2+x+1). \qquad (10)$$

Результаты вычислений сомножителей проверочных полиномов ГМВП для остальных примитивных полиномов поля GF(2^9), выступающих в качестве полиномов базисных МП, приведены в табл. 2.

Таблица 2

№ п/п	Корни $h_{МП}(x)$ базовой МП	Корни сомножителей $h_{ГМВ}(x)=h_{c1}(x)\, h_{c2}(x)\, h_{c3}(x)$			№ п/п	Корни $h_{МП}(x)$ базовой МП	Корни сомножителей $h_{ГМВ}(x)=h_{c1}(x)\, h_{c2}(x)\, h_{c3}(x)$		
		h_{c1}: α^3	h_{c2}: α^5	h_{c3}: α^{17}			h_{c1}: α^3	h_{c2}: α^5	h_{c3}: α^{17}
1	2	3	4	5	6	7	8	9	10
1	α^1	α^3	α^5	α^{17}	25	α^{59}	α^{43}	α^{79}	α^{123}
2	α^3	α^9	α^{15}	α^{51}	26	α^{61}	α^{183}	α^{51}	α^{15}
3	5	15	25	85	27	75	23	239	191
4	9	27	45	83	28	79	187	47	13
5	11	17	55	187	29	83	95	127	23
6	13	39	9	183	30	85	255	117	125
7	15	45	75	255	31	87	11	123	79
8	17	51	85	25	32	93	47	61	3
9	19	57	95	29	33	95	59	223	41
10	23	41	103	31	34	103	107	1	109
11	25	75	125	117	35	107	13	3	61
12	27	37	29	95	36	109	61	17	5
13	29	87	41	223	37	111	109	11	43
14	31	93	109	1	38	117	191	37	57
15	37	111	87	59	39	123	55	13	47
16	39	117	27	19	40	125	239	57	37
17	41	123	107	93	41	127	223	31	103
18	43	5	187	55	42	171	1	43	11
19	45	29	23	127	43	183	19	83	45
20	47	53	183	9	44	187	25	53	39
21	51	83	255	75	45	191	31	111	171
22	53	125	19	27	46	223	79	93	107
23	55	85	39	53	47	239	103	171	111
24	α^{57}	α^{171}	α^{59}	α^{87}	48	α^{255}	α^{127}	α^{191}	α^{239}

В табл. 2 использованы следующие обозначения: в графах 2 и 7 — корни (показатели степени корней) примитивных полиномов $h_{МП}(x)$ базисных МП; в графах 3—5 и 8—10 — корни (показатели степени корней) полиномов-сомножителей $h_{ci}(x)$ для ГМВП.

Например, требуется определить проверочный полином ГМВП для базисной МП с полиномом, одним из корней которого является элемент α^{127}. Корню α^{127} базисной МП соответствуют полиномы $h_{ci}(x)$ с корнями α^{223}, α^{31} и α^{103}. Тогда проверочный полином ГМВП имеет вид

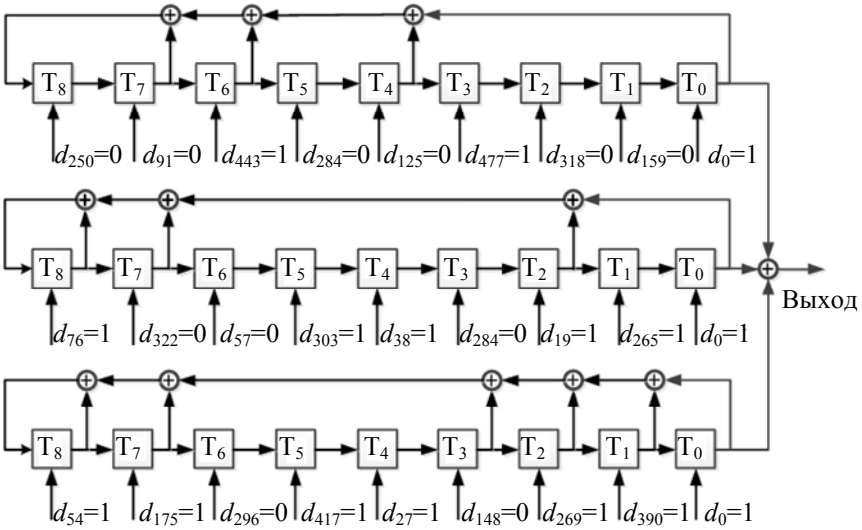
$$h_{ГМВ}(x) = h_{c1}(x)\, h_{c2}(x)\, h_{c3}(x) = h_{223}(x)\, h_{31}(x)\, h_{103}(x) =$$
$$= (x^9+x^8+x^5+x+1)\,(x^9+x^4+x^3+x+1)\,(x^9+x^7+x^5+x^3+x^2+x+1). \qquad (11)$$

Таким образом можно сформировать любой из 48 проверочных полиномов ГМВП.

Структура проверочного полинома ГМВП $h_{ГМВ}(x)$, представляющего собой для конечного поля GF$[(2^3)^3]$ произведение трех примитивных полиномов $h_{ci}(x)$ степени $s = mn = 9$, определяет возможность построения устройства формирования в виде совокупности трех РС ЛОС. Число ячеек, являющихся триггерами T_i, в каждом РС ЛОС равно s=9, т.е. степени полиномов $h_{ci}(x)$,

а сумматоры по mod 2 расставляются в соответствии с коэффициентами этих полиномов. Выходные сигналы РС ЛОС поступают на общий сумматор по mod 2, являющийся выходом устройства.

Структурная схема устройства формирования ГМВП с проверочным полиномом вида (10) приведена на рисунке. Самой трудной прцедурой при генерации ГМВП является определение начальных состояний регистров сдвига. Сложность этой процедуры можно показать путем сравнения ее с аналогичной процедурой при формировании последовательностей Голда. При их генерации с помощью двух РС ЛОС в одном из регистров устанавливается произвольное ненулевое состояние, а во втором последовательно используются всевозможные начальные состояния. При формировании ГМВП такой подход не представляется возможным.



В работе [17] предложен алгоритм, в соответствии с которым начальные состояния регистров сдвига ЛОС, входящих в устройство формирования ГМВП, определяются соотношением степеней корней полиномов $h_{ci}(x)$ и полинома базисной МП, на основе которой формируется ГМВП. На практике значения начальных символов для каждого регистра вычисляются путем децимации символов базисной МП по индексу децимации, зависящему от соотношения степеней корней полиномов $h_{МП}(x)$ и $h_{ci}(x)$.

В рамках алгоритма вычисления начальных состояний необходимо определить начало базисной МП в соответствии с выражением (1) при r=1, а затем провести децимацию символов данной МП по индексам децимации, равным наименьшим показателям степеней корней полиномов $h_{ci}(x)$, т.е. I_{d1}=3, I_{d2}=5, I_{d3}=17.

Одним из способов определения начала МП, т.е. символов d_0, d_1, d_2 и т.д., является способ, основанный на использовании свойства примитивных полиномов, в соответствии с которым для конечных полей характеристики p=2 значение функции следа $\mathrm{tr}_{s,1}\alpha^1$ равно значению коэффициента при (s–1)-й степени переменной x полинома $h_{МП}(x)$, а значение функции следа $\mathrm{tr}_{s,1}\alpha^{-1}$ — значению коэффициента при 1-й степени переменной x.

Для полинома $h_{МП}(x) = x^9+x^4+1$ функции следа $\mathrm{tr}_{9,1}\alpha^1 = 0$, $\mathrm{tr}_{9,1}\alpha^{-1} = 0$. Тогда символу d_1 МП в матрице (4) соответствует позиция, для которой сумма 1, 2, 4, 8, 16, 32, 64, 128 и 256-го символов (каждая позиция по очереди считается первой) равна нулю. Такая позиция единственная, и ей соответствует первый символ (начиная с нулевого) в первой строке матрицы (4). Для дальнейшего анализа МП записывается, начиная с символов d_0=1, d_1=0, d_2=0, d_3=0 и т.д. Тогда в устройстве формирования ГМВП начальные состояния ячеек первого регистра будут равны значениям символов d_0, d_3, d_6, d_9, d_{12}, d_{15}, d_{18}, d_{21}, d_{24}, второго регистра — d_0, d_5, d_{10}, d_{15}, d_{20}, d_{25}, d_{30}, d_{35}, d_{40}, третьего регистра — d_0, d_{17}, d_{34}, d_{51}, d_{68}, d_{85}, d_{102}, d_{119}, d_{136} базисной МП.

Если в качестве базисной взять МП с $h_{МП}(x)=h_{53}(x)=x^9+x^7+x^4+x^2+1$, то начальные символы „$c_i$“ новой базисной МП могут быть получены путем децимации символов исходной МП с $h_{МП}(x)=h_1(x)=x^9+x^4+1$: $c_0=d_0$, $c_1=d_{53}$, $c_2=d_{106}$, $c_3=d_{159}$, $c_4=d_{212}$ и т.д.

Особенность рассматриваемого алгоритма заключается в том, что для вычисления значений начальных состояний ячеек регистров сдвига не требуется формирование новой базисной МП. Номера символов для начальных состояний регистров определяются путем двойной децимации символов исходной базисной МП с $h_{МП}(x) = x^9+x^4+1$. Новые индексы децимации определяются умножением индексов $I_{d1}=3$, $I_{d2}=5$ и $I_{d3}=17$ на показатель степени корня полинома новой базисной МП $h_{МП}(x)= h_{53}(x)$, равный 53: $I_{d4}=53I_{d1}$ mod 511=159, $I_{d5}=53I_{d2}$ mod 511= =265, $I_{d6}=53I_{d3}$ mod 511=390.

Начальные состояния регистров сдвига выбираются из матрицы (4):

— для первого регистра с индексом децимации $I_{d4}=159$: d_0, d_{159}, d_{318}, d_{477}, d_{125}, d_{284}, d_{443}, d_{91}, d_{250};

— для второго регистра с индексом децимации $I_{d5}=265$: d_0, d_{265}, d_{19}, d_{284}, d_{38}, d_{303}, d_{57}, d_{322}, d_{76};

— для третьего регистра с индексом децимации $I_{d6}=390$: d_0, d_{390}, d_{269}, d_{148}, d_{27}, d_{417}, d_{296}, d_{175}, d_{54}.

Полученные значения символов начальных состояний приведены на рисунке.

Вычисление номеров символов выполняется по mod 511. Новая ГМВП с периодом $N=511$ формируется на выходе общего сумматора по модулю 2.

Таким образом, получен полный перечень проверочных полиномов для двоичных ГМВП с периодом $N=511$.

Для произвольного примитивного полинома, выбранного для базисной МП, начальные состояния определяются путем двойной индексации символов базисной МП с учетом показателей степени как корней ее полинома, так и полиномов-сомножителей. При этом не требуется вычисление непосредственно проверочного полинома для ГМВП.

Используя полученные результаты, можно применять ГМВП в системах передачи измерительной информации космических средств по широкополосным радиоканалам, к которым предъявляются повышенные требования по конфиденциальности и структурной скрытности. Показателем структурной скрытности является ЭЛС, значения которой для ГМВП на 3—6 дБ превышают значения для МП.

Полученные полиномы могут быть использованы как при разработке устройств формирования, основанных на РС ЛОС, так и при реализации программных методов формирования ГМВ-последовательностей. Также полученные результаты могут найти применение при разработке методов формирования других классов псевдослучайных последовательностей, допускающих аналитическое представление в конечных полях.

СПИСОК ЛИТЕРАТУРЫ

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

2. *Вишневский В. М., Ляхов А. И., Портной С. Л., Шахнович И. В.* Широкополосные беспроводные сети передачи информации. М.: Техносфера, 2005. 592 с.

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

4. CDMA: прошлое, настоящее, будущее / Под ред. *Л. Е. Варакина и Ю. С. Шинакова*. М.: МАС, 2003. 608 с.

5. *Ershen Wang, Shufang Zhang, Qing Hu*. GPS correlator research and FPGA implementation // J. of System Simulation. 2008. Vol. 20. P. 3582—3585.

6. *Golomb S. W., Gong G.* Signal Design for Good Correlation for Wireless Communication, Criptography and Radar. Cambridge University Press, 2005. 438 p.

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

8. *Прозоров Д. Е., Смирнов А. В., Баланов М. Ю.* Алгоритм быстрой кодовой синхронизации шумоподобных сигналов, построенных на последовательностях повышенной структурной сложности // Вестн. РГРТУ (Рязань). Сер. Радиотехника, радиолокация и системы связи. 2015. № 1 (вып. 51). С. 3—9.

9. *Golomb S. W.* Two-valued sequences with perfect periodic autocorrelation // IEEE Transact. on Aerospace and Electronic Systems. 1992. Vol. 28, № 2. P. 383—386.

10. *Lie-Liang Yang, Hanzo L.* Acquisition of m-sequences using recursive soft sequential estimation // Wireless Communications and Networking. 2003. Vol. 1. P. 683—687.

11. *Cho Chang-Min, Kim Ji-Youp, No Jong-Seon.* 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.

12. *Юдачев С. С., Калмыков В. В.* Ансамбли последовательностей GMW для систем с кодовым разделением каналов // Наука и образование: науч. изд. МГТУ им. Н. Э. Баумана. 2012. № 1. [Электронный ресурс]: <http:// elibrary.ru/item.asp?id=17650851> (дата обращения 13.11.2017).

13. *Стародубцев В. Г.* Алгоритм формирования последовательностей Гордона — Миллса — Велча // Изв. вузов. Приборостроение. 2012. Т. 55, № 7. С. 5—9.

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

15. *Chung H., 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.

16. *Стародубцев В. Г.* Проверочные полиномы последовательностей Гордона — Миллса — Велча // Изв. вузов. Приборостроение. 2013. Т. 56, № 12. С. 7—14.

17. *Стародубцев В. Г.* Формирование последовательностей Гордона — Миллса — Велча на основе регистров сдвига // Изв. вузов. Приборостроение. 2015. Т. 58, № 6. С. 451—457.

18. *Стародубцев В. Г., Попов А. М.* Последовательности Гордона — Миллса — Велча с периодом *N*=1023 // Изв. вузов. Приборостроение. 2017. Т. 60, № 4. С. 318—330.

19. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. М.: Мир, 1976. 594 с.

Сведения об авторах

Виктор Геннадьевич Стародубцев — канд. техн. наук, доцент; ВКА им. А. Ф. Можайского, кафедра технологий и средств автоматизации обработки и анализа информации космических средств; Университет ИТМО, кафедра беспроводных телекоммуникаций; E-mail: vgstarod@mail.ru

Валерия Михайловна Кузнецова — ВКА им. А. Ф. Можайского, кафедра технологий и средств автоматизации обработки и анализа информации космических средств; слушатель; E-mail: lera.zakozhurnikova@mail.ru

Поступила в редакцию
08.12.17 г.

Ссылка для цитирования: *Стародубцев В. Г., Кузнецова В. М.* Формирование последовательностей Гордона — Миллса — Велча с периодом *N*=511 // Изв. вузов. Приборостроение. 2018. Т. 61, № 3. С. 240—248.

FORMATION SEQUENCES OF GORDON — MILLS — WELCH WITH PERIOD *N* = 511

V. G. Starodubtsev, V. M. Kuznetsova

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

Based on developed algorithm for generating Gordon — Mills — Welch sequences, a full list of testing polynomials for GMW-sequences with the period *N* = 511 is obtained. Binary GMW-sequences are formed on the basis of base M-sequence over finite fields with double expansion GF[$(2^m)^n$] and can be represented as a matrix of dimension [J×L]=[$(2^m-1)\times(2^m+1)$]. A qualitative specifics of sequences with the period N = 511 consists in the fact that they are formed over a finite field GF[$(2^3)^3$] and are presented in the form of a matrix of dimension [J×L]=[7×73], but not in the form of quasi-quadratic matrix of dimension [$(2^m-1)\times(2^m+1)$]. Equivalent linear complexity of these sequences corresponds to the degree of the testing polynomial which can be represented as a product of three irreducible polynomials of the ninth degree. GMW-sequences with period N = 511 are formed using M-sequences of the same period. There are 48 primitive polynomials of the ninth degree in the field GF(2^9), the full list also contains 48 test polynomials for GMW-sequences.

Keywords: sequences of composite period, finite fields, indivisible and primitive polynomials, equivalent linear complexity

Data on authors

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

Valeriya M. Kuznetsova — A. F. Mozhaisky Military Space Academy, Department of Technologies and Means for Automation of Processing and Analysis of Space Systems Information; Student; E-mail: lera.zakozhurnikova@mail.ru

For citation: Starodubtsev V. G., Kuznetsova V. M. Formation of Gordon — Mills — Welch sequences with period *N* = 511. *Journal of Instrument Engineering*. 2018. Vol. 61, N 3. P. 240—248 (in Russian).

DOI: 10.17586/0021-3454-2018-61-3-240-248