ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

УДК 519.725
DOI: 10.17586/0021-3454-2016-59-3-202-210

ФОРМИРОВАНИЕ ТРОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОРДОНА — МИЛЛСА — ВЕЛЧА НА ОСНОВЕ РЕГИСТРОВ СДВИГА

В. Г. СТАРОДУБЦЕВ[1], А. Е. ЧЕРНЯВСКИХ[2]

[1]*Военно-космическая академия им. А. Ф. Можайского, 197198, Санкт-Петербург, Россия*
Университет ИТМО, 197101, Санкт-Петербург, Россия
E-mail: vgstarod@mail.ru

[2]*Военно-космическая академия им. А. Ф. Можайского, 197198, Санкт-Петербург, Россия*

Разработан алгоритм формирования троичных последовательностей Гордона — Миллса — Велча (ГМВ) и определения начальных состояний регистров сдвига, входящих в устройство формирования. Троичные ГМВ-последовательности, как и двоичные, формируются на основе совокупности регистров сдвига, линейные обратные связи которых определяются коэффициентами неприводимых полиномов, являющихся сомножителями проверочного полинома ГМВ-последовательности. В соответствии с предложенным алгоритмом начальные состояния регистров сдвига определяются путем децимации символов базисной М-последовательности, на основе которой формируется ГМВ-последовательность, по индексу децимации, зависящему от соотношения степеней корней полиномов-сомножителей и корней полинома базисной М-последовательности.

Ключевые слова: *троичные последовательности с составным периодом, конечные поля, неприводимые и примитивные полиномы, регистры сдвига с линейными обратными связями*

Последовательности Гордона — Миллса — Велча (ГМВ), и двоичные, и недвоичные, находят широкое применение в системах связи и управления, к которым предъявляются высокие требования как по конфиденциальности, так и по пропускной способности [1—6]. ГМВ-последовательности могут быть использованы в системах спутниковой связи с кодовым разделением сигналов [7—10], в интеллектуальных транспортных системах, охватывающих транспортную структуру мегаполисов [11], в подсистемах поиска и синхронизации сигналов[12—14].

Вследствие одноуровневой периодической автокорреляционной функции (ПАКФ), аналогичной ПАКФ М-последовательностей, ГМВ-последовательности также могут применяться в качестве скремблирующих и расширяющих последовательностей в системах связи и навигации [15—19].

Настоящая статья продолжает цикл публикаций, посвященных разработке алгоритмов формирования ГМВ-последовательностей и анализу их корреляционных и структурных свойств [20—22]. Так, в работах [20, 21] рассмотрены алгоритм формирования ГМВ-последовательностей, основанный на их матричном представлении, и алгоритм формирования проверочных полиномов ГМВ-последовательностей, в котором использованы структурные свойства конечных полей с двойным расширением. Получены перечни проверочных по-

линомов для двоичных ГМВ-последовательностей с периодами N=63, N=255 и для троичных ГМВ-последовательностей с N=80.

Алгоритм определения начальных состояний регистров сдвига с линейными обратными связями (РС ЛОС), входящих в устройство формирования двоичных ГМВ-последовательностей, представлен в работе [22]. Алгоритм опирается на свойство проверочных полиномов, заключающееся в том, что корни полиномов $h_{ci}(x)$ — сомножителей проверочного полинома $h_{\text{ГМВ}}(x)$ — являются степенями корней проверочного полинома $h_{\text{МП}}(x)$ базисной М-последовательности, с помощью которой формируется ГМВ-последовательность. Однако непосредственное применение данного алгоритма для определения начальных состояний РС ЛОС при формировании троичных ГМВ-последовательностей не приводит к положительному результату.

Цель настоящей статьи — разработка алгоритма формирования троичных ГМВ-последовательностей и определения начальных состояний РС ЛОС, входящих в устройство формирования.

Возможность построения устройства формирования p-ичной ГМВ-последовательности в виде совокупности нескольких РС ЛОС определяется тем, что структура полинома $h_{\text{ГМВ}}(x)$ представляет собой для полей GF(p^S) (p — характеристика поля, S — натуральное число) произведение нескольких неприводимых над полем GF(p) полиномов $h_{ci}(x)$ степени S.

Устройство формирования состоит из двух или более РС ЛОС, число ячеек $Я_i$ в каждом из которых равно S, т.е. степеням полиномов $h_{ci}(x)$, а сумматоры по mod p расставляются в соответствии с коэффициентами данных полиномов. Выходные символы РС ЛОС поступают на общий сумматор по mod p, являющийся выходом устройства.

Разрабатываемый алгоритм может рассматриваться как модификация представленного в работе [22] алгоритма для двоичных ГМВ-последовательностей, определяемая особенностями взаимосвязи функций следа и коэффициентов проверочных полиномов в конечных полях характеристики p=3.

Например, для поля GF(3^4) коэффициенты примитивного полинома для элемента α связаны с функциями следа следующим образом [3, 5, 15]:

$$h(x) = x^4 + 2x^3 + 2 = (x - \alpha)\,(x - \alpha^3)\,(x - \alpha^9)\,(x - \alpha^{27}) =$$
$$= x^4 - (\text{tr}_{4,1}\alpha^1)\,x^3 + (\text{tr}_{4,1}\alpha^4 + \text{tr}_{4,1}\alpha^{10})\,x^2 - (\text{tr}_{4,1}\alpha^{13})\,x + \alpha^{40}, \qquad (1)$$

где $\text{tr}_{4,1}(\cdot)$ — след элемента из расширенного поля GF(3^4) в простом поле GF(3); $\alpha \in$ GF(3^4) — примитивный элемент расширенного поля.

Для базисной М-последовательности с периодом N=80 символы d_0, d_1, d_2, d_3, …, d_{79} определены через функцию следа $d_i = \text{tr}_{2,1}(\text{tr}_{4,2}(\alpha^i))^r$ [20, выражение (1)]. В соответствии с алгоритмом для двоичных последовательностей [22] и индексами децимации для троичных последовательностей с периодом $N = 80$ ($I_{d1} = 7$, $I_{d2} = 13$, $I_{d3} = 5$ [21]) начальные состояния РС ЛОС должны были бы определяться следующими символами троичной М-последовательности:

$$\begin{gathered}\text{для } h_{c1}(x) \text{ — символами } d_0, d_7, d_{14}, d_{21};\\ \text{для } h_{c2}(x) \text{ — символами } d_0, d_{13}, d_{26}, d_{39};\\ \text{для } h_{c3}(x) \text{ — символами } d_0, d_5, d_{10}, d_{15}.\end{gathered} \qquad (2)$$

Однако вычисления, выполненные в соответствии с (2), не позволяют сформировать троичную ГМВ-последовательность с периодом $N = 80$.

Для коррекции выражений (2) найдем значения начальных состояний регистров сдвига путем решения системы линейных уравнений при заданном сегменте троичной ГМВ-последовательности длиной 12 символов.

Вычисления проведем для троичной ГМВ-последовательности с периодом $N = 80$, полином которой имеет следующий вид [21, выражения (11), (12)]:

$$h_{\text{ГМВ}}(x) = x^{12} + x^{11} + x^8 + 2x^7 + 2x^6 + x^4 + 2x^2 + x + 2 =$$
$$= h_{c1}(x)\,h_{c2}(x)\,h_{c3}(x) = (x^4 + x^3 + x^2 + 2x + 2)\,(x^4 + 2x + 2)\,(x^4 + 2x^2 + 2). \qquad (3)$$

Данная ГМВ-последовательность образована на основе базисной М-последовательности с проверочным полиномом $h_{\text{МП}}(x) = x^4 + 2x^3 + 2$ [21].

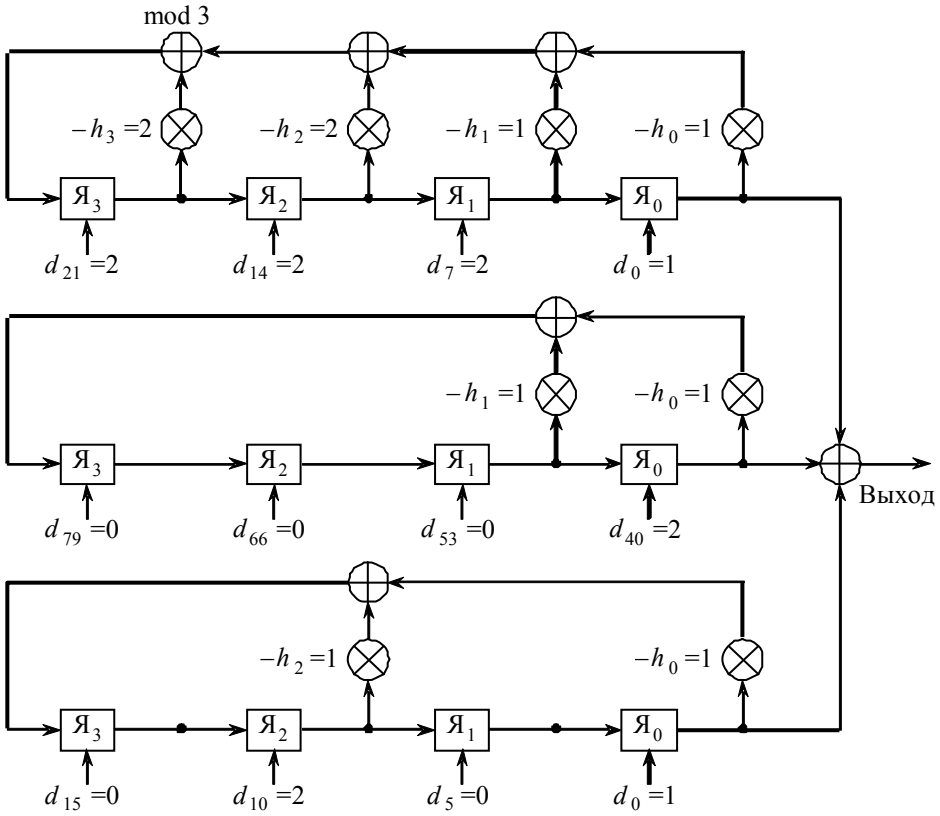
Устройство формирования троичной ГМВ-последовательности состоит из трех регистров сдвига (см. рисунок), символы на выходах которых определяются коэффициентами полиномов $h_{\text{с1}}(x) = x^4 + x^3 + x^2 + 2x + 2$, $h_{\text{с2}}(x) = x^4 + 2x + 2$ и $h_{\text{с3}}(x) = x^4 + 2x^2 + 2$ с помощью рекуррентных выражений

$$C_{4+i} = 2C_{3+i} + 2C_{2+i} + C_{1+i} + C_{0+i},\ i = 0, 1,\ldots, 75; \quad (4)$$

$$C_{4+i} = C_{1+i} + C_{0+i},\ i = 0, 1,\ldots, 75; \quad (5)$$

$$C_{4+i} = C_{2+i} + C_{0+i},\ i = 0, 1,\ldots, 10. \quad (6)$$

Выходные символы регистров сдвига складываются в сумматоре по mod 3, образуя на его выходе искомую ГМВ-последовательность с периодом $N = 80$. Заметим, что в первом и втором регистрах вследствие примитивности полиномов $h_{\text{с1}}(x)$ и $h_{\text{с2}}(x)$ формируются М-последовательности с периодом $N = 80$. В третьем регистре период формируемой последовательности равен 16, что соответствует периоду корней неприводимого, но не примитивного полинома $h_{\text{с3}}(x)$. При этом в одном периоде ГМВ-последовательности содержится пять периодов данной последовательности. (Приведенные на рисунке значения начальных состояний регистров сдвига формируются в результате разработки алгоритма.)



Система уравнений состоит из 12 линейных уравнений (три группы по четыре символа начального состояния для каждого регистра сдвига). Для наглядности обозначим неизвестные символы начального состояния трех регистров сдвига через x_i, y_i и z_i, $i = 0, 1, 2, 3$. Используя выражения (4)—(6), можно получить значения символов x_i, y_i и z_i для $i = 4, 5,\ldots, 11$.

Требуемый сегмент ГМВ-последовательности длиной 12 символов имеет следующий вид [21, выражение (10)]:

$$\begin{array}{cccccccccccc} C_0 & C_1 & C_2 & C_3 & C_4 & C_5 & C_6 & C_7 & C_8 & C_9 & C_{10} & C_{11} \\ 0 & 0 & 0 & 2 & 1 & 2 & 1 & 2 & 0 & 2 & 2 & 1 \end{array} \quad (7)$$

Сформируем систему уравнений вида $x_i + y_i + z_i = C_j$ ($i = 0, 1, 2, 3$; $j = 0, 1, \ldots, 11$; $C_j = 0, 1, 2$), каждое из которых определяется с помощью выражений (4)—(6):

$$\left.\begin{aligned}
&C_0: \quad x_0 + y_0 + z_0 = 0;\\
&C_1: \quad x_1 + y_1 + z_1 = 0;\\
&C_2: \quad x_2 + y_2 + z_2 = 0;\\
&C_3: \quad x_3 + y_3 + z_3 = 2;\\
&C_4: \quad x_0 + x_1 + 2x_2 + 2x_3 + y_0 + y_1 + z_0 + z_2 = 1;\\
&C_5: \quad 2x_0 + 2x_2 + y_1 + y_2 + z_1 + z_3 = 2;\\
&C_6: \quad 2x_1 + 2x_3 + y_2 + y_3 + z_0 + 2z_2 = 1;\\
&C_7: \quad 2x_0 + 2x_1 + x_3 + y_0 + y_1 + y_3 + z_1 + 2z_3 = 2;\\
&C_8: \quad x_0 + x_2 + 2x_3 + y_0 + 2y_1 + y_2 + 2z_0 = 0;\\
&C_9: \quad 2x_0 + x_2 + 2x_3 + y_1 + 2y_2 + y_3 + 2z_1 = 2;\\
&C_{10}: \quad 2x_0 + x_1 + x_2 + 2x_3 + y_0 + y_1 + y_2 + 2y_3 + 2z_2 = 2,\\
&C_{11}: \quad 2x_0 + x_1 + 2x_2 + 2x_3 + 2y_0 + y_2 + y_3 + 2z_3 = 1.
\end{aligned}\right\} \qquad (8)$$

В результате решения данной системы, например методом последовательного исключения неизвестных, получим следующие значения начальных состояний для трех регистров сдвига:

$$\begin{aligned}
&x_0 = 1;\ x_1 = 0;\ x_2 = 1;\ x_3 = 2;\\
&y_0 = 2;\ y_1 = 1;\ y_2 = 2;\ y_3 = 1;\\
&z_0 = 0;\ z_1 = 2;\ z_2 = 0;\ \ z_3 = 2.
\end{aligned} \qquad (9)$$

Можно показать, что при таких начальных состояниях трех регистров сдвига на выходе устройства будет формироваться троичная ГМВ-последовательность [21, выражение (10)].

Алгоритм формирования троичной ГМВ-последовательности и определения начальных состояний РС ЛОС включает следующие этапы.

Этап 1. Задание проверочного полинома базисной М-последовательности с периодом $N = 80$.

Выбирается проверочный полином степени $S = 4$ троичной М-последовательности [21, табл. 5]

$$h_{\text{МП}}(x) = x^4 + 2x^3 + 2, \qquad (10)$$

корнями которого являются элементы α^1, α^3, α^9, α^{27}.

Этап 2. Формирование М-последовательности и определение ее начала, т.е. символов d_0, d_1, d_2 и т.д.

В соответствии с проверочным полиномом формируется М-последовательность для произвольного начального состояния, например для состояния 0001 (табл. 1, строки d_i^*).

Таблица 1

$i_{\text{МП}}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	**16**	17	18	19
d_i^*	0	0	0	**1**	**1**	**1**	**1**	2	0	1	2	1	1	2	1	2	**0**	2	0	2
Сумма 1	1	3	3	3	**4**	7	4	7	2	6	4	5	4	7	2	4	2	6	5	6
Сумма 2	3	3	3	3	3	3	6	6	3	6	3	3	3	6	3	6	**0**	6	3	6
$i_{\text{МП}}$	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
d_i^*	2	1	1	0	2	0	1	1	0	0	1	2	2	2	0	2	1	0	0	2
Сумма 1	5	2	4	4	6	5	3	4	4	3	3	7	2	5	2	6	5	4	3	3
Сумма 2	6	6	3	3	3	6	6	6	6	3	3	6	3	6	3	6	6	3	3	3
$i_{\text{МП}}$	40	41	42	43	**44**	45	46	47	48	49	50	51	52	53	54	55	**56**	57	58	59
d_i^*	0	0	0	2	**2**	2	2	1	0	2	1	2	2	1	2	1	**0**	1	0	1
Сумма 1	2	6	3	6	**8**	5	5	5	1	6	5	4	5	5	4	2	1	3	4	6
Сумма 2	3	3	3	6	6	3	6	3	3	6	3	3	6	3	3	3	**0**	3	3	3
$i_{\text{МП}}$	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
d_i^*	1	2	2	0	1	0	2	2	0	0	2	1	1	1	0	1	2	0	0	1
Сумма 1	4	4	5	2	6	4	3	5	5	3	3	5	1	4	4	3	4	2	3	3
Сумма 2	3	6	3	3	3	3	6	6	3	6	3	6	3	6	3	6	6	3	3	3

Для упрощения записи в табл. 1 введены следующие обозначения:

$i_{МП}$ — номера позиций последовательности с полиномом $h_{МП}(x)$;

d_i^* — значение символа последовательности с полиномом $h_{МП}(x)$ для произвольного начального состояния;

$d_{i_{МП}}$ — значение символа последовательности с полиномом $h_{МП}(x)$;

сумма 1 — арифметическая сумма значений 1, 3, 9, 27-го символов для каждого символа последовательности, считаемого первым;

сумма 2 — арифметическая сумма значений 13, 31, 37, 39-го символов для каждого символа последовательности, считаемого первым.

Определение начала троичной М-последовательности является более трудоемким процессом, чем его определение для двоичных последовательностей, и существенным образом зависит от значений коэффициентов проверочного полинома. С учетом выражения (1) для рассматриваемого примера можно получить следующие значения функций следа:

$$\mathrm{tr}_{4,1}\alpha^0 = d_0 = 1;\ \mathrm{tr}_{4,1}\alpha^1 = d_1 = 1;\ \mathrm{tr}_{4,1}\alpha^{13} = d_{13} = 0;\ \mathrm{tr}_{4,1}\alpha^{40} = d_{40} = 2. \qquad (11)$$

Вычисление для всех позиций арифметических сумм значений символов позиций 1, 3, 9 и 27 (при этом каждая из сумм должна равняться четырем, так как p-сопряженные элементы поля имеют одинаковые функции следа) не позволяет непосредственно определить начало последовательности, так как сумма, равная четырем, встречается для значительного числа позиций (см. табл. 1, строки „Сумма 1“).

Для определения начала последовательности целесообразно использовать элементы, функция следа которых известна по коэффициентам примитивного полинома и равна нулю или двум. При этом сумма для четырех p-сопряженных элементов равна нулю или восьми. Поэтому в соответствии с выражениями (11), где $\mathrm{tr}_{4,1}\alpha^{13} = d_{13} = 0$, для каждой позиции $i_{МП}$ определим сумму символов 13, 31, 37 и 39-й позиций, которая для искомого символа d_{13} равна нулю (см. табл. 1, строки „Сумма 2“). В табл. 1 таких позиций две: 16-я и 56-я, т.е. данные позиции могут соответствовать символу d_{13}. Если в качестве символа d_{13} выбрать позицию 56, то символу d_1 соответствует позиция 44, для которой функция следа равна двум, что противоречит (11). При выборе позиции 16 символу d_1 соответствует позиция 4, для которой функция следа равна единице, что согласуется с (11). (Рассматриваемые символы выделены в табл. 1 подчеркиванием.)

Можно сделать вывод, что начало М-последовательности соответствует позициям с 3-й по 6-ю и определяется следующим образом:

$$d_0 = d_1 = d_2 = d_3 = 1. \qquad (12)$$

Для данного начального состояния формируется М-последовательность (табл. 2, строки d_i). Для удобства определения начальных состояний регистров сдвига табл. 2 приведена при описании 4-го этапа алгоритма.

Этап 3. Определение полиномов-сомножителей $h_{ci}(x)$ для проверочного полинома ГМВ-последовательности $h_{ГМВ}(x)$ и построение соответствующих регистров сдвига с обратными связями.

Для заданного полинома базисной М-последовательности $h_{МП}(x)$ вида (10) проверочный полином ГМВ-последовательности $h_{ГМВ}(x)$ определяется выражением (3).

Этап 4. Определение начальных состояний регистров сдвига по символам базисной М-последовательности.

Для определения начальных состояний регистров сдвига вернемся к необходимости коррекции выражений (2). Для этого на основе выражений (9) сформируем соответствующие последовательности и в результате их посимвольного суммирования получим ГМВ-после-

довательность [21, выражение (10)]. Результаты вычислений представлены в табл. 2, где, кроме принятых в табл. 1, использованы следующие обозначения:

i_{c1}, i_{c2}, i_{c3} — номера позиций последовательностей с полиномами $h_{c1}(x)$, $h_{c2}(x)$, $h_{c3}(x)$;

$d_{i_{c1}}$, $d_{i_{c2}}$, $d_{i_{c3}}$, $d_{i_{ГМВ}}$ — значения символов последовательностей с полиномами $h_{c1}(x)$, $h_{c2}(x)$, $h_{c3}(x)$, $h_{ГМВ}(x)$.

Отметим, что в качестве начальных состояний для последовательностей с полиномами $h_{c1}(x)$, $h_{c2}(x)$ и $h_{c3}(x)$ взяты значения символов, определяемые выражениями (9), а не выражениями (2).

Определим согласно табл. 2 (строки $d_{i_{МП}}$) начальные состояния регистров сдвига в соответствии с выражениями (2):

$$\begin{gathered} x_0^* = 1;\ x_1^* = 2;\ x_2^* = 2;\ x_3^* = 2; \\ y_0^* = 1;\ y_1^* = 0;\ y_2^* = 0;\ y_3^* = 0; \\ z_0^* = 1;\ z_1^* = 0;\ z_2^* = 2;\ z_3^* = 0. \end{gathered} \tag{13}$$

Найдем данные наборы символов в соответствующих последовательностях в табл. 2 (строки $d_{i_{c1}}$, $d_{i_{c2}}$, $d_{i_{c3}}$). Наборам x_i^* и z_i^* соответствуют позиции 43, 44, 45 и 46 М-последовательности; набор y_i^* совпадает с позициями 3, 4, 5 и 6, которые сдвинуты на полпериода М-последовательности относительно вышеназванных. Для троичных последовательностей это означает, что в качестве набора y_i^* на 43, 44, 45 и 46-й позициях необходимо использовать символы, обратные по сложению символам в выражениях(13), т.е. символы 2, 0, 0, 0, а не 1, 0, 0, 0.

Данный вывод подтверждается значениями символов в наборах x_i^*, y_i^* и z_i^* в табл. 2.

Таблица 2

$i_{МП}$	d_0	d_1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$d_{i_{МП}}$	1	1	1	1	2	0	1	2	1	1	2	1	2	0	2	0	2	2	1	1
i_{c1}	0	7	14	21	28	35	42	49	56	63	70	77	4	11	18	25	32	39	46	53
$d_{i_{c1}}$	1	0	1	2	1	1	1	1	0	1	1	2	1	2	0	1	2	2	0	1
i_{c2}	0	13	26	39	52	65	78	11	24	37	50	63	76	9	22	35	48	61	74	7
$d_{i_{c2}}$	2	1	2	**1**	**0**	**0**	**0**	1	0	0	1	1	0	1	2	1	1	0	0	2
i_{c3}	0	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	0	5	10	15
$d_{i_{c3}}$	0	2	0	2	0	1	0	0	0	1	0	**1**	**0**	**2**	**0**	0	0	2	0	2
$d_{i_{ГМВ}}$	**0**	**0**	**0**	**2**	**1**	**2**	**1**	**2**	**0**	**2**	**2**	**1**	**1**	**2**	**2**	**2**	**0**	**1**	**0**	**2**
$i_{МП}$	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
$d_{i_{МП}}$	0	2	0	1	1	0	0	1	2	2	2	0	2	1	0	0	2	0	0	0
i_{c1}	60	67	74	1	8	15	22	29	36	43	50	57	64	71	78	5	12	19	26	33
$d_{i_{c1}}$	0	1	0	0	1	0	2	2	0	0	1	1	1	2	2	1	0	0	0	1
i_{c2}	20	33	46	59	72	5	18	31	44	57	70	3	16	29	42	55	68	1	14	27
$d_{i_{c2}}$	1	0	2	0	1	2	2	1	0	1	0	1	1	1	1	2	2	2	0	1
i_{c3}	20	25	30	35	40	45	50	55	60	65	70	75	0	5	10	15	20	25	30	35
$d_{i_{c3}}$	0	1	0	0	0	1	0	**1**	**0**	**2**	**0**	0	0	2	0	2	0	1	0	0
$d_{i_{ГМВ}}$	**1**	**2**	**2**	**0**	**2**	**0**	**1**	**1**	**0**	**0**	**1**	**2**	**2**	**2**	**0**	**2**	**2**	**0**	**0**	**2**
$i_{МП}$	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
$d_{i_{МП}}$	2	2	2	2	1	0	2	1	2	2	1	2	1	0	1	0	1	1	2	2
i_{c1}	40	47	54	61	68	75	2	9	16	23	30	37	44	51	58	65	72	79	6	13
$d_{i_{c1}}$	2	0	2	**1**	**2**	**2**	**2**	2	0	2	2	1	2	1	0	2	1	1	0	2
i_{c2}	40	53	66	79	12	25	38	51	64	77	10	23	36	49	62	75	8	21	34	47
$d_{i_{c2}}$	1	2	1	**2**	**0**	**0**	**0**	2	0	0	2	2	0	2	1	2	2	0	0	1
i_{c3}	40	45	50	55	60	65	70	75	0	5	10	15	20	25	30	35	40	45	50	55
$d_{i_{c3}}$	0	1	0	**1**	**0**	**2**	**0**	0	0	2	0	2	0	1	0	0	0	1	0	**1**
$d_{i_{ГМВ}}$	**0**	**0**	**0**	**1**	**2**	**1**	**2**	**1**	**0**	**1**	**1**	**2**	**2**	**1**	**1**	**1**	**0**	**2**	**0**	**1**

Продолжение табл. 2

$i_{\text{МП}}$	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
$d_{i_{\text{МП}}}$	0	1	0	2	2	0	0	2	1	1	1	0	1	2	0	0	1	0	0	0
$i_{\text{с1}}$	20	27	34	41	48	55	62	69	76	3	10	17	24	31	38	45	52	59	66	73
$d_{i_{\text{с1}}}$	0	2	0	0	2	0	1	1	0	0	2	2	2	1	1	2	0	0	0	2
$i_{\text{с2}}$	60	73	6	19	32	45	58	71	4	17	30	43	56	69	2	15	28	41	54	67
$d_{i_{\text{с2}}}$	2	0	1	0	2	1	1	2	0	2	0	2	2	2	2	1	1	1	0	2
$i_{\text{с3}}$	60	65	70	75	0	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75
$d_{i_{\text{с3}}}$	**0**	**2**	**0**	0	0	2	0	2	0	1	0	0	0	1	0	**1**	**0**	**2**	**0**	0
$d_{i_{\text{ГМВ}}}$	2	1	1	0	1	0	2	2	0	0	2	1	1	1	0	1	1	0	0	1

Таким образом, коррекция выражений (2) заключается во введении дополнительного условия, определяющего символы базисной М-последовательности, которые участвуют в формировании начальных состояний трех регистров сдвига для каждого индекса децимации I_{d1}=7, I_{d2}=13, I_{d3}=5 и принимают следующие значения:

для $h_{\text{с1}}(x)$ — символы $d_0 = 1$, $d_7 = d_{14} = d_{21} = 2$;

для $h_{\text{с2}}(x)$ — символы $d_{40} = 2$, $d_{53} = d_{66} = d_{79} = 0$;

для $h_{\text{с3}}(x)$ — символы $d_0 = 1$, $d_5 = 0$, $d_{10} = 2$, $d_{15} = 0$.

Отметим, что изменения коснулись только регистра сдвига, начальное состояние которого определяется по символам базисной М-последовательности по индексу децимации $I_{d2} = 13$.

Этап 5. Формирование последовательностей с проверочными полиномами-сомножителями $h_{ci}(x)$ для полученных начальных состояний (см. рисунок и табл. 2, строки $d_{i_{\text{с1}}}$, $d_{i_{\text{с2}}}$, $d_{i_{\text{с3}}}$).

Этап 6. Формирование искомой ГМВ-последовательности путем сложения последовательностей на выходах РС ЛОС (см. табл. 2, строки $d_{i_{\text{ГМВ}}}$).

Таким образом, разработан алгоритм формирования троичных ГМВ-последовательностей и определения начальных состояний РС ЛОС, проверочные полиномы которых являются сомножителями полинома ГМВ-последовательности. В качестве исходных данных требуется только знание примитивного полинома степени S, задающего троичную базисную М-последовательность.

Показано, что начальные состояния регистров сдвига, построенных в соответствии с коэффициентами неприводимых полиномов, являющихся сомножителями проверочного полинома ГМВ-последовательности, полностью определяются соотношением степеней корней данных полиномов и полинома базисной М-последовательности.

С практической точки зрения, начальные состояния регистров сдвига определяются децимацией символов базисной М-последовательности по индексу децимации, зависящему от соотношения степеней корней полиномов.

Троичные ГМВ-последовательности могут быть использованы в системах мобильной связи стандарта GSM при разработке устройств синхронизации, к которым предъявляются повышенные требования по конфиденциальности, и в системах мобильной связи стандарта CDMA в качестве расширяющих последовательностей. Также данные последовательности могут найти применение при формировании широкополосных сигналов различного функционального типа в спутниковых навигационных системах.

СПИСОК ЛИТЕРАТУРЫ

1. *Варакин Л. Е.* Системы связи с шумоподобными сигналами. М.: Радио и связь, 1985. 384 с.

2. *Ипатов В. П.* Широкополосные системы и кодовое разделение сигналов. Принципы и приложения / Пер. с англ.; Под ред. *В. П. Ипатова*. М.: Техносфера, 2007. 488 с.

3. *Свердлик М. Б.* Оптимальные дискретные сигналы. М.: Сов. радио, 1975. 200 с.

4. *Мешковский К. А., Кренгель Е. И.* Генерация псевдослучайных последовательностей Гордона, Милза, Велча // Радиотехника. 1998. № 5. С. 25—28.

5. *Стельмашенко Б. Г., Тараненко П. Г.* Нелинейные псевдослучайные последовательности в широкополосных системах передачи информации // Зарубежная радиоэлектроника. 1988. № 9. С. 76—82.

6. *Кренгель Е. И.* О числе псевдослучайных последовательностей Гордона, Милза, Велча // Техника средств связи. Сер. ТРС. 1979. Вып. 3. С. 17—30.

7. *Калмыков В. В., Федоров И. Б., Юдачев С. С.* Системы сотовой и спутниковой связи. М.: Изд-во „Рудомино“, 2010. 280 с.

8. CDMA: прошлое, настоящее, будущее / Под ред. *Л. Е. Варакина* и *Ю. С. Шинакова*. М.: Международная академия связи, 2003. 608 с.

9. *Юдачев С. С., Калмыков В. В.* Ансамбли последовательностей GMW для систем с кодовым разделением каналов // Наука и образование: электронное науч.-техн. издание. 2012. № 1; [Электронный ресурс]: <http://technomag.edu.ru /issue/264798.html>.

10. *Юдачев С. С.* Последовательности на основе бент-функций для широкополосных систем с кодовым разделением каналов // Электронный науч.-техн. журн. „Инженерный вестник“ МГТУ им. Н. Э. Баумана. 2013. № 1. С. 531—540; [Электронный ресурс]: <http://engbul.bmstu.ru/file/out/601567>.

11. *Alasmary W., Zhuang W.* Mobility impact in IEEE 802.11p infrastructureless vehicular networks//Ad Hoc Networks. 2010. P. 1—9.

12. *Levanon N., Mozeson E.* Radar Signals. Chichester: John Wiley & Sons, 2005. 411 p.

13. *Прозоров Д. Е.* Быстрый поиск дальномерных кодов, сформированных на М-последовательностях // Электросвязь. 2008. № 8. С. 48—51.

14. *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.

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

16. *Golomb S. W.* Two-valued sequences with perfect periodic autocorrelation// IEEE Transact. on Aerospace and Electronic Systems. 1992. Vol. 28, N 2. P. 383—386.

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

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

19. *Леухин А. Н., Парсаев Н. В.* Бесконечные множества фазокодированных последовательностей с одноуровневой периодической автокорреляционной функцией // Радиотехника. 2009. № 12. С. 6—11.

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

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

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

Сведения об авторах

Виктор Геннадьевич Стародубцев — канд. техн. наук, доцент; ВКА им. А. Ф. Можайского, кафедра технологий и средств комплексной обработки и передачи информации в АСУ; ст. преподаватель; НИУ ИТМО, кафедра беспроводных телекоммуникаций; E-mail: vgstarod@mail.ru

Алина Евгеньевна Чернявских — ВКА им. А. Ф. Можайского, кафедра технологий и средств комплексной обработки и передачи информации в АСУ; слушатель; E-mail: vgstarod@mail.ru

Рекомендована кафедрой
беспроводных телекоммуникаций
НИУ ИТМО

Поступила в редакцию
04.12.15 г.

Ссылка для цитирования: *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.

GENERATION OF TERNARY GORDON—MILLS—WELCH SEQUENCES ON THE BASE OF SHIFT REGISTERS

V. G. STARODUBTSEV [1], A. E. CHERNYAVSKIKH [2]

[1] *A. F. Mozhaysky Military Space Academy, 197198, St. Petersburg, Russia*
ITMO University, 197101, St. Petersburg, Russia
E-mail: vgstarod@mail.ru

[2] *A. F. Mozhaysky Military Space Academy, 197198, St. Petersburg, Russia*

An algorithm for the generation of ternary Gordon—Mills—Welch (GMW) sequences and for determining the initial states of the shift registers, incorporated into the generation device, is developed. Ternary GMW-sequences, as well as binary, may be formed on the base of set of shift registers, which linear feedback are determined by coefficients of indivisible polynomials being the factors of testing polynomials of GMW-sequences. The main problem in the construction of devices generating ternary GMW-sequences based on shift registers is absence in literature of algorithms of definition of their initial states. In accordance with the proposed algorithm the initial state of shift registers is determined by the decimation of the symbols of the base M-sequence, on which GMW-sequence is formed. Decimation index depends on the ratio of the degrees of the roots of polynomials-factors and roots of polynomial of the base M-sequence.

Keywords: ternary sequences of composite period, finite fields, indivisible and primitive polynomials, shift register with linear feedback

Data on authors

Viktor G. Starodubtsev — PhD, Associate Professor; A. F. Mozhaysky Military Space Academy, Department of Technologies and Means of Complex Processing and Transfer of Information in Automated Control Systems; Senior Lecturer; ITMO University, Department of Wireless Communications, E-mail: vgstarod@mail.ru

Alina E. Chernyavskikh — Student; A. F. Mozhaysky Military Space Academy, Department of Technologies and Means of Complex Processing and Transfer of Information in Automated Control Systems; E-mail: vgstarod@mail.ru

For citation: *Starodubtsev V. G., Chernyavskikh A. E. G*eneration of ternary Gordon — Mills — Welch sequences on the base of shift registers // Izv. vuzov. Priborostroenie. 2016. Vol. 59, N 3. P. 202—210 (in Russian).

DOI: 10.17586/0021-3454-2016-59-3-202-210