УДК 519.725
DOI: 10.17586/0021-3454-2015-58-6-451-457

ФОРМИРОВАНИЕ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОРДОНА—МИЛЛСА—ВЕЛЧА НА ОСНОВЕ РЕГИСТРОВ СДВИГА

В. Г. СТАРОДУБЦЕВ

Университет ИТМО, 197101, Санкт-Петербург, Россия
E-mail: vgstarod@mail.ru

Разработан алгоритм определения начальных состояний регистров сдвига, входящих в устройство формирования последовательностей Гордона—Миллса—Велча (ГМВ). Известно, что предпочтительность применения в системах связи ГМВ-последовательностей определяется их более высокой структурной скрытностью по сравнению с М-последовательностями, однако основной проблемой при построении устройств формирования ГМВ-последовательностей на основе регистров сдвига является отсутствие в литературе алгоритмов определения их начальных состояний. Показано, что согласно предложенному алгоритму начальные состояния регистров сдвига определяются соотношением степеней корней полиномов $h_{ci}(x)$ и полинома исходной М-последовательности, на основе которой формируется ГМВ-последовательность, и на практике вычисляются путем децимации символов исходной М-последовательности по индексу децимации, зависящему от соотношения степеней корней полиномов.

Ключевые слова: *последовательность с составным периодом, конечное поле, неприводимый и примитивный полином, регистр сдвига с линейными обратными связями.*

Последовательности Гордона—Миллса—Велча (ГМВ) применяются в современных системах связи благодаря более высокой структурной скрытности по сравнению с М-последовательностями, которые также обладают одноуровневой периодической автокорреляционной функцией [1—5].

Настоящая статья продолжает цикл публикаций, посвященных разработке алгоритмов формирования ГМВ-последовательностей и анализу корреляционных и структурных свойств этих последовательностей [6, 7].

В статье [6] разработан алгоритм формирования ГМВ-последовательностей, основанный на матричном представлении последовательностей с составным периодом и использовании свойств проверочных полиномов, определяемых над конечными полями Галуа.

В работе [7] представлен алгоритм формирования проверочных полиномов ГМВ-последовательностей, основанный на использовании структурных свойств конечных полей с двойным расширением. Также получены полные перечни проверочных полиномов для двоичных ГМВ-последовательностей с периодами N=63, 255 и для троичных ГМВ-последовательностей с N=80.

Известны различные подходы к разработке устройств формирования ГМВ-последовательностей. Отличительной особенностью большинства подходов является то, что в состав реализуемых на их основе устройств формирования входят нелинейные элементы. Например, в работе [8] представлен способ, основанный на представлении ГМВ-последовательностей с помощью функции следа.

Использование проверочных полиномов ГМВ-последовательностей позволяет реализовать устройства их формирования с помощью регистров сдвига с линейными обратными связями (РС ЛОС).

Структура проверочного полинома ГМВ-последовательности $h_{\text{ГМВ}}(x)$, представляющего собой для конечных полей $\text{GF}(p^S)$ (p — характеристика поля, S — натуральное число) произ-

ведение двух или более неприводимых полиномов $h_{ci}(x)$ степени S, определяет возможность построения устройства формирования в виде совокупности нескольких РС ЛОС.

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

Основной задачей при построении устройств формирования ГМВ-последовательностей является определение начальных состояний регистров сдвига.

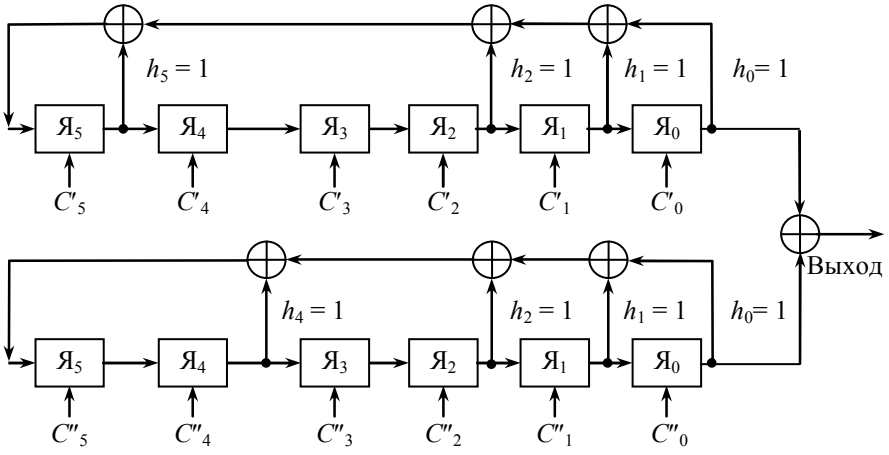
На основе значений символов сегмента формируемой ГМВ-последовательности длиной kS символов (k — число регистров сдвига) и коэффициентов полиномов $h_{ci}(x)$ путем решения системы линейных уравнений могут быть определены начальные состояния РС ЛОС. Недостатком такого подхода является необходимость предварительного формирования сегмента последовательности длиной kS символов.

В литературе нет сведений о методиках или алгоритмах, позволяющих однозначно определять начальные состояния всех РС ЛОС, входящих в устройство, при формировании ГМВ-последовательностей в условиях отсутствия информации о требуемом сегменте длиной kS символов.

Целью настоящей статьи является разработка алгоритма определения начальных состояний регистров сдвига с линейными обратными связями, входящих в устройство формирования, не требующего предварительного построения сегмента ГМВ-последовательности.

Алгоритм основан на использовании следующего структурного свойства проверочных полиномов: корни полиномов $h_{ci}(x)$ — сомножителей проверочного полинома $h_{ГМВ}(x)$ — являются определенными степенями корней проверочного полинома $h_{МП}(x)$ исходной М-последовательности, на основе которой формируется ГМВ-последовательность [5, 7].

Перед разработкой алгоритма определим начальные состояния регистров сдвига на примере устройства формирования ГМВ-последовательности (см. рисунок), решив систему линейных уравнений при известном сегменте формируемой ГМВ-последовательности. Проверочным полиномом исходной М-последовательности является $h_{МП}(x) = x^6 + x + 1$, его корни — примитивные элементы поля GF(2^6): α, α^2, α^4, α^8, α^{16}, α^{32}.



Устройство формирования представляет собой два РС ЛОС, число ячеек в каждом из которых равно шести, т.е. степеням полиномов $h_{ci}(x)$, а сумматоры по mod 2 расставляются в соответствии с коэффициентами этих полиномов.

Для рассматриваемого примера сомножителями проверочного полинома $h_{ГМВ}(x)$ являются [5, 7]:

$$h_{\text{ГМВ}}(x) = x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^2 + 1 =$$
$$= h_{c1}(x)\, h_{c2}(x) = (x^6 + x^4 + x^2 + x + 1)\,(x^6 + x^5 + x^2 + x + 1). \quad (1)$$

Наиболее интересным (без потери общности) представляется случай, когда начальные состояния двух регистров одинаковы. Для получения таких начальных состояний выберем сегмент ГМВ-последовательности длиной 12 символов ([6], выражение (5)), содержащий S нулей:

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

С учетом коэффициентов полиномов $h_{c1}(x)$ и $h_{c2}(x)$, а также (2) можно записать следующую систему уравнений для символов $C_i' = C_i'' = C^*_i$ ($i = \overline{0, 5}$):

$$\left.\begin{array}{l} C^*_5 + C^*_4 = 0, \\ C^*_0 + C^*_1 + C^*_2 = 1, \\ C^*_0 + C^*_3 = 0, \\ C^*_2 + C^*_3 + C^*_4 = 0, \\ C^*_1 = 0, \\ C^*_3 + C^*_4 = 1. \end{array}\right\} \quad (3)$$

Эта система линейных уравнений имеет единственное решение

$$C^*_0 = 0,\ C^*_1 = 0,\ C^*_2 = 1,\ C^*_3 = 0,\ C^*_4 = 1,\ C^*_5 = 1, \quad (4)$$

которое определяет начальное состояние первого и второго регистров сдвига при формировании ГМВ-последовательности с периодом $N = 63$ и будет использовано при разработке алгоритма определения начальных состояний.

Для поля GF(2^6) корни полинома $h_{c1}(x)$: α^3, α^6, α^{12}, α^{24}, α^{48}, α^{33} — являются третьими степенями корней полинома $h_{\text{МП}}(x)$, а корни полинома $h_{c2}(x)$: α^5, α^{10}, α^{20}, α^{40}, α^{17}, α^{34} — пятыми степенями его корней [5, 7].

На основе проверочного полинома $h_{\text{МП}}(x) = x^6 + x + 1$ формируем М-последовательность с периодом $N = 63$ для произвольного начального состояния, например, 101111 (табл. 1, строки d_i).

Таблица 1

i	0	1	2	3	4	5	6	7	8	**9**	10	11	12	13	14	15	16	17	18	19	20
d_i	1	0	1	1	1	1	1	1	0	**0**	0	0	0	1	0	0	0	0	1	1	0
Сумма	4	2	4	4	4	2	4	2	2	**0**	2	2	2	2	2	2	4	2	4	2	2
i	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
d_i	0	0	1	0	1	0	0	1	1	1	1	0	1	0	0	0	1	1	1	0	0
Сумма	2	4	4	4	2	2	4	4	2	6	2	4	2	2	4	4	4	4	4	2	2
i	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62
d_i	1	0	0	1	0	1	1	0	1	1	1	0	1	1	0	0	1	1	0	1	0
Сумма	2	2	4	4	2	4	4	2	4	6	4	2	4	4	2	2	4	2	4	4	4

Для упрощения записи в таблицах введены следующие обозначения:

— i — номер символа последовательности с полиномом $h_{\text{МП}}(x)$;

— d_i — значение символа последовательности с полиномом $h_{\text{МП}}(x)$;

— сумма — арифметическая сумма значений 1, 2, 4, 8, 16 и 32-го символов для каждого символа последовательности, считаемого первым.

Для дальнейшей разработки алгоритма необходимо определить начало М-последовательности в соответствии с выражением d_i=$\mathrm{tr}_{6,1}\,\alpha^i$, $i = 0, 1, \ldots, 62$ [5, 6, 8]: d_0, d_1, d_2 и т.д. Одним из способов решения этой задачи является использование свойства примитивных полиномов, согласно которому 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 $h_{\text{МП}}(x)$, а значение функции следа $\mathrm{tr}_{s,1}\alpha^{-1}$ — значению коэффициента при первой степени переменной x.

Для полинома $h_{\text{МП}}(x) = x^6 + x + 1$ функции следа $\mathrm{tr}_{6,1}\alpha^1 = \alpha^1 + \alpha^2 + \alpha^4 + \alpha^8 + \alpha^{16} + \alpha^{32} = 0$, $\mathrm{tr}_{6,1}\alpha^{-1} = 1$. Тогда символу d_1 М-последовательности в табл. 1 соответствует позиция, для которой сумма 1, 2, 4, 8, 16 и 32-го символов (каждый символ считается первым) равна нулю. Такая позиция единственная, и ей соответствует девятый символ (в табл. 1 выделен подчеркиванием), т.е. начало М-последовательности $d_0 = 0$, $d_1 = 0$ и т.д. Результаты вычислений приведены в табл. 1.

Для удобства дальнейших вычислений запишем М-последовательность, начиная с символов d_0, d_1 и т.д. (см. табл. 2, строки $d_{i_{\text{мп}}}$).

Таблица 2

$i_{\text{мп}}$	d_0	d_1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$d_{i_{\text{мп}}}$	0	0	0	0	0	1	0	0	0	0	1	1	0	0	0	1	0	1	0	0	1
$i_{\text{с1}}$	0	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60
$d_{i_{c1}}$	0	0	0	0	0	1	0	1	0	0	1	0	0	1	1	0	0	1	0	1	1
$i_{\text{с2}}$	0	5	10	15	20	25	30	35	40	45	50	55	60	2	7	12	17	22	27	32	37
$d_{i_{c2}}$	0	1	1	1	1	1	1	0	1	0	1	1	1	0	0	0	1	1	0	0	1
$i_{\text{мп}}$	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
$d_{i_{\text{мп}}}$	1	1	1	0	1	0	0	0	1	1	1	0	0	1	0	0	1	0	1	1	0
$i_{\text{с1}}$	0	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60
$d_{i_{c1}}$	0	0	0	0	0	1	0	1	0	0	1	0	0	1	1	0	0	1	0	1	1
$i_{\text{с2}}$	42	47	52	57	62	4	9	14	19	24	29	34	39	44	49	54	59	1	6	11	16
$d_{i_{c2}}$	1	1	0	1	1	0	0	0	0	0	1	1	1	1	0	0	1	0	0	1	0
$i_{\text{мп}}$	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62
$d_{i_{\text{мп}}}$	1	1	1	0	1	1	0	0	1	1	0	1	0	1	0	1	1	1	1	1	1
$i_{\text{с1}}$	0	3	6	9	12	15	18	21	24	27	30	33	36	39	42	**45**	**48**	**51**	**54**	**57**	**60**
$d_{i_{c1}}$	0	0	0	0	0	1	0	1	0	0	1	0	0	1	1	**0**	**0**	**1**	**0**	**1**	**1**
$i_{\text{с2}}$	21	26	31	36	41	46	51	56	61	3	8	13	18	23	28	**33**	**38**	**43**	**48**	**53**	**58**
$d_{i_{c2}}$	1	0	1	0	0	1	1	0	1	0	0	0	0	1	0	**0**	**0**	**1**	**0**	**1**	**1**

Затем формируем псевдослучайную последовательность с проверочным полиномом $h_{\text{с1}}(x) = x^6 + x^4 + x^2 + x + 1$, корни которого являются третьими степенями корней полинома $h_{\text{МП}}(x)$ и имеют период $\varepsilon = 21$. Полином $h_{\text{с1}}(x)$ является неприводимым, но не примитивным. Соответственно период псевдослучайной последовательности $N = 21$, и она представляет собой последовательность функций следа для элементов $\alpha^0, \alpha^3, \alpha^6, \alpha^9, \ldots, \alpha^{54}, \alpha^{57}, \alpha^{60}$, т.е. набор символов исходной М-последовательности $d_0, d_3, d_6, d_9, \ldots, d_{54}, d_{57}, d_{60}$. В табл. 2 (строки $d_{i_{c1}}$) записаны три периода последовательности. Процесс формирования этой последовательности можно интерпретировать как децимацию исходной М-последовательности по индексу децимации $I_{d_1} = 3$. При этом начала обеих последовательностей связаны между собой.

Так же формируем М-последовательность с проверочным полиномом $h_{\text{с2}}(x) = x^6 + x^5 + x^2 + x + 1$, корни которого являются пятыми степенями корней полинома $h_{\text{МП}}(x)$ и имеют период $\varepsilon = 63$. Полином $h_{\text{с2}}(x)$ является примитивным, поэтому период данной М-последовательности $N = 63$. Она представляет собой последовательность функций следа для элементов $\alpha^0, \alpha^5, \alpha^{10}, \alpha^{15}, \ldots, \alpha^{48}, \alpha^{53}, \alpha^{58}$ и приведена в табл. 2 (строки $d_{i_{c2}}$). Процесс формирования

этой последовательности также можно интерпретировать как децимацию исходной М-последовательности, но по индексу децимации $I_{d_2} = 5$.

Анализ показал, что символы псевдослучайной последовательности с проверочным полиномом $h_{c1}(x)$ с номерами 45, 48, 51, 54, 57, 60 (выделены подчеркиванием) и символы М-последовательности с проверочным полиномом $h_{c2}(x)$ с номерами 33, 38, 43, 48, 53, 58 совпадают и равны значениям в выражении (4). Данные значения определяют совпадающие начальные состояния двух регистров сдвига при формировании ГМВ-последовательности.

Таким образом, можно сделать важный вывод, 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 исходного полинома для М-последовательности.

На практике начальные состояния регистров сдвига определяются децимацией символов исходной М-последовательности по соответствующему индексу децимации, начиная с символа d_0. Для двоичных ГМВ-последовательностей с периодом $N = 63$ $I_{d_1} = 3$, $I_{d_2} = 5$.

Начальное состояние РС ЛОС с полиномом $h_{c1}(x)$ определяется символами d_0, d_3, d_6, d_9, d_{12}, d_{15}, а с полиномом $h_{c2}(x)$ — символами d_0, d_5, d_{10}, d_{15}, d_{20}, d_{25} исходной М-последовательности.

Для двоичных ГМВ-последовательностей с периодом $N = 255$ устройство формирования состоит из четырех регистров сдвига, определяемых полиномами восьмой степени [6]. При этом индексы децимации равны $I_{d_1} = 7$, $I_{d_2} = 11$, $I_{d_3} = 13$, $I_{d_4} = 37$.

Начальное состояние регистров сдвига определяется следующими символами исходной М-последовательности:

— для $h_{c1}(x)$ — d_0, d_7, d_{14}, d_{21}, d_{28}, d_{35};

— для $h_{c2}(x)$ — d_0, d_{11}, d_{22}, d_{33}, d_{44}, d_{55};

— для $h_{c3}(x)$ — d_0, d_{13}, d_{26}, d_{39}, d_{52}, d_{65};

— для $h_{c4}(x)$ — d_0, d_{37}, d_{74}, d_{111}, d_{148}, d_{185}.

Представим алгоритм определения начальных состояний регистров сдвига для формирования ГМВ-последовательностей с периодом N.

1. Задание проверочного полинома исходной М-последовательности с периодом N.

2. Формирование М-последовательности и определение символов d_0, d_1, d_2 и т. д.

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

4. Определение начальных состояний регистров сдвига из символов исходной М-последовательности для $N = 63$ — $I_{d_1} = 3$, $I_{d_2} = 5$, для $N = 255$ — $I_{d_1} = 7$, $I_{d_2} = 11$, $I_{d_3} = 13$, $I_{d_4} = 37$.

5. Формирование последовательностей с проверочными полиномами-сомножителями $h_{ci}(x)$ для полученных начальных состояний.

6. Формирование искомой ГМВ-последовательности путем посимвольного сложения последовательностей на выходах регистров сдвига.

Правильность формирования ГМВ-последовательности можно проверить следующим образом. Выбирается произвольный сегмент полученной ГМВ-последовательности, длина которого равна степени проверочного полинома $h_{\text{ГМВ}}(x)$. С учетом коэффициентов данного полинома формируются следующие символы последовательности, которые при благоприятном исходе должны совпадать с символами, полученными путем сложения на выходах регистров сдвига.

Таким образом, в статье разработан алгоритм определения начальных состояний РС ЛОС и формирования двоичных ГМВ-последовательностей, проверочные полиномы которых представляют собой произведение нескольких неприводимых полиномов. В качестве исходных данных выступает только примитивный полином степени S, задающий 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 этих полиномов и полинома исходной М-последовательности.

На практике начальные состояния регистров сдвига определяются децимацией символов исходной М-последовательности по индексу децимации, зависящему от соотношения степеней корней полиномов.

СПИСОК ЛИТЕРАТУРЫ

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

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

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

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

5. *Стародубцев В. Г.* Последовательности Гордона—Миллса—Велча. Свойства и алгоритмы формирования. Saarbrucken: LAP LAMBERT Academic Publishing, 2014. 95 с.

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

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

8. *Тараненко П. Г.* Псевдослучайные и кодовые последовательности: методы синтеза и анализа. СПб: ВИКУ им. А. Ф. Можайского, 1999. 112 с.

Сведения об авторе

Виктор Геннадьевич Стародубцев — канд. техн. наук, доцент; Университет ИТМО, кафедра беспроводных телекоммуникаций; ООО „Мультисервисные сети и Телекоммуникации“; начальник отдела; E-mail: vgstarod@mail.ru

Рекомендована кафедрой беспроводных телекоммуникаций

Поступила в редакцию 21.11.14 г.

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

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

V. G. Starodubtsev

ITMO University, 197101, Saint Petersburg, Russia
E-mail: vgstarod@mail.ru

An algorithm for determining the initial states of the shift registers with linear feedback, incorporated into the device generating Gordon—Mills—Welch sequences, is developed.

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

Data on author

Victor G. Starodubtsev — PhD, Associate Professor; ITMO University, Department of Wireless Telecommunications; Multiservice Networks and Telecommunication, Ltd.; Head of the Department;
E-mail: vgstarod@mail.ru

Reference for citation: *Starodubtsev V. G.* Generation of Gordon-Mills-Welch sequences on the base of shift registers // Izvestiya Vysshikh Uchebnykh Zavedeniy. Priborostroenie. 2015. Vol. 58, N 6. P. 451—457 (in Russian).

DOI: 10.17586/0021-3454-2015-58-6-451-457