ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ

УДК 519.725

В. Г. СТАРОДУБЦЕВ

АЛГОРИТМ ФОРМИРОВАНИЯ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОРДОНА — МИЛЛСА — ВЕЛЧА

Предлагается алгоритм формирования последовательностей Гордона — Миллса — Велча, основанный на матричном представлении М-последовательностей с составным периодом, образуемых над конечными полями с двойным расширением.

Ключевые слова: *последовательности с составным периодом, корреляционная функция, конечные поля, неприводимые и примитивные полиномы.*

Одно из направлений развития современных систем связи и навигации — применение сигналов с расширенным спектром. Для реализации процедуры расширения спектра сигнала используются псевдослучайные последовательности (ПСП), в частности последовательности Гордона — Миллса — Велча (ГМВ). По корреляционным свойствам ГМВ-последовательности (ГМВП) аналогичны М-последовательностям [1—3], но обладают более высокой эквивалентной линейной сложностью, определяющей их структурную скрытность [2].

ГМВ-последовательности формируются над конечными полями с двойным расширением вида $GF[(p^m)^n]$, вследствие чего период данных последовательностей является составным числом, т.е. $N = p^{mn} - 1$, где p — характеристика поля, m, n — натуральные числа. В настоящее время широкое применение получили двоичные ГМВП, формируемые над полями с двойным расширением вида $GF[(2^m)^n]$. Символы d_i данных последовательностей с периодом $N = 2^{mn}-1$ определяются в соответствии с выражением [4—6]

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

где $\mathrm{tr}_{mn,\,m}(\cdot)$ — след элемента поля с двойным расширением $GF[(2^m)^n]$, отображаемый в расширенном поле $GF(2^m)$; $\mathrm{tr}_{m1}(\cdot)$ — след элемента расширенного поля $GF(2^m)$, отображаемый в простом поле $GF(2)$; $\alpha \in GF[(2^m)^n]$ — примитивный элемент поля с двойным расширением; параметр r является числом, взаимно простым с порядком мультипликативной группы расширенного поля $GF(2^m)$, равным $2^m - 1$.

При $r = 1$ согласно свойству функции следа выражение (1) описывает М-последовательность

$$d_i = \mathrm{tr}_{m1}[\mathrm{tr}_{mn,m}(\alpha^i)] = \mathrm{tr}_{mn,1}(\alpha^i). \qquad (2)$$

При формировании ГМВП на основе выражения (1) необходимо построить расширенное поле $GF(2^m)$ и поле с двойным расширением $GF[(2^m)^n]$, а также определить следы всех элементов в расширенном и простом полях, что обусловливает значительную вычислительную сложность данной процедуры.

Цель настоящей статьи — разработка алгоритма формирования ГМВП, основанного на матричном представлении последовательностей с составным периодом и использовании структурных свойств проверочных полиномов.

Формирование ГМВП осуществляется на основе М-последовательности с аналогичным периодом, построение которой может быть реализовано с помощью проверочного полинома, определяемого из таблиц неприводимых полиномов [7, 8].

Для наглядности рассмотрим сначала процедуру формирования ГМВП на конкретном примере. Пусть требуется сформировать ГМВП с периодом $N = 63$. Сначала формируем М-последовательность (МП) с таким периодом. В качестве проверочного полинома выберем произвольный примитивный полином 6-й степени, например, $h_{\text{МП}}(x) = x^6 + x + 1$. Для начального состояния 000001 линейного регистра сдвига с обратными связями длиной $L = 6$ элементы искомой М-последовательности записываются построчно в виде матрицы размерностью $[J \times S] = [7 \times 9]$:

$$\mathbf{F}_{\text{МП}} = \begin{vmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{vmatrix}. \qquad (3)$$

Номера строк в матрице изменяются от нуля до $(J - 1)$, а номера столбцов — от нуля до $(S - 1)$. Заметим, что столбцы матрицы, за исключением нулевого, состоящего из одних нулей, представляют собой $S - 1 = 8$ некоторых сдвигов М-последовательности с периодом $J = 7$. Данная последовательность получила название „характеристической“, а последовательность, состоящая из нулей, называется нулевой [9].

Таким образом, можно сделать вывод, что М-последовательность с составным периодом формируется на основе М-последовательности с более коротким периодом. Нулевая последовательность необходима для выполнения условия сбалансированности М-последовательности.

Проверочным полиномом для полученной в рассматриваемом примере характеристической последовательности № 1 (ХП1) с периодом $J = 7$ является полином $h_{\text{ХП1}}(x) = x^3 + x^2 + 1$. Сформируем все сдвиги этой последовательности, произвольно выбрав в качестве нулевого сдвига третий столбец матрицы $\mathbf{F}_{\text{МП}}$ вида (3) — 0011101 (см. табл. 1).

Таблица 1

Номер сдвига	Сдвиг М-последовательности	Номер сдвига	Сдвиг М-последовательности
0	0011101	4	1101001
1	1001110	5	1110100
2	0100111	6	0111010
3	1010011		

В соответствии с табл. 1 определяем номера сдвигов характеристической последовательности для всех столбцов матрицы (3). Тогда М-последовательность с периодом $N = 63$, записанную в виде матрицы $\mathbf{F}_{\text{МП}}$, можно определить как последовательность элементов, представляющих собой номера сдвигов характеристической последовательности с периодом $J = 7$ с одним прочерком для обозначения нулевой последовательности. В результате получим правило формирования сдвигов в виде вектора из $S = 9$ компонент:

$$\mathbf{I}_{\text{МП}} = \{-, 2, 6, 0, 0, 3, 2, 0, 2\}. \qquad (4)$$

На основе полученного правила формирования можно синтезировать ГМВ-последовательность. Для этого в качестве характеристической последовательности № 2 необходимо выбрать другую М-последовательность с периодом $J = 7$, для которого существует всего одна такая последовательность с проверочным полиномом $h_{\text{ХП2}}(x) = x^3 + x + 1$. Сформируем все сдвиги данной характеристической последовательности для нулевого сдвига 0010111 (см. табл. 2).

Таблица 2

Номер сдвига	Сдвиг М-последовательности	Номер сдвига	Сдвиг М-последовательности
0	0010111	4	0111001
1	1001011	5	1011100
2	1100101	6	0101110
3	1110010		

ГМВ-последовательность можно представить в виде матрицы $\mathbf{F}_{\text{ГМВ}}$, аналогичной матрице (3), путем подстановки номеров сдвигов характеристической последовательности из табл. 2 в соответствии с правилом (4) (для удобства формирования последовательности данное правило повторено):

$$\mathbf{I}_{\text{МП}} = \{-,\ 2,\ 6,\ 0,\ 0,\ 3,\ 2,\ 0,\ 2\},$$

$$\mathbf{F}_{\text{ГМВ}} = \begin{vmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{vmatrix}. \qquad (5)$$

Возможность формирования ГМВП путем замены характеристической последовательности в правиле $\mathbf{I}_{\text{МП}}$ можно пояснить следующим образом.

В выражении (1) значение „внутренней“ функции следа $\text{tr}_{mn,m}(\alpha) = \text{tr}_{6,3}(\alpha)$ элемента α поля с двойным расширением $\text{GF}[(2^3)^2]$ является элементом расширенного поля $\text{GF}(2^3)$. Если r принимает значение больше единицы, то возведение следа в степень $(\text{tr}_{6,3}(\alpha)^r)$ означает децимацию элементов поля $\text{GF}(2^3)$ по индексу r. При этом в каждом столбце матрицы (3) также происходит децимация символов характеристической последовательности по индексу r. В случае когда двоичное представление числа r содержит одну единицу (числа 2, 4, 8 и т.д.), в результате децимации формируется циклический сдвиг М-последовательности, совпадающей с характеристической последовательностью № 1. В случае когда двоичное представление числа r содержит не менее двух единиц (числа 3, 5, 6), формируется другая „короткая“ М-последовательность, совпадающая с характеристической последовательностью № 2. Таким образом, возведение следа в степень r в выражении (1) эквивалентно замене в матричном представлении (3) характеристической последовательности № 1 на характеристическую последовательность № 2. В результате вместо М-последовательности с периодом $N = 63$ формируется ГМВ-последовательность.

В качестве примера реализации разработанного алгоритма рассмотрим процедуру формирования троичной ГМВ-последовательности с периодом $N = 80$.

1. По таблицам неприводимых полиномов [7, 10] над полем $\text{GF}[(3^2)^2]$ с характеристикой $p = 3$ выбираем примитивный полином $h_{\text{МП}}(x) = x^4 + 2x^3 + 2$ степени $k = mn = 4$, определяемой из равенства $N = 80 = 3^k - 1$.

2. На основе полинома $h_{\text{МП}}(x) = x^4 + 2x^3 + 2$ формируем троичную М-последовательность с периодом $N = 80$. Формирование выполняем с помощью рекуррентного выражения для символов М-последовательности вида $C_{4+i} = C_{3+i} + C_{0+i}$, $i = 0, 1, \ldots, 75$, которое получаем на основе полинома $h_{\text{МП}}(x)$ [11]. Сформированную троичную М-последовательность записываем в виде матрицы $\mathbf{F}_{\text{МП}}$ размерностью $[J \times S] = [8 \times 10]$ последовательно по строкам:

$$\mathbf{F}_{\text{МП}} = \begin{vmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 0 & 1 \\ 2 & 1 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 2 \\ 2 & 1 & 1 & 0 & 2 & 0 & 1 & 1 & 0 & 0 \\ 1 & 2 & 2 & 2 & 0 & 2 & 1 & 0 & 0 & 2 \\ 0 & 0 & 0 & 2 & 2 & 2 & 2 & 1 & 0 & 2 \\ 1 & 2 & 2 & 1 & 2 & 1 & 0 & 1 & 0 & 1 \\ 1 & 2 & 2 & 0 & 1 & 0 & 2 & 2 & 0 & 0 \\ 2 & 1 & 1 & 1 & 0 & 1 & 2 & 0 & 0 & 1 \end{vmatrix}. \qquad (6)$$

3. Формируем циклические сдвиги характеристической последовательности № 1, проверочным полиномом для которой является $h_{\text{ХП1}}(x) = x^2 + 2x + 2$ (см. табл. 3).

Таблица 3

Номер сдвига	Сдвиг М-последовательности	Номер сдвига	Сдвиг М-последовательности
0	02210112	4	01120221
1	20221011	5	10112022
2	12022101	6	21011202
3	11202210	7	22101120

4. Определяем номера сдвигов характеристической последовательности № 1 для всех столбцов матрицы $\mathbf{F}_{\text{МП}}$. М-последовательность с периодом $N = 80$ определяется в виде последовательности элементов, представляющих собой номера сдвигов характеристической последовательности с периодом $J = 8$ с одним прочерком для обозначения нулевой последовательности. В результате получим правило формирования в виде вектора из $S = 10$ компонент:

$$\mathbf{I}_{\text{МП}} = \{0, 4, 4, 2, 3, 2, 5, 7, –, 2\}. \qquad (7)$$

5. По таблицам неприводимых полиномов выбираем примитивный полином $h_{\text{ХП2}}(x) = x^2 + x + 2$ степени $m = 2$, отличный от полинома $h_{\text{ХП1}}(x)$. Заметим, что существует всего два примитивных полинома степени 2 над полем $\text{GF}(3^2)$. Формируем все циклические сдвиги этой характеристической последовательности № 2 для произвольно выбранного нулевого сдвига, например 02110122 (см. табл. 4).

Таблица 4

Номер сдвига	Сдвиг М-последовательности	Номер сдвига	Сдвиг М-последовательности
0	02110122	4	01220211
1	20211012	5	10122021
2	22021101	6	11012202
3	12202110	7	21101220

6. В соответствии с правилом $\mathbf{I}_{\text{МП}}$ вида (7) столбцы матрицы $\mathbf{F}_{\text{МП}}$ формируем на основе требуемых циклических сдвигов характеристической последовательности № 2. В результате получаем матрицу $\mathbf{F}_{\text{ГМВ}}$, в которой искомая ГМВ-последовательность записана по строкам:

$$\mathbf{F}_{\text{ГМВ}} = \begin{vmatrix} 0 & 0 & 0 & 2 & 1 & 2 & 1 & 2 & 0 & 2 \\ 2 & 1 & 1 & 2 & 2 & 2 & 0 & 1 & 0 & 2 \\ 1 & 2 & 2 & 0 & 2 & 0 & 1 & 1 & 0 & 0 \\ 1 & 2 & 2 & 2 & 0 & 2 & 2 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 2 & 1 & 2 & 1 & 0 & 1 \\ 1 & 2 & 2 & 1 & 1 & 1 & 0 & 2 & 0 & 1 \\ 2 & 1 & 1 & 0 & 1 & 0 & 2 & 2 & 0 & 0 \\ 2 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{vmatrix}.$$

И двоичные, и недвоичные ГМВ-последовательности, алгоритм формирования которых представлен в настоящей статье, могут быть использованы в качестве синхросигналов в системах мобильной связи стандарта GSM и широкополосных сигналов в системах мобильной связи стандарта CDMA. Данные последовательности могут также найти применение в качестве псевдослучайных последовательностей для расширения спектра информационного сигнала в помехозащищенных системах спутниковой связи и для формирования широкополосных сигналов различного функционального типа в спутниковых навигационных системах. При этом структурная скрытность ГМВ-последовательностей в два раза превышает этот показатель для М-последовательностей.

Разработанный алгоритм позволяет существенно уменьшить вычислительную сложность процедуры формирования ГМВП (на 3—6 дБ для последовательностей с периодом N=63 – 255) благодаря отсутствию необходимости производить вычисления в конечных расширенных полях.

СПИСОК ЛИТЕРАТУРЫ

1. *Варакин Л. Е.* Системы связи с шумоподобными сигналами. М.: Радио и связь, 1985. 384 с.
2. *Ипатов В. П.* Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992. 152 с.
3. *Свердлик М. Б.* Оптимальные дискретные сигналы. М.: Сов. радио, 1975. 200 с.
4. *Блейхут Р. Э.* Быстрые алгоритмы цифровой обработки сигналов: Пер. с англ. М.: Мир, 1989. 488 с.
5. *Прокис Дж.* Цифровая связь / Пер. с англ.; Под ред. *Д. Д. Кловского.* М.: Радио и связь, 2000. 788 с.
6. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение: Пер. с англ. М.: Изд. дом „Вильямс“, 2003. 1104 с.
7. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки / Пер. с англ.; Под ред. *Р. Л. Добрушина* и *С. И. Самойленко* М.: Мир, 1976. 596 с.
8. *Стародубцев В. Г., Павлов О. А.* Помехоустойчивые коды в телекоммуникационных и информационных системах. Вып. 1. Конечные поля Галуа: элементы теории и практики: Учеб. пособие. СПб: ВКА им. А. Ф. Можайского, 2003. 252 с.
9. *Стародубцев В. Г.* Алгоритм формирования и свойства дискретных редецимированных последовательностей для помехозащищенных систем связи // Сб. статей науч.-техн. конф. „Радио- и волоконно-оптическая связь, навигация, локация“. Воронеж, 1997. С. 238—246.
10. *Кларк Дж., Кейн Дж.* Кодирование с исправлением ошибок в системах цифровой связи: Пер. с англ. М.: Радио и связь, 1987. 392 с.
11. *Блейхут Р. Э.* Теория и практика кодов, контролирующих ошибки: Пер. с англ. М.: Мир, 1986. 576 с.

Сведения об авторе

Виктор Геннадьевич Стародубцев — канд. техн. наук; ООО „Мультисервисные сети и телекоммуникации“, Санкт-Петербург; начальник отдела; E-mail: vgstarod@mail.ru

Рекомендована кафедрой
сетей и систем связи космических комплексов
ВКА им. А. Ф. Можайского

Поступила в редакцию
18.01.12 г.