

ФОРМИРОВАНИЕ И ОБРАБОТКА ГМВ-ПОДОБНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ДВОЙСТВЕННОГО БАЗИСА

С.С. Владимир^{1*}, О.С. Когновицкий¹, В.Г. Стародубцев^{2,3}

¹Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

²Военно-космическая академия им. А.Ф. Можайского, Санкт-Петербург, 197198, Российская Федерация

³Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург, 197101, Российская Федерация

*Адрес для переписки: vladimirov.opds@gmail.com

Информация о статье

УДК 519.725

Статья поступила в редакцию 28.10.2019

Ссылка для цитирования: Владимир С.С., Когновицкий О.С., Стародубцев В.Г. Формирование и обработка ГМВ-подобных последовательностей на основе двойственного базиса // Труды учебных заведений связи. 2019. Т. 5. № 4. С. 16–27. DOI:10.31854/1813-324X-2019-5-4-16-27

Аннотация: Представлены алгоритмы обработки и определения с использованием двойственного базиса начальных состояний регистров сдвига, формирующих последовательности, подобные последовательностям Гордона – Миллса – Велча (ГМВ), которые характеризуются большим их количеством и более высокой структурной скрытностью, чем широко используемые М-последовательности. Показано, что предложенные алгоритмы, в отличие от известных, позволяют определять произвольные начальные состояния регистров сдвига и производить кодирование полезной информации, что расширяет возможности применения ГМВ-подобных последовательностей для решения различных задач при передаче цифровой информации в системах связи в условиях радиоэлектронного противодействия.

Ключевые слова: последовательности Гордона – Миллса – Велча, эквивалентная линейная сложность, конечные поля, примитивные и неприводимые многочлены, функция след, децимация, двойственный базис, регистр сдвига с линейной обратной связью.

В современных помехозащищенных системах передачи цифровой информации в условиях радиоэлектронного противодействия применяются широкополосные сигналы с прямым расширением спектра, формируемые на основе псевдослучайных последовательностей (ПСП), таких как М-последовательности (МП), последовательности Голда, большое и малое семейства последовательностей Касами [1–3]. Среди множества псевдослучайных последовательностей в настоящее время повышенное внимание уделяется и последовательностям Гордона – Миллса – Велча (ГМВ), обладающим хорошими корреляционными свойствами, не уступающими М-последовательностям, но обеспечивающими более высокую структурную скрытность, которая характеризуется эквивалентной линейной сложностью (ЭЛС) [4–6].

Исследованиям свойств и алгоритмам генерации ГМВ-последовательностей посвящено большое количество работ как в нашей стране, так и за рубежом. Можно назвать работы С.В. Голомба [4–5], Д.С. Но [6–7], Е.И. Кренгеля, К.А. Мешковского [8–9]

и ряда других авторов. Данные труды были направлены, главным образом, на поиск ГМВ-последовательностей с определенными свойствами, анализ алгоритмов формирования и оценки их корреляционных свойств.

Формирование двоичных ГМВ-последовательностей выполняется над конечными полями с двойным расширением $GF[(2^n)^k] = GF(2^m)$ ($m = n \cdot k$). Период последовательностей является составным числом, т. е. $N = 2^{nk} - 1$.

Символы d_i ГМВ-последовательности с периодом $N = 2^{nk} - 1$ определяются выражением [5–6, 10]:

$$d_i = T_{n1} \left[\left(T_{nk,n}(\varepsilon^i) \right)^r \right], \quad (1)$$

$$1 \leq r < 2^n - 1, (r, 2^n - 1) = 1,$$

где $\varepsilon \in GF[(2^n)^k]$ – примитивный элемент поля; $T_{nk,n}(\cdot)$ – след элемента, принадлежащего полю $GF[(2^n)^k]$, в расширенном поле $GF(2^n)$; $T_{n1}(\cdot)$ – след элемента поля $GF(2^n)$ в простом поле $GF(2)$; r – нату-

ральное число, взаимно простое с порядком мультипликативной группы поля $GF(2^n)$, равным $2^n - 1$. В дальнейшем нижний индекс при обозначении функции следа $T(\cdot)$ может не использоваться, если он понятен из контекста.

При значении параметра $r = 1$ в (1) данное выражение определяет МП в канонической форме.

Структурная скрытность ПСП определяется эквивалентной линейной сложностью, которая для двоичных ГМВ-последовательностей определяется выражением [6–7]:

$$l_s = n \cdot k^{g(r)}, \quad (2)$$

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

С физической точки зрения ЭЛС l_s характеризует количество последовательных символов произвольной рекуррентной ПСП, достаточное для определения вида характеристического многочлена, формирующего данную ПСП. При этом для решения поставленной задачи, в соответствии с алгоритмом Берлекэмп – Мессе, требуется минимальное число последовательных символов ПСП, равное удвоенной степени характеристического многочлена.

Количество различных ГМВ-последовательностей, без учета базисной М-последовательности, определяется как произведение числа примитивных полиномов в подполе $GF(2^n)$ на число примитивных полиномов в поле $GF[(2^n)^k]$ [11]:

$$M_{\text{ГМВ}} = \left(\frac{\psi(2^n - 1)}{n} - 1 \right) \cdot \frac{\psi(2^m - 1)}{m},$$

где $\psi(a)$ – функция Эйлера, равная числу чисел, взаимно простых с числом a , в ряду от 1 до $(a - 1)$.

М- и ГМВ-последовательности с периодом N обладают одинаковой двухуровневой периодической автокорреляционной функцией для произвольного сдвига τ [4, 6, 11, 12]:

$$R(\tau) = \begin{cases} N & \text{при } \tau = kN, \\ -1 & \text{при } \tau \neq kN. \end{cases} \quad k = 0, 1, 2, \dots, \quad (3)$$

Известны различные способы формирования ГМВ-последовательностей. Для конечных полей с двойным расширением $GF[(2^n)^k]$ при $n = 2$ известен алгоритм формирования ГМВ-последовательностей с периодом $N = 2^{nk} - 1$ [10, 13], основанный на матричном представлении базисной М-последовательности с аналогичным периодом. При использовании данного алгоритма для формирования каждой ГМВ-последовательности базисная М-последовательность представляется в виде квазиквадратной матрицы, в которой затем выполняется замена столбцов, являющихся различными циклическими сдвигами М-последовательности с более коротким периодом $J = 2^n - 1$, на соответствующие сдвиги другой М-последовательности с таким же периодом.

Например, ГМВ-последовательность с периодом $N = 2^6 - 1 = 63$ формируются над полем $GF[(2^3)^2]$. При

этом базисная М-последовательность представляется как матрица размерности $[J \times L] = [7 \times 9]$, ее столбцами являются М-последовательности с периодом $J = 7$, получившие название характеристических последовательностей. Так как в подполе $GF(2^3)$ существует всего два примитивных многочлена и, соответственно, две различные М-последовательности, то для периода $N = 63$ для каждой из шести М-последовательностей можно сформировать только по одной ГМВ-последовательности.

Другим способом является формирование ГМВ-последовательности на основе регистров сдвига [14, 17]. Процедура формирования ГМВ-последовательности с периодом $N = 63$ на основе двух регистров сдвига очень похожа на процедуру формирования последовательностей Голда с аналогичным периодом. Однако здесь можно отметить принципиальное отличие.

Последовательности Голда с периодом $N = 63$ формируются с помощью двух регистров сдвига, каждый из которых строится на основе примитивного полинома. При этом данные последовательности образуются как поэлементные суммы двух М-последовательностей, составляющих предпочтительную пару. Начальные состояния регистров могут выбираться произвольным образом.

Периодическая корреляционная функция является четырехуровневой и принимает следующие значения:

$$R(\tau) = \begin{cases} N & \text{при } \tau = kN, \\ (-17, -1, +15) & \text{при } \tau \neq kN. \end{cases} \quad k = 0, 1, 2, \dots, \quad (4)$$

ГМВ-последовательности с периодом $N = 63$ представляют собой сумму М-последовательностей и ПСП с периодом $N_1 = 21$ и формируются на основе двух регистров сдвига с фиксированными начальными состояниями. При изменении начальных состояний регистров сдвига может быть увеличено число последовательностей, формируемых на основе данных многочленов-сомножителей [17]. Платой за это увеличение числа ПСП является изменение корреляционных свойств, т.е. периодическая корреляционная функция таких последовательностей для периода $N = 63$ становится пятиуровневой:

$$R(\tau) = \begin{cases} N & \text{при } \tau = kN, \\ (-9, -1, +7, +15) & \text{при } \tau \neq kN. \end{cases} \quad k = 0, 1, 2, \dots, \quad (5)$$

Однако модуль максимального значения корреляционной функции, равный 15, меньше аналогичного значения для последовательностей Голда, равного 17.

Таким образом, последовательности, формируемые на основе многочленов, используемых для синтеза ГМВ-последовательностей, но характеризующиеся функцией корреляции вида (5), определяемой увеличением числа начальных состояний регистров сдвига, целесообразно называть ГМВ-подобными последовательностями.

Целью настоящей работы является анализ возможностей применения ГМВ-подобных последовательностей для решения задач, связанных с расширением спектра формируемых на их основе широкополосных сигналов, а также с повышением скрытности передаваемых данных, с одной стороны, и (или) с повышением достоверности передачи информации, с другой стороны.

Для решения этих связанных между собой задач в работе предлагается использовать двойственный базис [16, 17]. При этом для формирования ГМВ-последовательностей с периодом $N = 63$ используются алгоритмы, основанные на представлении двоичной базисной М-последовательности в виде матрицы размерности $[J \times L] = [7 \times 9]$, где J – число строк, а L – число столбцов матрицы $F_{МП}$ [10]. Формирование базисной М-последовательности осуществляется регистром сдвига, сумматоры в цепи обратной связи которого расставляются в соответствии с характеристическим многочленом $\varphi_{МП}(x) = x^6 + x + 1$.

Обозначим в общем виде М-последовательность:

$$\{s\} = (s_0, s_1, s_2, s_3, s_4, s_5, s_6, \dots, s_{60}, s_{61}, s_{62}), \quad (6)$$

где первый элемент будет равен функции след от некоторого элемента C расширенного поля $GF(2^6)$, образованного многочленом $\varphi_{МП}(x)$.

Тогда произвольный двоичный элемент s_i , $i = 0, 1, 2, \dots, 61, 62$, последовательности $\{s\}$ может быть представлен как след:

$$s_i = T(C\varepsilon^i) = \sum_{k=0}^{m-1} (C\varepsilon^i)^{2^k}, \quad (7)$$

где ε – примитивный элемент поля $GF(2^6)$; m – степень многочлена $\varphi_{МП}(x)$.

Таким образом, начальным элементом, формирующим М-последовательность $\{s\}$, является элемент поля C . Будем называть его в дальнейшем начальной фазой М-последовательности. Для формирования такой ненулевой последовательности может быть выбран произвольный ненулевой элемент поля.

Если выбрать $C = 1$, то будет сформирована каноническая М-последовательность вида:

$$\{s\} = [T(1), T(\varepsilon), T(\varepsilon^2), T(\varepsilon^3), T(\varepsilon^4), T(\varepsilon^5), \dots, T(\varepsilon^{61}), T(\varepsilon^{62})].$$

Применительно к полю $GF(2^6)$ произвольный элемент поля ε^i , представленный через левый степенной базис, будет:

$$\varepsilon^i = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4\varepsilon^4 + a_5\varepsilon^5.$$

При этом можно показать, что след элемента поля ε^i для заданного образующего многочлена $\varphi_{МП}(x)$ будет равен $T(\varepsilon^i) = a_5 \in GF(2)$. Следовательно, каноническая М-последовательность $\{s_{кан}\}$ будет записана выражением (8).

Аналогично, при другой ненулевой начальной фазе $C \neq 1$ будет иметь место такая же по структуре последовательность, но с циклическим сдвигом фазы влево относительно канонической М-последовательности на число шагов, равное индексу (степени) i при элементе поля ε в значении начальной фазы последовательности $C = \varepsilon^i$. Например, пусть $C = \varepsilon$, тогда М-последовательность будет представлена выражением (9). Первым шагом при формировании ГМВ- или ГМВ-подобной последовательности на передающей стороне является составление матрицы $F_{МП}$ из заданной М-последовательности.

Так как период МП $N = 63$ является составным, а именно: $N = J \times L$, где $J = 7$, а $L = 9$, то матрица $F_{МП}$ синтезируется путем последовательной построчной записи символов сформированной М-последовательности по L двоичных символов в каждой из J строк. Следует отметить, что в общем виде сомножитель J должен представлять собою порядок мультипликативной группы ненулевых элементов подполя $GF(2^n)$ в составе расширенного поля $GF(2^m)$ и, следовательно, число n должно быть делителем числа m . В нашем примере число $n = 3$ является делителем числа $m = 6$ и поэтому $J = 2^n - 1 = 7$. Тогда матрица $F_{МП}$, образованная из элементов МП $\{s\}$, будет иметь для $N = 63$ следующий вид, представленный выражением (10).

$$\{s_{кан}\} = \begin{bmatrix} s_0 & s_1 & s_2 & s_3 & s_4 & s_5 & s_6 & s_7 & s_8 & s_9 & s_{10} & \dots & s_{60} & s_{61} & s_{62} \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & \dots & 1 & 1 & 1 \end{bmatrix}. \quad (8)$$

$$\{s_{кан}\} = \begin{bmatrix} s_0 & s_1 & s_2 & s_3 & s_4 & s_5 & s_6 & s_7 & s_8 & s_9 & s_{10} & \dots & s_{60} & s_{61} & s_{62} \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & \dots & 1 & 1 & 0 \end{bmatrix}. \quad (9)$$

$$F_{МП} = \begin{bmatrix} s_0 & s_1 & s_2 & s_3 & s_4 & s_5 & s_6 & s_7 & s_8 \\ s_9 & s_{10} & s_{11} & s_{12} & s_{13} & s_{14} & s_{15} & s_{16} & s_{17} \\ s_{18} & s_{19} & s_{20} & s_{21} & s_{22} & s_{23} & s_{24} & s_{25} & s_{26} \\ s_{27} & s_{28} & s_{29} & s_{30} & s_{31} & s_{32} & s_{33} & s_{34} & s_{35} \\ s_{36} & s_{37} & s_{38} & s_{39} & s_{40} & s_{41} & s_{42} & s_{43} & s_{44} \\ s_{45} & s_{46} & s_{47} & s_{48} & s_{49} & s_{50} & s_{51} & s_{52} & s_{53} \\ s_{54} & s_{55} & s_{56} & s_{57} & s_{58} & s_{59} & s_{60} & s_{61} & s_{62} \end{bmatrix}. \quad (10)$$

Если принять, что $C = \varepsilon$, то элемент s_i , $i = 0, 1, 2, \dots, 61, 62$, матрицы (10) будет определяться как след от элемента поля $C\varepsilon^i = \varepsilon^{i+1}$, т. е. $s_i = T(C\varepsilon^i) = T(\varepsilon^{i+1}) = a_5$, где a_5 – старший разряд в векторном представлении элемента поля ε^{i+1} . Тогда матрица (10) при $C = \varepsilon$ приобретает следующий вид:

$$F_{МП} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}. \quad (11)$$

Таким образом, как видно из (10), каждый i -ый столбец ($i = 0, 1, 2, \dots, 8$) матрицы $F_{МП}$ представляется в общем виде как выражение:

$$[s_i, s_{i+9}, s_{i+18}, s_{i+27}, s_{i+36}, s_{i+45}, s_{i+54}]. \quad (12)$$

Из записи (12) следует, что столбцы матрицы $F_{МП}$ представляют собой последовательности из 7 элементов базисной М-последовательности, отстоящие друг от друга на индекс децимации $q = 9$. Очевидно, что, добавив к ряду (12) следующий элемент с таким же индексом децимации, получим $s_{i+54+9} = s_{i+63} = s_i$. Следовательно, каждый из столбцов матрицы $F_{МП}$ будет представлять собой определенную МП₁, т. е. последовательность с периодом $J = 2^3 - 1 = 7$, порождаемую некоторым неприводимым характеристическим многочленом $h_1(x)$ степени $n = 3$. Как известно из теории полей Галуа, корнями многочлена $h_1(x)$ в этом случае будут q -ые ($q = 9$ – индекс децимации) степени корней примитивного многочлена $\varphi_{МП}(x)$, порождающего исходную базисную МП и поле $GF(2^6)$. Пусть корнями многочлена $\varphi_{МП}(x)$ будут первообразные p -сопряженные элементы поля $\varepsilon, \varepsilon^2, \varepsilon^4, \varepsilon^8, \varepsilon^{16}, \varepsilon^{32}$. Тогда корнями многочлена $h_1(x)$ будут их q -ые ($q = 9$) степени, а именно $\varepsilon^9, \varepsilon^{18}, \varepsilon^{36}$. Отсюда, зная корни многочлена $h_1(x)$ и используя формулы Виета, найдем многочлен $h_1(x)$, который будет равен:

$$h_1(x) = 1 + x^2 + x^3. \quad (13)$$

Тогда столбцы матрицы $F_{МП}$ будут представлять собой МП₁ с характеристическим многочленом $h_1(x)$, при этом каждой из девяти МП₁ будет соответствовать определенная фаза в виде элемента λ , принадлежащего подполю $GF_1(2^3)$, порожденному многочленом (13). Ненулевые элементы $\lambda = b_0 + b_1\lambda + b_2\lambda^2$, $j = 0, 1, 2, \dots, 6$, подполя $GF_1(2^3)$ и их векторная запись показаны в таблице 1. В правой колонке представлена каноническая МП₁ с начальным фазовым элементом поля, равным 1. Из таблицы 1 следует, что начальные фазовые элементы столбцов матрицы $F_{МП}$ (11) будут иметь вид, приведенный в таблице 2. На этом заканчивается процедура построения матрицы $F_{МП}$ (11).

Далее рассмотрим некоторые алгоритмы преобразования матрицы $F_{МП}$ в матрицу $F_{ГМВ}$, отображаю-

щую ГМВ-последовательность. Для такого преобразования можно выбрать разные правила – от самых простых до самых сложных, к тому же алгоритмы, с целью большего сокрытия процесса передачи информации, могут быть итеративными, т. е. состоять из нескольких раундов. В самих алгоритмах могут быть заложены элементы секретности, которые должны быть известны только отправителю и получателю. В конечном счете, выбор алгоритма влияет на структуру и на процедуру обработки на приеме ГМВ- и ГМВ-подобных последовательностей.

В большинстве известных алгоритмов процесс формирования матрицы $F_{ГМВ}$ заключается в замене столбцов матрицы $F_{МП}$, т. е. МП₁ с характеристическим многочленом $h_1(x)$ на МП₂ с многочленом $h_2(x)$, двойственным по отношению к $h_1(x)$:

$$h_2(x) = x^3 h_1(x^{-1}) = 1 + x + x^3. \quad (14)$$

Так как многочлен $h_2(x)$ является двойственным по отношению к многочлену $h_1(x)$, то его корнями будут элементы, обратные корням многочлена $h_1(x)$, т. е. $\theta = \lambda^{-1}$, $\theta^2 = \lambda^{-2}$ и $\theta^4 = \lambda^{-4}$. Все ненулевые элементы $\theta^i = d_0 + d_1\theta + d_2\theta^2$ подполя $GF_2(2^3)$, образованного многочленом $h_2(x)$, и соответствующие им функции след и вектора представлены в таблице 3. Как и в таблице 2, в колонке «След элемента θ^i » находится каноническая МП₂ с периодом 7, порожденная многочленом $h_2(x)$, а в правой колонке приведено соответствие между элементами обоих подполей $GF_1(2^3)$ и $GF_2(2^3)$, образованных многочленами $h_1(x)$ и $h_2(x)$, соответственно.

Проведем анализ некоторых алгоритмов формирования матрицы $F_{ГМВ}$ на основе матрицы $F_{МП}$ и обработки ГМВ- и ГМВ-подобных последовательностей на приемной стороне с использованием двойственного базиса по методике, изложенной в [16, 17]. Коэффициенты двойственного базиса для рассматриваемых в работе многочленов $\varphi_{МП}(x)$, $h_1(x)$ и $h_2(x)$, представлены в таблице 4.

ТАБЛИЦА 1. Ненулевые элементы подполя $GF_1(2^3)$

$\lambda = b_0 + b_1\lambda + b_2\lambda^2$	(b_0, b_1, b_2)	$T(\lambda) = b_0 + b_1\lambda + b_2\lambda^2, \text{ mod } 2$
$\lambda^0 = 1$	(100)	$1 = T(1)$
λ	(010)	$1 = T(\lambda)$
λ^2	(001)	$1 = T(\lambda^2)$
$\lambda^3 = 1 + \lambda^2$	(101)	$0 = T(\lambda^3)$
$\lambda^4 = 1 + \lambda + \lambda^2$	(111)	$1 = T(\lambda^4)$
$\lambda^5 = 1 + \lambda$	(110)	$0 = T(\lambda^5)$
$\lambda^6 = \lambda + \lambda^2$	(011)	$0 = T(\lambda^6)$

ТАБЛИЦА 2. Начальные фазовые элементы столбцов матрицы $F_{МП}$

Номер столбца j	1	2	3	4	5	6	7	8	9
Начальный фазовый элемент поля, $\lambda_1(j) = \lambda^i$	λ^3	λ^6	λ^5	λ^5	λ^2	λ^3	λ^5	λ^3	0
Первая строка матрицы $F_{МП}$	0	0	0	0	1	0	0	0	0

ТАБЛИЦА 3. Ненулевые элементы подполя $GF_2(2^3)$.

$\theta^i = d_0 + d_1\theta + d_2\theta^2$	(d_0, d_1, d_2)	$T(\theta^i) = d_0 \in GF(2)$	θ^i VS λ^i
$\theta^0 = 1$	(100)	$1 = T(1)$	$\theta^0 = \lambda^0 = 1$
θ	(010)	$0 = T(\theta)$	$\theta = \lambda^{-1} = \lambda^6$
θ^2	(001)	$0 = T(\theta^2)$	$\theta^2 = \lambda^{-2} = \lambda^5$
$\theta^3 = 1 + \theta$	(110)	$1 = T(\theta^3)$	$\theta^3 = \lambda^{-3} = \lambda^4$
$\theta^4 = \theta + \theta^2$	(011)	$0 = T(\theta^4)$	$\theta^4 = \lambda^{-4} = \lambda^3$
$\theta^5 = 1 + \theta + \theta^2$	(111)	$1 = T(\theta^5)$	$\theta^5 = \lambda^{-5} = \lambda^2$
$\theta^6 = 1 + \theta^2$	(101)	$1 = T(\theta^6)$	$\theta^6 = \lambda^{-6} = \lambda$

ТАБЛИЦА 4. Коэффициенты двойственного базиса многочленов $\varphi_{МП}(x)$, $h_1(x)$ и $h_2(x)$

$\varphi_{МП}(x) = 1 + x + x^6$	$\alpha_1 = \varepsilon^{62}$	$\alpha_2 = \varepsilon^4$	$\alpha_3 = \varepsilon^3$	$\alpha_4 = \varepsilon^2$	$\alpha_5 = \varepsilon$	$\alpha_6 = 1$
$h_1(x) = 1 + x^2 + x^3$	$\gamma_1 = \lambda^4$	$\gamma_2 = \lambda^3$	$\gamma_3 = \lambda^5$			
$h_2(x) = 1 + x + x^3$	$\beta_1 = 1$	$\beta_2 = \theta^2$	$\beta_3 = \theta$			

Алгоритм № 1. Рассмотрим алгоритм, аналогичный описанному в [10]. Произвольно выберем МП₁, например, (0011101), присвоим ей номер 1 и обозначим как $v(1)$. Далее производим последовательные циклические сдвиги выбранной последовательности на один шаг вправо и увеличиваем номер последовательности на каждом сдвиге на единицу относительно предыдущего. В таблице 5 представлены все 7 ненулевых МП₁ $v(i)$ с номерами $i, i = 1, 2, \dots, 7$, и соответствующими начальными фазовыми элементами λ^i подполя $GF_1(2^3)$. Произвольно выберем в качестве МП₂ с номером 1 последовательность $w(1) = (0010111)$, аналогично алгоритму 1, и, производя циклические сдвиги вправо на один шаг, получим все возможные ненулевые циклические сдвиги МП₂, показанные в правой половине таблицы 5, с возрастающими порядковыми номерами. В правой колонке содержатся их начальные фазовые элементы θ^i подполя $GF_2(2^3)$, соответствующие МП₂.

ТАБЛИЦА 5. Таблица соответствия МП₁ и МП₂ для формирования ГМВ-подобной последовательности

Номер сдвига i	МП ₁		МП ₂	
	$v(i)$	λ^i	$w(i)$	θ^i
1	(0011101)	λ^5	(0010111)	θ
2	(1001110)	λ^4	(1001011)	1
3	(0100111)	λ^3	(1100101)	θ^6
4	(1010011)	λ^2	(1110010)	θ^5
5	(1101001)	λ	(0111001)	θ^4
6	(1110100)	1	(1011100)	θ^3
7	(0111010)	λ^6	(0101110)	θ^2

Сформулируем теперь правило построения матрицы $F_{ГМВ}$, которое будет состоять в замене столбцов матрицы $F_{МП}$, представляющих собой МП₁ с определенными начальными фазовыми элементами λ^i , на МП₂ с теми же порядковыми номерами. Для рассматриваемой в конкретном примере матрицы $F_{МП}$ (11) и таблицы 5 правило замены можно записать в виде строки из номеров соответствующих фазовых сдвигов:

$$I = (3, 7, 1, 1, 4, 3, 1, 3, 0), \quad (15)$$

где цифра 0 соответствует столбцу, состоящему из одних нулей.

Согласно этому правилу первый столбец в матрице $F_{МП}$ в виде МП₁ с номером 3 заменяется на МП₂ с таким же номером. Аналогичным образом происходит замена и других столбцов в матрице $F_{МП}$. Таким образом, вместо матрицы $F_{МП}$ будет сформирована матрица $F_{ГМВ}$ вида (16). ГМВ-последовательность, передаваемая в канал, будет состоять из последовательно считываемых строк матрицы $F_{ГМВ}$, начиная с левого элемента первой строки:

$$F_{ГМВ} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}. \quad (16)$$

На рисунке 1 приведены автокорреляционная функция (АКФ) ГМВ-подобной последовательности, сформированной по таблице 5, и ее взаимокорреляционная функция (ВКФ) с последовательностью, сформированной по другой аналогичной таблице. Для определения АКФ и ВКФ ГМВ-последовательности приводятся к биполярному виду: «1» → «-1»; «0» → «1».

Обработка (декодирование) ГМВ-последовательности на приеме. Будем считать, что на приемной стороне стоит задача определить информацию, закодированную начальным фазовым элементом $C \in GF(2^6)$ исходной МП, формируемой многочленом $\varphi_{МП}(x)$. Для решения этой задачи в данном алгоритме получателю на приемной стороне сообщаются начальные фазовые элементы λ^i МП₁ и θ^i МП₂ с номерами 1, что позволяет получателю сгенерировать последовательности МП₁ и МП₂ и соответствующие им номера. Это позволит по столбцам матрицы $F_{ГМВ}$, сформированной на приеме, определить правило замены столбцов (15). Рассмотрим теперь пошаговую процедуру декодирования.

Шаг 1. Как сказано выше, из принятой ГМВ-последовательности формируют матрицу $F_{ГМВ}$, которая, при отсутствии ошибок, будет иметь такой же вид, как и (16).

Шаг 2. По 3-элементным участкам МП₂ каждого столбца матрицы $F_{ГМВ}$ с помощью двойственного базиса многочлена $h_2(x)$ (таблица 4) находятся начальные фазовые элементы $\theta(j)$ для каждого j -го столбца в отдельности. В предположении, что ошибок нет, начальные фазовые элементы $\theta(j)$ могут быть определены по любому 3-элементному участку для каждого столбца, представляющего в общем виде 7-разрядную комбинацию $(w_0, w_1, w_2, w_3, w_4, w_5, w_6)$.

Так, для участка (w_i, w_{i+1}, w_{i+2}) , $i = 0, 1, 2, \dots, 6$ замкнутой в кольцо МП₂, начальный элемент $\theta(j)$ j -го столбца матрицы $F_{ГМВ}$ будет определяться как:

$$\theta(j) = \theta^{-i}(\beta_1 w_i + \beta_2 w_{i+1} + \beta_3 w_{i+2}). \quad (17)$$

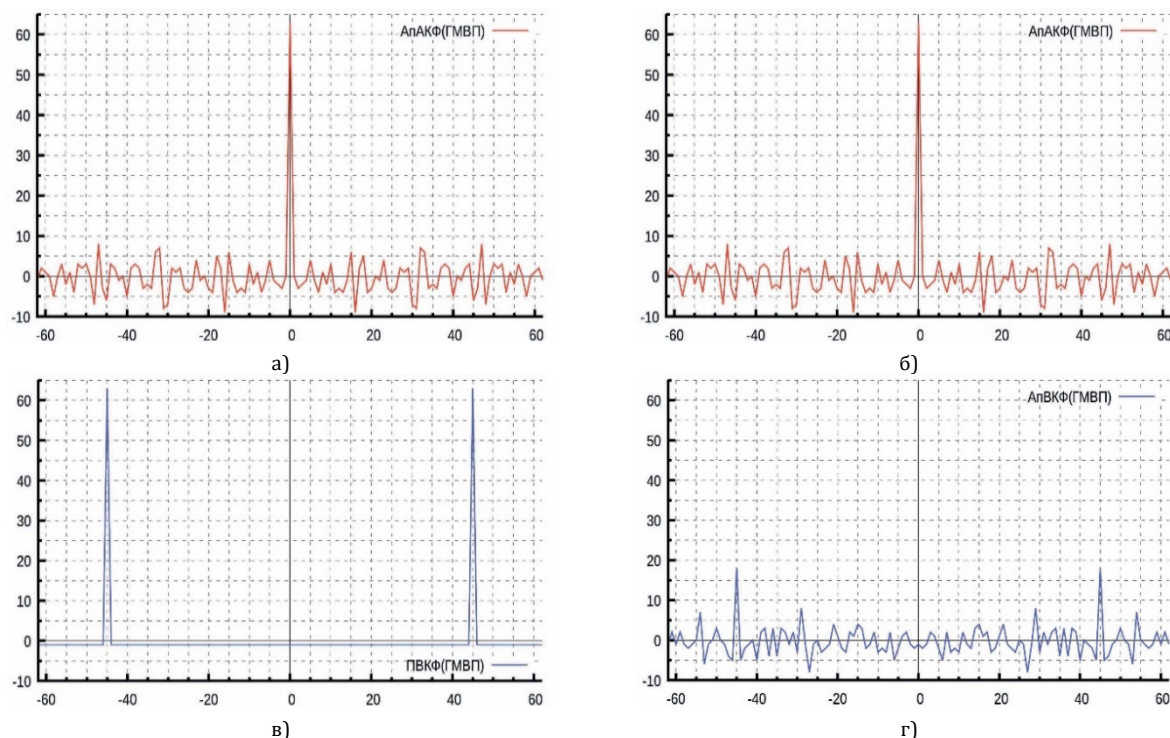


Рис. 1. Корреляционные свойства ГМВ-подобных последовательностей (16): а) периодическая АКФ б) аperiodическая АКФ; в) периодическая ВКФ; г) аperiodическая ВКФ

По выделенным участкам (w_i, w_{i+1}, w_{i+2}) находим:

- для 1-го столбца ($j = 1$) по участку $(w_0, w_1, w_2) = (1, 1, 0)$, $\theta(1) = \beta_1 + \beta_2 = 1 + \theta^2 = \theta^6$;
- для 2-го столбца ($j = 2$) по участку $(w_1, w_2, w_3) = (1, 0, 1)$, $\theta(2) = \theta^{-1}(\beta_1 + \beta_3) = \theta^2$;
- для 3-го столбца ($j = 3$) по участку $(w_2, w_3, w_4) = (1, 0, 1)$, $\theta(3) = \theta^{-2}(\beta_1 + \beta_3) = \theta$.

Аналогично находим начальные фазовые элементы для всех 9 столбцов, которые образуют следующую строку начальных фазовых элементов столбцов матрицы $F_{ГМВ}$:

$$(\theta^6, \theta^2, \theta, \theta, \theta^5, \theta^6, 0), \quad (18)$$

а по этим начальным фазовым элементам будет, в соответствии с таблицей 5, определено и само правило замены (15) – секретное ключевое слово I .

Легко проверить, что такие же начальные фазовые элементы будут получены благодаря мажори-

тарному принятию решения, если в столбцах возникнут однократные ошибки или парные ошибки в смежных позициях столбца. Например, 5-ый столбец содержит две ошибки в подчеркнутых позициях w_2 и w_3 , т. е. имеет вид:

$$(w_0, w_1, \underline{w_2}, \underline{w_3}, w_4, w_5, w_6) = (1, 1, \underline{0}, \underline{1}, 0, 1, 0).$$

Вычислим с использованием двойственного базиса начальные фазовые элементы по всем 3-элементным участкам замкнутого в кольцо 5-го столбца ($j = 5$):

$$\begin{aligned} i = 0; (w_0, w_1, w_2) &= (1, 1, 0) \quad \theta(5) = \beta_1 + \beta_2 = 1 + \theta^2 = \theta^6; \\ i = 1; (w_1, \underline{w_2}, \underline{w_3}) &= (1, 0, 1) \quad \theta(5) = \theta^{-1}(\beta_1 + \beta_3) = \theta^{-1}(1 + \theta) = \theta^2; \\ i = 2; (\underline{w_2}, \underline{w_3}, w_4) &= (0, 1, 0) \quad \theta(5) = \theta^{-2}\beta_2 = \theta^{-2}\theta^2 = 1; \\ i = 3; (\underline{w_3}, w_4, w_5) &= (1, 0, 1) \quad \theta(5) = \theta^{-3}(\beta_1 + \beta_3) = \theta^{-3}\theta^3 = 1; \\ i = 4; (w_4, w_5, w_6) &= (0, 1, 0) \quad \theta(5) = \theta^{-4}\beta_2 = \theta^{-4}\theta^2 = \theta^5; \\ i = 5; (w_5, w_6, w_0) &= (1, 0, 1) \quad \theta(5) = \theta^{-5}(\beta_1 + \beta_3) = \theta^{-5}(1 + \theta) = \theta^5; \\ i = 6; (w_6, w_0, w_1) &= (0, 1, 1) \quad \theta(5) = \theta^{-6}(\beta_2 + \beta_3) = \theta^{-6}(\theta^2 + \theta) = \theta^5. \end{aligned}$$

По большинству одинаковых оценок начальный фазовый элемент 5-го столбца при двух смежных ошибках, как видно из (18), будет определен правильно, т. е. $\theta(5) = \theta^5$.

Шаг 3. По цифрам полученного ключевого слова, имеющего вид (15), находим соответствующие этим цифрам (см. таблицу 5) начальные элементы $\lambda(j)$ столбцов матрицы $F_{МП}$. Беря след от элементов

$\lambda(j)$, получим первую строку матрицы в двоичном виде (см. таблицу 2).

Шаг 4. Наконец, используя двойственный базис многочлена $\Phi_{МП}(x)$ (см. таблицу 4), по 6-элементным участкам найдем начальный элемент $C \in GF(2^6)$, формирующий исходную МП и представляющий переданную закодированную информацию. Пусть, например, выделен безошибочный участок сформированной на приеме первой строки матрицы $F_{МП}$: $(s_2, s_3, s_4, s_5, s_6, s_7) = (001000)$. Вычисленный по этому участку начальный фазовый элемент C М-последовательности будет: $C = \varepsilon^{-2}\alpha_3 = \varepsilon^{-2}\varepsilon^3 = \varepsilon$.

Таким образом, начальный фазовый элемент $C = \varepsilon$ М-последовательности декодирован правильно, т. е. переданная информация в виде двоичной комбинации будет иметь вид (010000).

Эта информация может представлять собой определенный секрет для получателя. Например, это может быть начальная фаза скремблера, обеспечивающего рандомизацию передаваемых данных М-последовательностью с периодом $N = 2^6 - 1$, или некоторый идентификатор адреса получателя или отправителя и др.

Очевидно, что достоверность выделения начального фазового элемента C может быть увеличена путем восстановления на приеме всей матрицы $F_{МП}$ с последующим формированием базисной М-последовательности и применения мажоритарного декодирования 6-элементных ее участков с использованием двойственного базиса. Для определения вероятностных характеристик рассмотренных методов декодирования ГМВ-подобных последовательностей было произведено имитационное моделирование по методу Монте-Карло с использованием системы математических вычислений GNU/Octave. Была построена классическая модель системы передачи данных. Для формирования потока ошибок была использована модель цифрового двоично-симметричного канала без памяти.

Декодирование передаваемых по модели системы передачи данных ГМВ-подобных последовательностей по мажоритарному методу на основе двойственного базиса допускает три возможных исхода:

- правильное декодирование, когда результат на выходе декодера совпадает с начальными элементами передаваемой последовательности;
- неправильное декодирование, которое возникает при несовпадении начальных элементов;
- отказ от декодирования, когда декодер не может однозначно определить результат декодирования, т. е. обнаруженная неисправляемая ошибка.

Соответствующие оценочные значения вероятностных характеристик обозначаются $P_{пд}$, $P_{нд}$, $P_{од}$.

Поскольку декодирование по рассмотренному алгоритму проводится в два этапа: вначале декодируются 7-элементные М-последовательности (столбцы матрицы $F_{ГМВ}$ (16), а потом производится поиск начального фазового элемента исходной М-

последовательности длиной 63, то отказ от декодирования может произойти на каждом из этапов. При отказе от декодирования 7-элементной последовательности она помечается как стертая. Далее производится проверка возможности определения начального элемента C исходной 63-элементной М-последовательности. В том случае, если он не может быть рассчитан, фиксируется отказ от декодирования.

При более надежном мажоритарном декодировании исходной М-последовательности по 6-элементным участкам отказом от декодирования в рассматриваемом алгоритме будет считаться отказ декодирования хотя бы одной 7-элементной М-последовательности.

Графики вероятностных характеристик рассмотренных алгоритмов приведены на рисунке 2. Рисунок 2а содержит вероятностные характеристики простого алгоритма декодирования с определением начального элемента исходной М-последовательности по одному 6-элементному участку, а рисунок 2б – вероятностные характеристики усиленного алгоритма с мажоритарным декодированием замкнутой в кольцо исходной последовательности.

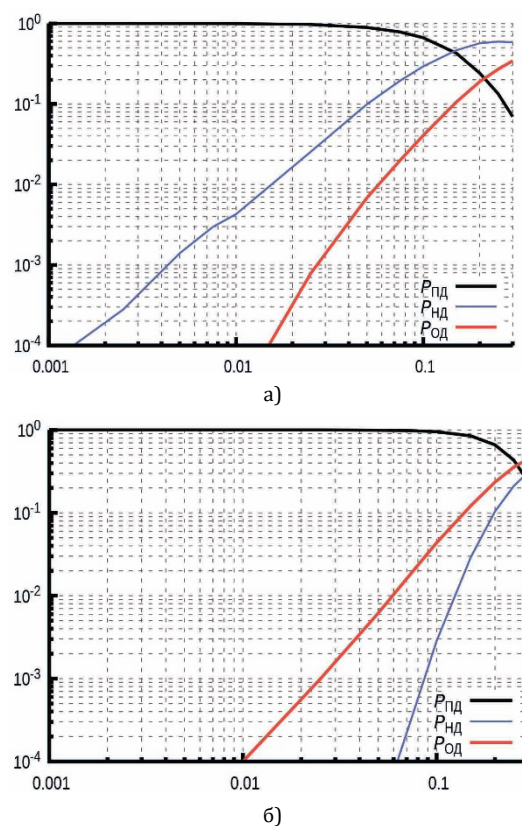


Рис. 2. Вероятностные характеристики алгоритма декодирования ГМВ-подобных последовательностей

Как видно из представленных графиков, мажоритарное декодирование исходной М-последовательности позволяет значительно увеличить вероятность правильного определения начального фазового элемента и на два порядка уменьшить долю неправильно декодированных последовательностей.

Рассмотрим еще один вариант, который позволяет в несколько раз увеличить долю информации, содержащейся в ГМВ- или в ГМВ-подобных последовательностях длиной 63. При этом возможны два алгоритма – мультипликативный и аддитивный.

Мультипликативный (пошаговый) алгоритм.

Передающая сторона.

Шаг 1а. Формируется матрица $F_{МП}$. Например, при той же начальной фазе $C = \varepsilon$ матрица $F_{МП}$ будет иметь вид (11). Тогда столбцами этой матрицы будут МП₁ с начальными элементами $\lambda(j)$, представленными в таблице 2. Для передачи информации в этом алгоритме будут задействованы первые 8 (кроме 9-го нулевого) начальных элементов $\lambda(j)$.

Шаг 2а. На следующем шаге алгоритма задается строка из 8 информационных элементов $\lambda_u(j)$, $j = 0, 1, \dots, 7$, принадлежащих полю $GF(2^3)$, порожденному примитивным многочленом $h_1(x)$. Пусть эти информационные элементы будут:

$$(\lambda^2, \lambda^5, \lambda, 1, \lambda^3, \lambda^3, \lambda^4, \lambda^5). \quad (19)$$

Шаг 3а. Далее эти элементы перемножаются по mod $h_1(x)$ с соответствующими начальными элементами $\lambda(j)$ первых 8 столбцов матрицы $F_{МП}$ (см. таблицу 2). В результате перемножения в таблице 6 будет получена строка из 8 новых элементов $\lambda(j)$ поля $GF(2^3)$, образованного примитивным многочленом $h_1(x)$, и соответствующих им двоичных векторов (b_0, b_1, b_2) .

Шаг 4а. На следующем шаге находятся по таблице 3 соответствующие векторам (b_0, b_1, b_2) элементы θ^y изоморфного поля $GF(2^3)$ с порождающим многочленом $h_2(x)$ (см. таблицу 6).

Шаг 5а. По полученным элементам θ^y , как начальным фазовым элементам, формируются первые 8 столбцов матрицы $F_{ГМВ}$, которая в виде МП₂-последовательностей, с учетом 9-го нулевого столбца, примет вид (20).

$$F_{ГМВ} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}. \quad (20)$$

ТАБЛИЦА 6. Замена элементов λ^i на θ^y

Номер столбца	1	2	3	4	5	6	7	8
Начальные фазовые элементы поля, λ^i	λ^5	λ^4	λ^6	λ^5	λ^5	λ^6	λ^2	λ
Векторная запись элементов λ^i	110	111	011	110	110	011	001	010
Соответствующие элементы $\theta^y \bmod h_2(x)$	θ^3	θ^5	θ^4	θ^3	θ^3	θ^4	θ^2	θ

Приемная сторона.

Декодирование ГМВ- или ГМВ-подобных последовательностей и извлечение из них информации на приеме осуществляется в обратном порядке по следующим шагам.

Шаг 1б. Используя коэффициенты двойственного базиса, соответствующего многочлену $h_2(x)$ (см. таблицу 4), для каждого замкнутого в кольцо столбца (кроме 9-го) принятой матрицы $F_{ГМВ}$ по смежным 3-элементным участкам находятся по мажоритарному принципу начальные фазовые элементы θ^y . Пусть первый столбец принятой матрицы $F_{ГМВ}$ с ошибкой в подчеркнутом элементе w_3 будет следующий:

$$(w_0, w_1, w_2, \underline{w_3}, w_4, w_5, w_6, w_7) = (1, 0, 1, 0, 1, 0, 0).$$

Проведя обработку двойственным базисом 3-элементных участков (w_i, w_{i+1}, w_{i+2}) выделенного и замкнутого в кольцо первого столбца принятой матрицы $F_{ГМВ}$, получим следующие результаты:

$$\begin{aligned} i=0; & (w_0, w_1, w_2) = (1, 0, 1); \quad \theta^y = \beta_1 + \beta_3 = 1 + \theta = \theta^3; \\ i=1; & (w_1, w_2, \underline{w_3}) = (0, 1, 0); \quad \theta^y = \theta^{-1}(\beta_2) = \theta^{-1} \cdot \theta^2 = \theta; \\ i=2; & (w_2, \underline{w_3}, w_4) = (1, 0, 1); \quad \theta^y = \theta^{-2}(\beta_1 + \beta_3) = \theta^{-2}\theta^3 = \theta; \\ i=3; & (\underline{w_3}, w_4, w_5) = (0, 1, 0); \quad \theta^y = \theta^{-3}(\beta_2) = \theta^{-3}\theta^2 = \theta^{-1} = \theta^6; \\ i=4; & (w_4, w_5, w_6) = (1, 0, 0); \quad \theta^y = \theta^{-4}\beta_1 = \theta^{-4} = \theta^3; \\ i=5; & (w_5, w_6, w_0) = (0, 0, 1); \quad \theta^y = \theta^{-5}(\beta_3) = \theta^{-5}\theta = \theta^{-4} = \theta^3; \\ i=6; & (w_6, w_0, w_1) = (0, 1, 0); \quad \theta^y = \theta^{-6}(\beta_2) = \theta^{-6}\theta^2 = \theta^{-4} = \theta^3. \end{aligned}$$

Несмотря на наличие однократной ошибки в первом столбце принятой матрицы $F_{ГМВ}$, в результате обработки двойственным базисом по мажоритарному принципу был правильно выделен в качестве начальной фазы элемент θ^3 . Таким образом, в предположении, что в каждом столбце матрицы $F_{ГМВ}$ не было ошибок или было не более одной ошибки или одной двукратной ошибки в паре смежных элементов, декодер правильно выделит начальные фазы θ^y всех восьми ненулевых столбцов матрицы

$F_{ГМВ}$ и соответствующие им вектора (d_0, d_1, d_2) , представленные в таблице 6.

Шаг 2б. Далее, в соответствии с полученными на предыдущем шаге двоичными векторами, будут определены 8 элементов λ^i (см. таблицу 6).

Шаг 3б. Декодер по известному только отправителю и получателю начальному фазовому элементу $C \in GF(2^6)$, аналогично кодеру, формирует начальные фазовые элементы λ^i матрицы $F_{МП}$, а именно:

$$(\lambda^3, \lambda^6, \lambda^5, \lambda^5, \lambda^2, \lambda^3, \lambda^5, \lambda^3). \quad (21)$$

Шаг 4б. На следующем шаге производится деление по $\text{mod } h_1(x)$ выделенных из матрицы $F_{\text{ГМВ}}$ элементов $\lambda(j)$, показанных в таблице 6, на соответствующие элементы $\lambda(j)$, являющиеся начальными фазовыми элементами j -ых столбцов матрицы $F_{\text{МП}}$ (21). В результате будут получены элементы (19), которые и будут являться информационными. Записав эти информационные элементы соответствующими двоичными векторами (см. таблицу 1), выделенная информация будет иметь вид:

{001 110 010 100 101 101 111 110}.

Значит, в принятой ГМВ- или в ГМВ-подобной последовательности длиной 63 двоичных элемента содержится 24 информационных бита, что соответствует относительной скорости передачи данных 0,38. Если же 9-ый нулевой столбец матрицы (15) не передавать (с его восстановлением на приеме), то скорость передачи данных по каналу возрастет до 0,42.

Оценим ожидаемую достоверность передачи данных с помощью ГМВ- или ГМВ-подобной последовательности по двоичному симметричному каналу с битовой вероятностью ошибки $p_0 = 10^{-2}$. Так как в рассматриваемом примере информация содержится в 8 столбцах ГМВ-матрицы (20), то вероятность гарантированного правильного декодирования информации будет определяться вероятностью того, что в каждом из 8 столбцов будет только одна ошибка, или две ошибки в смежных элементах, или ошибки будут отсутствовать. В этом случае вычисленная вероятность Q правильного выделения одного столбца с учетом 7 смежных парных ошибок в столбце будет равна:

$$Q = (1 - p_0)^7 + C_7^1 p_0 (1 - p_0)^6 + 7 p_0^2 (1 - p_0)^5 = 0,99856.$$

Исходя из этого, вероятность правильного декодирования с использованием двойственного базиса всех 8 столбцов ГМВ-матрицы и, следовательно, всех 24 информационных бита, будет равна:

$$Q^8 = (0,99856)^8 = 0,9885.$$

Тогда вероятность ошибочного декодирования хотя бы одного элемента λ^i будет равна:

$$P_{\text{нпд}} = 1 - 0,9885 = 1,14 \cdot 10^{-2}.$$

Повысить достоверность дополнительно можно благодаря применению децимаций [16] при обработке МП₂. Вероятностные характеристики при использовании мультипликативного алгоритма приведены на рисунке 3. Первый случай (рисунок 3а) относится к независимому декодированию отдельного информационного элемента λ^i . Во втором случае (рисунок 3б) приведены вероятностные характеристики декодирования всей 24-разрядной информационной последовательности. Из графиков видно, что использование децимаций позволяет значительно уменьшить вероятность неправильного декодирования ценой небольшого уменьшения доли правильно декодированных комбинаций.

Аддитивный алгоритм

При аддитивном алгоритме ожидается более простая реализация, т. к. использовано двоичное сложение векторов вместо умножения элементов поля.

Передающая сторона (кодирование).

Шаг 1в. Первый шаг аддитивного алгоритма не отличается от мультипликативного, т. е., при той же начальной фазе $C = \varepsilon$ формируется матрица $F_{\text{МП}}$, имеющая вид (11).

Шаг 2в. На следующем шаге алгоритма задается строка из девяти информационных элементов $\lambda_u(j)$, $j = 0, 1, \dots, 8$, принадлежащих полю $\text{GF}(2^3)$, порожденному примитивным многочленом $h_1(x)$. Пусть первые восемь информационных элементов будут такими же, как и в мультипликативном алгоритме (19), к которым добавлен девятый элемент, например, λ_6 .

Шаг 3в. Далее, двоичные вектора информационных элементов $\lambda_u(j)$, $j = 0, 1, \dots, 8$, поэлементно складываются по $\text{mod } 2$ с двоичными векторами, соответствующими элементам $\lambda(j)$, являющимися начальными фазовыми элементами j -ых столбцов матрицы $F_{\text{МП}}$ (21). В результате по полученным двоичным векторам определяются начальные фазовые элементы $\theta(j) \text{ mod } h_2(x)$ ГМВ-матрицы, как показано в таблице 7.

Шаг 4в. По полученным на шаге 3в начальным фазовым элементам $\theta(j)$ формируются, через функцию след, столбцы ГМВ-матрицы:

$$F_{\text{ГМВ}} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix} \quad (22)$$

ТАБЛИЦА 7. Определение начальных фазовых элементов

$\lambda_u(j)$	λ^2	λ^5	λ	1	λ^3	λ^3	λ^4	λ^5	λ^6
	001	110	010	100	101	101	111	110	011
$\lambda(j)$	λ^3	λ^6	λ^5	λ^5	λ^2	λ^3	λ^5	λ^3	0
	101	011	110	110	001	101	110	101	000
$\theta(j)$	100	101	100	010	100	000	001	011	011
	$\theta^0 = 1$	θ^6	$\theta^0 = 1$	θ	$\theta^0 = 1$	θ^6	$\theta^0 = 1$	θ	$\theta^0 = 1$

Приемная сторона (декодирование).

Шаг 1д. По семи элементным замкнутым в кольцо двоичным последовательностям каждого столбца принятой ГМВ-матрицы (17), используя двойственный базис многочлена $h_2(x)$, находим начальные фазовые элементы $\theta(j)$ всех девяти столбцов, которые, при отсутствии ошибок или при наличии однократных или смежных двукратных ошибок в столбцах, будут иметь вид, представленный в последней строке таблицы 7.

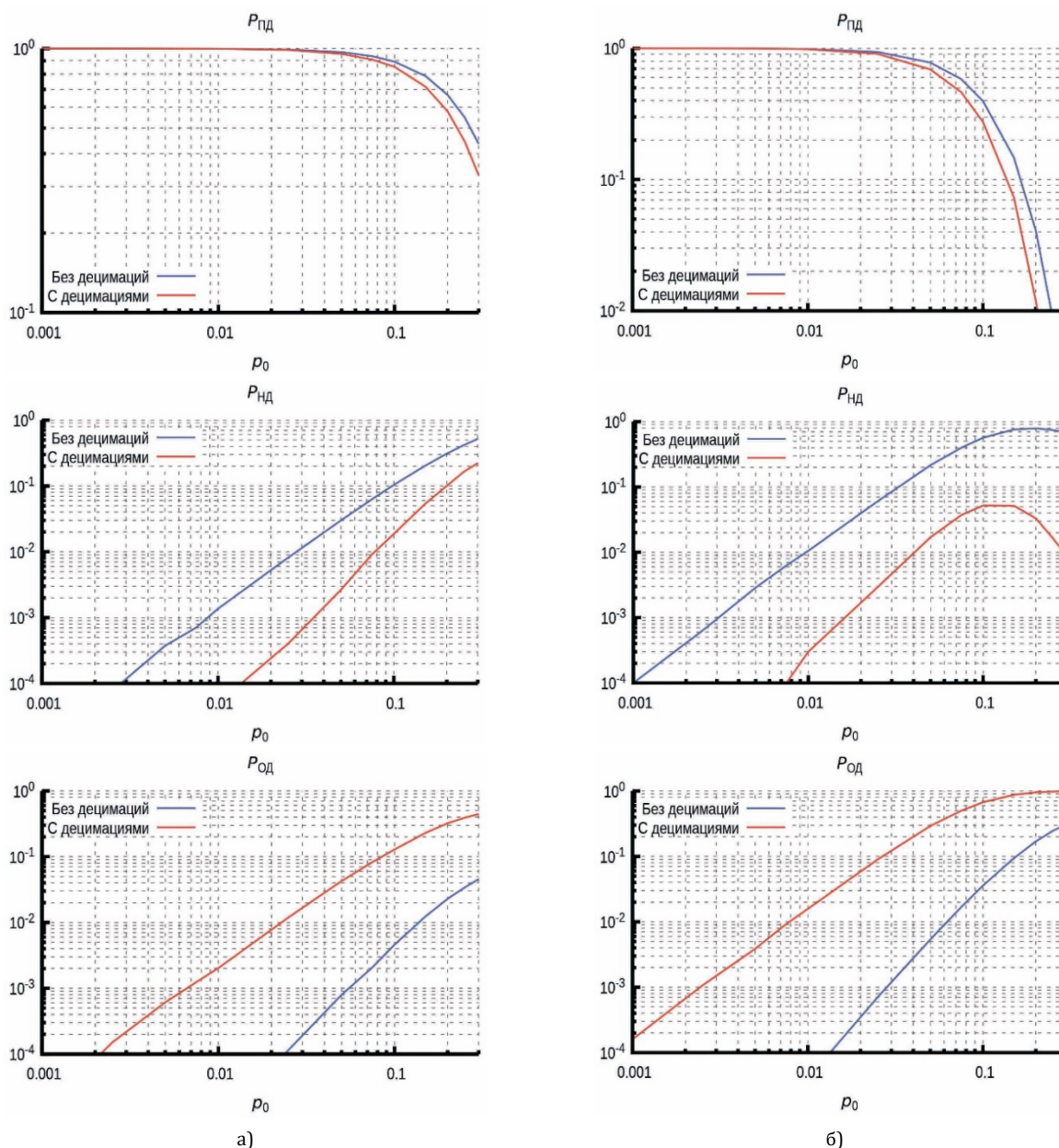


Рис. 3. Вероятностные характеристики при использовании мультипликативного алгоритма: а) декодирование отдельного информационного элемента λ^i (3 двоичных разряда); б) общая 24-разрядная информационная последовательность

Шаг 2д. Полученные на *шаге 1д* начальные фазовые элементы $\theta(j)$ столбцов ГМВ-матрицы (17) в виде векторов складываются поэлементно по mod 2 с двоичными векторами, соответствующими элементам $\lambda(j)$, являющимися начальными фазовыми элементами j -ых столбцов матрицы $F_{\text{мп}}$ (16), сформированной на приемной стороне из исходной М-последовательности по известному получателю начальному фазовому элементу $C \in GF(2^6)$. В результате будет получена информационная двоичная последовательность.

Сравнивая оба алгоритма, следует отметить, что скорость передачи данных у аддитивного алгоритма осталась такой же, как у мультипликативного при некотором снижении достоверности, которая, при той же вероятности ошибки в двоично-симметричном канале $p_0 = 10^{-2}$, составит без учета децимаций величину $Q^9 = (0,99856)^9 = 0,987$.

Выводы

В статье предложен новый вид псевдослучайных последовательностей – ГМВ-подобные последовательности. Они отличаются тем, что за счет изменения корреляционных характеристик, обеспечивают более высокую структурную скрытность по сравнению с классическими последовательностями ГМВ с двухуровневой периодической автокорреляционной функцией. Кроме того, за счет применения двойственного базиса при обработке таких последовательностей может быть существенно увеличено их количество и расширен диапазон скоростей передачи данных.

Применение ГМВ- и ГМВ-подобных последовательностей целесообразно как в существующих, так и в проектируемых широкополосных цифровых системах связи.

Список используемых источников

1. CDMA: прошлое, настоящее, будущее / под ред. Л.Е. Варакина и Ю.С. Шинакова. М.: МАС, 2003. 608 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. Golomb S.W., Gong G. Signal Design for Good Correlation: For Wireless Communication, Cryptography and Radar. Cambridge: Cambridge University Press, 2005. 438 p.
5. Golomb S.W. Two-valued sequences with perfect periodic autocorrelation // IEEE Transactions on Aerospace and Electronic Systems. 1992. Vol. 28. Iss. 2. PP. 383–386. DOI:10.1109/7.144563
6. No J.S. Generalization of GMW Sequences and No Sequences // IEEE Transactions on Information Theory. 1996. Vol. 42. Iss. 1. PP. 260–262.
7. Chung H., No J.S. Linear span of extended sequences and cascaded GMW sequences // IEEE Transactions on Information Theory. 1999. Vol. 45. Iss. 6. PP. 2060–2065. DOI:10.1109/18.782136
8. Мешковский К.А., Кренгель Е.И. Генератор псевдослучайных последовательностей Гордона, Милза, Велча // Техника средств связи. Серия: Техника радиосвязи. 1979. № 3. С. 17–30.
9. Кренгель Е.И. О числе псевдослучайных последовательностей Гордона, Милза, Велча // Техника средств связи. Серия: Техника радиосвязи. 1979. № 3. С. 31–34.
10. Стародубцев В.Г. Алгоритм формирования последовательностей Гордона – Милса – Велча // Известия высших учебных заведений. Приборостроение. 2012. Т. 55. № 7. С. 5–9.
11. Tong L., Chen F., Hua J., Meng L., Zhou S. Correlation Analysis and Realization of Gordon-Mills-Welch Sequences in Advanced Design System // Information Technology Journal. 2011. Vol. 10. Iss. 4. PP. 908–913. DOI:10.3923/itj.2011.908.913
12. Стародубцев В.Г. Формирование пятитричных последовательностей Гордона – Милса – Велча для систем передачи дискретной информации // Труды СПИИРАН. 2019. Т. 18. № 4. С. 912–948. DOI:10.15622/sp.2019.18.4.912-948
13. Юдачев С.С., Калмыков В.В. Ансамбли последовательностей GMW для систем с кодовым разделением каналов // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. 2012. №1. URL: <http://elibrary.ru/item.asp?id=17650851> (дата обращения 13.09.2019).
14. Стародубцев В.Г. Формирование последовательностей Гордона-Милса-Велча на основе регистров сдвига // Известия высших учебных заведений. Приборостроение. 2015. Т. 58. № 6. С. 451–457. DOI:10.17586/0021-3454-2015-58-6-451-457
15. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. Пер. с англ. / под ред. Р.Л. Добрушина и С.И. Самойленко. М.: Мир, 1976. 594 с.
16. Когновицкий О.С. Двойственный базис и его применение в телекоммуникациях. СПб.: Линк, 2009. 424 с.
17. Владимиров С.С., Когновицкий О.С. Обработка широкополосных последовательностей Гордона-Милса-Велча с использованием двойственного базиса на основе двух регистров // Труды учебных заведений связи. 2019. Т. 5. № 2. С. 49–58. DOI:10.31854/1813-324X-2019-5-2-49-58
18. Владимиров С.С., Когновицкий О.С. Малое множество последовательностей Касами и их декодирование на основе двойственного базиса // Труды учебных заведений связи. 2018. Т. 4. № 1. С. 22–31. DOI:10.31854/1813-324X-2018-1-22-31

* * *

FORMATION AND PROCESSING OF GMW-SIMILAR SEQUENCES BASED ON THE DUAL BASIS IN DIGITAL INFORMATION TRANSFER SYSTEMS

S. Vladimirov¹, O. Kognovitsky¹, V. Starodubtsev^{2,3}

¹The Bonch-Bruевич Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

²Mozhaisky Military Space Academy,
St. Petersburg, 197198, Russian Federation

³Saint Petersburg National Research University of Information Technologies, Mechanics and Optics,
St. Petersburg, 197101, Russian Federation

Article info

The article was received 28th October 2019

For citation: Vladimirov S., Kognovitsky O., Starodubtsev V. Formation and Processing of GMW-Similar Sequences Based on the Dual Basis in Digital Information Transfer Systems. *Proceedings of Telecommunication Universities*. 2019;5(4):16–27. (in Russ.) Available from: <https://doi.org/10.31854/1813-324X-2019-5-4-16-27>

Abstract: Algorithms for processing and determining, using a dual basis, the initial states of shift registers that form sequences similar to Gordon–Mills–Welch (GMW) sequences, which are characterized by their large number and higher structural secrecy comparing with the widely used M-sequences, are presented. It is shown that the proposed algorithms, unlike the known ones, make it possible to determine arbitrary initial states of shift registers and produce encoding of useful information, which expands the possibilities of using GMW-like sequences to solve various problems in the transmission of digital information in communication systems under electronic countermeasures.

Keywords: Gordon – Mills – Welch sequences, equivalent linear complexity, finite fields, primitive and irreducible polynomials, trace function, decimation, dual basis, shift register with linear feedback.

References

1. CDMA: *proshloe, nastoyashchee, budushchee* [CDMA: Past, Present, Future] / edited by L.E. Varakin and Y.S. Shinakov. Moscow: MAS Publ.; 2003. 608 p. (in Russ.)
2. Vishnevskiy V.M., Lyahov A.I., Portnoy S.L., Shahnovich I.V. *Shirokopolosnye besprovodnye seti peredachi informatsii* [Broadband Wireless Data Transmission Network]. Moscow: Tekhnosfera Publ.; 2005. 592 p. (in Russ.)
3. Sklar B. *Digital Communications: Fundamentals and Applications*. New York: Prentice Hall; 2001. 1079 p.
4. Golomb S.W., Gong G. *Signal Design for Good Correlation: For Wireless Communication, Cryptography and Radar*. Cambridge: Cambridge University Press; 2005. 438 p.
5. Golomb S.W. Two-valued sequences with perfect periodic autocorrelation. *IEEE Transactions on Aerospace and Electronic Systems*. 1992;28(2):383–386. Available from: <https://doi.org/10.1109/7.144563>
6. No J.-S. Generalization of GMW Sequences and No Sequences. *IEEE Transactions on Information Theory*. 1996;42(1):260–262.
7. Chung H., No J.S. Linear span of extended sequences and cascaded GMW sequences. *IEEE Transactions on Information Theory*. 1999;45(6):2060–2065. Available from: <https://doi.org/10.1109/18.782136>
8. Meshkovskiy K.A., Krengel E.I. Generator psevdosluchaynykh posleovatelnostey Gordona, Millsa, Velcha [Generator of Pseudo-Random Sequences of Gordon, Mills, Welch]. *Tekhnika sredstv svyazi. Seriya: Tekhnika radiosvyazi*. 1979;3:17–30. (in Russ.)
9. Krengel E.I. O chisle psevdosluchaynykh posleovatelnostey Gordona, Millsa, Velcha [On the Number of Pseudo-Random Sequences of Gordon, Mills, Welch]. *Tekhnika sredstv svyazi. Seriya: Tekhnika radiosvyazi*. 1979;3:31–34. (in Russ.)
10. Starodubtsev V.G. Algoritmy formirovaniya posleovatelnostey Gordona-Millsa-Velcha [The Algorithm of Formation of Gordon-Mills-Welch Sequences]. *Journal of Instrument Engineering*. 2012;55(7):5–9 (in Russ.)
11. Tong L., Chen F., Hua J., Meng L., Zhou S. Correlation Analysis and Realization of Gordon-Mills-Welch Sequences in Advanced Design System. *Information Technology Journal*. 2011;10(4):908–913. Available from: <https://doi.org/10.3923/itj.2011.908.913>
12. Starodubtsev V. G. Formation of Quinary Gordon-Mills-Welch Sequences for Discrete Information Transmission Systems. *SPIRAS Proceedings*. 2019;18(4):912–948 (in Russ.)
13. Yudachev S.S., Kalmykov V.V. Ensemble GMW sequences for systems with code channel separation. *Science and Education of Bauman MSTU*. 2012;1. (in Russ.) Available from: <http://elibrary.ru/item.asp?id=17650851> [Accessed 13th September 2019]
14. Starodubtsev V.G. Generation of Gordon-Mills-Welch sequences on the base of shift registers. *Journal of Instrument Engineering*. 2015;58(6):451–457 (in Russ.) Available from: <https://doi.org/10.17586/0021-3454-2015-58-6-451-457>
15. Peterson W.W., Weldon E.J. *Error-correcting codes*. Cambridge, Massachusetts and London: The MIT PRESS; 1972.
16. Kognovitskiy O.S. *Dvoistvennyiye bazy i ego primeneniye v telekommunikatsiyakh* [Dual Basis and Its Application in Telecommunications]. St. Petersburg: Link Publ.; 2009. 424 p. (in Russ.)
17. Vladimirov S., Kognovitskiy O. Dual Basis Based Processing of Wideband Gordon–Mills–Welch Sequences Based on Two Linear Registers. *Proceedings of Telecommunication Universities*. 2019;5(2):49–58. (in Russ.) Available from: <https://doi.org/10.31854/1813-324X-2019-5-2-49-58>
18. Vladimirov S., Kognovitskiy O. The Small Set of Kasami Sequences and their Decoding Based on the Dual Basis. *Proceedings of Telecommunication Universities*. 2018;4(1):22–31. (in Russ.) Available from: <https://doi.org/10.31854/1813-324X-2018-1-22-31>