

ФОРМИРОВАНИЕ КАСКАДИРОВАННЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОРДОНА–МИЛЛСА–ВЕЛЧА ДЛЯ СИСТЕМ ПЕРЕДАЧИ ЦИФРОВОЙ ИНФОРМАЦИИ

© 2024 г. В. Г. Стародубцев*

Военно-космическая академия им. А.Ф. Можайского,
ул. Ждановская, 13, Санкт-Петербург, 197198 Российская Федерация

*E-mail: vgstarod@mail.ru

Поступила в редакцию 22.06.2023 г.

После доработки 01.12.2023 г.

Принята к публикации 23.12.2023 г.

На основе модификации алгоритма определения вектора индексов децимации, являющегося основной составляющей метода синтеза последовательностей Гордона–Миллса–Велча (ГМВП), разработан алгоритм определения вектора индексов децимации $A(l, m, n, r_1, r_2)$ для синтеза каскадированных ГМВП (КГМВП) с периодом $N = 2^S - 1 = 2^{lmn} - 1$ ($l > 2$) в поле $GF((2^l)^m)^n$ путем суммирования последовательностей, формируемых на основе децимации по полученным индексам символов базисной M -последовательности (МП). Модификация алгоритма заключается в объединении векторов индексов децимации для различных сочетаний параметров r_1 и r_2 в выражении для результирующего вектора. Приведены результаты вычисления максимальных значений эквивалентной линейной сложности (ЭЛС) каскадированных $L_{\text{КГМВП}}$ и обычных $L_{\text{ГМВП}}$ ГМВП для периодов $2^{12} - 1 \leq N \leq 2^{36} - 1$. Показано, что ЭЛС каскадированных превышает ЭЛС обычных ГМВП, с увеличением периода выигрыш $B_S = L_{\text{КГМВП}} / L_{\text{ГМВП}}$ возрастает, и для периода $N = 2^{36} - 1$ он равен $B_{S=36} = 2.25$.

Ключевые слова: конечные поля, функция корреляции, M -последовательности, последовательности Гордона–Миллса–Велча, эквивалентная линейная сложность

DOI: 10.31857/S0033849424040093, **EDN:** JRLKZJ

ВВЕДЕНИЕ

Одним из направлений повышения структурной скрытности систем передачи цифровой информации, в которых используются сигналы с расширенным спектром, формируемые на основе псевдослучайных последовательностей, является применение последовательностей Гордона–Миллса–Велча (ГМВП), относящихся наряду с M -последовательностями (МП) к классу минимаксных последовательностей с двухуровневой периодической автокорреляционной функцией (ПАКФ) [1–6]. Повышение структурной скрытности обеспечивается за счет более высокой эквивалентной линейной сложности (ЭЛС) ГМВП по сравнению с МП [7–10]. Например, в [8, 9] приведены значения линейной сложности и объема множеств для обобщенных ГМВП и последовательностей, полученных Джоном Ноу. В [10] разработан метод формирования и получены выражения для определения ЭЛС недвоичных ГМВП.

Дальнейшим направлением повышения ЭЛС является применение каскадированных ГМВП (КГМВП). Рассмотрению данного вопроса посвящено большое количество публикаций [11–16]. В [11] построено новое семейство КГМВП, отличающееся большим значением ЭЛС

и характеризующееся тем, что во многих случаях взаимная корреляция с МП аналогичного периода является трехуровневой. В [12] показано, что линейная сложность КГМВП может быть определена аналогично сложности расширенных последовательностей, формируемых на основе идеально коррелированных последовательностей.

В [13, 14] решена задача определения циклических сдвигов КГМВП для трех типов параметров и определен критерий для определения данных сдвигов при изменении параметров. В [15] исследуются КГМВП произвольной характеристики. Приведены критерий и алгоритм построения каскадированных последовательностей, которые имеют гораздо большие линейные сложности, чем обычные ГМВП с одинаковыми периодами. В [16] получена рекуррентная формула для вычисления ЭЛС p -арных КГМВП без ограничений на параметры последовательности.

Каскадированные последовательности характеризуются более высокой ЭЛС $L_{\text{КГМВП}}$ по сравнению с ЭЛС $L_{\text{ГМВП}}$ обычных ГМВП. Выигрыш в структурной скрытности $B_S = L_{\text{КГМВП}} / L_{\text{ГМВП}}$ возрастает с увеличением периода последовательностей. Если для КГМВП с минимальным периодом $N = 2^{12} - 1$ выигрыш составляет $B_{S=12} = 216/196 = 1.12$, то для

периода $N = 2^{18} - 1$ выигрыш равен $B_{S=18} = 1.5$, а для периода $N = 2^{36} - 1$ выигрыш $B_{S=36} = 2.25$.

1. ПОСТАНОВКА ЗАДАЧИ

Двоичные КГМВП формируются в конечных полях с тройным расширением вида $GF((2^l)^m)^n = GF(2^S)$, ($S = lmn$, $l > 2$), вследствие чего их период является составным числом.

Для поля $GF((2^l)^m)^n$ символы c_i КГМВП с периодом $N = 2^S - 1$ определяются выражением [11, 13, 14]

$$c_i = \text{tr}_{l,1}[\text{tr}_{lm,l}[(\text{tr}_{lmn,lm}(\alpha^i))^r]^2], \quad (1)$$

где $\text{tr}_{a,b}(\cdot)$ — след элемента из поля $GF(2^a)$ в поле $GF(2^b)$; $\alpha \in GF(2^S)$ — примитивный элемент; $1 \leq r_1 < 2^{lm} - 1$, $1 \leq r_2 < 2^l - 1$ — натуральные числа, взаимно простые с порядками мультипликативных групп подполей $GF(2^{lm})$ и $GF(2^l)$ соответственно.

Эквивалентная линейная сложность обычных ГМВП в конечных полях с двойным расширением вида $GF((2^m)^n)$ определяется выражением [8, 12, 17]

$$L_{\text{ГМВП}} = mn^{g(r)}, \quad (2)$$

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

Для двоичных и недвоичных ГМВП разработаны методы формирования, не требующие построения конечных полей [10, 17, 18]. Основу методов составляют алгоритмы определения векторов индексов децимации $\mathbf{A}(m, n, r)$ базисной МП для суммируемых последовательностей, компоненты которых определяются непосредственно по значению параметра r . Однако известные алгоритмы не позволяют вычислять векторы индексов децимации КГМВП вследствие наличия двух параметров r_1 и r_2 в выражении (1).

Цель статьи — разработка модифицированного алгоритма определения векторов индексов децимации $\mathbf{A}(l, m, n, r_1, r_2)$ базисной МП для суммируемых последовательностей при формировании КГМВП.

Формирование как обычных ГМВП, так и КГМВП в соответствии с выражением (1) сопряжено со значительными вычислительными сложностями. Проведем сравнение требуемого числа операций $B_{\text{п}}$ и объема оперативной памяти $V_{\text{п}}$ при прямом формировании в соответствии с выражением (1) и при синтезе последовательностей в соответствии с разработанным модифицированным алгоритмом, характеризующим значениями $B_{\text{м}}$ и $V_{\text{м}}$.

Для формирования базисной МП с примитивным полиномом $f(x)$ или для построения поля $GF(2^S)$ требуется примерно $B_{\text{п1}} = B_{\text{м1}} \approx S \cdot 2^S$ операций сложения по mod 2. Для хранения элементов поля требуется $V_{\text{п1}} \approx S \cdot 2^S$ бит, для хранения символов базисной МП — $V_{\text{м1}} \approx 2^S$ бит.

Вычисления в конечных полях целесообразно проводить с помощью таблиц сложения и умножения. Для их составления необходимо выполнить $B_{\text{п2}} \approx (S+1)2^S$ операций. При этом требуемая память составляет $V_{\text{п2}} \approx S \cdot 2^{S+1}$ бит.

В соответствии с предлагаемым алгоритмом необходимо выполнить количество операций $B_{\text{м2}} \approx 2^{1+lm/2-2} + 2^{lm/2-1} + 2^{1,5lm-2}$ с объемом памяти $V_{\text{м2}} \approx 2S^2$ бит [18].

Для прямого формирования КГМВП в соответствии с (1) требуется $B_{\text{п3}} \approx (S+1)2^S$ операций сложения и умножения табличных значений. Примерно столько же операций требуется для формирования КГМВП в модифицированном алгоритме при суммировании децимированных последовательностей $B_{\text{м3}} \approx (S+1)2^S$.

Таким образом, при примерно равных затратах на операции непосредственного формирования МП и КГМВП разработанный алгоритм позволяет избежать построения таблиц сложения и умножения в конечном поле $GF(2^S)$ и обеспечивает выигрыш как в числе операций $W_B = B_{\text{п2}}/B_{\text{м2}}$, так и в объеме оперативной памяти $W_V = V_{\text{п2}}/V_{\text{м2}}$. Например, в поле $GF(2^{12})$ выигрыш в числе операций составляет $W_B \approx 270$, в объеме памяти $W_V \approx 1.4 \cdot 10^6$, а в поле $GF(2^{18})$ выигрыши равны $W_B \approx 1600$, $W_V \approx 3.8 \cdot 10^9$. Индекс B соответствует числу операций $B_{\text{п}}$ или $B_{\text{м}}$. Индекс V соответствует объему оперативной памяти $V_{\text{п}}$ или $V_{\text{м}}$.

2. АЛГОРИТМ ОПРЕДЕЛЕНИЯ ВЕКТОРА ИНДЕКСОВ ДЕЦИМАЦИИ

В качестве исходного алгоритма рассматривается алгоритм определения вектора индексов децимации $\mathbf{A}(m, n, r)$, разработанный в [18]. Число компонент вектора $\mathbf{A}(m, n, r) = (I_{d1}, I_{d2}, \dots, I_{dM})$ равно отношению ЭЛС ГМВП и МП, сформированных в поле $GF((2^m)^n)$

$$M_{\text{ГМВП}} = L_{\text{ГМВП}} / L_{\text{МП}} = n^{g(r)-1}. \quad (3)$$

В соответствии с алгоритмом для заданных значений параметров m, n, r определяется вектор $\mathbf{A}(m, n, r)$, компоненты которого используются для индексации суммируемых последовательностей при формировании ГМВП.

Модификация алгоритма заключается в представлении вектора $\mathbf{A}(l, m, n, r_1, r_2)$ для КГМВП в виде совокупности векторов индексов децимации типа $\mathbf{A}(m, n, r)$ для обычных ГМВП

$$\begin{aligned} \mathbf{A}(l, m, n, r_1, r_2) = \\ = [I_{di} \in \mathbf{A}(lmn, lm, I_{dj} r_1 \bmod (2^{lm} - 1))], \end{aligned} \quad (4)$$

где $I_{dj} \in \mathbf{A}(lm, l, r_2)$, $j = 1, 2, \dots, K = m^{g(r_2)-1}$.

Для каждого значения индекса j компоненты векторов индексов децимации $A(lmn, lm, I_{dj}r_1 \bmod(2^{lm}-1))$ относятся к различным циклотомическим классам размерности lmn [12], вследствие чего вектор $A(l, m, n, r_1, r_2)$ представляется в виде объединения векторов

$$A(l, m, n, r_1, r_2) = \bigcup_{j=1}^K A(lmn, lm, q_j), \quad (5)$$

где $q_j = I_{dj}r_1 \bmod(2^{lm}-1)$, $j=1, 2, \dots, K$.

Число компонент $M_{\text{КГМВП}}$ вектора индексов децимации $A(l, m, n, r_1, r_2)$ КГМВП определяется весами $g(q_j)$, т.е. числом единиц в двоичных представлениях числовых значений выражений $q_j = I_{dj}r_1 \bmod(2^{lm}-1)$

$$M_{\text{КГМВП}} = L_{\text{КГМВП}} / L_{\text{МП}} = \sum_{j=1}^K 2^{g(q_j)-1}. \quad (6)$$

С учетом того, что $L_{\text{МП}} = lmn$, ЭЛС КГМВП определяется выражением

$$L_{\text{КГМВП}} = lmn \sum_{j=1}^K 2^{g(q_j)-1}. \quad (7)$$

Алгоритм определения векторов индексов децимации $A(l, m, n, r_1, r_2)$ базисной МП для суммируемых последовательностей при формировании КГМВП формулируется следующим образом.

Шаг 1. Определение вектора индексов децимации для обычной ГМВП с периодом $N = 2^{lm}-1$ для заданных значений параметров l, m, r_2 в соответствии с алгоритмом, разработанным в [18]

$$A(lm, l, r_2) = [I_{d1}, I_{d2}, \dots, I_{dj}, \dots, I_{dK}], \quad K = m^{g(r_2)-1}. \quad (8)$$

Шаг 2. Вычисление значений выражений q_j и весов их двоичного представления $w_j = g(q_j)$

$$q_j = I_{dj}r_1 \bmod(2^{lm}-1), \quad j=1, 2, \dots, K. \quad (9)$$

Шаг 3. Определение векторов индексов децимации для значений q_j

$$A_j(lmn, lm, q_j) = [I_{dj1}, I_{dj2}, \dots, I_{dji}, \dots, I_{dji}, \dots, I_{dji}], \quad j=1, 2, \dots, K. \quad (10)$$

Шаг 4. Формирование результирующего вектора индексов децимации путем объединения векторов $A_j(lmn, lm, q_j)$ в соответствии с (5). Определение ЭЛС КГМВП в соответствии с (7).

В качестве примера в поле $GF(2^{12})$ с полиномом $f(x) = x^{12} + x^6 + x^4 + x + 1$ определим вектор индексов децимации для формирования КГМВП с периодом $N = 2^{12}-1 = 4095$ при следующих значениях параметров: $l = 3, m = 2, n = 2, r_1 = 5, r_2 = 3$. Отметим, что параметр r_1 может принимать 47 значений в интервале от 3 до 255, параметр $r_2 = 3$ принимает единственное значение (в пределах циклотомического класса).

Шаг 1. Определение вектора индексов децимации

$$A(lm, l, r_2) = A(6, 3, 3) = [I_{d1}, I_{d2}] = [3, 17], \quad K = 2.$$

Шаг 2. Вычисление значений выражений q_j и весов их двоичного представления $w_j = g(q_j)$ в соответствии с (9)

$$q_1 = 5 \cdot 3 \bmod 63 = 15; \quad 15_{10} = 1111_2; \quad w_1 = g(q_1) = 4;$$

$$q_2 = 5 \cdot 17 \bmod 63 = 22; \quad 22_{10} = 10110_2; \quad w_2 = g(q_2) = 3.$$

Шаг 3. Определение векторов индексов децимации $A_j(lmn, lm, q_j)$

$$A_1(lmn, lm, q_1) = A_1(12, 6, 15) = [15, 141, 267, 393, 519, 645, 771, 897], \quad K_1 = 8;$$

$$A_2(lmn, lm, q_2) = A_2(12, 6, 22) = [22, 148, 274, 400], \quad K_2 = 4.$$

Здесь и далее компоненты векторов $A_j(lmn, lm, q_j)$ заменяются на минимальные значения в своих циклотомических классах, что соответствует одинаковым значениям символов базисной МП при ее децимации $A_1(12, 6, 15) = [15, 141, 177, 291, 57, 165, 51, 39], \quad K_1 = 8;$
 $A_2(12, 6, 22) = [11, 37, 137, 25], \quad K_2 = 4.$

Шаг 4. Определение результирующего вектора индексов децимации при объединении векторов $A_1(12, 6, 15)$ и $A_2(12, 6, 22)$

$$A(l, m, n, r_1, r_2) = A(3, 2, 2, 5, 3) = [15, 141, 177, 291, 57, 165, 51, 39, 11, 37, 137, 25].$$

Тогда символы КГМВП определяются выражением $c_i = d_{15i} + d_{141i} + d_{177i} + d_{291i} + d_{57i} + d_{165i} + d_{51i} + d_{39i} + d_{11i} + d_{37i} + d_{137i} + d_{25i}$,

где $i = 0, 1, \dots, 2^S-2$; умножение в индексах выполняется по $\bmod(N = 2^{12}-1 = 4095)$; суммирование значений символов d_{ji} выполняется по $\bmod 2$.

Определение ЭЛС КГМВП

$$L_{\text{КГМВП}} = 12(2^3 + 2^2) = 144.$$

Отметим, что ЭЛС обычной ГМВП при значении $r_1 = 5$ равно $L_{\text{ГМВП}} = 24$.

В качестве второго примера определим вектор индексов децимации для формирования КГМВП с периодом $N = 2^{18}-1 = 262143$ при следующих значениях параметров: $l = 3, m = 3, n = 2, r_1 = 11, r_2 = 3$.

Шаг 1. Определение вектора индексов децимации

$$A(lm, l, r_2) = A(9, 3, 3) = [I_{d1}, I_{d2}, I_{d2}] = [3, 5, 17],$$

$$K = 3^{2-1} = 3.$$

Шаг 2. Вычисление значений выражений q_j и весов их двоичного представления $w_j = g(q_j)$:

$$q_1 = 11 \cdot 3 \bmod 511 = 33; \quad 33_{10} = 100001_2; \quad w_1 = g(q_1) = 2;$$

$$q_2 = 11 \cdot 5 \bmod 511 = 55; \quad 55_{10} = 110111_2; \quad w_2 = g(q_2) = 5;$$

$$q_3 = 11 \cdot 17 \bmod 511 = 187; \quad 187_{10} = 10111011_2; \quad w_3 = g(q_3) = 6.$$

Таблица 1. Формирование КГМВП с периодом $N = 2^{18} - 1 = 262143$ для вектора $A(l, m, n, r_1, r_2) = A(3, 3, 2, 5, 3)$ для трех ПСП $F_j = 17, 55, 187$

F_{17}		F_{55}		F_{187}	
Символ d_i	Значение	Символ d_i	Значение	Символ d_i	Значение
d_0	0	d_0	0	d_0	0
d_{17}	0	d_{55}	1	d_{187}	1
d_{34}	0	d_{110}	1	d_{374}	1
d_{51}	1	d_{165}	1	d_{561}	0
d_{68}	0	d_{220}	1	d_{748}	1
d_{85}	1	d_{275}	1	d_{935}	0
d_{102}	1	d_{330}	1	d_{1122}	0
d_{119}	1	d_{385}	0	d_{1309}	1
d_{136}	0	d_{440}	1	d_{1496}	1
d_{153}	1	d_{495}	0	d_{1683}	1
d_{170}	0	d_{550}	1	d_{1870}	0
d_{187}	1	d_{605}	1	d_{2057}	1
d_{204}	1	d_{660}	1	d_{2244}	0
d_{221}	1	d_{715}	0	d_{2431}	1

Шаг 3. Определение векторов индексов децимации $A_j(lmn, lm, q_j)$:

$$A_1(18, 9, 33) = [33, 17], K_1 = 2;$$

$$A_2(18, 9, 55) = [55, 1077, 2099, 3121, 1249, 9253, 4485, 8459, 369, 5393, 2441, 4371, 227, 1305, 397, 283], K_2 = 16;$$

$$A_3(18, 9, 187) = [187, 1209, 4275, 5297, 5473, 9385, 10435, 8613, 2481, 17561, 9413, 17737, 4451, 18633, 6369, 2281, 237, 4325, 3281, 12613, 1385, 10569, 2259, 8525, 437, 6481, 1237, 4437, 363, 2393, 215, 349], K_3 = 32.$$

Шаг 4. Определение результирующего вектора индексов децимации при объединении векторов:

$$A(3, 3, 2, 5, 3) = A_1(18, 9, 33) \cup A_2(18, 9, 55) \cup A_3(18, 9, 187). \quad (11)$$

Определение ЭЛС КГМВП $L_{\text{КГМВП}} = 18(2 + 2^4 + 2^5) = 900$. Отметим, что ЭЛС обычной ГМВП с периодом $N = 2^{18} - 1 = 262143$ при значении $r_1 = 11$ равно $L_{\text{ГМВП}} = 72$.

Для непосредственного формирования КГМВП с учетом (11) необходимо построить базисную МП, определить символы псевдослучайных последовательностей (ПСП) F_j , получаемые путем децимации МП по индексам, которые являются компонентами вектора индексов децимации $A(l, m, n, r_1, r_2)$, и провести суммирование по mod 2 символов данных последовательностей [18]. Отметим, что при децимации символов базисной МП по различным индексам могут быть сформированы как другие МП с таким же периодом, так и ПСП с периодами, являющимися делителями периода базисной МП.

В результате суммирования формируется последовательность, обладающая двухуровневой периодической автокорреляционной функцией и являющаяся КГМВП.

Для рассмотренного примера в качестве базисной МП при формировании КГМВП с периодом $N = 2^{18} - 1 = 262143$ используется МП с проверочным полиномом $h_{\text{МП}}(x) = x^{18} + x^7 + 1$, символы которой определяются выражением

$$d_{18+i} = d_{0+i} + d_{7+i}, i = 0 \dots 262124, \quad (12)$$

где суммирование символов выполняется по mod 2 с начальными символами $d_0, d_1, \dots, d_{17}$, равными соответственно 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0.

При данных значениях начальных символов базисная МП формируется в каноническом виде и соответствует выражению (1) при $r_1 = r_2 = 1$. В табл. 1 представлены сегменты длиной 14 символов трех из пятидесяти суммируемых последовательностей F_j с индексами 17, 55, 187. Остальные 47 последовательностей вычисляются аналогично. Таким образом, для формирования КГМВП в соответствии с (11) требуется знать только значения символов d_i базисной МП и вектор индексов децимации.

Таблица 2. Основные параметры КГМВП для вектора $A(3, 3, 2, r_1, 3)$

r_1	$g(r_1)$	q_1	$g(q_1)$	q_2	$g(q_2)$	q_3	$g(q_3)$	$M_{\text{КГМВП}}$	$M_{\text{ГМВП}}$	$L_{\text{КГМВП}}$	$L_{\text{ГМВП}}$
3	2	9	2	15	4	51	4	18	2	324	36
5	2	15	4	25	3	85	4	20	2	360	36
9	2	27	4	45	4	153	4	24	2	432	36
11	3	33	2	55	5	187	6	50	4	900	72
39	4	117	5	195	4	152	3	28	8	504	144
41	3	123	6	205	5	186	5	64	4	1152	72
43	4	129	2	215	6	220	5	50	8	900	144
191	7	62	5	444	6	181	5	64	64	1152	1152
223	7	158	5	93	5	214	5	48	64	864	1152
239	7	206	5	173	5	486	6	64	64	1152	1152
255	8	254	7	253	7	247	7	192	128	3456	2304

Для других значений параметра r_1 при формировании вектора $A(3,3,2, r_1, 3)$ вычисляются значения индексов q_j и векторов $A_j(lmn, lm, q_j)$ в соответствии с (9) и (10). В табл. 2 для одиннадцати из сорока семи значений r_1 приведены значения q_j , их веса $w_j = g(q_j)$, а также число суммируемых последовательностей $M_{\text{КГМВП}}$ и ЭЛС $L_{\text{КГМВП}}$ каскадированных и обычных ГМВП.

В большинстве случаев число суммируемых последовательностей $M_{\text{КГМВП}}$ и ЭЛС $L_{\text{КГМВП}}$ КГМВП превышает аналогичные значения обычных ГМВП. В рассмотренном примере максимальное значение ЭЛС КГМВП $L_{\text{КГМВПmax}} = 3456$ достигается при $r_1 = 255$ и превышает аналогичное значение обычной ГМВП, при этом выигрыш составляет

$$B_{S=18} = L_{\text{КГМВПmax}} / L_{\text{ГМВПmax}} = M_{\text{КГМВПmax}} / M_{\text{ГМВПmax}} = 3456/2304 = 1.5.$$

Результаты вычислений характеристик каскадированных и обычных ГМВП для периодов $2^{12}-1 \leq N \leq 2^{36}-1 = 68719476735$ для различных значений параметров l, m, n, r_1, r_2 ($l = 3, 4$) приведены в табл. 3 При $lm = 6$ параметр r_1 может принимать пять значений $r_1 = 5, 11, 13, 23, 31$, при $lm = 8$ — пятнадцать значений в диапазоне от 7 до 127, при $lm = 9$ — сорок семь значений в диапазоне от 3 до 255 и при $lm = 12$ — сто сорок три значения в диапазоне от 11 до 2047. Параметр r_2 принимает единственное значение $r_2 = 3$ при $l = 3$ и $r_2 = 7$ при $l = 4$, что определяется наличием только двух примитивных полиномов в подполях $GF(2^3)$ и $GF(2^4)$.

Анализ табл. 3 показал, что максимальное число суммируемых последовательностей $M_{\text{КГМВПmax}}$ при формировании КГМВП зависит только от параметров l, m и не зависит от параметра n . Выигрыш

в ЭЛС B_S возрастает при увеличении lm от $B_S = 1.13$ при $lm = 6$ до $B_S = 2.5$ при $lm = 12$.

При значении $l = 5$ параметр r_2 может принимать пять значений $r_2 = 3, 5, 7, 11, 15$, а при $l = 6$ параметр r_2 может принимать тоже пять значений $r_2 = 5, 11, 13, 23, 31$. Для каждого допустимого значения параметра r_2 может быть составлена таблица, аналогичная табл. 3.

Например, при $l = 5, m = 2, n = 2, r_1 = 125, r_2 = 15$ достигается максимальное значение ЭЛС КГМВП $L_{\text{КГМВПmax}} = 8160$, которое в 1.59 раз превышает максимальное значение ЭЛС обычной ГМВП.

ЗАКЛЮЧЕНИЕ

Таким образом, разработан алгоритм определения вектора индексов децимации $A(l, m, n, r_1, r_2)$ базисной МП для формирования КГМВП с периодом $N = 2^S - 1 = 2^{lmn} - 1$ ($l > 2$), формируемых в поле $GF((2^l)^m)^n$. Разработка алгоритма выполнена на основе модификации известного алгоритма определения вектора индексов децимации, являющегося основной составляющей метода синтеза ГМВП [17, 18]. Модификация заключается в двухэтапном применении известного алгоритма определения вектора индексов децимации $A(m, n, r)$. На первом этапе алгоритм применяется для определения вектора $A(lm, l, r_2)$, при этом полученные индексы децимации I_{dj} с учетом параметра r_1 используются для вычисления вспомогательных параметров q_j ($1 \leq j \leq m^{g(r_2)-1}$). Данные параметры являются аналогами параметра r и используются на втором этапе при вычислении векторов $A_j(lmn, lm, q_j)$, объединение которых позволяет определить результирующий вектор индексов децимации $A(l, m, n, r_1, r_2)$.

Формирование КГМВП выполняется путем суммирования по mod 2 последовательностей,

Таблица 3. Основные параметры КГМВП с периодами $2^{12}-1 \leq N \leq 2^{36}-1$

$N = 2^S - 1$	1	m	n	$M_{\text{Кmax}}^*$	M_{max}	$L_{\text{Кmax}}^{**}$	L_{max}	B_S
4095	3	2	2	18	16	216	192	1.13
262143	3	2	3	18	16	324	288	1.13
16777 215	3	2	4	18	16	432	384	1.13
1073 741823	3	2	5	18	16	540	480	1.13
262143	3	3	2	192	128	3456	2304	1.5
134217 727	3	3	3	192	128	5184	3456	1.5
68719 476735	3	3	4	192	128	6912	4608	1.5
16777 215	3	4	2	2048	1024	49152	24576	2.0
68719 476735	3	4	3	2048	1024	73728	36864	2.0
65535	4	2	2	92	64	1472	1024	1.44
16777 215	4	2	3	92	64	2208	1536	1.44
4294 967295	4	2	4	92	64	2944	2048	1.44
16777 215	4	3	2	2304	1024	55296	24576	2.25
68719 476735	4	3	3	2304	1024	82944	36864	2.25

* $M_{\text{КГМВПmax}}$, ** $L_{\text{КГМВПmax}}$

образованных децимацией символов базисной МП по индексам, являющимся компонентами вектора $\mathbf{A}(l, m, n, r_1, r_2)$.

Получены выражения для вычисления ЭЛС и числа суммируемых последовательностей при формировании КГМВП. Приведены результаты вычислений максимальных значений ЭЛС и числа суммируемых последовательностей для КГМВП с периодами $2^{12}-1 \leq N \leq 2^{36}-1$. Выигрыш в максимальном значении ЭЛС по сравнению с обычными ГМВП с увеличением произведения lm возрастает от 1.13 при $lm = 6$ до 2.5 при $lm = 12$.

Полученные результаты могут найти применение в помехозащищенных системах передачи цифровой информации, в которых используются фазоманипулированные сигналы с расширенным спектром и к которым предъявляются повышенные требования как по структурной скрытности, так и по корреляционным свойствам.

СПИСОК ЛИТЕРАТУРЫ

1. Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В. Широкополосные беспроводные сети передачи информации. М.: Техносфера, 2005.
2. Golomb S.W., Gong G. Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar. Cambridge: Univ. Press, 2005.
3. Инатов В.П. Широкополосные системы и кодовое разделение сигналов. Принципы и приложения. М.: Техносфера, 2007.
4. Склад Б. Цифровая связь. Теоретические основы и практическое применение. 2-е изд. / Пер. с англ. М.: Вильямс, 2003.
5. CDMA: прошлое, настоящее, будущее. М.: МАС, 2003.
6. Инатов В.П. Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992.
7. Golomb S.W. // IEEE Trans. 1992. V. AES-28. № 2. P. 383.
8. No Jong-Seon. // IEEE Trans. 1996. V. IT-42. № 1. P. 260.
9. Zhu J., Cheng F., Tong L. et al. // 2nd Int. Conf. on Information Science and Engineering. Hangzhou. 4–6 Dec. 2010. N.Y.: IEEE, 2010. P. 2107. <https://doi.org/10.1109/ICISE.2010.5691504>
10. Стародубцев В.Г. // ПЭ. 2023. Т. 68. № 7. С. 676.
11. Klapper A., Chan A., Goresky M. // IEEE Trans. 1993. V. IT-39. № 1. P. 177.
12. Chung H.B., No J.S. // IEEE Trans. 1999. V. IT-45. № 6. P. 2060.
13. Gong G., Dai Z.D., Solomon W. Golomb S.W. // IEEE Trans. 2000. V. IT-46. № 2. P. 474.
14. Golomb S.W., Gong G., Dai Z.D. // Discrete Mathematics. 2000. V. 219. P. 279.
15. Gong G. // IEEE Trans. 1996. V. IT-42. № 1. P. 263.
16. Tang X. // Science China Inform. Sci. 2007. V. 50. № 4. P. 551.
17. Стародубцев В.Г. // ПЭ. 2020. Т. 65. № 2. С. 15.
18. Стародубцев В.Г. // ПЭ. 2021. Т. 66. № 4. С. 380.
19. Пумперсон У., Уэлдон Э. Коды, исправляющие ошибки. М.: Мир, 1976. Ipatov V.P. Spread Spectrum and CDMA. Principles and Applications. New York: John Wiley and Sons Ltd. 2005.

FORMATION OF CASCADED GORDON–MILLS–WELCH SEQUENCES FOR DIGITAL INFORMATION TRANSMISSION SYSTEMS

V. G. Starodubtsev*

Mozhaisky Military Space Academy,
Zhdanovskaya Street, 13, Saint Petersburg, 197198 Russian Federation
*E-mail: vgstarod@mail.ru

Received June 22, 2023; revised December 1, 2023; accepted December 23, 2023

Based on the modification of the algorithm for determining the decimation index vector, which is the main component of the Gordon–Mills–Welch sequence (GMWS) synthesis method, an algorithm for determining the decimation index vector $\mathbf{A}(l, m, n, r_1, r_2)$ for the synthesis of cascaded GMWS (CGMWS) with a period $N = 2^S - 1 = 2^{lmn} - 1$ ($l > 2$) in the $GF[(2^l)^m]^n$ field by summing the sequences formed on the basis of decimation according to the obtained indices of the symbols of the basic M-sequence (MS). The modification of the algorithm consists in combining the vectors of the decimation indices for various combinations of the parameters r_1 and r_2 in the expression for the resulting vector. The results of calculating the maximum values of the equivalent linear complexity (ELC) of cascaded L_{CGMWS} and conventional L_{GMWS} GMWSs for periods $2^{12}-1 \leq N \leq 2^{36}-1$ are presented. It is shown that the ELC of cascaded exceeds the ELC of conventional GMWSs, with an increase in the period the gain $B_S = L_{\text{CGMWS}}/L_{\text{GMWS}}$ increases, and for the period $N = 2^{36}-1$ it is equal to $B_{S=36} = 2.25$.

Keywords: finite fields, correlation function, M-sequences, Gordon–Mills–Welch sequences, equivalent linear complexity