РАДИОТЕХНИКА И ЭЛЕКТРОНИКА, 2021, том 66, № 4, с. 380–385

ТЕОРИЯ И МЕТОДЫ ОБРАБОТКИ СИГНАЛОВ

УДК 519.725;512.62

АЛГОРИТМ ФОРМИРОВАНИЯ СВЕРХДЛИННЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОРДОНА–МИЛЛСА–ВЕЛЧА

© 2021 г. В. Г. Стародубцев[1, 2, *]

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

[2]*Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Кронверкский просп., 49, Санкт-Петербург, 197101 Российская Федерация*

**E-mail: vgstarod@mail.ru*

Поступила в редакцию 03.07.2020 г.
После доработки 30.08.2020 г.
Принята к публикации 04.09.2020 г.

На основе модификации алгоритма определения полиномов-сомножителей $h_{c_i}(x)$ проверочного полинома $h_{\text{ГМВП}}(x)$, являющегося главной составляющей метода синтеза последовательностей Гордона–Миллса–Велча (ГМВП), разработана программная реализация алгоритма формирования сверхдлинных последовательностей ГМВП, обладающих двухуровневой периодической автокорреляционной функцией, высокой структурной скрытностью и формируемых над конечным полем с двойным расширением $GF(2^S) = GF[(2^m)^n]$. В модифицированном алгоритме для различных значений параметра n определены выражения для числа операций при вычислении вектора альтернатив, из которого формируется вектор индексов децимации. Данные выражения также выступают в качестве верхних граничных оценок для числа суммируемых последовательностей. Для формирования сверхдлинных ГМВП с периодами от $N = 2^{12} - 1 = 4095$ до $N = 2^{20} - 1 = 1048575$ получены наборы векторов индексов децимации для допустимых значений параметров m и n.

DOI: 10.31857/S0033849421030189

В современных системах передачи цифровой информации (СПЦИ), включающих системы связи и управления, системы навигации и радиолокации, широкое применение получили сигналы с расширенным спектром (СРС), формируемые на основе псевдослучайных последовательностей (ПСП) [1–4]. В качестве ПСП используются последовательности, обладающие как хорошими корреляционными свойствами, так и высокой структурной скрытностью, одним из показателей которой является эквивалентная линейная сложность (ЭЛС).

Выбор ЭЛС в качестве показателя для оценки структурной скрытности последовательностей Гордона–Миллса–Велча (ГМВП) определяется тем, что сравнение осуществляется с М-последовательностями (МП), которые обладают аналогичными автокорреляционными свойствами, но характеризуются меньшей линейной сложностью. Использование других показателей, например эквивалентной квадратичной сложности, целесообразно при сравнении с нелинейными ПСП, такими как последовательности де Брейна, двоичные последовательности на основе бент-функций, составные нелинейные ПСП [1, 5, 6]. Показатель сложности по Лемпелю-Зиву, впервые предложенный в [7], определяется на основе учета повторяющихся сегментов в последовательности и является основой для таких алгоритмов последовательного сжатия как LZ77, LZSS, LZW.

М-последовательности получили большое распространение в СПЦИ благодаря прежде всего их корреляционным свойствам, а также достаточно простому алгоритму формирования как самих последовательностей, так и синтезируемых на их основе производных последовательностей, таких как последовательности Голда, малого и большого множеств Касами и др. [8–11]. Например, в навигационной системе ГЛОНАСС в специальном режиме используются укороченные ПСП на основе МП с периодом $N = 2^{14} - 1$, а в системе GPS МП с периодами $N = 2^{14} - 1$ в режиме общего доступа и с периодом $N > 2^{42}$ в специальном режиме [12, 13].

Однако МП обладают недостаточной линейной сложностью. Среди последовательностей, обладающих наряду с МП двухуровневой ПАКФ, можно выделить ГМВП, которые имеют более

высокую структурную скрытность по сравнению с МП [14, 15]. Например, для периода $N = 2^6 - 1$ выигрыш составляет два раза, а для периода $N = 2^{20} - 1$ – уже 256 раз [14, 16].

Алгоритмы формирования сверхдлинных ГМВП, которые обладали бы достаточно низкой вычислительной сложностью, в известной нам литературе отсутствуют. Решение данной задачи может быть реализовано на основе метода формирования ГМВП, разработанного в [17].

Цель статьи – разработка алгоритма формирования сверхдлинных ГМВП на основе модификации алгоритма определения полиномов-сомножителей $h_{ci}(x)$ проверочного полинома $h_{\text{ГМВП}}(x)$.

Алгоритм формирования сверхдлинных ГМВП в качестве одного из шагов включает алгоритм определения полиномов-сомножителей $h_{ci}(x)$ проверочного полинома ГМВП $h_{\text{ГМВП}}(x)$.

Научная новизна состоит в модификации алгоритма определения полиномов-сомножителей $h_{ci}(x)$, рассмотренного в [17]. Модификация заключается в том, что при вычислении полиномов $h_{ci}(x)$ используется только один элемент β^r из циклотомического класса, принадлежащий подполю $GF(2^m)$. При этом наряду с перечнем полиномов $h_{ci}(x)$ для программной реализации алгоритма формирования сверхдлинных ГМВП применяется понятие вектора индексов децимации $\mathbf{A}_{m,n,r}$, который необходим для синтеза суммируемых последовательностей, получаемых путем децимации символов базисной МП.

Формирование двоичных ГМВП с периодом $N = 2^{mn} - 1$ осуществляется над конечными полями с двойным расширением $GF[(2^m)^n] = GF(2^S)$, $S = mn$. Символы d_i ГМВП определяются выражением [2, 15]

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

где $\mathrm{tr}_{a,b}(\cdot)$ – след элемента из поля $GF(2^a)$ в поле $GF(2^b)$; $\alpha \in GF[(2^m)^n]$ – примитивный элемент; r – натуральное число, взаимно простое с порядком мультипликативной группы поля $GF(2^m)$, равным $2^m - 1$.

ЭЛС двоичных ГМВП определяется выражением [15, 17]

$$l_s = mn^{g(r)}, \tag{2}$$

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

В алгоритме определения полиномов-сомножителей $h_{ci}(x)$ проверочного полинома ГМВП, разработанного в [17], при вычислении полиномов, из которых производился выбор сомножителей $h_{ci}(x)$, использовались все элементы циклотомического класса для элемента $\beta^r = (\mathrm{tr}_{mn,m}(\alpha^i))^r$, принадлежащего подполю $GF(2^m)$, имеющие нечетные показатели степени. Кроме того, при каждой реализации алгоритма число операций заранее не было известно и определялось в зависимости от значения ЭЛС.

В модифицированном алгоритме при вычислениях в полях $GF[(2^m)^n]$ и $GF(2^m)$ используется только параметр r в выражении (1). Вместо термина “вектор сомножителей” используется термин “вектор индексов децимации $\mathbf{A}_{m,n,r}$”. Данный вектор вычисляется на основе вектора альтернатив $\mathbf{B}_{m,n,r}$, который определяется на начальных шагах алгоритма. При этом число операций T, необходимых для определения вектора альтернатив, определяется соотношением параметров m и n. Анализ результатов вычислений, полученных в соответствии с исходным алгоритмом, показал, что все индексы децимации, являющиеся компонентами вектора индексов децимации, могут быть определены путем прибавления к параметру r значений вспомогательного параметра k_i [17]

$$k_i = 2i(2^m - 1), \quad i = 0, 1, 2, \ldots, T. \tag{3}$$

Число операций T для различных значений параметра n определяется путем деления порядка мультипликативной группы поля $GF[(2^m)^n]$ на удвоенное значение параметра k_1 с учетом того, что искомые индексы децимации расположены в первой половине мультипликативной группы. Выражение для числа операций T имеет вид

$$T = \begin{cases} 2^{m-2} & \text{при } n = 2; \\ \{(2^{2m-2} + 2^{m-2}) & \text{при } n = 3; \\ (2^{2m} + 1)(2^m + 1)/4 & \text{при } n = 4. \end{cases} \tag{4}$$

Например, в поле $GF[(2^m)^n] = GF(2^{12})$ число операций определяется следующим образом:

при $m = 6$, $n = 2$: $T = 2^{m-2} = 16$;

при $m = 4$, $n = 3$: $T = 2^{2m-2} + 2^{m-2} = 68$;

при $m = 3$, $n = 4$: $T = (2^{2m} + 1)(2^m + 1)/4 = 146.25 \approx 146$.

В результате вычислений получаем $(T + 1)$ чисел (с учетом значения r при $i = 0$), которые являются компонентами вектора альтернатив $\mathbf{B}_{m,n,r}$ и которые включают все компоненты вектора индексов децимации $\mathbf{A}_{m,n,r}$. Для выбора компонент вектора альтернатив $\mathbf{B}_{m,n,r}$, являющихся одновременно компонентами вектора $\mathbf{A}_{m,n,r}$, требуется представить числа в двоичной системе счисления, выбрать те из них, которые удовлетворяют функции $g(r)$, и определить минимальные элементы в соответствующих циклотомических классах.

Таким образом, параметр T можно рассматривать как верхнюю границу числа суммируемых последовательностей при формировании ГМВП. Для значений параметра $n > 2$ данная граница до-

статочно грубая. Для значения $n = 2$ данная граница более точная и достигается в случае, когда параметр $r = 2^{m-1}-1$.

Отличие модифицированного алгоритма заключается в замене шагов 2–5 в алгоритме, разработанном в [17], на шаги 2–4.

Шаг 2. Определение в соответствии с (3) вектора альтернатив $\mathbf{B}_{m,n,r}$, содержащего $(T + 1)$ чисел, соответствующих индексам децимации, из которых выбираются компоненты вектора $\mathbf{A}_{m,n,r}$.

Шаг 3. Представление компонент вектора альтернатив $\mathbf{B}_{m,n,r}$ в двоичной системе счисления и выбор M чисел, которые соответствуют функции $g(r)$.

Шаг 4. Определение минимальных элементов в выбранных циклотомических классах и формирование вектора индексов децимации

$$\mathbf{A}_{m,n,r} = (I_{d1}, I_{d2}, \ldots, I_{dM}).$$

Вектор индексов децимации $\mathbf{A}_{m,n,r}$ содержит M компонент, однозначно определяемых для фиксированных значений параметров m, n и r.

Например, при формировании ГМВП с периодом $N = 4095$ и ЭЛС $l_s = 80$ в поле $GF[(2^6)^2]$ в соответствии с (4) параметр $T = 16$. Для значения $r = 11_{10} = 1011_2$, $g(r) = 3$ вектор альтернатив содержит 17 компонент и имеет вид

$$\mathbf{B}_{6,2,11} = (11, 137, 263, 389, 515, 641, 767, 893, 1019, 1145, 1271, 1397, 1523, 1649, 1775, 1901, 2027).$$

Из 17 компонент только четыре имеют $g(r) = 3$: 11, 137, 515, 641, тогда вектор индексов децимации равен $\mathbf{A}_{6,2,11} = (11, 137, 25, 37)$. При этом проверочный полином ГМВП имеет вид $h_{\text{ГМВП}}(x) = h_{11}(x)h_{137}(x)h_{25}(x)h_{37}(x)$. Здесь и в дальнейшем нижние цифровые индексы, используемые для обозначения полиномов, соответствуют минимальным показателям степени корней данных полиномов.

Для формирования сверхдлинных ГМВП целесообразно использовать программный способ реализации алгоритма. Это определяется тем, что для его выполнения необходим только один примитивный полином степени $S = mn$ для формирования базисной МП и вектор индексов децимации $\mathbf{A}_{m,n,r}$, с помощью которого формируются суммируемые последовательности из базисной МП.

В табл. 1 приведены примитивные полиномы с корнями $\alpha^1 = a$ в полях $GF(2^S)$ [18]. Также показаны начальные символы $C_0C_1\ldots C_{S-2}C_{S-1}$, необходимые для формирования МП с периодами $N = 2^S - 1$ в канонической форме, которые были получены в соответствии с методикой определения начальных состояний [19].

Формирование массива базисной МП осуществляется на основании примитивного полинома $h_{\text{МП}}(x) = h_1(x) = x^S + h_{S-1}x^{S-1} + \ldots + h_1x + 1$ в соответствии с выражением

$$\begin{aligned} C[S+i] &= C[0+i] + h_1C[1+i] + \ldots + \\ &+ h_{S-1}C[S-1+i], \quad i = 0\ldots N-S-1, \end{aligned} \tag{5}$$

где суммирование символов выполняется по mod 2.

Программная реализация алгоритма формирования сверхдлинных ГМВП.

Шаг 1. Ввод исходных данных (в соответствии с модифицированным алгоритмом).

Шаг 2. Формирование одномерного массива символов базисной МП в канонической форме $C[i]$, $i = 0\ldots N-1$ в соответствии с (5) и с учетом начальных символов $C_0C_1\ldots C_{S-2}C_{S-1}$ (табл. 1).

Шаг 3. Определение векторов индексов децимации $\mathbf{A}_{m,n,r}$ для заданных значений параметров m, n и r в соответствии с модифицированным алгоритмом.

Шаг 4. Формирование M массивов $CC_j[i] = C[I_{dj}\, i]$ $(j = 1\ldots M,\ i = 0\ldots N-1)$ для суммируемых последовательностей путем децимации символов базисной МП по индексам децимации I_{dj}, равным соответствующим компонентам вектора $\mathbf{A}_{m,n,r}$.

Шаг 5. Формирование массива ГМВП $G[i]$ путем суммирования по mod 2 полученных последовательностей

$$\begin{aligned} G[i] &= CC_1[i] + CC_2[i] + \ldots + \\ &+ CC_{M-1}[i] + CC_M[i], \quad i = 0\ldots N-1. \end{aligned} \tag{6}$$

Шаг 6. Конец алгоритма.

В соответствии с модифицированным алгоритмом были получены векторы индексов децимации $\mathbf{A}_{m,n,r}$ для ГМВП с периодами от $N = 2^6-1$ до $N = 2^{20}-1$ для допустимых значений параметров m, n в полях $GF[(2^m)^n]$.

В табл. 2 приведены векторы индексов децимации $\mathbf{A}_{m,n,r}$ при формировании ГМВП с периодами от $N = 63$ до $N = 65535$ для минимального и максимального значений ЭЛС. Полиномы для базисных МП соответствуют табл. 1.

В табл. 3 приведены векторы индексов децимации для минимального и максимального значений ЭЛС l_s при формировании ГМВП с периодом $N = 262143$ на основе базисной МП с проверочным полиномом $h_{\text{МП}}(x) = x^{18} + x^7 + 1$ и с периодом $N = 1048575$ на основе базисной МП с проверочным полиномом $h_{\text{МП}}(x) = x^{20} + x^3 + 1$.

Таблица 1. Примитивные полиномы в полях $GF(2^S)$

N	$h_{МП}(x) = h_1(x)$	$C_0C_1...C_{S-2}C_{S-1}$
2^5-1	$x^5 + x^2 + 1$	10010
2^6-1	$x^6 + x + 1$	000001
2^7-1	$x^7 + x^3 + 1$	1000000
2^8-1	$x^8 + x^4 + x^3 + x^2 + 1$	00000100
2^9-1	$x^9 + x^4 + 1$	100001000
$2^{10}-1$	$x^{10} + x^3 + 1$	0000000100
$2^{11}-1$	$x^{11} + x^2 + 1$	10000000010
$2^{12}-1$	$x^{12} + x^6 + x^4 + x + 1$	000000000001
$2^{13}-1$	$x^{13} + x^4 + x^3 + x + 1$	1000000001000
$2^{14}-1$	$x^{14} + x^{10} + x^6 + x + 1$	00000000000001
$2^{15}-1$	$x^{15} + x + 1$	100000000000000
$2^{16}-1$	$x^{16} + x^{12} + x^3 + x + 1$	0000000000000101
$2^{17}-1$	$x^{17} + x^3 + 1$	10000000000000000
$2^{18}-1$	$x^{18} + x^7 + 1$	000000000001000000
$2^{19}-1$	$x^{19} + x^5 + x^2 + x + 1$	1000000000000000010
$2^{20}-1$	$x^{20} + x^3 + 1$	00000000000000000100
$2^{21}-1$	$x^{21} + x^2 + 1$	100000000000000000010
$2^{22}-1$	$x^{22} + x + 1$	0000000000000000000001

Таблица 2. Векторы индексов децимации для периодов $N = 63...65535$

N	m, n	r	l_s	M	Векторы индексов децимации $\mathbf{A}_{m,n,r}$
63	3, 2	3	12	2	3, 5
255	4, 2	7	32	4	7, 11, 13, 37
511	3, 3	3	27	3	3, 5, 17
1023	5, 2	3	20	2	3, 17
1023	5, 2	15	80	8	15, 23, 27, 29, 77, 85, 89, 147
4095	6, 2	5	24	2	5, 17
4095	6, 2	31	192	16	31, 47, 55, 59, 61, 157, 173, 181, 185, 283, 299, 307, 313, 409, 425, 661
16383	7, 2	3	28	2	3, 65
16383	7, 2	63	448	32	63, 95, 111, 119, 123, 125, 317, 349, 365, 373, 377, 571, 603, 619, 627, 633, 825, 857, 873, 881, 1111, 1127, 1139, 1141, 1333, 1365, 1381, 1587, 1619, 2349, 2381, 2405
32767	5, 3	3	45	3	3, 17, 65
32767	5, 3	15	405	27	15, 23, 27, 29, 77, 85, 89, 139, 147, 153, 201, 209, 263, 275, 277, 325, 337, 387, 401, 449, 523, 525, 643, 649, 2185
65535	8, 2	7	64	4	7, 131, 193, 517
65535	8, 2	127	1024	64	127, 191, 223, 239, 247, 251, 253, 637, 701, 733, 749, 757, 761, 1147, 1211, 1243, 1259, 1267, 1273, 1657, 1721, 1753, 1769, 1777, 2167, 2231, 2263, 2279, 2291, 2293, 2677, 2741, 2773, 2789, 2801, 3187, 3251, 3283, 3299, 3313, 3697, 3761, 3793, 4717, 4781, 4813, 4837, 4841, 5227, 5291, 5323, 5347, 5353, 5737, 5801, 5833, 6343, 6373, 6757, 6821, 9371, 9419, 9427, 10837

Таблица 3. Векторы индексов децимации для периодов $N = 262143$, 1048575

N	m, n	r	M	Векторы индексов децимации $\mathbf{A}_{m,n,r}$
262143	9, 2	3	2	3, 5
262143	9, 2	85	8	85, 149, 165, 169, 2129, 2193, 2209, 4257
262143	9, 2	255	128	255, 383, 447, 479, 495, 503, 507, 509, 1277, 1405, 1469, 1501, 1517, 1525, 1529, 2299, 2427, 2491, 2523, 2539, 2547, 2553, 3321, 3449, 3513, 3545, 3561, 3569, 4343, 4471, 4535, 4567, 4583, 4595, 4597, 5365, 5493, 5557, 5589, 5605, 5617, 6387, 6515, 6579, 6611, 6627, 6641, 7409, 7537, 7601, 7633, 7649, 8559, 8623, 8655, 8679, 8683, 8685, 9453, 9581, 9645, 9677, 9701, 9705, 10475, 10603, 10667, 10699, 10723, 10729, 11497, 11625, 11689, 11721, 12519, 12647, 12711, 12743, 12771, 12773, 13541, 13669, 13733, 13765, 14563, 14691, 14755, 17629, 17757, 17821, 17869, 17877, 17881, 18651, 18779, 18843, 18891, 18899, 18905, 19673, 19801, 19865, 19913, 20823, 20887, 20935, 20947, 20949, 21717, 21845, 21909, 22739, 22867, 22931, 25805, 25933, 25997, 26057, 26955, 27081, 27849, 27977, 38069, 38197, 38293, 38309, 39219, 42285
1048575	10, 2	5	2	5, 257
1048575	10, 2	511	256	511, 767, 895, 959, 991, 1007, 1015, 1019, 1021, 2557, 2813, 2941, 3005, 3037, 3053, 3061, 3065, 4603, 4859, 4987, 5051, 5083, 5099, 5107, 5113, 6649, 6905, 7033, 7097, 7129, 7145, 7153, 8695, 8951, 9079, 9143, 9175, 9191, 9203, 9205, 10741, 10997, 11125, 11189, 11221, 11237, 11249, 12787, 13043, 13171, 13235, 13267, 13283, 13297, 14833, 15089, 15217, 15281, 15313, 15329, 16879, 17135, 17263, 17327, 17359, 17383, 17387, 17389, 18925, 19181, 19309, 19373, 19405, 19429, 19433, 20971, 21227, 21355, 21419, 21451, 21475, 21481, 23017, 23273, 23401, 23465, 23497, 23521, 25063, 25319, 25447, 25511, 25543, 25571, 25573, 27109, 27365, 27493, 27557, 27589, 27617, 29155, 29411, 29539, 29603, 29635, 29665, 31201, 31457, 31585, 31649, 35293, 35549, 35677, 35741, 35789, 35797, 35801, 37339, 37595, 37723, 37787, 37835, 37843, 37849, 39385, 39641, 39769, 39833, 39881, 39889, 41431, 41687, 41815, 41879, 41927, 41939, 41941, 43477, 43733, 43861, 43925, 43973, 43985, 45523, 45779, 45907, 45971, 46019, 46033, 47569, 47825, 47953, 48017, 49999, 50063, 50119, 50123, 50125, 51661, 51917, 52045, 52109, 52165, 52169, 53707, 53963, 54091, 54155, 54217, 55753, 56009, 56137, 56201, 57799, 58055, 58183, 58309, 59845, 60101, 60229, 70075, 70331, 70459, 70555, 70571, 70579, 70585, 72121, 72377, 72505, 72601, 72617, 74423, 74551, 74647, 74663, 74675, 74677, 76213, 76469, 76597, 76693, 76709, 78259, 78515, 78643, 78739, 78755, 84397, 84653, 84781, 84877, 84901, 84905, 86443, 86699, 86827, 86923, 86947, 86953, 88489, 88745, 88873, 90919, 91043, 91045, 92581, 92837, 92965, 94627, 94883, 95011, 102811, 103067, 103195, 103315, 103321, 104857, 105113, 107411, 107413, 108949, 109205, 111251, 149869, 150125, 150317, 150349, 150373, 152171, 152363, 152395, 158053, 158309, 174421

В качестве примера определим массив $G[i]$ ГМВП с периодом $N = 262143$ и ЭЛС $l_s = 144$.

Шаг 1. Исходные данные: поле $GF[(2^9)^2]$; базисная МП с полиномом $h_{\text{МП}}(x) = x^{18} + x^7 + 1$; параметр $r = 85$ с $g(r) = 4$; число сомножителей $M = 8$ (табл. 3).

Шаг 2. Формирование массива базисной МП $C[i]$ ($i = 0...262142$)

$$C[18 + j] = C[0 + j] + C[7 + j], \quad j = 0\ldots262124.$$

Шаг 3. Определение вектора индексов децимации (в соответствии с табл. 3)

$$\mathbf{A}_{m,n,r} = \\ = \mathbf{A}_{9,2,85} = (85, 149, 165, 169, 2129, 2193, 2209, 4257).$$

Шаг 4. Формирование $M = 8$ массивов $CC_j[i] = C[I_{dj}\, i]$ ($j = 1...8$, $i = 0...262142$) в соответствии с вектором индексов децимации $\mathbf{A}_{m,\,n,\,r} = \mathbf{A}_{9,\,2,\,85}$.

Шаг 5. Формирование массива ГМВП $G[i]$ путем суммирования $CC_j[i]$

$$G[i] = C[85i] + C[149i] + C[165i] + C[169i] + \\ + C[2129i] + C[2193i] + C[2209i] + C[4257i], \quad (7) \\ i = 0\ldots N-1.$$

Отметим, что последовательности CC_1, CC_2, CC_4, CC_5, CC_7 являются МП и имеют максимальный период. Последовательности CC_3, CC_6 соответствуют ПСП с периодом $N_1 = N/3 = 87381$, последовательность CC_8 имеет период $N_2 = N/9 = 29127$.

Таким образом, в статье разработана программная реализация алгоритма формирования сверхдлинных ГМВП при произвольной базисной МП на основе модификации алгоритма определения полиномов-сомножителей $h_{ci}(x)$ проверочного полинома $h_{\text{ГМВП}}(x)$. При программной реализации вектор полиномов-сомножителей $h_{ci}(x)$, получаемый в результате выполнения модифицированного алгоритма, рассматривается как вектор индексов децимации $\mathbf{A}_{m,n,r}$. Получены выражения для числа вычислительных операций в зависимости от значения параметра n, которые можно рассматривать как верхние граничные оценки для числа суммируемых последовательностей.

Определены векторы индексов децимации для периодов $N \le 2^{12}-1 = 4095$, подтверждающие известные в литературе результаты [16]. Впервые получены перечни векторов индексов децимации для сверхдлинных ГМВП с высокой структурной скрытностью с периодами $2^{14}-1 = 16\ 383 \le N \le$ $\le 2^{20} - 1 = 1048575$. Например, можно сформировать ГМВП с периодом $N = 2^{20}-1 = 1048575$ и ЭЛС $l_s = 5120$, что в 256 раз превышает значение ЭЛС для базисной МП. При этом выражение для символов ГМВП, аналогичное (7), будет содержать 256 слагаемых, а ПАКФ полученной последовательности с проверочным полиномом 5120-й степени будет двухуровневой, как и для базисной МП.

При программной реализации алгоритма формирования сверхдлинных ГМВП с периодом $N =$ $= 2^S - 1$ требуется знание только одного примитивного полинома степени S для базисной МП и перечня векторов индексов децимации. При этом вычислительная сложность алгоритма определяется только выполнением операций модульного сложения.

На практике полученные результаты могут быть использованы при синтезе ПСП для формирования сигналов с расширенным спектром в СПЦИ, функционирующих в условиях радиоэлектронного противодействия, к которым предъявляются повышенные требования по помехозащищенности и структурной скрытности.

СПИСОК ЛИТЕРАТУРЫ

1. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. 2-е изд. М.: Вильямс, 2003.
2. *Golomb S.W., Gong G.* Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar. Cambridge: Cambridge Univ. Press, 2005.
3. *Ипатов В.П.* Широкополосные системы и кодовое разделение сигналов. Принципы и приложения. М.: Техносфера, 2007.
4. *CDMA*: прошлое, настоящее, будущее. М.: МАС, 2003.
5. *Coulter R.S., Mesnager S.* // IEEE Trans. 2018. V. IT-64. № 4. P. 2979.
6. *Boztaş S., Özbudak F., Tekin E.* // IEEE Trans. 2018. V. IT-64. № 4. P. 2858.
7. *Lempel A., Ziv J.* // IEEE Trans. 1976. V. IT-22. № 1. P. 75.
8. *Lie-Liang Yang, Hanzo L.* // Wireless Communications and Networking. 2003. V. 1. P. 683.
9. *Ипатов В.П.* Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992.
10. *Popovic B.M.* // IEEE Trans. 2018. V. IT-64 № 4. P. 2876.
11. *Golomb S.W.* // IEEE Trans. 1992. V. AES-28. № 2. P. 383.
12. *Шатилов А.Ю.* Характеристики радиосигналов глобальных спутниковых радионавигационных систем ГЛОНАСС, GPS, Galileo, Beidou и функциональных дополнений SBAS. Учеб. пособие для вузов. М.: МЭИ, 2016.
13. *Ershen Wang, Shufang Zhang, Qing Hu* // J. System Simulation. 2008. V. 20. P. 3582.
14. *Chung H.B., No J.S.* // IEEE Trans. 1999. V. IT-45. № 6. P. 2060.
15. *No Jong-Seon* // IEEE Trans. 1996. V. IT-42. № 1. P. 260.
16. *Стародубцев В.Г., Бородько Д.Н., Мышко В.В.* // Авиакосмическое приборостроение. 2018. № 5. С. 3.
17. *Стародубцев В.Г.* // РЭ. 2020. Т. 65. № 2. С. 169.
18. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки / Пер. с англ., под ред. Р.Л. Добрушина, С.И. Самойленко. М.: Мир, 1976.
19. *Стародубцев В.Г., Чернявских А.Е.* // Изв. вузов. Приборостроение. 2016. Т. 59. № 3. С. 201.