РАДИОТЕХНИКА И ЭЛЕКТРОНИКА, 2023, том 68, № 7, с. 676–682

ТЕОРИЯ И МЕТОДЫ ОБРАБОТКИ СИГНАЛОВ

УДК 519.725;512.62

МЕТОД ФОРМИРОВАНИЯ НЕДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОРДОНА–МИЛЛСА–ВЕЛЧА ДЛЯ СИСТЕМ ПЕРЕДАЧИ ЦИФРОВОЙ ИНФОРМАЦИИ

© 2023 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 16.11.2022 г.
После доработки 06.12.2022 г.
Принята к публикации 10.12.2022 г.

На основе обобщения метода формирования двоичных последовательностей разработан метод формирования недвоичных последовательностей Гордона–Миллса–Велча (ГМВП) с периодом $N = p^{mn} - 1$, формируемых над полем $GF(p)$. Получено выражение для вычисления вектора индексов децимации $\mathbf{A}_{m,n,r}$ базисной М-последовательности (МП) для суммируемых последовательностей при синтезе ГМВП. Представлена методика формирования недвоичных ГМВП для произвольных МП. Показано, что значения компонент вектора сдвигов $\mathbf{C}_{m,n,r}$ базисной МП зависят от распределение цифр на позициях p-ичного представления соответствующих индексов децимации.

DOI: 10.31857/S0033849423060141, **EDN:** XNIMFO

ВВЕДЕНИЕ

Современные системы передачи цифровой информации (СПЦИ) по радиоканалам характеризуются широким использованием сигналов с расширенным спектром (СРС), формируемых с помощью псевдослучайных последовательностей (ПСП) [1–4]. Наряду с двоичными последовательностями в современных и перспективных СПЦИ могут применяться недвоичные ПСП, обладающие заданными корреляционными и структурными свойствами [3, 5–13]. Повышение помехозащищенности СПЦИ достигается применением ПСП с малым уровнем пиков корреляционной функции. К классу минимаксных последовательностей с двухуровневой периодической автокорреляционной функцией (ПАКФ) относятся как двоичные, так и недвоичные М-последовательности (МП) и последовательности Гордона–Миллса–Велча (ГМВП) [14–16]. При этом ГМВП имеют более высокую структурную скрытность, характеризуемую эквивалентной линейной сложностью (ЭЛС), что определяет приоритетность их применения в СПЦИ, к которым предъявляются повышенные требования по конфиденциальности [17, 18].

Недвоичные ГМВП характеризуются более высоким по сравнению с двоичными последовательностями выигрышем в структурной скрытности, который определяется отношением ЭЛС ГМВП и МП $M = l_{s\text{ГМВП}}/l_{s\text{МП}}$ при сопоставимых периодах. Например, для пятеричных ГМВП с периодом $N = 15624$ выигрыш составляет $M = 50$, а для двоичных ГМВП с периодом $N = 16383$ выигрыш составляет $M = 32$. С увеличением периода и значности p выигрыш возрастает. Так, для семеричных ГМВП с периодом $N = 117648$ выигрыш составляет $M = 196$, а для двоичных ГМВП с периодом $N = 262143$ выигрыш $M = 128$.

1. ПОСТАНОВКА ЗАДАЧИ

Формирование недвоичных ГМВП осуществляется над конечными полями $GF(p)$. Все вычисления производятся в полях

$$GF[(p^m)^n] = GF(p^S), \quad S = mn.$$

Период последовательностей является составным числом, т.е. $N = p^{mn} - 1$. Символы d_i ГМВП определяются выражением [3, 15]

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

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

Формирование недвоичных ГМВП в соответствии с (1) характеризуется достаточной вычислительной сложностью, определяемой необходимостью построения расширенного поля $GF[(p^m)^n]$ и двухэтапного вычисления функций следа $\mathrm{tr}_{a,b}(\cdot)$. Для построения поля $GF[(p^m)^n]$ требуется не менее $2(mn-2)p^{mn}$ операций модульного сложения и умножения.

Основную вычислительную нагрузку при прямом формировании ГМВП составляют вычисления функций следа. Например, при формировании троичной ГМВП с периодом $N = 3^6 - 1 = 728$ и параметрами $m = 3$, $n = 2$, $r = 5$ для определения символа d_1 выполняются следующие операции в поле $GF(3^6)$, построенном по полиному $f(x) = x^6 + x + 2$:

– вычисление функции следа из поля $GF(3^6)$ в подполе $GF(3^3)$

$$\mathrm{Tr}_{6.3}\alpha = \alpha + \alpha^{27} =$$
$$= 010000 + 222120 = 202120 = \alpha^{280};$$

– возведение элемента α^{280}, принадлежащего подполю $GF(3^3)$, в степень $r = 5$

$$(\alpha^{280})^5 = \alpha^{280\times 5 \bmod 728} = \alpha^{672};$$

– вычисление функции следа из подполя $GF(3^3)$ в простом поле $GF(3)$

$$\mathrm{Tr}_{3.1}\alpha^{672} = \alpha^{672} + \alpha^{672\times 3 \bmod 728} + \alpha^{672\times 9 \bmod 728} =$$
$$= \alpha^{672} + \alpha^{560} + \alpha^{224} = 010211 + 112001 +$$
$$+ 111121 = 200000 = 2.$$

При вычислениях необходимо выполнить несколько переходов от степенной формы записи элементов поля к векторной и обратно. Всего для нахождения всех символов ГМВП необходимо выполнить $N = p^{mn} - 1$ таких вычислительных процедур.

Для полей $GF[(p^m)^n]$ при $n = 2$ известны алгоритмы формирования троичных, пятеричных и семеричных ГМВП [11, 14, 16], основанные на представлении базисной МП в виде матрицы размерности $[(p^m-1) \times (p^m + 1)]$. Вычислительная сложность определяется необходимостью определения правил формирования циклических сдвигов столбцов матрицы базисной МП, нахождения проверочного полинома ГМВП по алгоритму Берлекэмпа–Месси, позволяющего вычислить вектор индексов децимации, и решения системы уравнений для вычисления вектора сдвигов базисной МП при формировании ГМВП.

Цель данной статьи – разработка метода формирования недвоичных ГМВП, основанного на аналитическом определении вектора индексов децимации $\mathbf{A}_{m,n,r}$ символов базисной МП и упрощенном вычислении вектора ее сдвигов для суммируемых последовательностей.

Метод формирования недвоичных ГМВП является обобщением метода для двоичных последовательностей [18] и включает алгоритм формирования вектора индексов децимации $\mathbf{A}_{m,n,r}$ символов базисной недвоичной МП, методику определения полных наборов векторов индексов децимации $\mathbf{A}_{m,n,r}$ для произвольных МП и алгоритм определения вектора сдвигов $\mathbf{C}_{m,n,r}$ базисной МП при формировании суммируемых последовательностей.

Разработанный метод характеризуется низким уровнем вычислительной сложности, обусловленным отсутствием необходимости построения конечных полей $GF[(p^m)^n]$ и двухэтапного вычисления функций следа. Формируется только одна базисная МП в каноническом виде по заданному примитивному полиному и известному начальному состоянию. При реализации алгоритма формирования вектора индексов децимации $\mathrm{A}_{m,n,r}$ основные преобразования выполняются с множеством целых чисел, что характеризуется низкой вычислительной сложностью.

2. АЛГОРИТМ ФОРМИРОВАНИЯ ВЕКТОРА ИНДЕКСОВ ДЕЦИМАЦИИ $\mathbf{A}_{m,n,r}$

Основной составляющей метода является алгоритм формирования вектора индексов децимации $\mathbf{A}_{m,n,r}$. Число компонент вектора $\mathbf{A}_{m,n,r} = (I_{d1}, I_{d2}, \ldots, I_{dM})$ равно отношению ЭЛС ГМВП и МП $M = l_{s\text{ГМВП}}/l_{s\text{МП}}$. Тогда ЭЛС формируемой ГМВП определяется выражением

$$l_{s\text{ГМВП}} = mnM. \quad (2)$$

Формирование ГМВП может быть реализовано аппаратным и программным способом. При аппаратной реализации формирование ГМВП выполняется на основе совокупности из M регистров сдвига с линейными обратными связями, определяемыми коэффициентами неприводимых полиномов $h_{ci}(x)$, являющихся множителями проверочного полинома ГМВП $h_{\text{ГМВП}}(x)$.

При программной реализации алгоритма структура полиномов $h_{ci}(x)$ не учитывается. Используется понятие вектора индексов децимации $\mathbf{A}_{m,n,r}$, компоненты которого I_{di} соответствуют индексам полиномов $h_{ci}(x)$.

Алгоритм формирования вектора индексов децимации $\mathbf{A}_{m,n,r}$ символов базисной недвоичной МП основан на модифицированном алгоритме формирования аналогичного вектора для двоичных последовательностей, разработанном в [19]. Первое отличие, определяющее научную новизну, заключается в модернизации выражения для вспомогательного параметра k_i

$$k_i = i(p^m - 1), \quad i = 0, 1, 2, \ldots, T-1, \quad (3)$$

Таблица 1. Исходные данные для формирования МП в каноническом виде

p	$S = mn$	Полином $h_1(x)$	Символы $d_0\, d_1 \ldots d_{S-1}$
3	$2 = 1 \times 2$	$x^2 + x + 2$	20
	$3 = 1 \times 3$	$x^3 + 2x + 1$	002
	$4 = 2 \times 2$	$x^4 + x + 2$	1000
	$5 = 1 \times 5$	$x^5 + 2x + 1$	20001
	$6 = 3 \times 2$	$x^6 + x + 2$	000001
	$6 = 2 \times 3$	$x^6 + x + 2$	000001
	$7 = 1 \times 7$	$x^7 + x^2 + 2x + 1$	1000010
	$8 = 2 \times 4$	$x^8 + 2x^3 + 2$	20000200
	$8 = 4 \times 2$	$x^8 + 2x^3 + 2$	20000200
	$9 = 3 \times 3$	$x^9 + x^4 + x^2 + 1$	000001020
5	$2 = 1 \times 2$	$x^2 + x + 2$	24
	$3 = 1 \times 3$	$x^3 + 3x + 2$	304
	$4 = 1 \times 4$	$x^4 + x^2 + 2x + 2$	4034
	$4 = 2 \times 2$	$x^4 + x^2 + 2x + 2$	4034
	$5 = 1 \times 5$	$x^5 + 4x + 2$	00004
	$6 = 1 \times 6$	$x^6 + x^2 + 2x + 2$	100010
	$6 = 2 \times 3$	$x^6 + x^2 + 2x + 2$	100010
	$6 = 3 \times 2$	$x^6 + x^2 + 2x + 2$	100010
7	$2 = 1 \times 2$	$x^2 + x + 3$	26
	$3 = 1 \times 3$	$x^3 + 3x + 2$	301
	$4 = 1 \times 4$	$x^4 + x^2 + 3x + 5$	4055
	$4 = 2 \times 2$	$x^4 + x^2 + 3x + 5$	4055
11	$2 = 1 \times 2$	$x^2 + x + 7$	2,10
	$3 = 1 \times 3$	$x^3 + x^2 + 5$	3,10,1
	$4 = 1 \times 4$	$x^4 + x + 2$	4008
	$4 = 2 \times 2$	$x^4 + x + 2$	4008

где параметр T равен числу компонент I_{bi} вектора альтернатив $\mathbf{B}_{m,n,r}$, в котором содержатся все индексы децимации I_{di}, являющиеся компонентами вектора $\mathbf{A}_{m,n,r}$. Для конечного поля $GF[(p^m)^n]$ параметр T определяется по выражению

$$T = (p^{mn} - 1)\big/(p^m - 1). \tag{4}$$

Вторым отличием является порядок вычисления функции $g(r)$. В двоичном случае ее значение определяется числом единиц в двоичном представлении параметра r. При $p > 2$ она равна арифметической сумме значений разрядов p-го представления данного параметра.

Компоненты I_{bi} вектора альтернатив $\mathbf{B}_{m,n,r}$ вычисляются в соответствии с заданным значением параметров r и k_i

$$I_{bi} = r + k_i, \quad i = 0, 1, 2, \ldots, T - 1. \tag{5}$$

Отметим, что при $i > T{-}1$ наступает циклическое повторение значений компонент I_{bi} по $\mathrm{mod}(p^{mn} - 1)$.

Для перехода от вектора альтернатив $\mathbf{B}_{m,n,r}$ к вектору индексов децимации $\mathbf{A}_{m,n,r}$ необходимо представить значения компонент I_{bi} в p-й системе счисления, выбрать те из них, которые удовлетворяют значению функции $g(r)$, и исключить компоненты, которые относятся к одинаковым циклотомическим классам.

При формировании ГМВП базисная МП представляется в каноническом виде, ее символы определяются выражением (1) при $r = 1$

$$d_i = \mathrm{tr}_{mn,1}(\alpha^i), \quad i = 0, 1, \ldots, p^{mn} - 2, \tag{6}$$

требующим построения расширенного поля $GF[(p^m)^n]$.

Формирование МП вместо (6) может быть реализовано без построения конечного поля на основании полинома

$$h_{\text{МП}}(x) = h_1(x) = x^S + h_{S-1}x^{S-1} + \ldots + h_1 x + h_0$$

в соответствии с выражением

$$\begin{gathered} d_{S+i} = -h_0 d_{0+i} - h_1 d_{1+i} - \ldots - h_{S-1} d_{S-1+i}, \\ i = 0, \ldots, N - S - 1, \end{gathered} \tag{7}$$

где d_j – символы начального состояния МП ($0 \le j < S$), а операции выполняются по mod p.

Для получения базисной МП в каноническом виде для различных сочетаний параметров p, m, n используются примитивные полиномы $h_1(x)$ степени $S = mn$ и начальные символы d_i ($i = 0, 1, \ldots, S - 1$), приведенные в табл. 1. При других начальных символах формируются МП не в каноническом виде.

В качестве примера определим вектор индексов децимации $\mathbf{A}_{3,2,17}$ в расширенном поле $GF[(p^m)^n] = GF[(3^3)^2]$ с примитивным полиномом $h_1(x) = x^6 + x + 2$ для значения параметра $r = 17_{10} = 122_3$ и функции $g(r) = 1{+}2{+}2 = 5$.

Компоненты I_{bi} вектора альтернатив $\mathbf{B}_{3,2,17}$, число которых равно $T = 28$, вычисляются в соответствии с (3) и (5)

$$\begin{gathered} \mathbf{B}_{3,2,17} = 17,\ 43,\ 69,\ 95,\ 121,\ 147,\ 173,\ 199,\ 22,\ 251,\ 277,\ 303,\ 329,\ 355,\ 381,\ 407, \\ 433,\ 459,\ 485,\ 511,\ 537,\ 563,\ 589,\ 615,\ 641,\ 667,\ 693,\ 719. \end{gathered}$$

После проверки функции $g(r) = 5$ и приведения компонент I_{bi} к минимальным значениям в циклотомических классах определяется вектор индексов децимации

$$\mathbf{A}_{3,2,17} = 17,\ 43,\ 23,\ 95,\ 121,\ 49,\ 101,\ 103,\ 25. \quad (8)$$

Линейная сложность ГМВП с периодом $N = 728$, сформированной путем сложения ПСП с данными индексами децимации базисной МП, в соответствии с (2) равна $l_s = 54$, т.е. в 9 раз превышает ЭЛС МП.

Методика определения полных наборов векторов индексов децимации $\mathbf{A}_{m,n,r}$ для произвольных МП основана на свойстве повторяемости соотношений между корнями проверочных полиномов базисной и произвольной МП и соответствует аналогичной методике для двоичного случая [18]. Символы произвольной МП с аналогичным периодом образуются путем децимации символов базисной МП по некоторому индексу $I_{\text{МП}}$. Компоненты вектора $\mathbf{A}_{m,n,r}$ преобразуются в компоненты вектора $\mathbf{A}_{m,n,r}^{\text{МП}}$ в соответствии с выражением

$$I_{di}^{\text{МП}} = I_{di} \times I_{\text{МП}} \bmod (p^{mn} - 1). \quad (9)$$

Полученные компоненты приводятся к минимальным значениям в соответствующих циклотомических классах.

В качестве примера рассмотрим формирование ГМВП в поле $GF[(3^3)^2]$, если произвольная МП образуется из базисной по индексу $I_{\text{МП}} = 97$. Преобразуя вектор индексов децимации вида (8) в соответствии с (9), получим новый вектор

$$\mathbf{A}_{3,2,17}^{97} = 115,\ 59,\ 47,\ 215,\ 73,\ 203,\ 37,\ 125,\ 241, \quad (10)$$

на основании которого может быть синтезирована новая ГМВП.

Число различных ГМВП, которые могут быть сформированы для заданных значений параметров p, m, n и r, равно числу МП с периодом $N = p^{mn} - 1$.

3. АЛГОРИТМ ОПРЕДЕЛЕНИЯ ВЕКТОРА СДВИГОВ $\mathrm{C}_{m,n,r}$

Алгоритм определения вектора сдвигов $\mathbf{C}_{m,n,r}$ базисной МП для суммируемых последовательностей при формировании недвоичных ГМВП является обобщением аналогичного алгоритма для двоичного случая. При $p = 2$ децимация всех последовательностей производится с символа d_0 базисной МП. Особенностью формирования недвоичных ГМВП является то, что децимация суммируемых последовательностей может начинаться с некоторого сдвига базисной МП. Анализ формирования ГМВП при $p = 3, 5, 7$ [11, 14, 16] показал, что возможные сдвиги определяются выражением

$$\lambda_i = kN/(p-1), \quad i = 1, 2, \ldots, M; \quad k = 0, 1, \ldots, p-2. \quad (11)$$

Таким образом, основная проблема при формировании недвоичных ГМВП с известным вектором индексов децимации $\mathbf{A}_{m,n,r}$ мощностью M заключается в нахождении начальных сдвигов λ_i базисной МП, образующих вектор сдвигов $\mathbf{C}_{m,n,r}$ аналогичной мощности, для каждого индекса децимации I_{di}.

В общем случае для определения вектора сдвигов $\mathbf{C}_{m,n,r}$ требуется выполнить число операций вычисления ПАКФ формируемых последовательностей

$$L_1 = (p-1)^M.$$

Для уменьшения числа операций был проведен анализ распределения сдвигов λ_i с учетом p-го представления индексов децимации I_{di}. Анализ показал, что последовательности, формируемые по индексам децимации, имеющим одинаковое распределение ненулевых цифр на позициях p-го представления, обладают одинаковыми начальными сдвигами. Например, при $p = 5$ и $g(r) = 3$ последовательности с индексами децимации $I_{d1} = 7_{10} = 12_5$, $I_{d2} = 11_{10} = 21_5$, $I_{d3} = 27_{10} = 102_5$, $I_{d4} = 51_{10} = 201_5$, $I_{d5} = 127_{10} = 1002_5$ имеют одинаковый начальный сдвиг $\lambda_1 = \lambda_2 = \lambda_3 = \lambda_4 = \lambda_5 = 3N/4$.

Данное свойство позволяет уменьшить число операций при определении вектора сдвигов $\mathbf{C}_{m,n,r}$. Объединим в группы индексы децимации I_{di} с одинаковым в каждой группе распределением цифр на позициях их p-го представления. Можно показать, что число M_1 групп для различных значений функции $g(r)$ ограничено сверху произведением $mn(p-1)/2$ и всегда меньше общего числа индексов децимации. При этом число операций вычисления ПАКФ равно

$$L_2 = (p-1)^{M_1}. \quad (12)$$

Выигрыш в вычислительной сложности составляет

$$W = L_1/L_2 = (p-1)^{M/M_1}. \quad (13)$$

Алгоритм определения вектора сдвигов $\mathbf{C}_{m,n,r}$ при децимации базисной МП записывается в следующем виде.

Шаг 1. Перевод компонент I_{di} вектора индексов децимации $\mathbf{A}_{m,n,r}$ в p-ю систему счисления.

Шаг 2. Объединение индексов децимации в группы с одинаковым распределением цифр на позициях их p-го представления.

Шаг 3. Вычисление ПАКФ формируемой последовательности для различных значений сдвига в каждой группе.

Таблица 2. Формирование ГМВП $F_{\text{ГМВП}}$ для векторов $\mathbf{A}_{3,2,17}$ и $\mathbf{C}_{3,2,17}$

ПСП	Сдвиг	Символы базисной МП и их значения													
F_{17}	0	d_0	d_{17}	d_{34}	d_{51}	d_{68}	d_{85}	d_{102}	d_{119}	d_{136}	d_{153}	d_{170}	d_{187}	d_{204}	d_{221}
		0	1	1	1	2	0	1	1	2	1	1	0	2	1
F_{43}	364	d_{364}	d_{407}	d_{450}	d_{493}	d_{536}	d_{579}	d_{622}	d_{665}	d_{708}	d_{23}	d_{66}	d_{109}	d_{152}	d_{195}
		0	1	0	1	1	2	0	2	1	1	0	2	1	2
F_{23}	0	d_0	d_{23}	d_{46}	d_{69}	d_{92}	d_{115}	d_{138}	d_{161}	d_{184}	d_{207}	d_{230}	d_{253}	d_{276}	d_{299}
		0	1	0	1	2	2	0	2	2	1	0	2	2	2
F_{95}	364	d_{364}	d_{459}	d_{554}	d_{649}	d_{16}	d_{111}	d_{206}	d_{301}	d_{396}	d_{491}	d_{586}	d_{681}	d_{48}	d_{143}
		0	1	2	1	1	0	2	1	1	1	2	0	1	1
F_{121}	0	d_0	d_{121}	d_{242}	d_{363}	d_{484}	d_{605}	d_{726}	d_{119}	d_{240}	d_{361}	d_{482}	d_{603}	d_{724}	d_{117}
		0	2	1	2	1	2	1	1	0	2	2	0	1	0
F_{49}	364	d_{364}	d_{413}	d_{462}	d_{511}	d_{560}	d_{609}	d_{658}	d_{707}	d_{28}	d_{77}	d_{126}	d_{175}	d_{224}	d_{273}
		0	2	0	2	1	0	0	2	2	2	0	1	1	0
F_{101}	0	d_0	d_{101}	d_{202}	d_{303}	d_{404}	d_{505}	d_{606}	d_{707}	d_{80}	d_{181}	d_{282}	d_{383}	d_{484}	d_{585}
		0	0	2	0	1	1	2	2	0	0	1	0	1	2
F_{103}	364	d_{364}	d_{467}	d_{570}	d_{673}	d_{48}	d_{151}	d_{254}	d_{357}	d_{460}	d_{563}	d_{666}	d_{41}	d_{144}	d_{247}
		0	2	1	2	1	2	1	1	1	2	1	2	1	0
F_{25}	0	d_0	d_{25}	d_{50}	d_{75}	d_{100}	d_{125}	d_{150}	d_{175}	d_{200}	d_{225}	d_{250}	d_{275}	d_{300}	d_{325}
		0	1	0	1	2	2	0	1	2	1	0	1	2	0
$F_{\text{ГМВП}}$		0	2	1	2	0	2	1	1	2	2	1	2	0	2

Шаг 4. При получении двухуровневой ПАКФ, соответствующей ГМВП, переход к окончанию алгоритма с определением финального вектора сдвигов $\mathbf{C}_{m,n,r}$.

В качестве примера определим вектор сдвигов $\mathbf{C}_{m,n,r} = \mathbf{C}_{3,2,17}$ для вектора индексов децимации $\mathbf{A}_{3,2,17}$ мощностью $M = 9$ из (8) при формировании ГМВП с периодом $N = 3^6 - 1 = 728$ в расширенном поле $GF[(3^3)^2]$ с примитивным полиномом $h_1(x) = x^6 + x + 2$ для значения параметра $r = 17_{10} = 122_3$.

Шаг 1. Перевод компонент вектора $\mathbf{A}_{3,2,17}$ в троичную систему счисления:

$$\mathbf{A}_{3,2,17} = (17,\ 43,\ 23,\ 95,\ 121,\ 49,\ 101,\ 103,\ 25)_{10} = \\ = (122,\ 1121,\ 212,\ 10112,\ 11111,\ 1211,\ 10202,\ 10211,\ 221)_3. \tag{14}$$

Шаг 2. Объединение индексов децимации в $M_1 = 3$ группы:

$$G_1 = (17,\ 23,\ 101,\ 25)_{10} = (122,\ 212,\ 10202,\ 221)_3;$$

$$G_2 = (43,\ 95,\ 49,\ 103)_{10} = \\ = (1121,\ 10112,\ 1211,\ 10211)_3;$$

$$G_3 = (121)_{10} = (11111)_3.$$

Шаг 3. Максимальное число вычислений ПАКФ равно $L_2 = 2^3 = 8$. Выигрыш в вычислительной сложности по сравнению с $L_1 = 2^9 = 512$ составляет $W = 2^6 = 64$. С увеличением p и M выигрыш возрастает.

Двухуровневая ПАКФ для ГМВП была получена при сдвигах $\lambda_{G1} = 0$, $\lambda_{G2} = N/2 = 364$, $\lambda_{G3} = 0$. Финальный вектор сдвигов $\mathbf{C}_{m,n,r}$ при децимации базисной МП имеет вид

$$\mathbf{C}_{3,2,17} = 0,\ 364,\ 0,\ 364,\ 0,\ 364,\ 0,\ 364,\ 0. \tag{15}$$

Шаг 4. Базисная МП строилась по проверочному полиному

$$h_{\text{МП}}(x) = h_1(x) = x^6 + x + 2$$

в соответствии с выражением

$$d_{6+i} = d_{0+i} + 2d_{1+i},\quad i = 0,\ldots,721, \tag{16}$$

где суммирование символов выполняется по mod 3 с начальными символами d_0, d_1, d_2, d_3, d_4, d_5, равными 0, 0, 0, 0, 0, 1 соответственно.

Двухуровневая ПАКФ была получена для ГМВП $F_{\text{ГМВП}}$, образованной путем суммирования девяти ПСП F_j (значение j соответствует индексу децимации) с символами d_i базисной МП из (16) и вектором сдвигов вида (15). В табл. 2 представлены

Таблица 3. Векторы индексов децимации $\mathbf{A}_{m,n,r}$ и сдвигов $\mathbf{C}_{m,n,r}$.

p	m	n	N	r_{10}	r_p	$g(r)$	M	$\mathbf{A}_{m,n,r}$	$\mathbf{C}_{m,n,r}$
3	2	3	728	5	12	3	6	5, 7, 13, 29, 31, 37	0, 0, 364, 0, 364, 364
	2	4	6560	5	12	3	10	5, 7, 13, 29, 31, 37, 55, 85, 109, 271	0, 0, 3280, 0, 3280, 3280, 0, 3280, 3280, 3280
	3	3	19682	7	21	3	6	7, 11, 37, 85, 163, 271	0, 0, 9841, 9841, 0, 9841
5	2	2	624	19	34	7	10	19, 23, 43, 47, 67, 71, 91, 193, 167, 187	0, 0, 312, 468, 0, 468, 312, 156, 156, 468
	1	5	3124	3	3	3	7	3, 7, 11, 27, 31, 51, 131	0, 781, 781, 781, 0, 781, 0
	3	2	15624	9	14	5	5	9, 101, 133, 257, 381	0, 0, 7812, 0, 7812
7	1	2	48	5	5	5	3	5, 11, 17	0, 40, 8
	2	2	2400	17	23	5	6	17, 23, 65, 71, 113, 401	0, 0, 2000, 1600, 2000, 1200
11	1	2	120	3	3	3	2	3, 13	0, 48
	2	2	14640	13	12	3	3	13, 23, 133	0, 0, 1464

Примечание. Пример векторов индексов децимации и сдвигов в первой строке: $\mathbf{A}_{m,n,r} = \mathbf{A}_{2,3,5}$ = 5, 7, 13, 29, 31, 37; $\mathbf{C}_{m,n,r} = \mathbf{C}_{2,3,5}$ = 0, 0, 364, 0, 364, 364.

сегменты данных последовательностей длиной 14 символов.

Отметим, что при формировании $F_{\text{ГМВП}}$ все суммируемые по mod 3 последовательности являются МП, кроме ПСП F_{49}, период которой равен 104. Значения индексов i в d_i вычисляются по mod 728.

Полученный вектор сдвигов $\mathbf{C}_{3,2,17}$ вида (15) может быть использован при формировании ГМВП для произвольной МП, например, образуемой из базисной МП по индексу $I_{\text{МП}} = 97$ с вектором индексов децимации $\mathbf{A}^{97}_{3,2,17}$ вида (10). Основное требование заключается в неизменности порядка следования компонентов векторов. Отметим, что в обоих случаях при формировании ГМВП используются только символы базисной МП вида (16).

Для некоторых значений параметров получены наборы векторов индексов децимации и векторов сдвигов базисных МП, которые представлены в табл. 3. Формирование МП проводилось в соответствии с исходными данными из табл. 1.

ЗАКЛЮЧЕНИЕ

Таким образом, разработан метод формирования недвоичных ГМВП, включающий алгоритм формирования вектора индексов децимации $\mathbf{A}_{m,n,r}$ для базисной МП, методику определения полных наборов векторов индексов децимации для произвольных МП и алгоритм определения вектора сдвигов $\mathbf{C}_{m,n,r}$ базисной МП при формировании суммируемых последовательностей. Отличие алгоритма формирования вектора $\mathbf{A}_{m,n,r}$ от двоичного случая заключается в выражении для вспомогательного параметра k_i при определении вектора альтернатив $\mathbf{B}_{m,n,r}$ и числа T его компонент. Вычисление вектора $\mathbf{A}_{m,n,r}$ не требует построения расширенных полей $GF[(p^m)^n]$. Новизна алгоритма определения вектора $\mathbf{C}_{m,n,r}$ определяется вычислением сдвигов базисной МП при ее децимации для получения суммируемых последовательностей в соответствии с индексами децимации I_{di}. Практическая значимость алгоритма заключается в уменьшении числа вычислительных операций, которое определяется тем, что процедура децимации символов базисной МП по индексам, имеющим одинаковое распределение цифр на позициях p-го представления, начинается с одинаковых начальных сдвигов МП.

Для различных значений параметров p, m, n и r определены векторы индексов децимации $\mathbf{A}_{m,n,r}$ и сдвигов $\mathbf{C}_{m,n,r}$, позволяющие синтезировать ГМВП по символам базисной МП.

Полученные результаты могут быть использованы в современных и перспективных СПЦИ с многофазными СРС, к которым предъявляются повышенные требования как по структурной скрытности, так и по корреляционным свойствам.

СПИСОК ЛИТЕРАТУРЫ

1. *Ипатов В.П.* Широкополосные системы и кодовое разделение сигналов. Принципы и приложения. М.: Техносфера, 2007.
2. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. М.: Вильямс, 2003.
3. *Golomb S.W., Gong G.* Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar. Cambridge: Univ. Press, 2005.

4. *Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В.* Широкополосные беспроводные сети передачи информации. М.: Техносфера, 2005.
5. *Ипатов В.П.* Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992.
6. CDMA: прошлое, настоящее, будущее. М.: МАС, 2003.
7. *Chen X., Zhang H.* // J. Theor. Appl. Inform. Technol. 2013. V. 52. № 1. P. 51.
8. *Shi X., Zhu X., Huang X., Yue Q.* // IEEE Commun. Lett. 2019. V. 23. № 7. P. 1132.
9. *Cho C.-M., Kim J.-Y., No J.S.* // IEICE Trans. Commun. 2015. V. E98. № 7. P. 1268.
10. *Kim Y.S., Chung J.S., No J.S., Chung H.* // IEEE Trans. 2008. V. IT-54. № 8. P. 3768.
11. *Стародубцев В.Г., Ткаченко В.В., Боброва Е.А.* // Изв. вузов. Приборостроение. 2020. Т. 63. № 5. С. 405.
12. *Liang H., Tang Y.* // Finite Fields and Their Appl. 2015. V. 31. P. 137.
13. *Kim J.Y., Choi S.T., No J.S., Chung H.* // IEEE Trans. 2011. V. IT-57. № 6. P. 3825.
14. *Стародубцев В.Г.* // Труды СПИИРАН. 2019. Т. 18. № 4. С. 912.
15. *No J.S.* // IEEE Trans. 1996. V. IT- 42. № 1. P. 260.
16. *Стародубцев В.Г.* // РЭ. 2022. Т. 67. № 8. С. 788.
17. *Chung H.B., No J.S.* // IEEE Trans. 1999. V. IT-45. № 6. P. 2060.
18. *Стародубцев В.Г.* // РЭ. 2020. Т. 65. № 2. С. 169.
19. *Стародубцев В.Г.* // РЭ. 2021. Т. 66. № 4. С. 380.