УДК 519.725
DOI: 10.17586/0021-3454-2024-67-8-637-646

МНОЖЕСТВА ПЯТЕРИЧНЫХ КАСАМИ-ПОДОБНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ СИСТЕМ ПЕРЕДАЧИ ЦИФРОВОЙ ИНФОРМАЦИИ

В. Г. Стародубцев, Я. Г. Морозов

Военно-космическая академия имени А. Ф. Можайского, 197198, Санкт-Петербург, Россия
vka@mil.ru

Аннотация. Для пятеричных базисных М-последовательностей с периодом $N = 5^S - 1$ ($S = 4, 6$) представлены наборы векторов индексов децимации $\mathbf{I}_{S,\text{МК}} = (d_1, d_2, \ldots, d_n)$, на основании которых в конечных полях GF(5^S) формируются малые множества касами-подобных последовательностей (КПП) с периодом $N < 20\,000$. Показано, что для значений $S = 4, 6$ периодическая взаимно корреляционная функция (ПВКФ) малого множества КПП является четырехуровневой с максимальным значением модуля ПВКФ $|R_{\max}|_{S,\text{МК}} = (5^{S/2} + 1)$. Приведены значения объемов малых множеств пятеричных КПП.

Ключевые слова: *конечное поле, корреляционная функция, М-последовательность, последовательность Касами, индекс децимации*

Ссылка для цитирования: *Стародубцев В. Г., Морозов Я. Г.* Множества пятеричных КАСАМИ-подобных последовательностей для систем передачи цифровой информации // Изв. вузов. Приборостроение. 2024. Т. 67, № 8. С. 637–646. DOI: 10.17586/0021-3454-2024-67-8-637-646.

SETS OF QUINARY KASAMI-LIKE SEQUENCES FOR DIGITAL INFORMATION TRANSMISSION SYSTEMS

V. G. Starodubtsev, Y. G. Morozov

A. F. Mozhaisky Military Space Academy, St. Petersburg, Russia
vka@mil.ru

Abstract. For quinary basic M-sequences (MS) with the period $N = 5^S - 1$ ($S = 4, 6$), sets of vectors of decimation indices $\mathbf{I}_{S,\text{MK}} = (d_1, d_2, \ldots, d_n)$ are presented, on the basis of which small sets of Kasami-like sequences (KLS) with the period $N < 20\,000$ are formed in the finite fields GF(5^S). It is shown that for values of $S = 4, 6$ the periodic cross-correlation function (PCCF) of a small set of KLS is four-level with a maximum value of the PCCF $|R_{\max}|_{S,\text{MK}} = (5^{S/2} + 1)$. The values of the volumes of small sets of quinary KLS are given.

Keywords: finite fields, correlation function, M-sequences, Kasami sequences, decimation indices

For citation: Starodubtsev V. G., Morozov Y. G. Sets of quinary Kasami-like sequences for digital information transmission systems. *Journal of Instrument Engineering*. 2024. Vol. 67, N 8. P. 637–646 (in Russian). DOI: 10.17586/0021-3454-2024-67-8-637-646.

Одной из тенденций развития систем передачи цифровой информации (СПЦИ), включающих, в частности, системы связи по спутниковым и космическим радиоканалам, является применение систем сигналов с расширенным спектром (СРС). В некоторых источниках для данных сигналов используется термин „сигналы сложной формы“ (ССФ). Это можно объяснить тем, что расширение спектра сигналов обеспечивается дополнительной модуляцией информационной последовательности с помощью псевдослучайных последовательностей (ПСП), обладающих хорошими авто- и взаимно корреляционными свойствами. При этом на длине информационного символа может укладываться от одного до нескольких периодов ПСП [1–4].

Расширение спектра сигналов позволяет повысить помехозащищенность СПЦИ по отношению как к мощным узкополосным, так и широкополосным преднамеренным помехам. Кроме того, применение СРС, формируемых на основе таких множеств ПСП, как множества последовательностей Голда, малые и большие множества Касами, множества предпочтительных пар М-последовательностей (МП), обеспечивает возможность организации кодового многостанционного доступа к ретранслятору в системах спутниковой связи. В современных СПЦИ в основном применяются двоичные сигналы, что определяет использование фазовой модуляции на 180° (ФМ-2), относительной фазовой модуляции (ОФМ), частотной модуляции, а также комбинированных видов модуляции [5–7].

Переход к многопозиционным и многофазным сигналам, формируемым на основе недвоичных последовательностей, позволяет повысить эффективность использования частотного спектра, на который накладываются ограничения в системах связи с применением радиоканалов, например, в системах мобильной и спутниковой связи [2, 4, 5]. Также многопозиционные сигналы обеспечивают более высокую структурную скрытность при передаче информации [8–10].

К недвоичным последовательностям, а также к множествам ПСП, с помощью которых формируются многофазные СРС, предъявляются жесткие требования как по корреляционным, так и по структурным свойствам. Основная задача при синтезе множеств ПСП заключается в разработке таких алгоритмов и методов формирования множеств, которые бы обеспечивали низкий уровень периодической взаимно корреляционной функции (ПВКФ) последовательностей при фиксированном объеме формируемых множеств.

Эти вопросы нашли отражение в большом количестве научных работ как в нашей стране, так и за рубежом [11–17]. Сравнительный анализ алгоритмов формирования недвоичных последовательностей с заданными корреляционными и структурными свойствами проведен в [11–13]. Вопросам повышения структурной скрытности недвоичных последовательностей и методам формирования множеств таких последовательностей уделено большое внимание в статьях [14, 15]. В работах [16, 17] рассмотрены алгоритмы формирования новых семейств недвоичных ПСП, проведен анализ корреляционных свойств, определены индексы децимации, обеспечивающие возможность синтеза троичных последовательностей с идеальной автокорреляционной функцией. В [18] получены индексы децимации для формирования множеств троичных касами-подобных последовательностей, обосновано применение данного термина при проведении исследований, касающихся вопросов формирования множеств недвоичных последовательностей.

Цель настоящей статьи заключается в нахождении в конечных полях $GF(5^S)$ со степенью расширения $S = 4, 6$ векторов индексов децимации $\mathbf{I}_S = (d_1, d_2, \ldots, d_n)$ для формирования малых множеств пятеричных КПП с низким уровнем взаимной корреляции.

Корреляционные свойства СРС полностью определяются корреляционными свойствами пятеричных ПСП, на основании которых проводилось расширение спектра сигнала [1, 3, 5]:

$$A = \{a_i\} = \{a_0, a_1, ..., a_{N-1}\}, \quad (1)$$

где $N = 5^S - 1$ — период последовательности, $a_i = \exp(j2\pi i/5)$; $(i = 0, 1, \ldots, 4)$ — элементы комплекснозначного алфавита (корни 5-й степени из единицы).

На рис. 1 представлены элементы комплекснозначного алфавита для значений $p = 2$ (*а*) и $p = 3$ (*б*). При формировании и анализе ПСП элементы a_i представляются как элементы, принадлежащие простому полю Галуа GF(p), т. е. $a_i = 0, 1, \ldots, p - 1$.

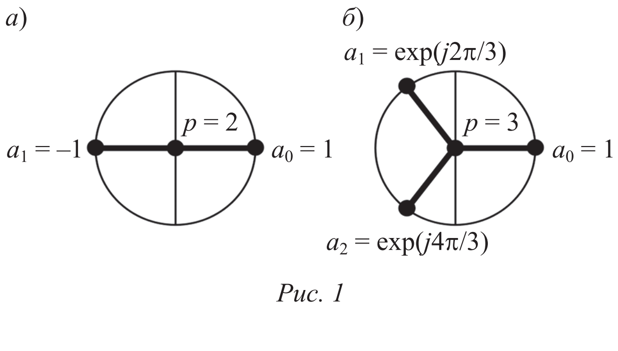

Рис. 1

Если элемент a_i принадлежит комплекснозначному алфавиту, то используется метрика в евклидовом пространстве. При этом для ПВКФ последовательностей A_j и A_k с периодом N справедливо выражение [5, 7, 10]:

$$R_{jk}(\tau) = \sum_{i=0}^{N-1} a_{ji} a^{*}_{k,i+\tau}, \tag{2}$$

где „*“ — знак комплексного сопряжения; τ — циклический сдвиг.

Если элемент a_i рассматривается как элемент простого поля GF(p), то вычисления проводятся в метрике Хемминга при $p = 2$ или в метрике Ли при $p > 2$ [3, 10]. Для определения корреляционной функции сначала находится расстояние между последовательностями A_j и A_k:

$$D_{jk}(\tau) = \sum_{i=0}^{N-1} d(a_{ji}, a_{k,i+\tau}), \tag{3}$$

где $d(a_{ji}, a_{k,i+\tau})$ — расстояние между символами последовательностей в метриках Хемминга или Ли.

Тогда ПВКФ последовательностей определяется выражением [10]:

$$R_{jk}(\tau) = N - \frac{4}{p} D_{jk}(\tau). \tag{4}$$

По аналогии с двоичным случаем формирование последовательностей малых множеств пятеричных КПП осуществляется следующим образом. Определяются символы c_i ($i = 0, \ldots, N-1$) базисной МП в соответствии с выражением [3, 5, 6]:

$$c_i = \mathrm{tr}_{S1}\alpha^i,\ i = 0, 1, \ldots, 5^S - 2, \tag{5}$$

где $\mathrm{tr}_{S1}(\alpha^i)$ — функция следа, т. е. отображение элемента α^i, принадлежащего расширенному полю GF(5^S), в простое поле GF(5).

Производится децимация символов базисной МП по индексам d_j, которые определяются с учетом выполнения условия НОД ($5^S - 1$; $5^{S/2} - 1$) = $5^{S/2} - 1$, где НОД (a, b) — наибольший общий делитель чисел a и b. Полученная МП с периодом $N_1 = 5^{S/2} - 1$ складывается с базисной МП, в результате чего образуются символы b_i последовательности малого множества КПП.

Процедура формирования последовательностей малого множества КПП с периодом $N = 5^S - 1$ может быть реализована как программным, так и аппаратным способом.

При программном способе формирования для получения символов b_i необходимо сложить по mod 5 символы c_i вида (5) и символы $c_{i\times d_j \mathrm{mod}(5^S-1)}$, полученные в результате децимации МП по индексу d_j

$$b_i = c_i \times c_{i\times d_j \mathrm{mod}(5^S-1)} \mathrm{mod}5;\ i = 0, 1, 2, \ldots, 5^S - 2. \tag{6}$$

Таким образом, для формирования малого множества КПП требуется только знание символов базисной МП и индекса децимации d_j.

Аппаратная реализация процедуры формирования основана на использовании двух регистров сдвига, охваченных цепью обратной связи. Первый регистр строится на основе проверочного полинома $h_1(x)$ степени S, а второй регистр — на основе проверочного полинома $h_{dj}(x)$ степени S/2. Умножители и сумматоры по mod 5 в цепи обратной связи регистров сдвига определяются коэффициентами проверочных полиномов. В этом случае для формирования малого множества КПП требуется знание структуры двух проверочных полиномов $h_1(x)$ и $h_{dj}(x)$, произведение которых соответствует проверочному полиному малого множества КПП $h_{\text{МК}}(x) = h_1(x)\, h_{dj}(x)$. Индексы в обозначениях проверочных полиномов $h_i(x)$, используемые в статье, соответствуют показателям степени корней этих полиномов.

Граничные оценки для модуля максимального значения ПВКФ $|R_{\max}|_{S,\text{МК}}$ и коэффициента корреляции $|r_{\max}|_{S,\text{МК}} = |R_{\max}|_{S,\text{МК}}/N$, а также объема малого множества КПП определяются выражениями [5, 6]:

$$|R_{\max}|_{S,\text{МК}} = 5^{S/2} + 1,\ |r_{\max}|_{S,\text{МК}} = (5^{S/2} - 1)^{-1}, \tag{7}$$

$$V_{S,\text{МК}} = 5^{S/2}. \tag{8}$$

Рассмотрим процедуру формирования малого множества КПП в конечном поле $GF(5^S) = GF(5^4)$ с примитивным полиномом $f(x) = h_1(x) = x^4 + x^2 + 2x + 2$.

В поле $GF(5^4)$ минимальный полином для примитивного элемента $\alpha = a$ в общем виде определяется выражением

$$h_1(x) = x^4 - x^3\sum_{i=0}^{3}\alpha^{5^i} + x^2\sum_{\substack{i=0\\i<j}}^{3}\sum_{j=0}^{3}\alpha^{5^i}\alpha^{5^j} + x\sum_{\substack{i=0\\i<j<k}}^{3}\sum_{j=0}^{3}\sum_{k=0}^{3}\alpha^{5^i}\alpha^{5^j}\alpha^{5^k} + \alpha^{5^0}\alpha^{5^1}\alpha^{5^2}\alpha^{5^3}. \tag{9}$$

После выполнения операций суммирования и группирования слагаемых в соответствии с функцией следа $tr_{S1}(\alpha^i)$ получим

$$h_1(x) = x^4 - tr_{41}(\alpha)x^3 + [tr_{41}(\alpha^6) + tr_{21}(\alpha^{26})]x^2 - tr_{41}(\alpha^{31})x + \alpha^{156}. \tag{10}$$

Коэффициенты полинома $h_1(x)$, представленного в общем виде

$$h_1(x) = x^S + h_{S-1}x^{S-1} + \ldots + h_1x + h_0 = x^4 + h_3x^3 + h_2x^2 + h_1x + h_0, \tag{11}$$

в соответствии с (10) определяются выражениями

$$h_3 = -tr_{41}(\alpha);\ h_2 = tr_{41}(\alpha^6) + tr_{21}(\alpha^{26});\ h_1 = -tr_{41}(\alpha^{31});\ h_0 = \alpha^{156}. \tag{12}$$

В поле $GF(5^4)$ существует 48 примитивных полиномов с индексами децимации $d_j = 1, 7, 11, \ldots, 373, 469, 499$. Значения коэффициентов для восемнадцати полиномов приведены в табл. 1 [19].

В подполе $GF(5^2)$ минимальные полиномы определяются выражением

$$h_i(x) = (x - \alpha^{26i})(x - \alpha^{130i}) = x^2 - tr(\alpha^{26i})x + \alpha^{130i}, \tag{13}$$

где $i = 1, 2, \ldots, 23$; операции умножения в показателях степени выполняются по mod 624.

Существует десять минимальных полиномов степени 2 с периодами $N = 24, 12, 8, 6, 3$, которые приведены в табл. 2.

Для формирования малого множества КПП могут быть использованы четыре полинома с периодом корней $N = 24$: $h_{26}(x) = x^2 + x + 2$; $h_{182}(x) = x^2 + 2x + 3$; $h_{338}(x) = x^2 + 4x + 2$ и $h_{494}(x) = x^2 + 3x + 3$.

***Таблица 1**. Примитивные полиномы в поле $GF(5^4)$, $f(x) = h_1(x) = x^4 + x^2 + 2x + 2$*

d_j	$h_j(x)$	d_j	$h_j(x)$	d_j	$h_j(x)$	d_j	$h_j(x)$	d_j	$h_j(x)$	d_j	$h_j(x)$
1	10122	17	11212	29	13302	239	11113	323	10133	373	120022
7	11013	19	13023	31	12203	313	10132	343	13203	469	10442
11	10123	23	13043	37	11202	319	14043	349	14202	499	11303

***Таблица 2**. Минимальные полиномы в подполе $GF(5^2)$, $f(x) = h_{26}(x) = x^2 + 2x + 2$*

d_j	$h_j(x)$	N	d_j	$h_j(x)$	N	d_j	$h_j(x)$	N	d_j	$h_j(x)$	N	d_j	$h_j(x)$	N
26	112	24	78	103	8	182	123	24	234	102	8	364	124	12
52	134	12	104	141	6	208	111	3	338	142	24	494	133	24

Анализ корреляционных свойств последовательностей, образованных с помощью проверочных полиномов $h_{\text{МК}}(x) = h_1(x) \cdot h_{dj}(x)$ для $d_j = 26$, 338, в соответствии с (2)–(4) показал, что ПВКФ данных последовательностей удовлетворяет граничной оценке (7) и принимает следующие четыре значения:

$$R_{S,\text{МК}}(\tau) = R_{4,\text{МК}}(\tau) = [-26; -8{,}725; -1; 19{,}225]. \quad (14)$$

Проверочные полиномы малых множеств КПП с периодом $N = 5^4 - 1 = 624$ определяются выражениями

$$h_{\text{МК}1}(x) = h_1(x) \cdot h_{26}(x) = (x^4 + x^2 + 2x + 2)(x^2 + x + 2),$$
$$h_{\text{МК}2}(x) = h_1(x) \cdot h_{338}(x) = (x^4 + x^2 + 2x + 2)(x^2 + 4x + 2). \quad (15)$$

Объем малых множеств КПП соответствует (8) и равен

$$V_{4,\text{МК}} = 5^{S/2} = 5^2 = 25. \quad (16)$$

Вектор индексов децимации при формировании малых множеств пятеричных КПП с периодом $N = 624$ имеет вид

$$\mathbf{I}_{S,\text{МК}} = \mathbf{I}_{4,\text{МК}} = (26, 338). \quad (17)$$

Общее число малых множеств пятеричных КПП с периодом $N = 624$ определяется числом примитивных полиномов в поле GF(5^4): $M_{S,\text{МК}} = M_{4,\text{МК}} = 96$. Корреляционные и структурные свойства характеризуются максимальными значениями $|R_{\max}|_{4,\text{МК}} = 26$, $|r_{\max}|_{4,\text{МК}} = 0{,}042$ и объемом $V_{4,\text{МК}} = 5^{4/2} = 25$.

Для каждого из 48 примитивных полиномов поля GF(5^4) можно сформировать малое множество КПП. С этой целью необходимо индексы множителей в выражении для $h_{\text{МК}}(x)$ умножить на индекс данного полинома. Например, для полинома $h_{31}(x)$ проверочные полиномы малого множества КПП равны $h_{\text{МК}3}(x) = h_{31}(x)h_{182}(x) = (x^4 + 2x^3 + 2x^2 + 3)(x^2 + 2x + 3)$, $h_{\text{МК}4}(x) = h_{31}(x)h_{494}(x)$. На рис. 2 приведен график сегмента длиной 126 символов ПВКФ малого множества КПП с полиномом $h_{\text{МК}3}(x) = h_{31}(x)\ h_{182}(x)$.

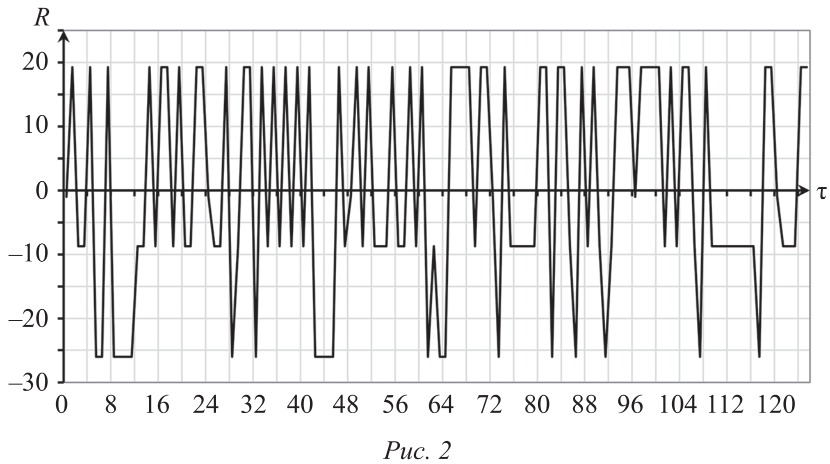

Рис. 2

Проверочный полином для синтеза пятеричных последовательностей большого множества КПП с периодом $N = 5^S - 1$ (S — четное) является произведением трех полиномов, два из которых степени S, а третий — степени $S/2$.

Проведенный анализ корреляционных свойств данных последовательностей как при $S = 4$, так и при $S = 6$ показал, что ПВКФ последовательностей полученных множеств не обладает ограниченным числом уровней и не удовлетворяет граничным оценкам для $|R_{\max}|_{S,\text{БК}}$ [7, 18].

Таким образом, формирование больших множеств пятеричных КПП с периодами $N = 624$, 15 624 не представляется возможным.

Рассмотрим процедуру формирования малого множества КПП в конечном поле $GF(5^S) = GF(5^6)$ с примитивным полиномом $f(x) = h_1(x) = x^6 + x^2 + 2x + 2$.

В поле $GF(5^6)$ минимальный полином для примитивного элемента α в общем виде определяется выражением

$$h_1(x) = x^6 - x^5\sum_{i=0}^{5}\alpha^{5^i} + x^4\sum_{\substack{i=0\\i<j}}^{5}\sum_{j=0}^{5}\alpha^{5^i}\alpha^{5^j} - x^3\sum_{\substack{i=0\\i<j<k}}^{5}\sum_{j=0}^{5}\sum_{k=0}^{5}\alpha^{5^i}\alpha^{5^j}\alpha^{5^k} + x^2\sum_{\substack{i=0\\i<j<\ldots l<m}}^{5}\sum_{j=0}^{5}\sum_{l=0}^{5}\sum_{m=0}^{5}\alpha^{5^i}\alpha^{5^j}\alpha^{5^l}\alpha^{5^m} -$$
$$- x\sum_{\substack{i=0\\i<j<\ldots l<m<n}}^{5}\sum_{j=0}^{5}\sum_{l=0}^{5}\sum_{m=0}^{5}\sum_{n=0}^{5}\alpha^{5^i}\alpha^{5^j}\alpha^{5^l}\alpha^{5^m}\alpha^{5^n} + \alpha^{5^0}\alpha^{5^1}\alpha^{5^2}\alpha^{5^3}\alpha^{5^4}\alpha^{5^5}. \quad (18)$$

После выполнения операций суммирования с учетом выражений для функций следа минимальный полином (18) преобразуется к виду

$$\begin{aligned} h_1(x) = x^6 - x^5\mathrm{tr}_{61}(\alpha) + x^4[\mathrm{tr}_{61}(\alpha^6) + \mathrm{tr}_{61}(\alpha^{26}) + \mathrm{tr}_{31}(\alpha^{126})] - \\ - x^3[\mathrm{tr}_{61}(\alpha^{31}) + \mathrm{tr}_{61}(\alpha^{131}) + \mathrm{tr}_{61}(\alpha^{151}) + \mathrm{tr}_{21}(\alpha^{651})] + \\ + x^2[\mathrm{tr}_{61}(\alpha^{156}) + \mathrm{tr}_{61}(\alpha^{656}) + \mathrm{tr}_{31}(\alpha^{756})] - x\mathrm{tr}_{61}(\alpha^{781})] + \alpha^{3906}. \end{aligned} \quad (19)$$

Коэффициенты h_i минимального полинома (19) представляют собой сумму функций следа как из основного поля $GF(5^6)$, так и из его подполей $GF(5^3)$ и $GF(5^2)$ в простом поле $GF(5)$.

Отметим, что значения данных коэффициентов можно вычислить путем сложения по mod 5 символов ПСП, получаемых в результате децимации символов базисной МП, представленной в каноническом виде, по индексам децимации, равным показателям степени элемента α в выражениях для функций следа $\mathrm{tr}(\alpha^i)$.

В поле $GF(5^6)$ имеется 720 примитивных полиномов, двенадцать из которых приведены в табл. 3 [19].

В подполе $GF(5^3)$ минимальные полиномы степени 3 определяются выражением

$$h_i(x) = (x - \alpha^{126i})(x - \alpha^{630i})(x - \alpha^{3150i}) = x^3 - \mathrm{tr}(\alpha^{126i})x^2 + \mathrm{tr}(\alpha^{756i})x - \alpha^{3906i}, \quad (20)$$

где $i = 1, 2,\ldots, 123$; операции умножения в показателях степени выполняются по mod 15624.

Существует 20 минимальных полиномов степени 3 с периодом $N = 124$, которые приведены в табл. 4.

Таблица 3. *Примитивные полиномы в поле $GF(5^6)$, $f(x) = h_1(x) = x^6 + x^2 + 2x + 2$*

d_j	$h_j(x)$	d_j	$h_j(x)$	d_j	$h_j(x)$	d_j	$h_j(x)$	d_j	$h_j(x)$	d_j	$h_j(x)$
1	1000122	13	1143012	19	1010343	9343	1440203	11719	1000113	11869	1223202
11	1113023	17	1241342	23	1314323	9349	1012422	11849	1043132	12499	1130003

Таблица 4. *Минимальные полиномы в подполе $GF(5^3)$, $f(x) = h_{126}(x) = x^3 + x^2 + 4x + 3$*

d_j	$h_j(x)$	d_j	$h_j(x)$	d_j	$h_j(x)$	d_j	$h_j(x)$	d_j	$h_j(x)$
126	1143	1386	1312	2646	1033	4914	1222	7938	1442
378	1302	1638	1203	2898	1412	5418	1032	8694	1343
882	1242	2142	1113	4158	1403	5922	1042	9198	1213
1134	1323	2394	1102	4662	1223	6174	1043	12474	1322

Проведенный в соответствии с (2)–(4) анализ корреляционных свойств последовательностей, образованных с помощью проверочных полиномов $h_{\text{МК}}(x) = h_1(x)\cdot h_{dj}(x)$, для значений d_j из табл. 4 показал, что только для двух полиномов возможно формирование малых множеств КПП.

Малые множества КПП с периодом $N = 15\,624$ формируются на основе проверочных полиномов вида

$$\begin{aligned} h_{\text{МК5}}(x) &= h_1(x)\cdot h_{126}(x) = (x^6 + x^2 + 2x + 2)(x^3 + x^2 + 4x + 3); \\ h_{\text{МК6}}(x) &= h_1(x)\cdot h_{7938}(x) = (x^6 + x^2 + 2x + 2)(x^3 + 4x^2 + 4x + 2). \end{aligned} \tag{21}$$

Взаимно корреляционная функция последовательностей данного множества является четырехуровневой, удовлетворяет граничной оценке (7) и принимает следующие значения:

$$R_{S,\text{МК}}(\tau) = R_{6,\text{МК}}(\tau) = [-126; -39{,}627; -1; 100{,}127]. \tag{22}$$

Объем малого множества КПП соответствует (8) и равен

$$V_{6,\text{МК}} = 5^{S/2} = 5^3 = 125. \tag{23}$$

Вектор индексов децимации при формировании малых множеств пятеричных КПП с периодом $N = 15\,624$ имеет вид

$$\mathbf{I}_{S,\text{МК}} = \mathbf{I}_{6,\text{МК}} = (126,\ 7938). \tag{24}$$

Общее число малых множеств пятеричных КПП с периодом $N = 15\,624$ равно $M_{S,\text{МК}} = M_{6,\text{МК}} = 1440$, максимальное значение модуля ПВКФ $|R_{\max|6,\text{МК}} = 126$, объем множеств равен $V_{6,\text{МК}} = 5^{6/2} = 125$.

Проверочные полиномы малых множеств КПП с периодом $N = 15\,624$ для произвольного примитивного полинома вычисляются путем умножения индексов множителей полиномов $h_{\text{МК5}}(x)$ или $h_{\text{МК6}}(x)$ из (21) на индекс произвольного примитивного полинома по mod N. Например, для примитивного полинома $h_{9343}(x)$ проверочные полиномы малого множества КПП равны $h_{\text{МК7}}(x) = h_{9343}(x)h_{5418}(x) = (x^6 + 4x^5 + 4x^4 + 2x^2 + 3)(x^3 + 3x + 2)$, $h_{\text{МК8}}(x) = h_{9343}(x)h_{13230}(x)$. На рис. 3 приведен график сегмента длиной 126 символов ПВКФ малого множества КПП с полиномом $h_{\text{МК7}}(x) = h_{9343}(x)h_{5418}(x)$.

Программный способ формирования пятеричных последовательностей малого множества КПП с периодом $N = 15\,624$ реализуется в соответствии с (6).

Реализация аппаратного способа формирования аналогична случаю $N = 624$. На рис. 4 показана схема устройства формирования малого множества КПП с проверочным полиномом $h_{\text{МК6}}(x) = h_1(x)\cdot h_{7938}(x)$.

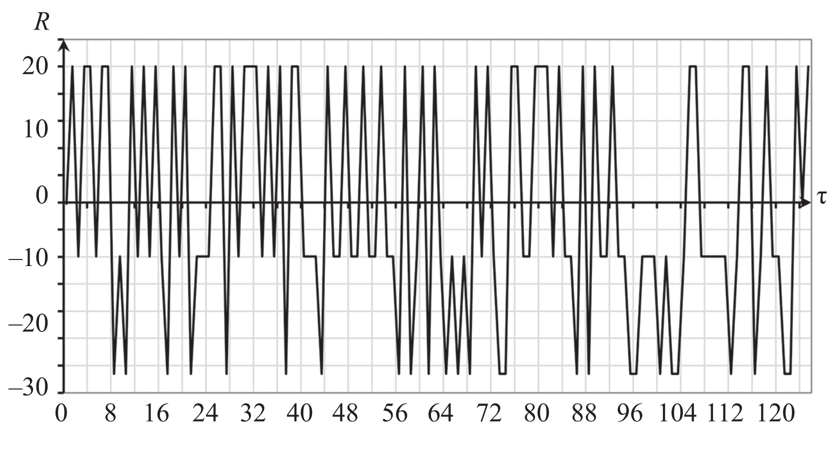

Рис. 3

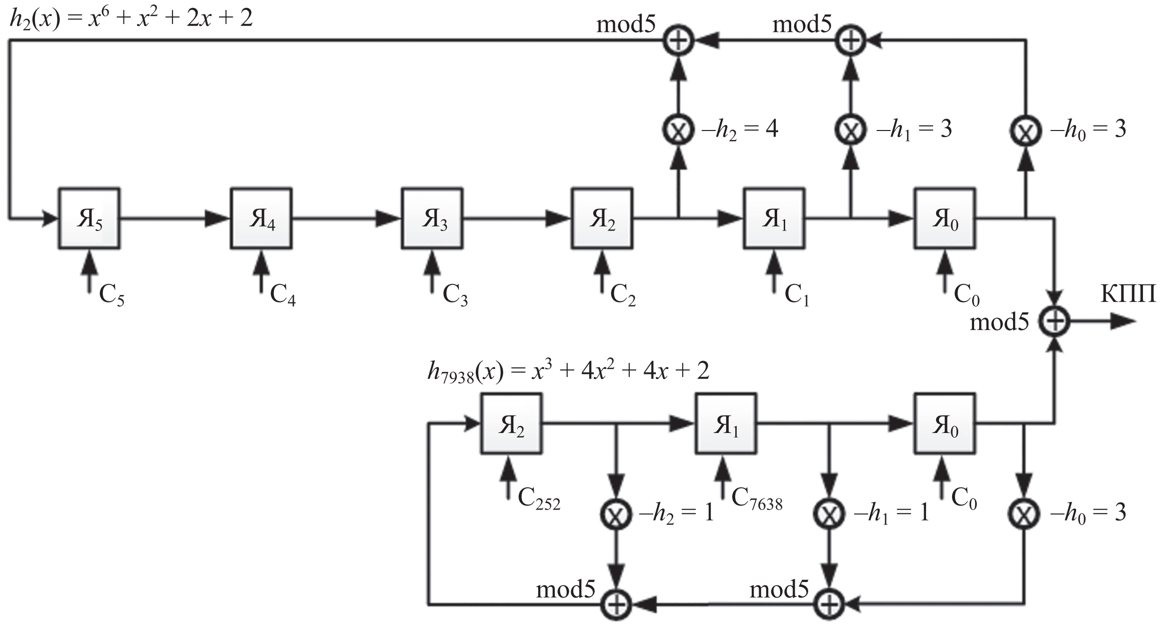

Рис. 4

Умножители и сумматоры в цепи обратной связи регистров сдвига определяются полиномами $h_1(x) = x^6 + x^2 + 2x + 2$ и $h_{7938}(x) = x^3 + 4x^2 + 4x + 2$. Ячейки регистра сдвига представляют собой устройства, которые могут находиться в пяти состояниях и строиться с помощью трех триггеров. На схеме в качестве начальных состояний первого регистра используются первые шесть символов записи МП в каноническом виде с полиномом $h_1(x)$. Начальное состояние второго регистра определено децимацией по индексу $d_j = 7938$ базисной МП с полиномом $h_1(x)$. Коэффициенты умножения в умножителях по mod 5 равны обратным по сложению коэффициентам h_i неприводимых полиномов. Выходы регистров подключены к общему сумматору по mod 5, который является выходом устройства.

Основные характеристики малых множеств КПП, формируемых в конечных полях GF(5^S) для четных значений параметра $S = 4, 6$, приведены в табл. 5.

***Таблица 5**. Характеристики малых множеств пятеричных КПП*

S	N	$\mathbf{I}_{S,\text{МК}} = (d_1, d_2)$	Значения ПВКФ	$\lvert R_{\max}\rvert$	$\lvert r_{\max}\rvert$	Число уровней ПВКФ	$V_{S,\text{МК}}$	$M_{S,\text{МК}}$
4	624	26, 338	–26; –8,73; –1; 19,23	26	0,042	4	25	96
6	15624	126, 7938	–126; –39,63; –1, 100,13	126	0,008	4	125	1440

Таким образом, на основе корреляционного анализа в статье получены полные наборы векторов индексов децимации $\mathbf{I}_{S,\text{МК}} = (d_1, \ldots, d_n)$ для формирования малых множеств пятеричных КПП с низким уровнем взаимной корреляции в полях GF(5^S) при $S = 4, 6$. Показано, что максимальные значения модуля взаимной корреляционной функции $|R_{\max}|_{S,\text{МК}}$, а также объем $V_{S,\text{МК}}$ малых множеств КПП удовлетворяют граничным оценкам, полученным в [5, 6] для двоичных последовательностей.

Полученные результаты могут применяться при формировании многофазных сигналов с расширенным спектром в СПЦИ для повышения помехозащищенности в случае передачи информации по радиоканалам.

СПИСОК ЛИТЕРАТУРЫ

1. *Ипатов В. П.* Широкополосные системы и кодовое разделение сигналов. Принципы и приложения. М.: Техносфера, 2007. 488 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. М.: Вильямс. 2003. 1104 с.
4. CDMA: прошлое, настоящее, будущее / Под ред. *Л. Е. Варакина и Ю. С. Шинакова*. М.: МАС, 2003. 608 с.
5. *Golomb S. W., Gong G.* Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar. Cambridge: Cambridge Univ. Press, 2005.
6. *Ипатов В. П.* Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992. 152 с.
7. *Gold R*. Maximal recursive sequences with 3-valued recursive cross-correlation functions // IEEE Trans. Inf. Theory. 1968. Vol. 14, N 1. P. 154.
8. *Boztaş S., Özbudak F., Tekin E*. Generalized nonbinary sequences with perfect autocorrelation flexible alphabets and new periods // Cryptogr. Commun. 2018. Vol. 10, N 3. P. 509.
9. *Cho Ch.-M., Kim J.-Y., No J. S.* New p-ary sequence families of period $(p^n - 1)/2$ with good correlation property using two decimated m-sequences // IEICE Transactions on Communications. 2015. Vol. E98, N 7. P. 1268.
10. *Стародубцев В. Г.* Формирование пятеричных последовательностей Гордона–Миллса–Велча для систем передачи дискретной информации // Тр. СПИИРАН. 2019. Т. 18, № 4. С. 912.
11. *Choi S. T., Lim T., No J. S., Chung H.* On the Cross-Correlation of a p-ary m- Sequence of Period $p^{2m} – 1$ and Its Decimated Sequences by $(p^m + 1)^2/2(p + 1)$ // IEEE Trans. Inf. Theory. 2012. Vol. 58, N 3. P. 1873.
12. *Xia Y., Chen S.* A new family of p-ary sequences with low correlation constructed from decimated sequences // IEEE Trans. Inf. Theory. 2012. Vol. 58, N 9. P. 6037.
13. *Lee W., Kim J.-Y., No J. S.* New families of p-ary sequence of period (pn– 1)/2 with low maximum correlation magnitude // IEICE Transactions on Communications. 2014. Vol. E97-B, N 1. P. 2311.
14. *Song M. K., Song H. Y.* A construction of odd length generators for optimal families of perfect sequences // IEEE Trans. Inf. Theory. 2018. Vol. 64, N 4. P. 2901.
15. *Стародубцев В. Г*. Множества недвоичных последовательностей с низким уровнем взаимной корреляции для систем передачи цифровой информации // Радиотехника и электроника. 2023. Т. 68, № 2. С. 146.
16. *Helleseth T., Kumar P. V., Martinsen H.* A new family of ternary sequences with ideal two-level autocorrelation function // Designs, Codes and Cryptography. 2001. Vol. 23, N 2. P. 157.
17. *Jang J. W., Kim Y. S., No J. S., Helleseth T.* New family of p-ary sequences with optimal correlation property and large linear span // IEEE Trans. Inf. Theory. 2004. Vol. 50, N 8. P. 1839.
18. *Стародубцев В. Г., Четвериков Е. А*. Формирование множеств троичных касами-подобных последовательностей для систем передачи цифровой информации // Изв. вузов. Приборостроение. 2023. Т. 66, № 10. С. 807.
19. *Стародубцев В. Г., Ткаченко В. В.* Формирование множеств пятеричных голд-подобных последовательностей для систем передачи цифровой информации // Изв. вузов. Приборостроение. 2024. Т. 67, № 2. С. 107.

СВЕДЕНИЯ ОБ АВТОРАХ

Виктор Геннадьевич Стародубцев — канд. техн. наук, доцент; Военно-космическая академия им. А. Ф. Можайского, кафедра технологий и средств автоматизации обработки и анализа информации космических средств; преподаватель; E-mail: vgstarod@mail.ru

Ян Геннадьевич Морозов — Военно-космическая академия им. А. Ф. Можайского, кафедра технологий и средств автоматизации обработки и анализа информации космических средств; слушатель; E-mail: vka@mil.ru

Поступила в редакцию 22.04.2024; одобрена после рецензирования 26.04.2024; принята к публикации 19.06.2024.

REFERENCES

1. Ipatov V.P. *Spread Spectrum and CDMA. Principles and Applications*, NY, John Wiley and Sons Ltd., 2005, 488 p.
2. Vishnevskij V.M., Lyahov A.I., Portnoj S.L., Shahnovich I.V. *Shirokopolosnye besprovodnye seti peredachi informacii* (Broadband Wireless Data Transmission Network), Moscow, 2005, 592 p. (in Russ.)
3. Sklar B. *Digital Communications: Fundamentals and Applications*, Prentice Hall, 2001, 1079 p.

4. Varakin L.E. and Shinakov Yu.S., ed., *CDMA: proshloe, nastoyashchee, budushchee* (CDMA: Past, Present, Future), Moscow, 2003, 608 p. (in Russ.)
5. Golomb S.W., Gong G. *Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar*, Cambridge, Cambridge Univ. Press, 2005.
6. Ipatov V.P. *Periodicheskie diskretnye signaly s optimal'nymi korrelyacionnymi svojstvami* (Periodic Discrete Signals with Optimum Correlation Properties), Moscow, 1992, 152 p. (In Russ.)
7. Gold R. *IEEE Trans. Inf. Theory*, 1968, no. 1(14), pp. 154.
8. Boztaş S., Özbudak F., Tekin E. *Cryptogr. Commun*., 2018, no. 3(10), pp. 509.
9. Cho Ch.-M., Kim J.-Y., No J.S. *IEICE Transactions on Communications*, 2015, no. 7(E98), pp. 1268.
10. Starodubtsev V.G. *Trudy SPIIRAN* (SPIIRAS Proceedings), 2019, no. 4(18), pp. 912. (in Russ.)
11. Choi S.T., Lim T., No J.S., Chung H. *IEEE Trans. Inf. Theory*, 2012, no. 3(58), pp. 1873.
12. Xia Y., Chen S. *IEEE Trans. Inf. Theory*, 2012, no. 9(58), pp. 6037.
13. Lee W., Kim J.-Y., No J.S. *IEICE Transactions on Communications*, 2014, no. 1(E97-B), pp. 2311.
14. Song M.K., Song H.Y. *IEEE Trans. Inf. Theory*, 2018, no. 4(64), pp. 2901.
15. Starodubtsev V.G. *Journal of Communications Technology and Electronics*, 2023, no. 2(68), pp. 128. (in Russ.)
16. Helleseth T., Kumar P.V., Martinsen H. *Designs, Codes and Cryptography*, 2001, no. 2(23), pp. 157.
17. Jang J.W., Kim Y.S., No J.S., Helleseth T. *IEEE Trans. Inf. Theory*, 2004, no. 8(50), pp. 1839.
18. Starodubtsev V.G., Chetverikov E.A. *Journal of Instrument Engineering*, 2023, no. 10(66), pp. 807. (in Russ.)
19. Starodubtsev V.G., Tkachenko V.V. *Journal of Instrument Engineering*, 2024, no. 2(67), pp. 107. (in Russ.)

DATA ON AUTHORS

Victor G. Starodubtsev	—	PhD, Associate Professor; A. F. Mozhaisky Military Space Academy, Department of Technologies and Automation Tools for Processing and Analysis of Spacecraft Information; Lecturer; E-mail: vgstarod@mail.ru
Yan G. Morozov	—	A. F. Mozhaisky Military Space Academy, Department of Technologies and Automation Tools for Processing and Analysis of Spacecraft Information; Student; E-mail: vka@mil.ru

Received 22.04.2024; approved after reviewing 26.04.2024; accepted for publication 19.06.2024.