МНОГОСТАНЦИОННЫЙ ДОСТУП НА ОСНОВЕ ЦИРКУЛЯРНЫХ МАТРИЦ МНОГОПОЗИЦИОННЫХ ЛИНЕЙНЫХ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

DOI: 10.36724/2072-8735-2025-19-3-37-53

Горгадзе Светлана Феликсовна,
Московский технический университет связи и информатики, Москва, Россия, **s.f.gorgadze@mtuci.ru**

Ермакова Анастасия Всеволодовна,
Московский технический университет связи и информатики, Москва, Россия, **msikisylia@gmail.com**

Кудряшова Анастасия Юрьевна,
Московский технический университет связи и информатики, Москва, Россия

Manuscript received 30 January 2025;
Accepted 05 March 2025

Ключевые слова: *дискретные ортогональные системы сигналов, функции Виленкина-Крестенсона, дискретные экспоненциальные функции, системы Уолша-Адамара, обобщенное быстрое преобразование Фурье, ортогональные и неортогональные поднесущие, компенсация взаимных помех*

Разработаны варианты построения систем ортогональных сигнатур на основе циркулярных матриц многопозиционных линейных рекуррентных последовательностей максимального периода. Показано, что любая матрица данного класса приводится к матрице функций Виленкина-Крестенсона с помощью уникального линейного оператора, основу которого составляет перестановка строк и столбцов циркулярной матрицы по возрастанию значений элементов мультипликативной группы расширенного поля Галуа по модулю неприводимого примитивного полинома, использовавшегося при формировании исходной последовательности. Установлено, что передача в радиоканале потока информационных символов на основе любой системы вышеупомянутых сигнатур и быстрая обработка результирующего сигнала в приемнике на основе обобщенного быстрого преобразования Фурье в базисе функций Виленкина-Крестенсона связаны с несколькими вариантами перемежения передаваемых информационных символов. Показано, что использование для передачи информации одновременно нескольких разных систем разработанных ортого-нальных сигнатур в сочетании с быстрым алгоритмом компенсации их взаимных помех на основе обобщенного быстрого преобразования Фурье в базисе функций Виленкина-Крестенсона позволяет в повысить пропускную способность канала связи в число раз, равное числу одновременно использующихся систем, по сравнению с методом передачи информации на основе одной системы ортогональных функций, и полностью скомпенсировать взаимные помехи. Новый способ компенсации взаимных помех является результатом ранее неизвестных свойств систем предлагаемых ортогональных сигналов, выявленных в данной работе. Данное увеличение пропускной способности канала связи возможно при совместной компенсации шумовой помехи.

Для цитирования:
Горгадзе С.Ф., Ермакова А.В., Кудряшова А.Ю. Многостанционный доступ на основе циркулярных матриц многопозиционных линейных рекуррентных последовательностей // T-Comm: Телекоммуникации и транспорт. 2025. Том 19. №3. С. 37-53.

For citation:
S. F. Gorgadze, A. V. Ermakova, A. Yu. Kudryashova, "Multi-station access based on circular matrices of multi-position linear recurrence sequences," *T-Comm*, 2025, vol. 19, no.3 pp. 37-53. (*in Russian*)

Введение

Модулированные системы ортогональных функций, при формировании и обработке которых используются спектральные преобразования, в настоящее время широко используются в телекоммуникационных системах, прежде всего, в сотовых сетях мобильной связи [1-5], в различных системах радиосвязи и радиовещания [6-8], при передаче телевизионных сигналов [1, 2] и т.д. Вместе с тем, в практических приложениях применяются лишь два типа таких систем функций, являющихся частными случаями системы Виленкина-Крестенсона (ВК), - это система дискретных экспоненциальных функций (ДЭФ) и система функций Уолша-Адамара. Спектральные преобразования на основе этих систем функций являются частным случаем соответствующего преобразования в системе ВК, называемого обобщенным преобразованием Фурье, а его быстрый вариант будем называть обобщенным быстрым преобразованием Фурье (БПФ) [9-15].

Применение ДЭФ рассматривалось в качестве основы для формирования телекоммуникационных сигналов еще в начале 60-х годов, а их теория развита в [12]. Как известно, дискретные аналоги сигналов OFDM (orthogonal frequency-division multiplexing) представляют собой ДЭФ, в результате чего при их демодуляции оказалось возможным применение традиционного БПФ [14]. Ортогональная система дискретных функций Уолша-Адамара и соответствующее ей быстрое преобразование Адамара (БПА) применяется в cdma-системах мобильной связи 3-его поколения и в спутниковой системе Globalstar [7, 8]. Как БПФ, так и БПА являются частными случаями обобщенного БПФ [12].

Число ортогональных сигналов в системе всегда соответствует размерности используемой матрицы дискретных функций, поэтому присоединение к ней любых дополнительных функций с целью повышения пропускной способности канала связи приводит к появлению взаимных помех одновременно передаваемых сигналов и, следовательно, позволяет получить необходимый результат только в случае возможности снижения требований к качеству передачи информации, по сравнению с вариантом использования только ортогональной системы сигналов. Компенсация взаимных помех, как правило, требует значительных вычислительных затрат [16-23]. Дополнительные сигналы не могут быть обработаны в контексте применяемого быстрого преобразования.

Основную идею этой статьи составляет рассмотрение возможности использования для передачи информации матриц-циркулянтов в общем случае скремблированных p-ичных линейных рекуррентных последовательностей (ЛРП), включая М-последовательности, в качестве наборов дискретных ортогональных сигналов. Как известно, частными случаями p-ичных ЛРП являются М-последовательности (МП), теория которых развита в работах [24-27]. Как показано в [25], их матрицы-циркулянты при перестановке столбцов приводятся к системам функций Уолша и, следовательно, при демодуляции соответствующих систем сигналов может использоваться БПА. Как показано в [26], все варианты матриц-циркулянтов таких функций одной и той же размерности преобразуются к одной и той же матрице функций Уолша. То есть, если для передачи информации используются одновременно несколько полных наборов матриц-циркулянтов разных МП одной и той же длины, то при линейном преобразовании входной смеси сигналов по некоторому правилу можно получить матрицу функций Уолша, модулированную набором информационных символов, при преобразовании той же смеси по другому правилу – получим ту же матрицу функций Уолша, но модулированную другим набором информационных символов и т.д. При этом будут образовываться взаимные помехи, соответствующие значениям периодической взаимно корреляционной функции (ПВКФ) используемых псевдослучайных последовательностей (ПСП). Очевидно, выбирая пары так называемых предпочтительных МП [28-32] для построения исходных ортогональных систем, можно получить в качестве взаимной помехи отсчеты ПВКФ ПСП Голда, то есть минимизировать уровень таких помех при передаче информации на основе двух систем ортогональных функций. Кроме того, оказывается возможным упростить процедуру обращения матриц при компенсации этих помех.

Вместе с тем, p-ичные ЛРП в настоящее время не применяются на практике для формирования шумоподобных сигналов, в литературе отсутствуют таблицы неприводимых примитивных полиномов, необходимых для их формирования, и не найдены предпочтительные ПСП для формирования p-ичных аналогов ПСП Голда. Но любая ПВКФ МП может быть вычислена с помощью БПА [26]. Кроме того, как показано ниже, ПВКФ p-ичной ЛРП может быть вычислена на основе обобщенного БПФ. Данное обстоятельство целесообразно использовать при построении алгоритма компенсации взаимных помех, образующихся при использовании одновременно нескольких систем ортогональных функций для передачи информации.

Цель работы. Разработка способов построения матриц-циркулянтов p-ичных ЛРП, а также их линейного преобразования к системам ВК и способов компенсации взаимных помех на основе обобщенного БПФ при одновременном использовании систем соответствующих ортогональных сигналов для передачи информации.

Построение матриц-циркулянтов p-ичных ЛРП

Принципы построения матриц-циркулянтов МП, являющихся частным случаем p-ичных ЛРП, рассмотрены в [25], поэтому в данной статье будем рассматривать более общий вариант – матрицы-циркулянты p-ичных ЛРП.

Как известно, любую p-ичную ЛРП с периодом $N = p^m - 1$ и элементами из множества $\{0,1,\ldots,(p-1)\}$ можно сформировать с помощью неприводимого примитивного полинома m-го порядка:

$$f_m(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_1 x + a_0, \tag{1}$$

где значения набора его коэффициентов $a_0, a_1, a_{m-2}, a_{m-1}, a_m$ также принадлежат множеству $\{0,1,\ldots,(p-1)\}$ [27,28] (в дальнейшем такой полином будем называть p-ичным полиномом m-го порядка). Сформированную ПСП представим как вектор-строку

$${}^{n}_{l_i}\mathfrak{I}_i = \left[x_{i,k}, \left(k = 0,\ldots,(N-1); i = 0,\ldots,m-1 \right) \right],$$

где $x_{i,k}$ – элементарный символ ПСП, k-номер ее символа, i – номер ее циклического сдвига на $l_i \in \{0,1,...,N-1\}$ символов относительно ПСП ${}_0^n\mathfrak{I}_0$ с циклическим сдвигом, принятым в качестве нулевого, n – номер способа упорядочения ПСП по их циклическим сдвигам.

С другой стороны, p-ичную ЛРП можно сформировать на основе циклической мультипликативной группы расширенного поля Галуа $GF(p^m)$ по модулю $f_m(x)$, каждый элемент которой представим как вектор-столбец $\boldsymbol{\alpha}^k = \left[x_{i,k},(k=0,...,N-1);(i=0,...,m-1)\right]^{\mathrm{T}}$, где $[\cdot]^{\mathrm{T}}$ – обозначение транспонированной матрицы. В данном случае k – номер элемента мультипликативной группы с первообразным элементом $\boldsymbol{\alpha}^0$, причем $\boldsymbol{\alpha}^k = \boldsymbol{H}_n\boldsymbol{\alpha}^{k-1}(n=1,...,4)$, где

$$\boldsymbol{H}_1 = \begin{bmatrix} 0 & 0 & ... & 0 & a_0 \\ 1 & 0 & ... & 0 & a_1 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & ... & 0 & a_{m-2} \\ 0 & 0 & ... & 1 & a_{m-1} \end{bmatrix}, \boldsymbol{H}_2 = [\boldsymbol{H}_1]^{\mathrm{T}},$$
$$\boldsymbol{H}_3 = \begin{bmatrix} a_{m-1} & 1 & ... & 0 & 0 \\ a_{m-2} & 0 & ... & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_1 & 0 & ... & 0 & 1 \\ a_0 & 0 & ... & 0 & 0 \end{bmatrix}, \boldsymbol{H}_4 = [\boldsymbol{H}_3]^{\mathrm{T}} \quad (2)$$

– варианты сопровождающей матрицы $f_m(x)$ размерностью $m \times m$.

Отметим, что для так называемого двойственного полинома $f_{mД}(x) = a^0x^m + a^1x^{m-1} + ... + a_{m-1}x + a_m$, являющегося неприводимым и примитивным, как и исходный полином,

$$\boldsymbol{H}_1 = \begin{bmatrix} 0 & 0 & ... & 0 & a_m \\ 1 & 0 & ... & 0 & a_{m-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & ... & 0 & a_2 \\ 0 & 0 & ... & 1 & a_1 \end{bmatrix}, \boldsymbol{H}_2 = [\boldsymbol{H}_1]^{\mathrm{T}},$$
$$\boldsymbol{H}_3 = \begin{bmatrix} a_1 & 1 & ... & 0 & 0 \\ a_2 & 0 & ... & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{m-1} & 0 & ... & 0 & 1 \\ a_m & 0 & ... & 0 & 0 \end{bmatrix}, \boldsymbol{H}_4 = [\boldsymbol{H}_3]^{\mathrm{T}}. \quad (3)$$

В результате при нумерации коэффициентов двойственного (зеркального) полинома, совпадающей с нумерацией исходного полинома, и формировании сопровождающих матриц в соответствии с (2), получим матрицы, на основе которых нельзя построить мультипликативные группы поля с максимальным периодом повторения элементов, равным N, так что $\boldsymbol{\alpha}^0 = \boldsymbol{\alpha}^N, \boldsymbol{\alpha}^1 = \boldsymbol{\alpha}^{N+1}$. При этом в качестве $\boldsymbol{\alpha}^0$ можно выбрать любой элемент группы. В качестве примера в табл. 1 приводятся элементы максимальных мультипликативных групп расширенных полей Галуа для троичных полиномов второго порядка $f_2(x) = 2x^2 + x + 1$ и $f_2'(x) = 2x^2 + x + 1$. Использовались матрицы $\boldsymbol{H}_1$ и $\boldsymbol{H}_3$ при первообразном элементе $\boldsymbol{\alpha}^0 = \begin{bmatrix}1 & 0\end{bmatrix}^{\mathrm{T}}$. В дальнейшем десятичное представление любого k-го элемента мультипликативной группы будем обозначать как $\left[\boldsymbol{\alpha}^k\right]_{10}$, так что $\left[\boldsymbol{\alpha}^0\right]_{10} = 3$. Отметим также, что в данном случае $\boldsymbol{H}_2 = [\boldsymbol{H}_1]^{\mathrm{T}} = \boldsymbol{H}_1$ и $\boldsymbol{H}_4 = [\boldsymbol{H}_3]^{\mathrm{T}} = \boldsymbol{H}_3$.

Таблица 1

k	$f_2(x)$		$f_2'(x)$	
	$\boldsymbol{H}_1$	$\boldsymbol{H}_3$	$\boldsymbol{H}_1$	$\boldsymbol{H}_3$
0	3	3	3	3
1	1	4	1	7
2	4	7	5	8
3	5	2	8	2
4	6	6	6	6
5	2	8	2	5
6	8	5	7	4
7	7	1	4	1

Для получения m циклических сдвигов p-ичной ЛРП рассмотрим матрицу, составленную из всех элементов мультипликативной группы, расположенных последовательно: $\begin{bmatrix}\boldsymbol{\alpha}^0 & \boldsymbol{\alpha}^1 & ... & \boldsymbol{\alpha}^{N-1}\end{bmatrix}, \boldsymbol{\alpha}^k = \boldsymbol{H}_n\boldsymbol{\alpha}^{k-1}$. Как известно, строки полученной матрицы являются циклическими сдвигами p-ичной ЛРП [25], то есть

$$\begin{bmatrix}\boldsymbol{\alpha}^0 & \boldsymbol{\alpha}^1 & ... & \boldsymbol{\alpha}^{N-1}\end{bmatrix} = \begin{bmatrix} {}_0^n\mathfrak{I}_0 \\ {}_{l_1}^n\mathfrak{I}_1 \\ ... \\ {}_{l_{m-1}}^n\mathfrak{I}_{m-1} \end{bmatrix} = \mathfrak{I}_{m,n}, \quad (4)$$

где $\mathfrak{I}_{m,n}$ – обозначение матрицы размерности $m \times N$, построенной на основе n-ой сопровождающей матрицы неприводимого примитивного полинома $f_m(x)$. Строки этой матрицы представляют собой циклические сдвиги p-ичной ЛРП на l_i ее символов относительно ${}_0^n\mathfrak{I}_0, i = 0,...,m-1$ – номер строки матрицы. Циклический сдвиг строки с нулевым номером считается равным нулю, то есть $l_0 = 0$. Как видно, нулевой циклический сдвиг, как и структура $\mathfrak{I}_{m,n}$, определяется выбором $\boldsymbol{H}_n$ и $\boldsymbol{\alpha}^0$. Так для матрицы $\boldsymbol{H}_1$ очевидно

$$\alpha^{k+1}=\begin{bmatrix} x_{0,k+1} \\ x_{1,k+1} \\ \dots \\ x_{m-1,k+1} \end{bmatrix}=\begin{bmatrix} 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & \dots & 0 & a_1 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & 0 & a_{m-2} \\ 0 & 0 & \dots & 1 & a_{m-1} \end{bmatrix}\begin{bmatrix} x_{0,k} \\ x_{1,k} \\ \dots \\ x_{m-1} \end{bmatrix}, \tag{5}$$

$k=0,\dots,N-1.$

В результате

$$\mathfrak{I}_{m,1}=\begin{bmatrix} x_{0,0} & x_{0,1} & \dots & x_{0,0} \\ x_{1,0} & x_{1,1} & \dots & x_{1,N-1} \\ \cdot & \cdot & \cdot & \cdot \\ x_{m-1,0} & x_{m-1,1} & \dots & x_{m-1,N-1} \end{bmatrix}. \tag{6}$$

Для полиномов $f_2(x)$, $f_2^{'}(x)$ и их сопровождающих матриц $\boldsymbol{H}_1$ и $\boldsymbol{H}_3$ элементы соответствующих матриц $\mathfrak{I}_{m,1}$ представлены в таблице 2.

Таблица 2

f_2(x)	H_1								f_2(x)	H_3							
Элементы группы	k								Элементы группы	k							
	0	1	2	3	4	5	6	7		0	1	2	3	4	5	6	7
	$[\alpha_k]_{10}$									$[\alpha_k]_{10}$							
	3	1	4	5	6	2	8	7		3	4	7	2	6	8	5	1
$x_{0,k}$	1	0	1	1	2	0	2	2	$x_{0,k}$	1	1	2	0	2	2	1	0
$x_{1,k}$	0	1	1	2	0	2	2	1	$x_{1,k}$	0	1	1	2	0	2	2	1
f'_2(x)	H_1								f'_2(x)	H_3							
Элементы группы	k								Элементы группы	k							
	0	1	2	3	4	5	6	7		0	1	2	3	4	5	6	7
	$[\alpha_k]_{10}$									$[\alpha_k]_{10}$							
	3	1	5	8	6	2	7	4		3	7	8	2	6	5	4	1
$x_{0,k}$	1	0	1	2	2	0	2	1	$x_{0,k}$	1	2	2	0	2	1	1	0
$x_{1,k}$	0	1	2	2	0	2	1	1	$x_{1,k}$	0	1	2	2	0	2	1	1

Таким образом, для любого n существует в общем случае четыре, а в частном случае две (когда $\boldsymbol{H}_2=\boldsymbol{H}_1$ и $\boldsymbol{H}_4=\boldsymbol{H}_3$) матрицы $\mathfrak{I}_{m,n}$ размерности $m\times N$, содержащих m несовпадающих циклических сдвигов p-ичной ЛРП на $l_0,l_1,\dots,l_{m-1}$ символов. Следующие m циклических сдвигов $l_m,l_{m+1},\dots,l_{2m-1}$, не совпадающих с $l_0,l_1,\dots,l_{m-1}$, можно получить при перемножении матриц $\boldsymbol{H}_n^m$ и $\mathfrak{I}_{m,n}$, следующий набор циклических сдвигов – при перемножении $\boldsymbol{H}_n^{2m}$ и $\mathfrak{I}_{m,n}$ и т.д. В результате матрица, предположительно содержащая все циклические сдвиги исходной ПСП, будет содержать число строк, делящееся нацело на m. Но общее число циклических сдвигов ПСП не может быть больше ее длины N, поэтому последний блок, полученный в соответствии с вышеописанным правилом, будет содержать циклические сдвиги, содержащиеся и в первом блоке $\mathfrak{I}_{m,n}$. При этом общее число блоков, полученных по правилу $\boldsymbol{H}_n^x\mathfrak{I}_{m,n}$ и содержащих не совпадающие циклические сдвиги $\boldsymbol{p}$-ичной ЛРП, будет равно $\dfrac{A(n)}{m}$, где $x=0,1,2\dots$, а $A(N)$ – число, делящееся нацело на m и наиболее близкое по значению к N, причем $A(N)>N$.

Матрицу, полученную в соответствии с правилом

$$\mathfrak{I}_{m,n,\text{ц}}=\begin{bmatrix} \mathfrak{I}_{m,n} \\ \boldsymbol{H}_n^m\mathfrak{I}_{m,n} \\ \boldsymbol{H}_n^{2m}\mathfrak{I}_{m,n} \\ \dots \\ \boldsymbol{H}_n^{C(N)m}\mathfrak{I}_{m,n} \end{bmatrix}, \tag{7}$$

будем называть матрицей-циркулянтом p-ичной ЛРП, где $C(N)=\left(\dfrac{A(N)}{m}\right)-1$. Ее размерность составит $A(N)\times N$.

Элементы матриц $\mathfrak{I}_{2,1,\text{ц}}$ и $\mathfrak{I}_{2,3,\text{ц}}$ сформированных на основе полиномов $f_2(x)$ и $f_2^{'}(x)$, приведены в таблице 3.

Таблица 3

$f_2(x)$	H_1										$f_2(x)$	H_3									
Циклические сдвиги МП	k								i	l_i	Циклические сдвиги МП	k								i	l_i
	0	1	2	3	4	5	6	7				0	1	2	3	4	5	6	7		
	$[\alpha_k]_{10}$											$[\alpha_k]_{10}$									
	3	1	4	5	6	2	8	7				3	4	7	2	6	8	5	1		
$x_{0,k}$	1	0	1	1	2	0	2	2	0	0	$x_{0,k}$	1	1	2	0	2	2	1	0	0	0
$x_{1,k}$	0	1	1	2	0	2	2	1	1	1	$x_{1,}$	0	1	1	2	0	2	2	1	1	7
$x_{2,k}$	1	1	2	0	2	2	1	0	2	2	$x_{2,k}$	2	0	2	2	1	0	1	1	2	2
$x_{3,}$	1	2	0	2	2	1	0	1	3	3	$x_{3,k}$	1	2	0	2	2	1	0	1	3	1
$x_{4,}$	2	0	2	2	1	0	1	1	4	4	$x_{4,k}$	2	2	1	0	1	1	2	0	4	4
$x_{5,}$	0	2	2	1	0	1	1	2	5	5	$x_{5,k}$	0	2	2	1	0	1	1	2	5	3
$x_{6,}$	2	2	1	0	1	1	2	0	6	6	$x_{6,k}$	1	0	1	1	2	0	2	2	6	6
$x_{7,}$	2	1	0	1	1	2	0	2	7	7	$x_{7,k}$	2	1	0	1	1	2	0	2	7	5
$f'_2(x)$	H_1										$f'_2(x)$	H_3									
Циклические сдвиги МП	k								i	l_i	Циклические сдвиги МП	k								i	l_i
	0	1	2	3	4	5	6	7				0	1	2	3	4	5	6	7		
	$[\alpha_k]_{10}$											$[\alpha_k]_{10}$									
	3	1	5	8	6	2	7	4				3	7	8	2	6	5	4	1		
$x_{0,}$	1	0	1	2	2	0	2	1	0	0	$x_{0,k}$	1	2	2	0	2	1	1	0	0	0
$x_{1,k}$	0	1	2	2	0	2	1	1	1	1	$x_{1,}$	0	1	2	2	0	2	1	1	1	7
$x_{2,}$	1	2	2	0	2	1	1	0	2	2	$x_{2,k}$	2	0	2	1	1	0	1	2	2	2
$x_{3,k}$	2	2	0	2	1	1	0	1	3	3	$x_{3,k}$	2	2	0	2	1	1	0	1	3	1
$x_{4,k}$	2	0	2	1	1	0	1	2	4	4	$x_{4,k}$	2	1	1	0	1	2	2	0	4	4
$x_{5,}$	0	2	1	1	0	1	2	2	5	5	$x_{5,k}$	0	2	1	1	0	1	2	2	5	3
$x_{6,k}$	2	1	1	0	1	2	2	0	6	6	$x_{6,k}$	1	0	1	2	2	0	2	1	6	6
$x_{7,}$	1	1	0	1	2	2	0	2	7	7	$x_{7,k}$	1	1	0	1	2	2	0	2	7	5

Из анализа этих таблиц следует, что использование сопровождающих матриц $\boldsymbol{H}_1$, $\boldsymbol{H}_2$ для построения матриц-циркулянтов привело к формированию так называемых упорядоченных матриц, у которых каждая последующая строка сдвинута циклически на один символ влево, по сравнению с предыдущей строкой [24]. Далее будем обозначать их как $\mathfrak{I}_{m,n,\text{цу}}$. В то же время при формировании матриц-циркулянтов на основе $\boldsymbol{H}_3$, $\boldsymbol{H}_4$ получаются псевдослучайные циклические сдвиги их строк. Но результаты исследований структур матриц-циркулянтов для МП, полученные в [24], позволяют предположить, что данный результат соответствует лишь рассматриваемым в этой статье вариантам неприводимых полиномов, для которых $\boldsymbol{H}_2 = \boldsymbol{H}_1$ и $\boldsymbol{H}_4 = \boldsymbol{H}_3$. В общем случае, когда $\boldsymbol{H}_2 \neq \boldsymbol{H}_1$ и $\boldsymbol{H}_4 \neq \boldsymbol{H}_3$, упорядоченные матрицы могут формироваться на основе $\boldsymbol{H}_2$ и $\boldsymbol{H}_4$, а матрицы с псевдослучайными сдвигами строк – на основе $\boldsymbol{H}_1$ и $\boldsymbol{H}_3$.

Начальный блок p-ичной ЛРП $\boldsymbol{b}_i$, находящейся в i-ой строке упорядоченной матрицы-циркулянта может быть вычислен по формуле:

$$\boldsymbol{b}_i = \boldsymbol{H}_2^i \boldsymbol{\alpha}^0, \tag{8}$$

где $\boldsymbol{b}_i = \left[x_{i,k}, k = 0, \ldots, m-1 \right]$. В дальнейшем $\boldsymbol{b}_i$ будем называть абсолютным циклическим сдвигом p-ичной ЛРП.

Отметим также, что выбор элемента любой мультипликативной группы $\boldsymbol{\alpha}^{0+y} (y = 1, 2, \ldots, N-1)$ в качестве первообразного приводит к ее циклическому сдвигу на y элементов, в результате чего все строки матриц-циркулянтов также сдвигаются циклически на y элементов. Таким образом, на основе каждого первообразного элемента $\boldsymbol{\alpha}^{0+y} (y = 0, 2, \ldots, N-1)$ и любой из матриц $\boldsymbol{H}_n$ можно сформировать матрицу-циркулянт p-ичной ЛРП. То есть существует $4N$ или $2N$ несовпадающих матриц-циркулянтов одной и той же ПСП рассматриваемого типа.

Формирование систем ортогональных многопозиционных сигнатур на основе *p*-ичных ЛРП и их свойства

На основе матриц-циркулянтов p-ичных ЛРП можно построить системы почти ортогональных сигнатур, которые будем представлять как строки матриц вида:

$$\boldsymbol{S}_N(i,k) = \left[W^{x_{i,k}} \right], \tag{9}$$

где $i = 1, \ldots, N$ – номер строки матрицы, $k = 1, \ldots, N$ – номер столбца, $N = p^m - 1, W = e^{j\frac{2\pi}{p}}$. В дальнейшем символы i и k в обозначении матрицы (9) опустим.

Для разъяснения сути предлагаемого подхода к построению совокупностей почти ортогональных и ортогональных сигнатур, способу передачи и выделения информационных символов на их основе, будем рассматривать упорядоченные матрицы-циркулянты p-ичных ЛРП. С этой целью можно использовать и неупорядоченные матрицы, но в этом случае усложняется изложение разрабатываемого метода без изменения его сути из-за необходимости описания дополнительных вариантов перестановок строк и столбцов матриц.

В качестве примера рассмотрим построение почти ортогональных сигнатур на основе упорядоченных матриц-циркулянтов, приведенных в таблицах 3 и 5. В результате получим матрицы:

$$\boldsymbol{S}_8^a = \begin{bmatrix} W^1 & W^0 & W^1 & W^1 & W^2 & W^0 & W^2 & W^2 \\ W^0 & W^1 & W^1 & W^2 & W^0 & W^2 & W^2 & W^1 \\ W^1 & W^1 & W^2 & W^0 & W^2 & W^2 & W^1 & W^0 \\ W^1 & W^2 & W^0 & W^2 & W^2 & W^1 & W^0 & W^1 \\ W^2 & W^0 & W^2 & W & W^1 & W^0 & W^1 & W^1 \\ W^0 & W^2 & W^2 & W^1 & W^0 & W^1 & W^1 & W^2 \\ W^2 & W^2 & W^1 & W^0 & W^1 & W & W^2 & W^0 \\ W^2 & W^1 & W^0 & W^1 & W^1 & W^2 & W^0 & W^2 \end{bmatrix},$$

$$\boldsymbol{S}_8^b = \begin{bmatrix} W^1 & W^0 & W^1 & W^2 & W^2 & W^0 & W^2 & W^1 \\ W^0 & W^1 & W^2 & W^2 & W^0 & W^2 & W^1 & W^1 \\ W^1 & W^2 & W^2 & W^0 & W^2 & W^1 & W^1 & W^0 \\ W^2 & W^2 & W^0 & W^2 & W^1 & W^1 & W^0 & W^1 \\ W^2 & W^0 & W^2 & W^1 & W^1 & W^0 & W^1 & W^2 \\ W^0 & W^2 & W^1 & W^1 & W^0 & W^1 & W^2 & W^2 \\ W^2 & W^1 & W^1 & W & W^1 & W^2 & W^2 & W^0 \\ W^1 & W^1 & W^0 & W^1 & W^2 & W^2 & W^0 & W^2 \end{bmatrix}, \tag{9}$$

где $\boldsymbol{S}_8^a, \boldsymbol{S}_8^b$ – две разные упорядоченные системы почти ортогональных сигнатур, для различения которых использованы буквенные символы a и b; $W = e^{j\frac{2\pi}{3}}$. В дальнейшем для упрощения рассуждений будем рассматривать упорядоченные системы, хотя выбор способа их построения не имеет принципиального значения.

На основе каждого неприводимого примитивного полинома и его сопровождающей матрицы $\boldsymbol{H}_2$ можно построить N упорядоченных систем почти ортогональных сигнатур при использовании для их построения разных первообразных элементов мультипликативной группы, соответствующих этой матрице. Если для построения последующей матрицы почти ортогональных сигнатур используется следующий элемент мультипликативной группы, то ее строки будут сдвинуты циклически относительно предыдущей матрицы на одну строку, то есть последняя строка станет первой, первая второй и т.д.

Учитывая, что каждая строка любой упорядоченной матрицы $\boldsymbol{S}_N$ является циклическим сдвигом выбранной p-ичной ЛРП на один символ влево, матрицу, строки которой представляют собой значения периодических автокорреляционных функций (ПАКФ) сигнатур, назовем циркулярной автокорреляционной матрицей (ЦАКМ). Ее можно рассчитать по формуле:

$$\chi_{\text{ЦАКМ}} = \frac{1}{N} \boldsymbol{S}_N \boldsymbol{S}_N^{*\mathrm{T}} = \frac{1}{N} \boldsymbol{S}_N \boldsymbol{S}_N^{*}, \tag{10}$$

где $\boldsymbol{S}_N^{*\mathrm{T}}$ – транспонированная матрица $\boldsymbol{S}_N$ с комплексно-сопряженными элементами, $\cdot^*$ – обозначение комплексно-сопряженной матрицы или ее комплексно-сопряженного элемента. Равенство в (10) справедливо, поскольку для упорядоченных матриц $\boldsymbol{S}_N = \boldsymbol{S}_N^{\mathrm{T}}$. В частности, для любой из систем почти ортогональных сигнатур (9) получим одинаковые матрицы:

$$Re\left[\chi_{\text{ЦАКМ}}\right]=\begin{bmatrix} 1 & -1/8 & -1/8 & -1/8 & -1/8 & -1/8 & -1/8 & 1/8 \\ -1/8 & 1 & -1/8 & -1/8 & -1/8 & -1/8 & -1/8 & 1/8 \\ -1/8 & -1/8 & 1 & -1/8 & -1/8 & -1/8 & -1/8 & 1/8 \\ -1/8 & -1/8 & 1/8 & 1 & -1/8 & -1/8 & -1/8 & 1/8 \\ -1/8 & -1/8 & -1/8 & 1/8 & 1 & -1/8 & -1/8 & -1/8 \\ -1/8 & -1/8 & -1/8 & 1/8 & -1/8 & 1 & -1/8 & -1/8 \\ -1/8 & -1/8 & -1/8 & 1/8 & -1/8 & -1/8 & 1 & -1/8 \\ -1/8 & -1/8 & -1/8 & 1/8 & -1/8 & -1/8 & 1/8 & 1 \end{bmatrix}, \qquad (11)$$

$$Im\left[\chi_{\text{ЦАКМ}}\right]=\mathbf{0},$$

где $\mathbf{0}$ – матрица, состоящая из нулей.

ПАКФ исходной p-ичной ЛРП в ее традиционном представлении можно получить путем преобразования любой строки ее ЦАКМ. В качестве примера на рисунке 1 приводится действительная часть ПАКФ $Re[\boldsymbol{\chi}_{\text{ПАКФ}}(k)]$, полученная из строки ЦАКМ с номером ноль. Значения ПАКФ при отрицательных значениях k соответствуют циклическим сдвигам второй сигнатуры влево относительно первой. В данном случае их можно получить при зеркальном отражении значений $Re\left[\chi_{\text{ПАКФ}}(k)\right]$ относительно оси ординат координатной плоскости $\left(Re\left[\chi_{\text{ПАКФ}}(k)\right],k\right)$. Таким образом, для двух рассматриваемых ПСП получили вид $Re\left[\chi_{\text{ПАКФ}}(k)\right]$ (см. рис. 1), характерный для всех p-ичных ЛРП, что является подтверждением их принадлежности к этому классу последовательностей. При этом $Im\left[\chi_{\text{ПАКФ}}(k)\right]=\mathbf{0}$ при всех значениях k.

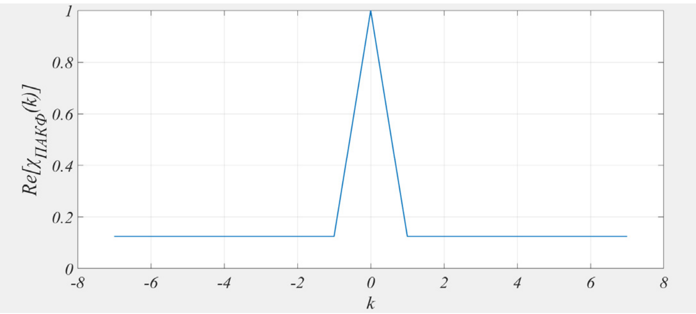

Рис. 1. Вид действительной части ПАКФ любой p-ичной ЛРП при $N = 8$

Циркулярная взаимно корреляционная матрица (ЦВКМ) любых двух упорядоченных систем почти ортогональных сигнатур a и b описывается формулой:

$$\chi_{\text{ЦВКМ},ab}=\frac{1}{N}\boldsymbol{S}_N^a\boldsymbol{S}_N^{b^{*\mathrm{T}}}=\frac{1}{N}\boldsymbol{S}_N^a\boldsymbol{S}_N^{b^*}. \qquad (12)$$

Также будем рассматривать

$$\chi_{\text{ЦВКМ},ba}=\frac{1}{N}\boldsymbol{S}_N^{b^*}\boldsymbol{S}_N^a. \qquad (13)$$

В частности, для систем (9) получим:

$$Re\left[\boldsymbol{\chi}_{\text{ЦВКМ}},ab\right]=\begin{bmatrix} 2/8 & 2/8 & -1/8 & -1/8 & 5/8 & -4/8 & -1/8 & -4/8 \\ -4/8 & 2/8 & 2/8 & -1/8 & -1/8 & 5/8 & -4/8 & -1/8 \\ -1/8 & -4/8 & 2/8 & 2/8 & -1/8 & -1/8 & 5/8 & -4/8 \\ -4/8 & -1/8 & -4/8 & 2/8 & 2/8 & -1/8 & -1/8 & 5/8 \\ 5/8 & -4/8 & -1/8 & -4/8 & 2/8 & 2/8 & -1/8 & -1/8 \\ -1/8 & 5/8 & -4/8 & -1/8 & -4/8 & 2/8 & 2/8 & -1/8 \\ -1/8 & -1/8 & 5/8 & -4/8 & -1/8 & -4/8 & 2/8 & 2/8 \\ 2/8 & -1/8 & -1/8 & 5/8 & -4/8 & -1/8 & -4/8 & 2/8 \end{bmatrix}, \qquad (14)$$

$$Im\left[\boldsymbol{\chi}_{\text{ЦВКМ}},ab\right]=\mathbf{0}.$$

$$Re\left[\boldsymbol{\chi}_{\text{ЦВКМ}},ba\right]=\begin{bmatrix} -1/8 & 2/8 & 2/8 & -1/8 & 2/8 & -1/8 & -1/8 & -1/8 \\ -1/8 & -1/8 & 2/8 & 2/8 & -1/8 & 2/8 & -1/8 & -1/8 \\ -1/8 & -1/8 & -1/8 & 2/8 & 2/8 & -1/8 & 2/8 & -1/8 \\ -1/8 & -1/8 & -1/8 & -1/8 & 2/8 & 2/8 & -1/8 & 2/8 \\ 2/8 & -1/8 & -1/8 & -1/8 & -1/8 & 2/8 & 2/8 & -1/8 \\ -1/8 & 2/8 & -1/8 & -1/8 & -1/8 & -1/8 & 2/8 & 2/8 \\ 2/8 & -1/8 & 2/8 & -1/8 & -1/8 & -1/8 & 1/8 & 2/8 \\ 2/8 & 2/8 & -1/8 & 2/8 & -1/8 & -1/8 & 1/8 & -1/8 \end{bmatrix}, \qquad (15)$$

$$Im\left[\boldsymbol{\chi}_{\text{ЦВКМ}},ba\right]=\mathbf{0}.$$

Как видно, обе ЦВКМ, так же, как и ЦАКМ, имеют циклическую структуру, в результате чего ПВКФ двух рассматриваемых p-ичных ЛРП можно получить путем преобразования любых их строк. В частности, при $k = 0,1,\ldots,N-1$ значения действительных частей ПВКФ $Re\left[\boldsymbol{\chi}_{\text{ПВКФ},ab}\right]$ и $Re\left[\boldsymbol{\chi}_{\text{ПВКФ},ba}\right]$ равняются элементам верхних строк их матриц-циркулянтов $Re\left[\boldsymbol{\chi}_{\text{ЦВКМ},ab}\right]$ (14) и $Re\left[\boldsymbol{\chi}_{\text{ЦВКМ},ba}\right]$ (15). При отрицательных значениях k, соответствующих циклическим сдвигам второй сигнатуры относительно первой вправо, значения ПВКФ соответствуют нижним строкам (14) и (15) без последнего символа. В качестве примера на рисунке 2 а,б приводится ПВКФ $Re\left[\boldsymbol{\chi}_{\text{ПВКФ},ab}\right]$ и $Re\left[\boldsymbol{\chi}_{\text{ПВКФ},ba}\right]$ рассматриваемых ПСП, образующих системы a и b.

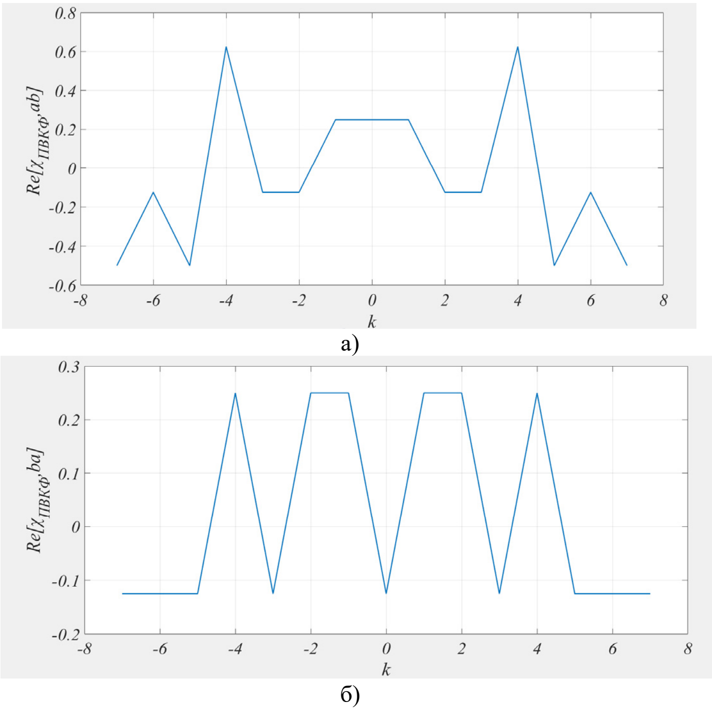

Рис. 2. Виды действительных частей ПВКФ $Re\left[\boldsymbol{\chi}_{\text{ПВКФ},ab}\right]$ (а) и $Re\left[\boldsymbol{\chi}_{\text{ПВКФ},ba}\right]$ (б) p-ичных ЛРП, образующих почти ортогональные системы a и b (9)

Заметим, что при добавлении к матрицам (9) строки сверху и столбца слева, элементы которых равны $W^0=1$, получим квадратные матрицы размерности 9, состоящие из ортогональных сигнатур:

$$\boldsymbol{s}_9{}^{a}=\begin{bmatrix}W^0 & W^0 & W^0 & W^0 & W^0 & W^0 & W^0 & W^0 & W^0\\ W^0 & W^1 & W^0 & W^1 & W & W^2 & W^0 & W^2 & W^2\\ W^0 & W^0 & W^1 & W^1 & W^2 & W^0 & W^2 & W^2 & W^1\\ W^0 & W^1 & W^1 & W^2 & W^0 & W^2 & W & W^1 & W^0\\ W^0 & W^1 & W^2 & W^0 & W^2 & W^2 & W^1 & W^0 & W^1\\ W^0 & W^2 & W & W^2 & W^2 & W^1 & W^0 & W^1 & W\\ W^0 & W^0 & W^2 & W^2 & W^1 & W^0 & W^1 & W^1 & W^2\\ W^0 & W^2 & W^2 & W^1 & W^0 & W^1 & W & W^2 & W^0\\ W^0 & W^2 & W^1 & W^0 & W^1 & W^1 & W^2 & W^0 & W^2\end{bmatrix},$$

$$\boldsymbol{s}_9{}^{b}=\begin{bmatrix}W^0 & W^0 & W & W^0 & W^0 & W^0 & W^0 & W^0 & W^0\\ W^0 & W^1 & W^0 & W^1 & W^2 & W^2 & W^0 & W^2 & W^1\\ W^0 & W^0 & W & W^2 & W^2 & W & W^2 & W^1 & W^1\\ W^0 & W^1 & W^2 & W^2 & W^0 & W^2 & W^1 & W^1 & W^0\\ W^0 & W^2 & W^2 & W^0 & W^2 & W^1 & W^1 & W & W^1\\ W^0 & W^2 & W^0 & W^2 & W^1 & W^1 & W^0 & W^1 & W^2\\ W^0 & W^0 & W^2 & W^1 & W^1 & W & W^1 & W^2 & W^2\\ W^0 & W^2 & W^1 & W^1 & W^0 & W^1 & W^2 & W^2 & W^0\\ W^0 & W^1 & W^1 & W & W^1 & W^2 & W^2 & W^0 & W^2\end{bmatrix}. \qquad (16)$$

Размерность систем ортогональных сигнатур составляет $p^m = N+1$, а $i,k = 0,\ldots,N$. Соответственно ЦАКМ каждой из них и ЦВКМ любых двух разных по структуре систем одной и той же размерности можно определить как:

$$\chi_{\text{ЦАКМ,о}}=\frac{1}{p^m}\boldsymbol{S}_{p^m}\left(\boldsymbol{S}_{p^m}{}^{*}\right)^{\mathrm{T}}=\frac{1}{p^m}\boldsymbol{S}_{p^m}\boldsymbol{S}_{p^m}{}^{*}=\frac{1}{p^m}\boldsymbol{S}_{p^m}{}^{*}\boldsymbol{S}_{p^m},$$

$$\chi_{\text{ЦВКМ,о},ab}=\frac{1}{p^m}\boldsymbol{S}_{p^m}{}^{a}\left(\boldsymbol{S}_{p^m}{}^{b^*}\right)^{\mathrm{T}}=\frac{1}{p^m}\boldsymbol{S}_{p^m}{}^{a}\boldsymbol{S}_{p^m}{}^{b^*},$$

$$\chi_{\text{ЦВКМ,о},ba}=\frac{1}{p^m}\boldsymbol{S}_{p^m}{}^{b}\left(\boldsymbol{S}_{p^m}{}^{a^*}\right)^{\mathrm{T}}=\frac{1}{p^m}\boldsymbol{S}_{p^m}{}^{b}\boldsymbol{S}_{p^m}{}^{a^*}, \qquad (17)$$

где $\boldsymbol{S}_{p^m}$ матрица размерности $p^m = N + 1$, описывающая систему ортогональных сигнатур. Для каждой из таких систем очевидно выполняется равенство: $\frac{1}{p^m}\boldsymbol{S}_{p^m}\boldsymbol{S}_{p^m}{}^{*\mathrm{T}}=\boldsymbol{I}$, где $\boldsymbol{I}$ – единичная матрица. Общее количество разных ортогональных сигнатур одной и той же размерности, построенных в соответствии с вышеописанным правилом, определяется числом разных p-ичных ЛРП максимального периода одной и той же длины, а также числом отличающихся по структуре сопровождающих матриц каждого полинома, на основе которого формируется ЛРП.

Рассмотрим очевидные, но весьма важные свойства ортогональных сигнатур, построенных на основе матриц-циркулянтов p-ичных ЛРП. Подчеркнем, что они будут формулироваться для упорядоченных систем, у которых каждая последующая строка матрицы-циркулянта циклически сдвинута на один символ вправо, по сравнению с предыдущей строкой. Кроме того, строки с столбцы с одинаковыми номерами совпадают, в результате чего для любой системы $\boldsymbol{S}_{p^m}{}^{a}=\left(\boldsymbol{S}_{p^m}{}^{a}\right)^{\mathrm{T}}$.

Свойство 1.

Матрица $\boldsymbol{S}_{p^m}$, описывающая любую упорядоченную систему ортогональных сигнатур, обращается, причем $\boldsymbol{S}_{p^m}{}^{-1}=\boldsymbol{S}_{p^m}{}^{*}$ и $\left(\boldsymbol{S}_{p^m}{}^{*}\right)^{-1}=\boldsymbol{S}_{p^m}$, поскольку $\frac{1}{p^m}\boldsymbol{S}_{p^m}{}^{*}\boldsymbol{S}_{p^m}=\frac{1}{p^m}\boldsymbol{S}_{p^m}\boldsymbol{S}_{p^m}{}^{*}=\boldsymbol{I}$.

Свойство 2.

Мнимые части матриц, описывающих корреляционные свойства систем ортогональных сигнатур состоят из нулей, то есть $Im\left[\chi_{\text{ЦАКМ,о}}\right]=\mathbf{0}$ и $Im\left[\chi_{\text{ЦВКМ,о},ab}\right]=Im\left[\chi_{\text{ЦВКМ,о},ba}\right]=\mathbf{0}$ для любой пары ортогональных систем (a и b) одной и той же размерности, поскольку $Im\left[\chi_{\text{ЦАКМ,о}}\right]=Re\left[\boldsymbol{S}_{p^m}{}^{a}\right]Im\left[\boldsymbol{S}_{p^m}{}^{a}\right]-Im\left[\boldsymbol{S}_{p^m}{}^{a}\right]Re\left[\boldsymbol{S}_{p^m}{}^{a}\right]$.

Свойство 3.

$Re\left[\boldsymbol{S}_{p^m}{}^{a}\right]Im\left[\boldsymbol{S}_{p^m}{}^{a}\right]=\mathbf{0}, Re\left[\boldsymbol{S}_{p^m}{}^{a}\right]Im\left[\boldsymbol{S}_{p^m}{}^{b}\right]\neq\mathbf{0}$.

Равенство нулю произведения действительной и мнимой частей матрицы, описывающей любую ортогональную систему, можно доказать при анализе ее структуры.

Действительно, при перемножении этих двух матриц необходимо сначала каждый элемент строки первой матрицы перемножить с соответствующим элементом столбца второй матрицы. В данном случае каждый элемент строки результирующей матрицы состоит из произведения $\cos\left(s_{ik}\right)\sin\left(s_{ik}\right)=\frac{1}{2}\sin\left(2s_{ik}\right)$, поскольку $s_{ik}=s_{ik}$ у упорядоченной матрицы, где s_{ik} – показатель экспоненты исходной матрицы-циркулянта, находящейся в i-ой строке и k-ом столбце. Далее, необходимо учесть, что при поэлементном перемножении любых строки и столбца исходной матрицы-циркулянта получается другая или та же самая строка или столбец исходной матрицы. Поэтому при суммировании элементов $\sin\left(2s_{ik}\right)$ по i или по k всегда получаем сумму синусов удвоенных значений показателей экспоненты соответствующей строки или столбца матрицы-циркулянта, которая всегда равна нулю.

Свойство 4.

Матрица, состоящая из действительной части матрицы-циркулянта любой ортогональной системы, образует условно ортогональную систему, поскольку $Re\left[\boldsymbol{S}_{p^m}{}^{a}\right]Re\left[\boldsymbol{S}_{p^m}{}^{a}\right]=I_{y1}$, где I_{y1} – условно единичная матрица. Очевидно, что I_{y1} – это диагональная матрица, у которой элемент главной диагонали с номером ноль равен p^m, а остальные элементы диагонали равны p. Таким образом $\left[Re\left[\boldsymbol{S}_{p^m}{}^{a}\right]\right]^{-1}=\left[I_{y1}\right]^{-1}Re\left[\boldsymbol{S}_{p^m}{}^{a}\right]$.

Свойство 5.

Матрица, состоящая из мнимой части матрицы-циркулянта любой ортогональной системы, образует условно ортогональную систему, поскольку $Im\left[\boldsymbol{S}_{p^m}{}^{a}\right]Im\left[\boldsymbol{S}_{p^m}{}^{a}\right]=I_{y2}$, где I_{y2} – условно единичная матрица, у которой элемент главной диагонали с номером ноль равен нулю, остальные элементы главной диагонали равны p^{m-1}.

Таким образом матрица $Im\left[\boldsymbol{S}_{p^m}{}^{a}\right]$ условно обращается, и $\left[Im\left[\boldsymbol{S}_{p^m}{}^{a}\right]\right]^{-1} = \left[I_{y2}\right]^{-1} Im\left[\boldsymbol{S}_{p^m}{}^{a}\right]$.

Свойство 6.

Любая матрица $\boldsymbol{\chi}_{\text{ЦВКМ,о},ab}$, равная $\frac{1}{p^m}\boldsymbol{S}_{p^m}{}^{a}\boldsymbol{S}_{p^m}{}^{b^*}$, обращается, причем $\left(\boldsymbol{\chi}_{\text{ЦВКМ,о},ab}\right)^{-1} = \frac{1}{p^m}\boldsymbol{S}_{p^m}{}^{b}\boldsymbol{S}_{p^m}{}^{a^*} = \boldsymbol{\chi}_{\text{ЦВКМ,о},ba}$ и $\left(\boldsymbol{\chi}_{\text{ЦВКМ,о},ba}\right)^{-1} = \boldsymbol{\chi}_{\text{ЦВКМ,о},ab}$, поскольку справедливо равенство: $\frac{1}{\left(p^m\right)^2}\boldsymbol{S}_{p^m}{}^{1}\boldsymbol{S}_{p^m}{}^{2^*}\boldsymbol{S}_{p^m}{}^{2}\boldsymbol{S}_{p^m}{}^{1^*} = \boldsymbol{I}$.

Учитывая, что *Свойство 6* выявлено здесь впервые, проиллюстрируем его с помощью сигнатур $\boldsymbol{S}_{\mathbf{9}}^{a}$ и $\boldsymbol{S}_{\mathbf{9}}^{b}$ (см. 14). Для них получим:

$$Re\left[\boldsymbol{\chi}_{\text{ЦВКМ,о},ab}\right] = \begin{bmatrix} 1 & \mathbf{0} & 0 & & & & & & \\ 0 & 1 & 0 & 3/9 & 6/9 & -3/9 & 0 & -3/9 & 3/9 \\ 0 & 3/9 & 1 & 0 & 3/9 & 6/9 & -3/9 & 0 & -3/9 \\ 0 & -3/9 & 3/9 & 1 & 0 & 3/9 & 6/9 & -3/9 & 0 \\ 0 & 0 & -3/9 & 3/9 & 1 & 0 & 3/9 & 6/9 & -3/9 \\ 0 & -3/9 & 0 & -3/9 & 3/9 & 1 & 0 & 3/9 & 6/9 \\ 0 & 6/9 & -3/9 & 0 & -3/9 & 3/9 & 1 & 0 & 3/9 \\ 0 & 3/9 & 6/9 & -3/9 & 0 & -3/9 & 3/9 & 1 & 0 \\ 0 & 0 & 3/9 & 6/9 & -3/9 & 0 & -3/9 & 3/9 & 1 \end{bmatrix},$$

$$Im\left[\boldsymbol{\chi}_{\text{ЦВКМ,о},ab}\right] = \mathbf{0}, \tag{17}$$

$$Re\left[\boldsymbol{\chi}_{\text{ЦВКМ,о},ba}\right] = \begin{bmatrix} 1 & \mathbf{0} & 0 & 0 & & & & & \\ 0 & 1 & 0 & -3/9 & 6/9 & 3/9 & 0 & 3/9 & 3/9 \\ 0 & 3/9 & 1 & 0 & -3/9 & 6/9 & 3/9 & 0 & 3/9 \\ 0 & 3/9 & 3/9 & 1 & 0 & -3/9 & 6/9 & 3/9 & 0 \\ 0 & 0 & 3/9 & 3/9 & 1 & 0 & -3/9 & 6/9 & 3/9 \\ 0 & 3/9 & 0 & 3/9 & 3/9 & 1 & 0 & -3/9 & 6/9 \\ 0 & 6/9 & 3/9 & 0 & 3/9 & 3/9 & 1 & 0 & -3/9 \\ 0 & -3/9 & 6/9 & 3/9 & 0 & 3/9 & 3/9 & 1 & 0 \\ 0 & 0 & -3/9 & 6/9 & 3/9 & 0 & 3/9 & 3/9 & 1 \end{bmatrix},$$

$$Im\left[\boldsymbol{\chi}_{\text{ЦВКМ,о},ba}\right] = \mathbf{0}, \tag{18}$$

Легко проверить, что

$$\boldsymbol{\chi}_{\text{ЦВКМ,о},ab}\boldsymbol{\chi}_{\text{ЦВКМ,о},ba} = \boldsymbol{\chi}_{\text{ЦВКМ,о},ba}\boldsymbol{\chi}_{\text{ЦВКМ,о},ab} = .$$

$$= Re\left[\boldsymbol{\chi}_{\text{ЦВКМ,о},ab}\right] Re\left[\boldsymbol{\chi}_{\text{ЦВКМ,о},ba}\right] = \boldsymbol{I}.$$

Свойство 7.

Пусть каждая строка матрицы $\boldsymbol{S}_{p^m}{}^{\boldsymbol{b}}$ умножена на одну и ту же последовательность комплексных ненулевых символов $J_k e^{j\varphi_{kJ}}\ (k = 0,\ldots,N)$, нарушающих ортогональность ее строк, то есть сформирована матрица

$$\boldsymbol{S}_{p^m,J}{}^{\boldsymbol{b}} = \boldsymbol{S}_{p^m}{}^{\boldsymbol{b}}\boldsymbol{J}, \boldsymbol{J} = \begin{bmatrix} J_0 e^{j\varphi_{0J}} & 0 & 0 & \ldots & 0 \\ 0 & J_1 e^{j\varphi_{1J}} & \ldots & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & J_N e^{j\varphi_{NJ}} \end{bmatrix}.$$

Данную процедуру в дальнейшем будем называть скремблированием ортогональной системы $\boldsymbol{S}_{p^m}{}^{b}$.

Тогда ЦАКМ скремблированной системы $\boldsymbol{\chi}_{\text{ЦАКМ,о},b\boldsymbol{J}} = \frac{1}{p^m}\boldsymbol{S}_{p^m}{}^{b}\boldsymbol{J}\boldsymbol{J}*\boldsymbol{S}_{p^m}{}^{b*} = \frac{1}{p^m}\boldsymbol{S}_{p^m}{}^{b}\boldsymbol{J}^2\boldsymbol{S}_{p^m}{}^{b*}$, поскольку $\left(\boldsymbol{S}_{p^m,J}{}^{b*}\right)^{\text{T}} = \boldsymbol{J}*\boldsymbol{S}_{p^m}{}^{b*}$. Соответственно для ЦВКМ $\boldsymbol{S}_{p^m}{}^{a}$ и $\boldsymbol{S}_{p^m,J}{}^{\boldsymbol{b}}$ можно записать:

$$\boldsymbol{\chi}_{\text{ЦВКМ,о},a,b\boldsymbol{J}} = \frac{1}{p^m}\boldsymbol{S}_{p^m}{}^{a}\left(\boldsymbol{S}_{p^m,J}{}^{b*}\right)^{\text{T}} =$$

$$= \frac{1}{p^m}\boldsymbol{S}_{p^m}{}^{a}\boldsymbol{J}*\boldsymbol{S}_{p^m}{}^{b*} = \frac{1}{p^m}\boldsymbol{S}_{p^m,J*}{}^{\boldsymbol{a}}\boldsymbol{S}_{p^m}{}^{b*},$$

где $\boldsymbol{S}_{p^m,J*}{}^{\boldsymbol{a}} = \boldsymbol{S}_{p^m}{}^{a}\boldsymbol{J}$. Кроме того,

$$\boldsymbol{\chi}_{\text{ЦВКМ,о},b\boldsymbol{J},a} = \frac{1}{p^m}\boldsymbol{S}_{p^m,J}{}^{b}\boldsymbol{S}_{p^m}{}^{a*} = \frac{1}{p^m}\boldsymbol{S}_{p^m}{}^{b}\boldsymbol{J}*\boldsymbol{S}_{p^m}{}^{a*}.$$

Свойство 8.

$$\boldsymbol{\chi}_{\text{ЦВКМ,о},a,b\boldsymbol{J}}\boldsymbol{\chi}_{\text{ЦВКМ,о},b\boldsymbol{J},a} = \frac{1}{p^{2m}}\boldsymbol{S}_{p^m}{}^{a}\boldsymbol{J}*\boldsymbol{S}_{p^m}{}^{b*}\boldsymbol{S}_{p^m}{}^{b}\boldsymbol{J}*\boldsymbol{S}_{p^m}{}^{a*} =$$

$$= \frac{1}{p^m}\boldsymbol{S}_{p^m}{}^{a}\boldsymbol{J}^2\boldsymbol{S}_{p^m}{}^{a*} = \boldsymbol{\chi}_{\text{ЦАКМ,о},a\boldsymbol{J}} \neq \boldsymbol{I}.$$

$$\boldsymbol{\chi}_{\text{ЦВКМ,о},b\boldsymbol{J},a}\boldsymbol{\chi}_{\text{ЦВКМ,о},a,b\boldsymbol{J}} = \frac{1}{p^{2m}}\boldsymbol{S}_{p^m}{}^{b}\boldsymbol{J}*\boldsymbol{S}_{p^m}{}^{a*}\boldsymbol{S}_{p^m}{}^{a}\boldsymbol{J}*\boldsymbol{S}_{p^m}{}^{b*} =$$

$$= \frac{1}{p^m}\boldsymbol{S}_{p^m}{}^{b}\boldsymbol{J}^2\boldsymbol{S}_{p^m}{}^{b*} = \boldsymbol{\chi}_{\text{ЦАКМ,о},b\boldsymbol{J}} \neq \boldsymbol{I}.$$

Наиболее известный альтернативный вариант ортогональных сигнатур соответствует системе ВК при трех вариантах упорядочения дискретных функций в их структуре – это системы ВК-Кронекера (ВК-К), ВК-Пэли (ВК-П) и ВК-Уолша (ВК-У) [12]. В частности, система ВК-К при $N+1=3^2=9$ выглядит следующим образом:

$$\boldsymbol{S}_{\mathbf{9},\text{ВК–К}} = \begin{bmatrix} W^0 & W^0 & W^0 & W^0 & W^0 & W & W^0 & W^0 & W^0 \\ W^0 & W^1 & W^2 & W^0 & W^1 & W^2 & W^0 & W & W^2 \\ W^0 & W^2 & W^1 & W^0 & W^2 & W^1 & W^0 & W^2 & W^1 \\ W^0 & W^0 & W^0 & W^1 & W^1 & W^1 & W^2 & W^2 & W^2 \\ W^0 & W^1 & W^2 & W^1 & W^2 & W^0 & W^2 & W^0 & W \\ W^0 & W^2 & W^1 & W^1 & W & W & W & W^1 & W^0 \\ W^0 & W^0 & W^0 & W^2 & W^2 & W^2 & W & W & W^1 \\ W^0 & W^1 & W^2 & W^2 & W & W & W^1 & W^2 & W^0 \\ W^0 & W^2 & W^1 & W^2 & W^1 & W^0 & W^1 & W^0 & W \end{bmatrix}. \tag{19}$$

Как известно, любая система ВК-К размерности p^m может быть представлена как m-я кронекеровская степень матрицы ДЭФ размерности p, то есть

$$\boldsymbol{S}_{p^m,\text{ВК–К}} = \left(\boldsymbol{S}_{p,\text{ДЭФ}}\right)^{[m]}, \tag{20}$$

где $[m]$ – обозначение m-ой кронекеровской степени матрицы [12]. В частности, $\boldsymbol{S}_{\mathbf{9},\text{ВК-К}} = \boldsymbol{S}_{\mathbf{3},\text{ДЭФ}}^{[3]}$, где

$$\boldsymbol{S}_{\mathbf{3},\text{ДЭФ}} = \begin{bmatrix} W^0 & W^0 & W^0 \\ W^0 & W^1 & W^2 \\ W^0 & W^2 & W \end{bmatrix} = \begin{bmatrix} W^0 & W^0 & W^0 \\ W^0 & W^1 & W^2 \\ W^0 & W^2 & W^1 \end{bmatrix}. \quad (21)$$

Отметим, что матрица $\boldsymbol{S}_{\mathbf{2},\text{ДЭФ}}$ при $W=e^{j\pi}$, совпадает с матрицей функций Уолша-Адамара 2-го порядка. Тогда ее m-я кронекеровская степень – это матрица Уолша-Адамара порядка 2^m. Таким образом, система Уолша-Адамара является частным случаем системы ВК-Кронекера.

Преобразование матрицы-циркулянта *p*-ичной ЛРП к матрице функций Виленкина-Крестенсона

Заметим, что при перестановке столбцов матрицы $\mathfrak{I}_{m,n}$, сформированной на основе любой сопровождающей матрицы исходного полинома (2) при любом значении первообразного элемента $\boldsymbol{\alpha}^0$, по возрастанию значений элементов мультипликативной группы в их десятичном представлении, получим матрицу, столбцы которой представляют собой последовательные значения чисел от 1 до (p^m-1) в p-ичной системе счисления. Эту прямоугольную матрицу размерности $m\times(p^m-1)$ обозначим как $\mathbf{Q}_m$, а дискретные функции, записанные в ее строках, пронумеруем от 0 до $(m-1)$ и обозначим как $\boldsymbol{q}_0,\boldsymbol{q}_1,\ldots,\boldsymbol{q}_{(m-1)}$. Тогда $\mathbf{Q}_m=\begin{bmatrix}\boldsymbol{q}_0 & \boldsymbol{q}_1 & \ldots & \boldsymbol{q}_{m-1}\end{bmatrix}^{\mathrm{T}}$. В частности, при вышеуказанной перестановке столбцов матрицы $\mathfrak{I}_{2,2}$, построенной для полинома $f_2(x)$ при $n=2$ и $p=3$, получим матрицу:

$$\mathbf{Q}_m = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 2 & 2 \\ 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix}. \quad (22)$$

При перестановке столбцов $\mathfrak{I}_{2,2,\text{ц}}$ по возрастанию значений элементов мультипликативной группы поля Галуа получим матрицу, состоящую из степеней элементов $W=e^{j\frac{2\pi}{p}}$ функций ВК без символов, номера которых равны нулю, то есть

$$\mathbb{Q}_{m,p,\text{ВК}} = \begin{bmatrix} \mathbf{Q}_m \\ \boldsymbol{H}_2^m\mathbf{Q}_m \\ \boldsymbol{H}_2^{2m}\mathbf{Q}_m \\ \ldots \\ \boldsymbol{H}_2^{C(N)m}\mathbf{Q}_m \end{bmatrix} = \begin{bmatrix} \boldsymbol{I}_m\mathbf{Q}_m \\ \boldsymbol{H}_2^m\mathbf{Q}_m \\ \boldsymbol{H}_2^{2m}\mathbf{Q}_m \\ \ldots \\ \boldsymbol{H}_2^{C(N)m}\mathbf{Q}_m \end{bmatrix} = \begin{bmatrix} \boldsymbol{I}_m \\ \boldsymbol{H}^m \\ \boldsymbol{H}^{2m} \\ \ldots \\ \boldsymbol{H}_2^{C(N)m} \end{bmatrix}\mathbf{Q}_m, \quad (23)$$

где $\boldsymbol{I}_m$ – единичная матрица размером $m\times m$. Строки матриц $\boldsymbol{H}_2^x\mathbf{Q}_m (x=m,2m,\ldots)$ образуются при суммировании по модулю p всех возможных комбинаций функций $\boldsymbol{q}_0,\boldsymbol{q}_1,\ldots,\boldsymbol{q}_{(m-1)}$ и представляют собой функции ВК без символа с номером ноль. Порядок расположения функций ВК в матрице $\mathbb{Q}_{m,p,\text{ВК}}$ определяется структурой матрицы

$$\boldsymbol{H} = \begin{bmatrix} \boldsymbol{H}_2^m \\ \boldsymbol{H}_2^{2m} \\ \ldots \\ \boldsymbol{H}_2^{C(N)m} \end{bmatrix}. \quad (24)$$

Далее, учитывая, что $\boldsymbol{H}_2^{\mathrm{T}}=\boldsymbol{H}_1$, запишем:

$$\boldsymbol{H}=\left(\boldsymbol{H}^{\mathrm{T}}\right)^{\mathrm{T}}=\left[\left(\left(\boldsymbol{H}_2^{\mathrm{T}}\right)^{\mathrm{T}}\right)^m \quad \left(\left(\boldsymbol{H}_2^{\mathrm{T}}\right)^{\mathrm{T}}\right)^{2m} \quad \ldots \quad \left(\left(\boldsymbol{H}_2^{\mathrm{T}}\right)^{\mathrm{T}}\right)^{C(N)m}\right]^{\mathrm{T}} =$$
$$\left[\left(\boldsymbol{H}_1^{\mathrm{T}}\right)^m \quad \left(\boldsymbol{H}_1^{\mathrm{T}}\right)^{2m} \quad \ldots \quad \left(\boldsymbol{H}_1^{\mathrm{T}}\right)^{C(N)m}\right]^{\mathrm{T}} = \begin{bmatrix} \left(\boldsymbol{H}_1^m\right)^{\mathrm{T}} \\ \left(\boldsymbol{H}_1^{2m}\right)^{\mathrm{T}} \\ \ldots \\ \left(\boldsymbol{H}_1^{C(N)m}\right)^{\mathrm{T}} \end{bmatrix}, \quad (25)$$

где

$$\left(\boldsymbol{H}_1\right)^m=\left(\boldsymbol{H}_1\right)^{m-1}\boldsymbol{H}_1=\left(\boldsymbol{H}_1\right)^{m-1}\begin{bmatrix} 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & \ldots & 0 & a_1 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & 0 & a_{m-2} \\ 0 & 0 & \ldots & 1 & a_{m-1} \end{bmatrix}. \quad (26)$$

Затем выберем первообразный элемент мультипликативной группы поля Галуа, совпадающим с крайним левым столбцом $\boldsymbol{H}_1$, то есть $\boldsymbol{\alpha}^0=\begin{bmatrix}0 & 1 & 0 & \ldots & 0 & 0\end{bmatrix}^{\mathrm{T}}$. Тогда $\boldsymbol{H}_1\boldsymbol{\alpha}^0=\boldsymbol{\alpha}^1=\begin{bmatrix}0 & 0 & 1 & \ldots & 0 & 0\end{bmatrix}^{\mathrm{T}}$ совпадает со вторым столбцом $\boldsymbol{H}_1$. Продолжая получим: $\boldsymbol{\alpha}^{m-1}=\boldsymbol{H}_1\boldsymbol{\alpha}^{m-2}=\boldsymbol{H}_1\begin{bmatrix}0 & 0 & \ldots & 0 & 1\end{bmatrix}^{\mathrm{T}}=\begin{bmatrix}a_0 & a_1 & \ldots & a_{m-1}\end{bmatrix}^{\mathrm{T}}$, то есть $\boldsymbol{\alpha}^{m-1}$ соответствует последнему столбцу матрицы $\boldsymbol{H}_1$, в результате чего при выборе в качестве $\boldsymbol{\alpha}^0$ первый столбец матрицы $\boldsymbol{H}_1$ получим формулу: $\boldsymbol{H}_1=\begin{bmatrix}\boldsymbol{\alpha}^0 & \boldsymbol{\alpha}^1 & \ldots & \boldsymbol{\alpha}^{m-1}\end{bmatrix}$. Но тогда

$$\left(\boldsymbol{H}_1\right)^m=\left[\left(\boldsymbol{H}_1\right)^{m-1}\boldsymbol{\alpha}^0 \quad \left(\boldsymbol{H}_1\right)^{m-1}\boldsymbol{\alpha}^1 \quad \ldots \quad \left(\boldsymbol{H}_1\right)^{m-1}\boldsymbol{\alpha}^{m-1}\right]=\left[\boldsymbol{\alpha}^{m-1} \quad \boldsymbol{\alpha}^m \quad \ldots \quad \boldsymbol{\alpha}^{2m-2}\right];$$
$$\left(\boldsymbol{H}_1\right)^{2m}=\left(\boldsymbol{H}_1\right)^{2m-1}\boldsymbol{H}_1=\left[\boldsymbol{\alpha}^{2m-1} \quad \boldsymbol{\alpha}^{2m} \quad \ldots \quad \boldsymbol{\alpha}^{3m-2}\right] \text{ и т.д.} \quad (27)$$

Таким образом,

$$\boldsymbol{H}=\left[\boldsymbol{\alpha}^{(m-1)^{\mathrm{T}}} \quad \boldsymbol{\alpha}^{m^{\mathrm{T}}} \quad \ldots \quad \boldsymbol{\alpha}^{(2m-2)^{\mathrm{T}}} \quad \boldsymbol{\alpha}^{(C(N)m-1)^{\mathrm{T}}} \quad \boldsymbol{\alpha}^{C(N)m^{\mathrm{T}}} \quad \ldots \quad \boldsymbol{\alpha}^{((C(N)+1)m-2)^{\mathrm{T}}}\right]^{\mathrm{T}} \quad (28)$$

где $\boldsymbol{\alpha}^0=\begin{bmatrix}0 & 1 & 0 & \ldots & 0 & 0\end{bmatrix}^{\mathrm{T}}$.

Анализ последней формулы позволяет сделать вывод: строки $\boldsymbol{H}$ являются элементами мультипликативной группы, сформированной с использованием матрицы $\boldsymbol{H}_1$, причем ее нулевая строка соответствует $(m-1)$-му элементу группы, а последняя – $((C(N)+1)m-2)$-му элементу. Первообразным элементом этой группы будет $\boldsymbol{\alpha}^{m-1} = \boldsymbol{H}_1^{\,m-1}\boldsymbol{\alpha}^0 = \begin{bmatrix} a_0 & a_1 & \dots & a_{m-1} \end{bmatrix}^{\mathrm{T}}$. Тогда

$$\mathbb{Q}_{m,p,\text{ВК}} = \begin{bmatrix} \boldsymbol{I}_m \\ \boldsymbol{H} \end{bmatrix} \mathbf{Q}_m = \begin{bmatrix} 1 & 0 & \dots & 0 \\ & \boldsymbol{H} & & \end{bmatrix} \mathbf{Q}_m =, \tag{29}$$

где $\boldsymbol{H}_p$ – матрица, строки которой представляют собой элементы мультипликативной группы поля Галуа, основанной на $\boldsymbol{H}_1$ при первообразном элементе группы $\boldsymbol{\alpha}^0 = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \end{bmatrix}^{\mathrm{T}}$. Кроме того, при умножении $\boldsymbol{H}_1$ на верхнюю строку матрицы $\boldsymbol{I}_m$ получим столбец $\begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \end{bmatrix}^{\mathrm{T}}$. Тогда первые N строк, матрицы $\begin{bmatrix} \boldsymbol{I}_m \\ \boldsymbol{H} \end{bmatrix}$– это полный набор элементов мультипликативной группы поля Галуа, построенной на основе сопровождающей матрицы $\boldsymbol{H}_1$, что соответствует $\mathfrak{I}_{m,1}^{\mathrm{T}}$. Таким образом,

$$\mathbb{Q}_{m,p,\text{ВК}} = \mathfrak{I}_{m,1}^{\mathrm{T}} \boldsymbol{Q}_m = \begin{bmatrix} x_{0,0} & x_{1,0} & \dots & x_{m-1,0} \\ x_{0,1} & x_{1,1} & \dots & x_{m-1,1} \\ . & . & . & . \\ x_{0,N-1} & x_{1,N-1} & \dots & x_{m-1,N-1} \end{bmatrix} \boldsymbol{Q}_m, \tag{30}$$

где $\boldsymbol{\alpha}^0 \boldsymbol{H}_1 = \begin{bmatrix} x_{0,0} & x_{1,0} & \dots & x_{m-1,0} \end{bmatrix}^{\mathrm{T}} = \begin{bmatrix} 1 & 0 & \dots & 0 & 0 \end{bmatrix}^{\mathrm{T}}$.
Полученные результаты можно распространить на случай использования матриц $\boldsymbol{H}_3$ и $\boldsymbol{H}_4$.

Из (26) следует, что для преобразования матрицы-циркулянта p -ичной ЛРП, построенной на основе сопровождающей матрицы неприводимого примитивного полинома $\boldsymbol{H}_2$ или $\boldsymbol{H}_4$ в матрицу, состоящую из степеней функций ВК без символа с номером ноль, надо переставить ее столбцы по возрастанию значений элементов мультипликативной группы (в их десятичном представлении) соответствующего поля Галуа, построенную на основе тех же $\boldsymbol{H}_2$ или $\boldsymbol{H}_4$ соответственно. Так, для полинома $f_2(x)$ и его сопровождающих матриц $\boldsymbol{H}_2$, $\boldsymbol{H}_4$, учитывая, что в данном случае $\boldsymbol{H}_1 = \boldsymbol{H}_2$ и $\boldsymbol{H}_3 = \boldsymbol{H}_4$, получим матрицы:

$$\mathbb{Q}_{2,3,\text{ВК}} = \begin{bmatrix} 0 & 0 & & & 1 & 2 & 2 & 2 \\ 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \\ 2 & 1 & 1 & 0 & 2 & & 1 & 0 \\ 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 \\ 2 & 1 & 0 & & 1 & 0 & & 1 \\ 2 & 1 & 2 & 1 & 0 & 1 & 0 & 2 \\ 1 & 2 & 2 & 0 & 1 & 1 & 2 & 0 \end{bmatrix},$$

$$\mathbb{Q}_{2,3,\text{ВК}} = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 2 & 0 & 1 & 2 & 0 & & 2 \\ 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \\ 1 & 2 & 2 & 0 & 1 & 1 & 2 & 0 \\ 2 & 1 & 0 & 2 & 1 & 0 & & 1 \\ 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 \\ 2 & 1 & 2 & 1 & 0 & 1 & 0 & 2 \end{bmatrix}. \tag{31}$$

Соответственно для полинома $f_2^{'}(x)$ – матрицы:

$$\mathbb{Q}_{2,3,\text{ВК}} = \begin{bmatrix} 0 & 0 & 1 & 1 & & 2 & 2 & 2 \\ 1 & 2 & 0 & & 2 & 0 & & 2 \\ 2 & 1 & 1 & 0 & 2 & 2 & 1 & 0 \\ 2 & 1 & 2 & 1 & 0 & 1 & 0 & 2 \\ 0 & 0 & 2 & 2 & & 1 & 1 & \\ 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 \\ 1 & 2 & 2 & 0 & 1 & 1 & 2 & 0 \\ 1 & 2 & 1 & 2 & 0 & 2 & 0 & \end{bmatrix},$$

$$\mathbb{Q}_{2,3,\text{ВК}} = \begin{bmatrix} 0 & 0 & 1 & 1 & & 2 & 2 & \\ 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \\ 2 & 1 & 1 & 0 & 2 & 2 & 1 & 0 \\ 0 & 0 & 2 & 2 & & 1 & 1 & \\ 2 & 1 & 2 & 2 & 1 & 0 & 2 & 1 \\ 2 & 1 & 0 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 2 & 0 & 1 & 1 & 0 & 2 \end{bmatrix}. \tag{32}$$

Учитывая, что систему ФВ-К без строки и столбца с номером ноль и представленную в виде степеней W можно сформировать как

$$\boldsymbol{S}_{p^m-1,\text{ВК-К}} = \begin{bmatrix} z_{0,0} & z_{1,0} & \dots & z_{m-1,0} \\ z_{0,1} & z_{1,1} & \dots & z_{m-1,1} \\ . & . & . & . \\ z_{0,N-1} & z_{1,N-1} & \dots & z_{m-1,N-1} \end{bmatrix} \boldsymbol{Q}_m, \tag{33}$$

где строки $\begin{bmatrix} z_{0,i} & z_{1,i} & \dots & z_{m-1,i} \end{bmatrix}$, $i = 0,\dots,(N-1)$ – номер строки являются представлениями чисел $(i+1)$ в p-ичной системе счисления, получим, что любую матрицу (31), (32) можно преобразовать в $\boldsymbol{S}_{p^m-1,\text{ВК-К}}$ путем перестановки ее строк по возрастанию соответствующих ей значений $\left[\boldsymbol{\alpha}^k\right]_{10}$, $k = 0,\dots,N-1$. Так, для $f_2(x)$ и $\boldsymbol{H}_1$ значения $\left[\boldsymbol{\alpha}^k\right]_{10}$ равны 3,1,4,5,6,2,8,7 (см.табл.2). Тогда 1-я строка левой матрицы (31) будет 3-ей в матрице $\boldsymbol{S}_{p^m-1,\text{ВК-К}}$, 2-я будет 1-ой, 3-я будет 4-ой и т.д. Легко проверить, что любая матрица (31), (32) преобразуется в матрицу:

$$\boldsymbol{S}_{p^m-1,\text{ВК-К}}=\begin{bmatrix}1&2&0&&2&0&&2\\2&1&0&2&1&0&&1\\0&0&1&1&&2&2&2\\1&2&1&2&0&2&0&1\\2&1&1&0&2&2&1&0\\0&0&2&2&&1&1&\\1&2&2&0&1&1&2&0\\2&1&2&1&0&1&0&2\end{bmatrix}. \quad (34)$$

Таким образом, доказано, что любая матрица-циркулянт p-ичной ЛРП размерности (p^m-1) преобразуется в матрицу из степеней $W=e^{j\frac{2\pi}{p}}$ элементов функций ВК размерности p^m при любом способе ее упорядочения путем перестановки строк и столбцов с последующим добавлением строки и столбца с номером ноль, состоящих из нулей.

Передача и обработка информационных сигналов на основе матрицы-циркулянта *p*-ичной ЛРП

Каждую строку матрицы ортогональной системы дискретных функций $\boldsymbol{S}_{p^m}{}^{*}$ размерности $p^m=(N+1)$ построенной на основе любой p-ичной ЛРП, будем считать низкочастотным дискретным представлением ортогональной негармонической поднесущей, использующейся для передачи информационных символов. Процедуру модуляции поднесущих в математической форме можно представить как перемножение матриц:

$$\boldsymbol{S}_{\text{и},p^m}{}^{*}=\boldsymbol{I}_{\text{и,м},A}\boldsymbol{S}_{p^m}{}^{a*},\boldsymbol{I}_{\text{и,м},A}=\begin{bmatrix}A_0e^{j\varphi_{0A}}&0&0&\dots&0\\0&A_1e^{j\varphi_{1A}}&\dots&\dots&0\\\dots&\dots&\dots&\dots&\dots\\0&0&0&\dots&A_Ne^{j\varphi_{NA}}\end{bmatrix},$$

$$\boldsymbol{S}_{p^m}{}^{a*}=\begin{bmatrix}s_{00}{}^{a*}&s_{01}{}^{a*}&\dots&s_{0N}{}^{a*}\\s_{10}{}^{a*}&s_{11}{}^{a*}&\dots&s_{1N}{}^{a*}\\\dots&\dots&\dots&\dots\\s_{N0}{}^{a*}&s_{N1}{}^{a*}&\dots&s_{NN}{}^{a*}\end{bmatrix}, \quad (35)$$

где $\boldsymbol{I}_{\text{и,м},A}$ – диагональная матрица, значения элементов главной диагонали которой равны передаваемым информационным символам; A_i,φ_i – значения амплитуды и фазы i-го информационного символа соответственно; $s_{ik}{}^{a*}$ – значения символов матрицы $\boldsymbol{S}_{\text{и},p^m}{}^{*}$; $i,k=0,\dots,N$ – номера строк и столбцов матриц $\boldsymbol{S}_{\text{и},p^m}{}^{*}$, $\boldsymbol{I}_{\text{и,м},A}$ и $\boldsymbol{S}_{p^m}{}^{a*}$.

Низкочастотный дискретный эквивалент результирующего информационного сигнала, передаваемого по каналу связи, образуется при суммировании строк матрицы $\boldsymbol{S}_{\text{и},p^m}{}^{*}$, в результате чего на входе приемника с учетом воздействия белого гауссовского шума с отсчетами $\xi_0,\xi_2,\dots,\xi_N$, получим:

$$\boldsymbol{X}^{\text{T}}=\begin{bmatrix}s_{00}{}^{a*}\\s_{01}{}^{a*}\\\dots\\s_{0N}{}^{a*}\end{bmatrix}A_0e^{j\varphi_{0A}}+\begin{bmatrix}s_{10}{}^{a*}\\s_{11}{}^{a*}\\\dots\\s_{1N}{}^{a*}\end{bmatrix}A_1e^{j\varphi_{1A}}+\dots+\begin{bmatrix}s_{N0}{}^{a*}\\s_{N1}{}^{a*}\\\dots\\s_{NN}{}^{a*}\end{bmatrix}A_Ne^{j\varphi_{NA}}+\begin{bmatrix}\xi_0\\\xi_1\\\dots\\\xi_N\end{bmatrix}. \quad (36)$$

Отметим, что из формулы (36) следует, что с точки зрения передающей стороны не имеет значения, какой способ упорядочения строк исходной системы $\boldsymbol{S}_{p^m}{}^{*}$ использовался для передачи информационных символов, поскольку столбцы в ней можно переставлять в произвольном порядке. Но, очевидно, что каждый информационный символ связан с определенной строкой матрицы $\boldsymbol{S}_{p^m}{}^{*}$. Но, как следует из предыдущего раздела, существует N ее вариантов, каждый из которых можно получить путем циклической перестановкой строк любой другой матрицы из их набора при выборе соответствующего первообразного элемента мультипликативной группы поля Галуа в сочетании с сопровождающей матрицей полинома $\boldsymbol{H}_2$, использующихся при построении матрицы. При этом все вышеуказанные варианты матриц $\boldsymbol{S}_{p^m}{}^{*}$ приводятся к одной и той же матрице функций ВК путем перестановки столбцов, начиная со столбца с номером один, в порядке возрастания значений элементов соответствующей мультипликативной группы, начиная с первого элемента. Поэтому, если с целью использования обобщенного БПФ при обработке сигналов на приемной стороне будет производиться перестановка символов начиная не с того первообразного элемента, который использовался для построения матрицы $\boldsymbol{S}_{p^m}{}^{*}$ на передающей стороне, то принимаемый информационный символ будет привязан не к той строке матрицы функций ВК, по сравнению со случаем, когда перестановка начиналась бы с того же первообразного элемента. Это обстоятельство позволяет использовать вариант перемежения информационных символов, когда заранее выбирается пара первообразных элементов, использующихся на передающей и приемной стороне и соответствующий им вариант перемежения информационных символов.

В дальнейшем, учитывая, что в упорядоченной матрице $\boldsymbol{S}_{p^m}{}^{a*}$ строки и столбцы с одинаковыми номерами одинаковые, будем считать, что

$$\boldsymbol{X}^{\text{T}}=\boldsymbol{S}_{p^m}{}^{a*}\boldsymbol{I}_{\text{и},A}+\xi,\boldsymbol{I}_{\text{и},A}=\begin{bmatrix}A_0e^{j\varphi_{0A}}\\A_1e^{j\varphi_{1A}}\\\dots\\A_Ne^{j\varphi_{NA}}\end{bmatrix}, \quad (37)$$

где ξ – столбец из отсчетов шумовой помехи, $\boldsymbol{I}_{\text{и},A}$ – столбец из информационных символов. Действительно,

$$\boldsymbol{S}_{p^m}{}^{a*}\boldsymbol{I}_{\text{и},A}=\begin{bmatrix} s_{00}{}^{a*} & s_{01}{}^{a*} & \dots & s_{0N}{}^{a*} \\ s_{10}{}^{a*} & s_{11}{}^{a*} & \dots & s_{1N}{}^{a*} \\ \dots & \dots & \dots & \dots \\ s_{N0}{}^{a*} & s_{N1}{}^{a*} & \dots & s_{NN}{}^{a*} \end{bmatrix}\begin{bmatrix} A_0 e^{j\varphi_{0A}} \\ A_1 e^{j\varphi_{1A}} \\ \dots \\ A_N e^{j\varphi_{NA}} \end{bmatrix}= \tag{38}$$

$$\begin{bmatrix} s_{00}{}^{a*}A_0e^{j\varphi_{0A}}+s_{01}{}^{a*}A_1e^{j\varphi_{1A}}+\dots+s_{0N}{}^{a*}A_Ne^{j\varphi_{NA}} \\ s_{10}{}^{a*}A_0e^{j\varphi_{0A}}+s_{11}{}^{a*}A_1e^{j\varphi_{1A}}+\dots+s_{1N}{}^{a*}A_Ne^{j\varphi_{NA}} \\ \dots \\ s_{N0}{}^{a*}A_0e^{j\varphi_{0A}}+s_{N1}{}^{a*}A_1e^{j\varphi_{1A}}+\dots+s_{NN}{}^{a*}A_Ne^{j\varphi_{NA}} \end{bmatrix}$$

Для упорядоченной матрицы $\boldsymbol{S}_{p^m}{}^{a*}$ для любых значений i,k справедливо $s_{ik}{}^{a*}=s_{ki}{}^{a*}$. Тогда после соответствующей перестановки символов итоговой матрицы (38) получаем сигнальную составляющую формулы (36).

Оптимальная обработка $\boldsymbol{X}^{\text{T}}$ в приемнике описывается как:

$$\begin{aligned}\boldsymbol{Y}_A &= \boldsymbol{S}_{p^m}{}^{a}\boldsymbol{X}^{\text{T}} = \boldsymbol{S}_{p^m}{}^{a}\boldsymbol{S}_{p^m}{}^{a*}\boldsymbol{I}_{\text{и},A}+\boldsymbol{S}_{p^m}{}^{a}\boldsymbol{\xi} = \\ &= p^m\boldsymbol{I}\boldsymbol{I}_{\text{и},A}+\boldsymbol{\xi}_1 = p^m\boldsymbol{I}_{\text{и},A}+\boldsymbol{\xi}_1,\end{aligned} \tag{39}$$

где ξ_1 – столбец из отсчетов шумовой помехи на входе решающего устройства (РУ). В действительности $\boldsymbol{S}_{p^m}{}^{a*}\boldsymbol{I}_{\text{и},A}$ присутствует во входной смеси в виде вектора, и производится однократное умножение на него матрицы $\boldsymbol{S}_{p^m}{}^{a}$.

С целью использования алгоритма обобщенного БПФ при этом перемножении, введем операторы $\boldsymbol{R}^{\rightarrow}_{\alpha,H_n}$ и $\boldsymbol{R}^{\uparrow}_{\alpha,H_n}$ перестановки столбцов матрицы (или символов строки) и ее строк (или элементов столбца), начиная со строки или столбца с номером один, по возрастанию значений элементов $\left[\boldsymbol{\alpha}^k\right]_{10}$ $(k=0,\dots,(N-1))$ мультипликативной группы расширенного поля Галуа по модулю некоторого неприводимого примитивного полинома. Данная группа построена на основе сопровождающей матрицы исходного полинома $\boldsymbol{H}_n$. Будем рассматривать также и операторы обратной перестановки, которые соответственно обозначим как $\boldsymbol{R}^{\leftarrow}_{\alpha,H_n}$ и $\boldsymbol{R}^{\downarrow}_{\alpha,H_n}$. Тогда сигнальная составляющая вектора-строки $\boldsymbol{R}^{\rightarrow}_{\alpha,H_2}\left[\boldsymbol{X}\right]$ представляет собой сумму всех дискретных функций ВК одного и того же набора, каждая из которых умножена на свой информационный символ, а сигнальная составляющая вектора-столбца $\boldsymbol{R}^{\uparrow}_{\alpha,H_2}\left[\boldsymbol{X}^{\text{T}}\right]$ соответствует транспонированной строке $\boldsymbol{R}^{\rightarrow}_{\alpha,H_2}\left[\boldsymbol{X}\right]$, то есть

$$\boldsymbol{R}^{\uparrow}_{\alpha,H_2}\left[\boldsymbol{S}_{p^m}{}^{a*}\boldsymbol{I}_{\text{и}}\right]=\boldsymbol{R}^{\uparrow}_{\alpha,H_2}\left[\boldsymbol{S}_{p^m}{}^{a*}\right]\boldsymbol{I}_{\text{и},A}. \tag{40}$$

Но для того, чтобы результат вычисления по (38) не изменился после такой перестановки, необходимо в нем вместо $\boldsymbol{S}_{p^m}{}^{a}$ использовать матрицу $\boldsymbol{R}^{\rightarrow}_{\alpha,H_2}\left[\boldsymbol{S}_{p^m}{}^{a}\right]$, в которой строки преобразованы к функциям ВК.

Далее, учитываем, что $\boldsymbol{R}^{\uparrow}_{\alpha,H_2}\left[\boldsymbol{R}^{\rightarrow}_{\alpha,H_2}\left[\boldsymbol{S}_{p^m}{}^{a}\right]\right]=\boldsymbol{S}_{p^m,\text{ВК-К}}$. Это значит, что после быстрого умножения $\boldsymbol{S}_{p^m,\text{ВК-К}}$ с помощью обобщенного БПФ на вектор $\boldsymbol{R}^{\uparrow}_{\alpha,H_2}\left[\boldsymbol{S}_{p^m}{}^{a*}\right]\boldsymbol{I}_{\text{и},A}$ получим вектор-столбец $\boldsymbol{R}^{\uparrow}_{\alpha,H_2}\left[\boldsymbol{I}_{\text{и},A}\right]$, то есть для восстановления исходной последовательности символов необходимо осуществить обратную перестановку элементов полученного столбца, то есть $\boldsymbol{R}^{\downarrow}_{\alpha,H_1}\left[\boldsymbol{R}^{\uparrow}_{\alpha,H_1}\left[\boldsymbol{I}_{\text{и},A}\right]\right]$. Напомним, что все перестановки, описываемые оператором $\boldsymbol{R}^{\uparrow}_{\alpha,H_n}$, начинаются с первообразного элемента $\alpha^0=\left[1\ \ 0\ \ \dots\ \ 0\right]$. В действительности $\boldsymbol{R}^{\downarrow}_{\alpha,H_1}[\boldsymbol{I}_{\text{и},A}]$ может быть произведена на передающей стороне и рассматриваться как вариант дополнительного перемежения передаваемых информационных символов.

Передача в общей полосе частот и обработка информационных сигналов на основе одновременно многих матриц-циркулянтов разных *p*-ичных ЛРП при компенсации их взаимных помех

Предположим, что для передачи информации используются одновременно две разные полные ортогональные системы *a* и *b*, сформированные на основе двух разных неприводимых примитивных полиномов одного и того же порядка. Тогда информационный сигнал, передаваемый в канале связи, имеет вид:

$$\boldsymbol{S}_{\text{и},p^m}=\boldsymbol{I}_{\text{и,м},A}\boldsymbol{S}_{p^m}{}^{a*}+\boldsymbol{I}_{\text{и,м},B}\boldsymbol{S}_{p^m}{}^{b*},$$

$$\boldsymbol{S}_{p^m}{}^{a*}=\begin{bmatrix} s_{00}{}^{a*} & s_{01}{}^{a*} & \dots & s_{0N}{}^{a*} \\ s_{10}{}^{a*} & s_{11}{}^{a*} & \dots & s_{1N}{}^{a*} \\ \dots & \dots & \dots & \dots \\ s_{N0}{}^{a*} & s_{N1}{}^{a*} & \dots & s_{NN}{}^{a*} \end{bmatrix},$$

$$\boldsymbol{S}_{p^m}{}^{b*}=\begin{bmatrix} s_{00}{}^{b*} & s_{01}{}^{b*} & \dots & s_{0N}{}^{b*} \\ s_{10}{}^{b*} & s_{11}{}^{b*} & \dots & s_{1N}{}^{b*} \\ \dots & \dots & \dots & \dots \\ s_{N0}{}^{b*} & s_{N1}{}^{b*} & \dots & s_{NN}{}^{b*} \end{bmatrix},$$

$$\boldsymbol{I}_{\text{и,м},A}=\begin{bmatrix} A_0e^{j\varphi_{0A}} & 0 & 0 & \dots & 0 \\ 0 & A_1e^{j\varphi_{1A}} & \dots & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & A_Ne^{j\varphi_{NA}} \end{bmatrix},$$

$$\boldsymbol{I}_{\text{и,м},B}=\begin{bmatrix} B_0e^{j\varphi_{0B}} & 0 & 0 & \dots & 0 \\ 0 & B_1e^{j\varphi_{1B}} & \dots & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & B_Ne^{j\varphi_{NB}} \end{bmatrix}, \tag{41}$$

где $\boldsymbol{I}_{\text{и,м,}A}$, $\boldsymbol{I}_{\text{и,м,}B}$ – диагональные матрицы, значения элементов диагоналей которых равны передаваемым информационным символам $A_i e^{j\varphi_{iA}}$ и $B_i e^{j\varphi_{iB}}$.

Результирующий сигнал на входе приемника формируется в соответствии с формулой:

$$\boldsymbol{X}^{\text{T}} = \begin{bmatrix} s_{00}{}^{a*} \\ s_{01}{}^{a*} \\ \dots \\ s_{0N}{}^{a*} \end{bmatrix} A_0 e^{j\varphi_{0A}} + \begin{bmatrix} s_{10}{}^{a*} \\ s_{11}{}^{a*} \\ \dots \\ s_{1N}{}^{a*} \end{bmatrix} A_1 e^{j\varphi_{1A}} + \dots + \begin{bmatrix} s_{N0}{}^{a*} \\ s_{N1}{}^{a*} \\ \dots \\ s_{NN}{}^{a*} \end{bmatrix} A_N e^{j\varphi_{NA}} + \begin{bmatrix} s_{00}{}^{b*} \\ s_{01}{}^{b*} \\ \dots \\ s_{0N}{}^{b*} \end{bmatrix} B_0 e^{j\varphi_{0B}} + \begin{bmatrix} s_{10}{}^{b*} \\ s_{11}{}^{b*} \\ \dots \\ s_{1N}{}^{b*} \end{bmatrix} B_1 e^{j\varphi_{1B}} + \dots + \begin{bmatrix} s_{N0}{}^{b*} \\ s_{N1}{}^{b*} \\ \dots \\ s_{NN}{}^{b*} \end{bmatrix} B_N e^{j\varphi_{NB}} + \begin{bmatrix} \xi_0 \\ \xi_1 \\ \dots \\ \xi_N \end{bmatrix}. \quad (42)$$

Далее, перепишем (41) аналогично (37), в результате чего получим:

$$\boldsymbol{X}^{\text{T}} = \boldsymbol{S}_{p^m}{}^{a*} \boldsymbol{I}_{\text{и,}A} + \boldsymbol{S}_{p^m}{}^{b*} \boldsymbol{I}_{\text{и,B}} + \boldsymbol{\xi}. \quad (43)$$

Допустим, в приемнике принимается решение о значениях информационных символов, описываемых столбцом $\boldsymbol{I}_{\text{и,}A}$, при полном подавлении взаимных помех, создаваемых из-за передачи в той же полосе частот информационных символов $\boldsymbol{I}_{\text{и,B}}$ с помощью набора ортогональных поднесущих $\boldsymbol{S}_{p^m}{}^{b*}$. Очевидно, что для полного обнуления их вклада в $\boldsymbol{X}^{\text{T}}$, независимо от их значений, следует матричное уравнение (43) слева и справа умножить слева на матрицу $\boldsymbol{U}$ такую, что $\boldsymbol{UX}^{\text{T}} \neq \boldsymbol{0}$, $\boldsymbol{US}_{p^m}{}^{a*} \neq \boldsymbol{0}$ и $\boldsymbol{US}_{p^m}{}^{b*} = \boldsymbol{0}$, где $\boldsymbol{0}$ – матрица, состоящая из нулей. То есть нужно решить матричное уравнение $\boldsymbol{US}_{p^m}{}^{b*} = \boldsymbol{0}$, причем целесообразно использовать такие его решения, при которых перемножение матриц $\boldsymbol{U}$ и $\boldsymbol{X}^{\text{T}}$ допускает использование обобщенного БПФ. Кроме того, $\boldsymbol{U}$ должна обращаться, и при умножении $\boldsymbol{U}^{-1}$ на вектор или матрицу так же целесообразно использовать обобщенное БПФ. Очевидно, что данная задача не имеет решения, так как требует подбора матрицы $\boldsymbol{U}$, строки которой состоят из дискретных функций, ортогональных по отношению к столбцам ортогональной системы $\boldsymbol{S}_{p^m}{}^{b*}$.

В качестве исходных ортогональных систем a и b будем использовать действительные части $\boldsymbol{S}_{p^m}{}^{a}$ и $\boldsymbol{S}_{p^m}{}^{b}$, а для обнуления в $\boldsymbol{X}^{\text{T}}$ вклада $\boldsymbol{I}_{\text{и,}B}$, передаваемых с помощью набора условно ортогональных поднесущих $\boldsymbol{S}_{p^m}{}^{b}$, будем использовать их мнимые части. В этом случае

$$\boldsymbol{X}^{\text{T}} = Re\left[\boldsymbol{S}_{p^m}{}^{a}\right]\boldsymbol{I}_{\text{и,}A} + Re\left[\boldsymbol{S}_{p^m}{}^{b}\right]\boldsymbol{I}_{\text{и,}B} + \boldsymbol{\xi}\cdot \quad (44)$$

Умножив матричное уравнение (44) слева и справа на $Im\left[\boldsymbol{S}_{p^m}{}^{b}\right]$ слева, получим:

$$Im\left[\boldsymbol{S}_{p^m}{}^{b}\right]Re\left[\boldsymbol{S}_{p^m}{}^{a}\right]\boldsymbol{I}_{\text{и,}A} + Im\left[\boldsymbol{S}_{p^m}{}^{b}\right]Re\left[\boldsymbol{S}_{p^m}{}^{b}\right]\boldsymbol{I}_{\text{и,}B} + \boldsymbol{\xi} = Im\left[\boldsymbol{S}_{p^m}{}^{b}\right]\boldsymbol{X}^{\text{T}}. \quad (45)$$

Далее, в силу *Свойства 3* из раздела 2 настоящей статьи получаем:

$$Im\left[\boldsymbol{S}_{p^m}{}^{b}\right]Re\left[\boldsymbol{S}_{p^m}{}^{a}\right]\boldsymbol{I}_{\text{и,}A} + Im\left[\boldsymbol{S}_{p^m}{}^{b}\right]\boldsymbol{\xi} = Im\left[\boldsymbol{S}_{p^m}{}^{b}\right]\boldsymbol{X}^{\text{T}} \quad (45)$$

Отметим, что при умножении $Im\left[\boldsymbol{S}_{p^m}{}^{b}\right]$ на $\boldsymbol{X}^{\text{T}}$ обнуляется и символ $A_0 e^{j\varphi_{0A}}$, передаваемый на поднесущей, находящейся в строке с номером ноль исходной ортогональной системы $Re\left[\boldsymbol{S}_{p^m}{}^{a}\right]$, поскольку строка с этим номером матрицы $Im\left[\boldsymbol{S}_{p^m}{}^{b}\right]$ состоит из нулей. Но данное обстоятельство не имеет значения, так как на поднесущей с номером ноль никогда не передается информационный символ. Обычно она используется для передачи синхросигнала, который обрабатывается до приема информации, после чего удаляется из входной смеси [1,2]. Таким образом, из (45) следует:

$$\begin{aligned} &\boldsymbol{I}_{\text{и,}A} + \left[Im\left[\boldsymbol{S}_{p^m}{}^{b}\right]\right]^{-1}\left[Re\left[\boldsymbol{S}_{p^m}{}^{a}\right]\right]^{-1}\boldsymbol{\xi} = \\ &= \left[Re\left[\boldsymbol{S}_{p^m}{}^{a}\right]\right]^{-1}\left(\left[Im\left[\boldsymbol{S}_{p^m}{}^{b}\right]\right]^{-1} Im\left[\boldsymbol{S}_{p^m}{}^{b}\right]\boldsymbol{X}^{\text{T}}\right) \end{aligned} \quad (46)$$

Отметим, что матричные произведения в левой части (46) должны быть реализованы последовательно. Сначала вычисляется $Im\left[\boldsymbol{S}_{p^m}{}^{b}\right]\boldsymbol{X}^{\text{T}}$, в результате чего обнуляется вклад $\boldsymbol{I}_{\text{и,}B}$ в $\boldsymbol{X}^{\text{T}}$, затем полученный результат умножается на $\left[Im\left[\boldsymbol{S}_{p^m}{}^{b}\right]\right]^{-1}$, после чего производится умножение на $\left[Re\left[\boldsymbol{S}_{p^m}{}^{a}\right]\right]^{-1}$. Но необходимо учитывать, что матрица $Im\left[\boldsymbol{S}_{p^m}{}^{b}\right]$ не обращается в строгом смысле, так как ее строка и столбец с номером ноль состоят из нулей. Далее, учитывая *Свойства 4 и 5* из раздела 2 этой статьи, перепишем (46) в виде:

$$\boldsymbol{I}_{\text{и,}A} + \boldsymbol{\xi}_A = \left[I_{y1}\right]^{-1} Re\left[\boldsymbol{S}_{p^m}{}^{a}\right]\left(\left[I_{y2}\right]^{-1} Im\left[\boldsymbol{S}_{p^m}{}^{b}\right]\left(Im\left[\boldsymbol{S}_{p^m}{}^{b}\right]\boldsymbol{X}^{\text{T}}\right)\right), \quad (47)$$

где $\xi_A = \left[I_{y1}\right]^{-1} Re\left[\mathbf{S}_{p^m}{}^a\right]\left[I_{y2}\right]^{-1} Im\left[\mathbf{S}_{p^m}{}^b\right]\xi$ – шумовая помеха.

Еще раз подчеркнем, что перемножение матриц в правой части (47) осуществляются строго с конца, причем при каждом перемножении предварительно производится перестановка строк и столбцов матриц в соответствии с правилами, описанными в предыдущем разделе данной статьи, после чего используется обобщенное БПФ, соответствующее вычислению его действительной или мнимой части, то есть число элементарных арифметических операций при вычислении правой части (47) всего лишь в 1,5 больше, чем при однократном обобщенном БПФ той же размерности.

Повторяя аналогичные рассуждения для случая подавления $\boldsymbol{I}_{\text{и},A}$, получим:

$$\boldsymbol{I}_{\text{и},B} + \xi_B = \left[I_{y1}\right]^{-1} Re\left[\mathbf{S}_{p^m}{}^b\right]\left(\left[I_{y2}\right]^{-1} Im\left[\mathbf{S}_{p^m}{}^a\right]\left(Im\left[\mathbf{S}_{p^m}{}^a\right]\mathbf{X}^{\mathrm{T}}\right)\right) \quad (48)$$

Очевидно, что формулы (47), (48) могут быть обобщены для любого числа ортогональных сигнатур, с помощью которых передается поток информационных символов в общей полосе частот.

Заключение

На основе любой линейной рекуррентной последовательности (ЛРП) максимального периода $p^m - 1$ можно построить системы ортогональных сигнатур, которые в данной работе представлены в виде матриц размерности p^m, где p и m – целые положительные числа. Элементы любой такой матрицы являются степенями комплексного числа $W = e^{j2\pi/p}$. Исключая из нее строки и столбца с номером ноль, состоящие из нулевых степеней W, и рассматривая только степени W, получим матрицу-циркулянт исходной ЛРП, построенную на основе одной из четырех мультипликативных групп расширенного поля Галуа по модулю неприводимого примитивного полинома, использовавшегося при формировании исходной ЛРП. Каждая мультипликативная группа связана с одним из четырех вариантов сопровождающих матриц исходного полинома. Кроме того, при выборе первообразного элемента любой такой группы можно получить $p^m - 1$ матриц-циркулянтов исходной ЛРП, циклически сдвинутых друг относительно друга. В этой работе подробно рассмотрены только две мультипликативные группы – на основе матриц $\boldsymbol{H}_1$ и $\boldsymbol{H}_2$ (см. (2)).

Показано, что матрица-циркулянт ЛРП, сформированная на основе $\boldsymbol{H}_2$, всегда является упорядоченной, то есть каждая последующая строка в ней циклически сдвинута на один символ относительно предыдущей строки. Кроме того, у этой матрицы строки и столбцы с одинаковыми номерами совпадают. В зависимости от выбора первообразного элемента мультипликативной группы, связанной с $\boldsymbol{H}_2$, можно получить $p^m - 1$ вариантов таких матриц, получающихся одна из другой путем циклических перестановок строк или столбцов. Перестановка столбцов любой такой матрицы по возрастанию значений элементов мультипликативной группы поля Галуа, связанной с $\boldsymbol{H}_2$, начиная с первообразного элемента поля, соответствующего данной матрице, при последующей перестановке ее строк по возрастанию элементов мультипликативной группы, связанной с $\boldsymbol{H}_1$, начиная с первообразного элемента $\begin{bmatrix}1 & 0 & \dots & 0\end{bmatrix}$, приводит данную матрицу к матрице, состоящей из степеней W матрицы функций Виленкина-Крестенсона, упорядоченной по Кронекеру, без строки и столбца с номером ноль. Таким образом, все вышеописанные системы ортогональных сигнатур размерности p^m, построенные на основе всех возможных неприводимых примитивных полиномов m-ой степени с коэффициентами, принадлежащими множеству $\{0,\dots,(p-1)\}$, приводятся к одной и той же системе функций Виленкина-Крестенсона размерности p^m, упорядоченной по Кронекеру. В результате этого, при использовании любой систему ортогональных сигнатур в качестве набора поднесущих для передачи потока канальных информационных символов по радиоканалу, для выделения последних в приемнике целесообразно использовать обобщенное быстрое преобразование Фурье (БПФ) в базисе функций Виленкина-Крестенсона. Учитывая, что каждый передаваемый информационный символ связан с определенной строкой системы сигнатур, выбранной на передающей стороне, при их обработке получаем уникальный способ перемежения информационных символов, определяющийся структурами мультипликативных групп, связанных как с $\boldsymbol{H}_1$, так и с $\boldsymbol{H}_2$, а также выбором первообразного элемента группы, связанной с $\boldsymbol{H}_2$.

В работе впервые введены в рассмотрение циркулярные авто- и взаимно корреляционные матрицы систем ортогональных сигнатур, построенных на основе многопозиционных ЛРП и исследованы их свойства. Полученные результаты позволили разработать новый способ подавления взаимных помех при использовании для передачи потока канальных информационных символов в общем радиоканале сразу нескольких систем ортогональных сигнатур, что позволяет повысить пропускную способность канала связи пропорционально числу одновременно использующихся ортогональных систем при сравнительно низкой вычислительной сложности алгоритма подавления взаимных помех из-за использования обобщенного БПФ.

В этой работе не рассмотрен способ построения физического радиоканала при компоновке канальных информационных сигналов, сформированных на основе модулированных систем ортогональных сигнатур, с синхросигналом. Вариант такой компоновки очевиден – передача длинного синхросигнала с помощью строк с номером ноль всех последовательно излучаемых систем сигнатур. С такой структурой физического канала связан и очевидный способ обработки многолучевых сигналов, который так же не рассматривается в этой статье.

Литература

1. *Beard C., Stallings W.* Wireless Communication Networks and Systems. L.: Pearson, 2016.

2. *Middlestead R.W.* Digital Communications with Emphasis on Data Modems. Theory, Analysis, Design, Simulation, Testing and Applications. Lesly (USA): Wiley, 2017.

3. *Maral G., Bousquet M., Sun Z.* Satellite Communications Systems. United Kingdom: Wiley, 2020.

4. *Ипатов В.П.* Широкополосные системы и кодовое разделение сигналов. М: Мир связи, 2007.

5. *Бакулин М.Г., Бен Режеб Т.Б.К., Крейнделин В.Б.* и др. Неортогональный множественный доступ (NOMA) как основа систем связи 5G и 6G М.: Горячая линия – Телеком. 2024. 264 с.

6. *Горгадзе С.Ф.* Обнаружение-различение адресных сложных сигналов с использованием быстрых спектральных преобразований при многостанционном доступе с кодовым разделением // Радиотехника и электроника. 2006. Т. 51. № 4. С. 428-436.

7. *Gorgadze S.F., Boikov V.V.* Test Signals with Multilevel Subcarriers as Applied to Satellite Radio-Navigation Systems// Journal of Communications Technology and Electronics. 2014. V. 59. № 3, pp. 245-258.

8. *Gorgadze S.F.* Composite Spread Spectrum Signals with Uniform Amplitude Envelope for Satellite Radio-Navigation Systems // Journal of Communications Technology and Electronics. 2017. Vol. 62. № 4, pp. 346-359.

9. *Be'ery Y., Snyders J.* Optimal soft dicision block decoders based on Fast Hadamard Transform // IEEE Trans. Inform. Theory, vol. IT-32, pp. 355-364, 1986.

10. *Be'ery Y., Snyders J.* A recursive Hadamard transform optimal soft decoding algorithm. // Journal algebraic discrete methods. 1987. Vol.8. No. 4, pp. 778-789.

11. *Li Ping W.K., Leung K.Y.* A simple approach to near-optimal multiuser detection: interleave-division multiple-access // IEEE Trans. 2003. V. IT-49. № 12. P. 3213.

12. *Трахтман А.М., Трахтман В.*А. Основы теории дискретных сигналов на конечных интервалах. М.: Сов. радио, 1975.

13. *Горгадзе С.Ф.* Асимметричные модификации обобщенного быстрого преобразования Фурье и Фурье-Адамара // Радиотехника и электроника. 2005. Т. 50. № 3. С. 302-308.

14. *Смольянинов В.М., Назаров Л.Е.* Оптимизация алгоритма спектрального анализа при распознавании дискретных мультипликативных сигналов // Радиотехника и электроника. 1989. Т.35. №12. С. 2651-2653.

15. *Канатова Л.В., Литвинов В.Л., Финк Л.М.* Быстрое корреляционное декодирование p-ичных кодов максимальной длины // Проблемы передачи информации. 1986. Т. 22. № 2. С. 98.

16. *Madhow U., Honig M.L.* MMSE interference suppression for direct sequence spread spectrum CDMA // IEEE Trans. Commun. 1994. Vol. 42, pp. 3178-3188.

17. *Смирнов Н.И., Горгадзе С.Ф.* Сравнение характеристик спектров различных типов шумоподобных сигналов // Радиотехника. 1990. № 6. С. 6.

18. *Wang X., Poor V.H.* Wireless Communication Systems. Advanced Techniques for Signal Reception. Prentice-Hall. Upper Saddle River. NJ.2004.

19. *Honig M., Tatsanis M.K.* Adaptive techniques for multiuser CDMA receivers // IEEE Signal Process. Magazine.2000. Vol. 17, pp. 49-61.

20. *Бакулин М.Г., Крейнделин В.Б., Панкратов Д.Ю.* Технологии в системах радиосвязи на пути к 5G. М.: Горячая линия – Телеком, 2018. 240 с.

21. *Castoldi P.* Multiuser Detection in CDMA Mobile Terminals. London. Artech House. 2002. 227 с.

22. *Duel-Hallen A., Holtzman J., Zvonar Z.* Multiuser Detection for CDMA systems // IEEE Personal Communications.1995. April, pp. 46-58.

23. *Крейнделин В.Б., Панкратов Д.Ю.* Линейные алгоритмы многопользовательского детектирования// Электросвязь. 2002. №11. С. 31-33.

24. *Горгадзе С.Ф., Ву Ши.Д., Ермакова А.В.* Синхронизация М-последовательностей на основе быстрого преобразования Адамара // Радиотехника и электроника. 2024. Т. 69. № 2. С. 122-136.

25. *Горгадзе С.Ф., Ву Ши.Д., Ермакова А.В.* Синхронизация последовательностей Голда на основе быстрого преобразования в усеченном базисе функций Уолша-Адамара // Радиотехника и электроника. 2024. Т. 69. № 2. С. 137-145.

26. *Лосев В.В., Бродская Е.Б., Коржик В.И.* Поиск и декодирование сложных дискретных сигналов / Под ред. В.И.Коржика. М.: Радио и связь. 1988.

27. Свердлик М.Б. Оптимальные дискретные сигналы. М.: Сов. радио. 1975.

28. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. М.: Мир. 1976.

29. *Gold R.* Optimal Binary Sequences for Spread Spectrum Multiplexing // IEEE Trans. on Information Theory. 1967. Vol. IT-13, № 4, pp. 619-621. DOI: 10.1109/TIT.1967.1054048

30. *Кузнецов В.С., Шевченко И.В., Волков А.С., Солодков А.В.* Генерация ансамблей кодов Голда для систем прямого расширения спектра // Труды МАИ. 2017. № 96. С. 17-17.

31. *Кузнецов В.С., Мордасов К.А.* Быстрое декодирование на основе пассивной согласованной фильтрации длинных псевдослучайных кодов // Известия высших учебных заведений. Электроника. 2010. №1 (81). С. 57.

32. *Kudryashova A.Y.* A method of efficient coding of color images under the condition of permissible and forbidden values of color gamut // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 6. С. 65-70. EDN: VSDJGJ

MULTI-STATION ACCESS BASED ON CIRCULAR MATRICES OF MULTI-POSITION LINEAR RECURRENCE SEQUENCES

Svetlana F. Gorgadze, *Moscow Technical University for Communication and Informatics, Moscow, Russia,* **s.f.gorgadze@mtuci.ru**
Anastasia V. Ermakova, *Moscow Technical University for Communication and Informatics, Moscow, Russia,* **msikisylia@gmail.com**
Anastasia Yu. Kudryashova, *Moscow Technical University for Communication and Informatics, Moscow, Russia*

Abstract
Variants of the construction of orthogonal signature systems based on circular matrices of multiposition linear recurrence sequences of maximum period are developed. It is shown that any matrix of this class is reduced to the matrix of Vilenkin-Krestenson functions by means of a unique linear operator whose basis is the permutation of rows and columns of the circular matrix by increasing values of the elements of the multiplicative group of the extended Galois field modulo an irreducible primitive polynomial used in the formation of the initial sequence. It is established that the transmission in a radio channel of a stream of information symbols on the basis of any system of the above signatures and the fast processing of the resulting signal in the receiver on the basis of the generalised fast Fourier transform on the basis of the Vilenkin-Krestenson functions are associated with several variants of the interleaving of the transmitted information symbols. It is shown that the use of several different systems of developed orthogonal signatures for simultaneous information transmission in combination with a fast algorithm for compensation of their mutual interference on the basis of generalised fast Fourier transform in the basis of Vilenkin-Krestenson functions allows to increase the bandwidth of the communication channel in the number of times equal to the number of simultaneously used systems in comparison with the method of information transmission on the basis of one system of orthogonal functions and to fully compensate mutual interference. The new method of mutual interference compensation is a result of previously unknown properties of the systems of pro-posed orthogonal signals revealed in this work. This increase in link capacity is made possible by common interference compensation.

Keywords: *discrete orthogonal signal systems, Vilen-Kin-Krestenson functions, discrete exponential functions, Walsh-Adamar systems, generalised fast Fourier transform, orthogonal and non-orthogonal subcarriers, mutual interference compensation*

References

[1] C. Beard, W. Stallings, "Wireless Communication Networks and Systems," L.: Pear-son, 2016.
[2] R.W. Middlestead, "Digital Communications with Emphasis on Data Modems. Theory, Analysis, Design, Simulation, Testing and Applications," Lesly (USA): Wiley, 2017.
[3] G. Maral, M. Bousquet, Z. Sun, "Satellite Communications Systems," United Kingdom: Wiley, 2020.
[4] V.P. Ipatov, "Broadband Systems and Code Division of Signals," Moscow: Mir svyaz, 2007.
[5] M.G. Bakulin, "Non-orthogonal multiple access (NOMA) as a basis of 5G and 6G communication systems," Moscow: Hotline – Telecom. 2024. 264 p.
[6] S.F. Gorgadze, "Detection-discrimination of address complex signals with the use of fast spectral transformations at multistation access with code division," *Radio engineering and electronics*. 2006. Vol. 51. No. 4, pp. 428-436.
[7] S.F. Gorgadze, V.V. Boikov, "Test Signals with Multilevel Subcarriers as Applied to Satellite Radio-Navigation Systems," *Journal of Communications Technology and Electronics*. 2014. Vol. 59. No. 3, pp. 245-258.
[8] S.F. Gorgadze, "Composite Spread Spectrum Signals with Uniform Amplitude En-velope for Satellite Radio-Navigation Systems," *Journal of Communications Tech-nology and Electronics*. 2017. Vol. 62. No. 4, pp. 346-359.
[9] Y. Be'ery, J. Snyders, "Optimal soft dicision block decoders based on Fast Hada-mard Transform," *IEEE Trans. Inform. Theory*. Vol. IT-32, pp. 355-364, 1986.
[10] Y. Be'ery, J. Snyders, "A recursive Hadamard transform optimal soft decoding al-gorithm," *Journal algebraic discrete methods*. 1987. Vol. 8. No.4, pp. 778-789.
[11] W.K. Li Ping, K.Y.Leung, "A simple approach to near-optimal multiuser detection: interleave-division multiple-access," *IEEE Trans*. 2003. Vol. IT-49. No. 12. P. 3213.
[12] A.M. Trakhtman, V.A. Trakhtman, "Fundamentals of the Theory of Discrete Signals on Konechnoi Intervals," Moscow: Sov. radio. 1975.
[13] S.F. Gorgadze, "Asymmetric modifications of the generalised fast Fourier and Fourier-Adamar transformation," *Radiotekhnika i elektronika*. 2005. Vol. 50. No. 3, pp. 302-308.
[14] V.M. Smolyaninov, L.E. Nazarov, "Optimisation of the spectral analysis algorithm for discrete multiplicative signals recognition," *Radio engi-neering and electronics.* 1989. Vol. 35. No.12, pp. 2651-2653.
[15] L.V. Kanatova, V.L. Litvinov, L.M. Fink, "Fast correlation decoding of p-ic codes of the maximum length," *Problems of information transfer*. 1986. Vol. 22. No. 2. P. 98.

[16] U. Madhow, M.L. Honig, "MMSE interference suppression for direct sequence spread spectrum CDMA," *IEEE Trans. Commun.* 1994. Vol. 42, pp. 3178-3188.
[17] N.I. Smirnov, S.F. Gorgadze, "Comparison of characteristics of spectra of different types of noise-like signals," *Radiotekhnika*. 1990. No. 6. P. 6.
[18] X. Wang, V.H. Poor, "Wireless Communication Systems. Advanced Techniques for Signal Reception," Prentice-Hall. Upper Saddle River. NJ.2004.
[19] M. Honig, M.K. Tatsanis, "Adaptive techniques for multiuser CDMA receivers," *IEEE Signal Process. Magazine*. 2000. Vol. 17, pp. 49-61.
[20] M.G. Bakulin, V.B. Kreindelin, D.Yu. Pankratov, "Technologies in radio communication systems on the way to 5G," Moscow: Hotline – Telecom. 2018. 240 p.
[21] P. Castoldi, "Multiuser Detection in CDMA Mobile Terminals," London. Artech House. 2002. 227 p.
[22] A. Duel-Hallen, J. Holtzman, Z. Zvonar, "Multiuser Detection for CDMA systems," *IEEE Personal Communications*.1995. April, pp. 46-58.
[23] V.B. Kreindelin, D.Yu. Pankratov, "Linear algorithms of multiuser detection," *Elektrosvyaz*. 2002. No.11, pp. 31-33.
[24] S.F. Gorgadze, Wu Shi. D., A.V. Ermakova, "Synchronisation of M-sequences on the basis of a fast Adamar transformation," *Radio engineering and electronics*. 2024. Vol. 69. No. 2, pp. 122-136.
[25] S.F. Gorgadze, Wu Shi. D., A.V. Ermakova, "Synchronisation of the Gold sequences on the basis of a fast transformation in the truncated basis of the Walsh-Adamar functions," *Radiotekhnika i elektronika*. 2024. Vol. 69. No. 2, pp. 137-145.
[26] V.V. Losev, E.B. Brodskaya, V.I. Korzhik, "Search and decoding of the complex discrete signals," Edited by V.I.Korzhik. Moscow: Radio and Communication. 1988.
[27] M.B. Sverdlik, "Optimal discrete signals," Moscow: Sov. radio. 1975.
[28] W. Peterson, E. Weldon, "Error-correcting codes," Moscow: Mir. 1976.
[29] R. Gold, "Optimal Binary Sequences for Spread Spectrum Multiplexing," *IEEE Trans. on Information Theory*. 1967. Vol. IT-13. No. 4, pp. 619-621. DOI: 10.1109/TIT.1967.1054048
[30] V.S. Kuznetsov, I.V. Shevchenko, A.S. Volkov, A.V. Solodkov, "Generation of an ensemble of Gold codes for direct spectrum expansion systems," Proc. of MAI. 2017. No. 96, pp. 17-17.
[31] V.S. Kuznetsov, K.A.Mordasov, "Fast decoding on the basis of the passive coordinated filtering of the long pseudo-random codes," *Izvestiya vysshe-educational institutions. Electronics*. 2010. No.1 (81). P. 57.
[32] A.Y. Kudryashova, "A method of efficient coding of color images under the condition of permissible and forbidden values of color gamut," *T-Comm*. 2019. Vol. 13. No. 6, pp. 65-70.