РАДИОТЕХНИКА И ЭЛЕКТРОНИКА, 2024, том 69, № 2, с. 122–136

ТЕОРИЯ И МЕТОДЫ ОБРАБОТКИ СИГНАЛОВ

УДК 621.396;621.59; 519.725

СИНХРОНИЗАЦИЯ М-ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ БЫСТРОГО ПРЕОБРАЗОВАНИЯ АДАМАРА

© 2024 г. С. Ф. Горгадзе*, Д. Ву Ши, А. В. Ермакова

Московский технический университет связи и информатики (МТУСИ), ул. Авиамоторная, 8а, Москва, 111024 Российская Федерация

**E-mail: s.f.gorgadze@mtuci.ru*

Поступила в редакцию 19.10.2022 г.
После доработки 18.07.2023 г.
Принята к публикации 27.07.2023 г.

Разработаны варианты построения матриц-циркулянтов любой М-последовательности (МП) на основе автоморфных мультипликативных групп расширенного поля Галуа, построенного при помощи неприводимого примитивного полинома, на основе которого сформирована исходная МП. Результатом данного подхода являются выявленные новые способы преобразования матриц-циркулянтов МП к матрице функций Уолша, упорядоченной по степеням первообразного элемента поля. Впервые показано, что в зависимости от начальных условий преобразования совокупность любого числа любых циклических сдвигов МП, сдвинутых друг относительно друга на один символ, может быть преобразована к любым строкам упорядоченной матрицы функций Уолша, следующим друг за другом. Данное обстоятельство позволяет упростить алгоритм синхронизации МП при известном диапазоне ее циклических сдвигов, особенно в случае больших периодов ее повторения, а также снизить вычислительную сложность алгоритма обработки при работе в усеченном базисе функций Уолша–Адамара.

Ключевые слова. М-последовательности, матрица-циркулянт, матрица функций Уолша, шумоподобные сложные сигналы, мультипликативные группы поля Галуа, быстрое преобразование Адамара.

DOI: 10.31857/S0033849424020031, **EDN:** KMXKJN

ВВЕДЕНИЕ

В настоящее время М-последовательности (МП) используются для формирования периодических шумоподобных сложных сигналов (СлС), применяемых в различных наземных и спутниковых радиосистемах [1–10]. На основе обработки таких СлС могут решаться задачи синхронизации по времени и частоте в каналах передачи информации [1, 11–13], позиционирования в системах радионавигации [3–5, 14], суммирования сигналов при их многолучевом распространении или излучении разнесенными ретрансляторами, включая спутниковые [1, 2, 5, 12, 15], выявления всех наземных станций, использующих спутниковую группировку, с целью контроля частотного ресурса [6, 7] и т.д. Во всех вышеперечисленных случаях ключевым этапом обработки СлС является синхронизация МП на основе многократного выполнения операции ее дискретной свертки на длительности времени одного, многих периодов ее повторения, либо ее сегмента значительной длины, порядка $2^9 \ldots 2^{17}$ и более [1, 3, 6, 16–18]. Это объясняется как требованиями к разрешающей способности при обнаружении-различении совокупности шумоподобных СлС, рассогласованных по частоте и временной задержке [7, 15], так и, как правило, низким отношением сигнал/помеха на входе приемника, когда помеха может превосходить полезный сигнал по мощности в сотни, тысячи, или десятки тысяч раз [6]. При этом ограничение по длительности времени обработки СлС в настоящее время связано только с высокой вычислительной сложностью алгоритма дискретной свертки соответствующих псевдослучайных последовательностей (ПСП), поскольку проблема нестабильности тактовых генераторов последних решается при повторной дискретизации входного СлС со сдвигом по времени на половину длительности его элементарного импульса [13, 19, 20], а нестабильность его несущей частоты приводит лишь к необходимости многократ-

ных повторных вычислений дискретной свертки ПСП [8, 19].

Значительные успехи в области использования быстрых спектральных преобразований в базисе функций Виленкина–Крестенсона и, в частности, Уолша–Адамара, при обработке дискретных сигналов были достигнуты в работах [4, 14, 21–28]. В [21] впервые предложены групповые дискретные мультипликативные сигналы, выявлена их связь с групповыми кодами и показано, что в основе оптимального правила их распознавания лежит спектральный анализ, при реализации которого можно использовать быстрые спектральные преобразования. В работах [22–27] развиты методы использования этих преобразований в теории помехоустойчивого кодирования. Применительно к задаче декодирования p-ичных кодов максимальной длины использование быстрых спектральных преобразований в дискретном базисе функций Виленкина–Крестенсона рассматривалось в работе [28], а непосредственно для синхронизации псевдослучайных кодов, в том числе и МП, в работах [4, 6, 14].

Также в [4] указывается на взаимосвязь задач поиска (синхронизации) СлС при их обработке в приемнике и декодирования блоковых кодов, построенных на основе циклических сдвигов их слов. В данной работе рассматривается задача синхронизации МП, чтобы подчеркнуть взаимосвязь решаемой задачи с синхронизацией периодического СлС при его обработке в приемнике. Под синхронизацией МП понимается определение ее циклического сдвига, начиная с момента начала наблюдения СлС, на основе которой он сформирован. Вопросы, связанные с выделением МП из этого СлС, не рассматриваются.

При быстром декодировании кода на основе быстрых спектральных преобразований необходимо знать способ преобразования его слов к дискретным функциям Виленкина–Крестенсона или, при использовании двоичных кодов, – к функциям Уолша [21]. В случае решения задачи синхронизации кода любой его циклический сдвиг должен преобразовываться к этим функциям [4, 14]. Но в [4, 6, 14, 28] не выявлено многообразие вариантов преобразования циклических сдвигов МП к дискретным функциями Уолша, вызванное как разнообразием мультипликативных групп расширенного поля Галуа, так и использованием их циклических сдвигов при таком приведении. Знание о таком многообразии делает алгоритм синхронизации МП более гибким и позволяет снизить его вычислительную сложность в определенных ситуациях, на которые указывается в данной статье. Кроме того, при решении задачи синхронизации МП с большими периодами повторения важное значение приобретает способ выявления соответствия номеров строк матрицы Уолша–Адамара и начальных блоков циклических сдвигов МП, т.е. в матричной интерпретации данной задачи – строкам матрицы-циркулянта МП, которая может быть построена разными способами, что не рассматривается в этих работах.

Цель данной работы – исследование вариантов построения матриц-циркулянтов МП на основе мультипликативных групп расширенного поля Галуа по модулю неприводимого примитивного полинома, а также вариантов приведения этих матриц к полной или усеченной матрице Адамара для разработки ускоренных алгоритмов синхронизации МП при обработке шумоподобных сложных сигналов.

1. ПОСТРОЕНИЕ МАТРИЦ-ЦИРКУЛЯНТОВ МП НА ОСНОВЕ МУЛЬТИПЛИКАТИВНЫХ ГРУПП ПОЛЯ ГАЛУА

Представим любую МП с элементами (0,1), сформированную на основе неприводимого примитивного полинома $f_m(x)$, в виде вектора-строки

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

где $i = 0,\ldots,m-1$ – номер циклического сдвига МП на $l_i \in \{0,1\ldots,N-1\}$ символов относительно МП ${}^{n}_{0}\mathfrak{I}_0$ с условно нулевым циклическим сдвигом, $N = 2^m - 1$ – длина (период) МП, m – порядок $f_m(x)$, n – номер выбранного способа упорядочения МП по их циклическим сдвигам [1, 29–32].

Как известно, можно выбрать такой способ упорядочения любых m МП, описанных выше, при котором столбцы

$$ \alpha^k = \left[x_{i,k},\ i = 0,\ldots,m-1 \right]^T, k = 0,\ldots,N-1, $$

образуют мультипликативную группу расширенного поля Галуа $GF\left(2^m\right)$ построенного по модулю $f_m(x)$, где k – номер элемента группы, $[\cdot]^T$ – обозначение транспонированной матрицы [21, 29, 30]. Такая группа имеет циклическую структуру и состоит из максимально возможного числа N несовпадающих ненулевых элементов,

являющихся степенями первообразного элемента $\boldsymbol{\alpha}^0$ поля, причем $\boldsymbol{\alpha}^k = \mathbf{H}_n\boldsymbol{\alpha}^{k-1}$, где $\mathbf{H}_n$ – сопровождающая матрица $f_m(x)$ [30]. Обычно рассматривают четыре типа таких матриц [28]:

$$\mathbf{H}_1 = \begin{bmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & 0 & a_{m-2} \\ 0 & 0 & \cdots & 1 & a_{m-1} \end{bmatrix},$$

$$\mathbf{H}_2 = \begin{bmatrix} 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & 0 & 1 \\ a_0 & a_1 & \cdots & a_{m-2} & a_{m-1} \end{bmatrix}, \quad (1)$$

$$\mathbf{H}_3 = \begin{bmatrix} a_{m-1} & 1 & \cdots & 0 & 0 \\ a_{m-2} & 0 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_1 & 0 & \cdots & 0 & 1 \\ a_0 & 0 & \cdots & 0 & 0 \end{bmatrix},$$

$$\mathbf{H}_4 = \begin{bmatrix} a_{m-1} & a_{m-2} & \cdots & a_1 & a_0 \\ 1 & 0 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 1 & \mathbf{0} \end{bmatrix},$$

где $a_0, a_1, \ldots, a_{m-2}, a_{m-1}$ – коэффициенты полинома $f_m(x)$, принадлежащие множеству $\{0, 1\}$; таким образом, размерность этих матриц будет $m \times m$. Важным является свойство цикличности группы, т.е. $\boldsymbol{\alpha}^0 = \boldsymbol{\alpha}^N$, $\boldsymbol{\alpha}^1 = \boldsymbol{\alpha}^{N+1}, \ldots$ Кроме того, в качестве $\boldsymbol{\alpha}^0$ можно выбрать любой ее элемент. Таким образом, m циклических сдвигов МП на l_i ее символов относительно ${}_0^n\mathfrak{J}_0$ с некоторым сдвигом, условно считающимся нулевым ($l_0 = 0$), можно представить в виде матрицы:

$$\mathfrak{J}_{m,n} = \begin{bmatrix} {}_0^n\mathfrak{J}_0 \\ {}_{l_1}^n\mathfrak{J}_1 \\ \cdots \\ {}_{l_{m-1}}^n\mathfrak{J}_{m-1} \end{bmatrix} = \begin{bmatrix} \boldsymbol{\alpha}^0 & \boldsymbol{\alpha}^1 & \cdots & \boldsymbol{\alpha}^{N-1} \end{bmatrix}, \quad (2)$$

$$\boldsymbol{\alpha}^k = \mathbf{H}_n\boldsymbol{\alpha}^{k-1}.$$

где столбцы $\boldsymbol{\alpha}^k$ могут быть получены любым из возможных способов, т.е. при выборе матрицы $\mathbf{H}_n$, что определяет значения циклических сдвигов МП l_i $(i = 0, \ldots, m-1)$ относительно МП ${}_0^n\mathfrak{J}_0$ при выбранном $\boldsymbol{\alpha}^0$. В качестве примера в табл. 1 приведены значения элементов четырех максимальных мультипликативных групп поля Галуа, полученных на основе полинома $f_5(x) = x^5 + x^3 + 1$ и представленных в десятичной системе счисления. Такое их представление в дальнейшем обозначаем как $\left[\boldsymbol{\alpha}^k\right]_{10}$. Был выбран первообразный элемент $\alpha^0 = [1\ 0\ 0\ 0\ 0]^m$, так что во всех случаях $\left[\boldsymbol{\alpha}^0\right]_{10} = 16$.

Таблица 1. Максимальные мультипликативные группы поля Галуа по модулю полинома $f_5(x) = x^5 + x^3 + 1$

k	H_1	H_2	H_3	H_4
0	16	16	16	16
1	8	1	1	8
2	4	2	18	20
3	2	5	13	10
4	1	10	26	21
5	18	21	29	26
6	9	11	19	29
7	22	23	15	14
8	11	14	30	23
9	23	29	21	27
10	25	27	3	13
11	30	22	6	6
12	15	24	12	3
13	21	17	24	17
14	24	3	25	24
15	12	7	27	28
16	6	6	31	30
17	3	15	23	31
18	19	31	7	15
19	27	30	14	7
20	31	28	28	19
21	29	25	17	25
22	28	19	11	12
23	14	6	22	22
24	7	13	5	11
25	17	26	10	5
26	26	20	20	18
27	13	9	1	9
28	20	18	2	4
29	10	4	4	2
30	5	8	8	1

Таким образом, например, для матрицы $\mathbf{H}_1$ элементы мультипликативной группы поля Галуа можно вычислить по формуле

$$\boldsymbol{\alpha}^{k+1} = \begin{bmatrix} x_{0,k+1} \\ x_{1,k+1} \\ \cdots \\ x_{m-1,k+1} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & 0 & a_{m-2} \\ 0 & 0 & \cdots & 1 & a_{m-1} \end{bmatrix} \begin{bmatrix} x_{0,k} \\ x_{1,k} \\ \cdots \\ x_{m-2} \\ x_{m-1} \end{bmatrix}, \quad (3)$$

$$k = 0,\ldots,N-1,$$

причем m циклических сдвигов порождаемой МП (т.е. на l_0, l_1,..., l_{m-1} символов относительно ${}^{1}_{0}\mathfrak{I}_0$) располагаются в строках матрицы $\mathfrak{I}_{m,1}$ [30], соответствующей $\mathbf{H}_1$:

$$\mathfrak{I}_{m,1} = \begin{bmatrix} x_{0,0} & x_{0,1} & \cdots & x_{0,N-1} \\ x_{1,0} & x_{1,1} & \cdots & x_{1,N-1} \\ \cdot & \cdot & \cdot & \cdot \\ x_{m-1,0} & x_{m-1,1} & \cdots & x_{m-1,N-1} \end{bmatrix}. \quad (4)$$

Ее столбцы представляют собой элементы мультипликативной группы поля Галуа по модулю $f_m(x)$ с коэффициентами $a_0, a_1, \ldots, a_{m-2}, a_{m-1}$.

В качестве примера в табл. 2 приводятся элементы матрицы $\mathfrak{I}_{5,1}$ для полинома $f_5(x) = x^5 + x^4 + x^2 + x + 1$, а в табл. 3 – для двойственного полинома $f_5(x) = x^5 + x^4 + x^3 + x + 1$.

Матрицу-циркулянт МП $\mathfrak{I}_{m,n,ц}$ с элементами (0,1), содержащую ее циклические сдвиги на $l_0, l_1, \ldots, l_{m-1}$ символов, а также все остальные сдвиги, не совпадающие с ними, сформируем в соответствии с правилом

$$\mathfrak{I}_{m,n,ц} = \begin{bmatrix} \mathfrak{I}_{m,n} \\ \mathbf{H}_n{}^{m}\mathfrak{I}_{m,n} \\ \mathbf{H}_n{}^{2m}\mathfrak{I}_{m,n} \\ \cdots \\ \mathbf{H}_n{}^{C(N)m}\mathfrak{I}_{m,n} \end{bmatrix}, \quad (5)$$

где $C(N) = \left(\frac{A(N)}{m}\right) - 1$, $A(N)$ – число, максимально близкое к N, делящееся нацело на m и удовлетворяющее неравенству $A(N) > N$. Таким образом, $\frac{A(N)}{m}$ – это общее число бло-

Таблица 2. Элементы мультипликативной группы поля Галуа на основе сопровождающей матрицы $\mathbf{H}_1$ полинома $f_5(x) = x^5 + x^4 + x^2 + x + 1$

Элементы группы	k																														
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
	$[\alpha^k]_{10}$																														
	16	8	4	2	1	27	22	11	30	15	28	14	7	24	12	6	3	26	13	29	21	17	19	18	9	31	20	10	5	25	23
$x_{0,k}$	1	0	0	0	1	1	1	0	1	0	1	0	0	1	0	0	0	1	0	1	1	1	1	1	0	1	1	0	0	1	1
$x_{1,k}$	0	1	0	0	0	1	0	1	1	1	1	1	0	1	1	0	0	1	1	1	0	0	0	0	1	1	0	1	0	1	0
$x_{2,k}$	0	0	1	0	0	0	1	0	1	1	1	1	1	0	1	1	0	0	1	1	1	0	0	0	0	1	1	0	1	0	1
$x_{3,k}$	0	0	0	1	0	1	1	1	1	1	0	1	1	0	0	1	1	1	0	0	0	0	1	1	0	1	0	1	0	0	1
$x_{4,k}$	0	0	0	0	1	1	0	1	0	1	0	0	1	0	0	0	1	0	1	1	1	1	1	0	1	1	0	0	1	1	1

Таблица 3. Элементы мультипликативной группы поля Галуа на основе сопровождающей матрицы $\mathbf{H}_1$ полинома $f_5(x) = x^5 + x^4 + x^3 + x + 1$

Элементы группы	k																														
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
	$[\alpha^k]_{10}$																														
	16	8	4	2	1	27	22	11	30	15	28	14	7	24	12	6	3	26	13	29	21	17	19	18	9	31	20	10	5	25	23
$x_{0,k}$	1	0	0	0	1	1	1	0	1	0	1	0	0	1	0	0	0	1	0	1	1	1	1	1	0	1	1	0	0	1	1
$x_{1,k}$	0	1	0	0	0	1	0	1	1	1	1	1	0	1	1	0	0	1	1	1	0	0	0	0	1	1	0	1	0	1	0
$x_{2,k}$	0	0	1	0	0	0	1	0	1	1	1	1	1	0	1	1	0	0	1	1	1	0	0	0	0	1	1	0	1	0	1
$x_{3,k}$	0	0	0	1	0	1	1	1	1	1	0	1	1	0	0	1	1	1	0	0	0	0	1	1	0	1	0	1	0	0	1
$x_{4,k}$	0	0	0	0	1	1	0	1	0	1	0	0	1	0	0	0	1	0	1	1	1	1	1	0	1	1	0	0	1	1	1

ков в матрице $\mathfrak{I}_{m,n,ц}$, содержащих матрицу $\mathfrak{I}_{m,n}$ или ее преобразование вида $\mathbf{H}_n{}^x\mathfrak{I}_{m,n}$. Размерность каждого блока составит $m\times(N-1)$. Таким образом, размерность матрицы $\mathfrak{I}_{m,n,ц}$ будет $A(N)\times(N-1)$, в результате чего последний блок $\mathfrak{I}_{m,n,ц}$ в своих $A(N)-N$ строках будет содержать МП, циклические сдвиги которых совпадают со сдвигами МП первого блока.

В качестве примера элементы $\mathfrak{I}_{5,1,ц}$, сформированной на основе $f_5(x)=x^5+x^3+1$ и $\mathbf{H}_1$, приведены в табл. 4. Из анализа данных табл. 4 следует, что последовательность $l_0,l_1,\ldots,l_{34}$, расположенная в последнем столбце, выглядит случайной, хотя второй блок $\mathfrak{I}_{5,1,ц}$ из $m=5$ ее строк сдвинут относительно первого блока из такого же количества строк на пять символов МП, третий блок сдвинут относительно него на десять символов и т.д. Кроме того, столбцы $\mathfrak{I}_{5,1,ц}$ не являются МП.

Совершенно другую структуру имеет $\mathfrak{I}_{5,2,ц}$, сформированная на основе того же полинома $f_5(x)=x^5+x^3+1$ и $\mathbf{H}_2$ и приведенная в табл. 5, поскольку в ее строках располагаются циклические сдвиги МП, смещенные вправо на один символ друг относительно друга. Кроме того, в ее столбцах содержатся циклические сдвиги той же МП, причем в каждом последующем столбце МП сдвинута циклически на один символ, по сравнению с предыдущим столбцом. Очевидно, что данное свойство характерно для всех $\mathfrak{I}_{m,2,ц}$, построенных на основе $\mathbf{H}_2$, и оно не свойственно $\mathfrak{I}_{m,1,ц}$, $\mathfrak{I}_{m,3,ц}$, $\mathfrak{I}_{m,4,ц}$, сформированным на основе $\mathbf{H}_1$, $\mathbf{H}_3$ и $\mathbf{H}_4$ соответственно. Будем называть все матрицы-циркулянты $\mathbf{H}_2$, упорядоченными по циклическим сдвигам или просто упорядоченными.

Важнейшим свойством упорядоченных матриц-циркулянтов является очевидная и простая взаимосвязь между номером их строки i и абсолютным циклическим сдвигом МП в этой строке, который определяется набором m ее символов:

$$\mathbf{H}_2{}^i\boldsymbol{\alpha}^0=\mathbf{b}_i, \tag{6}$$

где $\mathbf{b}_i=\left[x_{i,k},\ k=0,\ldots,m-1\right]$ – начальный блок МП, находящейся в i-й строке матрицы-циркулянта.

Другим важным свойством упорядоченной матрицы-циркулянта является циклический сдвиг последовательности элементов мультипликативных групп $\mathbf{H}_2{}^x\mathfrak{I}_{m,n}$ $(x=0,m,2m,\ldots)$ на один элемент вправо при выборе каждого следующего элемента группы в качестве первообразного, в результате чего существует N-вариантов этой матрицы. В любом из них в строках от i-й до $(i+m-1)$-й будут располагаться элементы мультипликативной группы поля Галуа, циклически сдвинутые на i символов относительно $\mathfrak{I}_{m,2}$, где i может принимать любое значение от 1 до $(N-1)$.

2. ПРЕОБРАЗОВАНИЕ МАТРИЦЫ-ЦИРКУЛЯНТА МП К МАТРИЦЕ, СОСТОЯЩЕЙ ИЗ ФУНКЦИЙ УОЛША

Переставим столбцы матрицы $\mathfrak{I}_{m,2,ц}$ при любом значении $\boldsymbol{\alpha}^0$ по возрастанию значений элементов мультипликативной группы поля Галуа $\left[\boldsymbol{\alpha}^k\right]_{10}$, сформированной на основе $\mathbf{H}_2$ при таком же значении $\boldsymbol{\alpha}^0$ [4, 14]. В результате $\mathfrak{I}_{m,2}$ будет преобразована в матрицу $\mathbf{R}_{ma}$, столбцы которой образуют так называемый простой двоичный код, а строки являются аналогами функций Радемахера [31] без нулевого символа при нумерации символов с нуля: $\mathbf{r}_{0a}$, $\mathbf{r},\ldots\mathbf{r}_{(m-1)a}$. Матрица $\mathbf{R}_{ma}=\left[\mathbf{r}_{0a}\,\mathbf{r}_{1a}\ldots\mathbf{r}_{(m-1)a}\right]^T$ при $m=5$ показана в табл. 6.

Тогда $\mathfrak{I}_{m,2,ц}$ преобразуется в матрицу

$$\mathbf{W}_{m,p(1,0)}=\begin{bmatrix}\mathbf{R}_{ma}\\ \mathbf{H}_2{}^m\mathbf{R}_{ma}\\ \mathbf{H}_2{}^{2m}\mathbf{R}_{ma}\\ \cdots\\ \mathbf{H}_2{}^{C(N)m}\mathbf{R}_{ma}\end{bmatrix}=\begin{bmatrix}\mathbf{I}_m\mathbf{R}_{ma}\\ \mathbf{H}_2{}^m\mathbf{R}_{ma}\\ \mathbf{H}_2{}^{2m}\mathbf{R}_{ma}\\ \cdots\\ \mathbf{H}_2{}^{C(N)m}\mathbf{R}_{ma}\end{bmatrix}=\begin{bmatrix}\mathbf{I}_m\\ \mathbf{H}_2{}^m\\ \mathbf{H}_2{}^{2m}\\ \cdots\\ \mathbf{H}_2{}^{C(N)m}\end{bmatrix}\mathbf{R}_{ma}, \tag{7}$$

где $\mathbf{W}_{m,p(1,0)}$ – расширенная матрица функций Уолша без нулевого символа с элементами (0,1), содержащая некоторое количество повторяющихся строк; $\mathbf{I}_m$ – единичная матрица размером $m\times m$. Строки матриц $\mathbf{H}_2{}^x\mathbf{R}_{ma}$ $(x=m,2m,\ldots)$ представляют собой комбинации сумм строк матрицы $\mathbf{R}_{ma}$ при сложении символов по модулю 2. Как известно, такие суммы образуют функции

Таблица 4. Матрица $\mathfrak{I}_{5,1,u}$, сформированная на основе $f_5(x) = x^5 + x^3 + 1$

Циклические сдвиги МП	k																															i	l_i
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30		
	$[\alpha^k]_{10}$																																
	16	8	4	2	1	18	9	22	11	23	25	30	15	21	24	12	6	3	19	27	31	29	28	14	7	17	26	13	20	10	5		
$x_{0,k}$	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	**0**	**0**
$x_{1,k}$	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	**1**	**30**
$x_{2,k}$	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	**2**	**29**
$x_{3,k}$	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	**3**	**2**
$x_{4,k}$	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	**4**	**1**
$x_{5,k}$	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	**5**	**5**
$x_{6,k}$	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	**6**	**4**
$x_{7,k}$	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	**7**	**3**
$x_{8,k}$	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	**8**	**7**
$x_{9,k}$	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	**9**	**6**
$x_{10,k}$	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	**10**	**10**
$x_{11,k}$	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	**11**	**9**
$x_{12,k}$	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	**12**	**8**
$x_{13,k}$	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	**13**	**12**
$x_{14,k}$	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	**14**	**11**
$x_{15,k}$	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	**15**	**15**
$x_{16,k}$	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	**16**	**14**
$x_{17,k}$	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	**17**	**13**
$x_{18,k}$	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	**18**	**17**
$x_{19,k}$	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	**19**	**16**
$x_{20,k}$	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	**20**	**20**
$x_{21,k}$	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	**21**	**19**
$x_{22,k}$	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	**22**	**18**
$x_{23,k}$	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	**23**	**22**
$x_{24,k}$	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	**24**	**21**
$x_{25,k}$	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	**25**	**25**
$x_{26,k}$	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	**26**	**24**
$x_{27,k}$	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	**27**	**23**
$x_{28,k}$	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	**28**	**27**
$x_{29,k}$	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	**29**	**26**
$x_{30,k}$	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	**30**	**30**
$x_{31,k}$	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	**31**	**29**
$x_{32,k}$	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	**32**	**28**
$x_{33,k}$	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	**33**	**1**
$x_{34,k}$	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	**34**	**0**

Таблица 5. Матрица $\mathfrak{I}_{5,2,u}$, сформированная на основе $f_5(x) = x^5 + x^3 + 1$

Циклические сдвиги МП	k																																i	l_i
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30			
	$[\alpha^k]_{10}$																																	
	16	1	2	5	10	21	11	23	14	29	27	22	12	24	17	3	7	15	31	30	28	25	19	6	13	26	20	9	18	4	8			
$x_{0,k}$	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	**0**	**0**
$x_{1,k}$	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	**1**	**1**
$x_{2,k}$	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	**2**	**2**
$x_{3,k}$	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	**3**	**3**
$x_{4,k}$	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	**4**	**4**
$x_{5,k}$	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	**5**	**5**
$x_{6,k}$	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	**6**	**6**
$x_{7,k}$	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	**7**	**7**
$x_{8,k}$	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	**8**	**8**
$x_{9,k}$	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	**9**	**9**
$x_{10,k}$	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	**10**	**10**
$x_{11,k}$	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	**11**	**11**
$x_{12,k}$	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	**12**	**12**
$x_{13,k}$	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	**13**	**13**
$x_{14,k}$	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	**14**	**14**
$x_{15,k}$	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	**15**	**15**
$x_{16,k}$	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	**16**	**16**
$x_{17,k}$	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	**17**	**17**
$x_{18,k}$	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	**18**	**18**
$x_{19,k}$	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	**19**	**19**
$x_{20,k}$	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	**20**	**20**
$x_{21,k}$	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	**21**	**21**
$x_{22,k}$	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	**22**	**22**
$x_{23,k}$	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	**23**	**23**
$x_{24,k}$	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	**24**	**24**
$x_{25,k}$	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	**25**	**25**
$x_{26,k}$	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	**26**	**26**
$x_{27,k}$	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	**27**	**27**
$x_{28,k}$	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	**28**	**28**
$x_{29,k}$	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	**29**	**29**
$x_{30,k}$	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	**30**	**30**
$x_{31,k}$	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	**31**	**0**
$x_{32,k}$	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	**32**	**1**
$x_{33,k}$	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	**33**	**2**
$x_{34,k}$	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	**34**	**3**

Таблица 6. Аналоги функций Радемахера при $m = 5$

Аналоги функций Радемахера	k																														
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
r_{0a}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
r_{1a}	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
r_{2a}	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
r_{3a}	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
r_{4a}	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Уолша без нулевых символов при нумерации символов с нуля. С целью выявления способа их упорядочения в (7) рассмотрим матрицу

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_2{}^{m} \\ \mathbf{H}_2{}^{2m} \\ \cdots \\ \mathbf{H}_2{}^{C(N)m} \end{bmatrix}. \tag{8}$$

Покажем, что ее строки образуют мультипликативную группу поля Галуа, сформированную на основе $\mathbf{H}_1$. Действительно,

$$\begin{aligned} \mathbf{H} &= \left(\mathbf{H}^{\boldsymbol{T}}\right)^{\boldsymbol{T}} = \\ &= \left[\left(\left(\mathbf{H}_2{}^{\boldsymbol{T}}\right)^{\boldsymbol{T}}\right)^{\boldsymbol{m}} \quad \left(\left(\mathbf{H}_2{}^{\boldsymbol{T}}\right)^{\boldsymbol{T}}\right)^{2m} \quad \cdots \quad \left(\left(\mathbf{H}_2{}^{\boldsymbol{T}}\right)^{\boldsymbol{T}}\right)^{C(N)m}\right]^{\boldsymbol{T}} = \\ &= \left[\left(\mathbf{H}_1{}^{\boldsymbol{T}}\right)^{\boldsymbol{m}} \quad \left(\mathbf{H}_1{}^{\boldsymbol{T}}\right)^{2m} \quad \cdots \quad \left(\mathbf{H}_1{}^{\boldsymbol{T}}\right)^{C(N)m}\right]^{\boldsymbol{T}} = \\ &= \begin{bmatrix} \left(\mathbf{H}_1{}^{m}\right)^{\boldsymbol{T}} \\ \left(\mathbf{H}_1{}^{2m}\right)^{\boldsymbol{T}} \\ \cdots \\ \left(\mathbf{H}_1{}^{C(N)m}\right)^{\boldsymbol{T}} \end{bmatrix}, \end{aligned} \tag{9}$$

поскольку $\mathbf{H}_2{}^{\boldsymbol{T}} = \mathbf{H}_1$. Кроме того, учтем, что

$$(\mathbf{H}_1)^{\boldsymbol{m}} = (\mathbf{H}_1)^{\boldsymbol{m-1}}\mathbf{H}_1 = (\mathbf{H}_1)^{\boldsymbol{m-1}} \begin{bmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ . & . & . & . & . \\ 0 & 0 & \cdots & 0 & a_{m-2} \\ 0 & 0 & \cdots & 1 & a_{m-1} \end{bmatrix}. \tag{10}$$

Далее, полагая, что первообразный элемент группы совпадает с первым столбцом $\mathbf{H}_1$, т.е. $\boldsymbol{\alpha}^0 = [0\,1\,0\,\ldots\,0\,0]^m$, заметим, что $\mathbf{H}_1\boldsymbol{\alpha}^0 = \boldsymbol{\alpha}^1 = [0\,0\,1\,\ldots\,0\,0]^{\boldsymbol{T}}$ и совпадает со вторым столбцом $\boldsymbol{H}_1$, и т.д. Последний элемент $\boldsymbol{\alpha}^{m-1} = \mathbf{H}_1\alpha^{m-2} = \mathbf{H}_1[0\,0\,\ldots\,0\,1]^T = [a_0 \;\; a_1 \;\; \ldots a_{m-1}]^{\boldsymbol{T}}$ совпадает с последним столбцом $\mathbf{H}_1$. Таким образом, $\mathbf{H}_1 = \left[\boldsymbol{\alpha}^0 \quad \boldsymbol{\alpha}^1 \quad \cdots \quad \boldsymbol{\alpha}^{m-1}\right]$. Тогда

$$\begin{aligned} &(\mathbf{H}_1)^{\boldsymbol{m}} = \\ &= \left[(\mathbf{H}_1)^{\boldsymbol{m-1}}\boldsymbol{\alpha}^0 \quad (\mathbf{H}_1)^{\boldsymbol{m-1}}\boldsymbol{\alpha}^1 \quad \cdots \quad (\mathbf{H}_1)^{\boldsymbol{m-1}}\boldsymbol{\alpha}^{m-1}\right] = \\ &= \left[\boldsymbol{\alpha}^{m-1} \quad \boldsymbol{\alpha}^{m} \quad \cdots \quad \boldsymbol{\alpha}^{2m-2}\right]. \end{aligned} \tag{11}$$

Аналогично получим $(\mathbf{H}_1)^{2m} = (\mathbf{H}_1)^{2m-1}\mathbf{H}_1 = \left[\boldsymbol{\alpha}^{2m-1} \quad \boldsymbol{\alpha}^{2m} \quad \cdots \quad \boldsymbol{\alpha}^{3m-2}\right]$ и т.д. В результате

$$\mathbf{H} = \left[\boldsymbol{\alpha}^{(m-1)^T}\boldsymbol{\alpha}^{m^T}\ldots\boldsymbol{\alpha}^{(2m-2)^T}\boldsymbol{\alpha}^{(C(N)m-1)^T}\boldsymbol{\alpha}^{C(N)m^T}\ldots\boldsymbol{\alpha}^{((C(N)+1)m-2)^T}\right]^T, \tag{12}$$

где $\alpha^0 = [0\,1\,0\,\ldots\,0\,0]^T$, причем $\mathbf{H}$ в своих строках содержит элементы мультипликативной группы, построенной на основе сопровождающей матрицы $\mathbf{H}_1$ – от $(m-1)$-го до $(\left(C(N)+1\right)m-2)$-го (при $m = 5$ от 4-го до 33-го, всего 30), т.е. группа, представленная в этой матрице, будет усеченной. Первообразным элементом усеченной группы будет

$$\boldsymbol{\alpha}^{(m-1)} = \mathbf{H}_1{}^{m-1}\boldsymbol{\alpha}^0 = [a_0 \;\; a_1\ldots a_{m-1}]^T.$$

Из формул (7), (8), (12) следует:

$$\mathbf{W}_{m,p(1,0)} = \begin{bmatrix} \mathbf{I}_m \\ \mathbf{H} \end{bmatrix} \mathbf{R}_{ma} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ & & \mathbf{H}_p & \end{bmatrix} \mathbf{R}_{ma}, \quad (13)$$

где $\mathbf{H}_p$ – расширенная матрица $\mathbf{H}$, содержащая в своих строках элементы мультипликативной группы, построенной на основе $\mathbf{H}_1$ – от элемента $\boldsymbol{\alpha}^0 = [0\,1\,0 \ldots 0\,0]^T$ до $((C(N)+1)m-2)$-го элемента, всего $(C(N)+1)m-1 > N$ элементов. Далее отметим, что $\mathbf{H}_1[1\,0 \ldots 0\,0]^m = [0\,1\,0 \ldots 0\,0]^m$. То есть, сохранив в матрице $\mathbf{W}_{m,p(1,0)}$ лишь N первых строк, можно записать матрицу, состоящую из функций Уолша без нулевого символа при их нумерации от нуля в следующем виде:

$$\mathbf{W}_{m(1,0)} = \mathfrak{I}_{m,1}{}^{T} \mathbf{R}_{ma} = \begin{bmatrix} x_{0,0} & x_{1,0} & \cdots & x_{m-1,0} \\ x_{0,1} & x_{1,1} & \cdots & x_{m-1,1} \\ . & . & . & . \\ x_{0,N-1} & x_{1,N-1} & \cdots & x_{m-1,N-1} \end{bmatrix} \mathbf{R}_{ma}, \quad (14)$$

причем все строки матрицы $\mathfrak{I}_{m,1}{}^{T}$ – это элементы мультипликативной группы поля Галуа, построенной на основе матрицы $\mathbf{H}_1$ с первообразным элементом

$$\boldsymbol{\alpha}^0{}_{\mathbf{H}_1} = \begin{bmatrix} x_{0,0} & x_{1,0} & \ldots & x_{m-1,0} \end{bmatrix}^T = [1\,0 \ldots 0\,0]^T.$$

Соответственно, для преобразования любого циклического сдвига МП в функцию Уолша без нулевого символа при их нумерации с нуля надо переставить ее элементарные символы по возрастанию значений элементов мультипликативной группы поля Галуа, построенной на основе сопровождающей матрицы полинома вида $\mathbf{H}_2$. При этом важное значение имеет выбор первообразного элемента группы $\boldsymbol{\alpha}^0{}_{\mathbf{H}_2}$, в зависимости от которого данный циклический сдвиг может быть преобразован к любой строке матрицы $\mathbf{W}_{m(1,0)}$. Но при заданном $\boldsymbol{\alpha}^0{}_{\mathbf{H}_2}$ соответствие между циклическими сдвигами преобразуемой МП и строками матрицы $\mathbf{W}_{m(1,0)}$ будет взаимно однозначным, т.е. МП с абсолютным циклическим сдвигом $\mathbf{b}$ будет преобразована в последовательность Уолша без нулевого символа при их нумерации с нуля, находящуюся в i-й строке матрицы $\mathbf{W}_{m(1,0)}$, где i можно найти, решив уравнение $\mathbf{H}_2{}^i \boldsymbol{\alpha}^0{}_{\mathbf{H}_2} = \mathbf{b}$. При этом в строках матрицы

$$\mathbf{W}_{m(1,0)} = \begin{bmatrix} x_{0,0}\mathbf{r}_{0a} \oplus x_{1,0}\mathbf{r}_{1a} \oplus \ldots \oplus x_{m-1,0}\mathbf{r}_{(m-1)a} \\ x_{0,1}\mathbf{r}_{0a} \oplus x_{1,1}\mathbf{r}_{1a} \oplus \ldots \oplus x_{m-1,1}\mathbf{r}_{(m-1)a} \\ \ldots \\ x_{0,N-1}\mathbf{r}_{0a} \oplus x_{1,N-1}\mathbf{r}_{1a} \oplus \ldots \oplus x_{m-1,N-1}\mathbf{r}_{(m-1)a} \end{bmatrix} \quad (15)$$

аналоги функций Радемахера складываются по модулю 2 с весовыми коэффициентами, представляющими собой символы элементов мультипликативной группы поля, построенной на основе сопровождающей матрицы полинома $\mathbf{H}_1$ с первообразным элементом $\alpha^0{}_{\mathbf{H}_1} = [1\,0 \ldots 0\,0]^T$. (В (15) $\oplus$ – обозначение операции суммирования по модулю 2.) Соответственно, в i-й строке матрицы $\mathbf{W}_{m(1,0)}$ будет находиться функция Уолша без нулевого символа при их нумерации с нуля, полученная путем суммирования аналогов функций Радемахера с весовыми коэффициентами, равными значениям символов вектора $\mathbf{x} = \mathbf{H}_1{}^i \boldsymbol{\alpha}^0{}_{\mathbf{H}_1}$. Таким образом, любая i-я строка матрицы (15)

$$\mathbf{w}_{i(1,0)} = x_{0,i}\mathbf{r}_{0a} \oplus x_{1,i}\mathbf{r}_{1a} \oplus \ldots \oplus x_{m-1,i}\mathbf{r}_{(m-1)a} \quad (16)$$

является функцией Уолша без нулевого символа при их нумерации с нуля, где

$$\begin{bmatrix} x_{0,i} \\ x_{1,i} \\ \ldots \\ x_{m-1,i} \end{bmatrix} = \mathbf{H}_1{}^i \begin{bmatrix} 1 \\ 0 \\ \ldots \\ 0 \end{bmatrix}. \quad (17)$$

Произведя замену символов МП в $\mathfrak{I}_{m,n,u}$ по правилу $0 \to 1, 1 \to -1$, получим

$$\mathbf{W}_{m(1,-1)} = \begin{bmatrix} \mathbf{r}_0{}^{x_{0,0}} \cdot \mathbf{r}_1{}^{x_{1,0}} \cdot \ldots \cdot \mathbf{r}_{(m-1)}{}^{x_{m-1,0}} \\ \mathbf{r}_0{}^{x_{0,1}} \cdot \mathbf{r}_1{}^{x_{1,1}} \cdot \ldots \cdot \mathbf{r}_{(m-1)}{}^{x_{m-1,1}} \\ \ldots \\ \mathbf{r}_0{}^{x_{0,N-1}} \cdot \mathbf{r}_1{}^{x_{1,N-1}} \cdot \ldots \cdot \mathbf{r}_{(m-1)}{}^{x_{m-1,N-1}} \end{bmatrix}, \quad (18)$$

где $\mathbf{r}_0,\ldots,\mathbf{r}_{(m-1)}$ – функции Радемахера с элементами (1,–1) без нулевого символа при их нумерации с нуля. При этом i-я строка матрицы $\mathbf{W}_{m(1,-1)}$ задается как

$$\mathbf{w}_{i(1,-1)} = \mathbf{r}_0^{\,x_{0,i}} \cdot \mathbf{r}_1^{\,x_{1,i}} \cdot \ldots \cdot \mathbf{r}_{(m-1)}^{\,x_{m-1,i}}, i = 0,\ldots,N-1, \quad (19)$$

где степени функций Радемахера по-прежнему рассчитываются по формуле (17).

Дополнив матрицу функций Уолша (18) нулевой строкой при их нумерации с нуля и крайним левым столбцом, состоящими из единиц, получим полный набор ортогональных базисных функций Уолша, способ упорядочения которых в этой матрице (кроме нулевой строки, состоящей лишь из единиц) определяется последовательностью элементов мультипликативной группы поля Галуа по модулю неприводимого примитивного полинома $f_m(x)$ с коэффициентами $a_0,a_1,\ldots,a_{m-2},a_{m-1}$ и его сопровождающей матрицей вида $\mathbf{H}_1$ при первообразном элементе $\boldsymbol{\alpha}^0{}_{\mathbf{H}_1} = [1\,0\ldots0\,0]^T$.

Рассмотрим матрицу $\mathbf{W}_{m(1,-1)}{}^T$. Она состоит из строк, в которых циклические сдвиги МП упорядочены по номеру строки, т.е. каждая МП начинается с блока из m символов, соответствующих двоичному представлению номера строки, в которой она находится в матрице $\mathbf{W}_{m(1,-1)}{}^T$, а по столбцам этой матрицы располагаются функции Уолша, упорядоченные по элементам мультипликативной группы поля Галуа, соответствующей матрице $\mathbf{H}_1$. Поэтому перестановка столбцов этой матрицы по возрастанию значений элементов мультипликативной группы поля Галуа, построенной на основе сопровождающей матрицы ее полинома вида $\mathbf{H}_1$ при первообразном элементе $\boldsymbol{\alpha}^0{}_{\mathbf{H}_1} = [1\,0\ldots0\,0]^T$, приводит эту матрицу к матрице Адамара без нулевых столбца и строки при их нумерации с нуля. В каждой i-й строке этой матрицы находится функция Уолша без нулевого символа при их нумерации с нуля

$$\mathbf{w}_{i(1,-1)\text{Ад}} = \mathbf{r}_0^{\,h_{0,i}} \cdot \mathbf{r}_1^{\,h_{1,i}} \cdot \ldots \cdot \mathbf{r}_{(m-1)}^{\,h_{m-1,i}}, \quad i = 0,\ldots,N-1, \quad (20)$$

где $h_{0,i},h_{1,i},\ldots,h_{m-1,i}$ – значения разрядов двоичного представления номера строки j ($h_{m-1,i}$ – младший разряд).

3. СИНХРОНИЗАЦИЯ МП

Первый способ синхронизации МП предполагает следующую последовательность действий:

1) значения дискретного сигнала $\mathbf{X}_N$, полученные с выхода синфазного или квадратурного канала приемника, переставляются по возрастанию значений элементов мультипликативной группы $\boldsymbol{\alpha}^0{}_{\mathbf{H}_2}, \boldsymbol{\alpha}^1{}_{\mathbf{H}_2} \ldots, \boldsymbol{\alpha}^{N-1}{}_{\mathbf{H}_2}$ при любом выбранном $\boldsymbol{\alpha}^0{}_{\mathbf{H}_2}$; т.е. значения $\mathbf{X}_N$ записываются в запоминающее устройство, причем нулевое значение при их нумерации с нуля – в ячейку памяти с адресом $\boldsymbol{\alpha}^0{}_{\mathbf{H}_2}$, первое – в ячейку с адресом $\boldsymbol{\alpha}^1{}_{\mathbf{H}_2}$ и т.д. при нумерации ячеек памяти от 0 до N; при этом нулевая ячейка памяти останется свободной, так как у мультипликативной группы поля Галуа отсутствует элемент 0 0 ... 0;

2) в ячейку памяти с номером 0 записывается единица, и производится быстрое преобразование Адамара (БПА) полученного вектора;

3) считывается номер ячейки i, в которой оказалось наибольшее значение результата БПА (нулевая ячейка игнорируется); таким образом, идентифицируется строка матрицы Адамара, к которой преобразован циклический сдвиг исходной МП;

4) обратное двоичное представление i, т.е. $h_{m-1,i}h_{m-2,i}\ldots h_{0,i}$ рассматривается как элемент мультипликативной группы поля Галуа, построенного на основе сопровождающей матрицы $\mathbf{H}_1$ используемого полинома при первообразном элементе $\boldsymbol{\alpha}^0{}_{\mathbf{H}_2} = [1\,0\ldots0\,0]^T$;

5) определяется номер строки, в которой находится полученная функция Уолша в $\mathbf{W}_{m(1,-1)}$, упорядоченной по значениям элементов мультипликативной группы поля Галуа, построенной на основе $\mathbf{H}_1$ (далее – группы 1), при решении уравнения $\mathbf{H}_1{}^i\boldsymbol{\alpha}^0{}_{\mathbf{H}_1} = [h_{m-1,j}h_{m-2,j}\ldots h_{0,j}]^m$ относительно i;

6) искомый начальный блок МП вычисляется по формуле $\mathbf{b} = \mathbf{H}_2{}^i\boldsymbol{\alpha}^0{}_{\mathbf{H}_2}$.

На практике решение матричного уравнения п. 5 и вычисления п. 6 можно реализовать с помощью генераторов мультипликативных групп поля Галуа, формируемых на основе сопровождающих матриц исходного полинома $\mathbf{H}_1$ и $\mathbf{H}_2$ (далее – группы 1 и 2). Для первого из них $\alpha^0{}_{\mathbf{H}_1} = [1\,0\ldots0\,0]^T$, а для второго первообразный

элемент совпадает с $\boldsymbol{\alpha}^0{}_{\mathbf{H}_2}$, с которого начиналась перестановка значений $\mathbf{X}_N$. Когда числа на выходе этих генераторов совпадут, на выходе генератора группы 2 будет искомый начальный блок МП.

Другой вариант этого алгоритма предполагает перестановку содержимого ячеек памяти запоминающего устройства после выполнения БПА в соответствии с последовательностью элементов группы 1. То есть после выполнения п. 2 надо запустить генератор этой группы с первообразным элементом $\boldsymbol{\alpha}^0{}_{\mathbf{H}_1} = [1\,0\,\ldots\,0\,0]^T$ и переставить содержимое 1-й ячейки по адресу $\boldsymbol{\alpha}^0{}_{\mathbf{H}_1}$, 2-й – по адресу $\boldsymbol{\alpha}^1{}_{\mathbf{H}_1}$ и т.д. Затем необходимо определить номер ячейки с максимальным содержимым. Этот номер будет соответствовать искомому начальному блоку МП, содержащейся в значения дискретного сигнала $\mathbf{X}_N$. Найденный начальный блок надо записать в генератор группы 2, с выхода которого будет формироваться опорная МП.

Таким образом, ключевыми элементами устройства синхронизации МП на основе БПА являются генераторы мультипликативных групп поля Галуа. Нетрудно показать, что генераторы групп 1 и 2 представляют собой варианты устройства формирования МП [1]. Действительно, учитывая структуры матриц $\mathbf{H}_1$ и $\mathbf{H}_2$, можно получить рекуррентные соотношения для элементов соответствующих мультипликативных групп:

для элементов группы 1 –

$$\begin{cases} x_{0,i} = a_0 x_{m-1,i-1}, (a_0 = 1), \\ x_{1,i} = x_{0,i-1} \oplus a_1 x_{m-1,i-1}, \\ \ldots \\ x_{m-1,i} = x_{m-2,i-1} \oplus a_{m-1} x_{m-1,i-1}; \end{cases} \tag{21}$$

для элементов группы 2 –

$$\begin{cases} x_{0,i} = x_{1,i-1}, \\ x_{1,i} = x_{2,i-1}, \\ \ldots \\ x_{m-1,i} = a_0 x_{0,i-1} \oplus a_1 x_{1,i-1} \oplus \ldots \oplus a_{m-1} x_{m-1,i-1}. \end{cases} \tag{22}$$

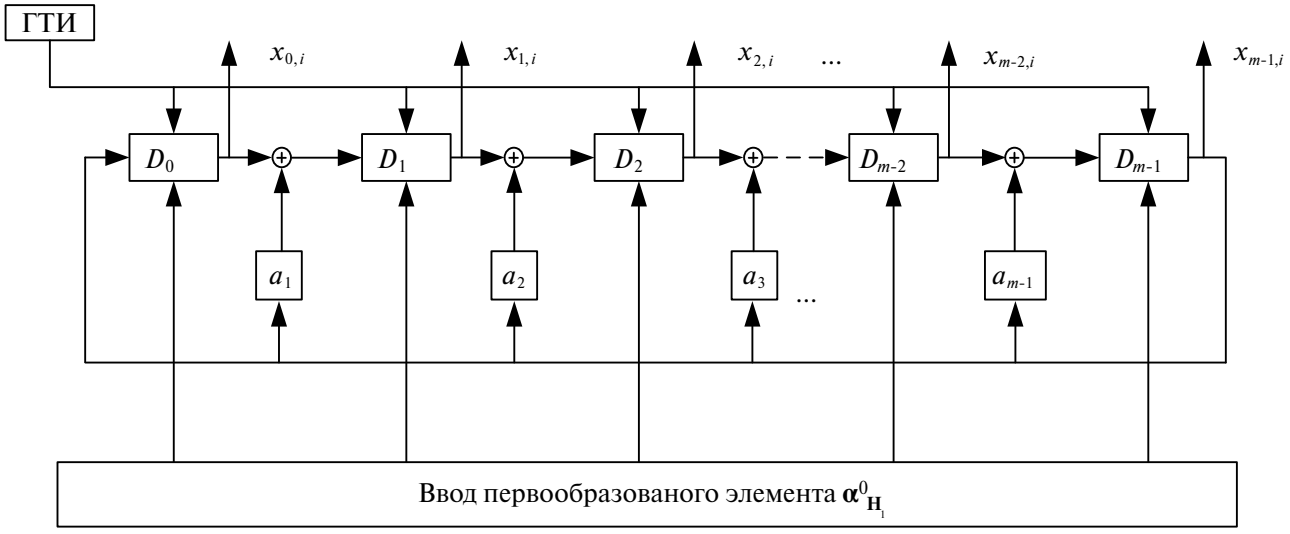
Следуя традиции рассматривать преобразования в полях Галуа, а также формирователи МП в виде сдвиговых регистров на D-триггерах [1, 21], представим функциональные схемы генераторов мультипликативных групп 1 и 2 так, как это показано на рис. 1а и 1б. Как видно, значения элементов групп считываются параллельно с выходов всех триггеров (ячеек памяти) сдвиговых регистров, а с каждого триггера последовательно – МП со сдвигами, соответствующими структуре матрицы $\mathbf{H}_1$ или $\mathbf{H}_2$.

В момент, в который в ячейках памяти генератора группы 2 окажется искомый начальный блок входной МП, последовательность $x_{0,i}, x_{0,i+1}, x_{0,i+2} \ldots$ с выхода его триггера D_0 будет формироваться синхронно с ней, если этот генератор, как и генератор группы 1, работает с тактовой частотой входной МП. Кроме того, необходимо, чтобы длительность времени всех преобразований и операций, описанных выше, была равно нулю, что невозможно. В действительности работа цифрового устройства синхронизации, разработанного с использованием современных микропроцессорных технологий, может осуществляться с максимально достижимой для него скоростью и своей тактовой частотой, и, подчеркнем еще раз, представление в этой работе генераторов мультипликативных групп в виде сдвиговых регистров на D-триггерах – лишь дань традиции.

Таким образом, необходимо, во-первых, фиксировать суммарную длительность времени всех выполненных операций, выражая ее в единицах длительности элементарного импульса входной МП, во-вторых, сдвинуть формируемую опорную МП с выхода триггера D_0 генератора группы 2 на соответствующее число элементарных символов; в-третьих, понизить тактовую частоту формируемой опорной МП до частоты входной МП. Таким образом, генератор группы 2 удобно использовать в качестве формирователя опорной МП, синхронной с входной МП, поскольку значения любых m элементарных символов формируемой МП, следующих с триггера D_0, совпадают с символами мультипликативной группы 2, оказавшихся записанными в ячейках памяти его сдвигового регистра в момент появления первого символа из этих m символов.

Второй, более простой алгоритм синхронизации МП, соответствует матрице $\mathbf{W}_{m(1,-1)}{}^T$: значения $\mathbf{X}_N$ надо переставить по возрастанию элементов мультипликативной группы поля Галуа, построенной на основе сопровождающей матрицы полинома вида $\mathbf{H}_1$, но только лишь при первообразном элементе $\alpha^0{}_{\mathbf{H}_1} = [1\,0\,\ldots\,0\,0]^T$. После выполнения БПА номер ячейки памяти запоминающего устройства, в которой оказа-

(а)



(б)

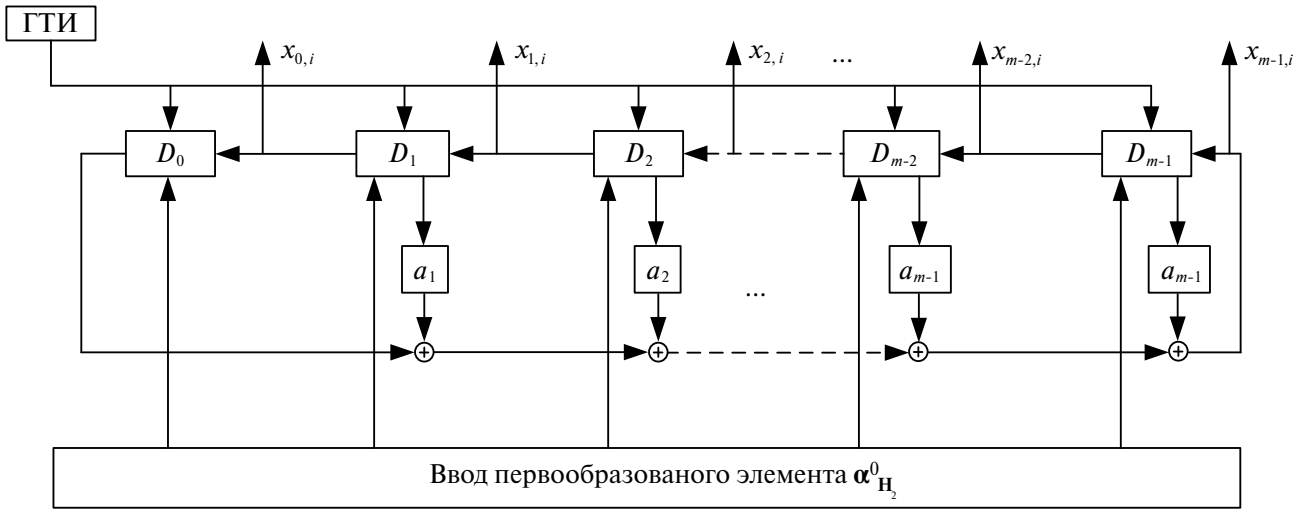


Рис. 1. Генераторы мультипликативных групп 1 (а) и 2 (б) поля Галуа по модулю неприводимого примитивного полинома с коэффициентами $a_0, a_1, \ldots, a_{m-2}, a_{m-1}$; ГТИ – генератор тактовых импульсов.

лось максимальное значение, представленное в двоичной системе счисления, и будет начальным блоком МП, содержавшейся в $\mathbf{X}_N$. Этот начальный блок следует записать в ячейки памяти генератора группы 2, в результате чего опорная МП будет формироваться именно с этого начального блока. Таким образом, в данном случае необходимо использовать как генератор группы 1, так и генератор группы 2.

Подчеркнем, что способ синхронизации МП, основанный на перестановке символов входной МП в соответствии с мультипликативной группой, формируемой на основе матрицы $\mathbf{H}_1$ (более простой алгоритм), предполагает единственный вариант перестановки такого рода, и мультипликативная группа, на основе которой она производится, всегда должна начинаться с $\boldsymbol{\alpha}^0{}_{\mathbf{H}_1} = [1\,0\,\ldots\,0\,0]^T$. Перестановка в соответствии с той же мультипликативной группой, но с другим первообразным элементом не позволит преобразовать МП к виду функции Уолша. Кроме того, данный подход предполагает, что соответ-

ствие между циклическим сдвигом МП и функцией Уолша в матрице Адамара является единственно возможным.

Напротив, перестановка символов МП в соответствии с мультипликативной группой, формируемой на основе матрицы $\mathbf{H}_2$ (более сложный алгоритм), может производиться с любого первообразного элемента $\boldsymbol{\alpha}^0{}_{\mathbf{H}_2}$, в результате чего любой циклический сдвиг входной МП можно привести к любой функции Уолша, но при выбранном $\boldsymbol{\alpha}^0{}_{\mathbf{H}_2}$ – только к одной такой функции. Кроме того, если заранее известен диапазон циклических сдвигов, в пределах которого может находиться сдвиг входной МП, либо несколько ее циклических сдвигов при многолучевом распространении сигнала, то перестановка символов МП в соответствии с мультипликативной группой 2 преобразует их в последовательности Уолша без нулевого символа при их нумерации от нуля, следующие непосредственно друг за другом в матрице из этих функций, упорядоченной в соответствии с мультипликативной группой 1. Тогда, учитывая, что в матрице Адамара сохраняются только эти функции, можно оптимизировать алгоритм БПА, снизив его вычислительную сложность. Другие циклические сдвиги входной МП могут быть приведены к тем же функциям Уолша без нулевого символа при их нумерации с нуля при выборе $\boldsymbol{\alpha}^0{}_{\mathbf{H}_2}$ группы 2, в соответствии с которой производится перестановка символов.

Таким образом, если известен диапазон возможных циклических сдвигов принимаемой МП, то можно выбрать соответствующее значение $\boldsymbol{\alpha}^0{}_{\mathbf{H}_2}$ и преобразовать ее к одной из нескольких функций Уолша, следующих друг за другом в матрице Адамара. Любой другой циклический сдвиг МП с той же шириной области неопределенности по времени может быть приведен к какой-то функции Уолша из того же их набора при выборе $\boldsymbol{\alpha}^0{}_{\mathbf{H}_2}$. Таким образом, для обнаружения любого циклического сдвига МП можно использовать БПА в одном и том же усеченном базисе функций Уолша–Адамара. Если этот усеченный базис содержит относительно небольшое число функций Уолша, то вычисления в соответствии с п. 5 и 6 могут не потребоваться.

ЗАКЛЮЧЕНИЕ

1. Алгоритм перестановки значений дискретного сигнала при его преобразовании к строке матрицы функций Уолша, а также способ идентификации циклического сдвига соответствующей ПСП после выполнения БПА, зависят от выбора структуры матрицы-циркулянта этой ПСП.

2. Матрица-циркулянт МП, строки которой начинаются с блоков двоичных символов, соответствующих десятичным номерам этих строк при их двоично-десятичном кодировании, может быть приведена к матрице Адамара без нулевых строки и столбца при их нумерации от нуля путем перестановки столбцов матрицы в соответствии со значениями единственной мультипликативной группы расширенного поля Галуа. Способ формирования этой группы соответствует рис. 1а и виду $\mathbf{H}_1$ сопровождающей матрицы исходного неприводимого примитивного полинома, и только при значении первообразного элемента этой группы $\boldsymbol{\alpha}^0{}_{\mathbf{H}_1} = [1\,0\,\ldots\,0\,0]^T$.

3. Любая из N упорядоченных матриц-циркулянтов МП может быть приведена к матрице из функций Уолша, упорядоченной по степеням мультипликативной группы расширенного поля Галуа, где N – длина МП. В этом случае перестановка столбцов матрицы-циркулянта должна производиться по возрастанию значений элементов мультипликативной группы поля Галуа, соответствующей виду матрицы $\mathbf{H}_2$. При этом любой циклический сдвиг МП может быть приведен к любой функции Уолша без нулевого символа при их нумерации от нуля в зависимости от выбора первообразного элемента $\boldsymbol{\alpha}^0{}_{\mathbf{H}_2}$ данной группы, который и определяет структуру матрицы-циркулянта. Но при данном значении $\boldsymbol{\alpha}^0{}_{\mathbf{H}_2}$ соответствие между преобразуемым циклическим сдвигом МП и функцией Уолша без нулевого символа при их нумерации от нуля является взаимно однозначным. Таким образом, все возможные матрицы-циркулянты МП, каждая последующая строка которой сдвинута циклически относительно предыдущей строки на один символ, приводятся к одной и той же матрице функций Уолша без нулевых символов при их нумерации от нуля. Получаемая матрица функций Уолша упорядочена по степеням элементов мультипликативной группы поля Галуа с первообразным элементом $\boldsymbol{\alpha}^0{}_{\mathbf{H}_1} = [1\,0\,\ldots\,0\,0]^m$ и соответствует сопровождающей матрице полинома вида $\mathbf{H}_1$, Отметим также важное свойство данного преобразования матриц: если при выбранном $\boldsymbol{\alpha}^0{}_{\mathbf{H}_2}$, определяющем структуру матрицы-циркулянта со строками, упорядоченными по циклическим сдвигам МП, некоторая ее i-я строка приводится к u-й строке матрицы функций Уолша без нулевого символа при их

нумерации от нуля, то при выборе в качестве первообразного элемента $\boldsymbol{\alpha}^{0+l}{}_{\mathbf{H}_2}$ эта же строка матрицы-циркулянта приводится к $(u+l)$-й строке матрицы функций Уолша.

4. Матрица Адамара может быть получена из матрицы функций Уолша, упорядоченной по степеням максимальной мультипликативной группы поля Галуа, путем перестановки ее строк по возрастанию значений элементов этой группы и добавлением нулевой строки и нулевого столбца при их нумерации от нуля.

5. Любой из способов преобразования МП в соответствии с правилами, описанными в п. 2 и 3, позволяет привести ее к функции Уолша без нулевого символа при их нумерации от нуля, а последующее добавление к ней этого символа и преобразование полученного вектора с помощью БПА – быстро вычислить периодическую автокорреляционную функцию МП с поправкой на разницу в длинах МП и последовательностей Уолша; выигрыш по вычислительной сложности будет в N/m раз по сравнению с традиционным алгоритмом вычисления дискретной свертки МП.

Авторы заявляют об отсутствии конфликта интересов.

СПИСОК ЛИТЕРАТУРЫ

1. *Ипатов В.П.* Широкополосные системы и кодовое разделение сигналов. М: Мир связи, 2007.
2. *Beard C., Stallings W.* Wireless Communication Networks and Systems. L.: Pearson, 2016.
3. *Middlestead R.W.* Digital Communications with Emphasis on Data Modems. Theory, Analysis, Design, Simulation, Testing and Applications. Lesly (USA): Wiley, 2017.
4. *Лосев В.В., Бродская Е.Б., Коржик В.И.* Поиск и декодирование сложных дискретных сигналов. М.: Радио и связь,1988.
5. *Maral G., Bousquet M., Sun Z.* Satellite Communications Systems. United Kingdom: Wiley, 2020.
6. *Волков Р.В., Саяпин В.Н., Севидов В.В.* // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 9. С. 14.
7. *Кулакова В.И.* // Системы управления, связи и безопасности. 2020. № 1. С. 33.
8. *Музыченко Н.Ю.* // РЭ. 2019. Т. 64. № 1. С. 44.
9. *Gold R.* // IEEE Trans. 1967. V. IT-13. № 4. P. 619. https://doi.org/10.1109/TIT.1967.1054048
10. *Зубарев В.Ю., Пономаренко Б.В., Шанин Е.Г., Вострецов А.Г.* // Изв. вузов России. Радиоэлектроника. 2020. Т. 23. № 2. С. 26.
11. *Варакин Л.Е.* Системы связи с шумоподобными сигналами. М.: Радио и связь, 1985.
12. *Смирнов Н.И., Горгадзе С.Ф.* // Зарубеж. радиоэлектроника.1997. № 5. С. 41.
13. *Горгадзе С.Ф., Ву Ши Д.* // T-Comm: Телекоммуникации и транспорт. 2023. Т. 10. № 8. С.4.
14. *Лосев В.В., Дворников В.Д.* // РЭ. 1983. Т. 28. № 8. С. 1540.
15. *Горгадзе С.Ф.* Синхронизация в инфокоммуникационных системах. М.: Медиа Паблишер, 2022.
16. *Шахтарин Б.И., Черныш А.В.* // Вестн. МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2009. № 3. С. 114.
17. *Горгадзе С.Ф.* // РЭ. 2005. Т. 50. № 3. С. 302.
18. *Горгадзе С.Ф.* // РЭ. 2006. Т. 51. № 4. С. 428.
19. *Ву Ши.Д., Горгадзе С.Ф.* // DPSA: Вопросы применения цифровой обработки сигналов. 2023. Т. 13. № 1. С. 31.
20. *Ву Ши.Д.*, *Горгадзе С.Ф.* // Телекоммуникации и информ. технологии. 2022. Т. 9. № 2. С. 1207.
21. *Смольянинов В.М.* // РЭ. 1985.Т. 30. № 12. С. 2391.
22. *Be'ery Y., Snyders J.* // IEEE Trans. 1986. V. IT-32. № 3. P. 355.
23. *Be'ery Y., Snyders J.* // J. Algebraic Discrete Methods. 1987. V. 8. № 4. P. 778.
24. *Смольянинов В.М., Назаров Л.Е.* // РЭ. 1987. Т. 32. № 11. С. 2341.
25. *Смольянинов В.М., Назаров Л.Е.* // РЭ. 1989. Т. 34. № 12. С. 2651.
26. *Смольянинов В.М., Назаров Л.Е., Прокофьев И.В.* // РЭ. 1989. Т. 34. № 8. С. 1686.
27. *Li Ping W.K., Leung K.Y.* // IEEE Trans. 2003. V. IT-49. № 12. P. 3213.
28. *Канатова Л.В., Литвинов В.Л., Финк Л.М.* // Проблемы передачи информации. 1986. Т. 22. Вып. 2. С. 98.
29. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. М.: Мир, 1976.
30. *Свердлик М.Б.* Оптимальные дискретные сигналы. М.: Сов. радио, 1975.
31. *Трахтман А.М., Трахтман В.А.* Основы теории дискретных сигналов на конечных интервалах. М.: Сов. радио, 1975.
32. *Ву Ши.Д., Горгадзе С.Ф.* // Технологии информационного общества: Сб. трудов XVI Междунар. отраслевой науч.-технич. конф. М., 2022. С. 88.

SYNCHRONIZATION OF M-SEQUENCES BASED ON FAST HADAMARD TRANSFORM

S. F. Gorgadze*, Dao Vu Shi, A. V. Ermakova

Moscow Technical University of Communication and Information, Moscow 111024 Russia

**E-mail: s.f.gorgadze@mtuci.ru*

Received October 19, 2022; revised July 18, 2023; accepted July 27, 2023

Options have been developed for constructing circulant matrices of any M-sequence (MS) based on automorphic multiplicative groups of the extended Galois field, constructed using an irreducible primitive polynomial, on the basis of which the original MS is formed. The result of this approach is the identification of new methods for transforming MS circulant matrices to a matrix of Walsh functions, ordered by the powers of the antiderivative element of the field. It is shown for the first time that, depending on the initial conditions of the transformation, a set of any number of any cyclic shifts of the MP, shifted relative to each other by one symbol, can be transformed to any rows of the ordered matrix of Walsh functions, following one another. This circumstance makes it possible to simplify the MS synchronization algorithm for a known range of its cyclic shifts, especially in the case of large periods of its repetition, and also to reduce the computational complexity of the processing algorithm when working in a truncated basis of Walsh–Hadamard functions.

Keywords: M-sequences, circulant matrix, Walsh function matrix, noise-like complex signals, multiplicative Galois field groups, fast Hadamard transform.