

SYNCHRONIZATION OF M-SEQUENCES AND GOLD PSEUDORANDOM SEQUENCES BASED ON THE FAST HADAMARD TRANSFORM

Sy. D. Vu ¹

¹ Le Quy Don Technical University, HaNoi, VietNam
daovs@viettel.com.vn

ABSTRACT

Methods have been developed for constructing circulant matrices for any maximal-length sequence (MLS) based on the automorphic multiplicative groups of an extended Galois field – a field constructed using the same irreducible primitive polynomial that defines the original MLS. This approach reveals new ways to transform the circulant matrices of an MLS into a matrix of Walsh functions, ordered according to the powers of the field's primitive element. It is demonstrated, for the first time, that – depending on the initial transformation conditions – any set of cyclic shifts of an MLS (where each shift is offset by a single symbol relative to the others) can be mapped to a sequence of consecutive rows within an ordered Walsh function matrix. This finding facilitates the simplification of MLS synchronization algorithms, particularly when the range of possible cyclic shifts is known – a significant advantage for sequences with long repetition periods. Furthermore, it reduces the computational complexity of processing algorithms when operating within a truncated Walsh-Hadamard basis. Based on an analysis of the structures of isomorphic multiplicative groups within extended Galois fields, it has been established that any cyclic shift of a Gold pseudorandom sequence can be transformed into a function belonging to the complete set of analogues of Rademacher functions for a given dimension. This insight has enabled the development of a new fast synchronization algorithm for Gold sequences, which relies on computing their discrete convolution via a fast spectral transform within a truncated Walsh-Hadamard basis.

DOI: 10.36724/2664-066X-2026-12-3-2-29

Received: 25.02.2026

Accepted: 12.05.2026

Citation: Sy. D. Vu, "Synchronization of m-sequences and Gold pseudorandom sequences based on the fast Hadamard transform," *Synchroinfo Journal* **2026**, vol. 12, no. 3, pp. 2-29.

Licensee IRIS, Vienna, Austria.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).



Copyright: © 2026 by the authors.

KEYWORDS: *noise-like signals, vector-matrix multiplication, Rademacher functions, periodic autocorrelation function, Galois field.*

Introduction

The previous article [1] points out the interrelation between the tasks of joint detection and parameter estimation for a low-power noise-like complex signal (NCS) and the decoding of block codes constructed based on cyclic shifts of their codewords. This article examines the problem of synchronizing a Gold pseudorandom sequence (PRS), highlighting the connection between this task and the synchronization of a periodic NCS during its processing at a receiver. In this context, PRS synchronization is defined as the determination of its cyclic shift – relative to the start of the observation interval for the NCS from which the PRS was generated.

When addressing the synchronization of PRS (pseudorandom sequences) with long repetition periods, it becomes crucial to identify the correspondence between the row indices of a Walsh-Hadamard matrix and the initial blocks of cyclic shifts of the PRS – or, in matrix terms, the rows of a circulant matrix derived from the PRS. As shown below, such a circulant matrix can be constructed in various ways. Consequently, this section explores methods for constructing PRS-based circulant matrices using multiplicative groups of an extended Galois field (defined modulo an irreducible primitive polynomial). It also examines techniques for transforming these matrices into full or truncated Hadamard matrices (or their analogues) to facilitate the development of accelerated PRS synchronization algorithms for processing noise-like signals. The findings presented in this section have been published by the author of this dissertation in [2-5].

Construction of circulant matrices based on multiplicative groups of a Galois field

Let us consider an arbitrary finite field (GF) with elements $\{0, 1\}$, constructed based on an irreducible primitive polynomial $f_m(x)$, as a row vector ${}_i^N \mathfrak{S}_i = [x_{i,k}, k = 0, \dots, N-1]$, where $i = 0, \dots, m-1$ – the number of the cyclic shift of the MS on $l_i \in \{0, 1, \dots, N-1\}$ symbols relative to the MS ${}_0^N \mathfrak{S}_0$ with a nominally zero cyclic shift, $N = 2^m - 1$ – length (period) of the MS, m – order $f_m(x)$, n – the number of the chosen method for ordering MSs based on their cyclic shifts [4, 6-8].

One can choose a way of ordering any m MS (as described above) such that the columns $\alpha^k = [x_{i,k}, i = 0, \dots, m-1]^T, k = 0, \dots, N-1$, form the multiplicative group of an extended Galois field $GF(2^m)$ built on a modular basis $f_m(x)$, where k – is the number of the group element, $[\cdot]^T$ – notation for a transposed matrix [7-9]. Such a group has a cyclic structure and consists of the maximum possible number N of distinct non-zero elements, which are powers of a primitive element α^0 fields, moreover $\alpha^k = H_n \alpha^{k-1}$, where H_n – companion matrix $f_m(x)$ [8]. Typically, four types of such matrices are considered [7]:

$$\begin{aligned} H_1 &= \begin{bmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & a_{m-2} \\ 0 & 0 & \cdots & 1 & a_{m-1} \end{bmatrix} & H_2 &= \begin{bmatrix} 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ a_0 & a_1 & \cdots & a_{m-2} & a_{m-1} \end{bmatrix} \\ H_3 &= \begin{bmatrix} a_{m-1} & 1 & \cdots & 0 & 0 \\ a_{m-2} & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_1 & 0 & \cdots & 0 & 1 \\ a_0 & 0 & \cdots & 0 & 0 \end{bmatrix} & H_4 &= \begin{bmatrix} a_{m-1} & a_{m-2} & \cdots & a_1 & a_0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}, \end{aligned} \quad (1)$$

where $a_0, a_1, \dots, a_{m-2}, a_{m-1}$ – polynomial coefficients $f_m(x)$, belonging to the set $\{0,1\}$; thus, the dimension of these matrices will be $m \times m$. An important property is the cyclicity of a group – that is, $\alpha^0 = \alpha^N, \alpha^1 = \alpha^{N+1}, \dots$. As α^0 you can select any of its elements. Thus,

$$\mathfrak{Z}_{m,1} = \begin{bmatrix} {}^n\mathfrak{Z}_0 \\ {}^n\mathfrak{Z}_1 \\ \dots \\ {}^n\mathfrak{Z}_{m-1} \end{bmatrix} = [\alpha^0 \quad \alpha^1 \quad \dots \quad \alpha^{N-1}], \quad \alpha^k = H_n \alpha^{k-1}, \quad (2)$$

where the columns α^k can be obtained by any of the possible methods – that is, when choosing a matrix H_n , which determines the values of the cyclic shifts of the MS l_i ($i = 0, \dots, m-1$) regarding the MS ${}^n\mathfrak{Z}_0$ with the selected α^0 . Table 1 shows the values of the elements of four maximal multiplicative groups of the Galois field obtained based on the polynomial $f_5(x) = x^5 + x^3 + 1$ and represented in the decimal numeral system. We shall henceforth denote this representation as $[\alpha^k]_{10}$. A primitive element was chosen $\alpha^0 = [1 \ 0 \ 0 \ 0 \ 0]^T$, so in all cases $[\alpha^0]_{10} = 16$.

Table 1

Maximal multiplicative groups of a Galois field modulo a polynomial $f_5(x) = x^5 + x^3 + 1$

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

For a matrix H_1 , The elements of the multiplicative group of a Galois field can be calculated using the formula:

$$\alpha^{k+1} = \begin{bmatrix} x_{0,k+1} \\ x_{1,k+1} \\ \dots \\ x_{m-1,k+1} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & \dots & 0 & a_1 \\ 0 & 0 & \dots & 0 & a_{m-2} \\ 0 & 0 & \dots & 1 & a_{m-1} \end{bmatrix} \begin{bmatrix} x_{0,k} \\ x_{1,k} \\ \dots \\ x_{m-1,k} \end{bmatrix}, \quad k = 0, \dots, N-1, \quad (2.3)$$

where m are cyclic shifts of the generated MS (that is, on $l_0, l_1, \dots, l_{m-1}$ characters relative to ${}^1\mathfrak{Z}_0$) are located in the rows of the matrix [7]:

$$\mathfrak{Z}_{m,1} = \begin{bmatrix} x_{0,0} & x_{0,1} & \dots & x_{0,N-1} \\ x_{1,0} & x_{1,1} & \dots & x_{1,N-1} \\ \dots & \dots & \dots & \dots \\ x_{m-1,0} & x_{m-1,1} & \dots & x_{m-1,N-1} \end{bmatrix}, \quad (2.4)$$

where $\mathfrak{Z}_{m,1}$ – corresponding matrix H_1 . Its columns represent the elements of the multiplicative group of the Galois field modul $f_m(x)$ with coefficients $a_0, a_1, \dots, a_{m-2}, a_{m-1}$. As an example, the elements of the matrix are presented in Table 2. $\mathfrak{Z}_{5,1}$ for a polynomial $f_5(x) = x^5 + x^4 + x^2 + x + 1$, and in Table 3 – for the dual polynomial $f_5(x) = x^5 + x^4 + x^3 + x + 1$.

Table 2

Elements of the multiplicative group of a Galois field based on the companion matrix H_1
 polynomial $f_5(x) = x^5 + x^4 + x^2 + x + 1$

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	29	19	20	10	5	31	18	9	25	17	21	23	22	11	24	12	6	3	28	14	7	30	15	26	13	27
$x_{0,k}$	1	0	0	0	1	1	1	1	0	0	1	1	0	1	1	1	1	1	0	1	0	0	0	1	0	0	1	0	1	0	1
$x_{1,k}$	0	1	0	0	0	1	0	0	1	0	1	0	1	1	0	0	0	0	1	1	1	0	0	1	1	0	1	1	1	1	1
$x_{2,k}$	0	0	1	0	0	1	0	1	0	1	1	0	0	0	0	1	1	1	0	0	1	1	0	1	1	1	1	1	0	1	0
$x_{3,k}$	0	0	0	1	0	0	1	0	1	0	1	1	0	0	0	0	1	1	1	0	0	1	1	0	1	1	1	1	1	0	1
$x_{4,k}$	0	0	0	0	1	1	1	0	0	1	1	0	1	1	1	1	1	0	1	0	0	0	1	0	0	1	0	1	0	1	1

Table 3

Elements of the multiplicative group of a Galois field based on the companion matrix H_1
 polynomial $f_5(x) = x^5 + x^4 + x^3 + x + 1$

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	0		0	1		0	1		0	0	1	0		1	1		1	0		1	0		1	1
$x_{1,k}$	0	1	0	0	0		0	1		1	1		0	1		0	0	1	1		0	0		0	1		0	1		1	0
$x_{2,k}$	0	0	1	0	0		1	0		1	1		1	0		1	0	0	1		1	0		0	0		1	0		0	1
$x_{3,k}$	0	0	0	1	0		1	1		1	0		1	0		1	1	1	0		0	0		1	0		0	1		0	1
$x_{4,k}$	0	0	0	0	1		0	1		1	0		1	0		0	1	0	1		1	1		0	1		0	0		1	1

Circulant matrix MS $\mathfrak{Z}_{m,n,\mathfrak{u}}$ with elements (0,1), containing its cyclic shifts by $l_0, l_1, \dots, l_{m-1}$ symbols, and also all other shifts that do not coincide with them, we shall form in accordance with the rule:

$$\mathfrak{Z}_{m,n,c} = \begin{bmatrix} \mathfrak{Z}_{m,n} \\ H_n^m \mathfrak{Z}_{m,n} \\ H_n^{2m} \mathfrak{Z}_{m,n} \\ \dots \\ H_n^{C(N)m} \mathfrak{Z}_{m,n} \end{bmatrix}, \quad (5)$$

where $C(N) = \left(\frac{A(N)}{m}\right) - 1$, $A(N)$ – a number as close as possible to N that is perfectly

divisible by m and satisfies the inequality $A(N) > N$. Thus, $\frac{A(N)}{m}$ – this is the total number of blocks in the matrix $\mathfrak{Z}_{m,n,c}$, containing a matrix $\mathfrak{Z}_{m,n}$ or a transformation of it of the form $H_n^x \mathfrak{Z}_{m,n}$. The size of each block will be $m \times (N - 1)$. Matrix dimension $\mathfrak{Z}_{m,n,c}$ will be $A(N) \times (N - 1)$, as a result of which the last block $\mathfrak{Z}_{m,n,c}$ in one's own $A(N) - N$ the rows will contain MPs whose cyclic shifts coincide with the shifts of the MPs in the first block. As an example, the elements $\mathfrak{Z}_{5,1,\mathfrak{u}}$, formed on the basis of $f_5(x) = x^5 + x^3 + 1$ and H_1 , are presented in Table 4.

Table 4

Matrix $\mathfrak{Z}_{5,1,c}$, formed on the basis of $f_5(x) = x^5 + x^3 + 1$

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	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	i	l_i
$x_{0,k}$	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	1	0	0	1	1	0	1	0	0	1	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	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	0	1	0	1	0	1	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	0	1	0	1	0	11
$x_{12,k}$	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	
$x_{13,k}$	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	
$x_{14,k}$	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	
$x_{15,k}$	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	
$x_{16,k}$	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	
$x_{17,k}$	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	
$x_{18,k}$	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	
$x_{19,k}$	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	
$x_{20,k}$	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	
$x_{21,k}$	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	
$x_{22,k}$	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	
$x_{23,k}$	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	
$x_{24,k}$	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	
$x_{25,k}$	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	
$x_{26,k}$	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	
$x_{27,k}$	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	
$x_{28,k}$	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	
$x_{29,k}$	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	
$x_{30,k}$	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	
$x_{31,k}$	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	
$x_{32,k}$	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	
$x_{33,k}$	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	
$x_{34,k}$	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	

From her analysis it follows that the sequence $l_0, l_1, \dots, l_{34}$, located in the last column of Table 4, looks random, although the second block $\mathfrak{Z}_{5,1,c}$ from $m = 5$ its rows are shifted by 5 character positions relative to the first block consisting of the same number of

rows, the third block is shifted by 10 character positions relative to that one, and so on. Furthermore, the columns $\mathfrak{Z}_{5,1,c}$ не являются МП.

It has a completely different structure $\mathfrak{Z}_{5,2,c}$, formed based on the same polynomial $f_5(x) = x^5 + x^3 + 1$ and H_2 and the one presented in Table 5, since its rows contain cyclic shifts of the MP, each shifted one symbol to the right relative to the others. Furthermore, its columns contain cyclic shifts of the same MP, with the MS in each successive column being cyclically shifted by one symbol compared to the preceding column. It is evident that this property is characteristic of all $\mathfrak{Z}_{m,2,c}$, built on the basis of H_2 , and it is not characteristic $\mathfrak{Z}_{m,1,c}$, $\mathfrak{Z}_{m,3,c}$, $\mathfrak{Z}_{m,4,c}$ formed on the basis of H_1 , H_3 и H_4 . We shall refer to all circulant matrices formed on the basis of H_2 as being ordered by cyclic shifts, or simply as ordered.

Table 5

Matrix $\mathfrak{Z}_{5,2,c}$, formed on the basis of $f_5(x) = x^5 + x^3 + 1$

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	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	i	l_i	
$x_{0,k}$	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	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	0	1	0	1	0	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	0	1	0	1	0	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	0	1	0	1	0	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	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	1	0	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	0	1	0	1	0	1	1	1	0	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	0	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	0	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	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	1	0	0	1	1	0	1	0	0	1	0	34	3	

A crucial property of ordered circulant matrices is the clear and simple relationship between their row index i and the absolute cyclic shift of the matrix pattern (MP) located in that row—a shift determined by the set of m symbols that make up the pattern:

$$H_2^i \alpha^0 = b_i, \quad (6)$$

where $b_i = [x_{i,k}, k = 0, \dots, m-1]$ – the initial block of the MS located in the i -th row of the circulant matrix.

Another important property of an ordered circulant matrix is the cyclic shift of the sequence of elements of multiplicative groups. $H_2^x \mathfrak{S}_{m,n}$ ($x = 0, m, 2m, \dots$) by one element to the right each time the next element of the group is chosen as the generator, resulting in N possible versions of this matrix. In any of these, the rows from the i -th to the $(i + m - 1)$ -th will contain the elements of the multiplicative group of a Galois field, cyclically shifted by i symbols relative to $\mathfrak{S}_{m,2}$, where i can take any value from 1 to $(N - 1)$.

Transformation of a circulant matrix into a matrix consisting of Walsh functions

Let's rearrange the columns of the matrix $\mathfrak{S}_{m,2,c}$ for any value α^0 in increasing order of the values of the elements of the multiplicative group of a Galois field $[\alpha^k]_{10}$, formed on the basis of H_2 at the same value α^0 [10, 11]. As a result $\mathfrak{S}_{m,2}$ will be converted into a matrix R_{ma} , the columns of which form a so-called simple binary code, while the rows are analogues of Rademacher functions [12, 13], excluding the zero symbol when indexing the symbols starting from zero: $r_{0a}, r_{1a}, \dots, r_{(m-1)a}$. Matrix $R_{ma} = [r_{0a} \ r_{1a} \ \dots \ r_{(m-1)a}]^T$ at $m = 5$ shown in Table 6.

Table 6

Analogues of Rademacher functions for $m = 5$

k	0	1						7	8					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																	1	1							
r_{1a}	0	0						1	1																	1	1							
r_{2a}	0	0						0	0																	0	0							
r_{3a}	0	1						0	0																	0	0							
r_{4a}	1	0						0	1																	0	1							

Then $\mathfrak{S}_{m,2,c}$ is transformed into a matrix

$$W_{m,p(1,0)} = \begin{bmatrix} R_{ma} \\ H_2^m R_{ma} \\ H_2^{2m} R_{ma} \\ \dots \\ H_2^{C(N)m} R_{ma} \end{bmatrix} = \begin{bmatrix} I_m R_{ma} \\ H_2^m R_{ma} \\ H_2^{2m} R_{ma} \\ \dots \\ H_2^{C(N)m} R_{ma} \end{bmatrix} = \begin{bmatrix} I_m \\ H_2^m \\ H_2^{2m} \\ \dots \\ H_2^{C(N)m} \end{bmatrix} R_{ma}, \quad (7)$$

where $W_{m,p(1,0)}$ – an extended Walsh function matrix without a zero symbol, with elements (0, 1), containing a certain number of repeating rows; I_m – identity matrix of size $m \times m$.

Matrix rows $H_2^x R_{ma}$ ($x = m, 2m, \dots$) are combinations of sums of the matrix rows R_{ma} upon addition of the symbols modul 2. As is well known, such sums form Walsh functions (excluding the zero-valued functions, when the symbols are indexed starting from zero).

In order to determine how they are ordered in (7), let us consider the matrix

$$H = \begin{bmatrix} H_2^m \\ H_2^{2m} \\ \dots \\ H_2^{C(N)m} \end{bmatrix}, \quad (8)$$

We will show that its rows form the multiplicative group of a Galois field constructed based on H_1 . Indeed,

$$\begin{aligned} H &= (H^T)^T = [((H_2^T)^T)^m \quad ((H_2^T)^T)^{2m} \quad \dots \quad ((H_2^T)^T)^{C(N)m}]^T = \\ &= [(H_1^T)^m \quad (H_1^T)^{2m} \quad \dots \quad (H_1^T)^{C(N)m}]^T = \begin{bmatrix} (H_1^m)^T \\ (H_1^{2m})^T \\ \dots \\ (H_1^{C(N)m})^T \end{bmatrix}, \end{aligned} \quad (9)$$

since $H_2^T = H_1$. In addition, we take into account that

$$(H_1)^m = (H_1)^{m-1} H_1 = (H_1)^{m-1} \begin{bmatrix} 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & \dots & 0 & a_1 \\ 0 & 0 & \dots & 0 & a_{m-2} \\ 0 & 0 & \dots & 1 & a_{m-1} \end{bmatrix}. \quad (10)$$

Assuming that the primitive element of the group coincides with the first column H_1 , that is $\alpha^0 = [0 \ 1 \ 0 \ \dots \ 0 \ 0]^T$, let us note that $H_1 \alpha^0 = \alpha^1 = [0 \ 0 \ 1 \ \dots \ 0 \ 0]^T$ and coincides with the second column H_1 etc.

The last element $\alpha^{m-1} = H_1 \alpha^{m-2} = H_1 [0 \ 0 \ \dots \ 0 \ 1]^T = [a_0 \ a_1 \ \dots \ a_{m-1}]^T$ coincides with the last column H_1 . Thus, $H_1 = [\alpha^0 \ \alpha^1 \ \dots \ \alpha^{m-1}]$. Then

$$(H_1)^m = [(H_1)^{m-1} \alpha^0 \quad (H_1)^{m-1} \alpha^1 \quad \dots \quad (H_1)^{m-1} \alpha^{m-1}] = [\alpha^{m-1} \ \alpha^m \quad \dots \quad \alpha^{2m-2}]. \quad (11)$$

Similarly, we obtain: $(H_1)^{2m} = (H_1)^{2m-1} H_1 = [\alpha^{2m-1} \ \alpha^{2m} \quad \dots \quad \alpha^{3m-2}]$ etc.

As a result

$$H = [\alpha^{(m-1)^T} \ \alpha^{m^T} \ \dots \ \alpha^{(2m-2)^T} \ \alpha^{(C(N)m-1)^T} \ \alpha^{C(N)m^T} \ \dots \ \alpha^{((C(N)+1)m-2)^T}]^T, \quad (12)$$

where $\alpha^0 = [0 \ 1 \ 0 \ \dots \ 0 \ 0]^T$, moreover H contains, in its rows, elements of a multiplicative group constructed based on the companion matrix H_1 – or $(m-1)$ -ro to $((C(N)+1)m-2)$ (at $m=5$ – from 4 to 33, in total 30), that is, the group represented in this matrix will be a truncated group. A primitive element of the truncated group will be $\alpha^{(m-1)} = H_1^{m-1} \alpha^0 = [a_0 \ a_1 \ \dots \ a_{m-1}]^T$.

From the formulas (7), (8), (12) it follows:

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

where $\mathbf{H}_p$ – augmented matrix $\mathbf{H}$, containing in its rows elements of a multiplicative group constructed based on $\mathbf{H}_1$ – from the element $\alpha^0 = [0 \ 1 \ 0 \dots 0 \ 0]^T$ to $((C(N) + 1)m - 2)$ element, total $(C(N) + 1)m - 1 > N$ elements. $\mathbf{H}_1[1 \ 0 \dots 0 \ 0]^T = [0 \ 1 \ 0 \dots 0 \ 0]^T$. In other words, by preserving within the matrix $\mathbf{W}_{m,p(1,0)}$ only N From the first few rows, one can construct a matrix consisting of Walsh functions – indexed starting from zero and excluding the zero-index function – in the following form:

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

moreover, all rows of the matrix $\mathfrak{Z}_{m,1}^T$ – these are elements of the multiplicative group of a Galois field constructed based on a matrix $\mathbf{H}_1$ with a primitive element $\alpha^0_{H_1} = [x_{0,0} \ x_{1,0} \ \cdots \ x_{m-1,0}]^T = [1 \ 0 \dots 0 \ 0]^T$.

Accordingly, to transform any cyclic shift of an M-sequence into a Walsh function (excluding the zero symbol, assuming a zero-based indexing), one must reorder its elementary symbols according to the ascending values of the elements of the multiplicative group of the Galois field, which is constructed based on the companion matrix of a polynomial of the form $\mathbf{H}_2$. In this context, the choice of a primitive element of the group is of great importance $\alpha^0_{H_2}$, depending on which, this cyclic shift can be transformed into any row of the matrix $\mathbf{W}_{m(1,0)}$. But given a specified $\alpha^0_{H_2}$ correspondence between the cyclic shifts of the MS being transformed and the rows of the matrix $\mathbf{W}_{m(1,0)}$ will be one-to-one; that is, an M-sequence with an absolute cyclic shift b will be transformed into a Walsh sequence (excluding the zero symbol, when indexed from zero) that is located in the i -th row of the matrix $\mathbf{W}_{m(1,0)}$, where i can be found by solving the equation: $\mathbf{H}_2^i \alpha^0_{H_2} = b$. At the same time, in the rows of the matrix

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

Analogous Rademacher functions are summed modulo 2 with weighting coefficients that are symbols of elements of the multiplicative group of a field constructed using the companion matrix of a polynomial $\mathbf{H}_1$ with a primitive element $\alpha^0_{H_1} = [1 \ 0 \dots 0 \ 0]^T$. In (15) $\oplus$ – notation for the operation of addition modul 2.

Accordingly, in the i -th row of the matrix $\mathbf{W}_{m(1,0)}$ the result is a Walsh function – excluding the zero-indexed one (when using zero-based numbering) – obtained by summing analogues of Rademacher functions, with weighting coefficients equal to the symbol values of the vector $\mathbf{x} = \mathbf{H}_1^i \boldsymbol{\alpha}^0_{H_1}$. Thus, any i -th row of the matrix (15)

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

is a Walsh function without a zero symbol when numbering them from zero, where

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

By replacing the MS symbols in $\mathfrak{S}_{m,n,\mathbb{U}}$ according to the rule $0 \rightarrow 1, 1 \rightarrow -1$, we get:

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

where $\mathbf{r}_0, \dots, \mathbf{r}_{(m-1)}$ – Rademacher functions with elements $\{1, -1\}$ (excluding zero), indexed starting from zero. In this context, the i -th row of the matrix $\mathbf{W}_{m(1,-1)}$ is defined as

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

where Powers of Rademacher functions are still calculated using formula (17).

By augmenting the Walsh function matrix (18) with a zero row (when indexing starts from zero) and an leftmost column – both consisting of ones – we obtain a complete set of orthogonal Walsh basis functions. The ordering of these functions within the matrix (excluding the zero row, which consists entirely of ones) is determined by the sequence of elements of the multiplicative group of a Galois field, defined modulo an irreducible primitive polynomial. $f_m(x)$ with coefficients $a_0, a_1, \dots, a_{m-2}, a_{m-1}$ and its companion matrix of the form $\mathbf{H}_1$ given a primitive element $\boldsymbol{\alpha}^0_{H_1} = [1 \ 0 \dots 0 \ 0]^T$.

Let us consider a matrix $\mathbf{W}_{m(1,-1)}^T$. It consists of rows in which the cyclic shifts of the sequences are ordered by row number; that is, each sequence begins with a block of m symbols corresponding to the binary representation of the row number in which it is located within the matrix $\mathbf{W}_{m(1,-1)}^T$. The columns of this matrix contain Walsh functions, ordered according to the elements of the multiplicative group of the Galois field corresponding to the matrix $\mathbf{H}_1$. Therefore, the columns of this matrix are rearranged in increasing order of the values of the elements of the multiplicative group of the Galois field, which is constructed based on the companion matrix of its polynomial of the form $\mathbf{H}_1$ given a primitive element $\boldsymbol{\alpha}^0_{H_1} = [1 \ 0 \dots 0 \ 0]^T$, transforms this matrix into a Hadamard matrix that contains no zero-valued columns or rows (when using zero-based indexing). Each i th row of this matrix consists of a Walsh function that contains no zero-valued symbols (again, using zero-based indexing).

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

where $h_{0,i}, h_{1,i}, \dots, h_{m-1,i}$ – values of the bits in the binary representation of the row number j ($h_{m-1,i}$ – least significant digit).

M-sequences (MS) synchronization

The first method for synchronizing the MS involves the following sequence of actions:

1) values of a discrete signal X_N . The signals obtained from the output of the in-phase or quadrature channel of the receiver are rearranged in increasing order of the values of the elements of the multiplicative group $\alpha^0_{H_2}, \alpha^1_{H_2} \dots, \alpha^{N-1}_{H_2}$ for any chosen $\alpha^0_{H_2}$; that is, the values X_N are written into a storage device, with the zero-indexed value – assuming a zero-based numbering scheme – being placed into the memory cell at the address $\alpha^0_{H_2}$, the first – into the cell with the address $\alpha^1_{H_2}$ and so on, with memory cells numbered from 0 to N ; in this arrangement, the zeroth memory cell remains unoccupied, since the multiplicative group of a Galois field lacks an element $00\dots 0$;

2) a unit is written to memory cell number 0, and the FAT of the resulting vector is performed;

3) the number of cell i is read, which contains the highest value of the FPA result (cell zero is ignored); thus, the row of the Hadamard matrix to which the cyclic shift of the original MS is converted is identified;

4) the reverse binary representation of i , that is $h_{m-1,i}h_{m-2,i} \dots h_{0,i}$ is considered as an element of the multiplicative group of a Galois field constructed based on the companion matrix H_1 of the polynomial being used, with respect to a primitive element $\alpha^0_{H_1} = [1\ 0 \dots 0\ 0]^T$;

5) the row number in which the obtained Walsh function is located is determined $W_{m(1,-1)}$, ordered according to the values of the elements of the multiplicative group of a Galois field, constructed on the basis of H_1 , (hereinafter referred to as groups 1), when solving the equation $H_1^i \alpha^0_{H_1} = [h_{m-1,j}h_{m-2,j} \dots h_{0,j}]^T$ relatively i ;

6) the required initial block of the MS is calculated using the formula: $b = H_2^i \alpha^0_{H_2}$.

In practice, solving the matrix equation and performing the calculations can be implemented using generators of the multiplicative groups of a Galois field, constructed based on the companion matrices of the original polynomial H_1 and H_2 (hereinafter referred to as Group 1 and Group 2). For the first of these $\alpha^0_{H_1} = [1\ 0 \dots 0\ 0]^T$, and for the second, the primitive element coincides with $\alpha^0_{H_2}$, from which the rearrangement of values began X_N . When the numbers at the outputs of these generators coincide, the output of the group 2 generator will yield the desired initial block for the MS (microprogram).

Another variant of this algorithm involves permuting the contents of the memory device cells after the execution of the BPA (basic microprogram algorithm), in accordance with the sequence of elements from group 1. That is, after completing step 2), one must launch the generator for this group using a primitive element $\alpha^0_{H_1} = [1\ 0 \dots 0\ 0]^T$ and move the contents of the 1st cell to the address $\alpha^0_{H_1}$, 2nd – to the address $\alpha^1_{H_1}$ etc. Next, it is necessary to determine the index of the cell with the maximum content.

This index will correspond to the target starting block of the memory area (MA) containing the values of the discrete signal X_N . The identified initial block must be loaded into the generator for group 2, the output of which will form the reference M-sequence.

The key components of an M-sequence synchronization device based on a Galois field primitive element (GFPE) approach are the generators for the multiplicative groups of the Galois field. It can be readily shown that the generators for group 1 and group 2 are, in fact, variations of an M-sequence generation device [10]. Indeed, by considering the structures of matrices H_1 and H_2 , one can derive recurrence relations for the elements of the corresponding multiplicative groups:

$$\text{– for the elements of group 1: } \begin{cases} x_{0,i} = a_0 x_{m-1,i-1}, (a_0 = 1), \\ x_{1,i} = x_{0,i-1} \oplus a_1 x_{m-1,i-1}, \\ \dots \\ x_{m-1,i} = x_{m-2,i-1} \oplus a_{m-1} x_{m-1,i-1}; \end{cases} \quad (21)$$

– for the elements of group 2:

$$\begin{cases} x_{0,i} = x_{1,i-1}, \\ x_{1,i} = x_{2,i-1}, \\ \dots \\ x_{m-1,i} = a_0 x_{0,i-1} \oplus a_1 x_{1,i-1} \oplus \dots \oplus a_{m-1} x_{m-1,i-1}. \end{cases} \quad (22)$$

Following the tradition of analyzing transformations within Galois fields – and considering the generators of maximal-length sequences (MLS) as shift registers based on D-flip-flops – we present the functional diagrams for the generators of multiplicative groups 1 and 2, as shown in Figure 1a, b.

As can be seen, the elements of the groups are read out in parallel from the outputs of all the flip-flops (memory cells) in the shift registers, while an MLS – with shifts corresponding to the structure of matrix H_1 or H_2 – is produced serially from each individual flip-flop. At the moment when the memory cells of the group 2 generator contain the required initial block of the input MLS, the sequence $x_{0,i}, x_{0,i+1}, x_{0,i+2} \dots$ from the output of its flip-flop D_0 will be generated synchronously with it, provided that this generator – much like the generator in group 1 – operates at the clock frequency of the input microprocessor.

Furthermore, it would be necessary for the duration of all the aforementioned transformations and operations to be zero, which is impossible. In reality, a digital synchronization device designed using modern microprocessor technology operates at the highest speed it can achieve, governed by its own clock frequency. It should be emphasized once again that, in this work, the generators of multiplicative groups are represented as shift registers using D flip-flops is merely a nod to tradition.

Thus, it is necessary, first, to record the total duration of all performed operations, expressed in units of the elementary pulse duration of the input multiplicative sequence (MS); second, to shift the generated reference MS – output from the D_0 flip-flop of the group 2 generator – by a corresponding number of elementary symbols; and third, to reduce the clock frequency of the generated reference MS to match the frequency of the input MS.

Consequently, the group 2 generator is well-suited for use as a source for a reference MS that is synchronous with the input MS, since the values of any m elementary symbols of the generated MS – as they emerge from the D_0 flip-flop – will correspond to the symbols of the multiplicative group 2 that were stored in the memory cells of its shift register at the moment the first of these m symbols appeared.

The second, simpler MS synchronization algorithm corresponds to the matrix $W_{m(1,-1)}^T$: values X_N . It is necessary to reorder the elements of the multiplicative group of a Galois field – constructed based on the companion matrix of a polynomial of a certain form – in ascending order H_1 , but only in the case of a primitive element $\alpha_{H_1}^0 = [1\ 0\ \dots\ 0\ 0]^T$. Upon completion of the BPA, the memory cell number – expressed in the binary numeral system – that contains the maximum value will serve as the starting block for the MS (microprogram) that was contained therein X_N .

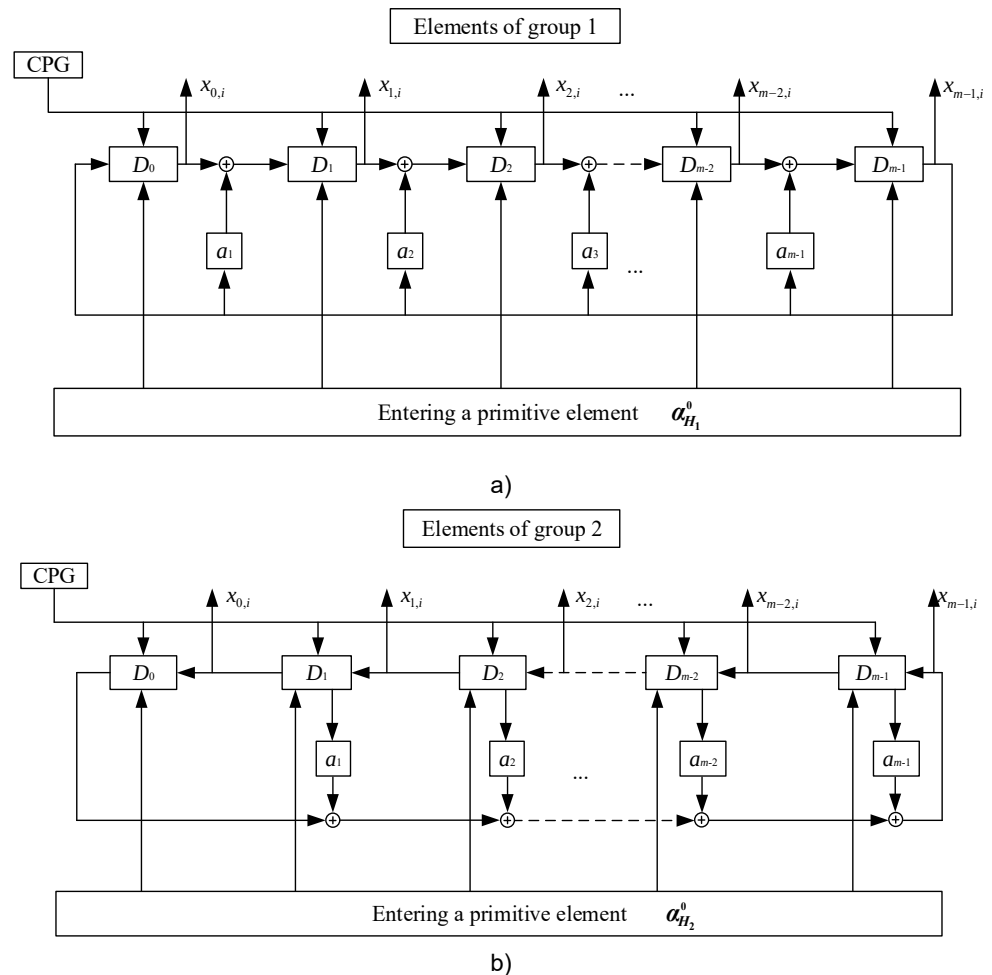


Fig. 1. Generators of multiplicative groups of a Galois field modulo an irreducible primitive polynomial with coefficients $a_0, a_1, \dots, a_{m-2}, a_{m-1}$; CPG – clock pulse generator

This initial block should be written into the memory cells of the generator of group 2, as a result of which the reference MS will be formed precisely from this initial block. Thus, in this case it is necessary to use both a group 1 generator and a group 2 generator.

We emphasize that the method of synchronizing the MP, based on the permutation of the symbols of the input MS in accordance with the multiplicative group formed on the basis of the matrix $\mathbf{H}_1$ (a simpler algorithm), assumes the only option for a permutation of this kind, and the multiplicative group on the basis of which it is made must always begin with $\alpha^0_{H_1} = [1\ 0\ \dots\ 0\ 0]^T$.

Permuting the sequence according to the same multiplicative group, but using a different primitive element, will not transform an M-sequence (maximal-length sequence) into a Walsh function. Furthermore, this approach assumes that the correspondence between a cyclic shift of an M-sequence and a Walsh function within a Hadamard matrix is the only one possible.

In contrast, permuting the symbols of an M-sequence according to a multiplicative group derived from the matrix $\mathbf{H}_2$ (a more complex algorithm) can be performed starting from any primitive element $\alpha^0_{H_2}$, as a result, any cyclic shift of the input MS can be reduced to any Walsh function, but for the chosen $\alpha^0_{H_2}$ – to only one such function. Furthermore, if the range of cyclic shifts – within which the shift of an input maximal-length sequence (MLS) might fall, or within which several of its cyclic shifts might occur due to multipath signal propagation – is known in advance, then permuting the symbols of the MLS according to multiplicative group 2 transforms them into Walsh sequences (excluding the zero-indexed symbol). In a matrix of such functions ordered according to multiplicative group 1, these resulting sequences appear consecutively. Consequently, given that only these specific functions are retained within a Hadamard matrix, the Fast Walsh-Hadamard Transform (FWHT) algorithm can be optimized, thereby reducing its computational complexity. Other cyclic shifts of the input MLS can be mapped to these same Walsh sequences (excluding the zero-indexed symbol) through an appropriate selection $\alpha^0_{H_2}$ group 2, according to which the symbols are rearranged.

Thus, if the range of possible cyclic shifts of the received sequence is known, an appropriate value can be selected $\alpha^0_{H_2}$ and transform it into one of several Walsh functions that appear in succession within a Hadamard matrix. Any other cyclic shift of an M-sequence with the same time-uncertainty region width can be mapped to a specific Walsh function from that same set, given an appropriate choice $\alpha^0_{H_2}$. Thus, to detect any cyclic shift of a binary pattern (BP), one can use a Walsh-Hadamard transform (WHT) within the same truncated basis of Walsh-Hadamard functions. If this truncated basis contains a relatively small number of Walsh functions, then computations may not be required.

Algorithm and block diagram of an M-sequence synchronization device

Time synchronization of an M-sequence reduces to implementing an algorithm for detecting and distinguishing its cyclic shifts. A simple rearrangement of the samples of the

received M-sequence, in accordance with the algorithm described in the previous section, yields a Walsh sequence, the symbols of which can be represented as a row vector of a matrix $\mathbf{W}_{m(1,-1)}$. As shown, this Walsh PRS corresponds uniquely to a specific cyclic shift of the original m-sequence, which is determined by its initial block of length m. The index i of the row in a Hadamard matrix of dimension 2^m – where this Walsh PRS is located – is $\mathbf{W}_{m(1,-1)}$, unambiguously linked to the code of the initial block of the original MS.

The square Hadamard matrix can be represented as the m-th Kronecker power of the second-order Hadamard matrix for $m=1$. As is known, when forming the Kronecker product of two matrices, each element of the second matrix is multiplied by all elements of the first matrix; as the number of matrices being multiplied increases, Kronecker products are found by a similar rule. Thus, if

$$\mathbf{W}_{1(1,-1)} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \mathbf{A} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \mathbf{A} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad (23)$$

for $\mathbf{W}_{m(1,-1)} = \mathbf{W}_{1(1,-1)}^m$. To use the fast Hadamard transform for multiplying the corresponding matrix by any given vector, one must utilize the factorization property of the Hadamard matrix—that is, the fact that it can be expressed as a product of simple, sparse matrices [14-16].

After the transformation of the MS, written as a string, we denote it as $\mathbf{X}_p \mathbf{X}_{np} \mathbf{X}_{np}$. Next, we convert the row into a column $\mathbf{X}_p^T$. After multiplying the matrix $\mathbf{W}_{m(1,-1)} \mathbf{X}_{np}^T \mathbf{X}_{np}^T$. Using this column, we obtain a column vector, which we denote as $\mathbf{Y}$. The maximum value of this vector corresponds to the main peak of the autocorrelation function (ACF) of the MS. The index of this value, within the sequential numbering of the elements of the column vector $\mathbf{Y}$, corresponds to a cyclic shift of the original M-sequence. Note that, due to a fundamental property of the periodic autocorrelation function (ACF) of an M-sequence, the remaining elements of the vector $\mathbf{Y}$ are all equal to "minus 1."

Thus, the determination of the cyclic shift index for a received M-sequence is described by the expression:

$$C = \max_i (\mathbf{Y} = \mathbf{W}_{m(1,-1)} \mathbf{X}_p^T), \quad (24)$$

where $i = 1, \dots, 2^m$ – номер элемента столбца $\mathbf{Y}$.

According to (23) and (24), the algorithm for accelerated MS detection consists of multiplying a column of input signal samples by a factorized Hadamard matrix.

$$\mathbf{W}_{m(1,-1)} = \mathbf{B}_2^m, \quad (25)$$

where $\mathbf{B}_2^m$ – simple m-th power of a matrix $\mathbf{B}_2$ on the order of $2^m N_{SPM} = 2^m$. Matrix element values $\mathbf{B}_2^m$ are determined in accordance with Good's theorem on the factorization of matrices that are Kronecker powers [17]. One version of such a matrix is:

$$B_{2^m} = \begin{bmatrix} 1 & 1 & & & & \dots & 0 & 0 \\ 0 & 0 & & & & \dots & 0 & 0 \\ 0 & 0 & & & & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & & & & \dots & 1 & 1 \\ 1 & -1 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & \dots & 0 & 0 \\ 0 & 0 & & & & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & & & & \dots & 1 & -1 \end{bmatrix}, \quad (26)$$

Given the structure of the matrix B_{2^m} and (24), we obtain an algorithm for accelerated detection of MPs

$$C = \max(Y = W_{m(1,-1)} X_p^T = B_{2^m}^{m-1} Y_{m-1} = B_{2^m} [B_{2^m} \dots (B_{2^m} X_p^T)]), \quad (27)$$

From (27) it follows that at the first stage of implementing this approach it is necessary to calculate the column $Y_1 = B_{2^m} X_p^T$. The second stage involves calculating a column $Y_2 = B_{2^m} Y_1$, etc. The m -th stage involves calculating a column $Y = Y_m = B_{2^m}^{m-1} Y_{m-1}$. The final column contains the values of the periodic autocorrelation function (PACF) of the received maximal-length sequence (MLS), adjusted to account for the discrepancy between the length of the MLS and the length of the Walsh function. The resulting values can be interpreted as a complete set of cross-correlation function (CCF) values for Walsh-based pseudorandom sequences (PRS), each calculated at a single point – that is, with zero time shift. One of these values corresponds to the autocorrelation function (ACF). It is well known that Walsh-based PRSs are orthogonal at this point; consequently, all the calculated values are zero, with the exception of one.

Column calculation procedures $Y_1, Y_2, \dots, Y_m$ are identical and can be described by an elementary graph, based on the factorization algorithm for a Hadamard matrix. An analysis of this graph shows that, to determine the elements of column Y , the received sequence must first be converted into a Walsh pseudorandom sequence (PRS), with its symbols stored in random-access memory (RAM). Next, during the calculation of Y_1 , the values of the Walsh PRS symbols stored in adjacent RAM memory locations – specifically, locations 1 and 2, 3 and 4, 5 and 6, and so on – must be added and subtracted using an arithmetic unit (AU) connected to the RAM. The results of these additions and subtractions are then written back into the RAM. Moreover, the sums of the symbols are written into memory cells numbered from 0 to 2^{m-1} -th, and the differences of the same symbols are written into RAM memory cells with numbers from $(2^{m-1} + 1)$ to 2^m .

When calculating $Y_2, \dots, Y_m$ the operations used during the calculation are applied each time Y_1 . As a result, we determine the elements of the vector $Y_m = Y$, in which one of the elements is equal to the value of the main peak of the ACF of the Walsh PRS corresponding to the received pseudorandom sequence (PRS), while the remaining elements of Y correspond to the peak values of the CCF between this Walsh PRS and the rows of the Hadamard matrix, assuming no relative time shifts between them.

Figure 2 shows a block diagram of a device for detecting a noise-like signal, which implements the aforementioned operating algorithm. After conversion to video frequency, the samples of the pseudo-random sequence (PRS) and noise from the analog-to-digital

converter (ADC) output are written into the random-access memory (RAM). Each sample is stored in a memory cell whose address corresponds to an element of a Galois field – generated by a Galois field generator (GFG) associated with either "group 1" or "group 2" – which is connected to the RAM's input/output address buses via a switching element (K1). The GFG unit incorporates generators for both group 1 and group 2; these are used by the decision-making unit (DMU) to determine the time shift of the received PRS.

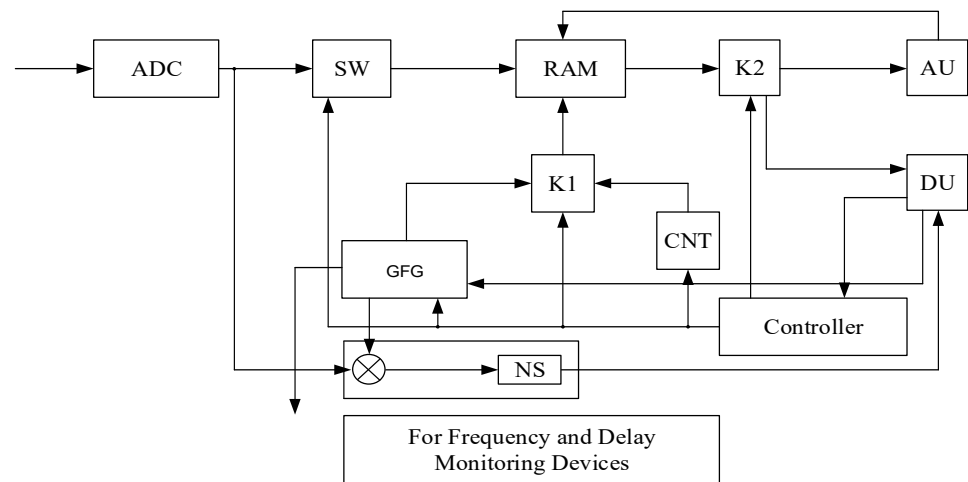


Fig. 2. Microprocessor accelerated synchronization unit

Thus, in accordance with the algorithm described above, a Walsh pseudorandom sequence (PRS) is written into the RAM. Neither its index within an ordered set of such sequences – for instance, as represented in a Hadamard matrix – nor its specific structure is known. To identify the index of the Walsh PRS within the Hadamard matrix, it is necessary to perform a high-speed multiplication of this matrix by the received additive mixture of noise and the unknown Walsh PRS. To achieve this, switch K1 is used to disconnect the pseudorandom sequence generator (PRSG) from the RAM and connect a counter (CNT). Simultaneously, switch K2 connects an arithmetic unit (AU) to the RAM data bus; the AU performs pairwise addition and subtraction of the values stored in the RAM, with the results then written back into available memory locations.

Following the algorithm defined by equations (26) and (27), after the m -th iteration of this procedure, the RAM will contain an auto-correlation function (ACF) of the maximal-length sequence (MLS) – cyclically shifted in a specific manner – summed with the samples resulting from the non-coherent accumulation of noise interference. At this stage, the position of the ACF's primary peak is unknown. The index of the memory location containing this primary peak determines the cyclic shift of the original MLS relative to the moment its samples began to be recorded in the RAM. Subsequently, switch K2 connects a decision unit (DU), which compares the values stored in the RAM and identifies the

memory location index where the maximum value was recorded. The relationship between this memory location index and the initial block of the MLS – from which the recording of its samples into the RAM commenced – is described in the preceding section.

Furthermore, it is necessary to account for the time required to calculate the autocorrelation function (ACF), as well as the fact that, during this interval, the incoming pseudorandom sequence (PRS) will have shifted in time; consequently, the initial segment of the PRS present at the receiver input will have changed. This new segment can be determined only with a certain margin of error, which depends on both the processing speed of the signal processor used in the device and the symbol rate (chip rate) of the PRS. This error manifests as an uncertainty equivalent to an unknown number of PRS chips. Therefore, an additional component – a serial or parallel correlator – is required. A pseudorandom sequence generator (PRSG) can serve as the reference PRS source, with the signal being tapped from one of the cells in its cyclic memory. This correlator, which can also function as a verification circuit, consists of a PRSG and a digital accumulator. In this way, a serial correlation search can be performed within the uncertainty region of the incoming PRS. Synchronization between the incoming PRS and the reference PRS is then verified using a decision unit.

Construction of a Gold PRS circulant matrix

The circulant matrices of Gold sequences are obtained by summing modulo two matrices $\mathfrak{J}_{m,2,c}$ [3] two so-called preferred MPs [18, 19]. Let, on the basis of the accompanying matrix H_2 of the first preferred polynomial and the primitive element $\alpha^0_{1H_2}$ a circulant matrix MS has been constructed $\alpha^0_{1H_2} \mathfrak{J}_{m,2,c}$, and based on a matrix H_2 , but of the second preferred polynomial and the primitive element $\alpha^{0+z}_{2H_2}$ – matrix $\alpha^{0+z}_{2H_2} \mathfrak{J}_{m,2,c}$. Then, the circulant matrices for the entire set of Gold sequences corresponding to these two preferred maximal-length sequences (excluding the sequences themselves) can be described as:

$$\mathfrak{J}_{m,2,c,g}(z) = \alpha^0_{1H_2} \mathfrak{J}_{m,2,c} \oplus \alpha^{0+z}_{2H_2} \mathfrak{J}_{m,2,c}, z = 0, \dots, N-1, \quad (28)$$

where $\oplus$ – notation for the operation of addition modul 2.

As an example, a circulant matrix of a Gold code constructed based on polynomials $f_5(x) = x^5 + x^4 + x^2 + x + 1$ and $f_5(x) = x^5 + x^3 + 1$ at $\alpha^0_{1H_2} = \alpha^0_{2H_2} = [1\ 0\ 0\ 0\ 0]^T$ and $z = 0$ is presented in Table 7. It is ordered, meaning that each subsequent row is cyclically shifted by one character relative to the preceding one [3].

Figure 3 shows the periodic cross-correlation function (PCCF) [20] $\chi_{PCCF}(i)$ Gold's PRS and MS, formed on the basis of the second of the two above polynomials. The PVCF values for negative i were obtained by mirroring the graph relative to the ordinate axis.

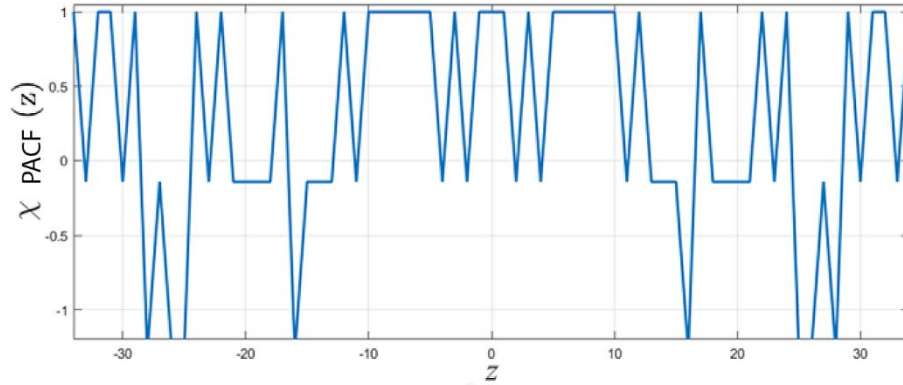


Fig. 3. Periodic autocorrelation function (PACF) of a Gold code

Thus, the matrix presented in Table 7 corresponds to a Gold sequence, as a three-valued periodic cross-correlation function (PCCF) is obtained.

Ordered circulant matrix of a Gold code for the selected values $\alpha^0_{1H_2}$, $\alpha^0_{2H_2}$ and z has the following form:

$$\mathfrak{Z}_{m,2,c,g}(z) = \begin{bmatrix} \mathfrak{Z}_{m,2}^1 \oplus \mathfrak{Z}_{m,2}^2 \\ H_{21}^m \mathfrak{Z}_{m,2}^1 \oplus H_{22}^m \mathfrak{Z}_{m,2}^2 \\ H_{21}^{2m} \mathfrak{Z}_{m,2}^1 \oplus H_{22}^{2m} \mathfrak{Z}_{m,2}^2 \\ \dots \\ H_{21}^{C(N)m} \mathfrak{Z}_{m,2}^1 \oplus H_{22}^{C(N)m} \mathfrak{Z}_{m,2}^2 \end{bmatrix}, \quad (29)$$

where $\mathfrak{Z}_{m,2}^1$ – matrix of m cyclic shifts of the first preferred MP, constructed based on the companion matrix H_{21} of its irreducible primitive polynomial, $\mathfrak{Z}_{m,2}^2$ – the corresponding matrix for the second preferred polynomial, constructed based on the companion matrix H_{22} of its irreducible primitive polynomial. In the notation for the companion matrices H_{21} and H_{22} , the first digit, 2, indicates that the matrices are of the type H_2 , while the second digit – 1 or 2 – denotes whether the matrix corresponds to the first or the second preferred polynomial.

It is evident that the columns of the first m rows of matrix (29) represent the sums of the powers of the primitive elements of two multiplicative groups; that is,

$$\mathfrak{Z}_{m,2}^1 \oplus \mathfrak{Z}_{m,2}^2 = \alpha^k_{1H_2} + \alpha^k_{2H_2}, k = 0, \dots, N - 1, \quad (30)$$

and meanings $[\alpha^k_{1H_2} + \alpha^k_{2H_2}]_{10}$ may coincide for different k . Furthermore, in (29), elements consisting solely of zeros may appear; that is, the sum of isomorphic maximal multiplicative groups of two distinct Galois fields does not form a multiplicative group.

Table 7

Circulant matrix of a Gold code corresponding to preferred polynomials

 $f_5(x) = x^5 + x^4 + x^2 + x + 1$ and $f_5(x) = x^5 + x^3 + 1$ at $\alpha^0_{1H_2} = \alpha^0_{2H_2} = [1\ 0\ 0\ 0\ 0]^T$ and $z = 0$

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	
$[\alpha^k_{1H_2} + \alpha^k_{2H_2}]_{10}$	0	0	1	2	4	8	16	1	2	5	11	23	15	30	29	27	23	15	30	28	24	16	0	1	2	4	9	18	4	8	16	i
$x_{1,0,k} \oplus x_{2,0,k}$	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0
$x_{1,1,k} \oplus x_{2,1,k}$	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	1
$x_{1,2,k} \oplus x_{2,2,k}$	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	2
$x_{1,3,k} \oplus x_{2,3,k}$	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	3
$x_{1,4,k} \oplus x_{2,4,k}$	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	4
$x_{1,5,k} \oplus x_{2,5,k}$	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	5
$x_{1,6,k} \oplus x_{2,6,k}$	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	6
$x_{1,7,k} \oplus x_{2,7,k}$	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	7
$x_{1,8,k} \oplus x_{2,8,k}$	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	8
$x_{1,9,k} \oplus x_{2,9,k}$	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	9
$x_{1,10,k} \oplus x_{2,10,k}$	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	10
$x_{1,11,k} \oplus x_{2,11,k}$	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	11
$x_{1,12,k} \oplus x_{2,12,k}$	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	0	0	0	1	12
$x_{1,13,k} \oplus x_{2,13,k}$	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	13
$x_{1,14,k} \oplus x_{2,14,k}$	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	14
$x_{1,15,k} \oplus x_{2,15,k}$	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	15
$x_{1,16,k} \oplus x_{2,16,k}$	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	16
$x_{1,17,k} \oplus x_{2,17,k}$	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	17
$x_{1,18,k} \oplus x_{2,18,k}$	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	18
$x_{1,19,k} \oplus x_{2,19,k}$	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	0	19
$x_{1,20,k} \oplus x_{2,20,k}$	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	0	1	20
$x_{1,21,k} \oplus x_{2,21,k}$	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	0	1	1	21
$x_{1,22,k} \oplus x_{2,22,k}$	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	0	1	1	1	22
$x_{1,23,k} \oplus x_{2,23,k}$	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	0	1	1	1	1	23
$x_{1,24,k} \oplus x_{2,24,k}$	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	0	1	1	1	1	0	24
$x_{1,25,k} \oplus x_{2,25,k}$	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	0	1	1	1	1	0	0	25
$x_{1,26,k} \oplus x_{2,26,k}$	0	1	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	0	1	1	1	1	1	0	0	0	26
$x_{1,27,k} \oplus x_{2,27,k}$	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	1	0	0	0	0	27
$x_{1,28,k} \oplus x_{2,28,k}$	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	1	0	0	0	0	1	28
$x_{1,29,k} \oplus x_{2,29,k}$	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	1	0	0	0	0	0	1	29
$x_{1,30,k} \oplus x_{2,30,k}$	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	1	0	0	0	0	0	1	0	30
$x_{1,31,k} \oplus x_{2,31,k}$	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	0	1	0	0	0
$x_{1,32,k} \oplus x_{2,32,k}$	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	0	1	0	0	1	1
$x_{1,33,k} \oplus x_{2,33,k}$	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	2
$x_{1,34,k} \oplus x_{2,34,k}$	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	3

Transformation of a Gold PRS circulant matrix into analogues of Rademacher functions

Having transformed the symbols $\alpha^k_{1H_2} + \alpha^k_{2H_2}$ according to the rule $0 \rightarrow 1, 1 \rightarrow -1$ and rearranging the columns (8) in ascending order $[\alpha^k_{1H_2} + \alpha^k_{2H_2}]_{10}$, By simultaneously summing identical values and replacing missing elements with zeros, we obtain functions that contain symbols other than 1 or -1, as well as symbols with zero values.

Thus, by rearranging the columns of the matrix shown in Table 7 according to this rule, we obtain the matrix presented in the rows of Table 8.

Table 8

The result of transforming a circulant matrix of a Gold code, ordered by the increasing values of the sum of multiplicative groups

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	i
r_{0a}	3	3	3	0	3	1	0	0	2	1	0	1	0	0	0	2	-3	0	-1	0	0	0	0	-2	-1	0	0	-1	-1	-1	-2	0
r_{1a}	3	3	3	0	3	1	0	0	-2	-1	0	-1	0	0	0	-2	3	0	1	0	0	0	0	2	-1	0	0	-1	-1	-1	-2	1
r_{2a}	3	3	3	0	-3	-1	0	0	2	1	0	1	0	0	0	-2	3	0	1	0	0	0	0	-2	1	0	0	1	-1	-1	-2	2
r_{3a}	3	3	-3	0	3	1	0	0	2	1	0	-1	0	0	0	-2	3	0	-1	0	0	0	0	-2	1	0	0	-1	1	1	-2	3
r_{4a}	3	-3	3	0	3	-1	0	0	2	-1	0	-1	0	0	0	-2	3	0	1	0	0	0	0	-2	1	0	0	-1	1	-1	2	4
r'_{5}	-1	3	1	0	1	-1	0	0	2	1	0	-1	0	0	0	2	1	0	1	0	0	0	0	-2	1	0	0	-1	1	-1	0	5
r'_{6}	1	1	-1	0	3	-1	0	0	0	1	0	-1	0	0	0	0	1	0	1	0	0	0	0	2	1	0	0	-1	1	-1	0	6
r'_{7}	3	-1	1	0	1	-1	0	0	2	1	0	1	0	0	0	0	-1	0	1	0	0	0	0	0	-1	0	0	1	1	-1	0	7
r'_{8}	1	1	-1	0	3	1	0	0	-2	1	0	-1	0	0	0	0	1	0	1	0	0	0	0	0	1	0	0	1	-1	1	0	8
r'_{9}	3	-1	3	0	-1	-1	0	0	0	1	0	-1	0	0	0	0	-1	0	1	0	0	0	0	0	1	0	0	1	1	1	0	9
r'_{10}	1	3	-1	0	1	-1	0	0	0	1	0	-1	0	0	0	0	1	0	-1	0	0	0	0	0	-1	0	0	1	1	1	2	10
r'_{11}	1	-1	-1	0	1	-1	0	0	0	-1	0	-1	0	0	0	2	3	0	1	0	0	0	0	0	1	0	0	1	-1	1	2	11
r'_{12}	1	-1	-1	0	-1	-1	0	0	2	1	0	1	0	0	0	2	-1	0	1	0	0	0	0	2	1	0	0	-1	1	1	0	12
r'_{13}	-1	-1	-3	0	3	1	0	0	-2	1	0	1	0	0	0	0	1	0	1	0	0	0	0	2	1	0	0	1	1	-1	2	13
r'_{14}	-1	-3	3	0	-1	1	0	0	0	1	0	1	0	0	0	2	-1	0	1	0	0	0	0	0	1	0	0	1	1	1	0	14
r'_{15}	-3	3	1	0	1	1	0	0	-2	1	0	1	0	0	0	0	-1	0	-1	0	0	0	0	2	1	0	0	-1	1	1	2	15
r'_{16}	1	1	1	0	-1	1	0	0	-2	-1	0	1	0	0	0	2	-1	0	1	0	0	0	0	0	1	0	0	1	1	-1	2	16
r'_{17}	1	1	1	0	-3	1	0	0	0	1	0	-1	0	0	0	2	1	0	-1	0	0	0	0	2	-1	0	0	1	1	1	0	17
r'_{18}	-1	1	-1	0	1	-1	0	0	0	-1	0	1	0	0	0	0	3	0	-1	0	0	0	0	2	1	0	0	1	-1	1	2	18
r'_{19}	-1	-1	1	0	-1	1	0	0	2	-1	0	1	0	0	0	2	1	0	-1	0	0	0	0	0	1	0	0	1	1	1	0	19
r'_{20}	-3	1	1	0	1	1	0	0	0	-1	0	-1	0	0	0	0	1	0	-1	0	0	0	0	2	1	0	0	1	1	1	2	20
r'_{21}	1	1	1	0	-1	-1	0	0	0	-1	0	1	0	0	0	2	-3	0	1	0	0	0	0	0	1	0	0	1	1	1	2	21
r'_{22}	1	1	-1	0	-1	1	0	0	-2	1	0	1	0	0	0	2	1	0	-1	0	0	0	0	2	-1	0	0	-1	1	1	2	22
r'_{23}	1	-1	1	0	-1	1	0	0	0	-1	0	1	0	0	0	2	1	0	-1	0	0	0	0	2	1	0	0	1	-1	-1	2	23
r'_{24}	1	1	1	0	-1	1	0	0	2	-1	0	1	0	0	0	2	-1	0	-1	0	0	0	0	2	-1	0	0	1	1	1	-2	24
r'_{25}	1	1	1	0	1	1	0	0	0	-1	0	1	0	0	0	-2	1	0	-1	0	0	0	0	2	-1	0	0	1	-1	1	2	25
r'_{26}	1	1	1	0	-1	1	0	0	2	-1	0	1	0	0	0	2	1	0	1	0	0	0	0	-2	-1	0	0	1	-1	1	0	26
r'_{27}	-1	1	-1	0	1	1	0	0	2	1	0	-1	0	0	0	0	3	0	1	0	0	0	0	2	-1	0	0	-1	-1	1	0	27
r'_{28}	1	-1	1	0	3	-1	0	0	2	1	0	1	0	0	0	0	-1	0	1	0	0	0	0	0	1	0	0	1	-1	-1	0	28
r'_{29}	-1	1	1	0	3	1	0	0	0	1	0	1	0	0	0	0	1	0	1	0	0	0	0	0	-1	0	0	-1	1	1	-2	29
r'_{30}	-1	1	3	0	1	1	0	0	2	1	0	1	0	0	0	-2	1	0	1	0	0	0	0	0	-1	0	0	-1	-1	-1	2	30
r_{0a}	3	3	3	0	3	1	0	0	2	1	0	1	0	0	0	2	-3	0	-1	0	0	0	0	-2	-1	0	0	-1	-1	-1	-2	0
r_{1a}	3	3	3	0	3	1	0	0	-2	-1	0	-1	0	0	0	-2	3	0	1	0	0	0	0	2	-1	0	0	-1	-1	-1	-2	1
r_{2a}	3	3	3	0	-3	-1	0	0	2	1	0	1	0	0	0	-2	3	0	1	0	0	0	0	-2	1	0	0	1	-1	-1	-2	2
r_{3a}	3	3	-3	0	3	1	0	0	2	1	0	-1	0	0	0	-2	3	0	-1	0	0	0	0	-2	1	0	0	-1	1	1	-2	3

As can be seen, half of the symbols in the transformed matrix – those in its second row – are either positive or zero, while the other half are either negative or zero. In the third row, the first 8 symbols are positive or zero, followed by 8 negative or zero symbols, then another 8 positive symbols, then 8 negative ones, and so on. That is, the first m rows of the circulant matrix of the Gold sequence, transformed according to the rule described

above, are analogs of the Rademacher functions (we denote them as r_{ia} , where $i = 0, \dots, (m-1)$ – function number), but the remaining rows of the original circulant matrix do not reduce to analogues of Walsh functions (excluding the zero symbol, when indexed from zero). Let us denote them as r'_i , where $i = m, \dots, (C(N) + 1)m - 1$, $C(N) = \left(\frac{A(N)}{m}\right) - 1$, $A(N)$ – a number as close as possible to N that is perfectly divisible by m and satisfies the inequality $A(N) > N$ [3].

But the functions r'_i can be reduced to analogs of Rademacher functions by choosing the corresponding primitive elements of the multiplicative groups. That is, by choosing $\alpha^0_{1H_2}$ and $\alpha^0_{2H_2}$ and by rearranging the columns of the Gold code's circulant matrix in ascending order $[\alpha^k_{1H_2} + \alpha^k_{2H_2}]_{10}$, we transform its first m rows into a matrix of analogues of Rademacher functions. However, if the columns of this matrix are permuted, starting from the element $\alpha^m_{1H_2} + \alpha^m_{2H_2}$, then the second m rows of the circulant matrix of the Gold code are transformed into analogs of the Rademacher functions. When rearranging starting from $\alpha^{2m}_{1H_2} + \alpha^{2m}_{2H_2}$ we transform the following m rows, etc.

This approach to mapping cyclic shifts of a Gold code to analogues of Rademacher functions is meaningful only if there exists a fast algorithm for multiplying a matrix of Rademacher functions by a vector – an algorithm whose computational complexity, in terms of the number of elementary mathematical operations, is significantly less than mN , given that mN is the complexity associated with multiplying a matrix of size $m \times N$ per column.

Gold's fast PRS synchronization algorithm

This algorithm effectively boils down to the accelerated multiplication of a matrix of Rademacher functions and a transformed Gold PRS.

At $m = 5$ the gain in the number of elementary arithmetic operations is approximately 1.84, compared to simple multiplication of the metric by the vector, but for typical PRS lengths used in constructing, for example, navigation codes, it is more significant – for $N = 511$ ($m = 9$) the winnings are 3 times, and when $N = 1023$ ($m = 10$) – 3.4 times [21].

The proposed algorithm for synchronizing Gold sequences based on FPA for a given cyclic shift of preferred MSs z is as follows: in order to ensure the possibility of synchronizing the entire set of Gold sequences, for the formation of which this pair of preferred MPs is used, select $\alpha^0_{1H_2}$ and $\alpha^0_{2H_2}$ multiplicative groups of their Galois fields and find the sums $\alpha^k_{1H_2} + \alpha^{k(z)}_{2H_2}$, where $k(z) = k + z$ at $k + z \leq N$ and $k(z) = k + z - N$ at $k + z > N$, $k = 0, \dots, N - 1$;

1) rearrange the values of the input discrete signal X_N , containing a Gold sequence with an unknown cyclic shift, in order of increasing values $[\alpha^k_{1H_2} + \alpha^{k(z)}_{2H_2}]_{10}$, writing these symbols into memory cells with the corresponding numbers; if the write addresses for different symbols coincide, they are written into the same cell and summed; elements $[\alpha^k_{1H_2} + \alpha^{k(z)}_{2H_2}]_{10}$, consisting solely of zeros, these determine the writing of an input code symbol into the zero-indexed cell and its summation with any symbols previously stored therein; the contents of any remaining empty cells are set to zero;

2) the resulting vector – whose symbol values are stored in the memory unit – is multiplied by a matrix of Rademacher functions; the resulting m values from this multiplication correspond to m values of the periodic autocorrelation function (PACF) of the Gold sequence;

3) to identify the primary peak of the PACF, it is advisable in this case to employ a threshold-based algorithm; if this peak is found among the calculated PACF values, the synchronization procedure is complete; otherwise, the next step is performed;

4) values X_N they are rearranged once again according to the rule described above, but this time in order of increasing values $[\alpha^{k+m}_{1H_2} + \alpha^{k(z)+m}_{2H_2}]_{10}$; After multiplying the resulting vector by the matrix of Rademacher functions, we obtain the following m values of the periodic autocorrelation function (PACF) for the Gold sequence, etc.

5) to synchronize another Gold sequence, it is necessary to change the value $z = 0, \dots, N - 1$.

Following the algorithm described above, the periodic autocorrelation function (PACF) of a Gold-sequence-based pseudorandom sequence (PRS) was calculated; its circulant matrix is presented in Table 7. The corresponding plot is shown in Figure 4, while Figure 5 displays the PACF of this Gold-sequence-based PRS, obtained by simply multiplying its circulant matrix by its first row (transposed into a column vector).

The slight discrepancy between the PACFs of the same sequence, when calculated using different methods, is attributable to the differing lengths of the Gold-sequence-based PRS and the Rademacher-Walsh function. The traditional method for calculating the periodic autocorrelation function (PACF), the reference pseudo-random sequence (PRS) must be shifted by one symbol at a time relative to the values of the received discrete signal, with each shift followed by the calculation of a single PACF value – a process that requires N multiply-accumulate operations. Consequently, computing the entire PACF necessitates N shifts of the reference PRS relative to the received signal and a total of N^2 multiply-accumulate operations.

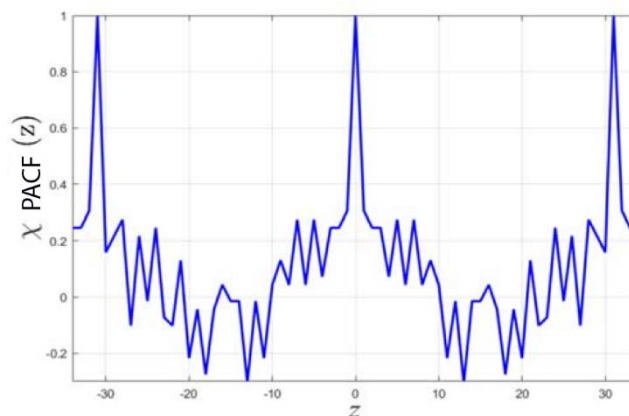


Fig. 4. Result of the accelerated computation of the periodic autocorrelation function (PACF) of a Gold code ($m = 5$)

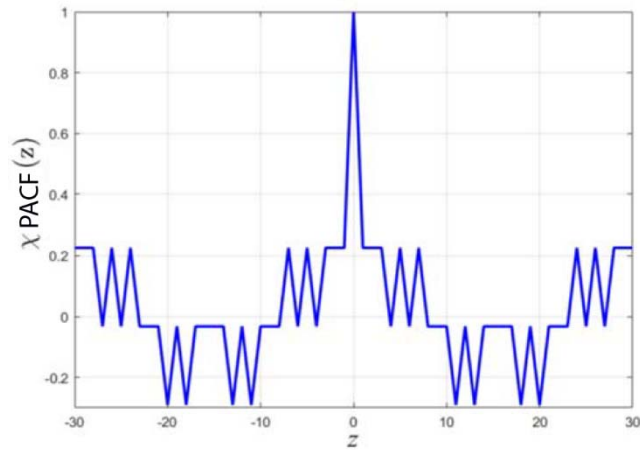


Fig. 5. Aperiodic Autocorrelation Function (AACF) of a Gold code ($m = 5$)

In the proposed algorithm, the number of permutations of the sequence's symbols is equal to $\frac{A(N)}{m}$, following each of these, m values of the periodic autocorrelation function (PACF) are computed simultaneously, requiring significantly fewer elementary summation operations than the traditional method for calculating m PACF values. The reduction in the number of arithmetic operations achieved by the proposed algorithm, compared to the traditional one, as a function of m . The rule for permuting the symbols of the input discrete signal is determined by the same Gold sequence generator used to produce the reference signal in the traditional PACF calculation algorithm.

Gold PRS accelerated synchronization device

The difference between this device and the one shown in Figure 2 is that a generator is used to write input signal samples into the RAM $\alpha^k_{1H_2} + \alpha^k_{2H_2}$. Furthermore, before each write operation to a RAM cell, its current content is added to the new value being written from the receiver input. The corresponding block diagram of the device is shown in Figure 6.

Let us examine the sequence generator. $\alpha^k_{1H_2} + \alpha^k_{2H_2}$. It corresponds to a version of a Gold code generator. Having derived the recurrence relations for the elements of a Gold code, let us present the generator $\alpha^k_{1H_2} + \alpha^k_{2H_2}$ as shown in Figure 7. This sequence originates from the outputs of the adders of the MS elements $x^1_{0,i+z} \oplus x^2_{0,i+z}$.

Conclusion

1. The algorithm for permuting the values of a discrete signal when transforming it into a row of a Walsh function matrix, as well as the method for identifying the cyclic shift of the corresponding PRS (pseudorandom sequence) after performing a Fast Walsh-Hadamard Transform (FWHT), depend on the choice of the circulant matrix structure for that PRS.

2. A circulant matrix MP , whose rows begin with blocks of binary symbols corresponding to the decimal indices of these rows (under binary-coded decimal representation), can be transformed into a Hadamard matrix – excluding the zero-indexed row and column – by permuting the matrix columns according to the elements of the unique multiplicative group of an extended Galois field. The method for constructing this group is illustrated in Figure 1a and corresponds to the form H_1 of the companion matrix associated with the original irreducible primitive polynomial; this transformation holds specifically when the primitive element of this group is assigned a particular value $\alpha^0_{H_1} = [1\ 0\ \dots\ 0\ 0]^T$.

3. Any of the N ordered circulant matrices of an M-sequence (where N is the length of the M-sequence) can be transformed into a matrix consisting of Walsh functions, ordered according to the powers of the multiplicative group of an extended Galois field. In this process, the columns of the circulant matrix must be permuted in increasing order of the elements of the Galois field's multiplicative group, corresponding to the form of the matrix H_2 . Furthermore, any cyclic shift of an M-sequence can be mapped to any Walsh function (excluding the one consisting of zeros, when indexed starting from zero), depending on the choice of the primitive element $\alpha^0_{H_2}$ of this group, which determines the structure of the circulant matrix. But for a given value $\alpha^0_{H_2}$ there is a one-to-one correspondence between a cyclically shifted M-sequence and a Walsh function (excluding the zero symbol), assuming both are indexed starting from zero. Consequently, all possible circulant matrices derived from an M-sequence – where each subsequent row is a cyclic shift of the preceding row by one symbol – can be reduced to the same matrix of Walsh functions (excluding zero symbols). In this representation, the functions are indexed from zero and ordered according to the powers of the elements of the multiplicative group of a Galois field, defined by a primitive element $\alpha^0_{H_1} = [1\ 0\ \dots\ 0\ 0]^T$, to the corresponding companion matrix of a polynomial of the form H_1 . Let us also note an important property of this matrix transformation: if, for the chosen $\alpha^0_{H_2}$, which defines the structure of a circulant matrix whose rows are ordered according to the cyclic shifts of an M-sequence, a certain i -th row of this matrix corresponds to the u -th row of a Walsh function matrix (excluding the zero-index row, when indexed starting from zero); thus, if one chooses as a primitive element $\alpha^{0+l}_{H_2}$ the same row of the circulant matrix is reduced to $(u + l)$ -th a row of a matrix of Walsh functions.

4. A Hadamard matrix can be obtained from a matrix of Walsh functions – ordered according to the powers of the maximal multiplicative group of a Galois field – by permuting its rows in increasing order of the values of the elements of this group, and by adding a zero row and a zero column (using zero-based indexing).

5. Any of the methods for transforming an M-sequence (according to the rules described in points 2 and 3) allows it to be converted into a Walsh function – excluding the zero symbol when using zero-based indexing. By subsequently appending this zero symbol and applying a Fast Walsh-Hadamard Transform (FWHT) to the resulting vector, one can efficiently compute the periodic autocorrelation function (PACF) of the M-sequence, with an adjustment made for the difference in length between the M-sequence and the Walsh sequences. This approach offers a computational complexity advantage of a factor of N/m compared to the traditional algorithm for calculating the discrete convolution of an M-sequence.

6. The first m rows of any ordered circulant matrix derived from a Gold sequence can be transformed into analogues of Rademacher functions by permuting the matrix columns according to the ascending order of the sums of the elements of the maximal multiplicative groups associated with the two preferred irreducible primitive polynomials used to construct the code. The structure of these groups is determined by the companion matrices of the preferred polynomials, specifically those of the form H_2 . Shifting the primitive elements of the constituent multiplicative groups by m positions results in the next m rows of the original matrix becoming Rademacher functions; a shift by $2m$ positions yields the same result for the subsequent m rows, and so on.

7. Transforming a Gold sequence allows for the rapid computation of its periodic autocorrelation function (PACF) using a fast transform algorithm (FTA) based on a truncated Walsh-Hadamard function basis; the gain in terms of the number of elementary operations depends on the length of the pseudorandom sequence (PRS) $N = 2^m - 1$.

REFERENCES

- [1] Wu Shi Dao, "Complex signal detection and vector-matrix multiplication algorithm," *Synchroinfo Journal* **2026**, vol. 12, no. 2, pp. 8-25.
- [2] S.F. Gorgadze, Sh.D. Wu., A.V. Ermakova, "Synchronization of M-sequences based on the fast Hadamard transform," *Radio Engineering and Electronics*. 2024. Vol. 69. No. 2, pp. 122-136.
- [3] S. F. Gorgadze, Sh. D. Wu, A. V. Ermakova, "Synchronization of Gold Sequences Based on Fast Transformation in a Truncated Basis of Walsh-Hadamard Functions," *Radio Engineering and Electronics*. 2024. Vol. 69. No. 2, pp. 137-145.
- [4] Sh.D. Vu, S.F. Gorgadze, "A device for accelerated acquisition of a noise-like signal," *Information Society Technologies. Proceedings of the XVI International Industry-Specific Scientific and Technical Conference*. Moscow, 2022, pp. 88-90.
- [5] S.F. Gorgadze, Sh.D. Vu, "Certificate of State Registration of a Computer Program No. 2024663135 (Russian Federation). Program for constructing circulant matrices for M-sequences and Gold codes based on multiplicative groups of extended Galois fields," applicant and copyright holder: MTUCI. No. 2024661989; filed May 28, 2024; published June 4, 2024.
- [6] V. P. Ipatov, "Wideband Systems and Code Division Multiple Access: Principles and Applications," Moscow: Tekhnosfera, 2007. 487 p.
- [7] W. Peterson, E. Weldon, "Error-Correcting Codes," Moscow: Mir, 1976. 593 p.
- [8] M. B. Sverdlik, "Optimal Discrete Signals," Moscow: Sovetskoye Radio, 1975. 200 p.
- [9] V. M. Smolyaninov, "Discrete Multiplicative Group Signals and Their Connection to Group Codes," *Radio Engineering and Electronics*. 1985. Vol. 30. No. 12, pp. 2391-2394.
- [10] V.V. Losev, E.B. Brodskaya, V.I. Korzhik, "Search and Decoding of Complex Discrete Signals,"; ed. by V.I. Korzhik. Moscow: Radio i Svyaz, 1988. 224 p.

-
- [11] V.V. Losev, V.D. Dvornikov, "Recognition of Address Sequences Using Fast Transforms," *Radio Engineering and Electronics*. 1983. No. 8, pp. 15-40.
- [12] A. M. Trakhtman, V. A. Trakhtman, "Fundamentals of the Theory of Discrete Signals on Finite Intervals," Moscow: Sovetskoye Radio, 1975. 205 p.
- [13] S. F. Gorgadze, "Asymmetric Modifications of the Generalized Fast Fourier and Fourier-Hadamard Transforms," *Radio Engineering and Electronics*. 2005. Vol. 50. No. 3, pp. 302-308.
- [14] Y. Be'ery, J. Snyders, "A recursive Hadamard transform optimal soft decoding algorithm," *Journal of Algebraic and Discrete Methods*. 1987. Vol. 8. No. 4, pp. 778-789.
- [15] V. M. Smolyaninov, L. E. Nazarov, "Specifics of spectral analysis in the recognition of discrete signals based on binary codes," *Radio Engineering and Electronics*. 1988. Vol. 32. No. 11, pp. 2341-2347.
- [16] V. M. Smolyaninov, L. E. Nazarov, "Optimization of the spectral analysis algorithm for the recognition of discrete multiplicative signals," *Radio Engineering and Electronics*. 1989. Vol. 35. No. 12, pp. 2651-2653.
- [17] V.Y. Mikhaylov, R.B. Mazepa, "Estimation of the Features of Application of the M-Sequences Subset with the Possibility of Joint Processing. DOI: 10.1109/SYNCHROINFO 51390.2021.9488414," *2021 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*. 2021. P. 1-6.
- [18] V.S. Kuznetsov, I.V. Shevchenko, A.S. Volkov, A.V. Solodkov, "Generation of Gold code ensembles for direct-sequence spread-spectrum systems," *Proceedings of the Moscow Aviation Institute (MAI)*. 2017. No. 96. <http://trudymai.ru/>.
- [19] V.S. Kuznetsov, K.A. Mordasov, "Fast decoding based on passive matched filtering of long pseudorandom codes," *Proceedings of Higher Educational Institutions. Electronics*. 2010. No. 1 (81), pp. 57-62.
- [20] L.E. Varakin, "Communication Systems Using Noise-Like Signals," Moscow: Radio i Svyaz, 1985. 384 p.
- [21] V.Y. Mikhaylov, R.B. Mazepa, "Using transformations in Galois fields for fast delay-based searching of Gold sequences," *T-Comm*. 2018. Vol. 12, no. 4. P. 4-9.