Synthesis method of circulant polynomial encoding matrices for the implementation of code-division multiplexing

P O Vinar¹, S V Rabin² and A V Rabin³

Saint-Petersburg State University of Aerospace Instrumentation (SUAI), 67, ul. Bolshaya Morskaya, lit. A, St. Petersburg, 190000, Russia

E-mail: polinavinar@yandex.ru¹, rabinserge@gmail.com², alexey.rabin@guap.ru³

Abstract. The method of the synthesis of circulant polynomial matrices for the implementation of the operation of code combining of channels on the transmitting side of the communication system has been developed. The structure of these matrices is the basis for reducing the complexity of encoder schemes and, consequently, the radiated power of radio transmitters of subscriber devices. The research results can be applied in communication systems with multiple access, with a wide coverage area, high quality of data transmission, high noise immunity, stability of communication channels from interception and eavesdropping.

1. Introduction

At present, there is a significant increase in the demand and importance of information technologies, and the amount of information transmitted via digital communication channels is growing strongly [1, 2]. Therefore, there is a need to develop a switching equipment that would provide fast and high-quality connection of a device and subscribers, as well as comply with modern standards for switching digital transmission channels [3-5].

Currently, the desire for the development of code-division access technology is explained by an increase in subscriber density, resistance to interference, as well as a high degree of protection of transmitted data from unauthorized access [6-8].

The complexity of transmitting and receiving devices can be reduced by using simple channel division and combining schemes. The simplicity of these schemes can be ensured by using special matrices. This paper discusses the procedure for constructing the circulant encoding matrix for some special cases.

2. Requirements for encoding matrices

Let’s consider circulant matrices that have the determinant of the form $D^{i}$, where $i$ is a non-negative integer. This procedure is quite simple if the method of calculating the determinant for circulant matrices is known. A sufficient condition, under which the procedure for finding the encoding matrix is greatly simplified, is presented in the work [9]. The proposed method summarizes this result into more general cases.

The circulant encoding matrix is as follows:
where \( g_i(D) \) for \( i = 1, 2, \ldots, N \) are some polynomials of finite degree of the variable \( D \). Therefore, the determinant of the matrix \( G(D) \) is uniquely determined by the polynomials \( g_1(D), g_2(D), \ldots, g_N(D) \).

It is assumed that the coefficients of the polynomials \( g_1(D), g_2(D), \ldots, g_N(D) \) take values from the finite field \( GF(2) \), that is, the problem of channel division when transmitting information over a binary communication channel was considered. More generally, it is assumed that the coefficients of these polynomials belong to the finite field \( GF(p) \) or even to some algebraic extension of this field. Nevertheless, the requirements for the encoding matrix remain the same. A similar approach was used to synthesize orthogonal matrices in order to build codes and provide a noise immunity for communication systems [10-13].

3. Synthesis of encoding matrices

Firstly, we will limit ourselves to the case when the number of users is \( N = 2^l \). Let’s consider a triangular matrix \( P_q \) of order \( N \), where \( q = \log_2 N \), with an iterative structure

\[
P_q = \begin{pmatrix} p_q^{-1} & p_q^{-1} \\ 0 & p_q^{-1} \end{pmatrix},
\]

and the original matrix has the form

\[
P = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.
\]

It is easy to see that \( P_q \) is a triangular matrix with all diagonal elements equal to one. Therefore, the determinant \( \det(P_q) \) is equal to one for all \( q \).

It can be noted that the encoding matrix (1) can be written in the following form

\[
G(D) = \begin{pmatrix} G_A(D) & G_B(D) \\ G_B(D) & G_A(D) \end{pmatrix},
\]

where \( G_A(D) \) and \( G_B(D) \) are submatrices of order \( 2^{q-1} \).

For example, let’s take a matrix of order eight

\[
G(D) = \begin{pmatrix} g_1(D) & \ldots & g_4(D) & g_5(D) & \ldots & g_8(D) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ g_6(D) & \ldots & g_3(D) & g_2(D) & \ldots & g_5(D) \\ g_7(D) & \ldots & g_4(D) & g_3(D) & \ldots & g_6(D) \\ \vdots & \ddots & \vdots & \ddots & \ddots & \vdots \\ g_2(D) & \ldots & g_5(D) & g_6(D) & \ldots & g_1(D) \end{pmatrix},
\]

The corresponding submatrices have the form

\[
G_A(D) = \begin{pmatrix} g_1(D) & g_2(D) & g_3(D) & g_4(D) \\ g_8(D) & g_1(D) & g_2(D) & g_3(D) \\ g_7(D) & g_8(D) & g_1(D) & g_2(D) \\ g_6(D) & g_7(D) & g_8(D) & g_1(D) \end{pmatrix},
\]
\[ G_{B_{1}}(D) = \begin{pmatrix} g_{5}(D) & g_{6}(D) & g_{7}(D) & g_{8}(D) \\ g_{4}(D) & g_{5}(D) & g_{6}(D) & g_{7}(D) \\ g_{3}(D) & g_{4}(D) & g_{5}(D) & g_{6}(D) \\ g_{2}(D) & g_{3}(D) & g_{4}(D) & g_{5}(D) \end{pmatrix}. \]

4. Properties of encoding matrices

Now consider the product \( P_{q} \cdot G(D) \cdot P_{q} \). We can check that we get a triangular matrix as a result. Truly,

\[
\begin{bmatrix} P_{q} \cdot G(D) \cdot P_{q} = \begin{pmatrix} P_{q-1} & P_{q-1} \\ 0 & P_{q-1} \end{pmatrix} \cdot \begin{pmatrix} G_{A}(D) & G_{B_{1}}(D) \\ 0 & G_{A}(D) \end{pmatrix} \cdot \begin{pmatrix} P_{q-1} & P_{q-1} \\ 0 & P_{q-1} \end{pmatrix} = \begin{pmatrix} P_{q-1} \cdot (G_{A}(D) + G_{B_{1}}(D)) \cdot P_{q-1} & P_{q-1} \cdot (G_{A}(D) + G_{B_{1}}(D)) \cdot P_{q-1} \\ 0 & P_{q-1} \end{pmatrix} \end{bmatrix}
\]

Note, that in the last triangular matrix on the main diagonal there are identical elements that have the following form:

\[ P_{q-1} \cdot (G_{A}(D) + G_{B_{1}}(D)) \cdot P_{q-1}. \]

We can make sure that the matrix \( (G_{A}(D) + G_{B_{1}}(D)) \) has exactly the same structure as the matrix (1).

In other words, this matrix can be written in the form

\[ (G_{A}(D) + G_{B_{1}}(D)) = \begin{pmatrix} G_{A_{1}}(D) & G_{B_{2}}(D) \\ G_{B_{1}}(D) & G_{A_{1}}(D) \end{pmatrix}. \]

Let’s illustrate this with an example of the encoding matrix \( G(D) \) from (3). After these transformations, the matrix \( (G_{A}(D) + G_{B_{1}}(D)) \) has the following form:

\[ G(D) = \begin{pmatrix} g_{1}(D) + g_{3}(D) & g_{2}(D) + g_{4}(D) & g_{5}(D) + g_{6}(D) & g_{7}(D) + g_{8}(D) \\ g_{4}(D) + g_{6}(D) & g_{5}(D) + g_{6}(D) & g_{7}(D) + g_{8}(D) \\ g_{3}(D) + g_{5}(D) & g_{4}(D) + g_{6}(D) & g_{7}(D) + g_{8}(D) \end{pmatrix}. \]

In other words, the submatrices \( G_{A_{1}}(D) \) and \( G_{B_{1}}(D) \) are written in this way:

\[ G_{A_{1}}(D) = \begin{pmatrix} g_{1}(D) + g_{3}(D) & g_{2}(D) + g_{4}(D) \\ g_{6}(D) + g_{4}(D) & g_{1}(D) + g_{3}(D) \end{pmatrix}, \]

\[ G_{B_{1}}(D) = \begin{pmatrix} g_{7}(D) + g_{5}(D) & g_{8}(D) + g_{4}(D) \\ g_{6}(D) + g_{5}(D) & g_{7}(D) + g_{5}(D) \end{pmatrix}. \]

This example shows that after transformation (4), the structure of the matrix \( (G_{A}(D) + G_{B_{1}}(D)) \) retained the structure of the original matrix \( G(D) \). For this reason, it can be shown that the multiplication of \( P_{q-1} \cdot (G_{A}(D) + G_{B_{1}}(D)) \cdot P_{q-1} \) in turn can be represented as follows:

\[
\begin{bmatrix} P_{q-1} \cdot (G_{A}(D) + G_{B_{1}}(D)) \cdot P_{q-1} & 0 \\ P_{q-1} \cdot G_{B_{1}}(D) \cdot P_{q-1} & P_{q-1} \cdot (G_{A}(D) + G_{B_{1}}(D)) \cdot P_{q-1} \end{bmatrix}
\]

Let’s substitute this representation of the matrix \( P_{q-1} \cdot (G_{A}(D) + G_{B_{1}}(D)) \cdot P_{q-1} \) into the multiplication (4). Then again we get a triangular matrix \( P_{q-1} \cdot G_{B_{1}}(D) \cdot P_{q-1} \), in which there are already four identical matrices of the form \( P_{q-2} \cdot (G_{A}(D) + G_{B_{1}}(D)) \cdot P_{q-2} \) on the main diagonal.
Continuing to analyze the process of replacing submatrices standing on the main diagonal with smaller submatrices, after \( q \) steps we obtain a lower triangular matrix of order \( N \), in which the sums of polynomials \( g_1(D) + g_2(D) + \ldots + g_N(D) \) are on the main diagonal.

From this we get that the determinant of the encoding matrix \( G(D) \) is equal to \((g_1(D) + g_2(D) + \ldots + g_N(D))^N\) [14].

The determinant of the encoding circulant matrix \( G(D) \) of order \( N = 2^i \) with elements \( g_1(D), g_2(D), \ldots, g_N(D) \) in each row is equal to \((g_1(D)^N + g_2(D)^N + \ldots + g_N(D))^N\), that is, \(\det(G(D)) = \sum_{i=1}^{N} g_i(D)^N\).

5. Implementation and extension of the synthesis’ method

Using the obtained result, we can simply calculate the determinants of circulant matrices of order \( 2^i \) with elements from the ring of polynomials in one variable over the finite field \( GF(2) \).

As an example, let’s assume that a circulant matrix of order eight is given in the following form

\[
\begin{pmatrix}
1 + D & 1 + D^2 & 1 + D & 1 + D + D^3 & 1 + D & 1 + D + D^2 & 1 & 1 + D + D^3 \\
1 & 1 + D + D^2 & 1 + D & 1 + D + D^3 & 1 + D & 1 + D + D^2 & 1 & 1 + D + D^3 \\
1 + D & 1 & 1 + D + D^2 & 1 + D & 1 + D + D^3 & 1 + D & 1 + D + D^2 & 1 \\
1 + D & 1 + D & 1 + D + D^2 & 1 + D & 1 + D + D^3 & 1 + D & 1 + D + D^2 & 1 \\
1 + D & 1 + D & 1 + D + D^2 & 1 & 1 + D + D^2 & 1 + D & 1 + D + D^2 & 1 \\
1 + D & 1 + D & 1 + D + D^3 & 1 & 1 + D + D^2 & 1 + D & 1 + D + D^2 & 1 \\
1 + D^2 & 1 + D & 1 + D + D^3 & 1 + D & 1 + D + D^2 & 1 & 1 + D + D^2 & 1 \\
1 + D^2 & 1 + D & 1 + D + D^3 & 1 + D & 1 + D + D^2 & 1 & 1 + D + D^2 & 1 \\
\end{pmatrix}
\]

It is simple to check that the sum of all the elements in each row of this matrix is equal to \( D^2 + D^3 \). In accordance with the previously proved formula, we obtain that the determinant of this matrix is equal to \( D^{16} + D^{24} \). It is difficult to calculate the determinant of this encoding matrix by conventional means.

Using the above method for calculating the determinants of circulant matrices of order \( 2^i \), it is relatively easy to choose an encoding matrix with the required properties. In the case of the finite field of characteristic two, in order to choose an encoding matrix of order \( 2^i \) with the required properties, it is enough to assign the elements of the matrix \( G(D) \) in such a way that the sum of the elements of each row is equal to the monomial \( D^i \), where \( i \) is a non-negative integer.

The considered sufficient condition for choosing the encoding matrix can be generalized to the case of a finite field by a simple module. So, if the finite field has characteristic three, then matrices of order \( N \), where \( N = 3^i \). The iterative matrix \( P_p \), by which the encoding matrix is reduced to a triangular shape, has the form

\[
P_q = \begin{pmatrix}
P_{q-1} & P_{q-1} & P_{q-1} \\
0 & 2P_{q-1} & P_{q-1} \\
0 & 0 & P_{q-1}
\end{pmatrix},
\]

and the original matrix for the field of characteristic three has the form

\[
P_1 = \begin{pmatrix}
1 & 1 & 1 \\
0 & 2 & 1 \\
0 & 0 & 1
\end{pmatrix}.
\]

As an example, let’s consider the encoding matrix, the elements of which are polynomials with coefficients from the finite field \( GF(3) \). Suppose that this matrix has the form
The sum of each row of this matrix is $D$, and therefore its determinant is $D^3$.

The presented restrictions on the size of circulant encoding matrices are not necessary, but they are sufficient conditions under which it is possible to simply calculate the value of the determinant of the encoding matrix. To make sure of this, let’s consider an example of an encoding matrix of a different order with elements from $GF(3)$, the sum of the elements in each row of which is $2 + D$, and its determinant is $2 + 2D + 2D^3$. This matrix has the form

$$G(D) = \begin{pmatrix} 2D & 2 + D & 2 & 1 + D \\ 1 + D & 2D & 2 + D & 2 \\ 2 & 1 + D & 2D & 2 + D \\ 2 + D & 2 & 1 + D & 2D \end{pmatrix}.$$ 

We can make sure that for circulant matrices of order $p^q$ over the finite field of characteristic $p$ the determinants are calculated in the same way in the case when the elements of the matrices are rational fractions. So, for a finite field of characteristic three, to obtain the determinant of a circulant matrix of order $3^q$ it is enough to calculate the sum of rational fractions of any row of the matrix and raise it to the power of $N = 3^q$.

Let’s consider the example. Let the matrix have the form:

$$G(D) = \begin{pmatrix} \frac{1 + 2D}{1 + D} & 1 + D & 1 \\ 1 & \frac{1 + 2D}{1 + D} & 1 + D \\ 1 + D & 1 & \frac{1 + 2D}{1 + D} \end{pmatrix}.$$ 

Adding the elements of one row of this matrix, we get $2D + 2D^3$. Therefore, the value of the determinant of this matrix is $2D^3 + 2D^6$. You can verify the validity of this result by directly calculating the value of the determinant of this matrix.

To confirm the considered fact, it is enough to bring all the elements of the matrix $G(D)$ to one common denominator, which can then be taken as the sign of the matrix. As a result, we obtain an encoding matrix, all elements of which are polynomials in the variable $D$. To this matrix, you can apply the above transformation to the triangular shape and get the desired result.

Unlike the previous encoding matrices, the last matrix has elements containing non-singular denominators. In this case, the output sequences obtained as a result of encoding are generally infinitely long and periodic, and, therefore, their Hamming weight can be arbitrarily large. It is rather difficult to analyze such sequences.

6. Conclusions
The advantage of the developed method is that it provides simple encoding schemes for combining channels on the transmitting side of the communication system. The simplicity of synthesized circulant matrices reduces the number of addition and multiplication operations in encoding operations.

The disadvantage is that all data transmission processes with subsequent channel division have to continue indefinitely, since their termination at an arbitrary time will lead to some kind of transient process. It will violate the verification relations on the receiving side of the system and lead to incorrect operation of the channel separation scheme for several cycles, the number of which depends on the degree of the polynomial standing in the denominator.
To avoid these difficulties, it is advisable to take the following measures. In the process of transmitting messages after channel division, the receiving side, having received the transmitted message, has to initiate the termination of the communication session. In this case, the receiving side has received all the necessary information, and the “transients” on the transmitting side no longer have any effect on the operation of other parallel communication channels.

The reliability of suggested approach is confirmed by the correspondence of the results of simulation modeling to theoretical proposals [15, 16].

Acknowledgments
The paper was prepared with the financial support of the Ministry of Science and Higher Education and of the Russian Federation, grant agreement No. FSRF-2020-0004, “Scientific basis for architectures and communication systems development of the onboard information and computer systems new generation in aviation, space systems and unmanned vehicles”.

References
[1] Proakis J G 2007 Digital communications (New York: McGraw Hill) 1150
[2] Sklar B 2017 Digital communications: fundamentals and applications Prentice Hall Communications Engineering and Emerging Technologies Series 1104
[3] Liang Y, Goldsmith A and Effros M 2009 Source-channel coding and separation for generalized communication systems IEEE Information Theory Workshop, Lake Tahoe, California 48
[4] Prucnal P R 2019 Optical code division multiple access: fundamentals and applications (CRC Press) 400
[5] Khina A, Gårding E R, Pettersson G M and Kostina V 2019 Control over Gaussian channels with and without source-channel separation IEEE Transactions on Automatic Control 64(9) 3690-706
[6] Talib M F, Rahman A K, Anuar M S, Rashidi C B M and Aljunid S A 2016 A novel hybrid optical code division multiple access in free space optical communication 6th International Conference on Photonics 7510039
[7] Cover T, El Gamal A and Salehi M 1980 Multiple access channels with arbitrarily correlated sources IEEE Transactions on Information Theory 26(6) 648-57
[8] Telang V P and Herro M A 1998 Error control coding for the N-user mod-2 multiple-access channel IEEE Transactions on Information Theory 44(4) 1632-42
[9] Davis P J 1994 Circulant matrices (New York: Chelsea, 2nd ed.) 250
[10] Rabin A V 2019 Encoding and decoding schemes in communication systems using orthogonal coding for noise immunity's increase (St. Petersburg: Proceedings of The Conference on Wave electronics and its application in information and telecommunication systems WECONF) 8840610
[11] Rabin A V 2019 Orthogonal coding for noise immunity's increase with the fixed code rate IOP Publishing: Journal of Physics. Conference Series 1333(2) 022013
[12] Rabin A V 2020 Matching orthogonal code symbols and modulation methods IOP Conference Series: Materials Science and Engineering 734(1) 012216
[13] Rabin A V 2020 Design of encoding and decoding devices in infocommunication systems with orthogonal coding Journal of Physics: Conference Series 1515(5) 052077
[14] Higham N J 2008 Functions of matrices: theory and computation Society for Industrial and Applied Mathematics 450
[15] Rabin A V and Vinar P O 2021 Formation of the output message of the encoding device for code division of channels Computer program Appl. 04.02.2020 no 2021610944 certificate 04.02.2021 no 2021611722 RU
[16] Rabin A V and Vinar P O 2021 Formation of the output message of the decoding device for code division of channels Computer program Appl. 04.02.2020 no 2021610945 certificate 04.02.2021 no 2021611723 RU