Synthesis method of orthogonal encoding and decoding matrices based on integers, providing the implementation of code division of channels

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 code division of binary channels based on the arithmetic analogue of convolutional codes is investigated. The synthesis method of encoding and decoding matrices is proposed for implementing a code division of channels regardless of the number of users. The synthesis and implementation of theses pairs of matrices will significantly simplify the schemes for constructing encoding and decoding devices. Research results can be used in various communication technologies: in real-time systems, in distributed systems in on-board equipment complexes, to ensure reliable information transfer.

1. Introduction
The efficient use of data transmission equipment often requires a sharing of resources by several users. Commonly used techniques of shared data access are time-division multiple access (TDMA), frequency-division multiple access (FDMA), code-division multiple access (CDMA), orthogonal frequency-division multiplexing (OFDM), carrier sense multiple access (CSMA), etc. [1-3]. CDMA technology has a high spectral efficiency, which allows the use of the same nominal operating frequencies throughout the entire service area. Provided that the same frequency resource is allocated, the potential throughput of CDMA systems exceeds that of systems using FDMA and TDMA [4-6].

We will assume that there are N users who want to use the binary communication channel at the same time [7]. When all N users are sending data, the total rate of information transfer is equal to the time-share rate. However, when fewer than N users are active, the unused channel capacity can be used to achieve the error control [8]. Arithmetic code combining on the transmitting side and code division of channels on the receiving side of the communication system are performed by using pairs of square encoding and decoding matrices. Matrices of order N are considered as encoding and decoding matrices, where N is the number of users. The elements of the encoding and decoding matrices are integers. The encoding matrix G is assumed to be non-degenerate.

The encoding matrix G and the decoding matrix H are related by the formula

\[ G \cdot H = d \cdot I \]

where I is the identity matrix of order N, d is a number of the form \( p^q \), p is a prime number, q is a non-negative integer.
2. Code-division multiplexing based on arithmetic codes

It is known that the canonical diagonal Smith normal form for any matrix $A$ of order $N$ exists and is unique [9]. This form corresponds to the following equation:

$$S = U \cdot A \cdot V,$$  \hspace{1cm} (2)

where $U$ and $V$ are unimodular matrices (whose determinants are equal to $\pm 1$) of order $N$.

Consider the matrix $T$ of order $N$, which is built based on the identity matrix, and the elements of the main diagonal $T$ are numbers of the form $p^q$. If in formula (2) the matrix $S$ is replaced by the matrix $T$, then as a result of such a replacement, instead of the original matrix $A$, we obtain a matrix $G$ of order $N$. $G$ is found as

$$G = U^{-1} \cdot T \cdot V^{-1},$$

where $U^{-1}$ and $V^{-1}$ are the inverse matrices of $U$ and $V$, respectively. The matrix $G$ is the sought encoding matrix.

Using (1), we find the decoding matrix $H$:

$$H = d \cdot G^{-1},$$

where $G^{-1}$ is the inverse of the encoding matrix $G$.

As an input sequence, consider the vector $U = (U_1, U_2, ..., U_N)$. The components of the vector $U$ are integers. The vector at the output of the encoding transformation is determined by the formula

$$V = U \cdot G.$$  \hspace{1cm} (3)

Its components are also integers. Here the output vector is $V = (V_1, V_2, ..., V_N)$.

The device performing the operation described by equation (3) is called an arithmetic encoder. The results of encoding one bit of each source are added bitwise and transmitted sequentially, symbol by symbol, over some binary communication channel.

The channel division operation on the receiving side of the communication system can be described with the following formula:

$$V = (V_1, V_2,., V_N) \cdot H = d \cdot U = (U_1, U_2,., U_N).$$  \hspace{1cm} (4)

As a result of this operation, we get the input sequence $U$, but with a delay of $q$ clock cycles, if $d = p^q$. The device performing this operation will be called an arithmetic decoding device.

3. Synthesis method for encoding and decoding matrices

We propose the method for the synthesis of the encoding matrix $G$ of order $\xi$. A similar approach was used to synthesize orthogonal matrices in order to build codes and provide a noise immunity for communication systems [10-13].

The synthesis is carried out as follows:

- Step 1. Let the $2z$ elements of the main diagonal be set to 1, $2z \leq \xi$. The number $z$ is an integer. It is important to note that there will always be an even number of ones ($2z$) on the main diagonal, since for an odd value ($2z + 1$), we get the encoding matrix $G$, where the determinant will be zero. This property is obtained due to the fact that the rows in the matrix become linearly dependent.
- Step 2. Set the last element of the main diagonal to 4.
- Step 3. Set the remaining elements of the main diagonal to 2.
- Step 4. Outside the main diagonal, the elements take on the following values: 1 and 0 alternate on odd lines, 0 and 1 alternate on even lines. The main diagonal will not be taken into account.

Thus, the encoding matrix $G$ of order $\xi$ has the form...
The reliability of the results is confirmed by the correct application of the mathematical apparatus and the correspondence of the results of simulation modeling to theoretical proposals [14, 15].

We present examples of pairs of encoding and decoding matrices for four and eight users, respectively. The encoding matrix for four users is:

$$G(D) = \begin{pmatrix}
1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 \\
\vdots & \vdots & \vdots & \vdots \\
0 & 1 & 0 & 1
\end{pmatrix}$$

The corresponding decoding matrix can be written as

$$H_4 = \begin{pmatrix}
6 & 0 & -3 & 0 \\
0 & 4 & 0 & -1 \\
-3 & 0 & 3 & 0 \\
0 & -1 & 0 & 1
\end{pmatrix}$$

Operations (3) and (4) for a given pair of matrices and an input vector $U = (1 1 0 0 \ldots)$ will be performed as follows:

$$U = (1 1 0 0 \ldots), \quad V = U \cdot G_4 = (1 1 1 1 \ldots),$$

$$U' = V \cdot H_4 = (3 3 0 0 \ldots) = 3^1 \cdot (1 1 0 0 \ldots).$$

The encoding matrix for eight users is:

$$G_8 = \begin{pmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 0 & 2 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 2 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 & 2 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 2 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 2 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 4
\end{pmatrix}$$

The corresponding decoding matrix can be written as
Operations (3) and (4) for a given pair of matrices and an input vector \( U = (1 1 1 1 0 1 0 0 ...) \) will be performed as follows:

\[
U = (1 1 1 1 0 1 0 0 ...), \quad V = U \cdot G_3 = (2 3 3 4 2 4 2 3 ...),
\]
\[
U' = V \cdot H_3 = (3 3 3 3 0 3 0 0 ...) = 3^3 \cdot (1 1 0 1 0 0 ...).
\]

When synthesizing matrices to implement code division of channels for \( 3^q \) users, relation (1) must be satisfied. Moreover, \( d \) will be a number of the form \( 3^q \), where \( q \) is a non-negative integer. The matrix synthesis method for \( 3^q \) users is similar to the matrix synthesis method for \( 2^q \) users.

Let’s present examples of pairs of encoding and decoding matrices for three and nine users, respectively. The encoding matrix for three users is:

\[
G_3 = \begin{pmatrix}
1 & 0 & 1 \\
0 & 2 & 0 \\
1 & 0 & 4
\end{pmatrix}
\]

The corresponding decoding matrix can be written as

\[
H_3 = \begin{pmatrix}
8 & 0 & -2 \\
0 & 3 & 0 \\
-2 & 0 & 2
\end{pmatrix}
\]

Operations (3) and (4) for a given pair of matrices and an input vector \( U = (1 1 0 ...) \) will be performed as follows:

\[
U = (1 1 0 ...), \quad V = U \cdot G_9 = (1 2 1 ...),
\]
\[
U' = V \cdot H_9 = (6 6 0 ...) = 2 \cdot 3^3 \cdot (1 1 0 ...).
\]

An example of a pair of encoding and decoding matrices for nine users is shown below:

\[
G_9 = \begin{pmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 0 & 2 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 2 & 0 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 2 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 2 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 2 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 4
\end{pmatrix}, \quad H_9 = \begin{pmatrix}
13 & 0 & -3 & 0 & -3 & 0 & -3 & 0 & -1 \\
0 & 12 & 0 & -3 & 0 & -3 & 0 & -3 & 0 \\
-3 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -3 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \\
-3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}
\]

In this case, operations (3) and (4) for the input vector \( U = (1 1 1 1 0 0 1 0 1 ...) \) can be written as:
The paper proposes a method for the synthesis of encoding and decoding matrices based on integers. It is shown that when using the synthesized pairs of matrices, the result of channel division coincides with information messages, but will be received with a time delay of one clock cycle. The synthesis and use of the above pairs of matrices will significantly simplify the schemes for constructing encoding and decoding devices. The obtained scientific results will make it possible to significantly simplify the operations of code combining and code division of channels. The technical implementation of the proposed code-division schemes is quite simple for various applications.

**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] 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

[2] Proakis J G 2007 Digital communications (New York: McGraw Hill) 1150

[3] Sklar B 2017 Digital communications: fundamentals and applications (Prentice Hall Communications Engineering and Emerging Technologies Series) 1104

[4] Prucnal P R 2019 Optical code division multiple access: fundamentals and applications (CRC Press) 400

[5] Yousif A H, Zeghid M, Imtiaz W A and Sharma T 2020 Two-dimensional permutation vectors’ (PV) code for optical code division multiple access systems (Entropy) 22(5) 576

[6] Morsy A, Morsy I, Abdulaziz A and Osama H G 2019 Performance analysis of optical code division multiple access networks for multimedia applications using multilength weighted modified prime codes (Optical Engineering) 5(3) 035101

[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] Stanley R P 2016 Smith normal form in combinatorics Journal of Combinatorial Theory Series A 144 476-95

[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 WECOMF) 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] Rabin A V and Vinar P O 2020 Synthesis of encoding and decoding matrices that ensure the implementation of code division of 2^q channels Computer program Appl. 16.12.2020 no 2020666518 certificate 16.12.2020 no 2020666764 RU

[15] Rabin A V and Vinar P O 2020 Synthesis of encoding and decoding matrices that ensure the
implementation of code division of $3^q$ channels Computer program Appl. 16.12.2020 no 2020666517 certificate 16.12.2020 no 2020666763 RU