Convolutional coding for code multiplexing of channels

Alexey Rabin*, *Sergei* Rabin, and *Andrey* Ovchinnikov

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

Abstract. This paper explores the application of convolutional codes and their extensions in the context of binary channel code division. A novel method for channel division utilizing convolutional coding is presented, alongside a comparative analysis with block coding techniques. While the approach for implementing convolutional codes in channel division shares similarities with block coding methods, it possesses distinct characteristics. The study introduces the use of elements from the field of formal power Laurent series, with coefficients drawn from a finite field, as components of both the transmitted message and code word. This innovative approach enhances the flexibility and efficiency of the coding process. Furthermore, the research investigates the feasibility and conditions for simultaneous error correction during the code division of channels. This dual functionality has the potential to significantly improve the reliability and performance of communication systems. By examining these advanced coding techniques, the paper contributes to the ongoing development of more robust and efficient channel division methods in digital communications.

1 Introduction

The field of channel division technology has seen widespread adoption, yet Russian manufacturers of switching equipment continue to rely on foreign suppliers for critical components. This dependency has sparked a pressing need to develop simplified switching device schemes using domestic resources, addressing the challenge of import substitution in this crucial sector [1-2].

The growing interest in advancing code division access technology stems from several key factors, including increasing subscriber density, enhanced resistance to interference and improved security of data transmission against unauthorized access.

This paper focuses primarily on the application of convolutional codes and their generalizations for channel code separation [3-5]. The primary objective of this research is to reduce the complexity of code channel division schemes through the implementation of a novel channel division method utilizing convolutional coding.

* Corresponding author: alexey.rabin@gmail.com

2 Channel division method using convolutional coding

In the design of code-division multiplexing communication systems or using convolutional codes for error correction in information transmission systems, it is usually sufficient to assume that transmitted messages from k users are a sequence of elements from the ring of polynomials $F_p[D]$. However, with maximum generalizations and sufficiently detailed studies, one has to assume that both transmitted messages from all users, represented by a row vector of length k, and code words of length N, consist of components belonging to the field of formal power series.

Usually, to obtain a convolutional code, the transmitted message is multiplied by a rectangular encoding matrix of size k x N, where $N > k$. To implement the possibility of code division of channels with N subscribers, the coding operation consists of multiplying by a square matrix of order N with certain properties.

Note that the elements of this square matrix can be any rational fractions, that is, elements from the field of binary rational functions $F_2(D)$, which is a subfield of the field of Laurent series $F_2((D))$, or any polynomials, that is, elements of the ring $F_p[D]$. If rational functions are used as elements of a square matrix, then the denominator of this function certainly has a nonzero free term, since otherwise the technical implementation of the scheme corresponding to such a fraction becomes impossible.

In addition, it should be noted that the square matrix $G(D)$ used in the encoding operation must be free of delay. This means that at least one element of this matrix must have a numerator with a nonzero intercept. If $G(D)$ is not free of delay, then it can be represented as

$$G(D) = D^i G_d(D) \tag{1}$$

where $i \geq 1$ and $G_d(D)$ is a delay-free matrix.

It is easy to see from the previous equality that a delay-free matrix can always be obtained. Therefore, the square matrix for performing the encoding operation will always be represented as a delay-free matrix.

In this paper, the focus is on the ability to divide channels using convolutional coding rather than on the construction of convolutional codes with a good correcting ability. Therefore, to perform encoding operations, square matrices are used [6].

At the same time, it should be noted that in order to obtain a conventional convolutional code, it is sufficient to assume that some of the users are not active. The remaining l, $l < N$, users make up a vector that can be considered as a new transmitted message. Then multiplying the row vector constituting this new transmitted message by the encoding matrix results in the convolutional code that detects and possibly corrects a number of errors. The number of errors corrected depends on the available redundancy, and the amount of this redundancy is proportional to the number of inactive users. The more inactive users there are, the more there is redundancy and the more opportunities there are for error detection and correction. A similar approach is used in the synthesis of orthogonal matrices for the purpose of constructing codes and ensuring noise immunity of communication systems.

For this reason, in the presence of inactive users, it is possible to carry out the code division of channels with simultaneous correction of a number of random errors [7,8].

3 Examples of use

Let's explore circulant matrices with determinants in the form D_i, where i is a non-negative integer [9]. This process becomes straightforward when one is familiar with the method for calculating determinants of circulant matrices. There exists a particular condition that significantly simplifies the process of identifying the encoding matrix.

The circulant encoding matrix can be represented as:

$$G(D)=\begin{pmatrix} g_1(D) & g_2(D) & \cdots & g_N(D) \\ g_N(D) & g_1(D) & \dots & g_{N-1}(D) \\ \vdots & \vdots & \ddots & \vdots \\ g_2(D) & g_3(D) & \dots & g_1(D) \end{pmatrix} \quad (2)$$

where $g_i(D)$ for $i = 1, 2, \dots, N$ are polynomials of finite degree of the variable D. Thus, the determinant of the matrix $G(D)$ is uniquely determined by the polynomials $g_1(D)$, $g_2(D)$, …, $g_N(D)$.

In the context of channel division for information transmission, we initially consider the coefficients of polynomials $g_1(D)$, $g_2(D)$, …, $g_N(D)$ as elements of the finite field GF(2).

This approach addresses the specific case of binary communication channels.However, we can expand this concept to a broader scenario. The coefficients of these polynomials can be drawn from the finite field GF(p), where p is a prime number, or even from an algebraic extension of this field. Despite this generalization, the fundamental requirements for the encoding matrix remain consistent.

To illustrate this concept, let's examine an encoding matrix where the polynomial elements have coefficients from the finite field GF(3). Consider the following matrix:

$$G(D)=\begin{pmatrix} 1+D & 1+2D & 1+D \\ 1+D & 1+D & 1+2D \\ 1+2D & 1+D & 1+D \end{pmatrix} \quad (3)$$

A notable property of this matrix is that the sum of elements in each row equals D. Consequently, the determinant of this matrix is D^3. This example demonstrates how the principles of channel division can be applied using more complex finite fields while maintaining the essential characteristics of the encoding matrix.

The constraints imposed on the dimensions of circulant encoding matrices, while not mandatory, provide a convenient framework for efficiently computing the determinant of the encoding matrix. To illustrate this point, let's examine an alternative encoding matrix with a different order, using elements from GF(3). In this case, the sum of elements in each row equals $2 + D$, resulting in a determinant of $2 + 2D + 2D^3$. The matrix is structured as follows:

$$G(D)=\begin{pmatrix} 2D & 2+D & 2 & 1+D \\ 1+D & 2D & 2+D & 2 \\ 2 & 1+D & 2D & 2+D \\ 2+D & 2 & 1+D & 2D \end{pmatrix} \quad (4)$$

This example demonstrates that the determinant calculation method extends to circulant matrices of order p^q over finite fields with characteristic p, even when the matrix elements are rational fractions. Specifically, for a finite field with characteristic three, the determinant of a circulant matrix of order 3^q can be obtained by summing the rational fractions in any row of the matrix and raising the result to the power of $N = 3^q$.

This generalization simplifies the determinant calculation process for a broader class of circulant matrices, providing a powerful tool for analyzing and designing encoding matrices in various applications of convolutional coding and channel division multiplexing.

For this example let the matrix have the form:

$$G(D)=\begin{pmatrix} \frac{1+2D}{1+D} & 1+D & 1 \\ 1 & \frac{1+2D}{1+D} & 1+D \\ 1+D & 1 & \frac{1+2D}{1+D} \end{pmatrix} \quad (5)$$

When we sum the elements in a single row of this matrix, we obtain the expression $2D + 2D^3$. Consequently, the determinant of this matrix can be calculated as $(2D + 2D^3)^3$, which simplifies to $2D^3 + 2D^6$. This result can be independently verified through direct computation of the matrix's determinant.

To further validate this observation, one can reduce all elements of the matrix $G(D)$ to a common denominator. This common denominator can then be factored out of the matrix. The resulting matrix will consist entirely of polynomial elements in the variable D. By applying the previously mentioned triangularization transformation to this new matrix, we can arrive at the same determinant result.

It's worth noting that this latest encoding matrix differs from its predecessors in that its elements contain non-singular denominators. This characteristic leads to encoded output sequences that are typically infinite in length and exhibit periodicity. As a consequence, these sequences can possess arbitrarily large Hamming weights. The complexity introduced by these properties makes the analysis of such sequences a challenging task.

4 Conclusion

The application of convolutional codes for channel division multiplexing has been explored presenting several key findings and contributions to the field. A novel method for channel division using convolutional coding has been developed, drawing parallels with block coding techniques while highlighting unique characteristics of convolutional codes. This approach utilizes elements from the field of formal power series (Laurent series) with coefficients from finite fields as components of both transmitted messages and code words.

The research demonstrates the possibility of simultaneous error correction during channel code division. By employing square matrices for encoding operations, the system can accommodate inactive users, allowing for channel division with concurrent random error correction. This dual functionality has the potential to significantly improve the reliability and performance of communication systems.

The proposed method shows significant potential for practical implementation in various communication scenarios, including space and satellite communications, real-time systems, distributed systems in on-board equipment complexes, and reliable information transmission scenarios. The practical significance of the method is validated by the correspondence between simulation results and theoretical propositions, indicating its robustness and reliability.

The paper was prepared with the financial support of the Russian Science Foundation, grant agreement No. 23-29-01005, «Research and development of mathematical methods for code division of channels in space and satellite communication systems with error-correcting coding and multi-position coded modulation».

References

1. R. Johannesson, K. S. Zigangirov, *Fundamentals of Convolutional Coding* (Wiley, IEEE Press, 1999).

2. B. Sklar, *Digital communications: fundamentals and applications* (Prentice Hall Communications Engineering and Emerging Technologies Series, 2017).
3. A. Morsy, I. Morsy, A. Abdulaziz, H. G. Osama, Optical Engineering **58(3)**, 035101 (2019).
4. T. Cover, A. El Gamal, M. Salehi, IEEE Transactions on Information Theory **26(6)**, 648-657 (1980).
5. V.P. Telang, M. A. Herro, IEEE Transactions on Information Theory **44**, 1632-1642 (1998).
6. F. R. Gantmacher, The Theory of Matrices (Moscow, Nauka, 1966), 110-115.
7. M. Effros, A. Goldsmith, *Capacity definitions and coding strategies for general channels with receiver side information* in: IEEE Int. Symp. Inform. Theory (1998).
8. L. Zheng, D.N.C. Tse, IEEE Transactions on Information Theory **49(5)**, 1073-1096 (2003).
9. P. O. Vinar, S. V. Rabin and A. V. Rabin, J. Phys.: Conf. Ser. 2094 032067 (2021).