SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I9P116

Volume 12 Issue 9, 188-193, September 2025


*Original Article*

# Even-Length Modified Linear Block Code for Space Links

Seema Talmale[1], B. K. Lande[2]

[1]*Department of Electronics Engineering, K.J. Somaiya School of Engineering (formerly known as K J Somaiya College of Engineering), SVU, Vidyavihar, Mumbai, India.*
[2]*Department of Electronics Engineering, D.M.C.E., Mumbai University, Mumbai, India.*

[1]*Corresponding Author : seematalmale@somaiya.edu*

Received: 16 July 2025 Revised: 18 August 2025 Accepted: 17 September 2025 Published: 29 September 2025

***Abstract*** *- This work introduces a new technique for constructing enhanced-distance linear block codes tailored for binary vector systems with even dimensions. The approach is based on the theory of completely controllable discrete-time systems, where the solution space of such systems is systematically adapted to generate the code structure. As a demonstration, a controllable system of order 20 is used to design a (40,20) block-structured linear code, corresponding to an information rate of 0.5. To strengthen the error-correcting capability, a specialized mapping method is applied, which increases the minimum separation among valid code words by permuting the binary vectors. By widening this distance, the code exhibits improved tolerance to transmission errors. Simulation studies show that the suggested design achieves a lower Bit-Error Rate (BER) and a smaller probability of undetected errors compared with other block codes having the same parameters. These attributes make the scheme highly suitable for applications requiring exceptional reliability, such as deep-space communication, where both accuracy and robustness are critical. The results highlight how integrating concepts from control theory with modern coding strategies can produce efficient error-correcting codes for demanding communication systems, and they point toward future research opportunities in control-based code design for advanced data transmission.*

***Keywords*** *- Generator matrix, Discrete-time system, Bounds, Minimum distance, Code word, BER (Bit Error Rate).*

## 1. Introduction

Error-Correcting Codes (ECCs) are fundamental tools in modern digital communication and storage systems. These systems help to identify and fix the errors that may occur during data transmission or storage, thereby maintaining the accuracy and reliability of the data. Within the broad family of error-correcting codes, linear block codes stand out as they combine a well-defined algebraic structure with decoding procedures that are computationally efficient. A particular class of these codes, designed using system theory and control principles, has shown significant promise in enhancing error-correction capabilities.

The interplay between linear systems and convolutional codes has been explored extensively, providing a rich mathematical framework to design efficient coding schemes [1]. Building on this foundation, connections between control theory and finite rings have further expanded the possibilities for designing error-correcting codes with optimal properties [2]. Kalman's seminal work on the general theory of control systems [3] has inspired innovative approaches for designing codes derived from system-theoretic concepts.

While linear block codes have been extensively studied, most existing designs focus on algebraic or combinatorial construction methods without drawing on system-theoretic principles. Enhanced-distance codes, which can offer stronger error correction, are typically achieved through modifications of known code families such as BCH or LDPC. However, these approaches rarely exploit the controllability properties of discrete-time systems, despite the fact that such systems naturally generate structured vector spaces suitable for coding. Furthermore, there is limited research on integrating control-theoretic state-space models into the design of block codes for binary vector systems of even length, particularly in ways that systematically increase minimum distance for improved error resilience.

In high-dependability communication environments such as deep-space links, error correcting codes must achieve low bit error rates and minimize undetected errors under severe channel conditions. Existing block code designs with similar parameters often fail to provide an optimal balance between structural simplicity, high minimum distance, and adaptability to even-length binary vector systems. The challenge is to develop a construction method that can

systematically generate such codes, enhance their error-correcting capability, and remain computationally feasible for practical implementation.

Currently, per the standards of the Consultative Committee of Space Data System (CCSDS), the binary Golay Code is used for deep space missions, and there is a proposal of using the Low-Density Parity Check Code (LDPC). The proposed (40, 20) Modified Linear Block Code (MLBC) in this research features a minimum code word distance of 10, which is better than the (24, 12) Golay code. As per history, in Voyager 1 and 2 other spacecrafts, Reed-Muller Code was replaced by Golay Code with a good code rate due to memory constraints. This work presents an error correcting code that maintains a code rate of 1/2 while offering strong BER characteristics, making it applicable for forward error correction in high-frequency radio environments.

This research article focuses on the design of even-length (n, k) codes using principles derived from completely controllable discrete-time systems. By integrating system-theoretic concepts into the code construction process, the proposed methodology aims to achieve a balance between computational efficiency and error correction performance.

The paper's layout is presented as follows: Sections 2, 3, and 4 give the literature survey and methodology for designing a length-modified linear block code for space links. Sections 5 and 6 present experimental, analytical and simulation results, comparing the performance of the proposed codes with existing schemes. Section 7 provides the conclusion of the study and outlines possible avenues for future investigation.

## 2. Literature Survey

Error-correcting codes have been an integral part of communication theory, particularly for their role in ensuring data integrity when messages are transmitted through noisy channels. The earliest systematic attempts to minimize redundancy while maintaining reliability can be traced back to Huffman's well-known coding approach [4].

Since then, the central concern has been to maximize the minimum Hamming distance between codewords, as this directly governs how effectively a code can detect and correct errors.

This study focuses on constructing enhanced-distance linear block codes by systematically exploiting controllability properties of discrete-time systems and augmenting them with mapping-based strategies. By doing so, it aims to provide a robust coding framework that is especially suited for environments such as deep-space communication, where extremely low error rates are a fundamental requirement.

### *2.1. Distance-Preserving and Distance-Increasing Mappings*

A considerable amount of work has been devoted to the design of mappings that preserve or increase code distances. The methodology described in [5, 6] provides a means to enhance the minimum distance between codewords. Lee [7] was among the first to introduce distance-preserving maps of odd length, while Lin et al. [8] later demonstrated that such techniques could be extended to ternary vectors. These studies indicated that suitable mappings could provide structural improvements in code design. Chee and Purkayastha [9] took this idea further by developing efficient decoding strategies for codes built from permutation-based mappings.

### *2.2. Systems-Theoretic Contributions to Coding*

A different but related strand of research has attempted to link coding theory with systems and control theory. Rosenthal [10] pointed out that several open problems in systems theory have direct implications for communication and coding. Earlier, Author's examined the state-transfer problem in linear systems, and this idea was later applied to the systematic construction of codes. Building upon these ideas, Author's proposed a class of Modified Linear Block Codes (MLBCs) that exploit controllability properties of discrete-time systems. Their work established methods for designing generator matrices and introduced distance-preserving mappings and efficient decoding algorithms, demonstrating the adaptability of control-theoretic approaches in achieving high error resilience.

### *2.3. Algebraic Approaches and Decoding Strategies*

Algebraic methods have remained a dominant research direction for decades. References [11-21] present several algebraic decoding methods for cyclic and quadratic residue codes, making use of approaches like Gröbner bases, error locator polynomials, and the Berlekamp-Massey algorithm. These contributions extended decoding capabilities to the true minimum distance, going well beyond classical error correction limits.

### *2.4. Specialized Coding for Channel Constraints*

Other researchers have studied coding strategies tailored to specific channel models. Tomás, Rosenthal, and Smarandache [22] analyzed the decoding of convolutional codes over erasure channels, where only partial information is available at the receiver. Their results illustrate the adaptability of convolutional structures under constrained channel conditions.

## 3. Methodology

In this work, a 5-bit error correcting Modified Linear Block Code (MLBC) has been developed. The code, represented as a (40,20) (n, k) system, originates from the solution space of a fully controllable discrete-time model. Its

generator matrix (G) is organized by permuting codewords, and the performance of the design was examined through simulation. A promising Bit Error Rate (BER) can be obtained for the constructed code. This code can be decoded by generally available existing decoding techniques for linear block codes.

Based on the analytical research of this code, a new lemma is developed. The probability of undetected error for the designed (40, 20) MLBC demonstrates improved performance over conventional block codes.

The progression of the discrete-time system is formulated using the state-space equation, shown here by Equation number (1):

$$x(k+1) = Ax(k) + bu(k) \quad \text{.....(1)}$$

In this formulation, x(k) denotes the state vector at the discrete instant k, and u(k) corresponds to the input vector.

A general form of the solution to Equation (1) is expressed as follows:

$$x(k) = A^k x(0) + \sum_{j=0}^{k-1} A^j bu(k-1-j) \quad \text{.....(2)}$$

Let us now examine an example of a third-order system, as outlined below:

Let,

$$x(k+1) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -6 & -11 & -6 \end{bmatrix} x(k) + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} u(k) \quad \text{.....(3)}$$

By applying Equation (2) to solve the matrix system in Equation (3) across various sampling instances and extending the analysis to a $20^{th}$-order system, the resulting state at the final sampling point is represented as x(20). This corresponds to the $20^{th}$-order system. Beginning with the initial state, it can be demonstrated that the final solution, x(20), is a vector consisting entirely of zeros.

As the system progresses, all subsequent outputs reduce to zero, meaning the initial state [11111111111111111111] eventually reaches [00000000000000000000] at the final sampling instant. The vectors x(0), x(1), and x(2) serve as the fundamental basis of the system. The vectors x(3) through x(19) are used to construct the generator matrix G. In this approach to linear block coding, the generator matrix G takes the form G = [I | P], with P created by placing the transposed vectors x(0) to x(19) as rows and I as the identity matrix. The matrix P assumes an upper triangular structure derived from the basis vectors. The corresponding parity-check matrix is given by $H = [P^T \mid I]$, which satisfies the standard linear block code conditions $G^TH = 0$ and $H^TC = 0$.

## 4. Designing of Basis Vectors for (40,20), (n, k) Code

From the above section of this article, the generator matrix for a 20th-order completely controllable discrete-time system can be established from the basis vectors of its solution space as follows: This established generator matrix will have 20 rows and 40 columns, which consists of an identity matrix and the solution space obtained from basis vectors.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0\cdots & 0 & 1 & 1 & \cdots & 1\cdots & 1 \\ 0 & 1 & 0 & 0\cdots & 0 & 1 & 1 & \cdots & \cdots & 0 \\ \vdots & 0 & 1 & 0\cdots & 0 & 1 & 1 & 1 & 0\cdots & 0 \\ \vdots & \vdots & 0 & 1\cdots & 0 & \vdots & \vdots & 0 & \cdots & 0 \\ 0 & \vdots & \vdots & 0\cdots & 1 & 1 & 0 & \cdots & \cdots & 0 \end{bmatrix}$$

It is verified that the condition $G \cdot H^T = 0$ holds, confirming a key property of linear block codes. Additionally, when this generator matrix is employed to form a linear block code, it can be verified that $H \cdot C^T = 0$, indicating that the resulting code adheres to all fundamental principles of linear block codes. Upon evaluating the code's error detection capability through minimum distance analysis, it is found to detect single-bit errors.

To enhance the error correction performance, permutations of the basis vectors in the generator matrix are applied using twisting and rotation techniques, while keeping the identity portion of the matrix unchanged. By this methodology, the designed code is observed in a 5-bit error correcting code and gives better Bit Error Rate (BER) performance.

## 5. Analytical Experimentation for the Basis Vectors Framework

First row $R_1$ of the generator matrix for the modified matrix is obtained by permutation of rows of the P part of G:

$$R_{1(modified)} = R_1 + R_{18} + R_{18} + R_{14} + R_{15} + R_{15} + R_{13} + R_{11} + R_5 + R_7 + R_3$$

For further rows of the generator matrix, we propose an increased distance mapping algorithm for a length-modified matrix, as shown in Figure 1.

(40, 20) Code is developed with this methodology, which can detect up to 10 errors made in the transmission system used for high-frequency transmission. Also, it can correct 5 errors that occurred in such a transmission. The probability of undetected errors is better for this designed code than the existing codes.

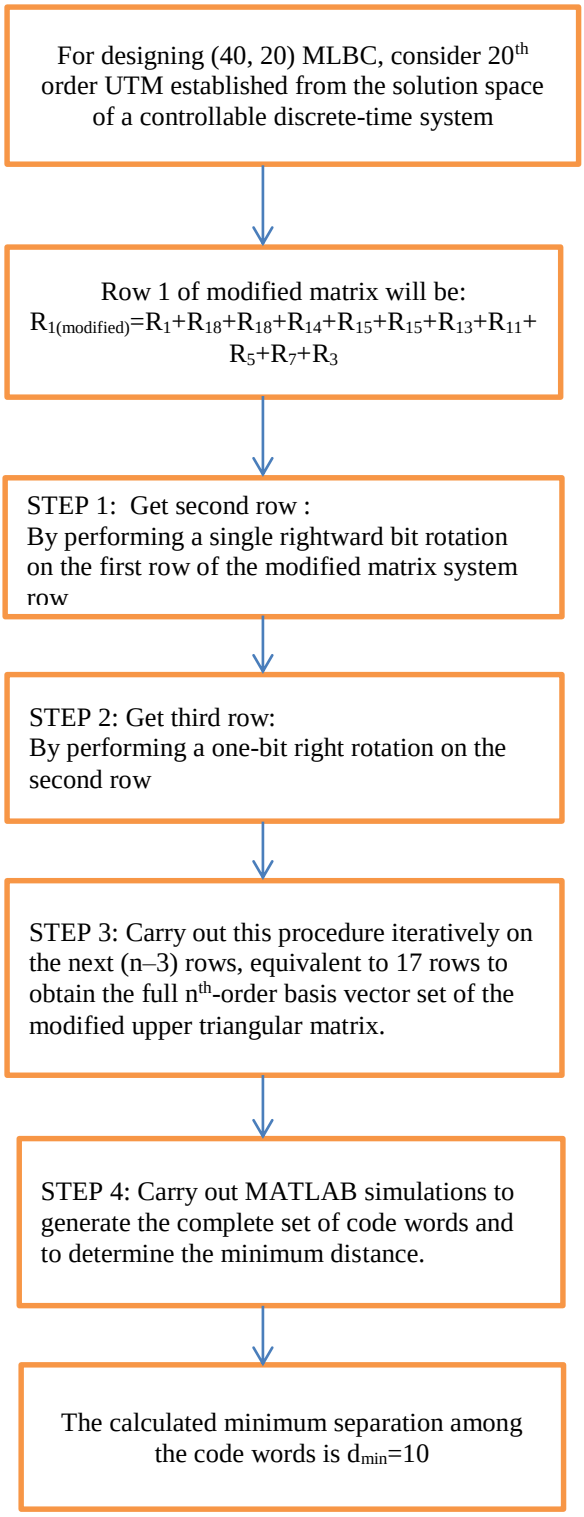


**Fig. 1 Increased Distance Mapping Algorithm for Designing (40,20), (n, k) MLBC**

## 6. Experimental Simulation and Results

The designed (40, 20), (n, k) code is simulated using MATLAB simulation and the BER performance is evaluated. The results are shown in Figure 2.

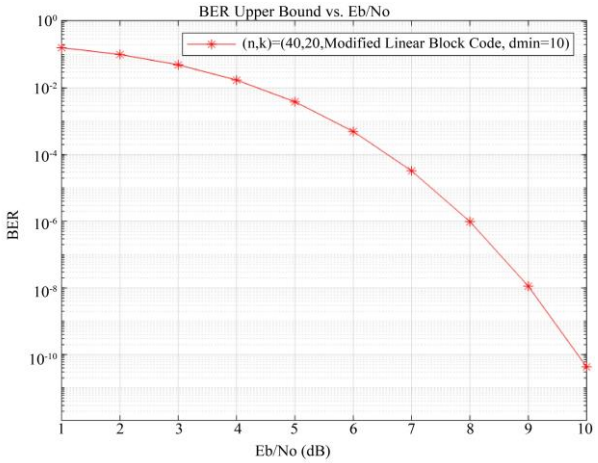


**Fig. 2 Eb/No Vs BER Performance**

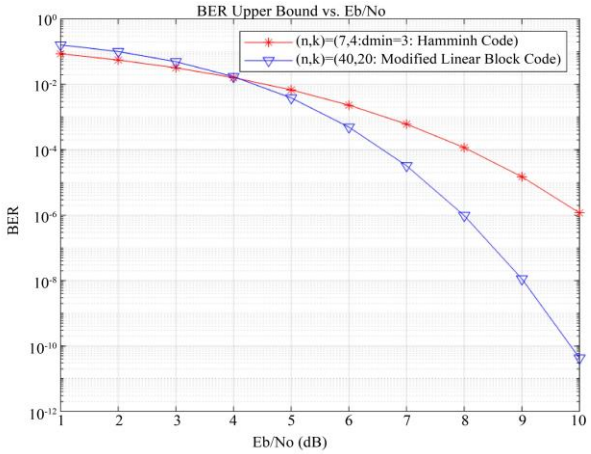


**Fig. 3 Comparison of Eb/No Performance of the (40,20) MLBC with Other Codes**

As illustrated in Figure 3, the bit error rate of the proposed MLBC outperforms that of the currently available codes.

**Table 1. Results of a few more designed error correcting codes with the help of permutation and twisting methodology**

| Name of the Code | Code length parameters | Rate of designed code | Modulation Technique | $d_{min}$ |
|---|---|---|---|---|
| MLBC | (18,9) | 0.5 | 16 QAM | 5 |
| MLBC | (34,17) | 0.5 | 16QAM | 6 |
| MLBC | (22,11) | 0.5 | 16QAM | 6 |
| MLBC | (28,14) | 0.5 | 16QAM | 6 |
| MLBC | (30,15) | 0.5 | 16QAM | 6 |
| MLBC | (82,18) | 0.219 | 16 QAM | 22 |
| MLBC | (79,15) | 0.189 | 16QAM | 22 |
| Hamming Code | (31,26) | 0.838 | 16 QAM | 3 |
| Hamming Code | (63,57) | 0.904 | 16 QAM | 3 |
| Hamming Code | (127,120) | 0.944 | 16 QAM | 3 |
| Hamming Code | (255,247) | 0.968 | 16 QAM | 3 |
| MLBC | (40,20) | 0.5 | 16 QAM | 10 |

## 7. Analytical Findings

### *7.1. Lemma*

By considering a discrete-time system of order 20 that is fully controllable, it is feasible to derive an error correcting code of (n = 40, k = 20) using its solution space. This code exhibits the minimum distance of 10.

## 8. Conclusion

Any form of audio or video communication is bound to face errors in a fading environment. The main objective of constructing error-correcting codes is to solve the issue of unreliable communication. In this research, a simple and effective error-correcting code is designed with improved error-correcting capacity. A novel variant of a linear block code based on permutation arrays is developed. Specifically, an even-length (40, 20) (n, k) linear block code with enhanced error-correcting capability is designed. This approach introduces a unique methodology involving permutation and twisting of the code words, which can be extended to construct longer codes. The resulting codes are particularly suitable for high-frequency radio signal transmission and reception applications.

## Acknowledgments

The authors express their gratitude to K. J. Somaiya School of Engineering for providing the necessary support throughout this research.

## References

[1] Joachim Rosenthal, "Connections between Linear Systems and Convolutional Codes," *Conference Proceedings: Codes, Systems, and Graphical Models*, pp. 39-66, 2001. [CrossRef] [Google Scholar] [Publisher Link]

[2] Joachim Rosenthal, *An Optimal Control Theory for Systems Defined Over Finite Rings*, Open Problems in Mathematical Systems and Control Theory, 1st ed., Springer, pp. 193-201, 1999. [CrossRef] [Google Scholar] [Publisher Link]

[3] R.E. Kalman, "On the General Theory of Control Systems," *IFAC Proceedings Volumes*, vol. 1, no. 1, pp. 491-502, 1960. [CrossRef] [Google Scholar] [Publisher Link]

[4] David A. Huffman, "A Method for the Construction of Minimum-Redundancy Codes," *Proceedings of the IRE*, vol. 40, no. 9, pp. 1098-1011, 1952. [CrossRef] [Google Scholar] [Publisher Link]

[5] Jen-Chun Chang, "Distance-Increasing Mappings from Binary Vectors to Permutations," *IEEE Transactions on Information Theory*, vol. 51, no.1, pp. 359-363, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[6] Marzieh Akbari, Neil I. Gillespie, and Cheryl E. Praeger, "Increasing the Minimum Distance of Codes by Twisting," *The Electronic Journal of Combinatorics*, vol. 25, no. 3, pp. 1-19, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[7] Kwankyu Lee, "New Distance-Preserving Maps of Odd Length," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2539-2543, 2004. [CrossRef] [Google Scholar] [Publisher Link]

[8] Jyh-Shyan Lin et al., "Distance-Preserving and Distance-Increasing Mappings from Ternary Vectors to Permutations," *IEEE Transactions on Information Theory*, vol. 54, no. 3, pp. 1334-1339, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[9] Yeow Meng Chee, and Punarbasu Purkayastha, "Efficient Decoding of Permutation Codes Obtained from Distance Preserving Maps," *2012 IEEE International Symposium on Information Theory Proceedings*, Cambridge, MA, USA, pp. 636-640, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[10] J. Rosenthal, "Some Interesting Problems in Systems Theory which are of Fundamental Importance in Coding Theory," *Proceedings of the 36th IEEE Conference on Decision and Control*, San Diego, California, USA, pp. 4574-4579, 1997. [CrossRef] [Google Scholar] [Publisher Link]

[11] Xuemin Chen et al., "Use of Grobner Bases to Decode Binary Cyclic Codes up to the True Minimum Distance," *IEEE Transactions on Information Theory*, vol. 40, no. 5, pp. 1654-1661, 1994. [CrossRef] [Google Scholar] [Publisher Link]

[12] I.S. Reed, X. Yin, and T.-K. Truong, "Algebraic Decoding of the (32, 16, 8) Quadratic Residue Code," *IEEE Transactions on Information Theory*, vol. 36, no. 4, pp. 876-880, 1990. [CrossRef] [Google Scholar] [Publisher Link]

[13] Trieu-Kien Truong et al., "Algebraic Decoding of the (89,45,17) Quadratic Residue Code," *IEEE Transactions on Information Theory*, vol. 54, no. 11, pp. 5005-5011, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[14] T.-K. Truong, J.-H. Jeng, and I.S. Reed, "Fast Algorithm for Computing the Roots of Error Locator Polynomials up to Degree 11 in Reed-Solomon Decoders," *IEEE Transactions on Communications*, vol. 49, no. 5, pp. 779-783, 2001. [CrossRef] [Google Scholar] [Publisher Link]

[15] E.R. Berlekamp, H. Rumsey, and G. Solomon, "On the Solution of Algebraic Equations Over Finite Fields," *Information and Control*, vol. 10, no. 6, pp. 533-564, 1967. [CrossRef] [Google Scholar] [Publisher Link]

[16] S.V. Fedorenko, and P.V. Trifonov, "Finding Roots of Polynomials Over Finite Fields," *IEEE Transactions on Communications*, vol. 50, no. 11, pp. 1709-1711, 2002. [CrossRef] [Google Scholar] [Publisher Link]

[17] Tsung-Ching Lin, T.K. Truong, and P.D. Chen, "A Fast Algorithm for the Syndrome Calculation in Algebraic Decoding of Reed–Solomon Codes," *IEEE Transactions on Communications*, vol. 55, no. 12, pp. 2240-2244, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[18] Chunming Rong, T. Helleseth, and J. Lahtonen, "On Algebraic Decoding of the Z/sub 4/-Linear Calderbank-McGuire Code," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1423-1434, 1999. [CrossRef] [Google Scholar] [Publisher Link]

[19] Georg Schmidt, Vladimir R. Sidorenko, and Martin Bossert, "Syndrome Decoding of Reed-Solomon Codes Beyond Half the Minimum Distance Based on Shift-Register Synthesis," *IEEE Transactions on Information Theory*, vol. 56, no. 10, pp. 5245-5252, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[20] Tsung-Ching Lin et al., "Algebraic Decoding of the (31, 16, 7) Quadratic Residue Code by Using Berlekamp-Massey Algorithm," *2010 International Conference on Communications and Mobile Computing*, Shenzhen, China, pp. 275-277, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[21] Pengwei Zhang et al., "Fast Decoding of the (47, 24, 11) Quadratic Residue Code Without Determining the Unknown Syndromes," *IEEE Communications Letters*, vol. 19, no. 8, pp. 1279-1282, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[22] Virtudes Tomas, Joachim Rosenthal, and Roxana Smarandache, "Decoding of Convolutional Codes Over the Erasure Channel," *IEEE Transactions on Information Theory*, vol. 58, no. 1, pp. 90-108, 2018. [CrossRef] [Google Scholar] [Publisher Link]