Journal of Information Systems Engineering and Management
2025, 10(16s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Generator Matrix Design for Enhanced Distance Linear Block Code in Deep Space Missions

Seema Talmale[1], B.K.Lande [2]
[1] *Faculty K.J.Somaiya School of Engineering, Department of Electronics Engineering, SVU, Mumbai, India*
[2] *Department of Electronics Engineering, Datta Meghe College of Engineering, Navi Mumbai, India*

ARTICLE INFO

Received: 10 Dec 2024

Revised: 28 Jan 2025

Accepted: 12 Feb 2025

ABSTRACT

Introduction: In this article, modified linear block codes (MLBCs) are constructed from a completely controllable discrete-time system. These codes are systematic codes where the information part and the parity part of the codes are explicitly separate. In this research, a new variant of block code using permutation arrays is designed. The MLBCs are designed to possess the best possible minimum distance characteristic which in turn leads to error correcting codes with good error correction capability. The constructed generator matrix for the designed MLBCs is developed with the help of distance-increasing mapping (DIM). DIM is established using permutation arrays (PAs) of binary vectors which are obtained from the solution space of a control system. The performance of the developed MLBCs is verified. The probability of undetected errors which is one of the key features of Error Correcting Codes is found to be higher than the Linear Block Codes. The designed code is decodable using the existing decoding algorithms. Constructed codes in this article can be used in high frequency radio environment for deep space mission.

Keywords: Bit Error Rate, Encoding, Decoding, Code Rate, Generator Matrix, Distance increasing Mapping, Modulation Scheme, Error detection, Error correction.

I. INTRODUCTION

Today's world is the world of digital communication. Most of the information is coded in the binary digits '0' and '1' and the efficiency of error correction of the transmitted message is one of the key benchmarks of a communication system. Linear block codes are the oldest and simplest, yet one of the most powerful error correction techniques, with the potential for improved efficiency and applications. Linear block codes deal with symbols defined over the Galois field GF(2). Linear block codes, in general, are given in terms of the generator matrix and parity check matrix.

Rosenthal [1] mentioned that there is a close connection between linear systems over finite fields and Error Correcting Codes. In [2], control theory for systems defined over finite rings is discussed. Kalman [3] gives the theoretical knowledge of the control system with the well-established fact that within n sampling intervals, the initial condition of a control system can be reset to all zero vectors.

Decoding of these codes can be done with the help of existing methods of decoding for linear block codes such as decoding using syndrome polynomials [4]. The twisting of arrays is suggested to increase the distance between the code words by Akbari [5]. In [6-13] various methodologies are discussed for establishing distance preserving mapping (DPM) and DIM from the array of a set of binary number vectors to an array of a set of natural number vectors. In the patent, by Talmale [8], the design of 3-bit error correcting codes is discussed which uses permutation arrays for making the designed error correcting code more effective with regard to its improved error correction capability.

In this research article, the generator matrix is designed from a subspace of a completely controllable discrete-time system (CCDTS). It is observed that by applying Kalman's principle, the solution space of a CCDTS forms an Upper Triangular Matrix. We propose to use this solution space as a subspace in designing of generator matrix

which can be utilized to design Modified Linear Block Codes. Also, this solution space is effectively used to design Distance Increasing Mapping (DIM) to develop increased distance modified linear bock code (IDMLBC). Bit error rate (BER) performance is evaluated with the help of experimentation and results are presented for the same. Based on the analytical and experimental research, the main result is presented in the form of lemma.

This paper is structured as follows: In section 2, a literature survey is discussed. Section 3 demonstrates the use of control system theory for the design of Modified Linear Block Codes. Section 4 gives designing of the generator matrix. Section 5 discusses the construction of permutation arrays for DIM. In section 6, an algorithm for the construction of the generator matrix for increased distance linear block code is developed. In section 7 results are presented and in section 8, this research article is concluded.

II. LITERATURE REVIEW

Research in the area of coding theory is an emerging area as there is a requirement for vast growth in the field of communication technology. Also, this is the era where there is an elegant growth in the field of discrete mathematics.

The classic techniques of mathematics such as permutation and vector transformation are used to improve the influential characteristics of the designed Error Correcting Codes which is the minimum distance between the codewords. The Error correction capability of linear block codes is dependent on the minimum distance between the codewords of a code.

Studies in coding initially branched in two directions, for noiseless channels and for noisy channels. Studies in noiseless channel coding matured quite early. These codes were of variable length. McMillan later extended the result for uniquely decodable codes. Huffman's construction method for optimal instantaneous codes practically answered all questions in the search for the most efficient codes for noiseless channels [14]. The other direction in which the coding theory developed was the area of error-correcting codes, i.e. the coding for noisy channels.

In contrast to constant-length codes, the developments in the study of variable length codes for noisy channels have shown little growth, while most of the time we have variable length messages for example password for a file to be opened, messages (voice or text) on a mobile to be sent, data in a file on a computer etc. and there is unwanted redundancy in making words of constant-length. This lag in development may have been due to a lack of mathematical techniques, in particular, the algebraic methods that influenced the development of constant length coding were unavailable for variable-length codes. Combinatorial search also lagged behind as algebraic search for constant length codes was the main focus area.

In [15], significant research questions are discussed in the area of coding theory from the perspective of control system theory. It is discussed that in the field of convolutional coding theory decoding is considered as a tracking problem that is computationally complex. Chen et al., [16] give the use of Grobner bases in the error detection and correction process. In [17-18], Sylvester resultant method is discussed for decoding of QR codes. This method can be used to compute the Newton identities that are nonlinear and multivariate equations of higher order. These methods become complex when the length of error-correcting codes increases.

Truong et al., [19] give an algebraic decoder for the (89, 45, 17) binary Quadratic Residue (QR) code. Then, Truong *et al.,* [20] developed an algorithm in order to find the roots of error-locator polynomials up to degree n = 11. Berlekamp, Rumsey, and Solomon [21] discuss the solutions of algebraic equations over fields. Fedorenko and In [22], Trifonov's procedure is developed to calculate the syndromes of decoders. In [23-24], various decoding methods and syndrome computation methods are discussed. Rong et al., [24] give a decoding algorithm for correcting the errors having Lee weight ≤ 5.

Schmidt et al., [25] give a new methodology for decoding Reed–Solomon codes. Algebraic decoding methods are discussed in [26-27].

The Error correction capability of linear block codes is dependent on the minimum distance between the codewords of a code.

In [28], permutation is applied to the rows of matrix and distance preserving mapping is proposed. In [29-30], distance- increasing mapping is developed by mapping the rows of binary elements to the set of vectors of natural numbers of equal length. In distance increasing mapping as discussed in [30] the minimum Hamming distance is increased by 2.

In [31], the application of permutation of arrays which is used in constructing DPM is discussed in power line communication. In DPM established by Swart and Ferreira [32], it was observed that mapping satisfies the upper bound on the sum of the Hamming distances. Shao Xia and Zhang Weidang [33] give shortening of turbo codes by designing interleavers with variable interleaving spans by using the concept of shortening the codes. Marc P. C. Fossorier and Shu Lin [34] ordered statistics-based soft-decision decoding which can be used for any binary block code and does not require any data storage. Martin et al., [35] give the working for the search of the closest codeword to the input through encoding and decoding procedures for different sequences. Godoy et al., [36] give decoding for codes based on available adaptive information sets. In [37] the real-time modified information set-based decoding algorithms for block codes are discussed. Brante et al., [38] give the decoding methodology based on the bit positions in the information set. The performance is very close to the maximum likelihood decoder. Guo et al., [39] give how to use the information set-based decoding algorithm for cryptographic applications. Chang et al., [40] suggest a method to construct constant composition codes by using DIM which is useful in powerline communication. Theo G. Swart and Hendrik C. Ferreira [41] established a decoding method for decoding the codes obtained with the help of DPM. B. Honary and G. Markarian [42] give a new simple encoder and trellis decoder for Golay codes. Cheng et al., [43] construct the method for finding the most suitable symbol mapping with the help of iterative decoding.

This extensive literature survey based on algebraic methods of encoding and decoding and the study of various distance-preserving and distance-increasing mapping techniques builds the foundation for this research work.

III. CONTROL SYSTEM THEORY FOR THE DESIGN OF MODIFIED LINEAR BLOCK CODES

Consider a completely controllable linear discrete-time control system as follows:

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

In this equation, input to the system is denoted by u (k), x (k) represents the system variable at any given time instant t, and real-time system matrices are denoted by A and b. Considering the smallest third-order system, x (o) represents the initial condition as $[1\ 1\ 1]^T$.

Kalman proposed the law of controllability of the control system. According to him, any nth-order control system can be stepped down to the origin in n sampling intervals. The connection between linear systems and codes was discussed by Rosenthal [1].

When the system defined by equation (1) is sampled at various instants of time, as per Kalman's principle last sample of the solution of the given system is found to be an all-zero vector. All the solutions after sampling can be used to form a linear block code and it is discussed in the further section.

IV. DESIGNING OF GENERATOR MATRIX

Consider the following system of equations applied to equation number (1):

Let

$$x(k+1) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -6 & -11 & -6 \end{bmatrix} x(k) + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} u(k) \text{.....} \quad (2)$$

As discussed in [7], equation number (1) will have the following solution:

$$x(k) = A^k x(0) + \sum_{j=0}^{k-1} A^j bu(k-1-j) \text{.....(3)}$$

By considering a third-order system, when the initial condition is considered as an all-one vector [1 1 1] and applied to the above set of equations (2) and (3), that is by solving expression number (2), with the help of equation number (3), the last sampling is observed to be an all-zero vector.

As per the theory of error control coding, the generator matrix G is expressed as $G = [I: P]$, where I is an identity matrix and P is the matrix obtained by arranging the transpose of the above solutions: x (0), x (1), and x (2) as the rows of P. In other words, P is the Upper Triangular Matrix (UTM), obtained from the basis vectors. $H = [P^T: I]$ where H is the parity check matrix. This code satisfies all the properties of a linear block code, namely, $GH^T = O$ and

$HC^T = O$.

The generator matrix for the above discussed system will be as follows:

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix} \quad \text{.....(4)}$$

A similar generator matrix can be obtained for any n^{th}-order completely controllable system in general.

V. CONSTRUCTION OF PERMUTATION ARRAYS FOR DIM

It is interesting to notice that when any (n, k) linear block code is constructed from the generator matrix designed in the above section, it satisfies the properties such as $GH^T = 0$ and $HC^T = 0$ but the established code turns out to be a single error detecting code having the minimum distance dmin as 2.

In this section, permutation arrays (PAs) are constructed with the help of the solution space of CCDTS described by equation (1). These PAs will be the 'P' part of G = [I: P]. DIM is constructed with the help of PAs. It is observed with the help of constructed DIM, when the modified linear block is again experimented it turns out to be a multiple error detecting and error correcting code.

Permutation arrays for DIM of fifth-order CCDTS:

Now, consider a fifth-order system as follows: UTM for the fifth-order system:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Generator matrix for this is

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \text{.....(5)}$$

Coctruction of DIM:

Transforming UTM by columnwise addition of all rows for odd order as follows:

$$P = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} \text{.....(6)}$$

Now the generator matrix by using this transformed matrix is as follows:

$$G_{NEW} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \text{.....(7)}$$

The increased distance modified linear block code (IDMLBC) obtained from the above generator matrix is (10, 5), (n, k) code, and with the help of DIM, the minimum distance between the code words for this (10,5) code is found

to be increased by 2. For (10, 5) IDMLBC, now, d_{min} = 4, and the code is now single error correcting and double error detecting code.

This DIM can be applied to any higher order CCDTS for designing higher order codes with even improved error correction capability. Decoding of the designed codes can be done by existing decoding algorithms.

VI. AN ALGORITHM FOR THE CONSTRUCTION OF A GENERATOR MATRIX FOR INCREASED DISTANCE LINEAR BLOCK CODE

In this section, an algorithm is designed for the construction of generator matrix for IDMLBC. Figure 1 gives the flow chart of the discussed construction.

Input: n^{th} odd-order completely controllable discrete- time system
Output: Generator matrix G= [I: P] for increased distance linear block code.

Steps to be followed:

1: Consider a n^{th} odd-order completely controllable discrete-time system $x(k+1) = Ax(k) + bu(k)$
2: Get the solution of this system by considering the initial condition of the system as n^{th} order all one vectors.
3: Solution space will lead to an upper triangular matrix
4: Use permutations of arrays method to transform the established UTM
5: Get the modified first row of the matrix by adding all the rows of UTM
6: If the modified first row has a total number of ones ≤ 5, go to step 8
7: If the modified first row has a total number of ones > 5, go to step 14
8: Perform the rotation of the first modified row by one bit to the right side to establish the second modified row of the matrix
9: Step 8 will be repeated for the rest of the remaining (n-2) rows and get the completely modified matrix
10: Use this modified matrix as a P part in the generator matrix
11: Do the experimental simulation work using MATLAB to get the generator matrix G = [I :P], where I is an n^{th}-order identity matrix
12: Get all the codewords of the designed code and do the simulation for calculating the increased distance
13: dmin should be ≤ 4. Stop.
14: Use a different way of permutation of arrays as mentioned below:
Perform the addition of all the rows of UTM, leaving the sixth and last row to get the modified first row of the transformed matrix. This processing will lead to an increase in the dmin parameter of the designed code and will increase its error correction capability.
15: If the total number of available zeros are found to be equal to 2, go to step 18
16: If the total number of available zeros are found to
be ≤ 4, go to step 20
17: If the total number of available zeros are found to be ≥ 5, go to step 22
18: Now, repeat steps 8 to 12
19: Computed dmin using simulation = 4. Stop
20: Now, repeat steps 8 to 12
21: Computed dmin using simulation = 2 + the available number of zeros in the transformed first row of the processed matrix. Stop
22: Now, repeat steps 8 to 12
23: Computed dmin using simulation = The count of zeros in the transformed first row of the processed matrix. Stop

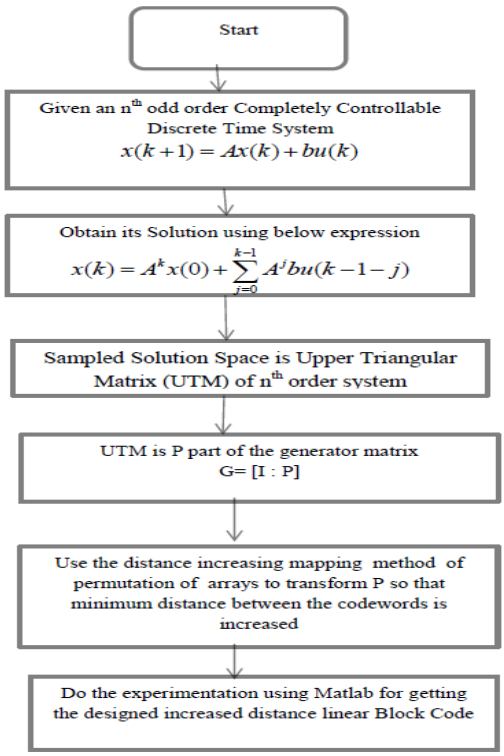

Figure1. Flow chart for designing of Increased Distance Linear Block Code

VII. RESULTS

With the help of the constructed DIM in above section 5, we have designed the following IDMLBC mentioned in Table 1:

Table 1. Comparison of designed IDMLBC with existing codes

Code	(n, k)	Code rate	d_{min}	Modulation scheme
Hamming Code	(7,4)	0.571	3	16 QAM
Designed IDMLBC	(10,5)	0.5	4	16 QAM
Designed IDMLBC	(18,9)	0.5	5	16 QAM
Designed IDMLBC	(34,17)	0.5	6	16 QAM
Designed IDMLBC	(22,11)	0.5	6	16 QAM
Designed IDMLBC	(28,14)	0.5	6	16 QAM
Designed IDMLBC	(30,15)	0.5	6	16 QAM
Hamming Code	(15,11)	0.733	3	16 QAM
Hamming Code	(31,26)	0.838	3	16 QAM

Hamming Code	(255,247)	0.968	3	16 QAM
Designed IDMLBC	(36,18)	0.5	8	16 QAM

Figure 2, 3, and 4 give the simulation results of the BER performance of our designed IDMLBC. Also comparison of the BER performance of these designed codes and the existing codes are presented in Figures 1, 2, and 3.

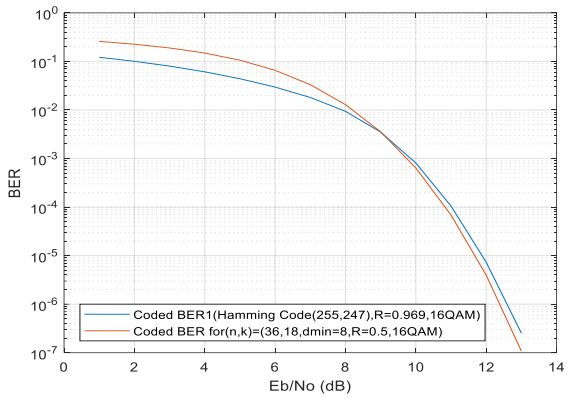

Figure 2. Eb/No versus BER: [(36, 18) IDMLBC Vs (255,247) Hamming]

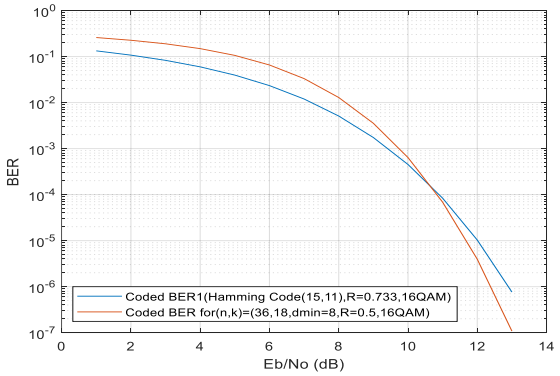

Figure 3. Eb/No versus BER: [(36, 18)IDMLBC Vs (15,11) Hamming**]**

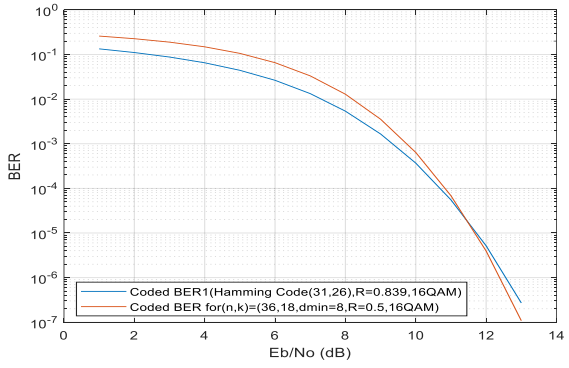

Figure 4. Eb/No versus BER: [(36, 18)IDMLBC Vs (31,26)Hamming]

Analytical Result

Lemma: For a given control system, the solution space of any n^{th} order system can be transformed to an upper triangular Matrix of the same order. Such an UTM when used as 'P' part of the generator matrix G [I:P] can be used as to construct linear block code.

Remark: By applying Kalman's principle to the initial state in which all one vector [1 1 1....1] can be steered to the origin that is all zero vector [0 0 0....0] when arranged in the matrix form leads to an upper triangular matrix.

VIII. CONCLUSION

In this research work the generator matrix is designed for increased distance modified linear block code from the solution space of a CCDTS. The bit error rate performance of the code has been verified with the help of experimental work. In the process of designing the generator matrix, DIM is constructed which is the major contribution of the work and can be used to design any higher order and higher length codes. These designed codes can be used in high-frequency radio environments for transmission and reception of signals. Based on the performed analytical and experimental research, the result in the form of Lemma is also discussed.

Conflict of interest: The author declares no competing interests.

REFERENCES

[1] Rosenthal, J. (2001) Connections between linear systems and convolutional codes. In: Marcus, B., Rosenthal, J. (eds) Codes, Systems, and Graphical Models. The IMA Volumes in Mathematics and its Applications, vol 123. Springer, New York, NY. https://doi.org/10.1007/978-1-4613-0165-3_2

[2] Rosenthal, J. (1999). An optimal control theory for systems defined over finite rings. In: Blondel, V., Sontag, E.D., Vidyasagar, M., Willems, J.C. (eds) Open Problems in Mathematical Systems and Control Theory. Communications and Control Engineering. Springer, London. https://doi.org/10.1007/978-1-4471-0807-8_38

[3] Kalman, R.E. (1960) On the general theory of control systems. In: IFAC Proceedings. Volume 1, 491-502. https://doi.org/10.1016/S1474-6670(17)70094-8

[4] Talmale, S., Unnikrishnan, S., Lande, B.K. (2019) Decoding algorithm for modified linear block code with syndrome polynomial. In: International Conference on Advances in Computing, Communication and Control (ICAC3), pp. 1-6, Mumbai, India. https://doi.org/10.1109/ICAC347590.2019.9036747

[5] Akbari, M., Gillespie, N.I. (2018) Increasing the minimum distance of codes by twisting. The electronic journal of Combinatorics 25(3), P3.36. https://doi.org/10.37236/5852

[6] Talmale, S., Unnikrishnan, S., Lande, B.K. (2017) A modified block code using controllability of linear system. In: International Conference on Advances in Computing, Communication and Control (ICAC3), Mumbai India. https://doi.org/10.1109/ICAC3.2017.8318774

[7] Talmale, S., Unnikrishnan, S., Lande, B.K. (2019) Modified linear block code with code rate 1/2 and less than 1/2. Journal of Discrete Mathematical Sciences and Cryptography, pp. 139-150. https://doi.org/10.1080/09720529.2019.1576335

[8] Seema Talmale, Srija Unnikrishnan, B.K.Lande, "3 Bit Error Correcting Modified Linear Block Code" *Indian Patent,* 415002.Application no. 202221010400, Dec. 2022

[9] Lee, K. (2004) New distance-preserving maps of odd length. IEEE Transaction on Information Theory, Vol. 50, Issue no. 10. https://doi.org/10.1109/TIT.2004.834742

[10] Talmale, S., Unnikrishnan, S., Lande, B.K. (2019) Distance preserving mapping and simple intelligent decoder for a modified block code. International Journal of Information Technology and Electrical Engineering, Volume 8, Issue 5, pp. 71-77. https://api.semanticscholar.org/CorpusID:208278483

[11] Lin, J-S., Chang, J-C., Chen, R-J., Kløve, T. (2008) Distance-preserving and distance-increasing mappings from ternary vectors to permutations. IEEE Transaction on Information Theory, Vol. 54,

[12] No. 3. https://doi.org/10.1109/TIT.2007.915706

[13] Chee, Y.M., Purkayastha, P. (2012) Efficient decoding of permutation codes obtained from distance preserving maps. In: IEEE International Symposium on Information Theory Proceedings, Cambridge, MA, USA. https://doi.org/10.1109/ISIT.2012.6284273

[14] Agashe S.D., Lande B. K. (1952) A new approach t state-transfer problem. J. Franklin Inst., Vol. 333(B), No. 1, pp. 15-21, 1996. https://doi.org/10.1016/0016-0032(96)00004-X

[15] Huffman D.A., (1952) Method for the construction of minimum redundancy Codes. In: Proceedings of the Institute of Radio Engineers, Vol. 40, pp. 1098-1101. https://doi.org/10.1109/JRPROC.1952.273898

[16] Rosenthal J. (1997) Some interesting problems in systems theory which are of fundamental importance in coding theory. In: Proc. of the 36th Conference on Decision & Control San Diego, Califomia USA. https://doi.org/10.1109/CDC.1997.649698

[17] Chen X., Reed I. S., Helleseth T., Truong T.K. (1994) Use of grobner bases to decode binary cyclic codes up to the true minimum distance. IEEE Transaction Information Theory, Vol.40, No.5, pp. 1654 – 1661. https://doi.org/10.1109/18.333885

[18] Reed I. S., Yin X., Truong T. K. (1990) "Algebraic decoding of the (32, 16, 8) quadratic residue code," *IEEE Trans. Inf. Theory,* vol. 36, no. 4, pp. 876–880. https://doi.org/10.1109/18.53750

[19] Tomás V., Rosenthal J., Smarandache R. (2012) Decoding of convolutional codes over the erasure channel. IEEE Transaction Informatio Theory, Vol. 58, No. 1, pp. 90 – 108. https://doi.org/10.1109/TIT.2011.2171530

[20] Truong K., Shih P., Su K., Lee D., Chang Y.(2008) Algebraic decoding of the (89, 45, 17) quadratic residue code. IEEE Trans. Infor. Theory, Vol.54, no. 11, pp. 5005 – 5011.

[21] https://doi.org/10.1109/TIT.2008.929956

[22] Truong T. K., Jeng J. H., Reed I. S. (2001) Fast algorithm for computing the roots of error locator polynomials up to degree 11 in Reed–Solomon decoders. IEEE Trans. Communication Vol. 49, no. 5, pp. 779–783. doi: 10.1109/26.923801

[23] Berlekamp E. R., Rumsey H., Solomon G. (1967) On the solution of algebraic equations over fields. Information and Control, Vol. 10, no. 6, pp. 553–564. https://doi.org/10.1016/S0019-9958(67)91016-9

[24] Fedorenko S. V., Trifonov P.V. (2002) Finding roots of polynomials over finite fields. IEEE Trans. Commun., Vol. 50, no. 11, pp. 1709–1711.

[25] https://doi.org/10.1109/TCOMM.2002.805269

[26] Lin T. C., Truong T. K., Chen P. D. (2007) A Fast algorithm for the syndrome calculation in algebraic decoding of reed–solomon codes. IEEE Trans. On Comm., Vol.55, No. 12.

[27] https://doi.org/10.1109/TCOMM.2007.910595

[28] Rong C, Helleseth T., Lahtonen J. (1999) On algebraic decoding of the linear calderbank–McGuire code. IEEE Trans. On Infor. Theory, Vol. 45, No. 5. https://doi.org/10.1109/18.771144

[29] Schmidt G, Sidorenko V. R., Bossert M. (2010) Syndrome decoding of Reed–Solomon codes beyond half the minimum distance based on shift-register synthesis. IEEE Trans. on Infor. Theory, Vol. 56, No. 10. https://doi.org/10.1109/TIT.2010.2060130

[30] Lin C., Shih Y., Su K., Truong K. (2010) Algebraic decoding of the (31, 16, 7) quadratic residue code by using Berlekamp-Massey algorithm. In: Proc. of Inc. on Communications and Mobile Computing. https://doi.org/10.1109/CMC.2010.345

[31] Zhang P., Li Y., Chang H.C., Liu H., Truong T.K. (2015) Fast decoding of the (47, 24, 11) quadratic residue code without determining the unknown syndromes. In: IEEE Communications Letters, Vol. 19, No. 8. https://doi.org/10.1109/LCOMM.2015.2440263

[32] Chang J.C., Chen R.J., Kløve T., Tsai S.C. (2003) Distance-preserving mappings from binary vectors to permutations. In: IEEE Transactions on Information Theory, Vol. 49, No. 4, pp. 1054–1059. https://doi.org/10.1109/TIT.2003.809507

[33] Chang J.C. (2005) Distance-increasing mappings from binary vectors to permutations. In: IEEE Transactions on Information Theory, Vol. 51, No. 1, pp. 359–363. https://doi.org/10.1109/TIT.2004.839527

[34] Chang J.C. (2006) Distance-increasing mappings from binary vectors to permutations that increase Hamming distances by at least two. In: IEEE Transactions on Information Theory, Vol. 52, No. 4, pp. 1683–1689. https://doi.org/10.1109/TIT.2006.871037

[35] Ferreira H.C., Vinck A.J.H. (2000) Inference cancellation with permutation trellis arrays. In: Proc. IEEE Vehicular Technology Conference. http://dx.doi.org/10.1109/VETECF.2000.883295

[36] Swart T.G., Ferreira H.C. (2006) Multilevel construction for mapping from binary sequences to permutation sequences. In: Proc. of IEEE International Symposium on Information Theory, Seattle, USA. https://doi.org/10.1109/ISIT.2006.261810

[37] Shao X., Zhang W. (2015) Shortening the turbo codes based on unequal error protection. In: International Journal of Multimedia and Ubiquitous Engineering, Vol. 10, No. 8, pp. 73–82. http://dx.doi.org/10.14257/ijmue.2015.10.8.08

[38] Fossorier M.P.C., Lin S. (1995) Soft-decision decoding of linear block codes based on ordered statistics. In: IEEE Transactions on Information Theory, Vol. 41, No. 5, pp. 1379–1396. https://doi.org/10.1109/18.412683

[39] Martin P.A., Taylor D.P., Fossorier M.P.C. (2002) Soft-input soft-output list-based decoding algorithm. In: Proc. of IEEE International Symposium on

[40] Information Theory. https://doi.org/10.1109/ISIT.2002.1023611

[41] Godoy W., Wille E.C.G., Cunha J.A.T. (2010) Adaptive decoding of binary linear block codes using information sets and erasures. In: Proc. of IEEE Inc. on Communication Theory, Reliability, and Quality of Service. https://doi.org/10.1109/CTRQ.2010.41

[42] Godoy W., Wille E.C.G. (2006) A simple acceptance criterion for binary block codes soft-decision algorithms. In: Proc. of IEEE Inc. on AICT-ICIW. https://doi.org/10.1109/AICT-ICIW.2006.33

[43] Brante G.G. de O., Muniz D.N., Godoy W. (2011) Information set based soft-decoding algorithm for block codes. In: IEEE Latin America Transactions, Vol. 9, No. 4, pp. 463–469. https://doi.org/10.1109/TLA.2011.5993729

[44] Guo Q., Johansson T., Mårtensson E., Stankovski P. (2017) Information set decoding with soft information and some cryptographic applications. In: Proc. of IEEE International Symposium on Information Theory. https://doi.org/10.1109/isit.2017.8006838

[45] Chang J.C., Tsai I.T., Wu H.L. (2010) Efficient decoding algorithm for constant composition codes. In: Proc. of International Symposium on Information Theory & Its Applications. https://doi.org/10.1109/isita.2010.5648975

[46] Swart T.G., Ferreira H.C. (2007) Decoding distance-preserving permutation codes for power-line communications. In: Proc. of IEEE AFRICON, pp. 1–7. https://ieeexplore.ieee.org/document/4401563

[47] Honary B., Markarian G. (1993) New simple encoder and trellis decoder for Golay codes. In: Electronics Letters, Vol. 29, No. 25, pp. 2170–2171. https://doi.org/10.1049/el:19931456

[48] Cheng Q., Xu X., Zhou S., Xiao L. (2005) A new labeling search method for bit-interleaved coded modulation with iterative decoding. In: Proc. of IEEE Vehicular Technology Conference. https://doi.org/10.1109/vetecs.2005.154335