The Eurasia Proceedings of Science, Technology,
Engineering & Mathematics (EPSTEM)
ISSN: 2602-3199

The Eurasia Proceedings of Science, Technology, Engineering and Mathematics (EPSTEM), 2025

Volume 38, Pages 151-158

IConTES 2025: International Conference on Technology, Engineering and Science

On LDPC Codes and Their Construction

Mohammed Amine Tehami
Djillali Liabes University of Sidi Bel Abbes

Malika Tehami
Djillali Liabes University of Sidi Bel Abbes

Boucif Beddad
Djillali Liabes University of Sidi Bel Abbes

Ahmed Hadji
Djillali Liabes University of Sidi Bel Abbes

Abstract: In this paper, we propose a novel method for constructing low-density parity-check (LDPC) codes that relies on circulant permutation matrices as the main principal elements. A key feature of this construction is the intentional avoidance of short cycles, particularly those of length four, which are known to degrade decoding performance. By eliminating these cycles, the approach contributes to lowering both encoding and decoding complexity, making the codes more efficient to implement. To assess their effectiveness, the proposed LDPC codes are evaluated and compared with uncoded binary phase shift keying (BPSK) transmission over an additive white Gaussian noise (AWGN) channel. The simulation outcomes demonstrate that the structured codes deliver competitive results, achieving error-rate performance similar to, and in some instances exceeding, well-known designs such as progressive edge growth (PEG) and quasi-cyclic (QC) codes.

Keywords: LDPC codes, Parity check matrix, Circulant permutation matrix, Girth, Bit error rate

Introduction

Low-Density Parity-Check (LDPC) codes, originally introduced by Gallager (1962), have attracted significant attention owing to their strong error-correcting capability and their potential to operate close to the Shannon capacity limit (Chung et al., 2001**).** As a subclass of linear block codes (Lin & Costello, 2004), they are defined through a sparse parity-check matrix H, of dimensions M×N, which contains only a small proportion of ones relative to zeros, hence the designation "low-density." Depending on the uniformity of the number of ones across rows and columns, LDPC codes are categorized as regular or irregular. The design of such codes requires careful consideration of parameters such as row and column weights, the girth of the associated Tanner graph, and the overall code length. Two principal design strategies exist: random (unstructured) (MacKay, 1999) and deterministic (structured) constructions (Shin et al., 2014; Moura et al., 2004; Tehami & Djebbari, 2018, 2019). While random approaches are straightforward and often yield strong performance, they typically demand substantial memory resources for encoding and decoding, particularly at large block lengths, which can result in high computational cost 'sometimes a more critical limitation than the error rate itself' (Tehami & Djebbari, 2018).

To overcome the limitations of random constructions, several structured design approaches have been introduced (Gallager, 1963; Richardson & Urbanke, 2008). By enforcing regular patterns in the parity-check matrix H, these methods facilitate more efficient hardware implementations for both encoding and decoding

- Selection and peer-review under responsibility of the Organizing Committee of the Conference

(MacKay, 1999). In such constructions, the connections between rows and columns follow predefined rules, which contribute to reducing overall system complexity (Fossorier, 2004; Kou et al., 2001; Lin & Costello, 2004; Zhong & Zhang, 2005; Zhang et al., 2008). Structured LDPC codes are particularly advantageous for short block lengths, where they often outperform their random counterparts (MacKay, 1999; Richardson & Urbanke, 2008). Nevertheless, they also exhibit inherent constraints, especially with respect to achievable code rates, block lengths, and girth, and their performance tends to deteriorate as the block length increases (Gallager, 1963; Kou et al., 2001).

The Tanner graph offers a useful graphical representation of the LDPC decoding process (Tanner, 1981). It is a bipartite graph composed of two types of nodes: variable nodes, corresponding to the columns of H, and check nodes, corresponding to the rows. The edges connecting these nodes define the overall structure of the code. Within this framework, a cycle refers to a closed path formed by a sequence of edges, and the girth of the graph denotes the length of its shortest cycle. Short cycles, particularly those of length four, are especially detrimental because they reduce the independence of the messages exchanged during iterative decoding, which in turn degrades the overall performance (Zhang et al., 2008). Although quasi-cyclic LDPC (QC-LDPC) codes provide several advantages, their encoding process continues to pose significant challenges. This issue has been addressed in multiple studies. A class of globally coupled (GC) LDPC codes was proposed by Zhu & Yang (2022), combining local LDPC structures with an overarching global parity constraint. This design achieves strong performance while maintaining relatively low complexity, yet the encoding process remains difficult to implement efficiently. Likewise, Mo et al. (2020) introduced in a new family of LDPC codes that can be encoded through approximate lower triangulation (ALT) (Richardson & Urbanke, 2001), which relies on row and column permutations of the parity-check matrix. Nevertheless, despite these efforts, decoding complexity remains substantial.

In this work, we present a novel category of LDPC codes that are explicitly constructed to eliminate length-4 cycles, thereby reducing both encoding and decoding complexity while delivering excellent bit error rate performance in the waterfall region. The remainder of the correspondence is organized as follows: Section 2 details the methodology for constructing the parity-check matrix H, emphasizing strategies for avoiding 4-cycles and discussing the impact of girth on LDPC performance. Section 3 analyzes encoding complexity, with particular attention to the role of column weights in determining the minimum distance and the trade-off between performance and implementation cost. Section 4 examines decoding complexity, showing its dependence on the number of branches in the Tanner graph and discussing the role of the belief propagation algorithm. Comparisons are also made with the codes of Gallager and MacKay in terms of branch density. Section 5 reports simulation results obtained via Monte Carlo experiments over an AWGN channel. Finally, Section 6 summarizes the key findings and concludes the paper.

Method

The girth, defined as the length of the shortest cycle within the Tanner graph of an LDPC code, is a critical parameter that strongly influences code performance. Some studies (Fossorier, 2004; Tanner, 1981; Hu et al., 2001, 2005; Richardson, 2003) have reported that increasing the girth can result in a higher error floor, whereas simulation-based investigations (MacKay & Postol, 2003) suggest that a larger girth typically improves bit-error-rate (BER) performance, which is generally adequate for practical use. For this reason, the development of LDPC codes with girth values greater than four has become a topic of considerable interest for real-world applications (Kou et al., 2001). The method proposed in this work focuses on constructing LDPC codes that completely eliminate 4-cycles. To achieve this, the parity-check matrix H, of size M×N (where M denotes the number of rows and N the number of columns), is generated through a two-step design procedure.

Step 1

The procedure starts with the construction of an identity matrix I of dimension m×m, where m is assumed to be an even integer. A new matrix C is then generated by reflecting I vertically while keeping the columns unchanged. More precisely, each element $C_{i,j}$ is defined as the entry of I located at row m+1−i and column j. This operation can be expressed as:

$$C_{i,j}=I_{m+1-i,j} \quad (1)$$

For i,j= 1,2,… ,m.

Step 2

To obtain the matrix C^k, a circular shift of k columns is applied to the identity matrix I, which has size m×m. This shift moves each column to the right by k positions.
This transformation can be defined using matrix multiplication:

$$C^k=I.P^k \tag{2}$$

Where
I is the m×m identity matrix.
P is a circular permutation matrix that performs a one-position leftward shift of the columns.
P^k indicates the matrix P raised to the kth power, effectively rotating the columns by k steps.
The full matrix H, having size $m^2 \times m^2$, is built through the systematic placement of the identity matrix and its shifted submatrices C^k, according to the following structure:

$$H=\begin{pmatrix} C & C & C & \dots & C \\ C & C^1 & C^2 & \dots & C^n \end{pmatrix} \tag{3}$$

Here, n denotes the number of shifted submatrices, is given by:

$$n=m-1 \tag{4}$$

Example

First, consider the 4×4 identity matrix

$$I=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Next, C^1 is obtained by applying a left circular shift of one position to I. This operation can be expressed as:

$$C^1=I.P^1=\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

where P^1 is the permutation matrix that performs a one-step right circular shift of the columns. Following the same procedure, the matrices $C^2=I.P^2$ and $C^3=I.P^3$ are generated by applying two-step and three-step right circular shifts, respectively:

$$C^2=I.P^2=\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$C^3=I.P^3=\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

By following the structure in (3), the resulting 8 × 16 parity-check matrix is obtained as:

$$H=\begin{pmatrix} 0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1\\ 0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0\\ 0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\ 1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\ 0&0&0&1&1&0&0&0&0&1&0&0&0&0&1&0\\ 0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0\\ 0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0\\ 1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1 \end{pmatrix}$$

Encoding Complexity

Gallager (1963) demonstrated that the minimum distance of LDPC codes grows only logarithmically with code length when the column weight equals 2. In contrast, when the column weight is at least 3, the minimum distance increases linearly with code length (Gallager, 1962). Such codes have shown effectiveness in several applications, including partial-response channels (Song et al., 2002; Song et al., 2004). Their relatively low computational demand stems from the reduced column weight. Despite these advantages, practical hardware implementation remains challenging (Malema & Liebelt, 2007) due to the random distribution of row–column connections and the typically large size of LDPC codes. Structured codes were later introduced to alleviate this complexity, providing more regular interconnections while maintaining good performance (Malema & Liebelt, 2007). Furthermore, constraining the row–column connections has been used to control the girth, i.e., the length of the shortest cycle in the Tanner graph (Fossorier, 2004).

Increasing the girth generally leads to improved decoding performance, as larger cycles reduce the likelihood of short, error-prone loops (O'Sullivan, 2006; Mao & Banihashemi, 2001). In summary, both structured design and girth optimization contribute significantly to enhancing the efficiency of LDPC codes. The structure of the parity-check matrix has a decisive impact on the efficiency of LDPC encoding (Tehami & Djebbari, 2019; Richardson & Urbanke, 2001). The proposed method, based on a sparse design of the submatrices C^k, offers several advantages:

- A sparse parity-check matrix H significantly reduces the memory required to store parity information (MacKay, 1999; Tehami & Djebbari, 2018).
- The use of permutation matrices contributes to an efficient and well-organized structure (Fossorier, 2004).
- Thanks to its sparsity, H enables low encoding complexity, making it highly suitable for practical implementations (Song et al., 2004).

Decoding Complexity

The decoding complexity of LDPC codes is primarily determined by the number of branches Br in the Tanner graph, or equivalently, by the number of nonzero entries ('1's) in the parity-check matrix (Berrou, 2010). The iterative decoding process, based on the belief propagation algorithm, involves multiple stages. At each iteration, both the extrinsic and total information associated with each node must be computed (Divsalar et al., 2009). For a regular code (N, W_C, W_R), where W_C and W_R denote the column and row weights respectively. The number of branches can be expressed as:

$$Br=W_C*N=W_R*M \tag{5}$$

Table 1. Comparison of proposed LDPC codes with Gallager codes and Mackay codes.

Block length	Proposed codes	Gallager codes	Mackay codes
N=500 and M=250	Br=1500	Br=1500	Br=1500
N=1000 and M=500	Br=2000	Br=3000	Br=3000

As shown in Table 1, the proposed LDPC codes require fewer branches compared to Gallager and Mackay codes. This reduction implies that the corresponding parity-check matrices H are sparser (containing fewer ones relative to zeros), which directly contributes to lowering the decoding complexity.

Results and Discussion

Monte Carlo simulations were performed to investigate the bit error rate (BER) performance of the proposed LDPC codes (MacKay, 1999). The iterative belief propagation (BP) algorithm was adopted as the decoding method (Gallager, 1963), and transmission was assumed over an additive white Gaussian noise (AWGN) channel. For simulation purposes, a code rate of R= 1/2 and a block length of N=4368 were selected. Each simulation involved at least 103 transmitted codewords, with the maximum number of decoding iterations capped at 80. The obtained results are presented in comparison with conventional LDPC codes to highlight the relative performance of the proposed design. The signal-to-noise ratio (SNR) definitions for both coded and uncoded binary phase-shift keying (BPSK) follow O'Sullivan (2004). Specifically:

$$SNR_{coded}=10\ \log_{10}\ (E_b/2\sigma^2R) \quad (6)$$

$$SNRuncoded=10\ \log10\ (E_b/2\sigma2) \quad (7)$$

Where Eb and σ^2 represent energy per bit and noise variance, respectively.

Figure 1 illustrates the BER performance of the proposed LDPC codes in comparison witn uncoded BPSK transmission. The parameters considered are: N=4368, W_C =2 and a code rate R=1/2. For reference, in BPSK-modulated system operating over a Gaussian channel, the BER is given by

$$BER=Q(SNR)^{1/2} \quad (8)$$

where the function Q represents the tail function of the normal distribution.

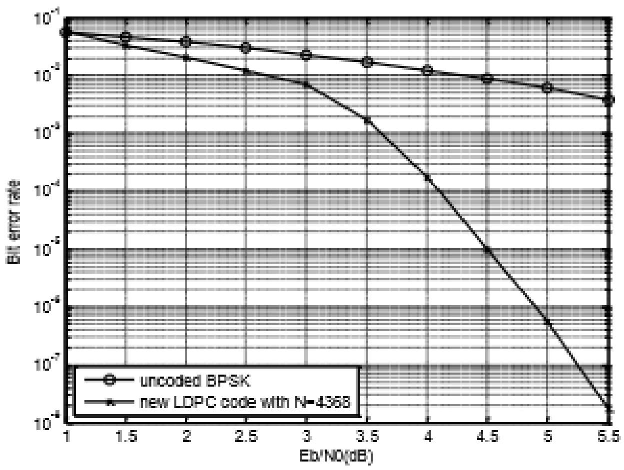

Figure 1. BER performance for the proposed LDPC codes for N=4368 and W_C= 2.

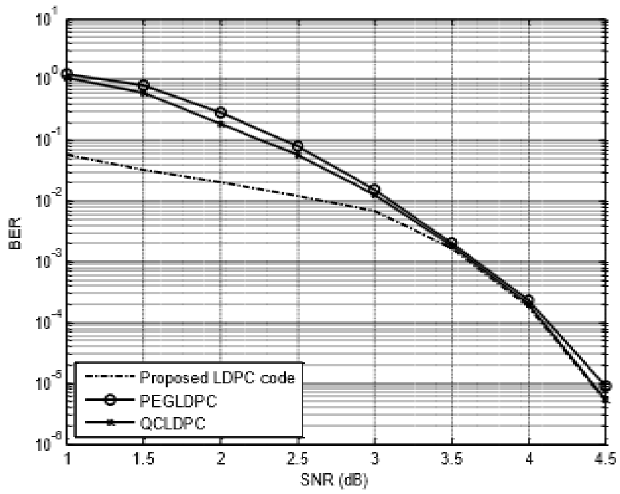

Figure 2. Comparison of BER performance between the proposed LDPC codes, PEG-LDPC codes and QCLDPC codes in the waterfall region.

As shown in Figure 1, the proposed LDPC code clearly outperforms uncoded BPSK. At a BER of 10^{-2}, a performance gain of approximately 1.95 dB is observed. This improvement can be attributed to the efficiency of LDPC codes with column weight W_C=2, which provide a significant advantage over uncoded transmission in terms of error-rate reduction. Figure 2 shows the BER performance of the proposed LDPC codes with N=4368 over the AWGN channel in the waterfall region. At a BER of 10^{-2}, the proposed codes achieve a gain of approximately 0.4 dB compared with both PEG LDPC and QC LDPC codes. Furthermore, at a BER of 10^{-3}, they outperform PEG-LDPC codes by about 0.05 dB. This performance improvement is mainly attributed to the simplified encoding process and the elimination of girth-4 cycles.

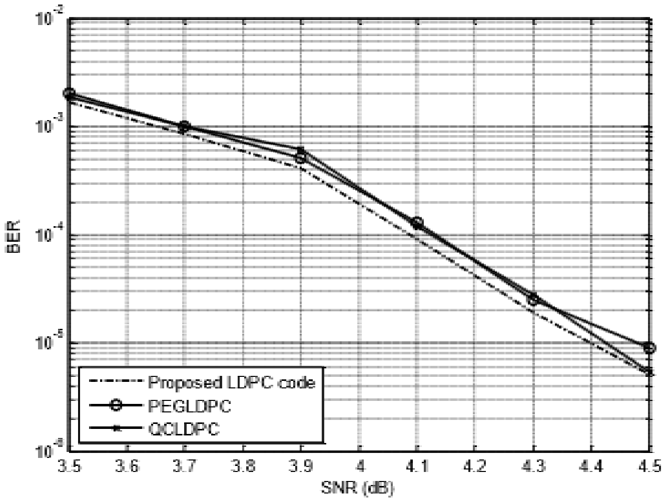

Figure 3. Comparison of BER performance between the proposed LDPC codes, PEG-LDPC codes and QCLDPC codes in the low error-floor region.

Figure 3 shows the BER performance of the proposed LDPC codes over the AWGN channel in the low error-floor region. At a BER of 10^{-4}, the proposed codes achieve a performance gain of about 0.5 dB compared to QC-LDPC codes. At a BER of 10^{-5}, they still provide a slight improvement over PEG-LDPC codes. These results indicate that the proposed design is able to approach the error-floor region even for large block lengths.

Conclusion

To address both implementation constraints and reception quality, LDPC codes must achieve a low error floor while maintaining reduced encoding and decoding complexity. In this work, we introduced a construction method for parity-check matrices that eliminates short cycles across different code rates. Additionally, the adoption of quasi-cyclic structures significantly lowers memory requirements. Simulation results confirm that the proposed LDPC codes exhibit strong performance over the AWGN channel, demonstrating their efficiency and practical applicability.

Scientific Ethics Declaration

* The authors declare that the scientific ethical and legal responsibility of this article published in EPSTEM journal belongs to the authors.

Conflict of Interest

* The authors declare that they have no conflicts of interest

Funding

* This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Acknowledgements or Notes

* This article was presented as a poster presentation at the International Conference on Technology, Engineering and Science (www.icontes.net) held in Antalya/Türkiye on November 12-15, 2025.

References

Berrou, C. (2010). *Codes and turbo-codes*. ENST Bretagne.

Chung, S., Forney, G. D., & Richardson, T. J. (2001). On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit. *IEEE Communications Letters, 5*(2), 58–60.

Divsalar, D., Dolinar, S., Jones, C. R., & Andrews, K. (2009). Capacity-approaching protograph codes. *IEEE Journal on Selected Areas in Communications, 27*(6), 876–888.

Fossorier, M. P. C. (2004). Quasi-cyclic low-density parity-check codes from circulant permutation matrices. *IEEE Transactions on Information Theory, 50*(8), 1788–1793.

Gallager, R. G. (1962). Low-density parity-check codes. *IRE Transactions on Information Theory, 8*(1), 21–28.

Gallager, R. G. (1963). *Low-density parity-check codes*. MIT Press.

Hu, X.-Y., Eleftheriou, E., & Arnold, D.-M. (2001). Progressive edge-growth Tanner graphs. *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM)*, 995–1001.

Hu, X.-Y., Eleftheriou, E., & Arnold, D.-M. (2005). Regular and irregular progressive edge-growth Tanner graphs. *IEEE Transactions on Information Theory, 51*(1), 386–398.

Kou, Y., Lin, S., & Fossorier, M. (2001). Low-density parity-check codes based on finite geometries: A rediscovery and new results. *IEEE Transactions on Information Theory, 47*(7), 2711–2736.

Lin, S., & Costello, D. J. (2004). *Error control coding: Fundamentals and applications* (2nd ed.). Prentice Hall.

MacKay, D. J. C. (1999). Good codes based on very sparse matrices. *IEEE Transactions on Information Theory, 45*(2), 399–431.

MacKay, D. J. C., & Postol, M. J. (2003). Weaknesses of Margulis and Ramanujan–Margulis low-density parity-check codes. *Electronic Notes in Theoretical Computer Science, 74*, 97–104.

Malema, G., & Liebelt, M. (2007). Quasi-cyclic LDPC codes of column-weight two using a search algorithm. *EURASIP Journal on Applied Signal Processing, 2007*(1), 1–8.

Mao, Y., & Banihashemi, A. H. (2001). A heuristic search for good low-density parity-check codes at short block lengths. *Proceedings of the IEEE International Conference on Communications*, 41–44.

Mo, S., Chen, L., Costello, D. J., Mitchell, D. G. M., Smarandache, R., & Qiu, J. (2020). Designing protograph-based quasi-cyclic spatially coupled LDPC codes with large girth. *IEEE Transactions on Communications, 68*(9), 5326–5337.

Moura, J. A., Abdel-Ghaffar, N. H., Rosenthal, J., & Smarandache, R. (2004). Algebraic constructions of LDPC codes with no short cycles. *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, 39.

Moura, J. M. F., Lu, J., & Zhang, H. (2004). Structured low-density parity-check codes. *IEEE Signal Processing Magazine, 21*(1), 42–55.

O'Sullivan, M. E. (2006). Algebraic construction of sparse matrices with large girth. *IEEE Transactions on Information Theory, 52*(2), 718–727.

Richardson, T. J. (2003). Error floors of LDPC codes. *Proceedings of the 41st Annual Allerton Conference on Communication, Control, and Computing*, 1426–1435.

Richardson, T. J., & Urbanke, R. L. (2001). Efficient encoding of low-density parity-check codes. *IEEE Transactions on Information Theory, 47*(2), 638–656.

Richardson, T. J., & Urbanke, R. L. (2008). *Modern coding theory*. Cambridge University Press.

Shin, B., Park, H., Hong, S., No, J. S., & Kim, S. H. (2014). Quasi-cyclic LDPC codes using overlapping matrices and their layered decoders. *AEU - International Journal of Electronics and Communications, 68*(5), 379–383.

Song, H., Liu, J., & Kumar, B. V. K. (2002). Low complexity LDPC codes for partial response channels. *Proceedings of the IEEE Global Telecommunications Conference*, 1294–1299.

Song, H., Liu, J., & Kumar, B. V. K. (2004). Large girth cycle codes for partial response channels. *IEEE Transactions on Magnetics, 40*(4), 3084–3086.

Song, L., Cruz, R., & Kumar, B. V. K. V. (2004). Low-density parity-check codes for partial response channels. *IEEE Transactions on Magnetics, 40*(2), 507–512.

Tanner, R. M. (1981). A recursive approach to low complexity codes. *IEEE Transactions on Information Theory, 27*(5), 533–547.

Tehami, M. A., & Djebbari, A. (2018). Low density parity check codes constructed from Hankel matrices. *Journal of Telecommunications and Information Technology, 3*, 37–41.

Tehami, M. A., & Djebbari, A. (2019). A new method for building low density-parity-check codes. *International Journal of Technology, 10*(3), 611–618.

Yahya, A., Sidek, O., & Salleh, M. (2009). A new quasi-cyclic low density parity check codes. *Proceedings of the IEEE Symposium on Industrial Electronics & Applications*, 239–242.

Zhang, F., Mao, X., Zhou, W., & Pfister, H. D. (2008). Girth-10 LDPC codes based on 3-D cyclic lattices. *IEEE Transactions on Vehicular Technology, 57*(2), 1049–1060.

Zhong, H., & Zhang, T. (2005). Block-LDPC: A practical LDPC coding system design approach. *IEEE Transactions on Circuits and Systems I: Regular Papers, 52*(4), 766–775.

Zhu, K., & Yang, H. (2022). Constructing girth eight GC-LDPC codes based on the GCD FLRM matrix with a new lower bound. *Sensors, 22*(19), 7247.

Author(s) Information

Mohammed Amine Tehami
Djillali Liabes University of Sidi Bel Abbes
Telecommunications and Digital Signal Processing Laboratory, Djillali Liabes University, P.O. Box 89 – 22000 Sidi Bel Abbes, Algeria
Contact e-mail : *chahoub_88@yahoo.com*

Malika Tehami
Djillali Liabes University of Sidi Bel Abbes
Applied Materials Laboratory, Research Center (CFTE), Djillali Liabes University, P.O. Box 89 – 22000 Sidi Bel Abbes, Algeria

Boucif Beddad
Djillali Liabes University of Sidi Bel Abbes
Telecommunications and Digital Signal Processing Laboratory, Djillali Liabes University, P.O. Box 89 – 22000 Sidi Bel Abbes, Algeria

Ahmed Hadji
Djillali Liabes University of Sidi Bel Abbes
Telecommunications and Digital Signal Processing Laboratory, Djillali Liabes University, P.O. Box 89 – 22000 Sidi Bel Abbes, Algeria

To cite this article:

Tehami, M. A., Tehami, M., Beddad, B & Hadji, A. (2025). On LDPC codes and their construction. *The Eurasia Proceedings of Science, Technology, Engineering and Mathematics (EPSTEM), 38,* 151-158.