Methods of information systems synthesis

UDC 519.728:512.74 **doi:** https://doi.org/10.20998/2522-9052.2026.2.03

Sergii Dunaiev[1], Stanislav Milevskyi[1], Oleksandr Kushnerov[2], Vladyslav Sokol[1], Oleksandr Voitko[3]

[1] National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
[2] Sumy State University, Sumy, Ukraine
[3] National Defence University of Ukraine, Kyiv, Ukraine

CONSTRUCTION OF LDPC CODES GENERATING MATRIX

Abstract. This paper presents a detailed analysis of the problem of constructing encoders for linear block codes, with a special emphasis on low-density parity-check (LDPC) codes. **The aim of this paper** is to provide a comprehensive description of the mathematical methods for the transition from the verification matrix to the efficient coding process. Both classical linear algebra approaches and specialized methods for sparse matrices. **Results.** The fundamental algebraic constructions underlying the duality between the generating and checking matrices over Galois fields, in particular GF (*2*), are considered. The classical Gaussian exclusion method for systematic coding is analyzed in detail and its shortcomings in the context of LDPC codes, related to the fill-in phenomenon and loss of sparsity, are revealed. The central place in the study is occupied by the Approximate Lower Triangulation method proposed by Richardson and Urbanky, which allows achieving linear coding complexity. The article contains a detailed description of matrix preprocessing algorithms, mathematical derivation of formulas for calculating parity bits, as well as an analysis of quasicyclic constructions used in modern telecommunications standards (5G, Wi-Fi). Full numerical examples of transformations for low-dimensional codes and a detailed analysis of the LDPC encoder architecture are given. **Conclusion.** The solution was to abandon the explicit use of the generating matrix in favor of approximate triangulation methods of the check matrix and the use of quasicyclic structures, which has become standard in 5G and Wi-Fi. The integration of algebraic-geometric methods opens up new prospects for creating codes with specified properties.

Keywords: low-density parity-check codes; generator matrix; parity-check matrix; approximate lower triangulation; quasi-cyclic LDPC; Gaussian elimination; linear encoding complexity.

Introduction

In the modern era of digital communications, data transmission reliability is a critical requirement. From fiber optic backbones to fifth-generation (5G) wireless networks and satellite communications, channel coding techniques are used everywhere to correct errors caused by noise, interference, and signal attenuation. Among the variety of error-correcting codes (ECC), Low-Density Parity-Check (LDPC) codes occupy a special place [1, 2].

Proposed by Robert Gallagher in his doctoral dissertation in 1960, LDPC codes remained "forgotten" for a long time due to the lack of computing power required for their decoding. Their "renaissance" in the 1990s, following the discovery of turbo codes, revolutionized information theory, as it was proven that LDPC codes allow approaching the Shannon limit - the theoretical maximum channel capacity – when using iterative decoding algorithms (Belief Propagation) [3, 4].

However, despite the decoding efficiency, the problem of encoding LDPC codes has long remained non-trivial [5]. Classical linear block codes are defined by a generating matrix *G*, multiplication by which transforms the information vector u into a codeword c. For LDPC codes, which are primarily defined by their check matrix *H* (which describes the constraints, not the method of generation), constructing the matrix *G* is a mathematical challenge [6, 7]. Direct transformation of a sparse matrix *H* into *G* usually results in a dense matrix *G*, which has a quadratic coding complexity of $O(n^2)$ with respect to the block length *n*. Given that modern standards (e.g. DVB-S2) use blocks of length $n \approx 64800$ bits, the quadratic complexity is unacceptable for high-speed systems [8, 9].

The aim of this paper is to provide a comprehensive description of the mathematical methods for the transition from the verification matrix to the efficient coding process. Both classical linear algebra approaches and specialized methods for sparse matrices, in particular the Richardson-Urbankey method, which is the de facto standard in LDPC engineering, are considered.

1. Theoretical foundations of linear block codes over GF (2)

For a deep understanding of the mechanisms of matrix construction, it is necessary to turn to the foundations of linear algebra over finite fields [10].

1.1. Vector spaces and subspaces

Binary linear block code $C(n,k)$ is defined as k-measure linear subspace of a vector space $V_n = \{0,1\}^n$ over the Galois field $GF(2)$. The code parameters have the following interpretation [11]:

- n – codeword length (number of bits transmitted in the channel);
- k – code dimension (number of information bits);
- $r = n - k$ – number of check characters (redundancy).

In the field $GF(2)$ all arithmetic operations are performed modulo 2. Addition is equivalent to the logical operation "exclusive OR" (XOR), and multiplication is equivalent to the logical "AND". An important property is that addition and subtraction in $GF(2)$ are identical operations: $x + y = x - y$ [12].

1.2. Dual definition of code: Image and Core

A linear code can be specified in two complementary ways, each of which relies on a matrix representation.

Generator Matrix. Code C can be considered as the image of a linear mapping given by the matrix G of dimension $k \times n$. The rows of this matrix form the basis of the code subspace. The process of encoding an information vector $u \in \{0,1\}^k$ is described by vector-matrix multiplication:

$$c = u \cdot G,$$

where $c \in C$ – obtained codeword.

Since G has full rank k, this mapping is injective, which guarantees the uniqueness of the codeword for each message.

Parity-Check Matrix. Alternatively, the code C can be defined as the kernel of a linear mapping given by the matrix H of dimension $r \times n$. This matrix describes the system r linear equations that each vector in the space must satisfy in order to be considered a valid codeword. Membership condition of a vector c to code C is written as:

$$c \cdot H^T = 0.$$

Matrix H rows form the basis of the dual space $C^{\perp}$, which is the orthogonal complement of C.

1.3. Orthogonality condition

The fundamental connection between G and H follows from the definition of the code. Since each row of the matrix G is a valid codeword, it must satisfy the parity checks specified by the matrix H. This means that the dot product of any string G on any line H (transposed column H^T) is equal to zero. In matrix form, this condition is written as:

$$G \cdot H^T = 0_{k \times r},$$

where $0_{k \times r}$ – zero matrix of the corresponding dimension. This equation is the key to the algorithmic construction of one matrix based on another.

2. Methods for constructing the generator matrix

2.1. Algorithm for constructing the generating matrix: Classical approach

In the general case, when we are dealing with an arbitrary linear code (for example, a Hamming code or a short-length BCH code), the transition from H to G is carried out by reducing the matrix to a systematic form. This process is based on the Gaussian elimination method [13].

Systematic code form. A code is called systematic if, in each codeword, the information bits are located at fixed positions (usually at the beginning) and the check bits follow them (or vice versa). For the verification matrix H a systematic form is the representation:

$$H_{sys} = [\, P \mid I_{n-k} \,],$$

where P –submatrix of dimension $r \times k$; I_{n-k} (or I_r) – unit matrix of dimension $r \times r$.

If the original matrix H does not have this form, it can be reduced to it using elementary row operations and column permutations.

Mathematical derivation of G from H_{sys}. Consider the parity check equation for a systematic code. Let the codeword be c divided into an informational part u (of length k) and the verification part p (of length r):

$$c = [\, u \mid p \,].$$

Equation $H \cdot c^T = 0$ takes the form:

$$[\, P \mid I_r \,] \cdot \begin{bmatrix} u^T \\ p^T \end{bmatrix} = 0.$$

Performing block multiplication, we get:

$$P \cdot u^T + I_r \cdot p^T = 0.$$

In the field $GF(2)$ addition is equal to subtraction, so we can carry the addition:

$$p^T = P \cdot u^T.$$

Transpose both sides of the equation to express the row vector p:

$$p = (P \cdot u^T)^T = u \cdot P^T.$$

Now we can write down the complete codeword c through the information vector u:

$$c = [\, u \mid p \,] = [\, u \mid u \cdot P^T \,] = u \cdot [\, I_k \mid P^T \,].$$

Since by definition $c = u \cdot G$, we obtain an explicit expression for the systematic generating matrix:

$$G_{sys} = [\, I_k \mid P^T \,].$$

So, the construction algorithm consists in selecting the submatrix P from a systematic form H and transposing it to form the right-hand side G.

Example of construction for code above a field $GF(2)$ in dimension 3. Let's consider the construction of matrices for a specific example according to the query ("code over field 2 in 3"). We interpret this as a length code $n = 3$ over $GF(2)$ with parameters $(3,2)$.

Step 1: Defining the verification matrix H.

For the code $(3,2)$ we have $n = 3, k = 2, r = 1$. Parity check equation (sum of all bits is 0):

$$c_1 + c_2 + c_3 = 0.$$

Matrix H has dimension of 1×3:

$$H = [1 \quad 1 \quad 1].$$

Step 2: Reduction to a systematic view.

Matrix H already looks like $[\, P \mid I_1 \,]$, where $I_1 = [1]$. Submatrix $P = [1 \quad 1]$.

Step 3: Construction of G.

We use the formula $G = [\, I_k \mid P^T \,]$. Here $k = 2$, then $I_k = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Transposed matrix $P^T = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$.

Let's combine them: $G = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$.

Verification:

$$G \cdot H^T = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1+1 \\ 1+1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

The orthogonality condition is satisfied.

2.2. Specificity of LDPC codes: Density problem

LDPC codes are defined by the fact that their check matrix H is sparse [14, 15]. This is a key property for the efficiency of iterative decoding.

However, using the Gaussian method to obtain H_{sys} leads to a *fill-in* effect. As a result, the submatrix P (and therefore G) becomes dense.

Implications for the coder:

- *Quadratic complexity:* Multiplication by a dense matrix G requires $O(n^2)$ operations. For $n \approx 64800$ (DVB-S2) that's billions of operations per word.
- *Memory requirements:* Dense matrix storage G requires significant resources.

Therefore, modern LDPC systems use coding methods directly through a sparse matrix H [16].

2.3. Richardson-Urbanki Method: Linear LDPC Coding

The Approximate Lower Triangulation (ALT) method allows to minimize the complexity of coding [17, 18].

Structure H_{ALT}. The goal is to bring H by permutations to the form:

$$H_{ALT} = \begin{pmatrix} A & B & T \\ C & D & E \end{pmatrix},$$

where the matrix T – sparse lower triangular matrix.

Algebraic derivation. Code word vector:

$$x = [s^T, p_1, p_2].$$

The system of equations breaks down into:

1. $As^T + Bp_1^T + Tp_2^T = 0$;
2. $Cs^T + Dp_1^T + Ep_2^T = 0$.

Parity finding algorithm:

1. Calculate p_1 from the equation

$$\varphi\, p_1^T = z,$$

where $\varphi = D - E\,T^{-1}\,B$ –gap matrix of size $g \times g$; $z = ET^{-1}As^T - Cs^T$.

2. Calculate p_2 by the method of inverse substitution through a triangular matrix T:

$$Tp_2^T = -A(s^T + Bp_1^T).$$

With a small gap size g coding complexity approaches linear $O(n)$.

2.4. Quasicyclic (QC-LDPC) codes: The modern standard

The 5G NR, Wi-Fi 6 (802.11ax) and DVB-S2 standards use a special subclass of LDPC codes – Quasi-Cyclic (QC) [5]. Check matrix H is built from an array of circulants (cyclically shifted identity matrices). This allows hardware-level encoding to be implemented using linear feedback shift registers (LFSRs) with high efficiency and minimal memory overhead.

Construction of a binary LDPC matrix. Let the verification matrix H be given of size 6×12 over the field $GF(2)$.

$$H = \left[\begin{array}{cccccc|cccccc} 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right].$$

Pay attention to the right side of the matrix (last 6 columns). It has a characteristic "bidiagonal" structure:

$$H_p = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

This matrix corresponds to the block T in the Richardson-Urbanki method (with $g = 0$).

Suppose we want to find parity p for vector $s = [1,0,1,0,1,0]$.

1. *Calculate the syndrome* $y = H_s \cdot s^T$:

$$y = [0,0,1,1,0,0]^T.$$

2. *Let's solve the system* $H_p \cdot p = y$ (back substitution):

$$p_1 = 0, p_1 + p_2 = 0 \Rightarrow p_2 = 0, p_2 + p_3 = 1 \Rightarrow p_3 = 1,$$
$$p_3 + p_4 = 1 \Rightarrow p_4 = 0, \ldots$$

Result: $p = [0,0,1,0,0,0]$. Full codeword

$$c = [\, s \mid p \,].$$

Construction of a non-binary LDPC code based on algebraic geometry (HEC). In addition to classical binary codes, consider constructing a check matrix for a non-binary code over the field $GF(4)$, using the Jacobian points of the hyperelliptic curve (HEC).

Construction parameters:

The code is built on a Galois field $GF(2^2)$, elements of which $\{0,1,\alpha,\alpha^2\}$ generated by a primitive polynomial $p(x) = x^2 + x + 1$.

Field properties: $\alpha^2 = \alpha + 1, \alpha^{-1} = \alpha^2$.

*Curve and matrix:*Curve used:

$$y^2 + (x^2 + \alpha x + 1)y = x^5 + x^3 + x + 1.$$

Verification matrix H_{NB} (Non-Binary) formed from points on a curve:

$$H_{NB} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & \alpha & \alpha \\ 1 & \alpha & \alpha^2 & 0 & \alpha & \alpha & \alpha^2 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

ALT encoding for $GF(4)$*:* System of equations for parity p over $GF(4)$ requires the use of inverse elements in the back substitution. Example of a solution fragment: If $\alpha^2 \cdot p_2 = S_2$, then $p_2 = S_2 \cdot (\alpha^2)^{-1} = S_2 \cdot \alpha$. This demonstrates that the Richardson-Urbankey method is successfully adapted for non-binary codes, providing higher error correction efficiency.

3. Discussion of the results of applying the proposed approaches to LDPC code construction

The development of modern 6G technologies requires further improvement not only in ensuring the appropriate level of information transmission speed, but also in ensuring security services [20–22]. For the first time, this applies to security services - confidentiality, integrity and authenticity [23–25].

Tables 1 and 2 show a comparison of the characteristics of 5G and 6G technologies, as well as a comparative analysis of the effectiveness of LDPC codes.

The analysis of Tables 1 and 2 showed that the use of LDPC codes is a promising area of research.

Table 1 – **Comparison of 5G and 6G characteristics**

№	Parameter	5G	6G
1	Data transfer rate	From 0.1 Gbps to 20 Gbps	From 1 Gbit/s to 1 Tbit/s
2	Reliability	Probability of error < 10^{-5}	Probability of error < 10^{-9}
3	Delay	Less than 5 ms	Less than 100 ns
4	Localization accuracy	Less than 10 cm in two dimensions	Less than 1 cm in three dimensions
5	Cryptography support	TLS/SSL	TLS/SSL + new encryption models
6	Coding mechanisms	Turbo, LDPC	LDPC, Polar, Post-Quantum Coding
7	AI support	Limited	Built-in (AI-native)

Table 2 **– Comparative analysis of the LDPC codes` efficiency**

Code type	Decoding difficulty	Corrective ability	Transmission speed	Resistance to attacks	Suitability for 6G
Hamming	Low	Medium (up to 1–2 bits/block)	High	Low	Limited
Reed-Solomon (RS)	High	High for block errors	Medium	Medium	Used in narrow channels
Turbo-codes	High	Very high	Medium	High	Used in 4G/5G
LDPC- codes	Medium	Very high (up to Shannon limit)	High	Very high (up to 40% BER reduction during channel attacks)	Optimal for 6G
Polar- codes	Medium	High at low SNR	High	High	Used in 5G, promising for 6G in combination with LDPC

In addition, works [26–28] proposed asymmetric cryptosystems that provide the necessary level of security in the post-quantum period (level 5–6 according to the requirements of the NIST Competition for post-quantum algorithms), and also integrated error control.

Work [29, 30] considered the issue of building crypto-code constructions based on LDPC codes.

Table 3 presents a comparative analysis of the characteristics of LT and LDPC codes.

The use of LDPC codes provides the possibility of creating post-quantum cryptosystems that can be used in smart technologies and mobile technologies, as well as 5–6G technologies [31, 32]

Table 4 shows the comparative characteristics of wireless and mobile Internet technologies.

Thus, to ensure security in SCFS, it is proposed to use post-quantum algorithms – crypto-code constructions, which, unlike modern mechanisms of security services (standards KNX, IEEE802.11h, IEEE802.16e – use symmetric encryption algorithms) allow to provide the required level of crypto-resistance.

Table 3 **– Comparative analysis of the LT and LDPC codes characteristics**

Characteristic	LT codes	LDPC codes
Encoding type	Stochastic, fountain codes	Linear block codes
Code rate	Dynamic, without fixed speed (adaptive)	Predefined, fixed structure
The need for a return channel	No need	Used to achieve optimal performance
Computational complexity	Encoding: low; decoding: moderate	Encoding: complex; decoding: multi-step, iterative
Broadcast support	Complete, high efficiency	Limited implementation possibilities
High loss resilience	High – preserve data recoverability	Average – depends on the parity check matrix parameters
Application in 6G systems	High suitability (scalability, flexibility)	High efficiency under stable channel conditions
Decoding method	Iterative	Iterative
Code redundancy	Adjusts dynamically depending on channel quality	Fixed for a given code structure
Computational complexity	O(KlogK)	From O(n) to $O(n^2)$, depending on the matrix density

Table 4 – **Comparative characteristics of wireless and mobile Internet technologies**

Technology	Providing security services					Degree of information confidentiality (βi)				
	A_i^C	A_i^I	A_i^A	A_i^{Au}	A_i^{Inv}	1,0	0,75	0,5	0,25	0,01
LTE (4G), LTE (5G)	–	–	+	–/+	–/+	–	–	–	–	–
IEEE 802.11 ac (WiFi 5)	–	–	+	–/+	–/+	–	–	–	–	–
IEEE 802.11ax, Wi-Fi 6+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE 802.16+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE802.16m (WiMAX2)	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE 802.15.1 Bluetooth 5+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE 802.15.4+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
Mobile technologies + *CCC* на *EC* (*MEC*)	+	+	+	+	+	+	+	+	+	+
Mobile technologies + *HCCC* на *EC* (*MEC*)	+	+	+	+	+	+	+	+	+	+
Mobile technologies + *CCC* на *LDPC-кодах*	+	+	+	+	+	–	–	+	+	+

$A_i^C, A_i^I A_i^A, A_i^{Au}, A_i^{Inv}$ – security services (A_i^C – confidentiality, A_i^I – integrity, A_i^A – accessibility, A_i^{Au} – authenticity, A_i^{Inv} – involvement); β_i – metric of the time and degree of information secrecy ratio (critical – 1,0; high – 0,75; medium – 0,5; low – 0,25; very low – 0,01).

In addition, crypto-code constructions on the proposed LDPC, algebraic and/or algebro-geometric codes allow to provide an integrated increase in the level of reliability (due to their error correction properties), efficiency (in terms of crypto-transformation speed, they are compatible with symmetric cryptography algorithms) and the required level of energy consumption, the results of comparative studies are given in the works [33–35].

Conclusions

The construction of the generating matrix *G* from the check matrix *H* is a fundamental problem in coding theory. For classical codes, this is a trivial linear algebra problem. However, for LDPC codes, the classical approach is unacceptable due to the loss of sparsity. The solution was to abandon the explicit use of *G* in favor of approximate triangulation (ALT) methods of the *H* matrix and the use of quasicyclic structures (QC-LDPC), which has become standard in 5G and Wi-Fi. The integration of algebraic-geometric methods (HEC) opens up new prospects for creating codes with specified properties.

Conflicts of interest

The authors declare that they have no conflicts of interest in relation to the current study, including financial, personal, authorship, or any other, that could affect the study, as well as the results reported in this paper.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the current work.

REFERENCES

1. Guruswami, V. (2006), *Iterative Decoding of Low-Density Parity Check Codes - CMU School of Computer Science*, University of Washington Seattle, WA 98195, 29 p., available at: https://www.cs.cmu.edu/~venkatg/pubs/papers/ldpc.pdf
2. Nozaki, T. (2016), "Parallel Encoding Algorithm for LDPC Codes Based on Block-Diagonalization", *2015 IEEE International Symposium on Information Theory* (ISIT), IEEE, China, doi: https://doi.org/10.1109/ISIT.2015.7282788
3. Zeng, Z., Feng, Y. and Sun, X. (2012), "An efficient LDPC encoder for CMMB using RU method", Procedia Engineering, vol. 29, pp. 1851–1855, doi: https://doi.org/10.1016/j.proeng.2012.01.225
4. Kuchuk, N., Mozhaiev, M., Kalinin, Y., Mozhaev, O. and Kuchuk, H. (2022), "Calculation of Signal Information Delay in Intelligent Communication Networks", *2022 IEEE 3rd KhPI Week on Advanced Technology*, KhPI Week 2022 - Conference Proceedings, doi: https://doi.org/10.1109/KhPIWeek57572.2022.9916323
5. Khodaiemehr, H. and Kiani, D. (2017), "Construction and Encoding of QC-LDPC Codes Using Group Rings", *IEEE Transactions on Information Theory*, vol. 63, is. 4, pp. 2039–2060, doi: https://doi.org/10.1109/TIT.2017.2655029
6. Nguyen, T. T. B., Nguyen Tan, T., and Lee, H. (2019), "Efficient QC-LDPC Encoder for 5G New Radio", *Electronics*, vol. 8(6), 668, doi: https://doi.org/10.3390/electronics8060668
7. İbrahimov B.G., Hasanov A.H. and Hashimov E.G. (2024), "Research and analysis of efficiency indicators of critical infrastructures in the communication system", *Advanced Information Systems*, vol. 8, no. 2, pp. 58–64, doi: https://doi.org/10.20998/2522-9052.2024.2.07
8. Yevseiev, S., Rzayev, K., Korol, O., and Imanova, Z. (2016), "Development of mceliece modified asymmetric crypto-code system on elliptic truncated codes", *Eastern-European Journal of Enterprise Technologies*, vol. 4(9(82)), pp. 18–26, doi: https://doi.org/10.15587/1729-4061.2016.75250
9. Rezanov, B., and Kuchuk, H. (2023), "Model of elemental data flow distribution in the Internet of Things supporting Fog platform", *Innovative Technologies and Scientific Solutions for Industries*, no. 3(25), pp. 88–97, doi: https://doi.org/10.30837/ITSSI.2023.25.088

10. Kuchuk, G., Kovalenko, A., Kharchenko, V. and Shamraev, A. (2017), "Resource-oriented approaches to implementation of traffic control technologies in safety-critical I&C systems", *Studies in Systems, Decision and Control*, vol. 105, pp. 313–337, doi: https://doi.org/10.1007/978-3-319-55595-9_15
11. Yevseiev, S., Korol, O., and Kots, H. (2017), "Construction of hybrid security systems based on the crypto-code structures and flawed codes", *Eastern-European Journal of Enterprise Technologies*, vol. 4(9 (88), pp. 4–21, doi: https://doi.org/10.15587/1729-4061.2017.108461
12. Kuchuk, G., Kharchenko, V., Kovalenko, A. and Ruchkov, E. (2016), "Approaches to selection of combinatorial algorithm for optimization in network traffic control of safety-critical systems", *Proceedings of 2016 IEEE East-West Design and Test Symposium*, EWDTS 2016, 7807655, doi: https://doi.org/10.1109/EWDTS.2016.7807655
13. Zhang, T., Li, C., Wu, X. and Wu, Y. (2024), "Reconstruction of LDPC code sparse check matrix based on modified LBP decoding", *Tongxin Xuebao Journal on Communications*, vol. 45(5), pp. 70–79, doi: https://doi.org/10.11959/j.issn.1000-436x.2024097
14. Pathak, R. and Awasthi, S.K. (2025), "Implementation of Low-Density Parity-Check (LDPC) Codes in Verilog HDL", *International Conference on Electronics AI and Computing Innovating for A Sustainable and Connected Future Eaic 2025*, doi: https://doi.org/10.1109/EAIC66483.2025.11101329
15. Vladyslav, Y. and Kosenko, V. (2024), "Low-power coding method in data transmission systems", *Innovative technologies and scientific solutions for industries*, no. 3 (29), pp. 121–129, doi: https://doi.org/10.30837/2522-9818.2024.3.121
16. Li, C., Zhang, T., Wu, Y. and Wu, X. (2025), "Reconstruction of QC-LDPC code sparse check matrix based on spatial compression", *Systems Engineering and Electronics*, vol. 47(10), pp. 3504–3511, doi: https://doi.org/10.12305/j.issn.1001-506X.2025.10.33
17. Ruban, I., Kuchuk, H., Kovalenko, A., Lukova-Chuiko, N. and Martovytsky, V. (2021), "Method for Determining the Structural Reliability of a Network Based on a Hyperconverged Architecture", *Studies in Computational Intelligence*, vol. 976, pp. 147–163, doi: https://doi.org/10.1007/978-3-030-74556-1_9
18. Balamurugan, K. and Janakiraman, N. (20250, "An Effective Non-linear Distortion Elimination and Data Transmission Using Hybrid BCH-LDPC Coding and 64-APSK Modulator Scheme in Satellite Forward Link", *Lecture Notes in Electrical Engineering*, 1323 LNEE, pp. 453–464, doi: https://doi.org/10.1007/978-981-96-1587-2_35
19. Mozhaev, O., Kuchuk, H., Kuchuk, N., Mykhailo, M. and Lohvynenko, M. (2017), "Multiservice network security metric", *2nd International Conference on Advanced Information and Communication Technologies*, AICT 2017 – Proceedings, pp. 133–136, doi**:** https://doi.org/10.1109/AIACT.2017.8020083
20. Kharchenko, V., Andrashov, A., Sklyar, V., Kovalenko, A. and Siora, O. (2013), "Gap-and-IMECA-Based Assessment of I&C Systems Cyber Security", *Complex Systems and Dependability. Advances in Intelligent and Soft Computing*, vol 170, Springer, Berlin, Heidelberg, https://doi.org/10.1007/978-3-642-30662-4_10
21. Korchenko, O. G., Tereikovskyi, I. A., Korystin, O. Y., Tereikovska, L. O. and Tereikovskyi, O.I. (2026), "A method for detecting financial phishing in instant messengers using an ensemble of dialogical intelligent assistants based on large language models", *Herald of Advanced of Information Technology*, vol. 9, no. 1, pp. 71–84, doi: https://doi.org/10.15276/hait.09.2026.06
22. Yevseiev, S., Korol, O., and Kots, H. (2017), "Construction of hybrid security systems based on the crypto-code structures and flawed codes" *Eastern-European Journal of Enterprise Technologies*, vol. 4(9 (88), pp. 4–21, doi: https://doi.org/10.15587/1729-4061.2017.108461
23. Dmitrishin, D. V., Khamitov, V. M., Antoshchuk, S.G. and Boltenkov, V. O. (2026), "A modified image encryption algorithm based on the chaotic Tent map", *Herald of Advanced of Information Technology*, vol. 9, no. 1, pp. 9–19, doi: https://doi.org/10.15276/hait.09.2026.01
24. Kuchuk, N., Kashkevich, S., Radchenko, V., Andrusenko, Y. and Kuchuk, H. (2024), "Applying edge computing in the execution IoT operative transactions", *Advanced Information Systems*, vol. 8, no. 4, pp. 49–59, doi: https://doi.org/10.20998/2522-9052.2024.4.07
25. Yevseiev, S., Tsyhanenko, O., Ivanchenko, S., Aleksiyev, V., Verheles, D., Volkov, S., Korolev, R., Kots, H., Milov, O., and Shmatko, O. (2018), "Practical implementation of the Niederreiter modified cryptocode system on truncated elliptic codes", *Eastern-European Journal of Enterprise Technologies*, vol. 6(4 (96), pp. 24–31, doi: https://doi.org/10.15587/1729-4061.2018.150903
26. Soloviova, D. V., Antoshchuk, S. G. and Boltenkov, V. O. (2026), "Research into the Possibilities of Improving Proof-of-Work Blockchain Technology", *Herald of Advanced of Information Technology*, vol. 7, no. 2, pp. 131–146, doi: https://doi.org/10.15276/hait.07.2024.9
27. Lada, N. and Rudnytska, Y. (2022), "Implementation of a method for synthesizing groups of symmetric double-operand operations of cryptographic information coding for block encryption systems *Innovative technologies and scientific solutions for industries*, no. 2 (20), pp. 35–43, doi: https://doi.org/10.30837/ITSSI.2022.20.035
28. Kuchuk, H., Kalinin, Y., Dotsenko, N., Chumachenko, I. and Pakhomov, Y. (2024), "Decomposition of integrated high-density IoT data flow", *Advanced Information Systems*, vol. 8, no. 3, pp. 77–84, doi: https://doi.org/10.20998/2522-9052.2024.3.09
29. Yevseiev, S., Tsyhanenko, O., Gavrilova, A., Guzhva, V., Milov, O., Moskalenko, V., Opirskyy, I., Roma, O., Tomashevsky, B., and Shmatko, O. (2019), "Development of Niederreiter hybrid crypto-code structure on flawed codes", *Eastern-European Journal of Enterprise Technologies*, vol. 1(9 (97), pp. 27–38, doi: https://doi.org/10.15587/1729-4061.2019.156620
30. Rezanov, B. And Kuchuk, H. (2022), Fast Two-Factor Authentication Method in Systems With a Centralized User's Database, *2022 IEEE 4th KhPI Week on Advanced Technology*, KhPI Week 2022 – Conference Proceedings, 03-07 October 2022, Code 183771, doi: https://doi.org/10.1109/KhPIWeek57572.2022.9916491
31. Kharchenko, V., Kovalenko, A., Andrashov, A. and Siora, A. (2012), "Cyber security of FPGA-based NPP I&C systems:challenges and solutions", *8th International Conference Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies*, San Diego, California, Westin San Diego, available at: https://www.researchgate.net/publication/319292444_CYBER_SECURITY_OF_FPGA-BASED_NPP_IC_SYSTEMS_CHALLENGES_AND_SOLUTIONS

32. Petrović, V. L., El Mezeni, D. M., and Radošević, A. (2021), “Flexible 5G New Radio LDPC Encoder Optimized for High Hardware Usage Efficiency”, *Electronics*, vol. 10(9), article number: 1106, doi: https://doi.org/10.3390/electronics10091106
33. Yevseiev, S., Hryshchuk, R., Zakovorotnyi, O., Milov, O., Kuchuk, H. and Milevskyi, S. (2024), “Intelligent Control and Security Systems Models Synthesis Methodology for Critical Infrastructure Objects”, *2024 IEEE 5th International Conference on Advanced Trends in Information Theory*, pp. 275–281, doi: https://doi.org/10.1109/ATIT64324.2024.11222460
34. Pohasii, S., Yevseiev, S., Zhuchenko, O., Milov, O., Lysechko, V., Kovalenko, O., Kostiak, M., Volkov, A., Lezik, A., and Susukailo, V. (2022), “Development of crypto-code constructs based on LDPC codes”, *Eastern-European Journal of Enterprise Technologies*, vol. 2(9 (116), pp. 44–59., doi: https://doi.org/10.15587/1729-4061.2022.254545
35. Milevskyi, S., Korol, O., Mykytyn, G., Lozova, I., Solnyshkova, S., Husarova, I., Hrebeniuk, A., Vlasov, A., Sukhoteplyi, V., and Balagura, D. (2024), “Development of the sociocyberphysical systems` multi-contour security methodology”, *Eastern-European Journal of Enterprise Technologies*, vol. 1(9 (127)), pp. 34–51, doi: https://doi.org/10.15587/1729-4061.2024.298844

Received (Надійшла) 18.11.2025
Accepted for publication (Прийнята до друку) 25.02.2026

ABOUT THE AUTHORS / ВІДОМОСТІ ПРО АВТОРІВ

Дунаєв Сергій Владиславович – аспірант кафедри кібербезпеки, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Sergii Dunaiev – PhD Student of the Department of Cybersecurity, National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine;
e-mail: serg.dynaev@gmail.com; ORCID Author ID: https://orcid.org/0000-0001-8736-3602;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58753666700.

Мілевський Станіслав Валерійович – доктор технічних наук, професор, професор кафедри кібербезпеки, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Stanislav Milevskyi – Doctor of Technical Sciences, Professor, Professor of the Department of Cybersecurity, National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine;
e-mail: milevskiysv@gmail.com; ORCID Author ID: h http://orcid.org/0000-0001-5087-7036;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57211218421.

Кушнерьов Олександр Сергійович – доктор філософії, старший викладач кафедри економічної кібернетики, Сумський державний університет, Суми, Україна;
Oleksandr Kushnerov – PhD, Senior Lecturer, Department of Economic Cybernetics, Sumy State University, Sumy, Ukraine;
e-mail: o.kushnerov@biem.sumdu.edu.ua; ORCID Author ID: https://orcid.org/0000-0001-8253-5698;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58318301800.

Сокол Владислав Євгенович – кандидат технічних наук, докторант кафедри кібербезпеки, Національний технічний університет «Харківський політехнічний інститут», Харків, Україна;
Vladyslav Sokol – Candidate of Technical Sciences, Doctoral Student of Cybersecurity Department, National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine;
e-mail: vladyslav.sokol@gmail.com; ORCID Author ID: https://orcid.org/0009-0009-9446-2049;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=56290096700.

Войтко Олександр Володимирович доктор військових наук, начальник навчально-наукового центру стратегічних комунікацій у сфері забезпечення національної безпеки та оборони, Національний університет оборони України, Київ, Україна;
Oleksandr Voitko – Doctor of Military Sciences, Chief of Educational and Scientific Center of Strategic Communications in the Field of Ensuring National Security and Défense, National Defence University of Ukraine, Kyiv, Ukraine;
e-mail: o.voitko@edu.nuou.org.ua; ORCID Author ID: https://orcid.org/0000-0002-4610-4476;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57210362201.

Побудова породжуючої матриці LDPC-кодів

С. В. Дунаєв, С. В. Мілевський, О. С. Кушнерьов, В. Є. Сокол, О. В. Войтко

Анотація. У цій статті подано детальний аналіз задачі побудови кодерів для лінійних блокових кодів із особливим акцентом на коди з низькою щільністю перевірок парності (LDPC). Метою роботи є надання всебічного опису математичних методів переходу від перевірочної матриці до ефективного процесу кодування. Розглядаються як класичні підходи лінійної алгебри, так і спеціалізовані методи для розріджених матриць. **Результати.** Розглянуто фундаментальні алгебраїчні конструкції, що лежать в основі дуальності між породжувальною та перевірочною матрицями над Galois fields, зокрема GF(2). Детально проаналізовано класичний метод гаусового виключення для систематичного кодування та виявлено його недоліки в контексті LDPC-кодів, пов’язані з явищем «заповнення» (fill-in) і втратою розрідженості. Центральне місце в дослідженні займає метод наближеної нижньої триангуляції, запропонований Tom Richardson та Rüdiger Urbanke, який дозволяє досягти лінійної складності кодування. Стаття містить детальний опис алгоритмів попередньої обробки матриць, математичне виведення формул для обчислення бітів парності, а також аналіз квазіциклічних конструкцій, що використовуються в сучасних телекомунікаційних стандартах, таких як 5G та Wi-Fi. Наведено повні числові приклади перетворень для кодів малої розмірності та детальний аналіз архітектури LDPC-кодера. **Висновки.** Рішенням стало відмовлення від явного використання породжувальної матриці на користь методів наближеної триангуляції перевірочної матриці та застосування квазіциклічних структур, що стало стандартом у 5G і Wi-Fi. Інтеграція алгебро-геометричних методів відкриває нові перспективи для створення кодів із заданими властивостями.

Ключові слова: коди з низькою щільністю перевірок парності; породжувальна матриця; перевірочна матриця; наближена нижня триангуляція; квазіциклічні LDPC; гаусове виключення; лінійна складність кодування.