http://doi.org/10.35784/iapgos.6623

*received: 25.09.2024 | revised: 6.01.2025 | accepted: 21.03.2025 | available online: 31.03.2025*

# MODIFICATION OF THE PETERSON ALGEBRAIC DECODER

**Dmytro Mogylevych[1], Iryna Kononova[2], Liudmyla Pogrebniak[1], Kostiantyn Lytvyn[1], Igor Gyrenko[3]**

[1]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Department of Special Electronic Communications Systems, Kyiv, Ukraine, [2]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Department of Theoretical Foundations of Operation of Special Telecommunication Systems, Kyiv, Ukraine, [3]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Institute of Special Communications and Information Protection, Kyiv, Ukraine

***Abstract.*** *The aim of the study is to increase the reliability of data transmission based on the modification of the Peterson algorithm. The modification of the Peterson algorithm is based on the control of the correctness of the error locator polynomial. An additional stage of checking the error locator polynomial is proposed. This check is carried out using the recursive calculation of syndrome components. This approach increases the reliability of data transmission by reducing the probability of erroneous decoding at noise levels exceeding the constructive minimum of the code distance. The recursive calculation of syndrome components ensures the efficient implementation of the algorithm and minimises computational complexity.*

**Keywords**: algebraic decoder, noise immunity, simulation

## MODYFIKACJA ALGEBRAICZNEGO DEKODERA PETERSONA

***Streszczenie.*** *Celem pracy jest zwiększenie niezawodności transmisji danych w oparciu o modyfikację algorytmu Petersona. Modyfikacja algorytmu Petersona polega na kontroli poprawności wielomianu lokalizatora błędów. Zaproponowano dodatkowy etap sprawdzania wielomianu lokalizatora błędów. Kontrola ta jest przeprowadzana przy użyciu rekurencyjnego obliczania składników syndromu. Podejście to zwiększa niezawodność transmisji danych poprzez zmniejszenie prawdopodobieństwa błędnego dekodowania przy poziomach szumu przekraczających konstruktywne minimum odległości kodowej. Rekursywne obliczanie składowych syndromu zapewnia wydajną implementację algorytmu i minimalizuje złożoność obliczeniową.*

**Słowa kluczowe**: dekoder algebraiczny, rozpoznawanie znaków, symulacyjny

## Introduction

Decoding of block codes is one of the main tasks of coding theory, which has a wide range of applications in modern communication networks. Algebraic decoding methods offer effective and reliable solutions to this problem. The Peterson algorithm is an effective algebraic method for decoding Bose-Chaudhury-Hockvingham codes and other block codes. Its main goal is to correct errors in codewords by constructing and solving a system of equations to find the error locator. The Peterson algorithm is sensitive to errors in syndromes that may arise due to data distortion. This can lead to incorrect determination of the error locator. Therefore, the article proposes a modification of the solution of the key equation of the "direct" Peterson algorithm, which is based on checking the correctness of the error locator polynomial. Correctness is checked by recursively generating the syndrome components. This allows for reducing the probability of erroneous decoding by a constructive threshold.

## 1. Literature review

The research [7] laid the foundation for further research and development of algebraic decoding methods. It describes in detail the basic principles of calculating syndromes, constructing error locator polynomials, and solving equations in the Galois field. In [8], the possibilities of integrating the Peterson algorithm with iterative decoding methods are considered. This is especially relevant for modern communication systems, such as 5G networks. This integration allows for achieving better results in difficult data transmission conditions. In [2], methods for optimizing the decoding process of quasi-cyclic codes with low parity-check density are proposed. These methods enhance the PGZ algorithm and create new opportunities for increasing communication systems' performance.

In [6], mathematical methods and algorithms for error correction, particularly the PGZ algorithm, are presented, and practical recommendations for their application are provided. In [3], the classical Peterson-Gorenstein-Zirler decoding algorithm is considered for a class of alternative codes, including Reed-Solomon, Bose-Chowdhury-Hockvingham, and classical Goppa codes. In addition, the authors propose an improvement of the method for determining the number of errors and constructing the error locator polynomial. In [5], the latest achievements in channel coding and error correction are discussed, and directions for further research are suggested.

The presented studies cover a wide range of aspects of algebraic decoding, from fundamental principles to modern applications. A review of the studies shows that the Peterson algorithm remains a relevant tool for error correction in digital systems. Its modifications are aimed at reducing computational complexity, adapting to modern technologies, integrating with the latest decoding methods, and reducing the probability of erroneous decoding. In general, modern studies of the Peterson algorithm are aimed at adapting it to the requirements of modern technologies and increasing efficiency in various data transmission systems. This ensures its relevance and applicability in future communication and information-processing technologies.

## 2. Description of the Peterson algorithm

An error-correcting decoder solves three tasks: it detects the presence of errors, determines their location, and calculates the error value. The a posteriori information used to solve these tasks is the received vector

$$v(x) = c(x) + e(x),\ deg\{v(x)\} = n-1 \tag{1}$$

$$s(x) = \mathbb{R}_{g(x)}\{v(x)\},\ s_j = v(\alpha^j) = e(\alpha^j) \tag{2}$$

where

$$c(x) = \begin{cases} i(x)g(x), deg\{c(x)\} = n-1 \\ deg\{i(x)\} = k-1 \\ x^{n-k}i(x) + \mathbb{R}_{g(x)}\{x^{n-k}i(x)\} \end{cases} \tag{3}$$

$c(x)$ – allowed code word; $e(x)$ – error vector; $i(x)$ – information; $g(x)$ – forming polynomials satisfying the condition.

$$g(x)h(x) = x^n - 1,\ deg\{g(x)\} = n-k \tag{4}$$

If $s(x) > 0$, then the syndrome's components (2) are used to calculate the polynomial of error locators $\Lambda(x)$, identifying the location of the distortion and determining the value of $\Omega(x)$ errors. A generalised scheme of the decoding algebraic device is shown in Fig. 1.

The error polynomial over $GF(q)[x]$ is defined by the expression

$$e(x) = \sum_{i=0}^{n-1} e_i x^i,\ deg\{e(x)\} = n-1 \tag{5}$$

where no more than $t$ coefficients and $e_i \neq 0$. Otherwise, the behaviour of the decoder is undefined. Probably

$$P_{eras.cc} = 1 - \sum_{j=0}^{q^k-1} \sum_{i=0}^{q^k-1} P\left\{c_j(x) | c_i(x)\right\} \quad (6)$$

the decoder will indicate decoding failure or add additional errors, where $P\left\{u_j(x) | c_i(x)\right\}$ – is the conditional probability of the event "the accepted word is in the $j_{th}$ sphere of attraction".

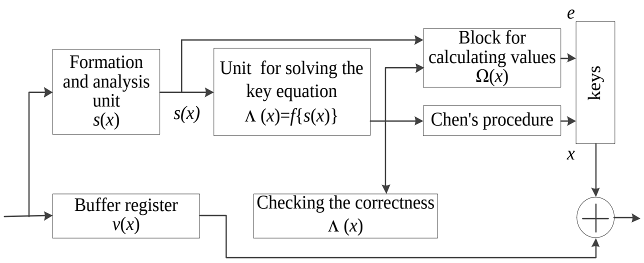



*Fig. 1. Structural scheme of algebraic decoder*

Suppose that there were ν errors corresponding to unknown positions. Then (5) is transformed into the expression

$$e(x) = e_{i1}x^{i1} + e_{i2}x^{i2} + \dots + e_{iv}x^{iv},\ \omega\{e(x)\} = v,\ 1 \le v \le t \quad (7)$$

As a rule, the construction of the code (3) in the $GF(q)$ field is based on the element α, possibly not primitive. Then, at points that are multiples of the degree of α, we can calculate the components of the syndrome $s(x)$ (2), which characterises (7). Having calculated the values of (2) for all degrees of the element α, included in (4), we obtain a system of $2t$ equations concerning ν of unknown locators and error values

$$s_i = \sum_{j=1}^{v} Y_j X_j^i, i = \overline{1,2t}\ , j = \overline{1,v} \quad (8)$$

where $X_l = \alpha^{i_l}$ – locator, $Y_l = e_{il}$ – is the value of the $l$-th error in the $i_l$ position of vector (1). In matrix form, system (8) can be written as

$$X_{j2t \times v}^{i} Y_{jv\times 1} = s_{i2t\times 1},\ \ i = \overline{1,2t}\ , j = \overline{1,v} \quad (9)$$

To solve the system of nonlinear equations (9), we use [1] a polynomial of error locators defined by the expression

$$\Lambda(x) = \prod_{i=1}^{v}(1 - xX_i) \quad (10)$$

The roots of the polynomial (10) are the inverse of the error locators $X_l^{-1}, l = \overline{1,\nu}$. By opening the brackets in (10), obtain

$$\Lambda(x) = \sum_{i=0}^{v} \lambda_i x^i \quad (11)$$

If it is possible to determine the coefficients $\lambda_i,\ i = \overline{1,\nu}$ of the polynomial (11), we need to find its roots for calculating error locators $X_l, l = \overline{1,\nu}$, multiplying both parts of equation (11) by $Y_l X_l^{j+\nu}$ and putting $x = X_l^{-1}$ obtain

$$Y_l X_l^{j+\nu}\left(\lambda_\nu X_l^{-\nu} + \lambda_{\nu-1} X_l^{-(\nu-1)} + \ldots + \lambda_1 X_l^{-1} + 1\right) = = Y_l\left(X_l^{j+\nu} + \lambda_1 X_l^{j+\nu-1} + \ldots + \lambda_{\nu-1} X_l^{j+1} + \lambda_\nu X_l^{j}\right) = 0 \quad (12)$$

Expression (12) is executed for each $l$ and for each $j$. Summing (12) over $l$ from 1 to $j$, obtain

$$\sum_{l=1}^{v} Y_l X_l^{j+v} + \lambda_1 \sum_{l=1}^{v} Y_l X_l^{j+v-1} + \dots + \lambda_\nu \sum_{l=1}^{v} Y_l X_l^{j} = 0 \quad (13)$$

The sums of (13) are components of the syndrome (8) so that the last equation reduces to

$$s_{j+\nu} + \lambda_1 s_{j+\nu-1} + \lambda_2 s_{j+\nu-2} + \ldots + \lambda_{\nu-1} s_{j+1} + \lambda_\nu s_j = 0 \quad (14)$$

Since $v \le t$ for $j$ in the interval $1 \le j \le v$ all indices set the known components of the syndrome (8), which allows to form a system of linear equations

$$\lambda_1 s_{j+\nu-1} + \lambda_2 s_{j+\nu-2} + \ldots + \lambda_\nu s_j = -s_{j+\nu},\ j = \overline{1,\nu} \quad (15)$$

which relates the known components of (8) to the unknown coefficients Λ(*x*) (11). In matrix form, the system is written as

$$s_{jv\times v} \lambda_{v+1-jv\times 1} = -s_{v+jv\times 1},\ \ j = \overline{1,v} \quad (16)$$

It was shown in [12] that the matrix of syndrome components is not degenerate, and the system (16) has a solution if its dimension is equal to $v$ – to the actual number of errors. Otherwise, the matrix is degenerate.

The algorithm for solving the key equation (10), called the "direct" PGC algorithm, consists of the following sequence of operations (Fig. 2). Correction of the accepted vector (1) begins with determining the weight of the error polynomial (7) and finding $v$. The evaluation criterion is the non-degeneracy of the matrix (16).

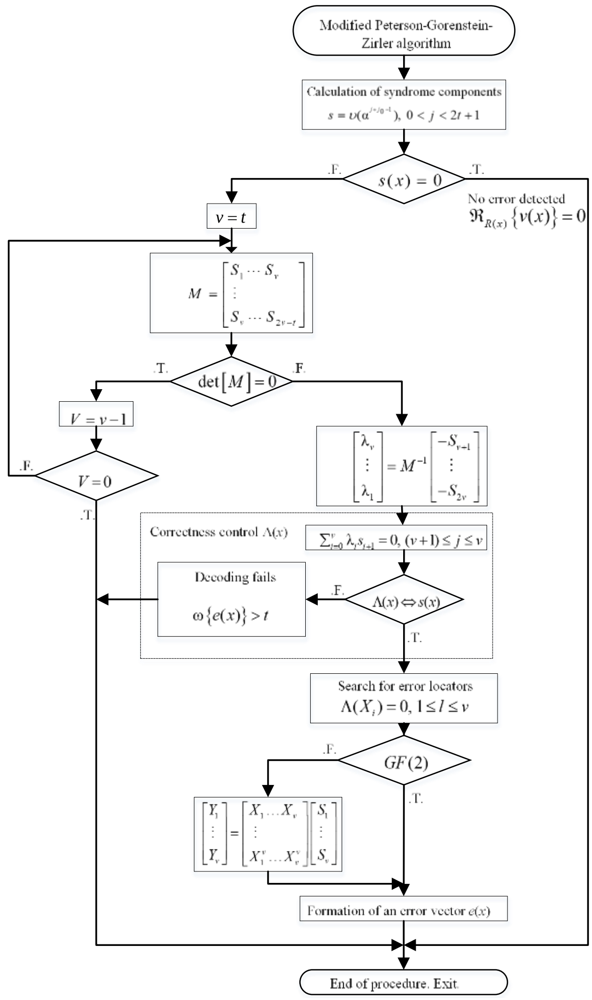



*Fig. 2. Modified Peterson algorithm*

Next, after converting the matrix of syndrome components, the values of the coefficients $\lambda_j,\ j = \overline{1,\nu}$ can be calculated. According to (10), the roots of $\Lambda(x)$ are the inverse of the error locators. Since the number of elements of the field $GF(q)$ is known, one way to determine the roots of (11) is the Chen procedure according to the Horner scheme [13].

$$\Lambda(\beta) = \left(\ldots\left(\left(\left(\lambda_\nu \cdot \beta + \lambda_{\nu-1}\right) \cdot \beta + \lambda_{\nu-2}\right) \cdot \beta + \lambda_{\nu-3}\right) \cdot \beta + \ldots + \lambda_0\right) \quad (17)$$

The roots of define the error locators. If the code is binary, the errors are obvious. For the $q$-th, return to equations (9), which define the syndrome's components. The first $\nu$ equations are solved concerning the error values $Y_1 = e_{il}$. The PGC algorithm does not fully implement the reliability indicators – the algorithm often "sabotages" the declaration of decoding failure. For example, for $n = 15$ with $d_{\min} = 7$ $\mathrm{GF}^{15}(2)$ has a polynomial of errors of a type.

$$e(x) = x^{14} + x^{13} + x^{12} + x^{10}, \quad \omega\{e(x)\} = 4 \tag{18}$$

leads to a sequence of syndrome components

$$s = \left\{\alpha^6, \alpha^{12}, \alpha^3, \alpha^9, \alpha^5, \alpha^6\right\} \tag{19}$$

obtained over $\mathrm{GF}\left(2^4\right)$, in the ring $\mathrm{GF}(2)[x] / \left(x^4 + x + 1\right)$.

Having constructed the matrix of syndrome components according to the PGC algorithm, the following numerical values of the matrix determinants for different values $v = \{1,2,3\} \Rightarrow \Delta_3 = \alpha^{-\infty},\ \Delta_2 = \alpha^{-\infty},\ \Delta_1 = \alpha^6$. can be obtained. Then, the error locator polynomial is defined by the expression

$$\Lambda(x) = \alpha^6 x + 1 \tag{20}$$

and the PGC algorithm "diverts" to the correction of a single error determined by the single root of the polynomial (20) – $\alpha^9$.

At first glance, there are no contradictions either from the algorithmic or analytical point of view: a nondegenerate matrix is defined, there is a polynomial of error locators $\Lambda(x)$, root $\alpha^9$ and the location of the error. That is, all the reasons to correct the vector $\upsilon(x)$. However, the situation is more complex than it initially appears. First, there is only one locator, and there are no real errors $\omega\{e(x)\} = 4$, and the locator itself shows the wrong location of the error, ultimately leading to error propagation. Secondly, the decoder does not try to indicate the failure of decoding and the impossibility of correct correction, knowing that $d_{\min} = 7$.

Opponents may argue: "If it says that $d_{\min} = 7$, and it needs to be fixed $v = 4$. It is known [4, 11, 14] that the correct decoding of a "hard" linear block code decoder is impossible in this case, and the actions of the decoder are uncertain. So, the question is resolved". Indeed, to correct multiplicity errors in a "hard" decoder $v > t$ (higher than structurally permissible) without additional soft information is impossible. But is it possible to detect the decoding failure and use feedback?

This question can be answered positively in some cases since the decoder cannot identify all situations similar to (20).

If return to (15) and check the ability of the polynomial of error locators (20) to generate a sequence of components of the syndrome (19) according to (1), the polynomial (20) generates a sequence of syndrome components of the form

$$\tilde{s} = \left\{\alpha^6, \alpha^{12}, \alpha^3, \alpha^9, \alpha^0, \alpha^6\right\} \tag{21}$$

differs from (19), an identifier of decoding failure and even a source of feedback "requests".

Thus, Peterson's algorithm (see Fig. 2) should be supplemented with a correctness checking block $\Lambda(x)$ by calculating the recurrence ratio [10]

$$\sum_{i=0}^{\nu} \lambda_i \cdot s_{j-i} \equiv 0,\ j = \overline{(\nu+1), 2t} \tag{22}$$

## 3. Modified Peterson-Gorenstein-Zirler algorithm

Figure 2 shows the "direct" modified Peterson-Gorenstein-Zirler algorithm. A dotted line bounds the modified area.

The upper bound of the gain can be estimated as follows. The implementation of algebraic decoding algorithms is based on a finite power field $q = n + 1$, where $n$ – is the length of the plain (not shortened) code. In this case, the procedure generates *2t* is the component of the syndrome (8), and *t* is determined by the minimum constructive hashing distance $t = (d-1)/2$ [1].

Each component of the syndrome is an element of the finite field $GF(q)$. Number of syndrome components in the matrix (9) of dimension $[t \times t] = t^2$ the number of their varieties $2t$. With all the power of the elements $q$ they can be selected in $(n+1)^{2t}$ ways. Thus, it is possible to form the same number of matrices of the syndrome component, some of which will be degenerate.

The nondegeneracy of a matrix is determined by a determinant other than zero. By definition, the determinants $D = \det[a_{ik}]$ square matrix $[t \times t]$ with $t^2$ elements $a_{ik} - sum\, t!$ elements $(-1)^r a_{1k1} a_{2k2\ldots} a_{tkt}$, each of which corresponds to one of the $t!$ of different ordered sets of the obtained $r$ pairwise permutations of elements from the set $|GF(q)| = \{1, 2, \ldots, t\}$ [9]. Based on the structure of the field $GF(q)$, an extension of $GF\left(2^m\right)$, the result $(-1)^r a_{1k1} a_{2k2\ldots} a_{tkt} = \alpha^{-\infty}$ will occur with a probability $p = q^{-1}$ under the assumption of equal probability of the components (8). Then, the number of degenerate matrices (9) in the Peterson algorithm can be estimated by

$$N_{vir.} = (n+1)^{-(2t+1)} \sum t! \tag{23}$$

A comparison of transmission systems is carried out at the coordinates of potential noise immunity characteristics $p_0 = f\left(h^2\right)$. The conclusion regarding the feasibility of using interference-resistant coding can be drawn by analysing the energy gain from coding (EGC). Suppose the energy gain from coding is positive. In that case, using a corrective code allows, despite reducing the signal power of a single element $(R_k < 1)$, to improve the system's reliability (otherwise, using the code is inappropriate).

Next, the reliability indicators are examined – the probability of false decoding of the code combination $P_{er.cc}$ and the equivalent error probability of a single element $p_{equ.}$, as an assessment of the "failed decoding" event over the entire range of error multiplicity values $\nu$ in

$$P(\nu, n) = B\{f(\nu; n, t)\} \cdot P\{f(p_0; \nu, n)\} \tag{24}$$

where $B\{\cdot\}$ – functionality of the total number of false decoding events; $P\{\cdot\}$ – event probability $B\{\cdot\}$.

For a communication channel with independent errors, the distribution (24) is determined by the well-known expression

$$P(\nu, n) = C_n^{\nu} p_0^{\nu} (1 - p_0)^{n-\nu} \tag{25}$$

For calculation $p_{equ.}$, information on the transformation of code vectors into the adjacent areas of standard arrangement decoding is required $c(x)$, which was the subject of the research. Specialised software was developed to address this issue.

## 4. Simulation model

The software package allows the numerical estimation of the probabilities of $P_{er.}\{f(\nu;n,t)\}$ and $p_{equ.}\{f(\nu;n,t)\}$ using codec modelling and statistical data processing. The model's core consists of the hard-decision algebraic decoding algorithms discussed above, which implement the maximum likelihood procedure with error correction in linear block codes.

Figure 3 shows the general algorithm of the simulation model. The package includes programs for generating an arbitrary finite field $GF(2^m)$, emulating field operations, calculating syndrome components $s(x)$, polynomial error locators $L(x)$, matrix conversion by the modified Jordan-Gauss method, searching for roots of polynomials, error generator $e(x)$, etc.

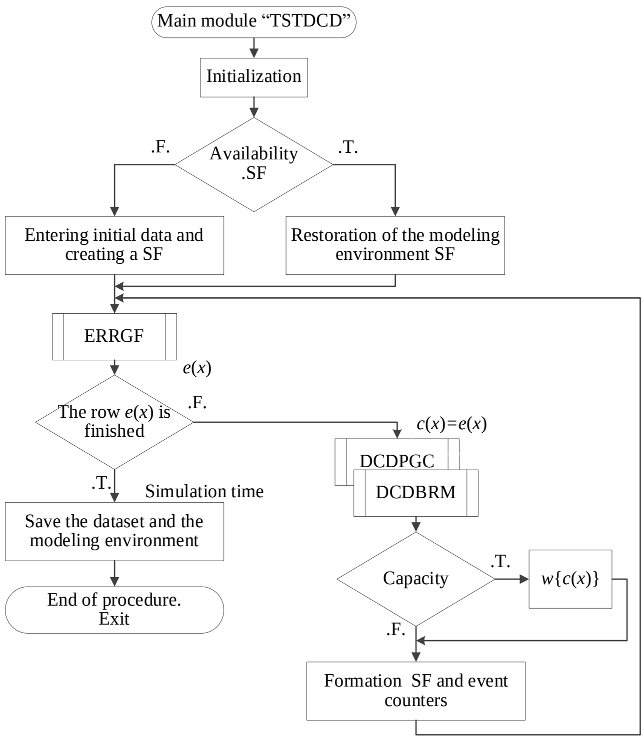



*Fig. 3. A generalised algorithm of the simulation model for studying algebraic decoders*

All modifications to the simulation model's state are systematically recorded in the state file and event counters.

The state file is a matrix of dimension $[n \times n]$ number of false decodings $N$, where the column number is identified with the weight of the error vector $n = \omega\{e(x)\}$, and the line number with the weight of the transformed codeword $m = \omega\{\bar{c}(x)\}$. Event counters count the number of erasures $N_{eras.}$, false decoding $N_{\text{er.}}$ and applications $N$ to the decoder and error generator subroutines. The state file displays the behaviour of the decoder with the specified correction properties $d_{\min}$ in the vector space $GF^n(q)$ and is a source of estimation of probability parameters.

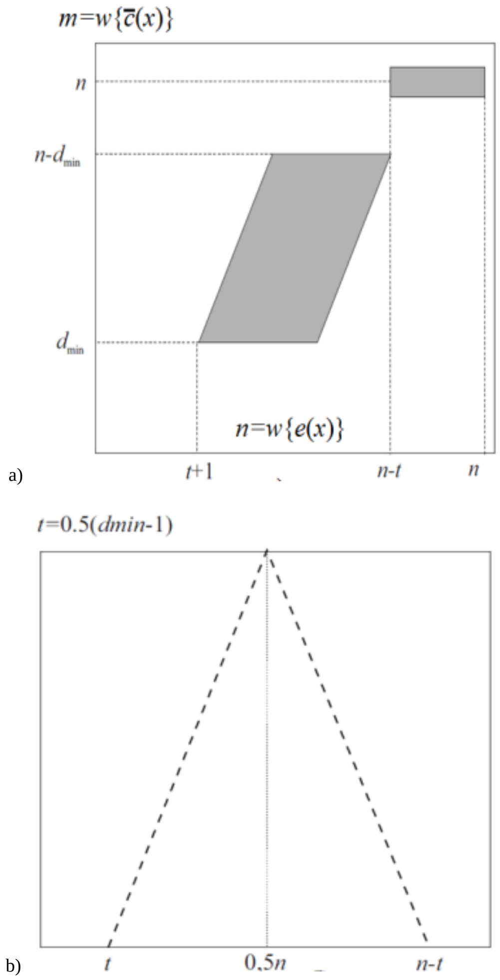



*Fig. 4. State file: a) geometric interpretation; b) grouping of failed decoding data zones*

## 5. Results

Fig. 5 shows an example of a real file map status (the inverse diagonal of the matrix is shown, taking into account "erasures"). Table 1 shows the number of false decodings and "erasures" (detected failed decodings), depending on the weight of the error vector $\omega\{e(x)\}$ and correction properties of the decoder *t*. Numerical values obtained for the lexicographic model $e(x)$.

The analysis of Table 2 allows us to distinguish three groups of data, and Fig. 4 shows their geometric interpretation:

a) zone 1: guaranteed correction $v < t$ – multiple errors (numerical data values equal to 0);
b) zone 2: symmetrically about the abscissa $0.5n$, values of the detected decoder errors are located;
c) zone 3: undetected decoder errors (probability of false decoding) $P_{er.\text{cc}} = 1$, the number of events is determined by a binomial coefficient $C_n^v$.

The meanings of the Zone 1 data are obvious. The physical meaning of Zone 3 data can be commented on with the following: if the corrective properties $(n,k)$ – codes allow guaranteed correction of multiplicity errors in a certain number of code combinations $1 \le v \le t$, then for the same number of code combinations of this code with probability $P = 1$).

*Table 1. The state of the hard decoder*

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **15** | | | | | | | | | | | | | | 15 | 1 |
| **14** | | | | | | | | | | | | | | | |
| **13** | | | | | | | | | | | | | | | |
| **12** | | | | | | | | | | | 420 | 35 | 105 | | |
| **11** | | | | | | | | | | 1155 | 105 | 420 | | | |
| **10** | | | | | | | | | 1680 | 168 | 840 | | | | |
| **9** | | | | | | | | 2520 | 280 | 1680 | | | | | |
| **8** | | | | | | | 3480 | 435 | 3045 | | | | | | |
| **7** | | | | | | 3045 | 435 | 3480 | | | | | | | |
| **6** | | | | | 1680 | 280 | 2520 | | | | | | | | |
| **5** | | | | 840 | 168 | 1680 | | | | | | | | | |
| **4** | | | 420 | 105 | 1155 | | | | | | | | | | |
| **3** | | 105 | 35 | 420 | | | | | | | | | | | |
| **2** | | | | | | | | | | | | | | | |
| **1** | | | | | | | | | | | | | | | |

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **15** | | | | | | | | | | | | | 105 | 15 | 1 |
| **14** | | | | | | | | | | | | | | | |
| **13** | | | | | | | | | | | | | | | |
| **12** | | | | | | | | | | | | 275 | | | |
| **11** | | | | | | | | | | | 825 | | | | |
| **10** | | | | | | | | 810 | 180 | 2508 | 90 | 180 | | | |
| **9** | | | | | | | 1080 | 270 | 4300 | 180 | 450 | | | | |
| **8** | | | | | | 420 | 120 | 4155 | 105 | 315 | | | | | |
| **7** | | | | | 315 | 105 | 4155 | 120 | 420 | | | | | | |
| **6** | | | | 450 | 180 | 4300 | 270 | 1080 | | | | | | | |
| **5** | | | 180 | 90 | 2508 | 180 | 810 | | | | | | | | |
| **4** | | | | 825 | | | | | | | | | | | |
| **3** | | | 275 | | | | | | | | | | | | |
| **2** | | | | | | | | | | | | | | | |
| **1** | | | | | | | | | | | | | | | |

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **15** | | | | | | | | | | | | 455 | 105 | 15 | 1 |
| **14** | | | | | | | | | | | | | | | |
| **13** | | | | | | | | | | | | | | | |
| **12** | | | | | | | | | | | | | | | |
| **11** | | | | | | | | | | | 840 | | | | |
| **10** | | | | | | | | | | 1848 | | | | | |
| **9** | | | | | | | | | 1960 | | | | | | |
| **8** | | | | | 840 | 420 | 3060 | 3375 | 2625 | 315 | 525 | | | | |
| **7** | | | | 525 | 315 | 2625 | 3375 | 3060 | 420 | 840 | | | | | |
| **6** | | | | | | 1960 | | | | | | | | | |
| **5** | | | | | 1848 | | | | | | | | | | |
| **4** | | | | 840 | | | | | | | | | | | |
| **3** | | | | | | | | | | | | | | | |
| **2** | | | | | | | | | | | | | | | |
| **1** | | | | | | | | | | | | | | | |

| **15** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **14** | | | | | | | | | | | 1365 | 455 | 105 | 15 | 1 |
| **13** | | | | | | | | | | | | | | | |
| **12** | | | | | | | | | | | | | | | |
| **11** | | | | | | | | | | | | | | | |
| **10** | | | | | | | | | | | | | | | |
| **9** | | | | | | | | | | 3003 | | | | | |
| **8** | | | | | | | | | 5005 | | | | | | |
| **7** | | | | | | | | 6435 | | | | | | | |
| **6** | | | | | | | 6435 | | | | | | | | |
| **5** | | | | | | 5005 | | | | | | | | | |
| **4** | | | | | 3003 | | | | | | | | | | |
| **3** | | | | | | | | | | | | | | | |
| **2** | | | | | | | | | | | | | | | |
| **1** | | | | | | | | | | | | | | | |
| **15** | | | | | | | | | | | | | | | |
| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |

*Table 2. Number of false decodes $N_{er}$*

| The number of requests | | Number of false decodes $N_{er}$ (erasures $N_{er\ as} = C_n^{\nu} - N_{er}$ )at a given $t$ | | | | | | |
|---|---|---|---|---|---|---|---|---|
| { | $C_n^{\nu}$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | **15** | | | | | | | |
| 2 | **105** | 105/0 | | | | | | |
| 3 | **455** | 455/0 | 180/275 | | | | | |
| 4 | **1365** | 1365/0 | 540/825 | 525/840 | | | | |
| 5 | **3003** | 3003/0 | 1413/1590 | 1155/1848 | 0/3003 | | | |
| 6 | **5005** | 5005/0 | 2355/2650 | 3045/1960 | 0/5005 | 0/5005 | | |
| 7 | **6435** | 6435/0 | 3135/3300 | 3915/2520 | 0/6435 | 0/6435 | 0/6435 | |
| 8 | **6435** | 6435/0 | 3135/3300 | 3915/2520 | 0/6435 | 0/6435 | 0/6435 | **6435**/0 |
| 9 | **5005** | 5005/0 | 2355/2650 | 3045/1960 | 0/5005 | 0/5005 | **5005**/0 | **5005**/0 |
| 10 | **3003** | 3003/0 | 1413/1590 | 1155/1848 | 0/3003 | **3003**/0 | **3003**/0 | **3003**/0 |
| 11 | **1365** | 1365/0 | 540/825 | 525/840 | **1365**/0 | **1365**/0 | **1365**/0 | **1365**/0 |
| 12 | **455** | 455/0 | 180/275 | **455**/0 | **455**/0 | **455**/0 | **455**/0 | **455**/0 |
| 13 | **105** | 105/0 | **105/0** | **105**/0 | **105**/0 | **105**/0 | **105**/0 | **105**/0 |
| 14 | **15** | **15**/0 | **15/0** | **15**/0 | **15**/0 | **15**/0 | **15**/0 | **15**/0 |
| 15 | **1** | **1**/0 | **1/0** | **1**/0 | **1**/0 | **1**/0 | **1**/0 | **1**/0 |

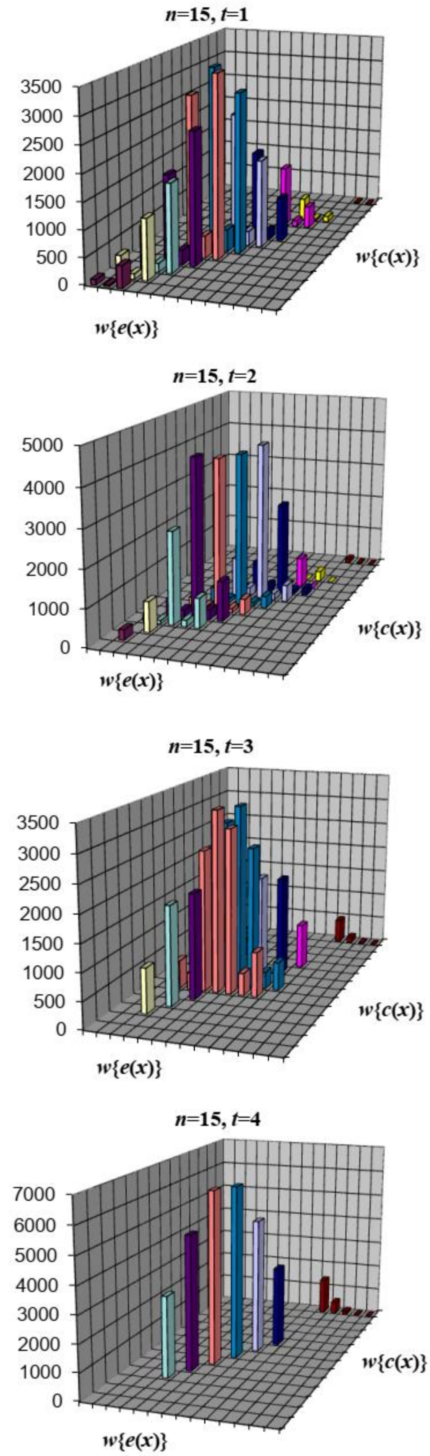



*Fig. 5. Distribution of the hard decoder state in the file map for different correction properties t over GF(16)*

## 6. Conclusions

To sum up, we can say:

1. The decoding of BCH and RS codes that correct *t*-fold errors and erasure is carried out by algebraic methods based on solving equations for locators $\Lambda(x)$ and values $\Omega(x)$ errors in the end fields $GF(q)$.
2. In algebraic decoders, an attempt to correct errors outside the constructive $d_{\min}$ boundary leads to an erroneous result, although the fact of the event $t < v \le (n-t)$ can be registered with some probability.

3. Thus, modifying the Peterson algebraic decoding algorithm based on the control of the correctness of the error locator polynomial allows a reduction of the probability of false decoding beyond the threshold of the constructive code distance. Studies have shown that the introduction of correctness control $\Lambda(x)$ reduces the probability of false decoding by an order of magnitude and, in some cases, by two or more.
4. The software for studying the transformation of code vectors of an arbitrary linear block code is developed. The software allows the estimation of the following parameters based on the modelling of "encoder-decoder-error generator" $P_{ош.кк}$ and $p_{екв.}$ The model's core consists of hard decision decoding algorithms: Burlecamp-Massie and modified Peterson-Gorenstein-Zirler, which implement an LDC decoder with error correction in the LBC. The package includes programs for generating the final field $GF\left(2^m\right)$, emulating operations on field elements, calculating syndrome components $s(x)$, polynomial error locators $\Lambda(x)$, matrix conversion by the modified Jordan-Gauss method, searching for roots of polynomials, error generator $e(x)$, etc.
5. In the experiments, the symmetry of the simulation results concerning the abscissa is observed $v = 0.5n$ .
6. The approximation of the simulation data allows to obtain numerical values of the probability of false decoding of algebraic decoders in engineering practice.
7. One of the promising areas of further research is to assess the possibility of using neural networks to improve decoding efficiency based on preliminary error analysis.

## References


[1] Ball S. A Course in Algebraic Error-Correcting Codes. Springer Nature, Switzerland AG, 2020, 177, [https://doi.org/10.1007/978-3-030-41153-4].

[2] Chen Y. Parhi K.: Overlapped Message Passing for Quasi-Cyclic Low-Density Parity Check Codes. IEEE Transactions on Circuits and Systems – IEEE Xplore 51(6), 2004, 1106–113, [https://doi.org/10.1109/TCSI.2004.826194].

[3] Farre R., Sayols N., Xambo-Descamps S.: On PGZ decoding of alternant codes. Computational and Applied Mathematics 38(17), 2019, [https://doi.org/10.1007/s40314-019-0795-7].

[4] Garlapati P., Yamuna B., Balasubramanian K.: A Low Power Hard Decision Decoder for BCH Codes. International Conference on Advances in Computing and Communications, Kochi, Kakkanad, India 2021, 1–6, [https://doi.org/10.1109/ICACC-202152719.2021.9708303].

[5] Gautam A., Thakur P., Singh G. Advanced Channel Coding Schemes for B5G/6G Networks: State-of-the-Art, Challenges, and Future Research Directions. International Journal of Communication Systems 13, 2024, 1–30, [https://doi.org/10.1002/dac.5855].

[6] Moon T. Error Correction Coding: Mathematical Methods and Algorithms. John Wiley & Sons, Inc., 2005, 576, [https://doi.org/10.1002/0471739219].

[7] Peterson W.W., Weldon E. J.: Error-correcting Codes. MIT Press, 1972, 560.

[8] Richardson T., Urbanke R.: Modern Coding Theory. Cambridge University Press, 2008, 576, [https://doi.org/10.1017/CBO9780511791338].

[9] Slinko A.: Algebra for Applications: Cryptography, Secret Sharing, Error-Correcting, Fingerprinting, Compression. Springer International Publishing, Switzerland 2015, 2020, 328, [https://doi.org/10.1007/978-3-319-21951-6].

[10] Spezia S.: Mathematical Theory and Applications of Error Correcting Codes. Arcler Press 2020, 527.

[11] Stark W.: Introduction to Digital Communications. Cambridge University Press, Cambridge 2023, 600, [https://doi.org/10.1017/9781009220859].

[12] Sudha K., Gahalod L., Changlani S.: Study of different Type of Error Detection and Correction in Wireless Communication. International Journal of Scientific Research in Science, Engineering and Technology 9(3), 2022, 448–455 [https://doi.org/10.32628/IJSRSET2293138].

[13] Tomlinson M. at al.: Error-Correction Coding and Decoding: Bounds, Codes, Decoders, Analysis and Applications. Springer Cham 2020, 522, [https://doi.org/10.1007/978-3-319-51103-0].

[14] Velayudham S. at al.: Power efficient error correction coding for on-chip interconnection links. IET Computers & Digital Techniques 14(6), 2020, 299–312, [https://doi.org/10.1049/iet-cdt.2019.0082].



**Prof. Dmytro Mogylevych**
e-mail: mogilev11@ukr.net

D.Sc., prof., Head of the Department of Special Electronic Communications Systems of the Institute of Special Communication and Information Protection of the National Technical University of Ukraine "Ihor Sikorskyi Kyiv Polytechnic Institute", Kyiv, Ukraine.
For 30 years of scientific and pedagogical activity, he is the author of more than 110 scientific, educational and methodological works in the field of digital signal processing theory.

https://orcid.org/0000-0002-4323-0709



**Ph.D. Iryna Kononova**
e-mail: viti21@ukr.net

Head of the Department of Theoretical foundations of operation of special telecommunication systems of the Institute of Special Communication and Information Protection of the National Technical University of Ukraine "Ihor Sikorskyi Kyiv Polytechnic Institute", Kyiv, Ukraine. For 15 years of scientific and pedagogical activity, she is the author of more than 60 scientific, educational and methodological works in the field of speech processing and recognition.

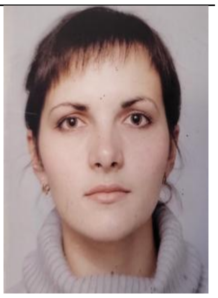
https://orcid.org/0000-0001-6945-0323



**Ph.D. Liudmyla Pogrebniak**
e-mail: pogrebniaklm@gmail.com

Associate professor of the Department of Special Electronic Communications Systems of the Institute of Special Communication and Information Protection of the National Technical University of Ukraine "Ihor Sikorskyi Kyiv Polytechnic Institute", Kyiv, Ukraine.
For 5 years of scientific and pedagogical activity, she is the author of more than 40 scientific, educational and methodological works in the field of communication systems.

https://orcid.org/0000-0002-9104-7781


**M.Sc. Kostiantyn Lytvyn**
e-mail: klitvin@gmail.com

Lecturer of the Department of Special Electronic Communications Systems of the Institute of Special Communication and Information Protection of the National Technical University of Ukraine "Ihor Sikorskyi Kyiv Polytechnic Institute", Kyiv, Ukraine.
For 25 years of scientific and pedagogical activity, he is the author of more than 40 scientific, educational and methodological works in the field of signal processing theory.

https://orcid.org/0000-0003-3901-6766



**Ph.D. Igor Gyrenko**
e-mail: igor_girenko@ukr.net

Deputy Head of the Institute of the Institute of Special Communications and Information Protection of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.
For 6 years of scientific and pedagogical activity, he is the author of more than 15 scientific, educational and methodological works in the field of digital signal processing.

https://orcid.org/0000-0002-7688-7926