computing@computingonline.net
www.computingonline.net

Print ISSN 1727-6209
On-line ISSN 2312-5381
International Journal of Computing

# NOISE IMMUNITY OF THE ALGEBRAIC GEOMETRIC CODES

**Alexandr Kuznetsov [1, 2], Ievgeniia Kolovanova [1], Oleksii Smirnov [3], Tetiana Kuznetsova [1]**

[1] V. N. Karazin Kharkiv National University, Svobody sq., 6, Kharkiv, 61022, Ukraine, kuznetsov@karazin.ua, e.kolovanova@gmail.com, kuznetsova.tatiana17@gmail.com
[2] JSC "Institute of Information Technologies", Bakulin St., 12, Kharkiv, 61166, Ukraine, kuznetsov@karazin.ua
[3] Central Ukrainian National Technical University, University Avenue 8, Kropyvnytskyi, 25006, Ukraine, dr.SmirnovOA@gmail.com

**Paper history:**
Received 20 November 2018
Received in revised form 15 September 2019
Accepted 20 December 2019
Available online 31 December 2019

**Keywords:**
algebraic geometric code;
energy gain;
orthogonal signal;
noise-immune coding.

**Abstract:** Linear block noise-immune codes constructed according to algebraic curves (algebraic geometric codes) are considered, their design properties are evaluated, algorithms of construction and decoding are studied. The energy efficiency of the transmission of discrete messages by *M*-ary orthogonal signals in the application of algebraic geometric codes is studied; the achievable energy gain from the use of noise-immune coding is estimated. The article shows that in discrete channels without memory it is possible to obtain a significant energy gain, which increases with the transition to long algebraic geometric codes constructed from curves with a large number of points relative to the genus of the curve. It is found that the computational complexity of implementing algebraic geometric codes is comparable to other known noise-immune codes, for example, Reed-Solomon codes and others. Thus, high energy efficiency in combination with the acceptable computational complexity of implementation confirms the prospects of algebraic geometric codes use in modern telecommunication systems and networks to improve the noise immunity of data transmission channels.

*Copyright © Research Institute for Intelligent Computer Systems, 2019. All rights reserved.*

## 1. INTRODUCTION

Algebraic geometric codes as linear systems on algebraic curves were first proposed by V.D. Goppa [1, 2]. The asymptotic properties of such codes were investigated in [3]. Codes constructed from curves with a large number of points in comparison with the genus lie above the Varshamov-Gilbert boundary [4-12]. Schemes of the practical application of these codes for noise-immune transmission of discrete messages [10-12], algorithms for their construction and decoding [7-9], the resulting energy gain from coding [13-15] are in the sphere of interest.

The aim of this paper is to study some algorithms for constructing and decoding algebraic geometric codes and to estimate the energy efficiency achieved. In addition, the paper presents the results of comparative studies of the complexity of the practical implementation of noise-immune coding and decoding using algebraic geometric codes and other (the most well-known and common) codes. The results of this research can be used to improve various code-based methods of information security [16-26].

The paper is structured as follows. In Section 2, the basic concepts and definitions of algebraic geometric codes are given, the constructive characteristics of the codes are evaluated, and their asymptotic properties are studied. Section 3 is devoted to the development and study of computationally efficient procedures for encoding and decoding of algebraic geometric codes. In particular, we have presented several options for constructing codes (in a systematic and non-systematic form) and a simple decoding algorithm. Section 4 examines the energy efficiency of algebraic geometric coding in the transmission of discrete messages by *M*-orthogonal signals. In Section 5, we conduct a comparative analysis of the complexity of the implementation of the encoding

and decoding algorithms. The conclusions of the work summarize the obtained results and show the promising areas for further research.

## 2. DEFINITION AND CONSTRUCTIVE PROPERTIES OF ALGEBRAIC GEOMETRIC CODES

Fix a finite field $GF(q)$ and denote by $X$ a smooth projective algebraic curve in projective space $P^n$. Consider the set of solutions $p_1(x_0, x_1, ..., x_n)$, $p_2(x_0, x_1, ..., x_n)$, ..., $p_N(x_0, x_1, ..., x_n)$ of a system of homogeneous irreducible algebraic equations of degree $d$ with coefficients from $GF(q)$.

Let $g = g(X)$ be the curve genus, and, according to [1-3]:

– if $d < n$, then $X$ is a degenerate curve;

– if $d = n$, then $X$ is a rational normal curve of genus 0;

– if $n < d < 2n$, then $g \le d - n$;

– if $d = 2n$, then $g \le n + 1$;

– if $d \ge 2n$, then $g \le \frac{m(m-1)}{2}(n-1) + m\varepsilon$,

where $m = \left[\frac{d-1}{n-1}\right]$, $\varepsilon = d - 1 - m(n-1)$.

Table 1 gives the upper bound for the genus of the curve $X$.

**Table 1. Upper bound for the genus $g$ of the curve $X$ in $P^n$**

| $d$ | $g(P^2)$ | $g(P^3)$ | $g(P^4)$ | $g(P^5)$ | $g(P^6)$ |
|---|---|---|---|---|---|
| 2 | 0 | - | - | - | - |
| 3 | 1 | 0 | - | - | - |
| 4 | 3 | 1 | 0 | - | - |
| 5 | 6 | 2 | 1 | 0 | - |
| 6 | 10 | 4 | 2 | 1 | 0 |
| 7 | 15 | 6 | 3 | 2 | 1 |
| 8 | 21 | 9 | 5 | 3 | 2 |
| 9 | 28 | 12 | 7 | 4 | 3 |
| 10 | 36 | 16 | 9 | 6 | 4 |

Let $X(GF(q))$ be the set of points of a curve $X$ over a finite field $GF(q)$, and $N = |X(GF(q))|$ be the number of these points. The number $N$ of the points of the curve $X$ over $GF(q)$ is bounded above by the Hasse-Weil expression [1-3]: $N \le 2\sqrt{q} \cdot g + q + 1$.

Table 2 gives the upper bound for the number of points of the curve over a finite field. The limit values of the number of points of smooth curves are summarized in Table 3.

Let $C$ be the divisor class on $X$ of power $\alpha$. Then $C$ defines a mapping $\phi: X \to P^m$, and a set of generator functions $y_i = \phi(x_i)$ specifies an algebraic geometric code of length $n \le N$.

**Table 2. Estimation of the upper boundary of the number of points of a smooth projective curve**

| $g$ | $d$ | $N = \|X(GF(q))\|$ | | | | |
|---|---|---|---|---|---|---|
| | | $GF(4)$ | $GF(8)$ | $GF(16)$ | $GF(32)$ | $GF(64)$ |
| 0 | 2 | 5 | 9 | 17 | 33 | 65 |
| 1 | 3 | 9 | 14 | 25 | 44 | 81 |
| 2 | 4 | 10 | 18 | 33 | 53 | 97 |
| 3 | 4 | 17 | 24 | 41 | 66 | 113 |
| 4 | 5 | 21 | 29 | 49 | 77 | 129 |
| 5 | 5 | | 34 | 57 | 88 | 145 |
| 6 | 5 | | 39 | 65 | 99 | 164 |
| 7 | 6 | | 44 | 73 | 110 | 180 |
| 8 | 6 | | 49 | 81 | 121 | 196 |
| 9 | 6 | | 54 | 89 | 132 | 212 |
| 10 | 6 | | 59 | 97 | 143 | 228 |
| 11 | 7 | | 64 | 105 | 154 | 244 |
| 12 | 7 | | 69 | 113 | 165 | 260 |
| 13 | 7 | | | 121 | 176 | 276 |
| 14 | 7 | | | 129 | 187 | 292 |
| 15 | 7 | | | 137 | 198 | 308 |

**Table 3. The maximum values of the points of the curve $X$ in $P^2$ over $GF(q)$**

| $d$ | $N = \|X(GF(q))\|$ | | | | |
|---|---|---|---|---|---|
| | $GF(4)$ | $GF(8)$ | $GF(16)$ | $GF(32)$ | $GF(64)$ |
| 3 | 9 | 14 | 25 | 44 | 81 |
| 4 | 14 | 24 | 34 | 63 | 113 |
| 5 | 17 | 28 | 65 | 99 | 164 |

Let $C$ be the divisor class on $X$ of power $\alpha$. Then $C$ defines a mapping $\phi: X \to P^m$, a set of generator functions $y_i = \phi(x_i)$ specifies an algebraic geometric code of length $n \le N$. The code characteristics $(n, k, d)$ are related by the relation $k + d \ge n - g + 1$ [1-3]. If $2g - 2 < \alpha \le n$, the code is related by characteristics $(n, \alpha - g + 1, d), d \ge n - \alpha$. A dual code to it is also

algebraic geometric with characteristics $(n, n-\alpha+g-1, d_\perp), d_\perp \geq \alpha - 2g + 2$.

As an evaluation of the potential of block codes, they are compared with the code boundaries. The code boundaries indicate the best theoretically possible linear block codes and are described in detail in [4-6].

The Singleton boundary indicates the maximum achievable code distance for the given code parameters $(n, k, d)$ and is written in the form

$$d \leq n - k + 1.$$

The codes lying on the Singleton boundary are called Maximum Distance Separable Codes (MDS codes).

The Varshamov-Gilbert boundary is the lower code boundary, i.e., it guarantees the existence of codes with parameters $(n, k, d)$ lying on this boundary. The generalization of the Varshamov-Gilbert boundary to non-binary codes has the form

$$q^{n-k} \geq \sum_{i=0}^{d-2} C_{n-1}^{i} (q-1)^{i},$$

or

$$n - k \geq \log_q \left( \sum_{i=0}^{d-2} C_{n-1}^{i} (q-1)^{i} \right).$$

For the code $(n, k, d)$, consider the following parameters: $R = k/n$ is the relative speed of the code, as the fraction of information symbols in the transmitted data; $\delta = d/n$ is the relative minimum distance of the code, as a fraction of errors in the received word that the code can commit. Tend $n \to \infty$. The asymptotic form of the Singleton boundary takes the form $R \leq 1 - \delta$. The asymptotic Varshamov-Gilbert boundary takes the form $R \leq 1 - H_q(\delta)$. In [3], the asymptotic boundary of algebraic geometric codes is given by $R \leq 1 - \delta - \left(\sqrt{q} - 1\right)^{-1}$. Fig. 1 shows the asymptotic boundaries: 1 is the Singleton boundary; 2 is the Varshamov-Gilbert boundary; 3 is the boundary of the algebraic geometric codes.

The above dependences show that as the power $q$ of the alphabet of code symbols increases, the asymptotic properties of algebraic geometric codes improve. Obviously, for large $q$, these codes lie above the Varshamov-Gilbert boundary, which indicates high potential characteristics.

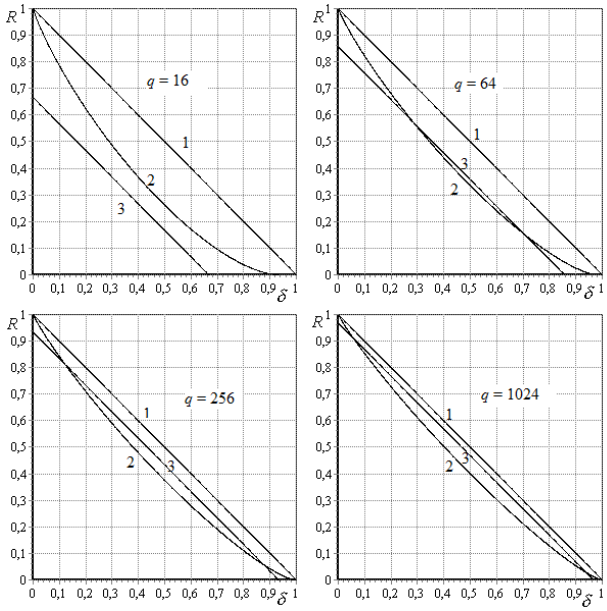


**Figure 1 - Asymptotic properties of algebraic geometric codes**

The constructive code characteristics of algebraic geometric codes over curves of genus $g = 0$, $g = 1$, $g = 3$, $g = 6$, over $GF(4)$ are summarized in Table 4. The corresponding constructive estimates of the code parameters for curves of the various genus values $g = 0$, $g = 1$, $g = 3$, $g = 6$, over $GF(8)$, $GF(16)$, $GF(32)$, $GF(64)$ are summarized in Tables 5-8.

## 3. CODING AND DECODING BY ALGEBRAIC GEOMETRIC CODES

We consider the coding operations by algebraic geometric codes for the general case. In other words, for curves defined in the projective space $P^u$ by the set of solutions $u-1$ of homogeneous irreducible algebraic equations in $n$ unknowns, we investigate algorithms for the formation of code words in a systematic and unsystematic manner.

**Table 4. Constructive code characteristics of algebraic geometric codes over $GF(4)$**

| deg f | $\deg X = 2$, $g = 0$ | | | $\deg X = 3$, $g = 1$ | | | $\deg X = 4$, $g = 3$ | | | $\deg X = 5$, $g = 6$ | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $a$ | $n,k,d$ | $n,k,d$ | $a$ | $n,k,d$ | $n,k,d$ | $a$ | $n,k,d$ | $n,k,d$ | $a$ | $n,k,d$ | $n,k,d$ |
| 1 | 2 | **5, 3, 3** | 5, 2, 4 | 3 | 9, 3, 6 | 9, 6, 3 | 4 | 14, 2, 10 | – | 5 | – | – |
| 2 | 4 | | | 6 | **9, 6, 3** | 9, 3, 6 | 8 | 14, 6, 6 | 14, 8, 4 | 10 | 17, 5, 7 | – |
| 3 | 6 | | | 9 | | | 12 | 14, 10, 2 | 14, 4, 8 | 15 | 17, 10, 2 | 17, 7, 5 |
| 4 | 8 | | | 12 | | | 16 | | | 20 | | 17, 2, 10 |

**Table 5. Constructive code characteristics of algebraic geometric codes over $GF(8)$**

| $\deg f$ | $\deg X=2,\ g=0$ | | | $\deg X=3,\ g=1$ | | | $\deg X=4,\ g=3$ | | | $\deg X=5,\ g=6$ | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $a$ | $n,k,d$ | $n,k,d$ | $a$ | $n,k,d$ | $n,k,d$ | $a$ | $n,k,d$ | $n,k,d$ | $a$ | $n,k,d$ | $n,k,d$ |
| 1 | 2 | 9, 3, 7 | 9, 6, 4 | 3 | 14, 3, 11 | 14, 11, 3 | 4 | 24, 2, 20 | – | 5 | – | – |
| 2 | 4 | 9, 5, 5 | 9, 4, 6 | 6 | 14, 6, 8 | 14, 8, 6 | 8 | 24, 6, 16 | 24, 18, 4 | 10 | 28, 5, 18 | – |
| 3 | 6 | **9, 7, 3** | 9, 2, 8 | 9 | **14, 9, 5** | 14, 5, 9 | 12 | 24, 10, 12 | **24, 14, 8** | 15 | 28, 10, 13 | 28, 18, 5 |
| 4 | 8 | | | 12 | 14, 12, 2 | 14, 2, 12 | 16 | 24, 14, 8 | 24, 10, 12 | 20 | 28, 15, 8 | 28, 13, 10 |
| 5 | 10 | | | 15 | | | 20 | 24, 18, 4 | 24, 6, 16 | 25 | 28, 20, 3 | 28, 8, 15 |
| 6 | 12 | | | 18 | | | 24 | | | 30 | | 28, 3, 20 |

**Table 6. Constructive code characteristics of algebraic geometric codes over $GF(16)$**

| $\deg f$ | $\deg X=2,\ g=0$ | | | $\deg X=3,\ g=1$ | | | $\deg X=4,\ g=3$ | | | $\deg X=5,\ g=6$ | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $a$ | $n,k,d$ | $n,k,d$ | $a$ | $n,k,d$ | $n,k,d$ | $a$ | $n,k,d$ | $n,k,d$ | $a$ | $n,k,d$ | $n,k,d$ |
| 1 | 2 | 17, 3, 15 | 17, 14, 4 | 3 | 25, 3, 22 | 25, 22, 3 | 4 | 34, 2, 30 | – | 5 | – | – |
| 2 | 4 | 17, 5, 13 | 17, 12, 6 | 6 | 25, 6, 19 | 25, 19, 6 | 8 | 34, 6, 26 | 34, 28, 4 | 10 | 65, 5, 55 | – |
| 3 | 6 | 17, 7, 11 | 17, 10, 8 | 9 | 25, 9, 16 | **25, 16, 9** | 12 | 34, 10, 22 | 34, 24, 8 | 15 | 65, 10, 50 | 65, 55, 5 |
| 4 | 8 | 17, 9, 9 | 17, 8, 10 | 12 | 25, 12, 13 | 25, 13, 12 | 16 | 34, 14, 18 | **34, 20, 12** | 20 | 65, 15, 45 | 65, 50, 10 |
| 5 | 10 | **17, 11, 7** | 17, 6, 12 | 15 | 25, 15, 10 | 25, 10, 15 | 20 | 34, 18, 14 | 34, 16, 16 | 25 | 65, 20, 40 | **65, 45, 15** |
| 6 | 12 | 17, 13, 5 | 17, 4, 14 | 18 | 25, 18, 7 | 25, 7, 18 | 24 | 34, 22, 10 | 34, 12, 20 | 30 | 65, 25, 35 | 65, 40, 20 |
| 7 | 14 | 17, 15, 3 | 17, 2, 16 | 21 | 25, 21, 4 | 25, 4, 21 | 28 | 34, 26, 6 | 34, 8, 24 | 35 | 65, 30, 30 | 65, 35, 25 |
| 8 | 16 | | | 24 | | | 32 | 34, 30, 2 | 34, 4, 28 | 40 | 65, 35, 25 | 65, 30, 30 |
| 9 | 18 | | | 27 | | | 36 | | | 45 | 65, 40, 20 | 65, 25, 35 |
| 10 | 20 | | | 30 | | | 40 | | | 50 | 65, 45, 15 | 65, 20, 40 |
| 11 | 22 | | | 33 | | | 44 | | | 55 | 65, 50, 10 | 65, 15, 45 |
| 12 | 24 | | | 36 | | | 48 | | | 60 | 65, 55, 5 | 65, 10, 50 |
| 13 | 26 | | | 39 | | | 52 | | | 65 | | 65, 5, 55 |

**Table 7. Constructive code characteristics of algebraic geometric codes over $GF(32)$**

| $\deg f$ | $\deg X=2,\ g=0$ | | | $\deg X=3,$ | | | $\deg X=4,\ g=3$ | | | $\deg X=5,\ g=6$ | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $a$ | $n,k,d$ | $n,k,d$ | $a$ | $n,k,d$ | $n,k,d$ | $a$ | $n,k,d$ | $n,k,d$ | $a$ | $n,k,d$ | $n,k,d$ |
| 1 | 2 | 33, 3, 31 | 33, 30, 4 | 3 | 44, 3, 41 | 44, 41, 3 | 4 | 63, 2, 59 | – | 5 | – | – |
| 2 | 4 | 33, 5, 29 | 33, 28, 6 | 6 | 44, 6, 38 | 44, 38, 6 | 8 | 63, 6, 55 | 63, 57, 4 | 10 | 99, 5, 89 | – |
| 3 | 6 | 33, 7, 27 | 33, 26, 8 | 9 | 44, 9, 35 | 44, 35, 9 | 12 | 63, 10, 51 | 63, 53, 8 | 15 | 99, 10, 84 | 99, 89, 5 |
| 4 | 8 | 33, 9, 25 | 33, 24, 10 | 12 | 44, 12, 32 | 44, 32, 12 | 16 | 63, 14, 47 | 63, 49, 12 | 20 | 99, 15, 79 | 99, 84, 10 |
| 5 | 10 | 33, 11, 23 | 33, 22, 12 | 15 | 44, 15, 29 | **44, 29, 15** | 20 | 63, 18, 43 | 63, 45, 16 | 25 | 99, 20, 74 | 99, 79, 15 |
| 6 | 12 | 33, 13, 21 | 33, 20, 14 | 18 | 44, 18, 26 | 44, 26, 18 | 24 | 63, 22, 39 | 63, 41, 20 | 30 | 99, 25, 69 | 99, 74, 20 |
| 7 | 14 | 33, 15, 19 | 33, 18, 16 | 21 | 44, 21, 23 | 44, 23, 21 | 28 | 63, 26, 35 | 63, 37, 24 | 35 | 99, 30, 64 | 99, 69, 25 |
| 8 | 16 | 33, 17, 17 | 33, 16, 18 | 24 | 44, 24, 20 | 44, 20, 24 | 32 | 63, 30, 31 | 63, 33, 28 | 40 | 99, 35, 59 | 99, 64, 30 |
| 9 | 18 | 33, 19, 15 | 33, 14, 20 | 27 | 44, 27, 17 | 44, 17, 27 | 36 | 63, 34, 27 | 63, 29, 32 | 45 | 99, 40, 54 | 99, 59, 35 |
| 10 | 20 | 33, 21, 13 | 33, 12, 22 | 30 | 44, 30, 14 | 44, 14, 30 | 40 | 63, 38, 23 | 63, 25, 36 | 50 | 99, 45, 49 | 99, 54, 40 |
| 11 | 22 | **33, 23, 11** | 33, 10, 24 | 33 | 44, 33, 11 | 44, 11, 33 | 44 | **63, 42, 19** | 63, 21, 40 | 55 | 99, 50, 44 | 99, 49, 45 |
| 12 | 24 | 33, 25, 9 | 33, 8, 26 | 36 | 44, 36, 8 | 44, 8, 36 | 48 | 63, 46, 15 | 63, 17, 44 | 60 | 99, 55, 39 | 99, 44, 50 |
| 13 | 26 | 33, 27, 7 | 33, 6, 28 | 39 | 44, 39, 5 | 44, 5, 39 | 52 | 63, 50, 11 | 63, 13, 48 | 65 | 99, 60, 34 | 99, 39, 55 |
| 14 | 28 | 33, 29, 5 | 33, 4, 30 | 42 | 44, 42, 2 | 44, 2, 42 | 56 | 63, 54, 7 | 63, 9, 52 | 70 | **99, 65, 29** | 99, 34, 60 |
| 15 | 30 | 33, 31, 3 | 33, 2, 32 | 45 | | | 60 | 63, 58, 3 | 63, 5, 56 | 75 | 99, 70, 24 | 99, 29, 65 |
| 16 | 32 | | | 48 | | | 64 | | 63, 1, 60 | 80 | 99, 75, 19 | 99, 24, 70 |
| 17 | 34 | | | 51 | | | 68 | | | 85 | 99, 80, 14 | 99, 19, 75 |
| 18 | 36 | | | 54 | | | 72 | | | 90 | 99, 85, 9 | 99, 14, 80 |
| 19 | 38 | | | 57 | | | 76 | | | 95 | 99, 90, 4 | 99, 9, 85 |
| 20 | 40 | | | 60 | | | 80 | | | 100 | | 99, 4, 90 |

**Table 8. Constructive code characteristics of algebraic geometric codes over $GF(64)$**

| deg$f$ | deg $X=2, g=0$ | | | deg $X=3, g=1$ | | | deg $X=4, g=3$ | | | deg $X=5, g=6$ | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $a$ | $n,k,d$ | $n,k,d$ | $a$ | $n,k,d$ | $n,k,d$ | $a$ | $n,k,d$ | $n,k,d$ | $a$ | $n,k,d$ | $n,k,d$ |
| 1 | 2 | 65,3,63 | 65,62,4 | 3 | 81,3,78 | 81,78,3 | 4 | 113,2,109 | – | 5 | – | – |
| 2 | 4 | 65,5,61 | 65,60,6 | 6 | 81,6,75 | 81,75,6 | 8 | 113,6,105 | 113,107,4 | 10 | 164,5,154 | – |
| 3 | 6 | 65,7,59 | 65,58,8 | 9 | 81,9,72 | 81,72,9 | 12 | 113,10,101 | 113,103,8 | 15 | 164,10,149 | 164,154,5 |
| 4 | 8 | 65,9,57 | 65,56,10 | 12 | 81,12,69 | 81,69,12 | 16 | 113,14,97 | 113,99,12 | 20 | 164,15,144 | 164,149,10 |
| 5 | 10 | 65,11,55 | 65,54,12 | 15 | 81,15,66 | 81,66,15 | 20 | 113,18,93 | 113,95,16 | 25 | 164,20,139 | 164,144,15 |
| 6 | 12 | 65,13,53 | 65,52,14 | 18 | 81,18,63 | 81,63,18 | 24 | 113,22,89 | 113,91,20 | 30 | 164,25,134 | 164,139,20 |
| 7 | 14 | 65,15,51 | 65,50,16 | 21 | 81,21,60 | 81,60,21 | 28 | 113,26,85 | 113,87,24 | 35 | 164,30,129 | 164,134,25 |
| 8 | 16 | 65,17,49 | 65,48,18 | 24 | 81,24,57 | 81,57,24 | 32 | 113,30,81 | 113,83,28 | 40 | 164,35,124 | 164,129,30 |
| 9 | 18 | 65,19,47 | 65,46,20 | 27 | 81,27,54 | **81,54,27** | 36 | 113,34,77 | 113,79,32 | 45 | 164,40,119 | 164,124,35 |
| 10 | 20 | 65,21,45 | 65,44,22 | 30 | 81,30,51 | 81,51,30 | 40 | 113,38,73 | 113,75,36 | 50 | 164,45,114 | 164,119,40 |
| 11 | 22 | 65,23,43 | 65,42,24 | 33 | 81,33,48 | 81,48,33 | 44 | 113,42,69 | 113,71,40 | 55 | 164,50,109 | 164,114,45 |
| 12 | 24 | 65,25,41 | 65,40,26 | 36 | 81,36,45 | 81,45,36 | 48 | 113,46,65 | 113,67,44 | 60 | 164,55,104 | 164,109,50 |
| 13 | 26 | 65,27,39 | 65,38,28 | 39 | 81,39,42 | 81,42,39 | 52 | 113,50,61 | 113,63,48 | 65 | 164,60,99 | 164,104,55 |
| 14 | 28 | 65,29,37 | 65,36,30 | 42 | 81,42,39 | 81,39,42 | 56 | 113,54,57 | 113,59,52 | 70 | 164,65,94 | 164,99,60 |
| 15 | 30 | 65,31,35 | 65,34,32 | 45 | 81,45,36 | 81,36,45 | 60 | 113,58,53 | 113,55,56 | 75 | 164,70,89 | 164,94,65 |
| 16 | 32 | 65,33,33 | 65,32,34 | 48 | 81,48,33 | 81,33,48 | 64 | 113,62,49 | 113,51,60 | 80 | 164,75,84 | 164,89,70 |
| 17 | 34 | 65,35,31 | 65,30,36 | 51 | 81,51,30 | 81,30,51 | 68 | 113,66,45 | 113,47,64 | 85 | 164,80,79 | 164,84,75 |
| 18 | 36 | 65,37,29 | 65,28,38 | 54 | 81,54,27 | 81,27,54 | 72 | 113,70,41 | 113,43,68 | 90 | 164,85,74 | 164,79,80 |
| 19 | 38 | 65,39,27 | 65,26,40 | 57 | 81,57,24 | 81,24,57 | 76 | **113,74,37** | 113,39,72 | 95 | 164,90,69 | 164,74,85 |
| 20 | 40 | 65,41,25 | 65,24,42 | 60 | 81,60,21 | 81,21,60 | 80 | 113,78,33 | 113,35,76 | 100 | 164,95,64 | 164,69,90 |
| 21 | 42 | **65,43,23** | 65,22,44 | 63 | 81,63,18 | 81,18,63 | 84 | 113,82,29 | 113,31,80 | 105 | 164,100,59 | 164,64,95 |
| 22 | 44 | 65,45,21 | 65,20,46 | 66 | 81,66,15 | 81,15,66 | 88 | 113,86,25 | 113,27,84 | 110 | 164,105,54 | 164,59,100 |
| 23 | 46 | 65,47,19 | 65,18,48 | 69 | 81,69,12 | 81,12,69 | 92 | 113,90,21 | 113,23,88 | 115 | **164,110,49** | 164,54,105 |
| 24 | 48 | 65,49,17 | 65,16,50 | 72 | 81,72,9 | 81,9,72 | 96 | 113,94,17 | 113,19,92 | 120 | 164,115,44 | 164,49,110 |
| 25 | 50 | 65,51,15 | 65,14,52 | 75 | 81,75,6 | 81,6,75 | 100 | 113,98,13 | 113,15,96 | 125 | 164,120,39 | 164,44,115 |
| 26 | 52 | 65,53,13 | 65,12,54 | 78 | 81,78,3 | 81,3,78 | 104 | 113,102,9 | 113,11,100 | 130 | 164,125,34 | 164,39,120 |
| 27 | 54 | 65,55,11 | 65,10,56 | 81 | | | 108 | 113,106,5 | 113,7,104 | 135 | 164,130,29 | 164,34,125 |
| 28 | 56 | 65,57,9 | 65,8,58 | 84 | | | 112 | 113,110,1 | 113,3,108 | 140 | 164,135,24 | 164,29,130 |
| 29 | 58 | 65,59,7 | 65,6,60 | 87 | | | 116 | | | 145 | 164,140,19 | 164,24,135 |
| 30 | 60 | 65,61,5 | 65,4,62 | 90 | | | 120 | | | 150 | 164,145,14 | 164,19,140 |
| 31 | 62 | 65,63,3 | 65,2,64 | 93 | | | 123 | | | 155 | 164,150,9 | 164,14,145 |
| 32 | | | | | | | | | | 160 | 164,155,4 | 164,9,150 |

## 3.1. ENCODING IN UNSYSTEMATIC FORM VIA THE GENERATING MATRIX

Fix a smooth projective algebraic curve $X$ in the projective space $P^u$ over a field $GF(q)$ as the collection of solutions $u-1$ of homogeneous irreducible algebraic equations in $n$ variables with coefficients from $GF(q)$:

$$\begin{cases} f_1(x_0, x_1, ..., x_{u-1}) = 0 \\ f_2(x_0, x_1, ..., x_{u-1}) = 0 \\ ... \\ f_{u-1}(x_0, x_1, ..., x_{u-1}) = 0 \end{cases}. \quad (1)$$

Let $p_0(x_0, x_1, ..., x_{u-1})$, $p_1(x_0, x_1, ..., x_{u-1})$, …, $p_{N-1}(x_0, x_1, ..., x_{u-1})$ be $N$ of the joint solutions of equations (1) for the points of the curve $X$.

We fix the divisor $D$ of the curve $X$ and the set of rational functions associated with the divisor $D$, i.e., the set consisting of zero and functions $F \neq 0$ for which $(F) + D \geq 0$. This is equivalent to the set of generator functions

$$F_0(x_0, x_1, ..., x_{u-1}),\ F_1(x_0, x_1, ..., x_{u-1}),$$
$$F_2(x_0, x_1, ..., x_{u-1}),\ ...,\ F_{w-1}(x_0, x_1, ..., x_{u-1}),$$

where $F_0, F_1, ..., F_w$ are forms with the same degree and $F_0(x_0, x_1, ..., x_{u-1}) \neq 0$.

In other words,

$$\phi(x) = (F_0(x), F_1(x), ..., F_{w-1}(x))$$

is a point in $P^w$.

Let $\alpha$ be the degree of the divisor class, $\alpha > g-1$, then the mapping $\phi: X \to P^w$ defines the generating matrix

$$G = \left\| F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{n,k}, \quad j = \overline{0, k-1},\ i = \overline{0, n-1}, \qquad (2)$$

of the algebraic geometric code with the constructive characteristics

$$\sum_{i=0}^{k-1} I_i F_i\left(p_j\left(x_0, x_1, ..., x_{u-1}\right)\right) = c_j,\ j = 0, ..., n-1,$$

(here and below the symbol $\|...\|$ is used to denote the matrix).

To form the code word $\left(c_0, c_1, ...c_{n-1}\right)$ of the algebraic geometric code given through the generator matrix, it suffices to multiply the information vector $\left(I_0, I_1, ...I_{k-1}\right)$ by matrix (2), i.e., for all $j = 0, ..., n-1$, perform the following conversion:

$$c_j = \sum_{i=0}^{k-1} I_i F_i\left(p_j\left(x_0, x_1, ..., x_{u-1}\right)\right). \qquad (3)$$

Obviously, the formation of the code word is carried out by an iterative procedure, allowing at each step of the algorithm to generate the appropriate code symbol.

## 3.2. CODING IN A SYSTEMATIC MANNER THROUGH A CHECK MATRIX

Let $\alpha > 2g-2$, then the mapping $\phi: X \to P^w$ generates the check matrix

$$H = \left\| F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{n,r}, \quad j = \overline{0, r-1},\ i = \overline{0, n-1}, \qquad (4)$$

of the algebraic geometric code with the constructive characteristics

$$\left(n \le N, k \ge n - \alpha + g - 1,\ d \ge \alpha - 2g + 2\right).$$

The algebraic geometric code from the curve $X$ over $GF(q)$ constructed through the verification matrix $H$ is a linear code consisting of all words $\left(c_0, c_1, ...c_{n-1}\right)$ of length $n \le N$ for which $\left(d + g - 1\right)$ equations are true

$$\sum_{i=0}^{n-1} c_i F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right) = 0,\ j = 0, ..., w. \qquad (5)$$

To form the code words of the algebraic geometric code given in this way on the space curves, we use the matrix inversion techniques [4-6].

We divide the code word $\left(c_0, c_1, ...c_{n-1}\right)$ into sets of information and verification positions (see Fig. 2). Let $U$ be the set of $k$ information positions of the code word (i.e., the set of position numbers included in the given information code set) and $W$ be the set of $r = n - k$ verification items. The union of the sets $U \cup W$ contains all the integers from 0 to $n-1$.

In $k$ information positions of the code word, i.e., in the positions of the set $U$, we place $k$ symbols of the message $\left(I_0, I_1, ...I_{k-1}\right)$, and in the verification positions of the set $W$, we place $r$ zero symbols.

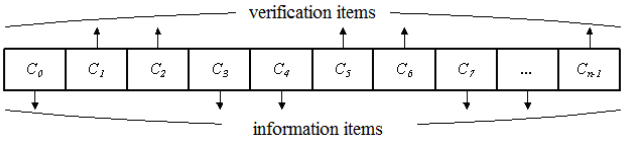


**Figure 2 – Splitting the code word into information and verification items**

Let us calculate the sums

$$S_j = \sum_{i=0}^{n-1} c_i F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right),\ j = \overline{0, r-1},$$

or in the matrix form,

$$\left\| S_j \right\|_r = \left\| F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{k,r} \left\| c_i \right\|_k^T. \qquad (6)$$

The task of forming a code word is to compute and put in $r$ verification positions symbols $c_i$, $i \in W$, satisfying equations (5).

It follows from the definition of an algebraic geometric code that the values of $r = n - k$ verification symbols can be found from a system of linear equations

$$\sum_{i \in W} c_i F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right) = -S_j,\ j = \overline{0, r-1}.$$

In the matrix representation, the last notation is equivalent to the expression

$$\left\| F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r} \left\| c_i \right\|_r^T = \left\| -S_j \right\|_r .$$

To find the values of $r = n - k$ verification symbols, using matrix inversion methods, we write

$$\left\| c_i \right\|_r = \left\| F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}^{-1} \left\| -S_j \right\|_r^T, \quad (7)$$

where $\left\| F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}^{-1}$ is the inverse matrix for the matrix $\left\| F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}$, i.e.,

$$\left\| \left\| F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}^{-1} \right\|_{r,r} = \left\| \frac{A\left[\left\| F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}\right]}{\Delta_{\left\| F_j \right\|_{r,r}}} \right\|_{r,r}.$$

Here, $A\left[\left\| F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}\right]$ is the algebraic complement of an element of the matrix $\left\| F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}$, and $\Delta_{\left\| F_j \right\|_{r,r}}$ is the determinant of the matrix $\left\| F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}$.

Since the placement of verification items is usually known and fixed, the inverse matrix for the system of equations (5) can be found in advance and all the verification symbols can be obtained by multiplying the vector $\left(S_0, S_1, ...S_{r-1}\right)$ by the matrix $\left\| F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}^{-1}$. Any $k$ code word positions can be selected as information. Therefore, it is always possible to choose a set of verification (and information) positions for which the matrix $\left\| F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}^{-1}$ is the most convenient for calculations.

Thus, to form the code word of the algebraic geometric code given through the verification matrix, it is sufficient to store the elements of matrixes $\left\| F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{k,r}$ and $\left\| F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}^{-1}$ or alternately, calculate the values $\left\| F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{k,r}$ as the values of generator functions at the points of the spatial curve.

## 3.3. DECODING OF ALGEBRAIC GEOMETRIC CODES

Consider a code word of an algebraic geometric $\left(n, k, d\right)$ code over $GF(q)$ constructed from algebraic curves in $P^u$. Suppose that an algebraic geometric code is given by a check matrix:

$$H = \begin{pmatrix} F_{0,0,...,0}\left(p_j\left(x_0, x_1, ..., x_{u-1}\right)\right) \\ F_{1,0,...,0}\left(p_j\left(x_0, x_1, ..., x_{u-1}\right)\right) \\ \\ F_{0,0,...,\deg F}\left(p_j\left(x_0, x_1, ..., x_{u-1}\right)\right) \end{pmatrix},$$

where $F_{i_0, i_1, ..., i_{u-1}}$ is a monomial of degree $i_0 + i_1 + ... + i_{u-1} \le \deg F$, i.e.

$$F_{i_0, i_1, ..., i_{u-1}} = x_0^{i_0} \cdot x_1^{i_1} \cdot ... \cdot x_{u-1}^{i_{u-1}},\ i = 0, ..., M-1,$$
$$M = C_{u+\deg F}^{u} - 1.$$

The equality holds:

$$C \cdot H^T = 0,$$

which implies the equality:

$$\sum_{j=0}^{n-1} C_j \cdot F_{i_0, i_1, ..., i_{u-1}}\left(p_j\left(x_0, x_1, ..., x_{u-1}\right)\right) = 0,$$

for all $i = 0, ..., M-1$.

Suppose that when transmitting via a channel with errors the codeword is distorted, then the error vector will be denoted by

$$e = \left(e_0, e_1, \ldots, e_{n-1}\right),$$

and the perceived word with mistakes will be denoted by

$$C^* = \left(C_0^*,\ C_1^*,\ \ldots,\ C_{n-1}^*\right) = C + e = \\ = (C_0 + e_0, C_1 + e_1,\ \ldots,\ C_{n-1} + e_{n-1}).$$

Define the syndrome sequence as a vector

$$s = \left( s_{0,0,\ldots,0}, s_{1,0,\ldots,0}, \ldots, s_{0,0,\ldots,\deg F} \right),$$

calculated according to the rule:

$$s_{i_0,i_1,\ldots,i_{u-1}} = \sum_{j=0}^{n-1} e_j \cdot F_{i_0,i_1,\ldots,i_{u-1}} \left( p_j \left( x_0, x_1, \ldots, x_{u-1} \right) \right),$$
$$i = 0, \ldots, M-1.$$

By definition, the value of the syndrome sequence $s$ depends only on the error vector $e$ and does not depend on the code word $C$. Indeed, we calculate the multiplication

$$C^* \cdot H^T = 0,$$

we obtain

$$(C+e) \cdot H^T = C \cdot H^T + e \cdot H^T = e \cdot H^T,$$

which implies the validity (for all $i = 0, \ldots, M-1$) of the equalities:

$$\sum_{j=0}^{n-1} (c_j + e_j) \cdot F_{i_0,i_1,\ldots,i_{u-1}} \left( p_j \left( x_0, x_1, \ldots, x_{u-1} \right) \right) =$$
$$= \sum_{j=0}^{n-1} e_j \cdot F_{i_0,i_1,\ldots,i_{u-1}} \left( p_j \left( x_0, x_1, \ldots, x_{u-1} \right) \right) = s_{i_0,i_1,\ldots,i_{u-1}}. \quad (8)$$

The problem of algebraic decoding is to find the vector

$$e = \left( e_0, e_1, \ldots, e_{n-1} \right)$$

with aid of a well-known syndrome sequence

$$s = \left( s_{0,0,\ldots,0}, s_{1,0,\ldots,0}, \ldots, s_{0,0,\ldots,\deg F} \right).$$

In its turn, found in this way vector $e$ makes it possible to restore the code word $C$ in a known sequence $C^*$:

$$C = C^* - e = (C_0^* - e_0, C_1^* - e_1, \ldots, C_{n-1}^* - e_{n-1}).$$

The solution of this problem is connected with finding $n$ unknowns from the system of $M$ linear equations, and $M < n$. Strictly speaking, when solving the problem by the methods of linear algebra, in general, one can find a set of solutions of the indicated system of equations. At the same time, it should be noted that only

$$v \le t = \left\lfloor \frac{(d-1)}{2} \right\rfloor$$

values of sequence $e = \left( e_0, e_1, \ldots, e_{n-1} \right)$ are not equal to zero; i.e., almost all $e_j = 0$ except for a certain (finite) number of them ($v$). With this restriction, there is one (unique) solution of the set of equations (8).

We denote the set $e_j \neq 0$ by the symbol $E$. To find the single-valued error vector, let us use an artificial technique related to the management of the polynomial of error locators:

$$\Lambda(x_0, x_1, \ldots, x_{u-1}) = x_0^{v-u+1} + a_{v-u,1,\ldots,0} \cdot x_0^{v-u} \cdot x_1 + \ldots +$$
$$+ a_{1,0,\ldots,0} \cdot x_0 + a_{0,1,\ldots,0} \cdot x_1 + \ldots + a_{0,0,\ldots,1} \cdot x_{u-1} + a_{0,0,\ldots,0}, \quad (9)$$

solutions of which are the locators. (Locators are such sets $(X_{0_j}, X_{1_j}, \ldots, X_{u-1_j})$ that nullify the polynomial (9) with the corresponding elements of the error vector $e_\xi \in E$.)

Polynomial (9) uniquely determines the location of the errors in the vector $e = \left( e_0, e_1, \ldots, e_{n-1} \right)$, since it uniquely points to its nonzero components. In other words, finding the coefficients $a_{i_0,i_1,\ldots,i_{u-1}}$ of the error locator polynomial $\Lambda(x_0, x_1, \ldots, x_{u-1})$ allows one to uniquely indicate the location of the errors that occurred during the transmission of the code word (but not their values, the true values of nonzero entries $e_j$), for example, by alternately substituting all sets

$$p_j \left( x_0, x_1, \ldots, x_{u-1} \right) = (X_{0_j}, X_{1_j}, \ldots, X_{u-1_j})$$

into the polynomial $\Lambda(x_0, x_1, \ldots, x_{u-1})$ and verifying that it equals zero.

We multiply polynomial (9) by $e_j$ and compute its value at the point $(X_{0_j}, X_{1_j}, \ldots, X_{u-1_j})$, i.e., we obtain:

$$e_j \cdot X_{0_j}^{v-u+1} + a_{v-u,1,\ldots,0} \cdot e_j \cdot X_{0_j}^{v-u} \cdot X_{1_j} + \ldots +$$
$$+ a_{1,0,\ldots,0} \cdot e_j \cdot X_{0_j} + a_{0,1,\ldots,0} \cdot e_j \cdot X_{1_j} + \ldots + \quad (10)$$
$$+ a_{0,0,\ldots,1} \cdot e_j \cdot X_{u-1_j} + a_{0,0,\ldots,0} \cdot e_j.$$

Let's analyze the expression obtained.

If $e_j \notin E$, i.e., $e_j = 0$, then all the terms of the resulting polynomial are zero; we have the whole expression (10) equal to zero.

If $e_j \in E$, i.e. $e_j = 0$, then the corresponding sets $(X_{0_j}, X_{1_j}, ..., X_{u-1_j})$ vanish polynomial (9) and hence polynomial (10) drops to zero.

Thus, for any value of $e_j$, expression (10) is zero.

We sum over all $j = 0, \ldots, n-1$, and obtain:

$$\sum_{j=0}^{n-1} e_j \cdot X_{0_j}^{v-u+1} + \sum_{j=0}^{n-1} a_{v-u,1,\ldots,0} \cdot e_j \cdot X_{0_j}^{v-u} \cdot X_{1_j} + \ldots + \\ + \sum_{j=0}^{n-1} a_{1,0,\ldots,0} \cdot e_j \cdot X_{0_j} + \sum_{j=0}^{n-1} a_{0,1,\ldots,0} \cdot e_j \cdot X_{1_j} + \ldots + \\ + \sum_{j=0}^{n-1} a_{0,0,\ldots,1} \cdot e_j \cdot X_{u-1_j} + \sum_{j=0}^{n-1} a_{0,0,\ldots,0} \cdot e_j. \quad (11)$$

Let's analyze the obtained expression. Values $a_{i_0,i_1,\ldots,i_{u-1}}$ do not depend on $j$, hence we can take them out beyond the summation sign. Taking into account the notation introduced above, the value of the monomial

$$F_{i_0,i_1,\ldots,i_{u-1}} = x_0^{i_0} \cdot x_1^{i_1} \cdot \ldots \cdot x_{u-1}^{i_{u-1}}$$

at the point $(X_{0_j}, X_{1_j}, ..., X_{u-1_j})$ has the form

$$F_{i_0,i_1,\ldots,i_{u-1}}(X_{0_j}, X_{1_j}, ..., X_{u-1_j}) = X_{0_j}^{i_0} \cdot X_{1_j}^{i_1} \cdot \ldots \cdot X_{u-1_j}^{i_{u-1}}.$$

Taking the latter into account, formula (11) can be rewritten as:

$$\sum_{j=0}^{n-1} e_j \cdot F_{v-u+1,0,\ldots,0}(X_{0_j}, X_{1_j}, ..., X_{u-1_j}) + \\ + a_{v-u,1,\ldots,0} \sum_{j=0}^{n-1} \cdot e_j \cdot F_{v-u,1,\ldots,0}(X_{0_j}, X_{1_j}, ..., X_{u-1_j}) + \ldots + \\ + a_{1,0,\ldots,0} \sum_{j=0}^{n-1} \cdot e_j \cdot F_{1,0,\ldots,0}(X_{0_j}, X_{1_j}, ..., X_{u-1_j}) + \\ + a_{0,1,\ldots,0} \sum_{j=0}^{n-1} \cdot e_j \cdot F_{0,1,\ldots,0}(X_{0_j}, X_{1_j}, ..., X_{u-1_j}) + \ldots + \\ + a_{0,0,\ldots,1} \sum_{j=0}^{n-1} \cdot e_j \cdot F_{0,0,\ldots,1}(X_{0_j}, X_{1_j}, ..., X_{u-1_j}) + \\ + a_{1,0,\ldots,0} \sum_{j=0}^{n-1} \cdot e_j = 0.$$

But by the above definition

$$s_{i_0,i_1,\ldots,i_{u-1}} = \sum_{j=0}^{n-1} e_j \cdot F_{i_0,i_1,\ldots,i_{u-1}}\left(p_j\left(x_0, x_1, ..., x_{u-1}\right)\right).$$

Therefore, we have:

$$s_{v-u+1,0,\ldots,0} + a_{v-u,1,\ldots,0} \cdot s_{v-u,1,\ldots,0} + \ldots + \\ + a_{1,0,\ldots,0} \cdot s_{1,0,\ldots,0} + a_{0,1,\ldots,0} \cdot s_{0,1,\ldots,0} + \ldots + \\ + a_{0,0,\ldots,1} \cdot s_{0,0,\ldots,1} + a_{0,0,\ldots,0} \cdot s_{0,0,\ldots,0} = 0.$$

We now return to the consideration of polynomial (9). We multiply it by an arbitrary monomial $x_0^{i_0} \cdot x_1^{i_1} \cdot \ldots \cdot x_{u-1}^{i_{u-1}}$ and carry out analogous arguments. By analogy with (10), the equality vanishes for any value of $e_j$. After summing over all $j = 0, \ldots, n-1$ and performing the obvious substitutions, we obtain the recurrence formula:

$$s_{i_0+v-u+1,i_1,\ldots,i_{u-1}} + a_{v-u,1,\ldots,0} \cdot s_{i_0+v-u,i_1+1,\ldots,i_{u-1}} + \ldots + \\ + a_{1,0,\ldots,0} \cdot s_{i_0+1,i_1,\ldots,i_{u-1}} + a_{0,1,\ldots,0} \cdot s_{i_0,i_1+1,\ldots,i_{u-1}} + \ldots + \\ + a_{0,0,\ldots,1} \cdot s_{i_0,i_1,\ldots,i_{u-1}+1} + a_{0,0,\ldots,0} \cdot s_{i_0,i_1,\ldots,i_{u-1}} = 0.$$

Performing the appropriate transformations for all $i = 0, ..., M-1$ we obtain a system of linear equations:

$$\begin{cases} s_{v-u+1,0,\ldots,0} + a_{v-u,1,\ldots,0} \cdot s_{v-u,1,\ldots,0} + \ldots + \\ + a_{1,0,\ldots,0} \cdot s_{1,0,\ldots,0} + a_{0,1,\ldots,0} \cdot s_{0,1,\ldots,0} + \ldots + \\ + a_{0,0,\ldots,1} \cdot s_{0,0,\ldots,1} + a_{0,0,\ldots,0} \cdot s_{0,0,\ldots,0} = 0; \\ s_{v-u+2,0,\ldots,0} + a_{v-u,1,\ldots,0} \cdot s_{v-u+1,1,\ldots,0} + \ldots + \\ + a_{1,0,\ldots,0} \cdot s_{2,0,\ldots,0} + a_{0,1,\ldots,0} \cdot s_{1,1,\ldots,0} + \ldots + \\ + a_{0,0,\ldots,1} \cdot s_{1,0,\ldots,1} + a_{0,0,\ldots,0} \cdot s_{1,0,\ldots,0} = 0; \\ \ldots \\ s_{2v-2u+2,0,\ldots,0} + a_{v-u,1,\ldots,0} \cdot s_{2v-2u+1,1,\ldots,0} + \ldots + \\ + a_{1,0,\ldots,0} \cdot s_{v-u+2,0,\ldots,0} + a_{0,1,\ldots,0} \cdot s_{v-u+1,1,\ldots,0} + \ldots + \\ + a_{0,0,\ldots,1} \cdot s_{v-u+1,0,\ldots,1} + a_{0,0,\ldots,0} \cdot s_{v-u+1,0,\ldots,0} = 0. \end{cases} \quad (12)$$

If the number of unknowns $z$ in the polynomial of error locators is less than the number of elements of the syndrome sequence, the system of linear equations (12) is solvable. The complexity of its solution, for example, by the Gaussian method is equal to $z^2$.

The solutions of system (12) give the values of the unknown coefficients of the polynomial (9) of the error locators $\Lambda(x_0, x_1, ..., x_{u-1})$, which in turn uniquely determines the values of the locators, such sets $(X_{0_j}, X_{1_j}, ..., X_{u-1_j})$ that vanish the polynomial (9), with the corresponding elements $e_i \in E$.

The search for $(X_{0_j}, X_{1_j}, ..., X_{u-1_j})$ can be performed, for example, by alternately substituting all $(X_{0_j}, X_{1_j}, ..., X_{u-1_j})$, $j = 0, \ldots, n-1$ into the polynomial $\Lambda(x_0, x_1, ..., x_{u-1})$ and checking for its equality to zero.

The found $(X_{0_j}, X_{1_j}, ..., X_{u-1_j})$ localize an error in the code word, i.e., equate to zero the $n-v$ unknowns in system (8). Because the number of remaining unknowns satisfies $v < M$, the system (8) is solvable. The complexity of its solution, for example, by the Gauss method, does not exceed $v^2$. The solution of system (8) gives the unknown (nonzero) values of the error vector $e = (e_0, e_1, ..., e_{n-1})$ i.e., the decoding problem is solved.

## 4. ENERGY EFFICIENCY OF ALGEBRAIC GEOMETRIC CODING

To estimate the energy efficiency of the algebraic geometric coding, consider the option of transmitting discrete messages by $M$-th orthogonal signals.

With uncoded message transmission, the probability of erroneous reception of $M$-th symbols in the case of coherent reception of orthogonal signals is determined by the expression [4-6]:

$$P_c = 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{u^2}{2}} \left[ \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{u+\sqrt{2\gamma}} e^{-\frac{z^2}{2}} dz \right]^{M-1} du, \quad (13)$$

where $\gamma$ is the signal-to-noise ratio for the $M$-th symbol, $M = 2^m$, $\gamma_2$ is the normalized signal-to-noise ratio per binary unit, $\gamma_2 = \gamma / m$.

Fig. 3 shows the dependence of the probability of erroneous reception of the $M$-th symbol in the coherent reception of orthogonal signals.

The transmission of $M$ orthogonal signals makes it possible to obtain a significant gain of noise immunity for a fixed signal-to-noise ratio, or a significant energy gain with a fixed error probability (for each symbol). As the power of the ensemble of signals increases, this gain goes up, too.

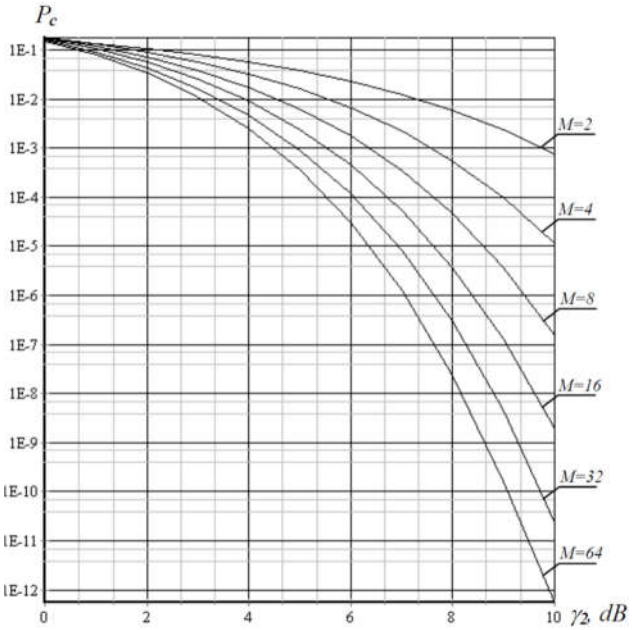


**Figure 3 - Dependencies of the probability of mistaken reception of $M$-th symbols from the normalized signal-to-noise ratio per one bit**

Let the code be $(n, k, d)$. We assume that the errors in consecutively transmitted code symbols occur independently with probability $P_o$. Then the probability of a multiplicity error on the block length $n$ will be equal to

$$P_i = C_n^i P_o^i (1 - P_o)^{n-i}. \quad (14)$$

If the decoder corrects $t = (d-1)/2$ errors, then the probability of erroneous decoding of the block is

$$P_{бл} = \sum_{i=t+1}^{n} P_i = \sum_{i=t+1}^{n} C_n^i P_o^i (1 - P_o)^{n-i}. \quad (15)$$

If we accept the assumption of a random occurrence of $2t+1$ and more errors as a result of erroneous decoding of the code word, then the mathematical expectation of the number of erroneous information symbols at the decoder output is determined by the expression [4-6]

$$m_{ош} = \sum_{i=t+1}^{n-t} \frac{(i+t)k}{n} P_i + k \sum_{i=n-t+1}^{n} P_i, \quad (16)$$

and the probability of erroneous decoding of the information symbol is

$$P_{од} = m_{ош} P_{бл}. \quad (17)$$

The use of codes that detect and correct errors leads to an increase in the redundancy of the transmitted data. If we fix the energy of the message transmitted to the channel, then the energy per one symbol will decrease proportionally to the redundancy introduced. To calculate the dependencies of the error probability on the symbol at the output of the decoder (14-17), taking into account the redundancy introduced, the signal-to-noise ratio $\gamma$ in expression (13) is reduced by $R = k/n$ times.

Let's consider a variant of transferring discrete messages by 4 orthogonal signals. The transmitted messages are encoded by an algebraic geometric code constructed above the field *GF*(4) (the selected code parameters are highlighted in color in Table 4). Figure 4 shows the dependencies of the error probability of the 4-th symbol on the normalized signal-to-noise ratio when four orthogonal signals are coherently received using noise-immune algebra-geometric codes.

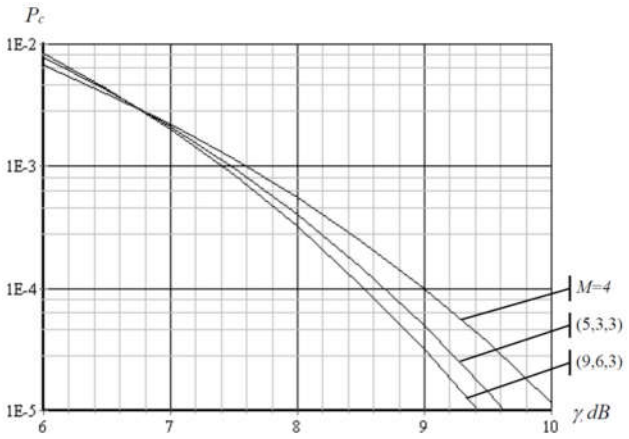


**Figure 4 - Energy efficiency of algebraic geometric codes with coherent reception of 4th orthogonal signals**

A relationship marked as "*M*=4" corresponds to an uncoded transmission. The dependence marked as (5,3,3) corresponds to an algebraic geometric code along a curve of genus $g = 0$ whose code characteristics lie on the Singleton boundary. This code with the maximum distance separable codes (MDS code) is the extended Reed-Solomon code. The greatest energy gain in algebraic geometric codes (including MDS codes) is given at the speed $R \approx 2/3$. The dependencies presented in Figure 4 show the advantages of using algebraic geometric codes for noise-immune message transmission. Thus, with the error probability per symbol $P_c = 10^{-5}$, the application of the code (9,6,3) gives an energy gain of ≈0,6dB compared to the uncoded message transmission and ≈0,2dB in comparison with the MDS code.

Let's consider a variant of transferring discrete messages by 8 orthogonal signals. The transmitted messages are encoded by an algebraic geometric code constructed over the field *GF*(8). The constructive code characteristics of the selected codes are highlighted in color in Table 5. Figure 5 shows the dependence of the error probability of the 8th symbol on the normalized signal-to-noise ratio when coherently receiving 8 orthogonal signals using noise-immune algebra-geometric codes. The relationship marked as "*M*=8" corresponds to the uncoded transmission. With the error probability per symbol is $P_c = 10^{-6}$, the use of the code (23,14,7) gives an energy gain of ≈2dB in comparison with the non-coded message transmission and ≈0,8dB in comparison with the MDS code.

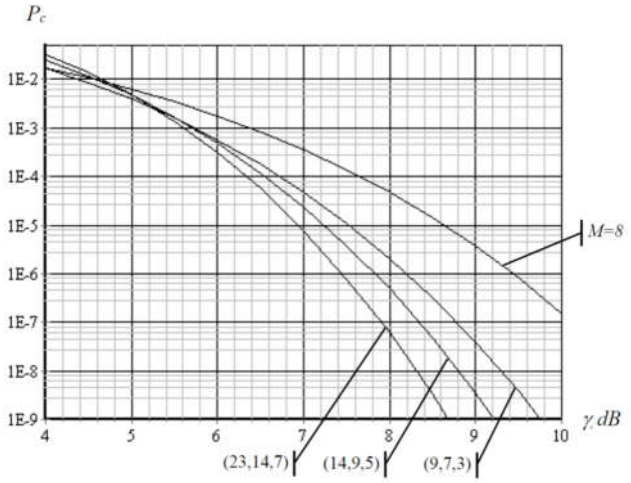


**Figure 5 - Energy efficiency of algebraic geometric codes with coherent reception of 8th orthogonal signals**

Let's consider a variant of transferring discrete messages by 16 orthogonal signals. The transmitted messages are encoded by an algebraic geometric code constructed over the field *GF*(16). The constructive code characteristics of the codes selected for the evaluation are outlined in Table 6. Figure 6 shows the dependencies of the error probability of the 16th character on the normalized signal-to-noise ratio when the coherent reception of 16 orthogonal signals using noise-immune algebra-geometric codes. The relationship marked as "*M*=16" corresponds to the uncoded transmission. With the error probability per symbol $P_c = 10^{-6}$, the application of the code (65,45,15) gives an energy

gain of ≈3dB in comparison with non-coded message transmission and ≈1dB in comparison with the MDS code.

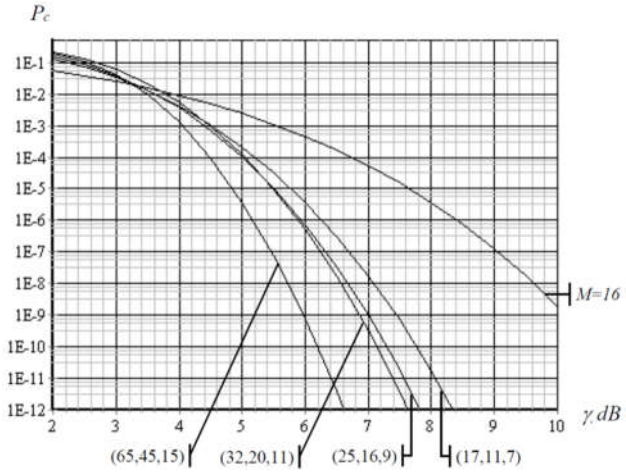


**Figure 6 - Energy efficiency of algebraic geometric codes with coherent reception of 16th orthogonal signals**

Let's consider the transfer variant of discrete messages by 32 orthogonal signals. The transmitted messages are encoded by an algebraic geometric code constructed over the field *GF*(32). The selected code characteristics are outlined in Table 7. Figure 7 shows the dependence of the error probability of the 32nd symbol on the normalized signal-to-noise ratio when the coherent reception of 32 orthogonal signals using noise-immune algebraic geometric codes. The relationship marked "*M*=32" corresponds to the uncoded transmission. With the error probability per symbol $P_c = 10^{-9}$, the use of the code (99,65,29) gives an energy gain of ≈4,5dB in comparison with the non-coded message transmission and ≈1dB in comparison with the MDS code.

Let's consider the transfer variant of discrete messages by 64 orthogonal signals. The transmitted messages are encoded by an algebraic geometric code constructed over a field *GF*(64) with the parameters highlighted in Table 8. Figure 8 shows the dependencies of the error probability of the 64th symbol on the normalized signal-to-noise ratio when coherently receiving 64 orthogonal signals using noise-immune algebraic geometry codes. A relationship marked as "*M*=64" corresponds to an uncoded transmission. With the error probability per symbol, the application of the code (164,110,49) gives an energy gain of ≈6dB as compared to non-coded message transmission and ≈0,8dB in comparison with the MDS code.

As follows from the dependencies presented in Figures 4-8, the use of algebraic geometric codes for increasing the noise immunity of message transmission in discrete channels without memory leads to a significant energy gain. Their use also makes it possible to significantly reduce the probability of error per symbol with a fixed signal-to-noise ratio per one transmitted bit. The energy gain increases with the transition to codes constructed from curves with a large number of points relative to the genus of the curve.

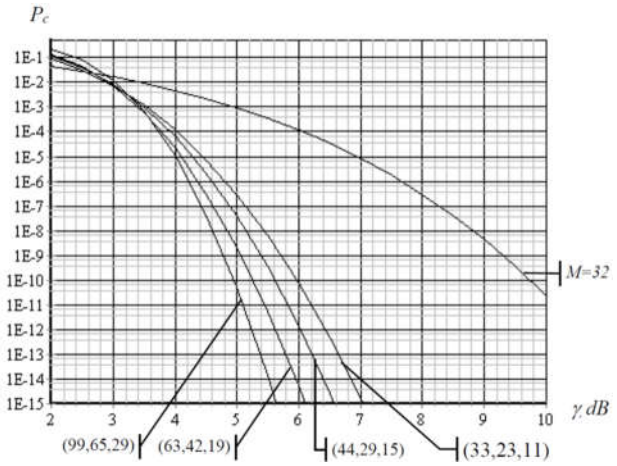


**Figure 7 - Energy efficiency of algebraic geometric codes with coherent reception of 32nd orthogonal signals**

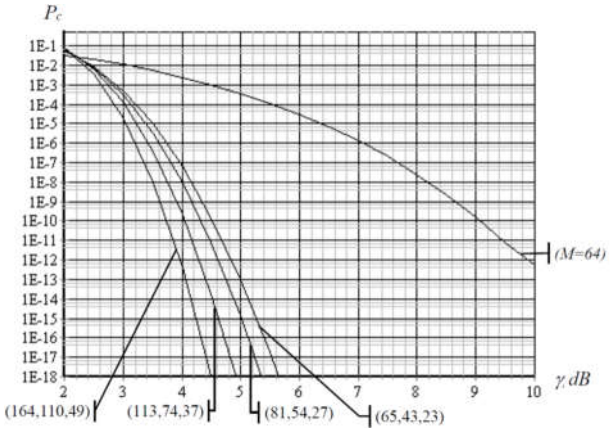


**Figure 8 - Energy efficiency of algebraic geometric codes with coherent reception of 64th orthogonal signals**

## 5. COMPARATIVE EVALUATION OF THE IMPLEMENTATION COMPLEXITY OF CODING AND DECODING

Let's make a comparative evaluation of the complexity of the implementation of the encoding-decoding procedures for the considered codes in comparison with the known schemes. The complexity of the encoding-decoding procedures (as well as the estimation of the energy gain of algebraic geometric coding) is evaluated in comparison with the Reed-Solomon codes.

If the code is given by the generator matrix *G*, the systematic encoding procedure is equivalent to multiplying the information word *I* by this matrix,

that is, $c=IG$, where $c$ is the code word. In this sense, the complexity of algorithms for systematic coding of algebraic geometric codes and Reed-Solomon codes is practically equivalent.

Reed-Solomon codes are a subclass of BCH codes, therefore, the same methods as for BCH codes are applied to their decoding. One of the most effective algorithms for algebraic decoding of BCH codes is the Berlekamp-Messi algorithm and its modifications (improvements). It is known [6] that the Berlekamp-Messi algorithm contains the number of multiplications, of order $t^2$, or, formally, the complexity of the algorithm $O(t^2)$. For large $t$, we use the accelerated Berlekamp-Massey algorithm, which makes it possible to reduce the computational complexity of the algorithm. Even more effective, in terms of computational complexity, is the recurrent algorithm of Berlekamp-Messi. The asymptotic complexity of decoding the Reed-Solomon codes, in this case, does not exceed $O(n\log^2 n)$, and is very close to the value of $O(n\log n)$.

Algorithms for decoding algebraic geometric codes were developed in [7-9]. So, in [7], a decoding algorithm is proposed, the complexity of which is determined by the value $O(n^3)$. Further development of the decoding procedure in [8] made it possible to reduce the computational complexity (shown by the example of Hermite curves) to $O(n^{7/3})$. In [9], the algorithm of decoding, of complexity $O(n^2)$, which allows parallelization of computations (on $n$ processors) is considered. Obviously, the existing algorithms for decoding algebraic geometric codes are comparable in computational complexity with the algorithms for decoding BCH codes.

## 6. CONCLUSION

A lot of studies have shown that algebraic geometric codes boast very constructive characteristics. In particular, the dependences given in Fig. 1 indicate that as the power of the alphabet increases, the code characteristics improve. With a large length, algebraic geometric codes lie above the Varshamov-Gilbert boundaries, which indicates high potential characteristics. We obtained code characteristics for various curves over finite fields $GF(2^m)$, $m$=2,…,6 (Tables 4-8).

As the studies show, the practical implementation of the algorithms for encoding and decoding algebraic geometric codes is reduced to simple and computationally efficient operations on finite fields. We presented several options for constructing codes (in a systematic and non-systematic form), and the simple decoding algorithms. The implementation of these algorithms does not require significant computational costs: as shown by the performed analysis, the complexity of encoding and decoding is comparable to other known classes of codes.

To evaluate the energy efficiency of algebraic geometric coding, we considered the option of discrete messages by $M$-orthogonal signals transmitting. As follows from the dependences shown in Figures 4-8, the use of algebraic geometric codes in discrete channels without memory leads to a significant energy gain. The energy gain increases with the transition to long codes constructed from curves with a large number of points relative to the genus of the curve.

The high energy efficiency of algebraic geometric coding in combination with an acceptable complexity of practical implementation allows us to talk about the possibility of constructing effective noise-immune systems based on the use of such codes [13-15]. Development and implementation of practical recommendations on the direct use of algebraic geometric codes in modern telecommunication systems and networks is a promising direction for further work. In addition, a prospective direction of further research is the argumentation of practical recommendations concerning the implementation of the introduced method and the ways of its use in different mechanisms of information security of telecommunications networks and systems.

## 7. REFERENCES

[1] V.D. Goppa, “Codes on algebraic curves,” *Report of Academy of Sciences of USSR*, vol. 259, no. 6, pp. 1289-1290, 1981. (in Russian)

[2] V.D. Goppa, “Codes and information,” *Uses of Mathematical Sciences*, vol. 30, no. 1 (235), pp. 77-120, 1984.

[3] M.A. Tsfasman, “The Goppa codes that lie above the Varshamov-Gilbert boundary,” *Problems of Information Transfer*, vol. 18, no. 3, pp. 3-6, 1982.

[4] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, New York, Oxford, 1977, 762 p.

[5] G.C. Clark, J.B. Cain, *Error-Correction Coding for Digital Communications*, Springer, 1981, 432 p.

[6] R. E. Blahut, *Theory and Practice of Error Control Codes*, Addison Wesley Publishing Company, Massachusetts, 1983, 500 p.

[7] G.L. Feng, T.R.N. Rao, “Decoding algebraic geometric codes up to the designed minimum distance,” *IEEE Trans. Inform. Theory*, vol. 39, no. 1, pp. 37-46, 1993.

[8] S. Sakata, J. Justesen, Y. Madelung, H.E. Jensen, T. Hoholdt, "Fast decoding of algebraic-geometric codes up to the designed minimum distance," *IEEE Trans. Inform. Theory*, vol. 41, no. 5, pp. 1672-1677, 1995.

[9] V. Olshevksy, A. Shokrollahi, "A displacement structure approach to decoding algebraic geometric codes," *Proceedings of the 31st annual ACM Symposium on Theory of Computing (STOC)*, 1999, pp. 235-244.

[10] M. Calderini and G. Faina, "Generalized algebraic geometric codes from maximal curves," *IEEE Transactions on Information Theory*, vol. 58, no. 4, pp. 2386-2396, 2012.

[11] W. Hu, H. Cai, Y. Wu and Z. Wang, "A note on the relationship between algebraic geometric codes and LDPC codes," *Proceedings of the 2010 2nd International Conference on Signal Processing Systems*, Dalian, 2010, pp. 56-58.

[12] S. Wu, L. Chen and M. Johnston, "Low-complexity Chase decoding of algebraic-geometric codes using Koetter's interpolation," *Proceedings of the 2016 IEEE Information Theory Workshop*, Cambridge, 2016, pp. 414-418.

[13] S. Chouhan, R. Bose and M. Balakrishnan, "Integrated energy analysis of error correcting codes and modulation for energy efficient wireless sensor nodes," *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 5348-5355, October 2009. DOI: 10.1109/TWC.2009.090279

[14] I. Gorbenko, O. Nariezhnii and I. Kudryashov, "Construction method and features of one class of cryptographic discrete signals," *Proceedings of the 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 156-160.

[15] V. Krasnobayev, S. Koshman, A. Yanko and A. Martynenko, "Method of error control of the information presented in the modular number system," *Proceedings of the 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2018, pp. 39-42. DOI: 10.1109/INFOCOMMST.2018.8632049

[16] N.T. Courtois, M. Finiasz, N. Sendrier, "How to achieve a McEliece-based digital signature scheme," *Proceedings of the 7th Int. Conf. on Theory and Application of Cryptology and Information Security-Advances in Cryptology-ASIACRYPT'2001*, 9–13 December 2001, pp. 157-174.

[17] W. Hongbin and R. Yan, "A code-based multiple grade proxy signature scheme," *Proceedings of the 2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, Compiegne, 2013, pp. 559-562.

[18] A. Kuznetsov, I. Svatovskij, N. Kiyan and A. Pushkar'ov, "Code-based public-key cryptosystems for the post-quantum period," *Proceedings of the 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 125-130. DOI: 10.1109/INFOCOMMST.2017.8246365

[19] P. Gaborit and J. Schrek, "Efficient code-based one-time signature from automorphism groups with syndrome compatibility," *Proceedings of the 2012 IEEE International Symposium on Information Theory Proceedings*, Cambridge, MA, 2012, pp. 1982-1986.

[20] A. Kuznetsov, A. Pushkar'ov, N. Kiyan and T. Kuznetsova, "Code-based electronic digital signature," *Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kyiv, Ukraine, 2018, pp. 331-336. DOI: 10.1109/DESSERT.2018.8409154

[21] J. Hu and R. C. C. Cheung, "Toward practical code-based signature: Implementing fast and compact QC-LDGM signature scheme on embedded hardware," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 8, pp. 2086-2097, Aug. 2017.

[22] M. Rajabzadeh Asaar, M. H. Ameri, M. Salmasizadeh and M. R. Aref, "A provably secure code-based concurrent signature scheme," *IET Information Security*, vol. 12, no. 1, pp. 34-41, 2018. DOI: 10.1049/iet-ifs.2017.0023

[23] A. Kuznetsov, M. Lutsenko, N. Kiian, T. Makushenko and T. Kuznetsova, "Code-based key encapsulation mechanisms for post-quantum standardization," *Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kyiv, Ukraine, 2018, pp. 276-281. DOI: 10.1109/DESSERT. 2018.8409144

[24] L. Dallot, "Towards a concrete security proof of Courtois Finiasz and Sendrier signature scheme," *Proceedings of the 2nd Western European Workshop on Research in Cryptology WEWoRC'2007*, 4–6 July 2008, pp. 65-77.

[25] L. Hua, M. Han, S. Ma and X. Feng, "An undeniable signature scheme based on quasi-dyadic codes," *Proceedings of the 2018 IEEE 3rd Advanced Information Technology,*

*Electronic and Automation Control Conference (IAEAC)*, Chongqing, 2018, pp. 2189-2194. DOI: 10.1109/IAEAC.2018.8577671

[26] O. Blazy, P. Gaborit, J. Schrek, and N. Sendrier, "A code-based blind signature," *Proceedings of the 2017 IEEE International Symposium on Information Theory (ISIT)*, Aachen, 2017, pp. 2718-2722.

***Alexandr A. Kuznetsov,*** *Doctor of Sciences (Engineering), Full Professor, Academician of the Academy of Applied Radioelectronics Sciences, Professor of the Department security information systems and technologies of the V. N. Karazin Kharkiv National University.*

*Areas of scientific interests: applied cryptology and coding theory.*

***Ievgeniia P. Kolovanova,*** *Candidate of Sciences (Engineering), Associate Professor of the Department security information systems and technologies of the V. N. Karazin Kharkiv National University. Areas of scientific interests: cryptography and coding, security information systems and technologies.*

***Oleksii A. Smirnov,*** *Doctor of Sciences (Engineering), Full Professor. Head of Cybersecurity & Software Academic Department at Central Ukrainian National Technical University, Ukraine.*

*Areas of scientific interests: applied cryptography and coding, security information systems and technologies.*

***Tatyana Y. Kuznetsova,*** *Researcher of the Department security information systems and technologies of the V. N. Karazin Kharkiv National University.*

*Areas of scientific interests: cryptography and coding, security information systems and technologies.*