Problems of Information Transmission, Vol. 40, No. 2, 2004, pp. 103–117. Translated from Problemy Peredachi Informatsii, No. 2, 2004, pp. 3–18.
Original Russian Text Copyright © 2004 by Gabidulin, Pilipchuk.

Symmetric Rank Codes

E. M. Gabidulin and N. I. Pilipchuk

Moscow Institute of Physics and Technology (State University)
gab@pop3.mipt.ru nina.pilipchuk@pop3.mipt.ru

Received April 10, 2003; in final form, March 4, 2004

Abstract—As is well known, a finite field $\mathbb{K}_n = GF(q^n)$ can be described in terms of $n \times n$ matrices A over the field $\mathbb{K} = GF(q)$ such that their powers A^i, $i = 1, 2, \ldots, q^n - 1$, correspond to all nonzero elements of the field. It is proved that, for fields $\mathbb{K}_n$ of characteristic 2, such a matrix A can be chosen to be symmetric. Several constructions of field-representing symmetric matrices are given. These matrices A^i together with the all-zero matrix can be considered as a $\mathbb{K}_n$-linear matrix code in the rank metric with maximum rank distance $d = n$ and maximum possible cardinality q^n. These codes are called *symmetric rank codes*. In the vector representation, such codes are maximum rank distance (MRD) linear $[n, 1, n]$ codes, which allows one to use known rank-error-correcting algorithms. For symmetric codes, an algorithm of erasure symmetrization is proposed, which considerably reduces the decoding complexity as compared with standard algorithms.

It is also shown that a linear $[n, k, d = n-k+1]$ MRD code $\mathcal{V}_k$ containing the above-mentioned one-dimensional symmetric code as a subcode has the following property: the corresponding transposed code is also $\mathbb{K}_n$-linear. Such codes have an extended capability of correcting *symmetric* errors and erasures.

1. INTRODUCTION

Codes in the rank metric, introduced in [1], can be described in two alternative ways: either as *matrix* or *vector* codes. Let $\mathbb{K}$ be a field of q elements, and let $\mathbb{K}_n$ be its extension field of degree n.

In the *matrix* representation, we consider the normed ring $M_n(\mathbb{K})$ of $n \times n$ matrices over the *ground* field $\mathbb{K}$ (in the present paper, square matrices are only considered). The *norm* of a matrix G is its rank, $\operatorname{rank}(G)$, and the *rank distance* $d(G_1, G_2)$ between two matrices G_1 and G_2 is the rank of their difference: $d(G_1, G_2) = \operatorname{rank}(G_1 - G_2)$. Any subset of matrices $\mathcal{M} \subseteq M_n(\mathbb{K})$ is called a *matrix code*. The *code distance* $d(\mathcal{M}) = d$ is the minimum pairwise distance between matrices of the code: $d = \min\bigl(\operatorname{rank}(G_1 - G_2) : G_1, G_2 \in \mathcal{M};\ G_1 \neq G_2\bigr)$. A code is called $\mathbb{K}$-*linear* if a linear combination of two code matrices with coefficients in $\mathbb{K}$ is also a code matrix. For a given code $\mathcal{M}$, the *transposed* code $\mathcal{M}^T$ is defined as the code consisting of transposed matrices: $\mathcal{M}^T = \{G^T : G \in \mathcal{M}\}$. It is clear that the cardinalities and code distances of the codes $\mathcal{M}$ and $\mathcal{M}^T$ are the same. If $\mathcal{M}$ is a $\mathbb{K}$-*linear* code, then $\mathcal{M}^T$ is also $\mathbb{K}$-*linear*.

In the *vector* representation, we consider the normed space $\mathbb{K}_n^n$ of n-vectors over the extended field $\mathbb{K}_n$. The *norm*, or *rank*, of a vector $\boldsymbol{g} \in \mathbb{K}_n^n$ is defined to be the maximum number $r(\boldsymbol{g})$ of its coordinates that are linearly independent over the ground field $\mathbb{K}$. The *rank distance* $d(\boldsymbol{g}_1, \boldsymbol{g}_2)$ between two vectors $\boldsymbol{g}_1$ and $\boldsymbol{g}_2$ is the norm of their difference: $d(\boldsymbol{g}_1, \boldsymbol{g}_2) = r(\boldsymbol{g}_1 - \boldsymbol{g}_2)$. Any subset of vectors $\mathcal{V} \subseteq \mathbb{K}_n^n$ is called a *vector code*. the *code distance* $d(\mathcal{V}) = d$ is the minimum pairwise distance between code vectors: $d = \min(r(\boldsymbol{g}_1 - \boldsymbol{g}_2) : \boldsymbol{g}_1, \boldsymbol{g}_2 \in \mathcal{V};\ \boldsymbol{g}_1 \neq \boldsymbol{g}_2)$. A code $\mathcal{V}$ is said to be $\mathbb{K}$-*linear* if a linear combination of two code vectors with coefficients in $\mathbb{K}$ is also a code vector. A code $\mathcal{V}$ is said to be $\mathbb{K}_n$-*linear* if a linear combination of two code vectors with coefficients in $\mathbb{K}_n$ is also a code vector, or, in other words, if $\mathcal{V}$ is a linear subspace of $\mathbb{K}_n^n$. Note that $\mathbb{K}$-linearity follows from

0032-9460/04/4002-0103 © 2004 MAIK “Nauka/Interperiodica”

$\mathbb{K}_n$-linearity; however, the converse is not true. It is shown in [1] that for $k = 1, 2, \ldots, n$ there exist linear $[n, k, d]$ codes with maximum possible rank distance $d = n - k + 1$ (MRD codes). They are k-dimensional subspaces of $\mathbb{K}_n^n$.

Let $\Omega = \{\omega_1, \omega_2, \ldots, \omega_n\}$ be a basis of $\mathbb{K}_n$ over $\mathbb{K}$. Let $\theta^{-1}\colon \mathbb{K}_n \Rightarrow \mathbb{K}^n$ be an isomorphism between the field $\mathbb{K}_n$ and the space of vector columns $\mathbb{K}^n$ over $\mathbb{K}$. Elements of the basis are mapped into linearly independent columns $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n \in \mathbb{K}^n$, where $\boldsymbol{b}_j = \theta^{-1}(\omega_j)$, $j = 1, 2, \ldots, n$.

Let $\theta\colon \mathbb{K}^n \Rightarrow \mathbb{K}_n$ be the inverse mapping: $\theta(\boldsymbol{b}) = \beta$. If we apply it to every column of a matrix $M \in M_n(\mathbb{K})$, we get a one-to-one mapping $\Theta\colon M_n(\mathbb{K}) \Rightarrow \mathbb{K}_n^n$ of the space of $n \times n$ matrices over $\mathbb{K}$ onto the space of n-vectors over $\mathbb{K}_n$. For the mapping $\Theta(M) = \boldsymbol{g}$ it is clear that the rank of the matrix M coincides with the rank of the vector $\boldsymbol{g}$, i.e., $\operatorname{rank}(M) = r(\boldsymbol{g})$.

The mapping Θ is isometric. Given a matrix code $\mathcal{M}$, it allows one to construct a vector code according to the rule $\mathcal{V} = \Theta(\mathcal{M})$. Conversely, given a vector code $\mathcal{V}$, one can construct a matrix code with the same metric properties using the rule $\mathcal{M} = \Theta^{-1}(\mathcal{V})$.

The vector representation is more useful for for the description of constructions of rank codes and their decoding algorithms (see, for example, [1]). The matrix representation is useful in code modulation theory, for example, in the theory of space-time codes [3].

Given a rank code, one can construct a new code with the same cardinality and code distance using the following procedure. For instance, let us be given a vector code $\mathcal{V}$, two mappings θ and $\widetilde{\theta}$, and the associated mappings Θ and $\widetilde{\Theta}$. Let us construct a new code $\mathcal{V}^T$ using the chain of mappings

$$\mathcal{V} \xrightarrow{\Theta^{-1}} \mathcal{M} \longrightarrow \mathcal{M}^T \xrightarrow{\widetilde{\Theta}} \mathcal{V}^{\mathcal{T}}. \tag{1}$$

The obtained code $\mathcal{V}^T$ is called the *transposed vector code*. It should be noted that the mappings θ and $\widetilde{\theta}$ can be different.

The codes $\mathcal{V}^T$ and $\mathcal{V}$ have the same cardinality and the same rank weight distribution. However, if $\mathcal{V}$ is $\mathbb{K}_n$-linear (say, is an $[n, k, d = n - k + 1]$ MRD code), the code $\mathcal{V}^T$ is not necessarily $\mathbb{K}_n$-linear, though it is always $\mathbb{K}$-linear. This is a drawback of the construction since no direct fast decoding algorithms for such codes are known. Of course, it is possible to convert a distorted code vector $\boldsymbol{y} = \boldsymbol{w} + \boldsymbol{e}$, $\boldsymbol{w} \in \mathcal{V}^T$, into a distorted vector $\boldsymbol{z} = \boldsymbol{v} + \widetilde{\boldsymbol{e}}$, $\boldsymbol{v} \in \mathcal{V}$, by means of (1) and then use a standard algorithm for $\mathcal{V}$. However, in this case the question arises of why at all we should use the code $\mathcal{V}^T$. Another drawback of a code which is only $\mathbb{K}$-linear is a larger size of the generator matrix.

Let us illustrate this by the following example.

Example 1. Let $q = 2$. As $\mathcal{V}$, choose the following one-dimensional $\mathbb{K}_3$-linear $[n, 1, n]$ code:

$$\mathcal{V} = \Big\{(0,0,0),\ (1,\alpha,\alpha^2),\ (\alpha,\alpha^2,\alpha^3),\ (\alpha^2,\alpha^3,\alpha^4),\ (\alpha^3,\alpha^4,\alpha^5),\ (\alpha^4,\alpha^5,\alpha^6),\ (\alpha^5,\alpha^6,1),\ (\alpha^6,1,\alpha)\Big\},$$

where α is a root of the irreducible polynomial $f(\lambda) = \lambda^3 + \lambda^2 + 1$. The generator matrix of this code consists of one row: $\boldsymbol{G} = (1, \alpha, \alpha^2)$. Information vectors are one-dimensional: $\boldsymbol{u} = (u)$, $u \in GF(2^3)$. Code vectors are given by $\boldsymbol{v} = \boldsymbol{u}\boldsymbol{G} = (u, u\alpha, u\alpha^2)$.

Let θ^{-1} be defined by $1 \leftrightarrow (1,0,0)^T$, $\alpha \leftrightarrow (0,1,0)^T$, and $\alpha^2 \leftrightarrow (0,0,1)^T$. Then the corresponding matrix code $\mathcal{M}$ is the following set of 3×3 matrices:

$$M_0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad M_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad M_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \qquad M_3 = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix},$$

$$M_4 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \qquad M_5 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \qquad M_6 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \qquad M_7 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

If we transpose these matrices and convert them into vectors by means of the map θ, we obtain the code

$$\mathcal{V}^T = \Big\{(0,0,0),\ (1,\alpha,\alpha^2),\ (\alpha^2,1,\alpha^6),\ (\alpha^6,\alpha^2,\alpha^4),\ (\alpha^4,\alpha^6,\alpha^3),\ (\alpha^5,\alpha^4,\alpha^3),\ (\alpha^3,\alpha^5,\alpha),\ (\alpha,\alpha^3,1)\Big\},$$

which is $\mathbb{K}$-linear but *is not* a linear subspace, i.e., is not $\mathbb{K}_3$-linear. The generator matrix of the transposed code is

$$\boldsymbol{G} = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ \alpha^2 & 1 & \alpha^6 \\ \alpha^6 & \alpha^2 & \alpha^4 \end{pmatrix},$$

information vectors are $\boldsymbol{u} = (u_1, u_2, u_3)$, $u_1, u_2, u_3 \in GF(2)$, and code vectors are given by $\boldsymbol{w} = \boldsymbol{u}\boldsymbol{G} = (u_1 + u_2\alpha^2 + u_3\alpha^6,\ u_1\alpha + u_2 + u_3\alpha^2,\ u_1\alpha^2 + u_2\alpha^6 + u_3\alpha^4)$.

Problem statement. Let a $\mathbb{K}_n$-linear $[n,k,d=n-k+1]$ MRD vector code $\mathcal{V}$ be given. Find mappings Θ and $\widetilde{\Theta}$ (if exist) such that the transposed vector code $\mathcal{V}^T$ is also a $\mathbb{K}_n$-linear $[n,k,d=n-k+1]$ MRD code.

In this paper we give an answer for the particular case of one-dimensional $[n,1,d=n]$ MRD codes and fields $\mathbb{K}_n$ of characteristic 2, i.e., $q = 2^r$. As is easily seen from relation (1), if the set $\mathcal{M}$ consists of *symmetric* matrices, then $\mathcal{M} = \mathcal{M}^T$, and for $\Theta = \widetilde{\Theta}$ we obtain $\mathcal{V} = \mathcal{V}^T$. A linear $[n,1,d=n]$ MRD code $\mathcal{V}$ can be defined by a generator matrix consisting of one row:

$$\boldsymbol{G} = (g_1, g_2, \ldots, g_n),$$

where the coordinates $g_j \in \mathbb{K}_n$, $j = 1,2,\ldots,n$, are linearly independent over $\mathbb{K}$. In this case, the vector code $\mathcal{V}$ consists of the all-zero code vector $\mathbf{0}$ and vectors of the form $\alpha^s\boldsymbol{G}$, $j = 0,1,\ldots,q^n-2$. We prove that there exist a generator row $\boldsymbol{G}$ and a map Θ such that $\Theta^{-1}(\alpha^s\boldsymbol{G}) = A^s$, where A is a symmetric matrix.

Moreover, we prove that a linear $[n,k,d=n-k+1]$ MRD code $\mathcal{V}_k$ containing the above-mentioned one-dimensional symmetric code as a subcode has the following property: the transposed vector code $\mathcal{V}_k^T$ is also $\mathbb{K}_n$-linear. Such codes have an extended capability of correcting *symmetric* errors and erasures.

2. MATRIX AND VECTOR REPRESENTATIONS OF AN EXTENDED FINITE FIELD

Consider a matrix $A \in M_n(\mathbb{K})$.

Definition 1. A matrix A *represents* the field $\mathbb{K}_n$ if and only if the polynomial algebra $\mathbb{K}[A]$ is isomorphic to $\mathbb{K}_n$.

A representation of $\mathbb{K}_n$ by a matrix A is said to be *primitive* if all matrices A^s, $s = 1,2,\ldots,q^n-1$, are different.

Primitive representations are characterized by the following lemma.

Lemma 1. *A representation of $\mathbb{K}_n$ by A is primitive if and only if its characteristic polynomial* $\det(\lambda I_n - A)$ *coincides with a primitive*[1] *polynomial $f(\lambda)$ of degree n over $\mathbb{K}$*

$$f(\lambda) = \lambda^n + f_{n-1}\lambda^{n-1} + f_{n-3}\lambda^{n-2} + \ldots + f_1\lambda^1 + f_0. \tag{2}$$

Proof. Let $\det(\lambda I_n - A) = f(\lambda)$. Then $f(A) = 0_n$, where 0_n denotes the all-zero $n \times n$ matrix. Since the polynomial $f(\lambda)$ divides $\lambda^{q^n-1} - 1$ but does not divide the binomials $\lambda^s - 1$, $1 \le s \le q^n - 2$,

[1] A polynomial $f(\lambda)$ of degree n irreducible over $\mathbb{K}$ is called primitive if $f(\lambda)$ divides the binomial $\lambda^{q^n-1} - 1$ but does not divide the binomials $\lambda^s - 1$, $1 \le s \le q^n - 2$.

we have $A^{q^n-1} = I_n$, and all the matrices A^s, $s = 1, 2, \ldots, q^n - 1$, are different. Moreover, each matrix A^s can be represented as a linear combination of the matrices $I_n, A, A^2, \ldots, A^{n-1}$ using the relation $A^n = -f_{n-1}A^{n-1} - f_{n-2}A^{n-2} - \ldots - f_1A - f_0I_n$. Hence, the algebra $\mathbb{K}[A]$ of matrix polynomials is isomorphic to the field $\mathbb{K}_n = \mathbb{K}(\alpha)$ formed by the adjunction of a root α of the primitive polynomial $f(\lambda)$. Therefore, the matrix A represents the field $\mathbb{K}_n$, and this representation is primitive.

Conversely, let a matrix A represent the field $\mathbb{K}_n$ primitively. Then the minimal polynomials of A and α are identical and coincide with a primitive polynomial $f(\lambda)$. Since the minimal polynomial divides the characteristic polynomial and has the same degree and leading coefficient, we have $\det(\lambda I_n - A) = f(\lambda)$. △

Corollary 1. *All matrices A representing a field are similar to the matrix*

$$C = \begin{pmatrix} 0 & 0 & \ldots & 0 & -f_0 \\ 1 & 0 & \ldots & 0 & -f_1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & -f_{n-2} \\ 0 & 0 & \ldots & 1 & -f_{n-1} \end{pmatrix},$$

i.e., $A = QCQ^{-1}$, where $Q \in M_n(\mathbb{K})$ is a nonsingular matrix and $f_0, f_1, \ldots, f_{n-1}$ are the coefficients of a reduced primitive polynomial $f(\lambda) = \lambda^n + f_{n-1}\lambda^{n-1} + f_{n-3}\lambda^{n-2} + \ldots + f_1\lambda^1 + f_0$.

Proof. Characteristic polynomials of similar matrices are identical. Note that $\det(\lambda I_n - C) = \lambda^n + f_{n-1}\lambda^{n-1} + f_{n-2}\lambda^{n-2} + \ldots + f_1\lambda^1 + f_0 = f(\lambda)$. Let A be an $n \times n$ matrix with the characteristic polynomial $\det(\lambda I_n - A) = f(\lambda)$. Since $f(\lambda)$ is a primitive polynomial, the sets of invariant polynomials (for definitions and properties, see [2]) of the matrices $\lambda I_n - A$ and $\lambda I_n - C$ coincide and consist of the polynomials $f(\lambda), 1, \ldots, 1$. Hence, by the necessary and sufficient criterion of similarity (see [2]), the matrix A is similar to C, or $A = QCQ^{-1}$, where Q is a nonsingular matrix with entries in the ground field $\mathbb{K}$. △

Denote by $M[j]$ the jth column of the matrix M. Let A be a matrix which primitively represents the field $\mathbb{K}_n$. Define the *induced* vector representation of $\mathbb{K}_n$ by the relation

$$\begin{aligned} \theta^{-1}(0) &= 0_n[1], & \theta(0_n[1]) &= 0, \\ \theta^{-1}(\alpha^s) &= A^s[1], & \theta(A^s[1]) &= \alpha^s, \quad s = 0, 1, \ldots, q^n - 2. \end{aligned} \tag{3}$$

This map is well defined for any n-column since a nonzero column $\boldsymbol{b}$ is equal to $A^s[1]$ for some s, and the zero column is equal to $0_n[1]$.

We call this representation *associated* with the matrix A.

Lemma 2. *Let $c \in \mathbb{K}_n$. Then*

$$\theta^{-1}(\alpha c) = A\theta^{-1}(c).$$

Proof. Since $c = \alpha^s$ for some s, we have $\theta^{-1}(\alpha c) = \theta^{-1}(\alpha^{1+s}) = A^{1+s}[1] = AA^s[1] = A\theta^{-1}(c)$. △

For a vector $\boldsymbol{c} = (c_1, c_2, \ldots, c_n) \in \mathbb{K}_n^n$, put

$$\Theta^{-1}(\boldsymbol{c}) = (\theta^{-1}(c_1), \theta^{-1}(c_2), \ldots, \theta^{-1}(c_n)). \tag{4}$$

Thus, $\Theta^{-1}(\boldsymbol{c}) = M$ is an $n \times n$ matrix over $\mathbb{K}$.

It is clear that

$$\Theta^{-1}(\alpha\boldsymbol{c}) = A\Theta^{-1}(\boldsymbol{c}) = AM$$

and, in the general case,

$$\Theta^{-1}(\alpha^s \boldsymbol{c}) = A^s\Theta^{-1}(\boldsymbol{c}) = A^s M, \quad s = 1, 2, \ldots. \tag{5}$$

Conversely,

$$\Theta(A^s M) = \alpha^s \Theta(M) = \alpha^s \boldsymbol{c}.$$

Furthermore, if $\boldsymbol{c} \in \mathbb{K}_n^n$ and R is an $n \times m$ matrix over $\mathbb{K}$, then

$$\Theta^{-1}(\boldsymbol{c}R) = \Theta^{-1}(\boldsymbol{c})R = MR.$$

3. SYMMETRIC MATRICES REPRESENTING A FIELD

Let us show that, if $\mathbb{K}_n$ is a field of characteristic 2, a matrix A representing the field can be chosen to be symmetric.[2] The first symmetric construction was proposed in [4]. It used $2n-1$ free parameters. Here we describe a simpler construction, containing only n free parameters.

3.1. Auxiliary Matrices and Determinants

All operations are performed in the field $\mathbb{K}$. Let $D_n(\lambda)$ be the three-diagonal $n \times n$ matrix where all elements on the main diagonal equal λ and all elements on the neighboring upper and low diagonals equal 1:

$$D_n(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \ldots & 0 & 0 & 0 \\ 1 & \lambda & 1 & \ldots & 0 & 0 & 0 \\ 0 & 1 & \lambda & \ldots & 0 & 0 & 0 \\ \multicolumn{7}{c}{\dotfill} \\ 0 & 0 & 0 & \ldots & \lambda & 1 & 0 \\ 0 & 0 & 0 & \ldots & 1 & \lambda & 1 \\ 0 & 0 & 0 & \ldots & 0 & 1 & \lambda \end{pmatrix}.$$

Denote by $d_n(\lambda)$ the determinant of this matrix.

Let $H_n(\lambda)$ be the three-diagonal $n \times n$ matrix where all elements on the main diagonal except for the last one equal λ and the last element is $\lambda + 1$. All elements on the neighboring upper and low diagonals equal 1:

$$H_n(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \ldots & 0 & 0 & 0 \\ 1 & \lambda & 1 & \ldots & 0 & 0 & 0 \\ 0 & 1 & \lambda & \ldots & 0 & 0 & 0 \\ \multicolumn{7}{c}{\dotfill} \\ 0 & 0 & 0 & \ldots & \lambda & 1 & 0 \\ 0 & 0 & 0 & \ldots & 1 & \lambda & 1 \\ 0 & 0 & 0 & \ldots & 0 & 1 & \lambda+1 \end{pmatrix}.$$

Denote by $h_n(\lambda)$ the determinant of this matrix.

By the definition, put $d_{-1}(\lambda) = 0$, $d_0(\lambda) = 1$, $h_{-1}(\lambda) = 1$, and $h_0(\lambda) = 1$. It is easily seen that $d_1(\lambda) = \lambda$ and $h_1(\lambda) = \lambda + 1$.

[2] Examples show that for $n = 2, 3$ there exist symmetric matrices representing a field for an arbitrary characteristic p. For instance, the matrix $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ represents the field $GF(3^2)$. However, we do not know whether symmetric matrices representing $\mathbb{K}_n$ exist for arbitrary n. For some fields of characteristic 0, for example, for $\mathbb{C}$, representation by symmetric matrices is impossible.

Then the determinants $d_n(\lambda)$ and $h_n(\lambda)$ can be calculated recursively:

$$\begin{aligned} d_n(\lambda) &= d_1(\lambda)d_{n-1}(\lambda) + d_{n-2}(\lambda), \quad n \ge 2, \\ h_n(\lambda) &= d_1(\lambda)h_{n-1}(\lambda) + h_{n-2}(\lambda), \quad n \ge 2. \end{aligned} \tag{6}$$

Moreover, repeating equations (6), we obtain for $s \ge 1$ the relations

$$\begin{aligned} d_n(\lambda) &= d_s(\lambda)d_{n-s}(\lambda) + d_{s-1}(\lambda)d_{n-s-1}(\lambda), \quad n \ge 2, \\ h_n(\lambda) &= d_s(\lambda)h_{n-s}(\lambda) + d_{s-1}(\lambda)h_{n-s-1}(\lambda), \quad n \ge 2. \end{aligned} \tag{7}$$

3.2. Main Construction

First, we prove the general result on the existence of symmetric matrices with a prescribed characteristic polynomial.

Theorem 1. *Let*

$$g(\lambda) = \lambda^n + g_{n-1}\lambda^{n-1} + g_{n-3}\lambda^{n-2} + \ldots + g_1\lambda^1 + g_0 \tag{8}$$

be an arbitrary monic polynomial of degree n over $\mathbb{K}$.

There exists a symmetric matrix $A \in M_n(\mathbb{K})$ for which $g(\lambda)$ is the characteristic polynomial.

Proof. All elements of a binary field are squares. Choose elements a_{n-1}, $a_{n-2} = b_{n-2}^2$, $a_{n-3} = b_{n-3}^2$, ..., $a_0 = b_0^2 \in \mathbb{K}$. Let $\boldsymbol{b} = (b_{n-2}, b_{n-3}, \ldots, b_0)$. Consider the bordered symmetric matrix of the following form:

$$A = \begin{pmatrix} a_{n-1} & \boldsymbol{b} \\ \boldsymbol{b}^T & H_{n-1}(0) \end{pmatrix} = \begin{pmatrix} a_{n-1} & b_{n-2} & b_{n-3} & b_{n-4} & \ldots & b_2 & b_1 & b_0 \\ b_{n-2} & 0 & 1 & 0 & \ldots & 0 & 0 & 0 \\ b_{n-3} & 1 & 0 & 1 & \ldots & 0 & 0 & 0 \\ b_{n-4} & 0 & 1 & 0 & \ldots & 0 & 0 & 0 \\ \hdotsfor{8} \\ b_2 & 0 & 0 & 0 & \ldots & 0 & 1 & 0 \\ b_1 & 0 & 0 & 0 & \ldots & 1 & 0 & 1 \\ b_0 & 0 & 0 & 0 & \ldots & 0 & 1 & 1 \end{pmatrix}. \tag{9}$$

Calculate the characteristic polynomial

$$\chi_n(\lambda) = \det(\lambda I_n + A) = \det \begin{pmatrix} \lambda + a_{n-1} & \boldsymbol{b} \\ \boldsymbol{b}^T & H_{n-1}(\lambda) \end{pmatrix}$$

$$= \det \begin{pmatrix} \lambda + a_{n-1} & b_{n-2} & b_{n-3} & b_{n-4} & \ldots & b_2 & b_1 & b_0 \\ b_{n-2} & \lambda & 1 & 0 & \ldots & 0 & 0 & 0 \\ b_{n-3} & 1 & \lambda & 1 & \ldots & 0 & 0 & 0 \\ b_{n-4} & 0 & 1 & \lambda & \ldots & 0 & 0 & 0 \\ \hdotsfor{8} \\ b_2 & 0 & 0 & 0 & \ldots & \lambda & 1 & 0 \\ b_1 & 0 & 0 & 0 & \ldots & 1 & \lambda & 1 \\ b_0 & 0 & 0 & 0 & \ldots & 0 & 1 & \lambda + 1 \end{pmatrix}.$$

Expanding the determinant by the first row, then expanding the obtained determinants by the first column, and collecting similar terms, we obtain the relation

$$\begin{aligned} \chi_n(\lambda) &= (\lambda + a_{n-1})h_{n-1}(\lambda) + b_{n-2}^2 h_{n-2}(\lambda) \\ &\quad + b_{n-3}^2 d_1(\lambda)h_{n-3}(\lambda) + \ldots + b_1^2 d_{n-3}(\lambda)h_1(\lambda) + b_0^2 d_{n-2}(\lambda) \\ &= (\lambda + a_{n-1})h_{n-1}(\lambda) + a_{n-2}h_{n-2}(\lambda) \\ &\quad + a_{n-3}d_1(\lambda)h_{n-3}(\lambda) + \ldots + a_1 d_{n-3}(\lambda)h_1(\lambda) + a_0 d_{n-2}(\lambda), \end{aligned} \tag{10}$$

where the polynomials $h_i(\lambda)$ and $d_i(\lambda)$ are defined by equations (6).

Equation (10) can be interpreted as the statement that the characteristic polynomial $\chi_n(\lambda)$ is a linear combination of the polynomials

$$(\lambda h_{n-1}(\lambda), h_{n-1}(\lambda), h_{n-2}(\lambda), d_1(\lambda)h_{n-3}(\lambda), \ldots, d_{n-3}(\lambda)h_1(\lambda), d_{n-2}(\lambda)) \tag{11}$$

with the coefficients $(1, a_{n-1}, a_{n-2}, \ldots, a_1, a_0)$.

Let us show that polynomials (11) are linearly independent over $\mathbb{K}$. The polynomial $\lambda h_{n-1}(\lambda)$ is of degree n, the polynomial $h_{n-1}(\lambda)$ is of degree $n-1$, and the other polynomials

$$(h_{n-2}(\lambda), d_1(\lambda)h_{n-3}(\lambda), \ldots, d_{n-3}(\lambda)h_1(\lambda), d_{n-2}(\lambda)) \tag{12}$$

are of degree $n-2$. It suffices to prove that polynomials (12) are linearly independent. Add the polynomial $h_{n-2}(\lambda)$ of system (12) to all the other polynomials $d_s(\lambda)h_{n-2-s}(\lambda)$, $s = 1, 2, \ldots, n-2$. Using relation (7), we obtain

$$h_{n-2}(\lambda) + d_s(\lambda)h_{n-2-s}(\lambda) = d_{s-1}(\lambda)h_{n-3-s}(\lambda),$$

where the degrees of the polynomials $d_{s-1}(\lambda)h_{n-3-s}(\lambda)$ equal $n-4$. As a result, system (12) is transformed into the system

$$(h_{n-2}(\lambda), h_{n-4}(\lambda), d_1(\lambda)h_{n-5}(\lambda), \ldots, d_{n-5}(\lambda)h_1(\lambda), d_{n-4}(\lambda), d_{n-3}(\lambda)). \tag{13}$$

The first polynomial in (13) is of degree $n-2$, the last polynomial is of degree $n-3$, and the other polynomials are of degree $n-4$ and have the same form as (12). Iteratively continuing this procedure, we reduce system (12) to the system

$$\begin{aligned}
&(h_{n-2}(\lambda), h_{n-4}(\lambda), h_{n-6}(\lambda), \ldots, h_2(\lambda), h_0(\lambda), d_1(\lambda), d_3(\lambda), \ldots, d_{n-3}(\lambda)), \quad n \text{ even},\\
&(h_{n-2}(\lambda), h_{n-4}(\lambda), h_{n-6}(\lambda), \ldots, h_1(\lambda), d_0(\lambda), d_2(\lambda), d_4(\lambda), \ldots, d_{n-3}(\lambda)), \quad n \text{ odd}.
\end{aligned}$$

All polynomials of this system have different degrees. Therefore, they are linearly independent over $\mathbb{K}$. △

Hence, there exists a nonsingular matrix $L_n \in M_n(\mathbb{K})$ such that

$$(\lambda h_{n-1}(\lambda), h_{n-1}(\lambda), h_{n-2}(\lambda), d_1(\lambda)h_{n-3}(\lambda), \ldots, d_{n-3}(\lambda)h_1(\lambda), d_{n-2}(\lambda))^T = L_n(\lambda^n, \lambda^{n-1}, \lambda^{n-2}, \ldots, \lambda, 1)^T. \tag{14}$$

Rows of the matrix L_n consist of the coefficients of the corresponding polynomials from the left-hand side of (14).

Thus, if polynomial (8) is given, elements of symmetric matrix (9) for which this polynomial is characteristic can be obtained from the equation

$$(1, a_{n-1}, a_{n-2}, \ldots, a_1, a_0) = (1, g_{n-1}, g_{n-2}, \ldots, g_1, g_0)L_n^{-1}$$

by taking square roots of a_s, $s = 1, 2, \ldots, n-1$.

In particular, if polynomial (8) coincides with primitive polynomial (2), then the matrix A represents the field $\mathbb{K}_n$.

Example 2. Let $q = 4$, $\mathbb{K} = GF(4)$, $n = 2$, $\mathbb{K}_2 = GF(q^2) = GF(16)$. Let β be a primitive element of $\mathbb{K}$, i.e., $\beta^2 + \beta + 1 = 0$. The polynomial $f(\lambda) = \lambda^2 + \lambda(\beta + 1) + (\beta + 1)$ is irreducible over $\mathbb{K}$ and primitive. The symmetric matrix

$$A = \begin{pmatrix} \beta & \beta \\ \beta & 1 \end{pmatrix}$$

represents the field $\mathbb{K}_2 = GF(q^2) = GF(16)$ because its characteristic polynomial is $f(\lambda)$.

Example 3. Let $q = 2$, $\mathbb{K} = GF(2)$, $n = 4$, $\mathbb{K}_4 = GF(2^4) = GF(16)$. The polynomial $f(\lambda) = \lambda^4 + \lambda^3 + 1$ is irreducible over $\mathbb{K}$ and primitive. The symmetric matrix

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

represents the field $\mathbb{K}_4 = GF(2^4) = GF(16)$ because its characteristic polynomial is $f(\lambda)$.

3.3. Other Constructions

Let $n = ms$. Then the field $\mathbb{K}_n$ can be defined by a primitive polynomial of degree s over $\mathbb{K}_m$. Let β be a primitive element of $\mathbb{K}_m$. Let a symmetric $s \times s$ matrix $A(a_{ij}) \in M_s(\mathbb{K}_m)$ represent $\mathbb{K}_n$. Its element a_{ij} is either zero or a power of β: $a_{ij} = \beta^{k_{ij}}$.

In turn, let a symmetric $m \times m$ matrix $B \in M_m(\mathbb{K})$ represent the field $\mathbb{K}_m$. If we replace each element a_{ij} of A by either the all-zero matrix 0_m or the corresponding symmetric matrix $B^{k_{ij}}$, we obtain a symmetric matrix D of size $ms = n$ with elements in $\mathbb{K}$. The characteristic polynomial of this matrix is irreducible. If, in addition, it is primitive, then the $n \times n$ matrix D represents $\mathbb{K}_n$. Otherwise, we should find a linear combination of powers of the matrix D with a primitive characteristic polynomial.

Example 4. The matrix $B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ represents the field $GF(4)$. Let us replace elements β of the matrix from Example 2 with the matrix B and replace the element 1 by I_2:

$$A = \begin{pmatrix} \beta & \beta \\ \beta & 1 \end{pmatrix} \longrightarrow D = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

The characteristic polynomial of D is the primitive polynomial $\lambda^4 + \lambda + 1$, so D represents the field $GF(16)$ primitively.

4. RANK METRIC CODES CONSISTING OF SYMMETRIC MATRICES

Let a symmetric matrix $A \in M_n(\mathbb{K})$ represent the field $\mathbb{K}_n$. Consider the matrix code $\mathcal{M}$ consisting of q^n matrices:

$$\mathcal{M} = \left\{0_n, I_n, A, A^2, \ldots, A^{q^n-2}\right\}. \qquad (15)$$

Lemma 3. *The code $\mathcal{M}$ is $\mathbb{K}$-linear with maximum rank distance $d = n$.*

Proof. Since A represents $\mathbb{K}_n$, we see that a $\mathbb{K}$-linear combination of matrices from $\mathcal{M}$ is also a matrix belonging to $\mathcal{M}$. In addition, the difference of any two distinct matrices from $\mathcal{M}$ is a nonzero matrix from $\mathcal{M}$ and hence is of rank n. The cardinality of the code $\mathcal{M}$ is maximum possible for the distance $d = n$. Indeed, for any matrix code of cardinality greater than q^n there exists a pair of matrices such that their difference contains a zero row; therefore, the distance between these matrices is strictly less than n. $\triangle$

Transform the matrix code $\mathcal{M}$ into the vector code $\mathcal{V}_1$ using field representation (3) compatible with the matrix A.

Lemma 4. *The vector code $\mathcal{V}_1$ is a $\mathbb{K}_n$-linear $[n, 1, n]$ MRD code.*

Proof. Choose the vector $\Theta(I_n)$ as a generator (row) matrix:

$$\boldsymbol{g}_0 = (g_1, g_2, \ldots, g_n) = \Theta(I_n). \tag{16}$$

This matrix generates a $\mathbb{K}_n$-linear $[n, 1, n]$ MRD code $\mathcal{V}_1$ consisting of the vectors

$$\mathbf{0},\ \boldsymbol{g}_0,\ \alpha\boldsymbol{g}_0,\ \alpha^2\boldsymbol{g}_0,\ \ldots,\ \alpha^{q^n-2}\boldsymbol{g}_0. \tag{17}$$

According to (5), we have $\Theta^{-1}(\alpha\boldsymbol{g}_0) = A\Theta^{-1}(\boldsymbol{g}_0) = AI_n = A$. Similarly, $\Theta^{-1}(\alpha^s\boldsymbol{g}_0) = A^s\Theta^{-1}(\boldsymbol{g}_0) = A^sI_n = A^s$, $s = 2, \ldots, q^n - 2$. This proves that vector linear code (17) is the inverse image of matrix code (15). △

It is clear that the transposed code $\mathcal{V}_1^T$ coincides with $\mathcal{V}_1$. Hence, it is also linear.

5. CORRECTION OF RANK ERASURES BY SYMMETRIC RANK CODES

It is convenient to define the concept of a rank erasure in terms of the matrix representation of an extension field. For general MRD codes, joint correction of rank errors and rank erasures was considered in [5].

In practical applications, a code vector is represented as a signal matrix, whose elements are transmitted through the channel. At the receiver end, hard decision about each element is made. Then the decision matrix is transformed into a vector for further algebraic decoding. A received matrix is of the form $Y = M + E$, where M is the code matrix and E is an error matrix. If $\mathrm{rank}(E) \le (d-1)/2$, then the algebraic decoder corrects the error [1].

Sometimes it is possible to evaluate the unreliability of each hard decision. Then, together with the matrix Y, a decoding algorithm can use the unreliability matrix Z, whose element z_{ij} is the unreliability of the element y_{ij} of the matrix Y. We consider the ideal situation where the unreliability matrix Z consists solely of zeros and ones. If an element of this matrix is 0, this means that the decision for the corresponding element of the matrix Y is right for sure. If an element of the matrix Z is 1, this means that the decision for the corresponding element of the matrix Y *could be* wrong. In this case, it is traditionally said about a symbol *erasure*, although, in fact, some decision about the symbol is made. The matrix E is called a *rank erasure*. At the receiver end, upon receiving the matrix Y and computing the matrix Z, we know the positions where there are no errors for sure. It is said that the matrix E is *compatible* with the unreliability matrix Z.

The rank of the matrix E is called the *rank of erasure*. Consider *all* matrices E compatible with Z. Let $r_{\max}(Z)$ denote the maximum possible rank of E. It is clear that the code with rank distance d corrects a rank erasure E compatible with Z if $r_{\max}(Z) \le d - 1$.

To evaluate $r_{\max}(Z)$, it is convenient to use the concept of the *term rank* of a matrix, introduced in combinatorial analysis (see, e.g., [6]).

The *term rank* of a matrix A (denoted by $\mathrm{termrank}(A)$) is defined to be the maximum possible number t of nonzero elements of the matrix that can be chosen in such a way that no two of them lie in the same line (row or column).

It follows from the definition that $\mathrm{rank}(E) \le \mathrm{termrank}(E)$. In turn, for any matrix E compatible with Z, we have the inequality $\mathrm{termrank}(E) \le \mathrm{termrank}(Z)$. Hence,

$$r_{\max}(Z) \le \mathrm{termrank}(Z).$$

Lemma 5 [6]. *The term rank of a $(0,1)$-matrix Z is equal to the minimum number t of lines (rows and columns) containing all nonzero elements of Z.*

The lemma implies the following equality.

Lemma 6. *We have* $r_{\max(Z)} = \operatorname{termrank}(Z)$.

Proof. Let t be the minimum number of lines containing all the erasures (possible errors). Let there be s rows and m columns among them, $s + m = t$. Then it is possible to choose s nonzero elements in s rows and m nonzero elements in m columns in such a way that no two of them lie in the same line. Otherwise, the term rank would be less than t. Let us choose the matrix E compatible with Z such that only the t positions mentioned above are nonzero. Then the algebraic rank of the matrix is t; i.e., $r_{\max}(Z) \geq \operatorname{termrank}(Z)$.

The inverse inequality obviously follows from the definition of the term rank. △

Consider correction of rank erasures by the code $\mathcal{V}_1$ defined in (15) and (16).

Introduce the notation $[j] = q^j$ if $j \geq 0$ and $[j] = q^{n+j}$ if $j < 0$. The expression $g^{[j]} = g^{q^j}$ is called the jth Frobenius power of an element g. In particular, $g^{[n]} = g^{q^n} = g$. The Frobenius power of a vector is defined componentwise.

For decoding, the parity-check matrix of the form

$$\boldsymbol{H}_{n-1} = \left(h_j^{[i]}\right), \quad i = 0, 1, \ldots, n-2, \quad j = 1, 2, \ldots, n,$$

is used such that $\boldsymbol{g}_0 \boldsymbol{H}_{n-1}^T = \mathbf{0}$.

Let $\boldsymbol{y} = \alpha^s \boldsymbol{g}_0 + \boldsymbol{e}$ be a received signal in the vector representation, where $\boldsymbol{e} = (e_1, e_2, \ldots, e_n)$ is the vector representation of a rank erasure E. Calculation of a syndrome leads to a system of $n-1$ equations over $\mathbb{K}_n$:

$$\sum_{j=1}^{n} e_j h_j^{[i]} = s_i, \quad i = 0, 1, \ldots, n-2.$$

Since the positions of possible errors in the matrix E are known, we can rewrite this system as a system of $n(n-1)$ linear equations over the ground field, where possible errors are unknowns. The number of unknowns depends on the matrix configuration of E. If an erasure is of rank $n-1$, and errors are located in $n-1$ rows (or $n-1$ columns), then the number of unknowns is maximal and equals $n(n-1)$. In this case, the complexity of solving the system is maximal. If the rank of erasure is $n-1$ and errors are located in $\lfloor n/2 \rfloor$ rows and $\lfloor (n-1)/2 \rfloor$ columns, where $\lfloor \cdot \rfloor$ denotes the integer part, then the number s of unknowns is $n(n-1) - \lfloor n/2 \rfloor \lfloor (n-1)/2 \rfloor$, which is approximately less by quarter. Thus, syndrome decoding of erasures is reduced to solving the system of $n(n-1)$ linear equations over $\mathbb{K}$ in $n(n-1)$ or less (in the general case) unknowns. The less the number of unknowns, the less is the complexity of solving the system.

For symmetric rank codes, the number of unknowns can considerably be reduced using a trick called the *symmetrization* procedure.

Let $Y = M + E$ be a received signal in the matrix representation, and let E be a rank erasure. We can get additional information about errors by calculating the matrix $Q = Y + Y^T = M + M^T + E + E^T$. Since for symmetric codes we have $M = M^T$, $M \in \mathcal{M}$, for *binary* fields we have $M + M^T = 0_n$. Therefore, we know the matrix

$$Q = Y + Y^T = E + E^T.$$

The unreliability matrix Z shows the zero entries of E. This allows one, by analyzing $E + E^T$, to directly find a part of errors and get additional information about the others.

Let us illustrate possible situations by examples.

Example 5. Let $n = 4$, $d = 4$, and let the unreliability matrix be of the form

$$Z = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

This means that the erasure matrix is of the form

$$E = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_5 & a_6 & a_7 & a_8 \\ 0 & 0 & 0 & a_9 \\ 0 & 0 & 0 & a_{10} \end{pmatrix},$$

and the maximum possible rank is $d-1=3$. In total, the matrix contains *ten* binary unknowns a_i at known positions. Then

$$Q = E + E^T = \begin{pmatrix} 0 & a_2+a_5 & a_3 & a_4 \\ a_5+a_2 & 0 & a_7 & a_8 \\ a_3 & a_7 & 0 & a_9 \\ a_4 & a_8 & a_9 & 0 \end{pmatrix}.$$

From this matrix, the errors a_3, a_4, a_7, a_8, and a_9 can immediately be found. Also, we obtain the sum $a_2+a_5=b$, where b is known. However, no information can be obtained about the "diagonal" errors a_1, a_6, and a_{10}.

Now, let us modify the received matrix Y by adding the upper triangular matrix with known values

$$R = \begin{pmatrix} 0 & b & a_3 & a_4 \\ 0 & 0 & a_7 & a_8 \\ 0 & 0 & 0 & a_9 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

As a result, we obtain the modified matrix

$$Y_{\mathrm{mod}} = Y + R = M + E + R = M + E_{\mathrm{mod}},$$

where

$$E_{\mathrm{mod}} = \begin{pmatrix} a_1 & a_5 & 0 & 0 \\ a_5 & a_6 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a_{10} \end{pmatrix}.$$

The modified erasure matrix is a *symmetric* matrix with only *four* binary unknowns located at known positions. This procedure is called the *symmetrization* of erasures.

The matrix Y_{mod} is used for syndrome decoding of erasures. The symmetrization reduced the number of unknowns from ten to four.

Remark 1. For the class of codes under consideration, any line (row or column) of a code matrix can be regarded as an information set. If, for each line, we *preliminarily* find the matrix for the computation of the other lines, the decoding procedure is considerably simplified if one of the lines of the received matrix is free of errors. In Example 5, symmetrization leads to the erasure matrix containing zero lines (the third column or third row), so we can avoid syndrome decoding.

In the general case, symmetrization makes the number of unknowns at least half as large.

Thus, for the case where the rank of erasure is $d-1=n-1$, and all errors are located in $n-1$ rows, symmetrization reduces the number of unknowns to $n(n-1)/2$, as compared with the initial $n(n-1)$ unknowns.

Let $n=2s+1$. If the rank of erasure is $n-1$, and all errors are located in the first s rows and last s columns, then symmetrization reduces the number of unknowns from the initial value $\dfrac{(3n^2-2n-1)}{4}$ to $\dfrac{(n^2-1)}{4}$, which is approximately a third.

6. RANK CODES BASED ON SYMMETRIC MATRICES

Consider a $\mathbb{K}_n$-linear $[n, k, d = n - k + 1]$ MRD code $\mathcal{V}_k$ with the generator matrix

$$\boldsymbol{G}_k = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[1]} & g_2^{[1]} & \cdots & g_n^{[1]} \\ \dots & \dots & \dots & \dots \\ g_1^{[k-1]} & g_2^{[k-1]} & \cdots & g_n^{[k-1]} \end{pmatrix}. \tag{18}$$

As the first row of this matrix, choose components of the vector $\boldsymbol{g}_0$ from equation (16).

A code $\mathcal{V}_k$ is said to be *based* on symmetric matrices if it contains a one-dimensional subcode $\mathcal{V}_1$ consisting of symmetric matrices.

Let the transposed code $\mathcal{V}_k^T$ be obtained by mappings Θ and Θ^{-1} defined in (3) and (4). We will show that the code $\mathcal{V}_k^T$ is also $\mathbb{K}_n$-linear and is based on symmetric matrices. Moreover, combined use of the codes $\mathcal{V}_k$ and $\mathcal{V}_k^T$ allows one to correct not only ordinary rank errors (or erasures) but also *symmetric* errors (erasures) beyond the bound $\lfloor (d-1)/2 \rfloor$.

6.1. Auxiliary Results

Denote by

$$\boldsymbol{g}_i = \left(g_1^{[i]}, g_2^{[i]}, \dots, g_n^{[i]}\right), \quad i = 0, 1, 2, \dots, n-1,$$

the successive Frobenius powers of a vector $\boldsymbol{g}_0 = (g_1, g_2, \dots, g_n)$. These vectors are linearly independent over $\mathbb{K}$.

Components of each of them form a basis of $\mathbb{K}_n$ over $\mathbb{K}$. Therefore, there exists a nondegenerate matrix $D \in M_n(\mathbb{K})$ such that $\boldsymbol{g}_1 = \boldsymbol{g}_0 D$. Hence it follows that $\boldsymbol{g}_i = \boldsymbol{g}_0 D^i$. Moreover, $D^i \neq I_n$ if $i \le n-1$, but $D^n = I_n$ since $\boldsymbol{g}_n = \boldsymbol{g}_0 D^n = (g_1^{[n]}, g_2^{[n]}, \dots, g_n^{[n]}) = (g_1, g_2, \dots, g_n) = \boldsymbol{g}_0$. The matrix representation of $\boldsymbol{g}_i$ is

$$G_i = \Theta^{-1}(\boldsymbol{g}_i) = D^i. \tag{19}$$

Lemma 7. *We have the relations*

$$\boldsymbol{g}_0 A = \alpha \boldsymbol{g}_0, \tag{20}$$

$$\boldsymbol{g}_1 A = \alpha^q \boldsymbol{g}_1, \tag{21}$$

$$DA = A^q D, \tag{22}$$

$$D^r A^s = A^{sq^r} D^r, \quad r = 0, 1, \dots, n-1, \quad s = 0, 1, \dots, q^n - 2. \tag{23}$$

Proof. To prove (20), apply the mapping Θ^{-1} to both sides: $\Theta^{-1}(\boldsymbol{g}_0 A) = \Theta^{-1}(\boldsymbol{g}_0) A = I_n A = A$. On the other hand, according to (5) we have $\Theta^{-1}(\alpha \boldsymbol{g}_0) = A\Theta^{-1}(\boldsymbol{g}_0) = A I_n = A$. Equality (21) follows from (20) by raising both sides of (20) to the first Frobenius power and taking into account the fact that $A \in M_n(\mathbb{K})$. Equality (22) follows from (21) by applying Θ to both sides of (21). Equality (23) follows from (22) by successively isolating the multipliers DA on the left-hand side of (23) and using equality (22). △

Lemma 8. *The matrices D and D^T are related by the equality*

$$D^T = A^m D^{n-1}, \tag{24}$$

where m is an integer.

Proof. Transpose the matrices in (22) and take into account that A is a symmetric matrix. Then $D^TA^q = AD^T$. Left multiply both sides of equation (22) by D^T. We obtain $D^TDA = D^TA^qD = AD^TD$. Hence it follows that the matrix D^TD commutes with A. Since all eigenvalues of the matrix A are different (in some extension), the matrix D^TD is necessarily a polynomial of A (see, e.g., [2]); hence, it is equal to some power m of A. △

6.2. Matrix Representation of the Code $\mathcal{V}_k$

The generator matrix of the code $\mathcal{V}_k$ consists of the first k vectors $\boldsymbol{g}_j$, $j = 0, 1, \ldots, k-1$. Let components of an information vector $\boldsymbol{u} = (u_0, u_1, \ldots, u_{k-1})$ be presented by powers of α, i.e., $\boldsymbol{u} = (\varepsilon_0\alpha^{s_0}, \varepsilon_1\alpha^{s_1}, \ldots, \varepsilon_{k-1}\alpha^{s_{k-1}})$. Here the coefficients ε_j are equal to zero if $u_j = 0$ and to 1 otherwise. Then the corresponding code vector is

$$\boldsymbol{g}(\boldsymbol{u}) = \sum_{j=0}^{k-1} \varepsilon_j \alpha^{s_j} \boldsymbol{g}_j.$$

Using (5) and (19), find the matrix representation of $\boldsymbol{g}(\boldsymbol{u})$:

$$M(\boldsymbol{u}) = \Theta^{-1}(\boldsymbol{g}(\boldsymbol{u})) = \sum_{j=0}^{k-1} \varepsilon_j A^{s_j} D^j. \tag{25}$$

The set of matrices $\mathcal{M} = \{M(\boldsymbol{u})\}$ for all information vectors $\boldsymbol{u}$ is the matrix representation of the code $\mathcal{V}_k$.

6.3. Matrix and Vector Representation of the Transposed Code

Let us find the transposed matrix code $\mathcal{M}^T = \{M(\boldsymbol{u})^T\}$:

$$M(\boldsymbol{u})^T = \sum_{j=0}^{k-1} \varepsilon_j (D^j)^T A^{s_j}.$$

Using equations (24) and (23) and changing the summation order, we obtain

$$M(\boldsymbol{u})^T = \sum_{i=n-k+1}^{n} \varepsilon_{n-i} A^{m_i} D^i,$$

where

$$m_i = s_{n-i}q^i + m(q^{i+1} + q^{i+2} + \ldots + q^n), \quad i = n-k+1, n-k+2, \ldots, n-1, \qquad m_n = s_0 q^n.$$

Now, using the mapping Θ, we obtain the vector representation of the transposed code:

$$\widetilde{\boldsymbol{g}}(\boldsymbol{u}) = \Theta(M(\boldsymbol{u})^T) = \sum_{i=n-k+1}^{n} \Theta(\varepsilon_{n-i} A^{m_i} D^i) = \sum_{i=n-k+1}^{n} \varepsilon_{n-i} \alpha^{m_i} \boldsymbol{g}_i. \tag{26}$$

Vector (26) can be interpreted as a code vector of a $\mathbb{K}_n$-linear $[n, k, d = n-k+1]$ MRD rank code $\mathcal{V}_k^T$ with the generator matrix

$$\widetilde{\boldsymbol{G}}_k = \begin{pmatrix} g_1^{[n-k+1]} & g_2^{[n-k+1]} & \cdots & g_n^{[n-k+1]} \\ g_1^{[n-k+2]} & g_2^{[n-k+2]} & \cdots & g_n^{[n-k+2]} \\ \cdots & \cdots & \cdots & \cdots \\ g_1^{[n]} & g_2^{[n]} & \cdots & g_n^{[n]} \end{pmatrix},$$

the corresponding information vector being $\widetilde{\boldsymbol{u}} = (\varepsilon_{k-1}\alpha^{m_0}, \varepsilon_{k-2}\alpha^{m_1}, \ldots, \varepsilon_0\alpha^{m_{k-1}})$. This code contains a one-dimensional subcode $\mathcal{V}_1$, which consists of symmetric matrices. It is defined by the last row of $\widetilde{\boldsymbol{G}}_k$.

Thus, it is proved that the transposed code $\mathcal{V}_k^T$ is also $\mathbb{K}_n$-linear and is based on symmetric matrices.

6.4. Combined Use of the Codes $\mathcal{V}_k$ and $\mathcal{V}_k^T$ for the Decoding

Let a parity-check matrix of $\mathcal{V}_k$ be written as

$$\boldsymbol{H}_{n-k} = \begin{pmatrix} h_1 & h_2 & \cdots & h_n \\ h_1^{[1]} & h_2^{[1]} & \cdots & h_n^{[1]} \\ h_1^{[2]} & h_2^{[2]} & \cdots & h_n^{[2]} \\ \cdots & \cdots & \cdots & \cdots \\ h_1^{[d-2]} & h_2^{[d-2]} & \cdots & h_n^{[d-2]} \end{pmatrix}. \tag{27}$$

One can show that the parity-check matrix of $\mathcal{V}_k^T$ can be written as

$$\widetilde{\boldsymbol{H}}_{n-k} = \begin{pmatrix} h_1^{[d]} & h_2^{[d]} & \cdots & h_n^{[d]} \\ h_1^{[d+1]} & h_2^{[d+1]} & \cdots & h_n^{[d+1]} \\ h_1^{[d+2]} & h_2^{[d+2]} & \cdots & h_n^{[d+2]} \\ \cdots & \cdots & \cdots & \cdots \\ h_1^{[2d-2]} & h_2^{[2d-2]} & \cdots & h_n^{[2d-2]} \end{pmatrix}. \tag{28}$$

First, consider *rank error correction*. Let the vector representation of a received signal be $\boldsymbol{y} = \boldsymbol{g}(\boldsymbol{u}) + \boldsymbol{e}$, where $\boldsymbol{e} = (e_1, e_2, \ldots, e_n)$ is the vector representation of an error. Let E be the matrix representation of this error.

For the transposed form of this representation, we have $\widetilde{\boldsymbol{y}} = \widetilde{\boldsymbol{g}(\widetilde{\boldsymbol{u}})} + \widetilde{\boldsymbol{e}}$, where $\widetilde{\boldsymbol{e}} = (\widetilde{e}_1, \widetilde{e}_2, \ldots, \widetilde{e}_n)$ is the error vector with the matrix representation of the error $\widetilde{E} = E^T$. For the decoding, we have to calculate two syndromes, $\boldsymbol{r} = \boldsymbol{y}\boldsymbol{H}_{n-k}^T = \boldsymbol{e}\boldsymbol{H}_{n-k}^T$ and $\widetilde{\boldsymbol{r}} = \widetilde{\boldsymbol{y}}\widetilde{\boldsymbol{H}}_{n-k}^T = \widetilde{\boldsymbol{e}}\widetilde{\boldsymbol{H}}_{n-k}^T$. Using both syndromes has no advantages as compared with the standard decoding if errors $\boldsymbol{e}$ of the general type are considered. In this case it suffices to have only one of the syndromes. If the rank of an error is not greater than $t = (d-1)/2$, then the error will be corrected given the syndrome $\boldsymbol{r}$.

However, for correction of errors of a special form, it may be useful to employ both syndromes. Such a class of errors is *symmetric* errors, whose matrix representations are symmetric matrices: $E = \widetilde{E} = E^T$, or, equivalently, $\boldsymbol{e} = \widetilde{\boldsymbol{e}}$. In this case, we use the combined syndrome

$$\boldsymbol{R} = (\boldsymbol{r}, \widetilde{\boldsymbol{r}}) = \left(\boldsymbol{e}\boldsymbol{H}_{n-k}^T, \widetilde{\boldsymbol{e}}\widetilde{\boldsymbol{H}}_{n-k}^T\right) = \left(\boldsymbol{e}\boldsymbol{H}_{n-k}^T, \boldsymbol{e}\widetilde{\boldsymbol{H}}_{n-k}^T\right). \tag{29}$$

The syndrome $\boldsymbol{R}$ can be considered as the syndrome of a code with the parity-check matrix consisting of *different* rows of *both* matrices (27) and (28). There are two cases, depending on the code rate.

1. Let $2d-2 < n$; i.e., $R = k/n > 1/2$. Then all rows of both matrices are different. The corresponding code can have distance up to $D = 2d-1$. Thus, using the syndrome $\boldsymbol{R}$, we can correct *many symmetric* errors of rank not greater than $(D-1)/2 = d-1$.
2. Let $2d-2 \geq n$; i.e., $R = k/n \leq 1/2$. Then the number of different rows in both matrices equals $n-1$. The corresponding code has distance $D = n$; so, using the syndrome $\boldsymbol{R}$, we can correct *all symmetric* errors of rank not greater than $(n-1)/2$.

Similar results are valid for correction of *symmetric rank erasures.* If $R = k/n > 1/2$, then, for some codes, using the syndrome $\boldsymbol{R}$ one can correct *many symmetric* erasures of rank not greater than $D-1 = 2d-2$. If $R = k/n \leq 1/2$, then, using the syndrome $\boldsymbol{R}$, one can correct *all symmetric* erasures of rank not greater than $n-1$.

7. CONCLUSION

It is shown that finite fields of characteristic 2 can be represented by symmetric matrices A.

The matrix code $\mathcal{M}$ consisting of powers of A and the zero matrix has the maximum possible distance ($d = n$) and cardinality ($|\mathcal{M}| = q^n$). The corresponding vector code is linear. For correction of rank erasures with the help of this code, a symmetrization procedure is proposed, which allows one to reduce the number of unknowns for syndrome decoding to a half or a third.

For a class of linear codes $\mathcal{V}_k$ based on symmetric matrices, it is shown that the corresponding transposed codes are also linear. Combined use of both codes in the decoding of *symmetric* errors makes the error-correction capacity of the code almost twice as large.

The authors are grateful to the reviewer, whose constructive remarks helped them to improve the paper.

REFERENCES

1. Gabidulin, E.M., Theory of Codes with Maximal Rank Distance, *Probl. Peredachi Inf.*, 1985, vol. 21, no. 1, pp. 3–16 [*Probl. Inf. Trans.* (Engl. Transl.), 1985, vol. 21, no. 1, pp. 1–12].
2. Gantmakher, F.R., *Teoriya matrits*, Moscow: Nauka, 1988, 4th ed. Translated under the title *The Theory of Matrices*, 2 vols., Providence: AMS Chelsea, 1998.
3. Gabidulin, E.M., Bossert, M., and Lusina, P., Space-Time Codes Based on Rank Codes, in *Proc. 2000 IEEE Int. Symp. on Information Theory, Sorrento, Italy*, p. 283.
4. Gabidulin, E.M. and Pilipchuk, N.I., Representation of a Finite Field by Symmetric Matrices and Applications, in *Proc. 8th Int. Workshop on Algebraic and Combinatorial Coding Theory, Tsarskoe Selo, Russia, 2002*, pp. 120–123.
5. Gabidulin, E.M., Paramonov, A.V., and Tret'yakov, O.V., Rank Errors and Rank Erasures Correction, in *Proc. 4th Int. Colloq. on Coding Theory, Dilijan, Armenia, 1991*, Yerevan, 1992, pp. 11–19.
6. Brualdi, R.A. and Ryser, H.J., *Combinatorial Matrix Theory*, Encyclopedia of Mathematics and Its Applications, vol. 39, Cambridge: Cambridge Univ. Press, 1991.