Transposed rank codes based on symmetric matrices

Ernst M. Gabidulin
gab@pop3.mipt.ru

Nina I. Pilipchuk
nina.pilipchuk@pop3.mipt.ru

Moscow Institute of Physics and Technology

Abstract

Let $\mathcal{V}$ be a F_n-linear maximum rank distance (MRD) (n,k,d) code over the field F_n. All the code words are $n-$vectors over F_n. One refers to this code as a code in the *vector* representation. It also can be represented as a set $\mathcal{M}$ of $n \times n$ matrices over the base field F_1 by some mapping $B: F_n \Longrightarrow F_1^n$. Thus a code vector $\mathbf{g} = (g_1, g_2, \ldots, g_n),\ g_j \in F_n$, is (reversibly) mapped to a code matrix $M = (M_{i,j}),\ M_{i,j} \in F_1,\ i,j = 1,2,\ldots,n$. One refers to the set $\mathcal{M}$ as a code in the *matrix* representation.

The set $\mathcal{M}^T$ of all transposed code matrices $\mathbf{C}^T$ is known as the *transposed* rank code in the matrix representation. It can be rewritten as a code in the vector representation by the inverse map B^{-1} but this code is only F_1-linear, *not necessarily* F_n-linear. Hence no fast decoding algorithms are known for transposed rank codes.

In this paper, we consider a special class of MRD codes based on symmetric matrices. We show that some mapping exists for the set $\mathcal{M}^T$ such that resulted code is the F_n-linear code in the vector representation. This property allows more flexible fast decoding algorithms.

1 Introduction

Codes in rank metric (or, in brief, rank codes) are of interest to communications, cryptography, space-time coding, etc., [1, 2, 3]. Rank codes can be considered in a *vector* or in a *matrix* representation. We remind some notations and definitions.

Let $F_1 = GF(q)$ be a base field and let $F_n = GF(q^n)$ be an extension of degree n of the field F_1.

Let $F_1^{n\times n}$ be a normalized space of square matrices of order n over F_1. The *rank* norm of a matrix $G \in F_1^{n\times n}$ is defined as ordinary rank of this matrix, i.e., the *maximal number* of rows (or, columns) which are linearly independent over F_1. We denote the rank norm of G as $rank(G)$. The *rank distance* between G_1 and G_2 is defined as $d(G_1, G_2) = rank(G_1 - G_2)$.

A (matrix) code $\mathcal{M} \subset F_1^{n\times n}$ is any set of matrices. A code $\mathcal{M}$ is said to be F_1-linear (or, simply linear) if any linear combination of code matrices with coefficients in F_1 is a code matrix too. Given a code $\mathcal{M}$ one can construct a code $\mathcal{M}^T = \left\{G^T : G \in \mathcal{M}\right\}$ where G^T means the transposed matrix. The code $\mathcal{M}^T$ is called the *transposed* code (given $\mathcal{M}$). It is clear that many characteristics of $\mathcal{M}$ and $\mathcal{M}^T$, such as code distance, weight distribution, linearity, and others are identical.

Let F_n^n be a normalized vector space of dimension n over F_n where the *rank* norm of a vector $\mathbf{g} = (g_1, g_2, \ldots, g_n),\ \mathbf{g} \in F_n^n$, is defined as the *maximal number* of coordinates g_j which are linearly independent over the base field F_1. We denote the rank norm of $\mathbf{g}$ as $r(\mathbf{g})$.

A code $\mathcal{V} \subset F_n^n$ is said to be F_1-linear if a linear combination of code vectors with coefficients in F_1 is a code vector too. A code $\mathcal{V} \subset F_n^n$ is said to be F_n-linear if a linear

combination of code vectors with coefficients in F_n is a code vector too, or, equivalently, if $\mathcal{V}$ is a subspace of F_n^n. A code can be F_1-linear but not F_n-linear.

Let $\Omega = \{\omega_1, \omega_2, \ldots, \omega_n\}$ be a basis of the extension field F_n over the base field F_1. Each element $\beta \in F_n$ can be uniquely represented in the form

$$\beta = b_1\omega_1 + b_2\omega_2 + \ldots + b_n\omega_n = (\omega_1, \omega_2, \ldots, \omega_n) \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}, \tag{1.1}$$

where $b_i \in F_1,\ i = 1, \ldots, n$. Thus Eq (1.1) defines a one-to-one mapping

$$B_\Omega :\ F_n \Rightarrow F_1^n, \tag{1.2}$$

i.e., each element of $\beta \in F_n$ is uniquely mapped into a column vector $b = (b_1, b_2, \ldots, b_n)^T \in F_1^n$. Each column $b = (b_1, b_2, \ldots, b_n)^T \in F_1^n$ is uniquely mapped into the element β using inverse mapping B_Ω^{-1} (1.1).

Define one-to-one mapping vectors $\mathbf{g} = (g_1, g_2, \ldots, g_n) \in F_n^n$ into matrices $G \in F_1^{n\times n}$ by the formula

$$B_\Omega(\mathbf{g}) = G = (B_\Omega(g_1), B_\Omega(g_2), \ldots, B_\Omega(g_n)). \tag{1.3}$$

Mapping (1.3) being applied to a chosen *vector* code $\mathcal{V} \subset F_n^n$ gives a *matrix* code $\mathcal{M} = B_\Omega(\mathcal{V}) \subset F_1^{n\times n}$. It is clear that B_Ω is norm- and distance-preserving mapping: $r(\mathbf{g}) = rank(B_\Omega(\mathbf{g}))$; $rank(G) = r(B_\Omega^{-1}(G))$. Hence given B_Ω we can say on the *vector* or *matrix* representation of a code and use vector or matrix notations by context.

The vector representation is more convenient to describe code constructions and decoding algorithms (see, e.g., [1]) while the matrix representation is useful in the coding modulation area, for example, in the theory of space-time codes (see, e.g., [3]).

One can construct new codes in rank metric using known codes. Let a code $\mathcal{V}$ be given in the vector representation. Let two bases Ω and $\widetilde{\Omega}$ be given. Then construct a new code $\mathcal{V}^T$ as follows:

$$\mathcal{V} \overset{B_\Omega}{\longrightarrow} \mathcal{M} \longrightarrow \mathcal{M}^T \overset{B_{\widetilde{\Omega}}^{-1}}{\longrightarrow} \mathcal{V}^T. \tag{1.4}$$

We call $\mathcal{V}^T$ the transposed code in the vector representation. Note that bases Ω and $\widetilde{\Omega}$ can be different.

The code $\mathcal{V}^T$ preserves all the distance properties of the code $\mathcal{V}$ with the only exception. If the code $\mathcal{V}$ is F_n-linear then $\mathcal{V}^T$ may not be F_n-linear though it is still F_1-linear. This is a grave disadvantage since fast decoding algorithms are known only for F_n-linear codes.

We illustrate this with the following example.

Example 1 *Let $q = 2$ and $\mathcal{V}$ be F_3-linear code*

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

where α is a root of the irreducible polynomial $f(x) = x^3+x+1$. Let B_Ω be defined by relations $1 \leftrightarrow (1,0,0)^T, \alpha \leftrightarrow (0,1,0)^T, \alpha^2 \leftrightarrow (0,0,1)^T$. Then $\mathcal{M}$ is a set of 3×3 matrices over the field $GF(2)$:

$$M_0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \; M_7 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; M_1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \; M_2 = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix},$$

$$M_3 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \; M_4 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \; M_5 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \; M_6 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

If we transpose these matrices and convert them into vectors by B_Ω^{-1}, we get the code

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

which is not F_3-linear, only F_1-linear.

In this paper, we show that for a special class of linear maximum rank distance (MRD) codes $\mathcal{V}$ there exist bases Ω and $\widetilde{\Omega}$ such that both $\mathcal{V}$ and transposed code $\mathcal{V}^T$ are F_n-linear.

2 A class of MRD codes

From now on we consider binary fields only, i.e., $q = 2$.

The standard generator matrix of a linear maximum rank distance code in the vector representation has a form [1]

$$\mathbf{G} = \begin{bmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^2 & g_2^2 & \cdots & g_n^2 \\ g_1^{2^2} & g_2^{2^2} & \cdots & g_n^{2^2} \\ \cdots & \cdots & \cdots & \cdots \\ g_1^{2^{k-1}} & g_2^{2^{k-1}} & \cdots & g_n^{2^{k-1}} \end{bmatrix}, \tag{2.5}$$

where $g_1, g_2, \ldots, g_n$ are linearly independent over the base field F_1.

These codes achieve the Singlton bound $d = n - k + 1$ for code rank distance.

The first row of the generator matrix (2.5) generates an F_n-linear $(n, 1, n)$ code. It is shown in [4] that there exists so-called symmetric representation for this code such that a transposed code is also F_n-linear. In this case all the code matrices in the matrix representation are symmetric.

We consider a class of MRD codes (2.5) for which *the first row defines a $(n, 1, n)$ subcode with the symmetric representation.* We refer to these codes as MRD codes based on symmetric matrices.

The main statement is as follows.

Theorem 1 (Main) *Let $\mathcal{V}$ be a F_n-linear MRD (n, k, d) code based on symmetric matrices with generator matrix (2.5). Then the corresponding transposed code $\mathcal{V}^T$ is also a F_n-linear*

MRD (n,k,d) *code based on symmetric matrices with generator matrix*

$$\mathbf{G} = \begin{bmatrix} g_1^{2^{n-k+1}} & g_2^{2^{n-k+1}} & \cdots & g_n^{2^{n-k+1}} \\ g_1^{2^{n-k}} & g_2^{2^{n-k}} & \cdots & g_n^{2^{n-k}} \\ \cdots & \cdots & \cdots & \cdots \\ g_1^{2^{n-1}} & g_2^{2^{n-1}} & \cdots & g_n^{2^{n-1}} \\ g_1 & g_2 & \cdots & g_n \end{bmatrix}. \tag{2.6}$$

In Section 3, matrix and vector representations of an extension field are described. Proof of the Main theorem is given in Section 4.

3 Matrix and vector representations of an extension field

Let α be a root of an irreducible primitive monic polynomial

$$f(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + a_{n-3}\lambda^{n-2} + \ldots + a_1\lambda^1 + a_0. \tag{3.7}$$

Then α is a primitive element of an extension field F_n. The elements $\alpha^j,\ j = 1, 2, \ldots, 2^n - 1$ are all non zero elements of F_n. Moreover, for $i \neq j$, we have $\alpha^i - \alpha^j = \alpha^k$.

Let A be an $n \times n$ matrix over the base field F_1. We say that the matrix A represents the field F_n) if and only if all the powers $A^j,\ j = 1, 2, \ldots, 2^n - 1$ are distinct, $A^{2^n-1} = I_n$, where I_n is the identity matrix of order n, and $A^i - A^j = A^k,\ i \neq j$.

A matrix A represents the extension field F_n with image α if and only if its characteristic polynomial $\det(\lambda I_n - A)$ coincides with the irreducible primitive polynomial $f(\lambda)$ of Eq (3.7).

There exist many matrices representing the extension field F_n with the same image α.

Lemma 1 *Let C be a matrix representing the field F_n with image α. Let Q be a non singular matrix in F_1 of order n. Then the matrix $A = Q^{-1}CQ$ also represents the field F_n with image α.*

Proof. Matrices C and $A = Q^{-1}CQ$ are similar. Hence they have identical characteristic polynomials. □

It is known (see, e.g., [5]) that the companion matrix C of the polynomial (3.7)

$$C = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & -a_{n-2} \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix} \tag{3.8}$$

represents the field F_n with image α since the characteristic polynomial of this matrix is $f(\lambda)$ from Eq (3.7). By Lemma 1, all the other matrices representing the same field are of the form $A = Q^{-1}CQ$, where Q is a square nonsingular matrix of order n over the base field F_1.

Denote $A[j]$ the jth column of a matrix A. Note that for non zero column b=$(b_1, b_2, \ldots, b_n)^T$ $\in F_1^n$ there exists the only integer j such that $b = A^j[1]$.

Let A be a matrix representing the field F_n with image α. Define one-to-one mapping B_A by relations

$$B_A(0) = (0, 0, \ldots, 0)^T,\ B_A(\alpha^j) = A^j[1],\ j = 1, \ldots, 2^{n-1}, \tag{3.9}$$

(we use notation B_A instead of more general notation B_Ω.) We say that B_A defines the *vector representation* of the field F_n with image α.

For a vector $\mathbf{g} = (g_1, g_2, \dots, g_n),\ g_j \in F_n$, we define

$$B_A(\mathbf{g}) = (B_A(g_1), B_A(g_2), \dots, B_A(g_n)).$$

Thus $G = B_A(\mathbf{g})$ is an $n \times n$ matrix in F_1.

Lemma 2 *Let $\beta \in F_n$. Then*

$$B_A(\alpha\beta) = AB_A(\beta).$$

PROOF. If $\beta = 0$ then nothing to prove. If $\beta \neq 0$ then $\beta = \alpha^s$ for some integer s. Therefore

$$B_A(\alpha\beta) = B_A(\alpha^{1+s}) = A^{1+s}[1] = AA^s[1] = AB_A(\beta).$$

□

Corollary 1 *Let $\mathbf{g} \in F_n^n$ and $B_A(\mathbf{g}) = G$. Then $B_A(\alpha\mathbf{g}) = AB_A(\mathbf{g}) = AG$ and, inversely, $B_A^{-1}(AG) = \alpha B_A^{-1}(G)$. By recursion, for integer s, $B_A^{-1}(A^sG) = \alpha^s B_A^{-1}(G) = \alpha^s\mathbf{g}$.*

Corollary 2 *Let $\mathbf{g} \in F_n^n$. Let R be a $n \times m$ matrix in F_1. Then*

$$B_A(\mathbf{g}R) = B_A(\mathbf{g})R.$$

4 Proof of the Main theorem

It is shown in [4] that symmetric matrices $A = A^T$ exist representing binary fields F_n. From now on, we consider only symmetric matrices A.

Choose the first row in the generator matrix (2.5) as $B_A^{-1}(I_n)$, i.e., the vector representation of the identity matrix I_n:

$$\mathbf{g}_0 = (g_1, g_2, \dots, g_n) = B_A^{-1}(I_n) = (\alpha^{i_1}, \alpha^{i_2}, \dots, \alpha^{i_n}), \tag{4.10}$$

where $i_1 = 0$.

The next row $\mathbf{g}_1$ can be represented as

$$\mathbf{g}_1 = (g_1^2, g_2^2, \dots, g_n^2) = (\alpha^{2i_1}, \alpha^{2i_2}, \dots, \alpha^{2i_n}).$$

Let $D = B_A(\mathbf{g}_1)$ be the $n \times n$ nonsingular matrix in F_1.

Lemma 3

$$\mathbf{g}_1 = \mathbf{g}_0 D.$$

PROOF. It follows from Corollary 2

$$\mathbf{g}_1 = B_A^{-1}(D) = B_A^{-1}(I_n D) = B_A^{-1}(B_A(\mathbf{g}_0)D) = \mathbf{g}_0 D.$$

□

For $s = 0, 1, 2, \dots, n-1$, define

$$\mathbf{g}_s = (g_1^{2^s}, g_2^{2^s}, \dots, g_n^{2^s}). \tag{4.11}$$

Lemma 4

$$\mathbf{g}_s = \mathbf{g}_{s-1}D = \mathbf{g}_0 D^s. \tag{4.12}$$

PROOF. We have from Lemma 3 that $g_j^2 = \sum_{i=1}^n g_i D_{ij}$, where D_{ij} are binary entries of the matrix D. Hence, jth coordinate of the vector $\mathbf{g}_s$ is $g_j^{2^s} = \sum_{i=1}^n g_i^{2^{s-1}} D_{ij}$, or, $\mathbf{g}_s = \mathbf{g}_{s-1}D$. □

Lemma 5 *Let $\mathbf{a}_s = B_A^{-1}(A^s)$ be the vector representation of the matrix A^s. Then*

$$\mathbf{a}_s = (\alpha^{s+i_1}, \alpha^{s+i_2}, \dots, \alpha^{s+i_n}). \tag{4.13}$$

PROOF. We have using Corollary 1 $\mathbf{a}_s = B_A^{-1}(A^s) = B_A^{-1}(A^s I_n) = \alpha^s B_A^{-1}(I_n) = \alpha^s \mathbf{g}_0 = (\alpha^{s+i_1}, \alpha^{s+i_2}, \dots, \alpha^{s+i_n})$. □

Corollary 3

$$\mathbf{g}_0 A = \alpha \mathbf{g}_0 = (\alpha^{1+i_1}, \alpha^{1+i_2}, \dots, \alpha^{1+i_n}),$$

or, equivalently, $\sum_{s=1}^n g_s A_{sj} = \alpha^{1+ij}$, $j = 1, \dots, n$, where A_{sj} are (binary) entries of the matrix A.

PROOF. It is enough to prove that mapping B_A of both sides are identical. $B_A(\mathbf{g}_0 A) = B_A(\mathbf{g}_0)A = I_n A = A$. On the other hand, $B_A(\alpha \mathbf{g}_0) = A B_A(\mathbf{g}_0) = A I_n = A$. □

Lemma 6

$$D^s \neq I_n,\ 1 \leq s \leq n;\ D^n = In. \tag{4.14}$$

PROOF. *Vectors $\mathbf{g}_s$, $s = 0, 1, \dots, n-1$ are linearly independent [5]. Therefore $D^s \neq I_n$, $1 \leq s \leq n-1$. On the other hand, $\mathbf{g}_n = \mathbf{g}_0 D^n = (g_1^{2^n}, g_2^{2^n}, \dots, g_n^{2^n}) = (g_1, g_2, \dots, g_n) = \mathbf{g}_0$. Hence, $D^n = I_n$.* □

Lemma 7

$$DA = A^2 D. \tag{4.15}$$

PROOF. Calculate

$$B_A^{-1}(DA) = B_A^{-1}(D)A = \mathbf{g}_1 A = (\sum_{i=1}^n g_i^2 A_{ij},\ j = 1, \dots, n)$$

$$= ((\sum_{i=1}^n g_i A_{ij})^2,\ j = 1, \dots, n) = (\alpha^{2+2i_1}, \alpha^{2+2i_2}, \dots, \alpha^{2+2i_2}) = \alpha^2 \mathbf{g}_1.$$

Hence

$$B_A(B_A^{-1}(DA)) = DA = B_A(\alpha^2 \mathbf{g}_1) = A^2 B_A(\mathbf{g}_1) = A^2 D.$$

□

Lemma 8 *For* $r, s = 0, 1, \ldots, n-1$,

$$D^r A^s = A^{2^s} D^r. \tag{4.16}$$

PROOF. It follows from Lemma 7 using some iteration procedure. For example,

$$DA^2 = (DA)A = (A^2D)A = A^2(DA) = A^2(A^2D) = A^{2^2}D,$$

or,

$$D^2A = D(DA) = D(A^2D) = (DA)(AD) = (A^2D)(AD) = A^2(DA)D = A^2(A^2D)D = A^{2^2}D^2,$$

etc. □

Lemma 9

$$D^T = A^u D^{n-1} \tag{4.17}$$

for some integer u.

PROOF. Transpose matrices in (4.15) and note that A is the symmetric matrix: $D^TA^2 = AD^T = D^TDAD^{-1}$, or, $D^TDA = AD^TD$. Thus the matrix D^TD commute with A and should be equal to degree, say, u of A. We have $D^T = A^uD^{-1} = A^uD^{n-1}$. (In fact, one can prove that $D^T = D^{n-1}$ but we use this fact without proof). □

It follows from this Lemma that

$$(D^T)^j A^s = A^{2^s} D^{n-j}. \tag{4.18}$$

Let F_n-linear MRD code $\mathcal{V}$ be given defined by the generator matrix

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-2} \\ \mathbf{g}_{k-1} \end{bmatrix}, \tag{4.19}$$

where rows $\mathbf{g}_s$ are defined by Eq (4.10, 4.11).

Let an information vector $\mathbf{u}$ of dimension k be given by $\mathbf{u}=(\varepsilon_0\alpha^{m_0}, \varepsilon_1\alpha^{m_1}, \ldots, \varepsilon_{k-1}\alpha^{m_{k-1}})$, where $\varepsilon_j \in \{0, 1\}$ and $0 \le m_j \le 2^n - 1$ are integers. Then a code vector is equal to

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

The corresponding code matrix is as follows

$$M(\mathbf{u}) = B_A(\sum_{j=0}^{k-1} \varepsilon_j \alpha^{m_j} \mathbf{g}_j) = \sum_{j=0}^{k-1} \varepsilon_j B_A(\alpha^{m_j} \mathbf{g}_j) = \sum_{j=0}^{k-1} \varepsilon_j A^{m_j} D^j. \tag{4.20}$$

The *transposed code* matrix is

$$M(\mathbf{u})^T = \sum_{j=0}^{k-1} \varepsilon_j (D^T)^j A^{m_j}. \tag{4.21}$$

By Eq (4.18), it can be rewritten as

$$M(\mathbf{u})^T = \sum_{j=0}^{k-1} \varepsilon_j A^{2^{m_j}} D^{n-j}. \tag{4.22}$$

This means that the transposed code $\mathcal{V}_T$ in vector representation can be described as

$$\widetilde{\mathbf{g}}(\mathbf{u}) = B_A^{-1}(M(\mathbf{u})^T) = \sum_{j=0}^{k-1} \varepsilon_j B_A^{-1}(A^{2^{m_j}} D^{n-j}) = \sum_{j=0}^{k-1} \varepsilon_j \alpha^{2^{m_j}} \mathbf{g}_{n-j}.$$

In turn, this expression shows that the transposed code $\mathcal{V}^T$ is F_n-linear and may be given by the following generator matrix

$$\widetilde{\mathbf{G}} = \begin{bmatrix} \mathbf{g}_{n-k+1} \\ \mathbf{g}_{n-k} \\ \vdots \\ \mathbf{g}_{n-1} \\ \mathbf{g}_0 \end{bmatrix} = \begin{bmatrix} g_1^{2^{n-k+1}} & g_2^{2^{n-k+1}} & \cdots & g_n^{2^{n-k+1}} \\ g_1^{2^{n-k}} & g_2^{2^{n-k}} & \cdots & g_n^{2^{n-k}} \\ \cdots & \cdots & \cdots & \cdots \\ g_1^{2^{n-1}} & g_2^{2^{n-1}} & \cdots & g_n^{2^{n-1}} \\ g_1 & g_2 & \cdots & g_n \end{bmatrix}. \tag{4.23}$$

If we denote $\widetilde{g}_1 = g_1^{2^{n-k+1}}, \widetilde{g}_2 = g_2^{2^{n-k+1}}, \ldots, \widetilde{g}_n = g_n^{2^{n-k+1}}$, then the generator matrix $\widetilde{\mathbf{G}}$ can be rewritten in the canonical form of Eq (2.5):

$$\mathbf{G}^{Tr} = \begin{bmatrix} \widetilde{g}_1 & \widetilde{g}_2 & \cdots & \widetilde{g}_n \\ \widetilde{g}_1^q & \widetilde{g}_2^q & \cdots & \widetilde{g}_n^q \\ \widetilde{g}_1^{2^2} & \widetilde{g}_2^{2^2} & \cdots & \widetilde{g}_n^{2^2} \\ \cdots & \cdots & \cdots & \cdots \\ \widetilde{g}_1^{2^{k-1}} & \widetilde{g}_2^{2^{k-1}} & \cdots & \widetilde{g}_n^{2^{k-1}} \end{bmatrix}. \tag{4.24}$$

5 Conclusions

We proposed F_n-linear MRD codes based on symmetric matrices such that corresponding transposed codes are also F_n-linear MRD codes. This allows to use either fast decoding based on columns of received corrupted code matrix, or fast decoding based on rows that matrix, or both.

References

[1] E.M.Gabidulin, "Theory of Codes with Maximum Rank Distance," *Problems of Information Transmission*, v. 21, No. 1, pp. 3-14, 1985.

[2] E.M. Gabidulin, A.V. Paramonov, O.V. Tretjakov "Ideals over a Non-Commutative Ring and Their Application in Cryptology," Lecture Notes in Computer Science, v. 547, Advances in Cryptology, Proceedings of EUROCRYPT'91, Brighton, UK, April 1991, pp. 482-489.

[3] E.M. Gabidulin, M. Bossert, P. Lusina, "Space-Time Codes Based on Rank Codes," *Proceedings of the 2000 IEEE International Symposium on Information Theory*, 25 - 30 June, 2000, p. 283, Sorrento, Italy.

[4] E.M. Gabidulin, N.I. Pilipchuk,"Representation of a finite field by symmetric matrices and applications," *Proceedings* of the Eighth International Workshop "Algebraic and combinatorial coding theory", 8 -14 September, 2002, Tsarskoe Selo, Russia, p. 120-123.

[5] F.J. MacWilliams, N.J.A. Sloane, "The Theory of Error Correcting Codes," 8th ed, North Holland Press, Amsterdam, 1993.