Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 108-118*

New systematic easy decoding symmetric rank codes

Ernst Gabidulin[1] gab@mail.mipt.ru
Moscow Institute of Physics and Technology (State University), RUSSIA

Abstract. A family of rank-metric codes over binary fields with lengths $N_s = 2^s$, $s = 0, 1, \ldots$, is constructed. Codes of length N_s are designed recursively from codes of length N_{s-1}. This provides very high degree of symmetry of code matrices. In turn, it allows to decode corrupted received matrices recursively starting with small lengths. The construction allows to use many simple algorithms for decoding in rank metric such as majority rules and similar.

1 Introduction

Rank-metric codes are of interest to communications, cryptography, space-time coding, network coding, etc., [1, 2, 4, 5, 6]. Symmetric rank-metric codes were introduced in [7] and investigated in [8]-[14]. Symmetry allows to simplify decoding and to correct some rank errors beyond the error capability bound. In this paper, we propose a recursive construction of rank codes over *binary* fields starting with length 2. The length is doubled at each step and is equal to $N_s = 2^s$ after step s. In matrix representation, code words are $N_s \times N_s$ matrices. They are constructed by means of $N_{s-1} \times N_{s-1}$ code matrices obtained at the previous step. This leads to very high degree of symmetry of code matrices. First, each code matrix of size $2^s \times 2^s$ is element wise symmetric. Second, if this matrix is represented as a $2^{s-1} \times 2^{s-1}$ block matrix consisting of blocks of size 2×2, then the matrix will be block wise symmetric for these blocks and all blocks are element wise symmetric. Further, if the original code matrix is represented as a $2^{s-2} \times 2^{s-2}$ block matrix with blocks of size $2^2 \times 2^2$, then the matrix will be block wise symmetric for these blocks and all $2^2 \times 2^2$ blocks are both element wise symmetric and 2×2 subblocks wise symmetric. Finally, represent the $2^s \times 2^s$ code matrix as 2×2 block matrix with four blocks of size $2^{s-1} \times 2^{s-1}$. Then the matrix will be block wise symmetric for these blocks. Moreover, each block element of the code matrix is in turn a symmetric matrix with the same properties.

For example, the binary code matrix for length $N_1 = 2$ has the form

$$V_1(x_1, x_2) = \begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 + x_2 \end{pmatrix}, \tag{1.1}$$

where x_1 and x_2 are information bits. Each nonzero 2×2 code matrix has rank 2 and is symmetric.

[1] This work was partially supported under Grant 05-01-39017 GFEN-a

Code matrices of length $N_2 = 4$ constructed by our approach have the form

$$V_2(x_1,x_2,x_3,x_4) = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_1+x_2 & x_4 & x_3+x_4 \\ x_3 & x_4 & x_1+x_4 & x_2+x_3+x_4 \\ x_4 & x_3+x_4 & x_2+x_3+x_4 & x_1+x_2+x_3 \end{pmatrix} \tag{1.2}$$

$$= \begin{pmatrix} V_1(x_1,x_2) & V_1(x_3,x_4) \\ V_1(x_3,x_4) & V_1(x_1,x_2)+\Gamma_1 V_1(x_3,x_4) \end{pmatrix},$$

where x_1, x_2, x_3, x_4 are information bits. The matrix $\Gamma_1 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ provides a property that each nonzero 4×4 code matrix has rank 4 and is symmetric. It can be represented as a 2×2 block matrix with symmetric blocks $V_1(\cdot,\cdot)$ of size 2×2.

In general, if code matrices $V_{s-1}(x_1,\ldots,x_{2^{s-1}})$ of length $N_{s-1} = 2^{s-1}$ are constructed, then code matrices $V_s(x_1,\ldots,x_{2^{s-1}},x_{2^{s-1}+1},\ldots,x_{2^s})$ of length $N_s = 2^s$ will have the form

$$V_s(x_1,\ldots,x_{N_s}) = \begin{pmatrix} V_{s-1}(x_1,\ldots,x_{N_{s-1}}) & V_{s-1}(x_{N_{s-1}+1},\ldots,x_{N_s}) \\ V_{s-1}(x_{N_{s-1}+1},\ldots,x_{N_s}) & V_{s-1}(x_1,\ldots,x_{N_{s-1}})+\Gamma_{s-1}V_{s-1}(x_{N_{s-1}+1},\ldots,x_{N_s}) \end{pmatrix}, \tag{1.3}$$

where $x_1,\ldots,x_{N_{s-1}},x_{N_{s-1}+1},\ldots,x_{N_s}$ are information bits. The matrix Γ_{s-1} of size $N_{s-1} \times N_{s-1}$ is calculated using the previous matrix Γ_{s-2}. It provides a property that each nonzero $N_s \times N_s$ code matrix has rank N_s and is symmetric.

We will exploit super symmetry to construct new decoding algorithms to correct rank and array errors.

2 Auxiliary results

2.1 Notations and definitions

Let F_2 be a base field and let F_{2^n} be an extension of degree n of F_2. Let $F_{2^n}^n$ be a normalized vector space of dimension n over F_{2^n}.

The *rank* norm of a vector $\mathbf{g} = (g_1, g_2, \ldots, g_n)$, $\mathbf{g} \in F_{2^n}^n$, is defined as the *maximal number* of coordinates g_j which are linearly independent over F_2. We denote the rank norm of $\mathbf{g}$ by $r(\mathbf{g})$.

A *vector* code $\mathcal{V} \subset F_{q^n}^n$ is any set of vectors. A *linear* vector code $\mathcal{V}$ is a subspace of $F_{2^n}^n$.

Let $F_2^{n\times n}$ be a normalized space of square matrices of order n over F_q. The *rank* norm of a matrix $M \in F_2^{n\times n}$ is defined as ordinary rank of this matrix, i.e., the *maximal number* of rows (or, columns) which are linearly independent over F_2. We denote the rank norm of M as $\mathrm{rank}(M)$.

A *matrix* code $\mathcal{M} \subset F_2^{n\times n}$ is any set of binary matrices. A code $\mathcal{M}$ is said to be linear if $\mathcal{M}$ is subspace of $F_2^{n\times n}$. Given a code $\mathcal{M}$ one can construct a code $\mathcal{M}^T = \{M^T : M \in \mathcal{M}\}$ where M^T means the transpose of M. A code $\mathcal{M}$ is said to be symmetric if $\mathcal{M} = \mathcal{M}^T$.

2.2 Relations between vector rank-metric codes and matrix rank-metric codes

Let $\mathbf{g} = (g_1, g_2, \ldots, g_n)$, $\quad g_j \in F_{2^n}$, be a basis of F_{2^n} over F_2. Then any vector $\mathbf{m} = (m_1, m_2, \ldots, m_n) \in F_n^n$ can be uniquely represented as

$$\mathbf{m} = (m_1, m_2, \ldots, m_n) = \mathbf{g}M = (g_1, g_2, \ldots, g_n)M,$$

where M is the $n \times n$-matrix in F_q. One refers to the matrix M as the matrix $\mathbf{g}$-representation of the vector $\mathbf{m}$. Note that $r(\mathbf{m}) = \operatorname{rank}(M)$.

Given a vector code $\mathcal{V}$ and a basis $\mathbf{g}$, one can get a corresponding matrix code $\mathcal{M}$ in $\mathbf{g}$-representation as $\mathcal{V} = \mathbf{g}\mathcal{M}$, and vice versa.

2.3 Self-orthogonal bases

Let

$$\mathbf{g} = (g_1, g_2, \ldots, g_n), \quad g_j \in F_{2^n}, \tag{2.4}$$

be a basis of F_{2^n} over F_2. Associate with the vector $\mathbf{g}$ the $n \times n$-matrix

$$\mathbf{G} = \begin{bmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[1]} & g_2^{[1]} & \cdots & g_n^{[1]} \\ g_1^{[2]} & g_2^{[2]} & \cdots & g_n^{[2]} \\ \cdots & \cdots & \cdots & \cdots \\ g_1^{[n-1]} & g_2^{[n-1]} & \cdots & g_n^{[n-1]} \end{bmatrix}. \tag{2.5}$$

We use the notation $[i] := 2^i$, if $i \geq 0$ and $[i] := 2^{n+i}$, if $i < 0$. It is known [15] that the matrix $\mathbf{G}_n$ is non singular.

Definition 1 *A basis $\mathbf{g} = (g_1, g_2, \ldots, g_n)$ is called a* ***self-dual*** *basis if $Tr(g_i g_j) = \delta_{ij}$, where $Tr(\cdot)$ is the trace function of F_{2^n} into F_2 defined as $Tr(g) = g + g^{[1]} + g^{[2]} + \cdots + g^{[n-1]} \in F_2,\ g \in F_{2^n}$.*

Definition 2 (Equivalent) *A basis $\mathbf{g} = (g_1, g_2, \ldots, g_n)$ is called a* ***self-dual*** *basis if*

$$\mathbf{G}^T\mathbf{G} = \mathbf{I}_n,$$

where $\mathbf{G}^T$ is the transpose of $\mathbf{G}$ and $\mathbf{I}_n$ is the identity matrix of order n.

Definition 3 *A basis* $\mathbf{g} = (g_1, g_2, \ldots, g_n)$ *is called a* ***self-orthogonal*** *basis if*

$$\mathbf{G}\mathbf{G}^T = \mathbf{I}_n,$$

It is clear that a self-dual basis is also a self-orthogonal basis, and vice versa.

Definition 4 *A basis* $\mathbf{g} = (g_1, g_2, \ldots, g_n)$ *is called a* ***weak self-orthogonal*** *basis if*

$$\mathbf{G}\mathbf{G}^T = \mathbf{B},$$

where $\mathbf{B}$ *is a diagonal matrix in* F_{2^n}*, but not multiple of the identity matrix* $\mathbf{I}_n$*.*

Note that a *weak* self-orthogonal basis is not a self-dual basis. For example, let $\mathbf{G} = \left(\begin{smallmatrix} 1 & \gamma \\ 1 & \gamma^2 \end{smallmatrix}\right)$, where γ is a primitive element of F_{2^2}. Then $\mathbf{G}\mathbf{G}^T = \left(\begin{smallmatrix} \gamma & 0 \\ 0 & \gamma^2 \end{smallmatrix}\right)$. Hence the basis $(1\ \gamma)$ is the weak self-orthogonal one. On the other hand we have $\mathbf{G}^T\mathbf{G} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Hence the basis $(1\ \gamma)$ is *not* self-dual.

2.4 One-dimensional rank codes

Let $\mathbf{g} = (g_1, g_2, \ldots, g_n)$ be a basis of F_{2^n} over F_2. We shall use this vector in two manner. First, it will be used to represent elements of the field F_{2^n}. An element $\gamma \in F_{2^n}$ is represented as $\gamma = x_1g_1 + x_2g_2 + \cdots + x_ng_n$, where coefficients $x_j \in F_2$ are called information bits of γ.

On the other hand, the vector $\mathbf{g} = (g_1, g_2, \ldots, g_n)$ will be used as the generator vector of a linear $[n, 1, d = n]$ rank-metric vector code $\mathcal{V}_1$. The code $\mathcal{V}_1$ consists of the all zero vector $\mathbf{0} = (0, 0, \ldots, 0)$ and code vectors $\{\mathbf{g}_s = \alpha^s(g_1, g_2, \ldots, g_n),\ s = 0, 1, \ldots, 2^n - 2\}$, where α is a primitive element of F_{2^n}. In terms of the primitive element α the vector $\mathbf{g}$ can be rewritten as $\mathbf{g} = (\alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_n})$, where $i_1, i_2, \ldots, i_n$ are some integers.

Find the matrix representation $\mathcal{M}_1$ of the vector code $\mathcal{V}_1$. Consider the matrix representation of the vector $\alpha\mathbf{g}$:

$$\alpha\mathbf{g} = \mathbf{g}A, \tag{2.6}$$

where A is the $(n \times n)$-matrix in F_2. It follows, that α is an eigenvalue and $\mathbf{g}$ is an eigenvector of A. Hence, A has as the characteristic polynomial a monic primitive polynomial of degree n over F_2. Moreover, all non-zero code vectors are given by

$$\alpha^s\mathbf{g} = \mathbf{g}A^s, \quad s = 0, 1, \ldots, 2^n - 2. \tag{2.7}$$

Therefore the rank-metric matrix code $\mathcal{M}_1$ consists of the all zero matrix $\mathbf{O}$ and code matrices $\{A^s\ s = 0, 1, \ldots, 2^n - 2\}$.

If an element $\gamma = x_1g_1 + x_2g_2 + \cdots + x_ng_n$, then the corresponding code matrix is

$$M(\gamma) = x_1A^{i_1} + x_2A^{i_2} + \cdots + x_nA^{i_n}.$$

Let $\mathbf{g} = (g_1, g_2, \ldots, g_n)$ be a (*weak*) *self-orthogonal basis* of F_{2^n} over F_2. Then the matrix A defined above is the symmetric matrix (see, [12]).

2.5 A recursive construction of a weak self-orthogonal basis – the vector representation

As mentioned before, a weak self-orthogonal basis provides the symmetry of the matrix A. Let $N_s = 2^s,\ q_s = 2^{N_s},\ s = 1, 2, \ldots$. We construct sequentially bases for the fields $F_{q_2} \subset F_{q_3} \subset \cdots \subset F_{q_s}$. Assume that the weak self-orthogonal basis is already constructed for the field F_{q_s}:

$$\mathbf{g}(N_s) = (g_1, g_2, \ldots, g_{N_s}) \tag{2.8}$$

Choose in the superfield $F_{q_{s+1}}$ an element f_{N_s+1} of order $q_s + 1$. Construct the vector

$$\mathbf{g}(N_{s+1}) = (g_1, g_2, \ldots, g_{N_s}, g_{N_s+1}, g_{N_s+2}, \ldots, g_{N_{s+1}}), \tag{2.9}$$

where $(g_{N_s+1}, g_{N_s+2}, \ldots, g_{N_{s+1}}) = (f_{N_s+1}g_1, f_{N_s+1}g_2, \ldots, f_{N_s+1}g_{N_s})$.

Lemma 1 *The vector* $\mathbf{g}(N_{s+1})$ *is a weak self-orthogonal basis for the field* $F_{q_{s+1}}$.

Proof. Let $\mathbf{G}(N_s)$ be the associated matrix of the vector $\mathbf{g}(N_s)$:

$$\mathbf{G}(N_s) = \begin{bmatrix} g_1 & g_2 & \cdots & g_{N_s} \\ g_1^{[1]} & g_2^{[1]} & \cdots & g_{N_s}^{[1]} \\ g_1^{[2]} & g_2^{[2]} & \cdots & g_{N_s}^{[2]} \\ \cdots & \cdots & \cdots & \cdots \\ g_1^{[N_s-1]} & g_2^{[N_s-1]} & \cdots & g_{N_s}^{[N_s-1]} \end{bmatrix}.$$

We have $\mathbf{G}(N_s)\mathbf{G}(N_s)^T = \mathbf{\Lambda}$, where $\mathbf{\Lambda}$ is a diagonal matrix.

It is easy to show that the associated matrix $\mathbf{G}(N_{s+1})$ of the vector $\mathbf{g}(N_{s+1})$ is of the form

$$\mathbf{G}(N_{s+1}) = \begin{bmatrix} \mathbf{G}(N_s) & \mathbf{F}\mathbf{G}(N_s) \\ \mathbf{G}(N_s) & \mathbf{F}^{q_s}\mathbf{G}(N_s) \end{bmatrix}, \tag{2.10}$$

where $\mathbf{F} = \mathrm{diag}[f_{N_s+1}, f_{N_s+1}^{[1]}, \ldots, f_{N_s+1}^{[N_s-1]}]$ is the diagonal matrix. Note that $\mathbf{F}^{q_s+1} = \mathbf{I}_{N_s}$.

Calculate the product

$$
\begin{aligned}
\mathbf{G}(N_{s+1})\mathbf{G}(N_{s+1})^T &= \begin{bmatrix} \mathbf{G}(N_s)\mathbf{G}(N_s)^T+\mathbf{F}\mathbf{G}(N_s)\mathbf{G}(N_s)^T\mathbf{F} & \mathbf{G}(N_s)\mathbf{G}(N_s)^T+\mathbf{F}\mathbf{G}(N_s)\mathbf{G}(N_s)^T\mathbf{F}^{q_s} \\ \mathbf{G}(N_s)\mathbf{G}(N_s)^T+\mathbf{F}^{q_s}\mathbf{G}(N_s)\mathbf{G}(N_s)^T\mathbf{F} & \mathbf{G}(N_s)\mathbf{G}(N_s)^T+\mathbf{F}^{q_s}\mathbf{G}(N_s)\mathbf{G}(N_s)^T\mathbf{F}^{2^{2^s}} \end{bmatrix} \\
&= \begin{bmatrix} \mathbf{\Lambda}(\mathbf{I}_{N_s}+\mathbf{F}^2) & \mathbf{\Lambda}(\mathbf{I}_{N_s}+\mathbf{F}^{q_s+1}) \\ \mathbf{\Lambda}(\mathbf{I}_{N_s}+\mathbf{F}^{q_s+1}) & \mathbf{\Lambda}(\mathbf{I}_{N_s}+\mathbf{F}^{q_{s+1}}) \end{bmatrix} \\
&= \begin{bmatrix} \mathbf{\Lambda}(\mathbf{I}_{N_s}+\mathbf{F}^2) & \mathbf{O}_{N_s} \\ \mathbf{O}_{N_s} & \mathbf{\Lambda}(\mathbf{I}_{N_s}+\mathbf{F}^{q_{s+1}}) \end{bmatrix}.
\end{aligned}
\tag{2.11}
$$

This matrix is diagonal. Therefore the basis $\mathbf{g}(N_{s+1})$ is the weak self-orthogonal basis. □

We have to choose an element $f_{N_s+1} \in F_{q_{s+1}}$ of order q_s+1. Consider the last component $g_{N_s} \in F_{q_s} \subset F_{q_{s+1}}$ of the basis $\mathbf{g}(N_s)$. Assume that $\mathrm{Tr}_{F_{q_s}}(g_{N_s}) = 1$. Consider the polynomial $f_s(x) = x^2 + xg_{N_s}^m + 1$, where $m = 2^{N_s-1} - 1$.

Lemma 2 *The polynomial $f_s(x)$ is irreducible over the field F_{q_s}. Hence its roots belong to the field $F_{q_{s+1}}$. Moreover, the order of roots is $q_s + 1$.*

Proof. Consider the polynomial $r(x) = f_s(xg_{N_s}^m) = g_{N_s}^{2m}(x^2 + x + g_{N_s}^{-2m}) = g_{N_s}^{2m}(x^2+x+g_{N_s})$. This polynomial is irreducible over F_{q_s} because $\mathrm{Tr}_{F_{q_s}}(g_{N_s}) = 1$. So is the polynomial $f_s(x)$. Further, by f_{N_s+1} denote a root of $f_s(x)$. Another root is $f_{N_s+1}^{q_s}$. We have by Viète theorem $f_{N_s+1} \cdot f_{N_s+1}^{q_s} = f_{N_s+1}^{q_s+1} = 1$, or, $\mathrm{ord}(f_{N_s+1}) = q_s + 1$. □

By construction, the last component of the basis $\mathbf{g}(N_{s+1})$ is $g_{N_{s+1}} = f_{N_s+1}g_{N_s}$.

Lemma 3 $\mathrm{Tr}_{F_{q_{s+1}}}(g_{N_{s+1}}) = 1$.

Proof. By definition, we have

$$f_{N_s+1}^2 + f_{N_s+1}g_{N_s}^m + 1 = 0, \tag{2.12}$$

where $m = 2^{N_s-1} - 1$. Multiply this equation by $g_{N_s}^2$. We obtain

$$g_{N_{s+1}}^2 + g_{N_{s+1}}g_{N_s}^{2^{N_s-1}} + g_{N_s}^2 = 0. \tag{2.13}$$

By Viète theorem, $g_{N_{s+1}} + g_{N_{s+1}}^{q_s} = g_{N_s}^{2^{N_s-1}}$. Hence $\mathrm{Tr}_{F_{q_s}}(g_{N_{s+1}} + g_{N_{s+1}}^{q_s}) = \mathrm{Tr}_{F_{q_s}}(g_{N_s}^{2^{N_s-1}}) = \mathrm{Tr}_{F_{q_s}}(g_{N_s}) = 1$. On the other hand,

$$\mathrm{Tr}_{F_{q_s}}(g_{N_{s+1}} + g_{N_{s+1}}^{q_s}) = \sum_{i=0}^{N_s-1}(g_{N_{s+1}} + g_{N_{s+1}}^{q_s})^{2^i} = \sum_{i=0}^{N_{s+1}-1} g_{N_{s+1}}^{2^i} = \mathrm{Tr}_{F_{q_{s+1}}}(g_{N_{s+1}}).$$

□

Example 1 *For $s=1,\ N_1=2$, a weak self-orthogonal basis is*

$$\mathbf{g}(N_1)=(g_1,g_2)=(1,g_2), \tag{2.14}$$

where g_2 is a root of the polynomial $f(x)=x^2+x+1$.

For $s=2,\ N_2=4$, a weak self-orthogonal basis is

$$\mathbf{g}(N_2)=(g_1,g_2,g_3,g_4)=(1,g_2,f_3,f_3g_2), \tag{2.15}$$

where $g_3=f_3$ is a root of the polynomial $f_1(x)=x^2+xg_2+1$ and $\mathrm{Tr}_{F_{q_2}}(g_4)=\mathrm{Tr}_{F_{q_2}}(f_3g_2)=1$.

For $s=3,\ N_3=8$, a weak self-orthogonal basis is

$$\mathbf{g}(N_3)=(g_1,g_2,g_3,g_4,g_5,g_6,g_7,g_8)=(1,g_2,g_3,g_4,f_5,f_5g_2,f_5g_3,f_5g_4), \tag{2.16}$$

where $g_5=f_5$ is a root of the polynomial $f_2(x)=x^2+xg_4^7+1$ and $\mathrm{Tr}_{F_{q_3}}(g_8)=\mathrm{Tr}_{F_{q_3}}(f_5g_4)=1$.

2.6 A recursive construction of a weak self-orthogonal basis – the matrix representation

The matrix representation can be obtained from the vector representation if we replace elements g_j in the basis by suitable matrices. Note that if an element $\beta\in F_{q_s}$ is represented as a $N_s\times N_s$ matrix B over the base field F_2, then being considered as an element of the superfield $F_{q_{s+1}}$ its representation will be a block-diagonal $N_{s+1}\times N_{s+1}$ matrix $\left[\begin{smallmatrix} B & O\\ O & B\end{smallmatrix}\right]$.

Example 2 *For $s=1,\ N_1=2$, the vector basis* (2.14) *is replaced by the matrix basis*

$$I_{N_1}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, G_2(N_1)=\begin{bmatrix}0 & 1\\ 1 & 1\end{bmatrix}. \tag{2.17}$$

The corresponding code matrix is given by Eq. (1.1).

For $s=2,\ N_2=4$, the vector basis (2.15) *is replaced by the matrix basis*

$$\begin{gathered} I_{N_2}=\left[\begin{smallmatrix} I_{N_1} & O_{N_1}\\ O_{N_1} & I_{N_1}\end{smallmatrix}\right], G_2(N_2)=\left[\begin{smallmatrix} G_2(N_1) & O_{N_1}\\ O_{N_1} & G_2(N_1)\end{smallmatrix}\right],\\ G_3(N_2)=\left[\begin{smallmatrix} O_{N_1} & I_{N_1}\\ I_{N_1} & G_2(N_1)\end{smallmatrix}\right], G_4(N_2)=\left[\begin{smallmatrix} O_{N_1} & G_2(N_1)\\ G_2(N_1) & G_2(N_1)^2\end{smallmatrix}\right]. \end{gathered} \tag{2.18}$$

The corresponding code matrix is given by (1.2).

For $s = 3$, $N_3 = 8$, the vector basis (2.16) is replaced by the matrix basis

$$\begin{array}{l} I_{N_3} = \left[\begin{smallmatrix} I_{N_2} & O_{N_2} \\ O_{N_2} & I_{N_2} \end{smallmatrix}\right], G_2(N_3) = \left[\begin{smallmatrix} G_2(N_2) & O_{N_2} \\ O_{N_2} & G_2(N_2) \end{smallmatrix}\right], \\ G_3(N_3) = \left[\begin{smallmatrix} G_3(N_2) & O_{N_2} \\ O_{N_2} & G_3(N_2) \end{smallmatrix}\right], G_4(N_3) = \left[\begin{smallmatrix} G_4(N_2) & O_{N_2} \\ O_{N_2} & G_4(N_2) \end{smallmatrix}\right], \\ G_5(N_3) = \left[\begin{smallmatrix} O_{N_2} & I_{N_2} \\ I_{N_2} & G_4(N_2)^7 \end{smallmatrix}\right], G_6(N_3) = \left[\begin{smallmatrix} O_{N_2} & G_2(N_2) \\ G_2(N_2) & G_4(N_2)^7 G_2(N_2) \end{smallmatrix}\right], \\ G_7(N_3) = \left[\begin{smallmatrix} O_{N_2} & G_3(N_2) \\ G_3(N_2) & G_4(N_2)^7 G_3(N_2) \end{smallmatrix}\right], G_8(N_3) = \left[\begin{smallmatrix} O_{N_2} & G_4(N_2) \\ G_4(N_2) & G_4(N_2)^8 \end{smallmatrix}\right] \end{array}. \tag{2.19}$$

The corresponding code matrix is given by

$$V_3(x_1, \dots, x_8) = \begin{pmatrix} V_2(x_1, \dots, x_4) & V_2(x_5, \dots, x_8) \\ V_2(x_5, \dots, x_8) & V_2(x_1, \dots, x_4) + \Gamma_2 V_2(x_5, \dots, x_8) \end{pmatrix}, \tag{2.20}$$

where

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

3 Decoding super-symmetric rank-metric codes

Here we consider decoding one-dimensional rank-metric matrix codes. Let $V_s(x_1, \dots, x_{N_s})$ be a code matrix of rank N_s and E is an error matrix of size $N_s \times N_s$ over F_2. If a received matrix is $Y = V_s(x_1, \dots, x_{N_s}) + E$ and $\mathrm{rank}(E) = t \le N_{s-1} - 1$, then standard methods (see, [1] and others) allow to correct all such errors.

On the other hand, use of Eq. (1.3) and represent E as $\left(\begin{smallmatrix} E_{11} & E_{12} \\ E_{21} & E_{22} \end{smallmatrix}\right)$. Then

$$Y = \begin{pmatrix} V_{s-1}(x_1 \dots x_{N_{s-1}}) + E_{11} & V_{s-1}(x_{N_{s-1}+1} \dots x_{N_s}) + E_{12} \\ V_{s-1}(x_{N_{s-1}+1} \dots x_{N_s}) + E_{21} & V_{s-1}(x_1 \dots x_{N_{s-1}}) + \Gamma_{s-1} V_{s-1}(x_{N_{s-1}+1} \dots x_{N_s}) + E_{22} \end{pmatrix}. \tag{3.21}$$

One can see that decoding the $N_s \times N_s$ code matrices can be reduced to decoding several code matrices of order $N_{s-1} = N_s/2$. Namely, we have to decode the code submatrix $V_{s-1}(x_1 \dots x_{N_{s-1}})$ depending only on half information variables $x_1, \dots, x_{N_{s-1}}$. It satisfies conditions from Eq. (3.21):

$$\begin{array}{lcl} V_{s-1}(x_1 \dots x_{N_{s-1}}) + E_{11} & = & Y_{11}, \\ V_{s-1}(x_1 \dots x_{N_{s-1}}) + E_{22} + \Gamma_{s-1} E_{12} & = & Y_{22} + \Gamma_{s-1} Y_{12}, \\ V_{s-1}(x_1 \dots x_{N_{s-1}}) + E_{22} + \Gamma_{s-1} E_{21} & = & Y_{22} + \Gamma_{s-1} Y_{21}. \end{array} \tag{3.22}$$

Similarly, the code submatrix $V_{s-1}(x_{N_{s-1}+1}\dots x_{N_s})$ satisfies conditions

$$\begin{array}{lcl} V_{s-1}(x_{N_{s-1}+1}\dots x_{N_s})+E_{12} & = & Y_{12}, \\ V_{s-1}(x_{N_{s-1}+1}\dots x_{N_s})+E_{21} & = & Y_{21}, \\ V_{s-1}(x_{N_{s-1}+1}\dots x_{N_s})+E_{11}+\Gamma_{s-1}^{-1}E_{22} & = & Y_{11}+\Gamma_{s-1}^{-1}Y_{22}. \end{array} \tag{3.23}$$

If $\min\{\mathrm{rank}(E_{12}),\mathrm{rank}(E_{21}),\mathrm{rank}(E_{22}+\Gamma_{s-1}E_{21})\}\le N_{s-2}-1$ and $\min\{\mathrm{rank}(E_{11}),\mathrm{rank}(E_{22}+\Gamma_{s-1}E_{12}),\mathrm{rank}(E_{11}+\Gamma_{s-1}^{-1}E_{22})\}\le N_{s-2}-1$, then decoding will be successful.

Note that $\mathrm{rank}(E)$ of the original error matrix may be greater than $N_{s-1}-1$. Hence the symmetry of a code matrix $V_s(x_1\dots x_{N_s})$ allows to correct many rank errors beyond the one half distance bound. For example, the code $V_3(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8)$ has rank distance 8 and can correct all rank errors up to rank 3. The error matrix

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

has rank 6 and can not be corrected by general fast algorithms. But Eq.'s (3.22) and (3.23) allow to correct this error. On the other hand, the error matrix

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

has rank 3 and can be corrected by general fast algorithms. But Eq.'s (3.22) and (3.23) do not allow to correct this error. Therefore general algorithms and symmetry algorithms should be used in common: first a general algorithm but if it failes use a symmetry algorithm.

The proposed approach can be iterated until we get the best conditions from the point of view of complexity.

4 Conclusion

We proposed one-dimensional rank-metric matrix codes generated by weak self-orthogonal bases. These codes allow to correct not only all errors of rank not greater than $\lfloor (d-1)/2 \rfloor$ but also many specific (namely, symmetric) errors beyond this bound.

References

[1] E. M. Gabidulin, Theory of codes with maximum rank distance, *Probl. Inform. Transm.* 21, 1985, 3-14.

[2] E. M. Gabidulin, A. V. Paramonov, O. V. Tretjakov, Ideals over a non-commutative ring and their application in cryptology, *Lect. Notes Comp. Sci.* 547, Adv. Crypt., Proc. Eurocrypt91, Brighton, UK, 1991, 482-489.

[3] E. M. Gabidulin, A fast matrix decoding algorithm for rank-error-correcting codes, (Eds G. Cohen, S. Litsyn, A. Lobstein, G. Zemor), *Lect. Notes Comp. Sci.* 573, Alg. Coding, Springer-Verlag, Berlin, 1992, 126-132.

[4] E. M. Gabidulin, M. Bossert, P. Lusina, Space-time codes based on rank codes, *Proc. IEEE Intern. Symp. Inform. Theory*, 2000, Sorrento, Italy, 283.

[5] R. Koetter, F. R. Kschischang, Coding for errors and erasures in random network coding, *Proc. IEEE Intern. Symp. Inform. Theory*, Nice, France, 2007, 791-795.

[6] E. M. Gabidulin, N. I. Pilipchuk, Error and erasure correcting algorithms for rank codes, *Des., Codes Crypt.*, Springer Netherlands, DOI 10.1007/s10623-008-9185-7. Online: 11 March 2008.

[7] E. M. Gabidulin, N. I. Pilipchuk, Representation of a finite field by symmetric matrices and applications, *Proc. Eighth Intern. Workshop ACCT*, 2002, Tsarskoe Selo, Russia, 120-123.

[8] E. M. Gabidulin, N. I. Pilipchuk, Transposed rank codes based on symmetric matrices, *Proc. WCC2003*, 2003, Versailles (France), 203-211.

[9] E. M. Gabidulin, N. I. Pilipchuk, A new method of erasure correction by rank codes, *Proc. IEEE Intern. Symp. Inform. Theory*, Yokohama, Japan, 2003, 423.

[10] E. M. Gabidulin, N. I. Pilipchuk, Symmetric rank codes, *Probl. Inform. Transm.* 40, 2004, 3-17.

[11] E. M. Gabidulin, N. I. Pilipchuk, Correcting of rank erasures by symmetrization and information sets, *Proc. Ninth Intern. Workshop ACCT*, 2004, Kranevo, Bulgaria, 333-337.

[12] E. M. Gabidulin, N. I. Pilipchuk, Symmetric matrices and codes correcting rank errors beyond the $\lfloor \frac{d-1}{2} \rfloor$ bound, *Discr. Appl. Math.* 154, 2006, 305-312.

[13] A. Kshevetskiy, Information set decoding for codes in rank metric, *Proc. Ninth Intern. Workshop ACCT*, 2004, Kranevo, Bulgaria, 254-259.

[14] N. I. Pilipchuk, E. M. Gabidulin, Decoding of symmetric rank codes by information sets, *Proc. Tenth Intern. Workshop ACCT*, 2006, Zvenigorod, Russia, 214-219.

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