New systematic easy decoding symmetric rank codes

EERNST GABIDULIN\textsuperscript{1} \hspace{1cm} 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 $2 \times 2$, 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 $2 \times 2$ subblocks wise symmetric. Finally, represent the $2^s \times 2^s$ code matrix as $2 \times 2$ 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

\[ V_1(x_1, x_2) = \begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 + x_2 \end{pmatrix}, \]

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

\textsuperscript{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

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

(1.2)

$$= \left( \begin{array}{cc} V_1(x_1, x_2) & V_1(x_3, x_4) \\ V_1(x_3, x_4) & V_1(x_1, x_2) + \Gamma_1 V_1(x_3, x_4) \end{array} \right),$$

where $x_1, x_2, x_3, x_4$ are information bits. The matrix $\Gamma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ 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

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

(1.3)

where $x_1, \ldots, x_{N_{s-1}}, x_{N_{s-1} + 1}, \ldots, x_{N_s}$ are information bits. The matrix $\Gamma_{s-1}$ of size $N_{s-1} \times N_{s-1}$ is calculated using the previous matrix $\Gamma_{s-2}$. 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 $F_{2^n}^m$ be a normalized vector space of dimension $n$ over $F_{2^n}$.

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

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

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

$$m = (m_1, m_2, \ldots, m_n) = gM = (g_1, g_2, \ldots, g_n)M,$$

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

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

2.3 Self-orthogonal bases

Let

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

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

$$G = \begin{bmatrix}
g_1 & g_2 & \cdots & g_n \\
g_1[1] & g_2[1] & \cdots & g_n[1] \\
\vdots & \vdots & \ddots & \vdots \\
g_1[n-1] & g_2[n-1] & \cdots & g_n[n-1]
\end{bmatrix}.$$ (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 $G_n$ is non singular.

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

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

$$G^T G = I_n,$$

where $G^T$ is the transpose of $G$ and $I_n$ is the identity matrix of order $n$. 
Definition 3 A basis \( g = (g_1, g_2, \ldots, g_n) \) is called a **self-orthogonal** basis if
\[
GG^T = I_n,
\]
It is clear that a self-dual basis is also a self-orthogonal basis, and vice versa.

Definition 4 A basis \( g = (g_1, g_2, \ldots, g_n) \) is called a **weak self-orthogonal** basis if
\[
GG^T = B,
\]
where \( B \) is a diagonal matrix in \( F_2^n \), but not multiple of the identity matrix \( I_n \).

Note that a weak self-orthogonal basis is not a self-dual basis. For example, let \( G = \begin{pmatrix} 1 & \gamma \\ \gamma & 1 \end{pmatrix} \), where \( \gamma \) is a primitive element of \( F_2^2 \). Then \( GG^T = \begin{pmatrix} \gamma & 0 \\ 0 & \gamma \end{pmatrix} \). Hence the basis \((1, \gamma)\) is the weak self-orthogonal one. On the other hand we have \( G^T G = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \). Hence the basis \((1, \gamma)\) is not self-dual.

2.4 One-dimensional rank codes

Let \( g = (g_1, g_2, \ldots, g_n) \) 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 \( \gamma = x_1 g_1 + x_2 g_2 + \cdots + x_n g_n \), where coefficients \( x_j \in F_2 \) are called information bits of \( \gamma \).

On the other hand, the vector \( g = (g_1, g_2, \ldots, g_n) \) 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 \( \{g_s = \alpha^s g_1, g_2, \ldots, g_n\}, s = 0, 1, \ldots, 2^n - 2 \} \), where \( \alpha \) is a primitive element of \( F_2^n \). In terms of the primitive element \( \alpha \) the vector \( g \) can be rewritten as \( g = (\alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_n}) \), where \( i_1, i_2, \ldots, i_n \) are some integers.

Find the matrix representation \( M_1 \) of the vector code \( \mathcal{V}_1 \). Consider the matrix representation of the vector \( \alpha g \):
\[
\alpha g = g A^s, \quad s = 0, 1, \ldots, 2^n - 2.
\]

Therefore the rank-metric matrix code \( \mathcal{M}_1 \) consists of the all zero matrix \( \mathbf{0} \) and code matrices \( \{A^s \mid s = 0, 1, \ldots, 2^n - 2\} \).
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 \( g = (g_1, g_2, \ldots, g_n) \) 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 \( F_{q_s} \):
\[
g(N_s) = (g_1, g_2, \ldots, g_{N_s}) \quad (2.8)
\]

Choose in the superfield \( F_{q_s+1} \) an element \( f_{N_s+1} \) of order \( q_s + 1 \). Construct the vector
\[
g(N_{s+1}) = (g_1, g_2, \ldots, g_{N_s}, g_{N_s+1}, g_{N_s+2}, \ldots, g_{N_{s+1}}), \quad (2.9)
\]
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 \( g(N_{s+1}) \) is a weak self-orthogonal basis for the field \( F_{q_{s+1}} \).

**Proof.** Let \( G(N_s) \) be the associated matrix of the vector \( g(N_s) \):
\[
G(N_s) = \begin{bmatrix}
g_1 & g_2 & \cdots & g_{N_s} \\
g_1^{[1]} & g_2^{[1]} & \cdots & g_{N_s}^{[1]} \\
g_1^{[2]} & g_2^{[2]} & \cdots & g_{N_s}^{[2]} \\
\vdots & \vdots & \ddots & \vdots \\
g_1^{[N_s-1]} & g_2^{[N_s-1]} & \cdots & g_{N_s}^{[N_s-1]}
\end{bmatrix}
\]

We have \( G(N_s)G(N_s)^T = A \), where \( A \) is a diagonal matrix.

It is easy to show that the associated matrix \( G(N_{s+1}) \) of the vector \( g(N_{s+1}) \) is of the form
\[
G(N_{s+1}) = \begin{bmatrix}
G(N_s) & FG(N_s) \\
G(N_s) & F^{q_s}G(N_s)
\end{bmatrix}, \quad (2.10)
\]
where \( F = \text{diag}[f_{N_s+1}, f_{N_s+1}^{[1]}, \ldots, f_{N_s+1}^{[N_s-1]}] \) is the diagonal matrix. Note that \( F^{q_{s+1}} = I_{N_s} \).
By Viète theorem, we have
\[ g(N_s) = \prod_{i=1}^{s} (x - \alpha_i), \]
where \( \alpha_i \) are the roots of \( g(N_s) \) over \( \mathbb{F}_q \). Consider the polynomial
\[ f_s(x) = x^2 + xg_N + 1. \]
This polynomial is irreducible over the field \( \mathbb{F}_q \). Moreover, the order of roots is \( q_s + 1 \).

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

**Proof.** Consider the polynomial \( r(x) = f_s(xg_N) = g_N^{2m}(x^2 + x + g_N^{2m}) = g_N^{2m}(x^2 + x + g_N) \). This polynomial is irreducible over \( \mathbb{F}_q \) because \( \text{Tr}_{\mathbb{F}_q}(g_N) = 1 \). So is the polynomial \( f_s(x) \). Further, by \( f_{N,s+1} \) denote a root of \( f_s(x) \). Another root is \( f_{N,s+1}^q \). We have by Viète theorem \( f_{N,s+1} \cdot f_{N,s+1}^q = f_{N,s+1} = 1 \), or, \( \text{ord}(f_{N,s+1}) = q_s + 1 \).

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

**Lemma 3** \( \text{Tr}_{\mathbb{F}_{q_{s+1}}}(g_{N_{s+1}}) = 1 \).

**Proof.** By definition, we have
\[ f_{N,s+1}^2 + f_{N,s+1}g_N + 1 = 0, \]
where \( m = 2^{N_s} - 1 \). Multiply this equation by \( g_N^2 \). We obtain
\[ g_{N_{s+1}}^2 + g_{N_{s+1}}g_N^{2^{N_s} - 1} + g_N^2 = 0. \]
By Viète theorem, \( g_{N_{s+1}} + g_N^{2^{N_s} - 1} = g_N^{2^{N_s}} \). Hence \( \text{Tr}_{\mathbb{F}_{q_s}}(g_{N_{s+1}} + g_N^{2^{N_s} - 1}) = \text{Tr}_{\mathbb{F}_{q_s}}(g_N^{2^{N_s} - 1}) = \text{Tr}_{\mathbb{F}_{q_s}}(g_N) = 1 \). On the other hand,
\[ \text{Tr}_{\mathbb{F}_{q_s}}(g_{N_{s+1}} + g_N^{2^{N_s} - 1}) = \sum_{i=0}^{N_{s+1} - 1} (g_{N_{s+1}} + g_N^{2^i}) = \sum_{i=0}^{N_{s+1} - 1} g_{N_{s+1}}^{2^i} = \text{Tr}_{\mathbb{F}_{q_{s+1}}}(g_{N_{s+1}}). \]
Example 1  For \( s = 1, N_1 = 2 \), a weak self-orthogonal basis is

\[
g(N_1) = (g_1, g_2) = (1, g_2),
\]

(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

\[
g(N_2) = (g_1, g_2, g_3, g_4) = (1, g_2, f_3, f_3 g_2),
\]

(2.15)

where \( g_3 = f_3 \) is a root of the polynomial \( f_1(x) = x^2 + x g_2 + 1 \) and \( \text{Tr}_{F_{q^2}}(g_4) = \text{Tr}_{F_{q^2}}(f_3 g_2) = 1 \).

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

\[
g(N_3) = (g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8) = (1, g_2, g_3, g_4, f_5, f_5 g_2, f_5 g_3, f_5 g_4),
\]

(2.16)

where \( g_5 = f_5 \) is a root of the polynomial \( f_2(x) = x^2 + x g_7 + 1 \) and \( \text{Tr}_{F_{q^3}}(g_8) = \text{Tr}_{F_{q^3}}(f_5 g_4) = 1 \).

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 \( [\; B \; O \;] \).

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

\[
I_{N_1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad G_2(N_1) = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.
\]

(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

\[
I_{N_2} = \begin{bmatrix} I_{N_1} & O_{N_1} \\ O_{N_1} & I_{N_1} \end{bmatrix}, \quad G_2(N_2) = \begin{bmatrix} G_2(N_1) & O_{N_1} \\ O_{N_1} & G_2(N_1) \end{bmatrix},
\]

(2.18)

\[
G_3(N_2) = \begin{bmatrix} O_{N_1} & I_{N_1} \\ I_{N_1} & G_2(N_1) \end{bmatrix}, \quad G_4(N_2) = \begin{bmatrix} O_{N_1} & G_2(N_1) \\ G_2(N_1) & G_2(N_1)^2 \end{bmatrix}.
\]

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

\[
I_{N_3} = [I_{N_2} \ O_{N_2}], \ G_2(N_3) = [G_2(N_2) \ O_{N_2} \ G_2(N_2)],
\]

\[
G_3(N_3) = [G_3(N_2) \ O_{N_2} \ G_3(N_2)], \ G_4(N_3) = [G_4(N_2) \ O_{N_2} \ G_4(N_2)],
\]

\[
G_5(N_3) = [O_{N_2} \ I_{N_2} \ G_5(N_2)], \ G_6(N_3) = [G_6(N_2) \ G_6(N_2)^T G_2(N_2)],
\]

\[
G_7(N_3) = [O_{N_2} \ G_7(N_2) \ G_7(N_2)], \ G_8(N_3) = [O_{N_2} \ G_8(N_2)^T].
\]

The corresponding code matrix is given by

\[
V_3(x_1, \ldots, x_8) = \begin{pmatrix} V_2(x_1, \ldots, x_4) \\ V_2(x_5, \ldots, x_8) \\ V_2(x_1, \ldots, x_4) + \Gamma_2 V_2(x_5, \ldots, x_8) \end{pmatrix}, \quad (2.20)
\]

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 \( V_s(x_1, \ldots, x_{N_s}) \) 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 \( Y = V_s(x_1, \ldots, x_{N_s}) + E \) and rank(\( E \)) = \( t \leq N_{s-1} - 1 \), 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 \( \begin{pmatrix} E_{11} & E_{12} \\ E_{21} & E_{22} \end{pmatrix} \). Then

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

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 \( V_{s-1}(x_1 \ldots x_{N_{s-1}}) \) depending only on half information variables \( x_1, \ldots, x_{N_{s-1}} \). It satisfies conditions from Eq. \( (3.21) \):

\[
\begin{align*}
V_{s-1}(x_1 \ldots x_{N_{s-1}}) + E_{11} &= Y_{11}, \\
V_{s-1}(x_1 \ldots x_{N_{s-1}}) + E_{22} + \Gamma_{s-1} E_{12} &= Y_{22} + \Gamma_{s-1} Y_{12}, \\
V_{s-1}(x_1 \ldots x_{N_{s-1}}) + E_{22} + \Gamma_{s-1} E_{21} &= Y_{22} + \Gamma_{s-1} Y_{21}.
\end{align*} \quad (3.22)
\]
Similarly, the code submatrix \( V_{s-1}(x_{N_s-1+1} \ldots x_{N_s}) \) satisfies conditions

\[
\begin{align*}
V_{s-1}(x_{N_s-1+1} \ldots x_{N_s}) + E_{12} & = Y_{12}, \\
V_{s-1}(x_{N_s-1+1} \ldots x_{N_s}) + E_{21} & = Y_{21}, \\
V_{s-1}(x_{N_s-1+1} \ldots x_{N_s}) + E_{11} + \Gamma_{s-1}^{-1}E_{22} & = Y_{11} + \Gamma_{s-1}^{-1}Y_{22}.
\end{align*}
\] (3.23)

If \[ \min\{\text{rank}(E_{12}), \text{rank}(E_{21}), \text{rank}(E_{22} + \Gamma_{s-1}E_{21})\} \leq N_s - 2 - 1 \] and \[ \min\{\text{rank}(E_{11}), \text{rank}(E_{22} + \Gamma_{s-1}E_{12}), \text{rank}(E_{11} + \Gamma_{s-1}^{-1}E_{22})\} \leq N_s - 2 - 1, \] then decoding will be successful.

Note that \( \text{rank}(E) \) of the original error matrix may be greater than \( N_s - 1 \). Hence the symmetry of a code matrix \( V_s(x_1 \ldots x_{N_s}) \) 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

\[
E = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0
\end{pmatrix}
\]

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

\[
E = \begin{pmatrix}
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}
\]

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


