# Correcting Erasures and Errors in Random Network Coding

Ernst M. Gabidulin and Nina I. Pilipchuk
Department of Radio Engineering
National Research University MIPT
Moscow, Russia
Email: {ernst.gabidulin, pilipchuk.nina}@gmail.com

Martin Bossert
Telecommunications and Applied Information Theory
University of Ulm
Ulm, Germany
Email: martin.bossert@uni-ulm.de

***Abstract*— Rank-metric codes in matrix representation are used by Koetter, Kschischang, Silva in their theory of random network coding. They showed that the decoding procedure can be reduced to decoding of rank codes. In this paper, we analyzed situations under different conditions at the decoder and establish if there are errors only or some type of mixture of errors and erasures. For correcting we used Gabidulin decoding algorithms. In many situations this analysis helps to choose a suitable algorithm and to eliminate some of computing operations. An example is given.**

***Keywords*— *matrix rank code; vector rank code; random rank error; rank row erasure; rank column erasure; network coding; fast decoding algorithm.***

## I. Introduction

We consider Koetter, Kschischang, Silva random network codes [1] – [4]. The code construction is based on rank-metric codes in matrix representation [5] and the decoding procedure can be reduced to decoding Gabidulin rank codes.

Our aim is to show that it is possible to eliminate some computation operations at the decoding procedure if preliminary to analyze code matrix parameters at the receiver side. In this case, we know what a specific situation occurs: there are errors only or a definite type of errors and erasures. We can recomend to use a suitable decoding algorithm. In many situations it allows to eliminate some of computing operations, hence, to decrease complexity.

Gabidulin's fast decoding algorithms for rank codes were proposed in [5], [6]. The notions "rank column erasures" and "rank row erasures" were introduced in [7], as well as the first fast algorithm for the simultaneous correcting random rank errors and rank erasures. New algorithms were proposed for generalized erasures in [8], [9], [10]. Independently, the algorithms for the simultaneous correcting random rank errors and generalized rank erasures were proposed in [1]-[4] in connection with the random network coding. Let us remark that in these papers generalized row erasures and generalized column erasures are called "erasures" and "deviations" correspondingly.

The paper is constructed as follows. In Section II, we give main notations, definitions and remind some results concerning rank metric codes. In Section III, we refer to Köetter, Kschischang, Silva network codes to present their communication network model and lifting construction of the code. In Section IV, we present our way of preliminary transformations. It is similar to the approach of the paper [2]. It follows to the same construction of the received code matrix and does not pretend to look as a new result. Here, we prove two lemmas, one of them is about a low bound of error rank, another is about an auxiliary invertible matrix. In Sections V, we analyze different situations at the decoder and recommend a suitable decoding algorithm. The rank decoding algorithm for the most difficult situation is demonstrated by an example. Section VI concludes the paper.

## II. Rank metric and rank codes

Let $\mathbb{F}_q$ be a finite field of $q$ elements and $\mathbb{F}_{q^n}$ an extension field of degree $n$. Let $\mathbb{F}_q^{n\times m}$ be the set of $n \times m$ matrices over $\mathbb{F}_q$.

We denote by $\mathbb{F}_q^{n\times m}$ the set of $n \times m$ *matrices* over the field $\mathbb{F}_q$. We denote by $\mathbb{F}_{q^n}^m$ the set of *vectors* with length $m$ over the extension field $\mathbb{F}_{q^n}$. There exists a one-to-one correspondence between $\mathbb{F}_{q^n}^m$ and $\mathbb{F}_q^{n\times m}$. For a chosen basis of the extension field $\mathbb{F}_{q^n}$ over the base field $\mathbb{F}_q$, replace each coordinate $v_i$ in a vector $\mathbf{v} \in \mathbb{F}_{q^n}^m$ by the $n$-column of coefficients in $\mathbb{F}_q$ representing this element. It gives a matrix $\mathbf{M} \in \mathbb{F}_q^{n\times m}$ corresponding to $\mathbf{v}$.

The *rank norm* of a matrix $\mathbf{M} \in \mathbb{F}_q^{n\times m}$ is defined as the ordinary algebraic rank $\rho(\mathbf{M})$ of $M$. The *rank distance* between two conformed matrices $\mathbf{M}_1$ and $\mathbf{M}_2$ is defined as the rank of their difference: $d_{\rm rank}(\mathbf{M}_1, \mathbf{M}_2) = \rho(\mathbf{M}_1 - \mathbf{M}_2)$.

The *rank norm* $\rho(\mathbf{v} \mid \mathbb{F}_q)$ of a vector $\mathbf{v} \in \mathbb{F}_{q^n}^m$ is defined as the minimal number of coordinates $v_i$ of $\mathbf{v}$ which are linearly independent over the base field $\mathbb{F}_q$. The *rank distance* between two vectors $\mathbf{v}_1$ and $\mathbf{v}_2$ is defined as the rank of their difference: $d_{\rm rank}(\mathbf{v}_1, \mathbf{v}_2) = \rho(\mathbf{v}_1 - \mathbf{v}_2)$.

A *matrix code* $\mathcal{M}$ is defined to be any subset of the set of $n \times m$ matrices $\mathcal{M} \subseteq \mathbb{F}_q^{n\times m}$. For any code $\mathcal{M}$, the *code rank distance* $d(\mathcal{M}) = d_r$ is defined by $d_r = \min(\rho(\mathbf{M}_1 - \mathbf{M}_2) : \ \mathbf{M}_1, \mathbf{M}_2 \in \mathcal{M};\ \mathbf{M}_1 \neq \mathbf{M}_2)$. It is clear, that $d_r \leq \min\{n, m\}$.

A *vector code* $\mathcal{V}$ is defined to be any subset of the set of vectors $\mathcal{V} \subseteq \mathbb{F}_{q^n}^m$ with length $m$. For any code $\mathcal{V}$, the *code rank distance* $d(\mathcal{V}) = d_r$ is defined by $d_r = \min(\rho(\mathbf{v}_1 - \mathbf{v}_2 \mid \mathbb{F}_q) : \ \mathbf{v}_1, \mathbf{v}_2 \in \mathcal{M};\ \mathbf{v}_1 \neq \mathbf{v}_2)$. It is clear, that $d_r \leq \min\{n, m\}$. The one-to-one correspondence mentioned above allows to construct a matrix code $\mathcal{M}$ using a given vector code $\mathcal{V}$. Conversely, given a matrix code $\mathcal{M}$ one can construct a vector code $\mathcal{V}$ with the same

metric properties. It is clear, that $|\mathcal{M}| = |\mathcal{V}|$. The vector representation is useful for rank code constructions and for the description of decoding algorithms (see, [5]). The matrix representation is useful for the code modulation theory, for the space-time coding theory [11], and for random network coding [2]. For a given $d_r$, the cardinality of any matrix code $\mathcal{M}$, respectively, of the corresponding vector code $\mathcal{V}$, satisfies the Singleton-style bound [5]:

$$\log_q |\mathcal{M}| = \log_q |\mathcal{M}| \leq mn - (d_r - 1)\max\{n, m\}.$$

Codes reaching this bound are called *maximum rank distance* codes, or, MRD codes. First linear *matrix* MRD codes were constructed in [12]. First linear *vector* MRD codes and associated *matrix* codes were proposed in [5].

Let a code matrix $\mathbf{M}$ of a code $\mathcal{M}$ with distance $d_r$ be transmitted through a channel. Let $\mathbf{Y} = \mathbf{M}+\mathbf{E}$ be a received matrix, where $\mathbf{E}$ is a matrix of errors. An error is to be correctable, if one can recover uniquely a code matrix $\mathbf{M}$ from the received matrix $\mathbf{Y}$.

Sorts of correctable errors depend on a priory knowledge on the structure of $\mathbf{E}$. Assume, there is no knowledge. Call $\mathbf{E}$ a random rank error, denote by $\mathbf{E}_{\rm rand}$ and represent as $\mathbf{E}_{\rm rand} = \mathbf{TU}$, where a matrix $\mathbf{T}$ is a full rank $n \times t$ matrix over $\mathbb{F}_q$ ***unknown*** to the decoder; a matrix $\mathbf{U}$ is a full rank $t \times m$ matrix over $\mathbb{F}_q$ ***unknown*** to the decoder; the rank $t$ of matrices $\mathbf{E}_{\rm rand}$, $\mathbf{T}$, $\mathbf{U}$ is ***unknown*** to the decoder. A random rank error $\mathbf{E}_{\rm rand}$ is a correctable matrix of errors, if $2t \leq d_r - 1$. Correcting random rank errors is fulfilled in the vector mode by converting a matrix $\mathbf{Y} \in \mathbb{F}_q^{n\times m}$ into a vector $\mathbf{y} \in \mathbb{F}_{q^n}^m$ ( [5], [6]).

A matrix of errors is called an erasure, if there exists a side information on the error at the receiver. A matrix of errors denoted $\mathbf{E}_{\rm row}$ is called a rank row erasure if it is of the form $\mathbf{E}_{\rm row} = \mathbf{AR}$, where a matrix $\mathbf{A}$ is a full rank $n\times v$ matrix ***known*** to the decoder; a matrix $\mathbf{R}$ is a full rank $v\times m$ matrix ***unknown*** to the decoder; the row erasure rank $v$ is ***known*** to the decoder. A matrix $\mathbf{E}_{\rm row}$ is a correctable row erasure matrix, if $v \leq d_r - 1$.

A matrix of errors denoted $\mathbf{E}_{\rm col}$ is called a rank column erasure if it is of the form $\mathbf{E}_{\rm col} = \mathbf{WC}$, where a $n \times l$ matrix $\mathbf{W}$ is ***unknown*** to the decoder; the $l \times m$ matrix $\mathbf{C}$ is ***known*** to the decoder; the column erasure rank $l$ is ***known*** to the decoder. A matrix $\mathbf{E}_{\rm col}$ is a correctable column erasure matrix, if $l \leq d_r - 1$.

In general, a matrix $\mathbf{E}$ can be represented in the form

$$\mathbf{E} = \mathbf{E}_{\rm rand} + \mathbf{E}_{\rm row} + \mathbf{E}_{\rm col}.$$

It is a correctable matrix of errors, if the following condition is satisfied [7], [2]:

$$2t + v + l \leq d_r - 1.$$

## III. Kötter–Kschischang–Silva Codes

### A. Communication network model

Consider a communication network, where a single source transmits information to a single destination. The source formats the information to be transmitted into $n$ packets $X_1, \ldots, X_n$ of length $n + m$ over the finite field $\mathbb{F}_q$ and constructs a $(n \times (n + m))$ matrix $\mathbf{X}$ with these packets as rows. In the Kötter–Kschischang–Silva model ([1], [2]) the row spanned subspace of $\mathbf{X}$ is considered as the message. Therefore the matrix $\mathbf{X}$ can be treated as a generator matrix of the subspace.

Each intermediate node calculates random linear combinations of ingoing packets, where a packet is represented as an element of a finite field $\mathbb{F}_{q^{n+m}}$. The node retransmits randomly calculated packets. Therefore, the destination collects a random number $n_r$ of packets $Y_1, \ldots, Y_{n_r}$ of length $n+m$ and creates a $(n_r \times (n+m))$ matrix $\mathbf{Y}$. The number $n_r$ of received packets can be less than, equal to or greater than the number $n$ of transmitted packets. The problem is to recover the original packets $X_1, \ldots, X_n$ or the matrix $\mathbf{X}$ from the received matrix $\mathbf{Y}$. The transmitted matrix $\mathbf{X}$ and the received matrix $\mathbf{Y}$ are related by the equation

$$\mathbf{Y} = \mathbf{AX} + \mathbf{E}_{\rm out}, \tag{1}$$

where $\mathbf{A}$ is an $n_r \times n$ matrix corresponding to the overall linear transformation applied by intermediate nodes of the network. In general, the matrix $\mathbf{A}$ introduces an *inner* corruptions of the transmitted matrix $\mathbf{X}$. A matrix $\mathbf{E}_{\rm out}$ is an *outer* $n_r \times (n + m)$ matrix of errors. For example, it can be created by Byzantine intruders inside the network introducing error packets $z_1, \ldots, z_l$ of length $n + m$ each. They can be considered as rows of a $l \times (n + m)$ matrix $\mathbf{Z}$. Later, on route to the destination, the overall linear transformation applied to $z_1, \ldots, z_l$ are described by a $n_r \times l$ matrix $\mathbf{B}$. In this case, the outer matrix of errors is the matrix $\mathbf{E}_{\rm out} = \mathbf{BZ}$ with rank $l$, where $\mathbf{B}$ is $n_r \times l$ matrix. In wireless networks, a matrix $\mathbf{E}_{\rm out}$ can appear from a special noise source outside of the network. If its rank is equal to $l$, it can be still represented as $\mathbf{BZ}$ simulating the previous model. The relation (1) is the basic model, it is called random network coding channel (RNCC) [2].

### B. Lifting construction of the network code

Let $\mathcal{M}$ be a matrix code consisting of matrices $\mathbf{M}$ of size $n \times m$.

A lifting construction network code $\mathcal{C}$ is a set of the generator matrices $\mathcal{X}$ of the form

$$\mathcal{X} = \left\{\mathbf{X} : \mathbf{X} = \begin{bmatrix}\mathbf{I}_n & \mathbf{M}\end{bmatrix}\right\},$$

where $\mathbf{I}_n$ is the identity matrix of order $n$ while $\mathbf{M}$ is a code matrix.

In [2], it is proposed to use rank-metric Gabidulin codes in the matrix representation as $\mathcal{M}$. We denote such a code in the lifting construction as a KKS lifting code.

Assume that a source uses a KKS lifting code $\mathcal{X}$ and transmits a matrix $\mathbf{X} = \begin{bmatrix}\mathbf{I}_n & \mathbf{M}\end{bmatrix}$. At the destination side a matrix

$$\mathbf{Y} = \mathbf{AX} + \mathbf{E}_{\rm out}$$

is received, where $\mathbf{A}$ is a random $n_r \times n$ matrix, $\mathbf{E}_{\text{out}}$ is a $n_r \times (n+m)$ matrix of errors. Represent $\mathbf{AX}$ and $\mathbf{E}_{\text{out}}$ as

$$\begin{aligned}\mathbf{AX} &= \begin{bmatrix}\mathbf{A} & \mathbf{AM}\end{bmatrix},\\ \mathbf{E}_{\text{out}} &= \begin{bmatrix}\mathbf{E}_1 & \mathbf{E}_2\end{bmatrix},\end{aligned}$$

where $\mathbf{E}_1$ and $\mathbf{E}_2$ are matrices of sizes $n_r \times n$ and $n_r \times m$, respectively. Then

$$\mathbf{Y} = \begin{bmatrix}\mathbf{A}+\mathbf{E}_1 & \mathbf{AM}+\mathbf{E}_2\end{bmatrix} = \begin{bmatrix}\mathbf{Y}_1 & \mathbf{Y}_2\end{bmatrix}. \quad (2)$$

The problem is to recover the matrix $\mathbf{M}$. It is assumed that the received matrix $\mathbf{Y}$ has rank $n_r$.

## IV. Preliminary transformations

Let rank $\rho(\mathbf{Y}_1) = r \le \min\{n_r, n\}$ and rank $\rho(\mathbf{E}_{\text{out}}) = l$. Since $\mathbf{A} = \mathbf{Y}_1 - \mathbf{E}_1$, rewrite Eq. (2) as

$$\mathbf{Y} = \begin{bmatrix}\mathbf{Y}_1 & \mathbf{Y}_1\mathbf{M} - \mathbf{E}_1\mathbf{M} + \mathbf{E}_2\end{bmatrix}. \quad (3)$$

Apply to the matrix $\mathbf{Y}$ those linear transformations which corresponds Gauss' elimination procedure applied to the matrix $\mathbf{Y}_1$. There exists the unique non singular $n_r \times n_r$ matrix $\mathbf{S}$ which transforms the matrix $\mathbf{Y}_1$ to the reduced row echelon form. Multiply both sides of Eq. (3) to the left by the matrix $\mathbf{S}$:

$$\begin{aligned}\mathbf{SY} &= \begin{bmatrix}\mathbf{SY}_1 & \mathbf{SY}_1\mathbf{M} - \mathbf{SE}_1\mathbf{M} + \mathbf{SE}_2\end{bmatrix}\\ &= \begin{bmatrix}\mathbf{G} & \mathbf{R}\\ \mathbf{0} & \mathbf{C}\end{bmatrix},\end{aligned} \quad (4)$$

where $\mathbf{G}$ is the $r \times n$ matrix with leading "1"'s in each row and $\mathbf{O}$ is the all zero $(n_r - r) \times n$ matrix.

The matrix $\mathbf{R} = \mathbf{GM} + \mathbf{S}_1(-\mathbf{E}_1\mathbf{M} + \mathbf{E}_2)$ and the matrix $\mathbf{C} = \mathbf{S}_2(-\mathbf{E}_1\mathbf{M} + \mathbf{E}_2)$ are known, rank $(\mathbf{C})$ is known: $\rho(\mathbf{C}) = n_r - r$. The matrix $\mathbf{S}_1$ consists of the $r$ upper rows of $\mathbf{S}$. The matrix $\mathbf{S}_2$ consists of the $n_r - r$ last rows of $\mathbf{S}$.

*Lemma 1:* The following inequality is valid:

$$n_r - r \le l. \quad (5)$$

*Proof:* We have

$$\begin{aligned}\rho(\mathbf{C}) = n_r - r &= \rho(\mathbf{S}_2(-\mathbf{E}_1\mathbf{M} + \mathbf{E}_2))\\ &\le \min\{\rho(\mathbf{S}_2), \rho(-\mathbf{E}_1\mathbf{M} + \mathbf{E}_2)\}.\end{aligned}$$

Since $\rho(\mathbf{S}_2) = n_r - r$, it follows

$$\rho(\mathbf{S}_2) \le \rho(-\mathbf{E}_1\mathbf{M} + \mathbf{E}_2) \le l.$$

■

Represent the matrix $\mathbf{E}_{\text{out}}$ as

$$\mathbf{E}_{\text{out}} = \mathbf{BZ}, \quad (6)$$

where $\mathbf{B}$ is a $n_r \times l$ matrix of rank $l$ and $\mathbf{Z}$ is a $l \times (n+m)$ matrix of rank $l$. This representation is not unique.

*Lemma 2:* There exists a representation (6) with $\mathbf{B} = \begin{bmatrix}\mathbf{B}_1 & \mathbf{B}_2\end{bmatrix}$, where $\mathbf{B}_1$ is a $n_r \times (n_r - r)$ submatrix of rank $n_r - r$, $\mathbf{B}_2$ is a $n_r \times (l - n_r + r)$ submatrix of rank $l - n_r + r$, such that the square matrix $\mathbf{T} = \mathbf{S}_2\mathbf{B}_1$ of order $n_r - r$ is invertible.

*Proof:* The matrix $\mathbf{S}_2\mathbf{B}$ has size $(n_r - r) \times l$ and should have rank $n_r - r$. Otherwise the rank of $\mathbf{C}$ would be strictly less than $n_r - r$. Hence there exist $n_r - r$ columns $\mathbf{H} = \begin{bmatrix}\mathbf{b}_{j_1} & \mathbf{b}_{j_2} & \dots & \mathbf{b}_{j_{n_r - r}}\end{bmatrix}$ of $\mathbf{B}$ such that $\mathbf{S}_2\mathbf{L}$ is a invertible matrix. One can move these columns to the first $n_r - r$ places choosing a suitable matrix $\mathbf{V}$. Thus $\mathbf{B}_1 = \mathbf{H}$ and $\mathbf{T} = \mathbf{S}_2\mathbf{B}_1$ is invertible. ■

We have also $\mathbf{E}_1 = \mathbf{BZ}_1$, $\mathbf{E}_2 = \mathbf{BZ}_2$, where $\mathbf{Z} = \begin{bmatrix}\mathbf{Z}_1 & \mathbf{Z}_2\end{bmatrix}$. Rewrite the matrix $-\mathbf{E}_1\mathbf{M} + \mathbf{E}_2$ as

$$\begin{aligned}-\mathbf{E}_1\mathbf{M} + \mathbf{E}_2 &= \mathbf{B}(-\mathbf{Z}_1\mathbf{M} + \mathbf{Z}_2)\\ &= \mathbf{B}_1\mathbf{W}_1 + \mathbf{B}_2\mathbf{W}_2.\\ -\mathbf{Z}_1\mathbf{M} + \mathbf{Z}_2 &= \begin{bmatrix}\mathbf{W}_1\\ \mathbf{W}_2\end{bmatrix}.\end{aligned}$$

The relation (4) can be rewritten as

$$\mathbf{SY} = \begin{bmatrix}\mathbf{G} & \mathbf{GM} + \mathbf{S}_1\mathbf{B}_1\mathbf{T}^{-1}\mathbf{TW}_1 + \mathbf{S}_1\mathbf{B}_2\mathbf{W}_2\\ \mathbf{O} & \mathbf{TW}_1 + \mathbf{S}_2\mathbf{B}_2\mathbf{W}_2\end{bmatrix}. \quad (7)$$

Since $\mathbf{TW}_1 = \mathbf{C} - \mathbf{S}_2\mathbf{B}_2\mathbf{W}_2$, we obtain

$$\mathbf{R} = \mathbf{GM} + \mathbf{S}_1(\mathbf{B}_1\mathbf{T}^{-1})\mathbf{C} - \mathbf{S}_1(\mathbf{B}_1\mathbf{T}^{-1}\mathbf{S}_2 - \mathbf{S}_1)\mathbf{B}_2\mathbf{W}_2). \quad (8)$$

The matrix $\mathbf{R}$ has $r$ rows. It should be extended to $n$ rows by inserting the all zero rows in the specific manner as proposed in [2]. Thus the matrix $\mathbf{R}$ with inserted zero rows is denoted $\widehat{\mathbf{R}}$ etc. We have

$$\widehat{\mathbf{R}} = \widehat{\mathbf{G}}\mathbf{M} + \widehat{\mathbf{S}}_1\mathbf{B}_1\mathbf{T}^{-1}\mathbf{C} - \widehat{\mathbf{S}}_1(\mathbf{B}_1\mathbf{T}^{-1}\mathbf{S}_2 - \mathbf{S}_1)\mathbf{B}_2\mathbf{W}_2). \quad (9)$$

Represent the $n \times n$ matrix $\widehat{\mathbf{G}}$ as

$$\widehat{\mathbf{G}} = \mathbf{I}_n + \mathbf{L},$$

where $\mathbf{L}$ has exactly $n - r$ non zero columns. Denote by $\mathbf{D} = \widehat{\mathbf{S}}_1\mathbf{B}_1\mathbf{T}^{-1}$ and by $\mathbf{E}_{\text{rest}} = -\widehat{\mathbf{S}}_1(\mathbf{B}_1\mathbf{T}^{-1}\mathbf{S}_2 - \mathbf{S}_1)\mathbf{B}_2\mathbf{W}_2)$. The rank of $\mathbf{D}$ is not greater than $\rho(\mathbf{B}_1) = n_r - r$. The rank of $\mathbf{E}_{\text{rest}}$ is not greater than $\rho(\mathbf{B}_2) = l - n_r + r$. Then

$$\widehat{\mathbf{R}} = \mathbf{M} + \mathbf{LM} + \mathbf{DC} + \mathbf{E}_{\text{rest}}. \quad (10)$$

The term $\widehat{\mathbf{R}}$ in the left side of the equation (10) can be interpreted as received matrix as if a code matrix of a rank code is transmitted. The first term $\mathbf{M}$ in the right side corresponds to the transmitted code of a rank code. The second term $\mathbf{LM}$ ($\mathbf{L}$ is known) corresponds to a generalized rank *row erasure* of rank $n - r$. The third term $\mathbf{DC}$ ($\mathbf{C}$ is known) corresponds to a generalized rank *column erasure* of rank $n_r - r$. The fourth term $\mathbf{E}_{\text{rest}}$ corresponds to a random rank error of rank $t = l - n_r + r$.

## V. Analysis and decoding

From now on, we can use rank decoding algorithms [7]-[10]. The matrix $\mathbf{M}$ can be successfully recovered, if the following condition is satisfied ([10]):

$$(n-r)+(n_r-r)+2(l-n_r+r) = 2l+n-n_r \le d_r - 1 \quad (11)$$

First, let us analyze parameters $n, n_r, r, l$ at receiver side. All of them, except $l$, are known. There are the following

relations between them: $n \geq r$, $n_r \geq r$, $l \geq n_r - r$. It gives 4 different cases to use different variants of the rank decoding algorithm.

1) Let be $n_r = n = r$. That means there is no erasure of any types. We use the decoding algorithm which can correct errors only. If $t > 0$, that is $l > n_r - r = 0$, this algorithm corrects errors under condition $2l \leq d_r - 1$. If $t = 0$, that is $l = n_r - r = 0$, the syndrome is all zero component vector, there is no errors.
2) Let be $n_r < n$, $n_r = r$. That means there are row erasures with rank $n - r$, there is no column erasure. We use the decoding algorithm which can correct row erasures and errors under condition $2l + (n - r) \leq d_r - 1$. If $l = n_r - r = 0$, there is no error. If $l > n_r - r = 0$, errors exists.
3) Let be $n_r > n$, $n = r$. That means there are column erasures with rank $n_r - r$. We use the decoding algorithm which can correct column erasures and errors under condition $2l + (n_r - r) \leq d_r - 1$. If $l > (n_r - r)$, errors exist, if $l = (n_r - r)$, there is no error, only column erasures.
4) Let be $n > r$, $n_r > r$. That means there are row erasures with rank $n - r$ and column erasures with rank $n_r - r$. We use the decoding algorithm which can correct both types of erasures and errors under condition (11). If $l = n_r - r$, there is no error, there are row erasures and column erasures only. If $l > n_r - r > 0$, there are errors and both types of erasures.

Hence, the fourth case is the most computable. We show this rank decoding algorithm by an example.

*Example 1:* Let $q = 2$. Construct $(5, 1, d_r = 5)$-rank code using the irreducible polynomial $f(\lambda) = \lambda^5 + \lambda^2 + 1$ with a primitive root $\alpha$. The parity check matrix is

$$H_4 = \begin{bmatrix} \alpha^2 & \alpha^{29} & \alpha^5 & \alpha^{14} & \alpha^9 \\ \alpha^4 & \alpha^{27} & \alpha^{10} & \alpha^{28} & \alpha^{18} \\ \alpha^8 & \alpha^{23} & \alpha^{20} & \alpha^{25} & \alpha^5 \\ \alpha^{16} & \alpha^{15} & \alpha^9 & \alpha^{19} & \alpha^{10} \end{bmatrix}.$$

Choose a code vector

$$g = \begin{bmatrix} \alpha & \alpha^{30} & \alpha^{18} & \alpha^7 & \alpha^{20} \end{bmatrix}.$$

The destination receives the corrupted matrix

$$\begin{aligned} \mathbf{Y} &= \begin{bmatrix} \mathbf{Y}_1 & \mathbf{Y}_2 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}. \end{aligned}$$

First of all, let us analyze the code matrix parameters.

We have $n_r = n = 5, r = 4$, that is $n > r$, $n_r > r$. Hence, there exist row erasures with rank 1, column erasures with rank 1. We know code distance $d_r = 5$, so the equation (11) is valid for $l = 2$. We can correct simultaneously row erasure with rank 1, column erasures with rank 1 and error with rank $t = l - 1 = 1$.

After preliminary transformation we have

$$\widehat{\mathbf{R}} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} = \mathbf{M} + \mathbf{LM} + \widehat{\mathbf{D}}\mathbf{C} + \mathbf{E}_{\text{rest}}, \quad (12)$$

where the matrix $\mathbf{L}$ has all columns, except the last one, with all zero entries, the last column as a vector is $(01001)^T$, the matrix $\mathbf{C}$ is $C = 00100$.

Let us start the decoding procedure corresponding to the fourth case. In consists in the following actions.

- Convert the matrix $\widehat{\mathbf{R}}$ in a vector $y$:

$$y = [\alpha \ \alpha^5 \ \alpha^{12} \ \alpha^{18} \ \alpha^{29}]. \quad (13)$$

- Write down the total error as a sum of its parts:

$$e_{\text{total}} = (e_{\text{rand}} + e_{\text{row}} + e_{\text{col}}), \quad (14)$$

where $e_{\text{rand}} = e_1 u_1$ is random error of rank 1, $e_1$ is an element of the field $F_{2^5}$, $u_1 = [u_{11} \ u_{12} \ u_{13} \ u_{14} \ u_{15}]$ is a vector with five components in the base field $F_2$. Elements $e_1$ and $u_1$ are unknown. We have $e_{\text{row}} = ar_1$, where $a = \alpha^{30}$ corresponds to the last column of the matrix $L$. A vector $r_1 = [r_{11} \ r_{12} \ r_{13} \ r_{14} \ r_{15}]$ is an unknown vector with five components of the base field. We have $e_{\text{col}} = w_1[0\ 0\ 1\ 0\ 0]$, where $w_1$ is an unknown element of the field $F_{2^5}$ and $[0\ 0\ 1\ 0\ 0] = \mathbf{C}$.
- Calculate the main syndrome $Si$ and its parts $Si_{rand}$, $Si_{row}$,$Si_{col}$.

$$\begin{aligned} &Si = yH^T = [\alpha^5 \ \alpha^{28} \ \alpha^3 \ 0] = [Si_0 \ Si_1 \ Si_2 \ Si_3]; \\ &Si_{rand} = e_1 u_1 H^T = e_1 x_1 + e_1 x_1^2 + e_1 x_1^4 + e_1 x_1^8; \\ &Si_{row} = a r_1 H^T = \alpha^{30}\theta_1 + \alpha^{30}\theta_1^2 + \alpha^{30}\theta_1^4 + \alpha^{30}\theta_1^8; \\ &Si_{col} = w_1 C H^T = w_1\gamma_1 + w_1\gamma_1^2 + w_1\gamma_1^4 + w_1\gamma_1^8, \end{aligned} \quad (15)$$

where there are the following notions:

$$\begin{aligned} &x_1 = \alpha^2 u_{11} + \alpha^{29} u_{12} + \alpha^5 u_{13} + \alpha^{14} u_{14} + \alpha^9 u_{15}, \\ &\theta_1 = \alpha^2 r_{11} + \alpha^{29} r_{12} + \alpha^5 r_{13} + \alpha^{14} r_{14} + \alpha^9 r_{15}, \\ &\gamma_1 = \alpha^5. \end{aligned} \quad (16)$$

Get a system of the main syndrome equations by equalizing of the corresponding syndrome components:

$$\begin{aligned} &\alpha^5 = e_1 x_1 + \alpha^{30}\theta_1 + w_1\gamma_1; \\ &\alpha^{28} = e_1 x_1^2 + \alpha^{30}\theta_1^2 + w_1\gamma_1^2; \\ &\alpha^3 = e_1 x_1^4 + \alpha^{30}\theta_1^4 + w_1\gamma_1^4; \\ &0 = e_1 x_1^8 + \alpha^{30}\theta_1^8 + w_1\gamma_1^8, \end{aligned} \quad (17)$$

- Elimination of generalized column erasures.

Introduce the linearized polynomial $\Gamma(x) = \Gamma_0 x + \Gamma_1 x^2$, which roots are $\gamma_1$ and 0. Put $\Gamma_1 = 1$, obtain $\Gamma_0 = \alpha^5$. Construct the matrix

$$\mathbf{\Gamma} = \begin{bmatrix} \Gamma_0 & 0 & 0 \\ \Gamma_1 & \Gamma_0^2 & 0 \\ 0 & \Gamma_1^2 & \Gamma_0^4 \\ 0 & 0 & \Gamma_1^4 \end{bmatrix} = \begin{bmatrix} \alpha^5 & 0 & 0 \\ 1 & \alpha^{10} & 0 \\ 0 & 1 & \alpha^{20} \\ 0 & 0 & 1 \end{bmatrix}.$$

$$\begin{aligned} \widetilde{Si}_0 &= \alpha^{11} = e_1\widetilde{x_1} + \alpha^{30}\widetilde{\theta_1}, \\ \widetilde{Si}_1 &= \alpha^{13} = e_1\widetilde{x_1}^2 + \alpha^{30}\widetilde{\theta_1}^2, \\ \widetilde{Si}_2 &= \alpha^{23} = e_1\widetilde{x_1}^4 + \alpha^{30}\widetilde{\theta_1}^4, \end{aligned} \tag{18}$$

where $\widetilde{x_1} = \Gamma(x_1)$, $\widetilde{\theta_1} = \Gamma(\theta_1)$. Let us raise both sides of this system: raise the first equation to a power $2^n = 2^5$, the second equation to a power $2^{n-1} = 2^4$, the third equation to a power $2^{n-2} = 2^3$. We get the system

$$\begin{aligned} \widetilde{Si}_0 &= \alpha^{11} = e_1\widetilde{x_1} + \alpha^{30}\widetilde{\theta_1}, \\ \widetilde{Si}_1 &= \alpha^{22} = e_1^{16}\widetilde{x_1} + \alpha^{15}\widetilde{\theta_1}, \\ \widetilde{Si}_2 &= \alpha^{23} = e_1^{8}\widetilde{x_1} + \alpha^{16}\widetilde{\theta_1}. \end{aligned} \tag{19}$$

- Elimination of generalized row erasures.
  Introduce the linearized polynomial $V(x) = V_0 x + V_1 x^2$, which roots are $\alpha^{30}$ and 0. Put $V_1 = 1$, obtain $V_0 = \alpha^{30}$. Construct the matrix

$$\mathbf{V} = \begin{bmatrix} V_1^{16} & 0 \\ V_0^{16} & V_1^3 \\ 0 & V_0^8 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \alpha^{15} & 1 \\ 0 & \alpha^{23} \end{bmatrix}.$$

  Multiply each component of the syndrome vector $\widetilde{Si}$ to the left by the matrix $\mathbf{V}$ and get a new modified system of the syndrome equations:

$$\begin{aligned} \widehat{Si}_0 &= \alpha^8 = \widetilde{x_1}\widetilde{e_1}^2, \\ \widehat{Si}_1 &= \alpha^8 = \widetilde{x_1}\widetilde{e_1}, \end{aligned} \tag{20}$$

  where $\widetilde{e_1} = (V(e_1))^8$. The solution of this system is $\widetilde{x_1} = \alpha^8$, $\widetilde{e_1} = 1$. Now, remind $\widetilde{x_1} = \Gamma(x_1)$, $\widetilde{e_1} = (V(e_1))^8$. Get the equations:

$$\begin{aligned} \widetilde{x_1} &= \alpha^8 = x_1^2 + \alpha^5 x_1, \\ \widetilde{e_1} &= 1 = (\alpha^{30}e_1 + e_1^2)^8. \end{aligned} \tag{21}$$

  Take solutions $x_1 = \alpha^{12}$, $e_1 = \alpha^5$, which were obtained by exhaustive search.
  Use the first equation (16) and get $u_1 = [0\ 1\ 0\ 1\ 1]$. The random error in the the vector form is

$$e_{\text{rand}} = e_1 u_1 = \alpha^5[0\ 1\ 0\ 1\ 1].$$

- Let us go to correcting row erasures.
  Use the first equation of the modified syndrome system (19), the obtained values $e_1 = \alpha^5$, $\widetilde{x_1} = \alpha^8$ and obtain $\widetilde{\theta_1} = \alpha^{17}$. Use the notion for $\widetilde{\theta_1} = \Gamma(\theta_1)$ and obtain $\theta_1 = \alpha^7$. Use the notation for $\theta_1$ (16) and obtain the vector $r_1 = [0\ 1\ 0\ 1\ 0]$, hence, $e_{\text{row}} = \alpha^{30}[0\ 1\ 0\ 1\ 0]$.
- To get solution for column erasure use the first equation of the main syndrome system (17) and obtain $w_1 = \alpha^8$. Hence, $e_{\text{col}} = \alpha^8[0\ 0\ 1\ 0\ 0]$.
- After all, collect all parts of the error and erasure and get the total error:

$$e_{\text{total}} = (e_{\text{rand}} + e_{\text{row}} + e_{\text{col}}) = [0\ \alpha^{26}\ \alpha^8\ \alpha^{26}\ \alpha^5].$$

$$\begin{aligned} y + e_{\text{total}} &= (\alpha\ \alpha^5\ \alpha^{12}\ \alpha^{18}\ \alpha^{29}) + (0\ \alpha^{26}\ \alpha^8\ \alpha^{26}\ \alpha^5) \\ &= (\alpha\ \alpha^{30}\ \alpha^{18}\ \alpha^7\ \alpha^{20}) = g. \end{aligned}$$

## VI. Conclusions

The analysis is given, when decoding Kötter–Kschischang–Silva codes can be reduced to correcting only rank erasures, only random rank errors, or, simultaneously rank erasures and random rank errors. Ranks of row erasures as well as column erasures can be found exactly from a received matrix. Lower bound of random error rank can be easily estimated. The conditions for different situations are obtained and a suitable decoding algorithm is proposed.

## References


[1] R. Koetter and F. R. Kschischang, *Coding for errors and erasures in random network coding*, Proc. 2007 IEEE International Symposium on Information Theory (ISIT 2007), Nice, France, 24-29 June 2007, pp. 791-795.

[2] D.Silva, F. R. Kschischang, R. Koetter, *A Rank-Metric Approach to Error Control in Random Network Coding*, IEEE Transactions on Information Theory, vol. 54, pp. 3951-3967, No. 9, Sept. 2008.

[3] D. Silva and F. R. Kschischang, *Fast Encoding and Decoding of Gabidulin Codes*, Proc. of 2009 IEEE International Symposium on Information Theory, ISIT'09, 2009.

[4] D. Silva *Error Control for Network Coding*, PhD Thesis, University of Toronto, 2009.

[5] E.M. Gabidulin, *Theory of Codes with Maximum Rank Distance*, Probl. Inform. Transm., vol. 21, No. 1, pp. 1–12, July, 1985.

[6] E. M. Gabidulin, *A Fast Matrix Decoding Algorithm for Rank-Error-Correcting Codes*, In G. Cohen, S. Litsyn, A. Lobstein, G. Zemor (Eds.) ALGEBRAIC CODING, pp. 126 - 133; Lecture Notes in Computer Science, v. 573, Springer-Verlag, 1991.

[7] E. M. Gabidulin, A.V. Paramonov, O.V. Tretjakov, *Rank Errors and Rank Erasures Correction*, Proceedings of the 4th International Colloquium on Coding Theory, 30 Sept. - 7 Oct. 1991, Dilijan, Armenia, pp. 11-19, Yerevan, 1992.

[8] *Adaptive decoding algorithm of $n, k, d$-rank codes for channels under non Gaussian noise*Proc. of 2007 International Symposium on Communication Theory and Applications, ISCTA-2007.

[9] E. M. Gabidulin and N. I. Pilipchuk, *Error and erasure correcting algorithms for rank codes*, Designs, Codes and Cryptography, Springer Netherlands, DOI 10.1007/s10623-008-9185-7. V.49, 2008, pp.105-122.

[10] E. M. Gabidulin, N. I. Pilipchuk, M. Bossert, *Correcting Generalized Matrix Erasures with Applications to Random Network Coding* // Proc. International ITG Confrence on Source and Channel Coding (SCC'2010). Siegen, Germany. January 18-21, 2010.

[11] E. M. Gabidulin, P. Lusina, M. Bossert, "Maximum Rank Codes as Space-Time Codes," IEEE Trans. Inform. Theory, 2003. Vol. IT–46. No 10. P. 2757-2760.

[12] P. Delsarte, Bilinear Forms over a Finite Field, with Applications to Coding Theory // Journal of Combinatorial Theory A, vol. 25, pp. 226-241, 1978.