ISSN 0032-9460, Problems of Information Transmission, 2013, Vol. 49, No. 1, pp. 40–53. © Pleiades Publishing, Inc., 2013.
Original Russian Text © E.M. Gabidulin, N.I. Pilipchuk, 2013, published in Problemy Peredachi Informatsii, 2013, Vol. 49, No. 1, pp. 46–60.

CODING THEORY

Rank Subcodes in Multicomponent Network Coding[1]

E. M. Gabidulin and N. I. Pilipchuk

Moscow Institute of Physics and Technology (State University)
ernst.gabidulin@gmail.com pilipchuk.nina@gmail.com

Received August 13, 2012; in final form, December 3, 2012

Abstract—A new class of subcodes in rank metric is proposed; based on it, multicomponent network codes are constructed. Basic properties of subspace subcodes are considered for the family of rank codes with maximum rank distance (MRD codes). It is shown that nonuniformly restricted rank subcodes reach the Singleton bound in a number of cases. For the construction of multicomponent codes, balanced incomplete block designs and matrices in row-reduced echelon form are used. A decoding algorithm for these network codes is proposed. Examples of codes with seven and thirteen components are given.

DOI: 10.1134/S0032946013010043

1. INTRODUCTION

Let $\mathbb{K}_q = \mathbb{K}$ be a finite field of q elements. Let $\mathbb{K}^n$ be a fixed n-dimensional space over $\mathbb{K}$. Denote by $\mathcal{P}(n)$ the set of all subspaces of $\mathbb{K}^n$. A subspace V of dimension $k \le n$ consists of q^k vectors of length n over $\mathbb{K}$. It can be considered as a *row spanned* space of some $k \times n$ matrix $M(V)$ over $\mathbb{K}$ of full rank k. There exist many matrices generating the subspace V. If M is such a matrix and T is a nonsingular $k \times k$ matrix over $\mathbb{K}$, then the matrix $\widetilde{M} = TM$ generates the same subspace.

It is known from linear algebra that any matrix can be transformed by elementary row operations (Gaussian elimination) into *row-reduced echelon form*. For a $k \times n$ matrix of rank k, its row-reduced echelon form is as follows:

- In each row *the first nonzero element is* 1. It is called the *leading* element. Thus, all elements before the leading are 0;
- The leading element of a row occurs *to the right* of the leading element of the previous row;
- Each leading element is *the only nonzero* element in its column;
- Other elements of the matrix in row-reduced echelon form can be arbitrary. They are called *free* elements.

Location of leading elements can be described by means of a multiindex $\mathcal{I} = \{i_1, i_2, \ldots, i_k\}$ defined as a set of integers satisfying the condition $1 \le i_1 < i_2 < \ldots < i_k \le n$. The integer i_1 means the number of a column where the leading element of the *first row* is located, i_2 is the number of a column where the leading element of the *second row* is located, etc. All free elements of a matrix in row-reduced echelon form are located in a submatrix of size $k \times (n-k)$. However, the number of free elements depends on a multiindex. The number of *different* subspaces having the *same* multiindex $\mathcal{I} = \{i_1, i_2, \ldots, i_k\}$ is

$$N(i_1, i_2, \ldots, i_k) = q^{kn - \frac{k(k-1)}{2} - (i_1 + i_2 + \ldots + i_k)}.$$

Hereinafter, subspaces will be given by their generator matrices in row-reduced echelon form.

[1] Supported in part by the Russian Foundation for Basic Research, project no. 12-07-00122-a.

The *subspace* (or Grassmann) distance between subspaces U and V in $\mathcal{P}(n)$ is defined as follows:

$$\begin{aligned} d_{\text{sub}}(U,V) &= \dim(U \uplus V) - \dim(U \cap V) \\ &= \dim U + \dim V - 2\dim(U \cap V) \\ &= 2\dim(U \uplus V) - \dim U - \dim V. \end{aligned} \tag{1}$$

In terms of generator matrices, the distance between an m-dimensional subspace U with generator matrix A and a k-dimensional subspace V with generator matrix B is given as

$$d_{\text{sub}}(U,V) = 2\,\text{rank}\begin{pmatrix} A \\ B \end{pmatrix} - m - k. \tag{2}$$

A code with minimum Grassmann distance d and cardinality M is referred to as an $[n, M, d]$ code. A code consists of subspaces $\{V_1, \ldots, V_M\}$ given by their generator matrices $\{X_1, \ldots, X_M\}$, and $\min\limits_{i \neq j} d_{\text{sub}}(V_i, V_j) = d$.

If all subspaces V_i have the same dimension k, then a code is called a *constant-dimension* $[n, M, d, k]$ *code*. In this case the distance $d_{\text{sub}} = 2(m+1)$ is an even integer.

The main problem of network coding theory is constructing $[n, M, d, k]$ and $[n, M, d]$ codes. The following upper bound for $[n, M, d = 2m+2, k]$ codes is known [1]:

$$M \leq \frac{\begin{bmatrix} n \\ k-m \end{bmatrix}}{\begin{bmatrix} k \\ k-m \end{bmatrix}}, \tag{3}$$

where

$$\begin{bmatrix} n \\ s \end{bmatrix} = \frac{(q^n-1)(q^n-q)\ldots(q^n-q^{s-1})}{(q^s-1)(q^s-q)\ldots(q^s-q^{s-1})}.$$

The problem of constructing multicomponent codes containing unions of codes with certain correcting properties attracts attention of many researchers working towards improving the efficiency of communication systems and networks.

A family of network $[n, M, d = 2m+2, k]$ codes was first proposed in [2]. An equivalent class was introduced almost immediately in [3]; now these codes are called SKK codes. All generator matrices of such a code have the same multiindex $\mathcal{I} = \{1, 2, \ldots, k\}$, i.e., start with the identity matrix. Free elements of each code matrix are chosen as $k \times (n-k)$ matrices of a *rank* code [4] with rank distance $d_r = m+1$. This construction is known as the lifting structure of a rank code. The code cardinality is

$$M = \begin{cases} q^{(n-k)(k-m)} & \text{if } 2k \leq n, \\ q^{k(n-k-m)} & \text{if } 2k > n. \end{cases} \tag{4}$$

Network codes of higher cardinality with an SKK code as the first component are well represented in papers of 2008–2011 [5–14]. Research is this direction is being continued (see, e.g., [15]).

In [9], components were added to the code of [2] to increase the cardinality. A formula for the number of codewords was found. However, codes of [9] were found to have smaller cardinality than codes obtained by other constructions (for instance, [7, 11]).

In [10], matrix components with submatrices equivalent to direct products of rank codes of various sizes were added to an SKK code [3].

In a series of papers [11–14], to construct network codes of larger cardinality, an approach was used based on representation of added components as matrices in row-reduced echelon form and

selecting a structure called a Ferrer diagram [16] there. An unsolved problem is constructing a rank code compatible with a selected Ferrer diagram. Iterative encoding and decoding algorithms were proposed exploiting constant-Hamming-weight codes.

In [5,6], matrix components having the all-zero matrix as a prefix were added to an SKK code [3]. A multilevel structure of a code was proposed. The cardinality of such a multicomponent codes is equal to the sum of cardinalities of component codes. An iterative decoding algorithm was proposed. In [7], parameters of all-zero prefixes were optimized, which allowed to increase the code cardinality. A modified decoding algorithm was developed for this case.

In subsequent papers [8, 15], multicomponent codes based on balanced incomplete block designs [17] were constructed.

It should be noted that the upper bound (3) can be rewritten in the form

$$\frac{\begin{bmatrix} n \\ k-m \end{bmatrix}}{\begin{bmatrix} k \\ k-m \end{bmatrix}} = q^{(n-k)(k-m)} + q^{(n-k)(k-m)-m-1}(1+O(1));$$

on the other hand, the cardinality of an SKK code for $k \le n/2$ is $M = q^{(n-k)(k-m)}$, i.e., coincides with the first (maximal) term. This means that adding new components to an SKK code can only slightly increase the cardinality, though the number of new code components may be rather large.

When modifying an SKK code by adding new components, one has to solve two problems:

1. If the multiindex of a component is already chosen, then free element submatrices should form a matrix rank code of rank distance $d_r = m+1$. Then the Grassmann distance $d_{\text{sub}} = 2(m+1)$ between different matrices inside the same component will be guaranteed. The difficulty of this task is as follows: a free element matrix should have many prescribed zero entries, and this puts obstacles to the standard use of known $k \times (n-k)$ rank codes.
2. Multi-indices of different components should be chosen in such a way that the Grassmann distance between any two code matrices of different components is not less than $d_{\text{sub}} = 2(m+1)$.

We propose a new family of subcodes of rank codes to solve the first problem. These subcodes are also known as restricted rank codes. Nonuniformly restricted subcodes in a number of cases reach the Singleton bound. When choosing a proper subcode, one can use restrictions introduced by free element matrices (namely, location of prescribed zero entries). This completely solves the problem of encoding inside a component.

To solve the second problem, one has to construct a list of suitable multiindices. The problem of choosing an *optimal* (in the sense of maximal cardinality) list of multiindices is presently unsolved. As an alternative, we suggest to use sets of blocks of a balanced incomplete block design to construct such a list. An encoding algorithm is proposed. Examples are given for codes with seven and thirteen components.

Subspace subcodes, as well as standard rank codes, are intended to correct errors in such structures where information is presented as two-dimensional arrays and errors may occur along rows and/or columns. Examples are multichannel recording on a tape or rectangular memory arrays. Subcodes can also be used in constructions of space-time codes with optimal rate-diversity trade-off (see, e.g., [18, 19]) and in cryptography [20]. Using rank codes in random network coding is well known [3, 21].

The rest of the paper is organized as follows. Section 2 contains rather complete background on rank codes, including matrix and vector representations, systematic and nonsystematic encoding, and nonuniformly restricted rank codes. Also, a new family of subspace subcodes is presented. In Section 3 subcodes of matrix rank codes for network coding are described. Section 4 shows how balanced incomplete block designs can be implemented for constructing multicomponent codes with

prescribed parameters. Examples of codes with seven and thirteen components are given. Section 5 contains the main conclusions.

2. RANK CODES AND SUBCODES

Codes in the rank metric, introduced in [4], have two alternative descriptions: the *matrix* and *vector* representation.

Let $\mathbb{K}$ and $\mathbb{K}_{q^N}$ be a field of q elements and its extension of degree N, respectively.

2.1. Matrix Representation of Rank Codes

In the *matrix* representation, the space $\mathbb{K}^{N\times n}$ of matrices of size $N \times n$ over the *ground* field $\mathbb{K}$ is considered. We assume without loss of generality that $N \geq n$.

The *rank* distance $d(G_1, G_2)$ between two matrices G_1, G_2 is defined as the rank of their difference: $d(G_1, G_2) = \mathrm{rk}(G_1 - G_2)$.

A *matrix rank code* $\mathcal{M} \subseteq \mathbb{K}^{N\times n}$ is any set of matrices.

The *rank code distance* $d(\mathcal{M}) = d$ is defined as the minimal pairwise distance: $d = \min\{\mathrm{rk}(G_1 - G_2) :\ G_1, G_2 \in \mathcal{M},\ G_1 \neq G_2\}$.

A code is referred to as a *matrix* $(N \times n, M, d)$ *code* if it consists of M matrices of size $N \times n$ and has rank code distance d.

A matrix $(N \times n, M, d)$ code satisfies the Singleton bound [4]:

$$M \leq q^{N(n-d+1)}. \tag{5}$$

If we have equality in (5), then a code has the *maximum rank distance* and is referred to as a matrix MRD code.

An $(N \times n, M, d)$ code $\mathcal{M}$ is said to be a $\mathbb{K}$-*linear* code of dimension k if $\mathcal{M}$ is a k-dimensional subspace of the space $\mathbb{K}^{N\times n}$.

2.2. Vector Representation of Rank Codes

In the *vector* representation, a normalized space $\mathbb{K}_{q^N}^n$ of vectors of length n over the *extension* field $\mathbb{K}_{q^N}$ is considered.

The *rank* of a vector $\boldsymbol{g} \in \mathbb{K}_{q^N}^n$ is defined as the maximal number $r(\boldsymbol{g})$ of its coordinates that are linearly independent over the ground field $\mathbb{K}$.

The *rank* distance $d(\boldsymbol{g}_1, \boldsymbol{g}_2)$ between vectors $\boldsymbol{g}_1, \boldsymbol{g}_2$ is defined as the rank of their difference: $d(\boldsymbol{g}_1, \boldsymbol{g}_2) = r(\boldsymbol{g}_1 - \boldsymbol{g}_2)$.

A *vector* code $\mathcal{V} \subseteq \mathbb{K}_{q^N}^n$ is any set of vectors.

The *rank code distance* $d(\mathcal{V}) = d$ is defined as the minimal pairwise distance between code vectors:

$$d = \min\{r(\boldsymbol{g}_1 - \boldsymbol{g}_2) :\ \boldsymbol{g}_1, \boldsymbol{g}_2 \in \mathcal{V},\ \boldsymbol{g}_1 \neq \boldsymbol{g}_2\}.$$

A code $\mathcal{V}$ is called a $\mathbb{K}_{q^N}$-*linear* code of dimension k if $\mathcal{V}$ is a k-dimensional subspace of the space $\mathbb{K}_{q^N}^n$. A code of distance d are referred to as an $[n, k, d]$ code. For these codes the Singleton bound is valid [4]:

$$k \leq n - d + 1. \tag{6}$$

If we have equality in (6), then a code has the *maximum rank distance* and is referred to as a vector MRD code.

2.3. Relation between Matrix and Vector Rank Codes

Let $\Omega = \{\omega_1, \omega_2, \ldots, \omega_N\}$ be a basis of the extension field $\mathbb{K}_{q^N}$ over the ground field $\mathbb{K}$.

A vector $\boldsymbol{x} = \begin{pmatrix} x_1 & \ldots & x_n \end{pmatrix} \in \mathbb{K}_{q^N}^n$ over the extension field $\mathbb{K}_{q^N}$ can be uniquely transformed into a matrix $X(\boldsymbol{x})$ of size $N \times n$ over the ground field $\mathbb{K}$:

$$\boldsymbol{x} \iff X(\boldsymbol{x}) = \begin{pmatrix} x_{11} & x_{12} & \ldots & x_{1n} \\ x_{21} & x_{22} & \ldots & x_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ x_{N1} & x_{N2} & \ldots & x_{Nn} \end{pmatrix}. \tag{7}$$

The jth column of the matrix $X(\boldsymbol{x})$ consists of coefficients of the representation of the jth coordinate $x_j \in \mathbb{K}_{q^N}$ of the vector:

$$x_j = x_{1j}\omega_1 + x_{2j}\omega_2 + \ldots + x_{Nj}\omega_N,$$

where the coefficients x_{ij}, $i = 1, \ldots, n$, belong to the ground field $\mathbb{K}$.

It is clear that the rank of the matrix $X(\boldsymbol{x})$ coincides with the rank of the vector $\boldsymbol{x}$, i.e., $\mathrm{rk}(X(\boldsymbol{x})) = r(\boldsymbol{x})$.

Therefore, given a *vector* code $\mathcal{V}$, one can construct a *matrix* code $\mathcal{M}$ with the same metric properties by mapping each code vector to the corresponding code matrix.

Conversely, if a *matrix* code $\mathcal{M}$ is given, one can construct the corresponding *vector* code $\mathcal{V}$ by replacing each column of the code matrix by the corresponding element of the extension field.

Vector representation is more convenient for describing constructions of rank codes and performing fast encoding and decoding.

Matrix representation is useful in practical applications, for instance, in the theory of space-time codes [18, 19] or in network coding [3, 11].

2.4. Constructions of Linear Vector Rank Codes

Following [4], we present constructions of linear vector rank codes. Introduce the notation $[i] \stackrel{\text{def}}{=} q^i$ if $i \geq 0$, and $[i] \stackrel{\text{def}}{=} q^{Ns+i}$ if $i < 0$, where s is the minimal integer such that $Ns + i \geq 0$.

A linear vector MRD $[n, k, d]$ code $\mathcal{V}$ can be given by a generator matrix of the form

$$\boldsymbol{G} = \begin{pmatrix} g_1 & \ldots & g_n \\ \ldots & \ldots & \ldots \\ g_1^{[k-1]} & \ldots & g_n^{[k-1]} \end{pmatrix}, \tag{8}$$

where elements $g_1, \ldots, g_n \in \mathbb{K}_{q^N}$ are linearly independent over the ground field.

A parity-check matrix $\boldsymbol{H}$ of $\mathcal{V}$ has a similar form:

$$\boldsymbol{H} = \begin{pmatrix} h_1 & \ldots & h_n \\ \ldots & \ldots & \ldots \\ h_1^{[d-2]} & \ldots & h_n^{[d-2]} \end{pmatrix}, \tag{9}$$

where elements $h_1, \ldots, h_n \in \mathbb{K}_{q^N}\ \mathbb{K}$ are linearly independent over the ground field. The matrix $\boldsymbol{H}$ satisfies the condition $\boldsymbol{G}\boldsymbol{H}^\top = \boldsymbol{0}$.

The code $\mathcal{V}$ has length n, dimension k, code rank distance $d = n - k + 1$, and it is an MRD code. It corrects rank errors up to rank $t = \lfloor (d-1)/2 \rfloor$.

Let $\boldsymbol{i} = (i_0\ i_1\ \ldots\ i_{k-1}) \in \mathbb{K}_{q^N}^k$ be an information vector. It can be encoded in either a nonsystematic or systematic form.

Nonsystematic encoding. A code vector is computed as follows:

$$\boldsymbol{g}(\boldsymbol{i}) = \boldsymbol{i}\boldsymbol{G}. \tag{10}$$

Positions of information symbols are not specified explicitly.

Systematic encoding. A code vector is computed in the form

$$\boldsymbol{g}(\boldsymbol{i}) = \left(\boldsymbol{v}\ \ \boldsymbol{i}\right), \tag{11}$$

where information symbols $\boldsymbol{i} = (i_0\ i_1\ \ldots\ i_{k-1})$ are placed in the last k positions, while the subvector $\boldsymbol{v} = (v_0\ \ldots\ v_{d-2})$ contains parity-check symbols.

Represent the parity-check matrix in the block form $\boldsymbol{H} = (\boldsymbol{H}_1\ \boldsymbol{H}_2)$, where $\boldsymbol{H}_1$ is a square nonsingular submatrix of order $d-1$ and $\boldsymbol{H}_2$ is a submatrix of size $(d-1)\times(n-d+1)$. Then the parity-check subvector $\boldsymbol{v}$ of the vector $\boldsymbol{g}(\boldsymbol{i})$ is computed as

$$\boldsymbol{v} = -\boldsymbol{i}\boldsymbol{H}_2^{\top}(\boldsymbol{H}_1^{\top})^{-1}. \tag{12}$$

Presently, several decoding algorithms for MRD codes with polynomial complexity are known; see, e.g., [4, 22–26].

2.5. Subspaces of Extension Fields and Subspace Subcodes

Consider the extension field $\mathbb{K}_{q^N}$ as an N-dimensional vector space over the ground field $\mathbb{K}$. Denote by $\boldsymbol{b} = \{b_1, \ldots, b_s\}$, $s \le N$, $b_i \in \mathbb{K}_{q^N}$, a set of s elements of the extension field that are linearly independent over the ground field $\mathbb{K}$. Let $V_{\boldsymbol{b}}(s)$ be an s-dimensional subspace of the N-dimensional space $\mathbb{K}_{q^N}$ spanned by the elements of $\boldsymbol{b}$. Choose n (possibly different) subspaces $V_{\boldsymbol{b}_j}(s_j)$, $j = 1, \ldots, n$. Define the direct product of these subspaces:

$$\Phi = V_{\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n}(s_1, s_2, \ldots, s_n) = V_{\boldsymbol{b}_1}(s_1) \otimes V_{\boldsymbol{b}_2}(s_2) \otimes V_{\boldsymbol{b}_n}(s_n).$$

Elements of the space Φ can be considered as vectors of length n such that the first coordinate belongs to $V_{\boldsymbol{b}_1}(s_1)$, the second to $V_{\boldsymbol{b}_2}(s_2)$, …, the nth to $V_{\boldsymbol{b}_n}(s_n)$.

Choose an MRD $[n, k, d]$ code $\mathcal{V}$. By definition, a vector subcode of the code $\mathcal{V}$ over the subspace Φ is the following intersection:

$$\mathcal{V}|_{\Phi} = \mathcal{V} \cap \Phi.$$

Our principal goal is to construct subcodes $\mathcal{V}|_{\Phi}$ for a given Φ.

If Φ is a product of identical subspaces, the subcodes are said to be uniformly restricted. Otherwise, they are nonuniformly restricted subcodes.

Matrix subcodes are constructed as matrix representations of equivalent vector subcodes.

2.6. Nonuniformly Restricted Rank Codes

Assume that $d-1$ subspaces $V_{\boldsymbol{b}_i}(s_i)$ coincide with $\mathbb{K}_{q^N}$, i.e., there are no restrictions for values of entries in the chosen $d-1$ coordinates of a code vector. The other $n-d+1$ coordinates should belong to $V_{\boldsymbol{b}_1}(s_1), V_{\boldsymbol{b}_2}(s_2), \ldots, V_{\boldsymbol{b}_{n-d+1}}(s_{n-d+1})$. The subspace Φ is of the form

$$\Phi = \left(\mathbb{K}_{q^N}\right)^{d-1} \otimes V_{\boldsymbol{b}_1}(s_1) \otimes V_{\boldsymbol{b}_2}(s_2) \otimes \ldots \otimes V_{\boldsymbol{b}_{n-d+1}}(s_{n-d+1}).$$

A code vector of the subspace subcode $\mathcal{V}|_{\Phi} = \mathcal{V} \cap \Phi$ has the following structure:

$$(v_1\ \ldots\ v_{d-1}\ c_1 \ldots c_{n-d+1}) = (\boldsymbol{v}\ \ \boldsymbol{c}),$$

where $\boldsymbol{v} = (v_1 \ \ldots \ v_{d-1})$, $\boldsymbol{c} = (c_1 \ldots c_{n-d+1})$. In this case $c_i \in V_{\boldsymbol{b}_i}(s_i)$, $i = 1, \ldots, n-d+1$. In other words,

$$\boldsymbol{c} \in V_{\boldsymbol{b}_1}(s_1) \otimes V_{\boldsymbol{b}_2}(s_2) \otimes \ldots \otimes V_{\boldsymbol{b}_{n-d+1}}(s_{n-d+1}).$$

The code can be considered as a polyalphabetic code, where different coordinates belong to different alphabets. The Singleton bound in the Hamming metric for this case was found in [27] in the form

$$|\mathcal{V}|_{\Phi}| \le |V_{\boldsymbol{b}_1}(s_1) \otimes V_{\boldsymbol{b}_2}(s_2) \otimes \ldots \otimes V_{\boldsymbol{b}_{n-d+1}}(s_{n-d+1})| = q^{s_1+s_2+\ldots+s_{n-d+1}}. \tag{13}$$

The bound was generalized for the rank metric in [4].

Systematic encoding (11) and (12) can be used to construct a code with these restrictions. The vector $\boldsymbol{c}$ is treated as an information vector, whereas the vector $\boldsymbol{v} = -\boldsymbol{c}\boldsymbol{H}_2^{\top}(\boldsymbol{H}_1^{\top})^{-1}$ is a parity-check vector. Note that this construction meets the Singleton bound (13).

Subcodes with these restrictions can be used in multicomponent network codes [3,6,8,11]. They are also referred to as restricted rank codes.

Restricted matrix rank codes: an example. Consider a vector MRD (n, k, d) code with a generator matrix $\boldsymbol{G}$ and a parity-check matrix $\boldsymbol{H}$. Let an information vector be $\boldsymbol{u} = (u_1, \ldots, u_k)$, and let systematic encoding (11) and (12) be used. A code vector is transformed into an equivalent code matrix

$$M((\boldsymbol{v} \ \ \boldsymbol{u})) = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{N1} & a_{N2} & \ldots & a_{Nn} \end{pmatrix},$$

where the last k symbols correspond to information symbols, and the first $d-1 = n-k$, to parity-check symbols.

A code matrix is called a *restricted matrix* if some columns must take values in some prescribed subspaces. A rank code consisting of such matrices is known as a *restricted matrix rank code*.

We are solving the following problem: construct a *restricted matrix rank code* having a specified rank code distance.

The following steps are used: a matrix rank code is transformed into a vector rank code. Restrictions for coordinates of a code vector are established. A *vector* code with these restriction is constructed. Then it is transformed into the *matrix* form.

Let us construct a matrix rank code $\widetilde{\mathcal{M}}$ with matrices of size 4×3, with code distance $d_r = 2$, and with the following restrictions:

$$M((\boldsymbol{v} \ \ \boldsymbol{u})) = \begin{pmatrix} a_{11} & 0 & 0 \\ a_{21} & 0 & 0 \\ a_{31} & a_{32} & a_{33} \\ a_{41} & a_{42} & a_{43} \end{pmatrix}.$$

This matrix subcode corresponds to a vector subcode of the MRD $[3, 2, 2]$ code with the generator and parity-check matrices

$$\boldsymbol{G} = \begin{pmatrix} g_0 & g_1 & g_2 \\ g_0^2 & g_1^2 & g_2^2 \end{pmatrix}, \qquad \boldsymbol{H} = \begin{pmatrix} h_0 & h_1 & h_2 \end{pmatrix}$$

defined over the field $GF(2^2)$. For instance, choose

$$\boldsymbol{G} = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{pmatrix}, \qquad \boldsymbol{H} = \begin{pmatrix} 1 & \alpha^{10} & \alpha^{12} \end{pmatrix},$$

where α is a root of the primitive polynomial $f(x) = x^4 + x^3 + 1$. A code vector has the form $\boldsymbol{g} = (v\ u_1\ u_2)$, where u_1, u_2 are information symbols. The parity-check symbol v is computed from relations (11) and (12): $v = u_1\alpha + u_2\alpha^2$. By the above restriction conditions, information symbols u_1 and u_2 belong to the 2-dimensional subspace with basis $\boldsymbol{b} = (\alpha^2, \alpha^3)$; i.e., $u_1 = a_{32}\alpha^2 + a_{42}\alpha^3$ and $u_2 = a_{33}\alpha^2 + a_{43}\alpha^3$, where $a_{32}, a_{42}, a_{33}, a_{43}$ are *binary information bits*. Accordingly, we obtain

$$v = (a_{42} + a_{33} + a_{43})1 + a_{43}\alpha + 0\alpha^2 + (a_{32} + a_{42} + a_{33} + a_{43})\alpha^3.$$

The Singleton bound (13) in this case has the form

$$\left|\widetilde{\mathcal{M}}\right| \le 2^{2+2} = 16.$$

By transforming the code vector $\boldsymbol{g} = (v\ u_1\ u_2)$ to an equivalent code matrix, we obtain a restricted matrix code $\widetilde{\mathcal{M}}$ in the form

$$\widetilde{\mathcal{M}} = \left\{ M((v\ u_1\ u_2)) = \begin{pmatrix} a_{42} + a_{33} + a_{43} & 0 & 0 \\ a_{43} & 0 & 0 \\ 0 & a_{32} & a_{33} \\ a_{32} + a_{42} + a_{33} + a_{43} & a_{42} & a_{43} \end{pmatrix} \right\}.$$

The total number of matrices in this code is $2^4 = 16$. Hence, the code meets the Singleton bound.

3. SUBCODES OF RANK MATRIX CODES IN NETWORK CODING

The set of basic matrices in row-reduced echelon form corresponding to k-dimensional subspaces can be split into a set of equivalence classes. An equivalence class consists of all matrices having the same multiindex. Inside an equivalence class, matrices differ by their free elements. The structure of free elements can be described as follows. The first row of a basic matrix contains $n-k+1-i_1$ free elements, the second contains $n-k+2-i_2$ free elements, ..., the $(k-1)$th row contains $n-k+(k-1)-i_{k-1}$ free elements, and the last (kth) row contains $f_k = n-k+k-i_k$ free elements.

For example, consider a basic matrix in row-reduced echelon form with $k = 3$, $n = 6$, and multiindex $\mathcal{I} = \{i_1, i_2, i_3\} = \{1, 3, 4\}$. This matrix is of the form

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

The symbol $\boxtimes$ stands for a free element. The matrix has seven free elements, which can be arbitrarily chosen over the field $\mathbb{K}$. Therefore, there are q^7 different 3-dimensional subspaces with the same multiindex.

Consider a submatrix obtained by deleting columns that contain leading elements. This submatrix contains all the free elements and also several zero elements. In the example above, we obtain the submatrix

$$\widetilde{A} = \begin{pmatrix} \boxtimes & \boxtimes & \boxtimes \\ 0 & \boxtimes & \boxtimes \\ 0 & \boxtimes & \boxtimes \end{pmatrix}.$$

In the general case, let $\widetilde{A}$ denote a matrix obtained from A by deleting columns labeled by the multiindex $\mathcal{I} = \{i_1, i_2, \ldots, i_k\}$. For brevity, we refer to this matrix as the free element submatrix.

It is of size $k \times (n-k)$ and has the following structure:

$$\widetilde{A} = \begin{pmatrix} \overbrace{0\ldots0}^{i_1-1} & \overbrace{\boxtimes\ldots\boxtimes}^{n-k+1-i_1} \\ \overbrace{0\ldots0}^{i_2-2} & \overbrace{\boxtimes\ldots\boxtimes}^{n-k+2-i_2} \\ \cdots\cdots\cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots\cdots\cdots \\ \overbrace{0\ldots0}^{i_{k-1}-k+1} & \overbrace{\boxtimes\ldots\boxtimes}^{n-k+k-1-i_{k-1}} \\ \overbrace{0\ldots0}^{i_k-k} & \overbrace{\boxtimes\ldots\boxtimes}^{n-k+k-i_k} \end{pmatrix}. \tag{14}$$

Denote by $\widetilde{A}_{\mathrm{red}}$ the reduced free element submatrix obtained from $\widetilde{A}$ by deleting all-zero rows and all-zero columns, if any[2]. There are (i_1-1) all-zero columns in $\widetilde{A}$ if $i_1 > 1$. There are s all-zero rows in $\widetilde{A}$ if the last integers in the multiindex are $i_{k-s+1} = n-s+1$, …, $i_{k-1} = n-1$, $i_k = n$.

3.1. Subspace Distances in Terms of Row-Reduced Echelon Matrices

In what follows, we assume that k-dimensional subspaces are given by basic $k \times n$ matrices A in row-reduced echelon form or, equivalently, by multiindices $\mathcal{I} = \{i_1, i_2, \ldots, i_k\}$ and free element matrices $\widetilde{A}$.

First consider the case where matrices A and B are in the same equivalence class with a multiindex $\mathcal{I} = \{i_1, i_2, \ldots, i_k\}$ and differ only in free element matrices $\widetilde{A}$ and $\widetilde{B}$.

Lemma 1. *The subspace distance between subspaces $\mathcal{A}$ and $\mathcal{B}$ from the same equivalence class is given by*

$$d_{\mathrm{sub}}(\mathcal{A}, \mathcal{B}) = 2\,\mathrm{rk}(\widetilde{A} - \widetilde{B}) = 2\,\mathrm{rk}(\widetilde{A}_{\mathrm{red}} - \widetilde{B}_{\mathrm{red}}). \tag{15}$$

Proof. The proof literally repeats the proof in [2] for the case of $\mathcal{I} = \{1, 2, \ldots, k\}$. △

Let now a k-dimensional subspace $\mathcal{A}$ be given by a multiindex $\mathcal{I} = \{i_1, i_2, \ldots, i_k\}$ and a free element matrix $\widetilde{A}$. Let an m-dimensional subspace $\mathcal{B}$ be given by a multiindex $\mathcal{J} = \{j_1, j_2, \ldots, j_m\}$ and a free element matrix $\widetilde{B}$. For definiteness, assume that $m \le k$. Denote by $\mathcal{L} = \{l_1, \ldots, l_\lambda\}$ the set of common indices in the multiindices, where

$$\lambda = |\mathcal{I} \cap \mathcal{J}|.$$

Consider the $\lambda \times n$ submatrix A_1 of A consisting of rows with the multiindex $\mathcal{L}$. It is clear that the subspace $\mathcal{A}_1$ spanned by these rows intersects the subspace spanned by the remaining rows at the all-zero row only. Similarly, the subspace $\mathcal{B}_1$ spanned by the rows of the $\lambda \times n$ submatrix B_1 of the matrix B that contain the multiindex $\mathcal{L}$ intersects the subspace spanned by the remaining rows of the matrix B at the all-zero row only. It is also clear that subspaces spanned by the remaining rows of matrices A and B meet at the all-zero vector only. Hence,

$$\dim(\mathcal{A} \cap \mathcal{B}) = \dim(\mathcal{A}_1 \cap \mathcal{B}_1). \tag{16}$$

In turn, the subspaces $\mathcal{A}_1$ and $\mathcal{B}_1$ have basic matrices with the same multiindex $\mathcal{L}$. Using (1), (15), and (16), we arrive at the following result.

[2] In [11] $\widetilde{A}_{\mathrm{red}}$ are called Ferrer diagrams because of their similarity with diagrams in the theory of partitions [16].

Lemma 2. *We have*

$$d_{\text{sub}}(\mathcal{A},\mathcal{B}) = k+m-2\dim(\mathcal{A}\cap\mathcal{B}) = k+m-2\lambda+2\lambda-2\dim(\mathcal{A}_1\cap\mathcal{B}_1)$$
$$= k+m-2\lambda+d_{\text{sub}}(\widetilde{\mathcal{A}}_1,\widetilde{\mathcal{B}}_1) = k+m-2\lambda+2\,\text{rk}(\widetilde{A}_1-\widetilde{B}_1). \quad (17)$$

Here $\widetilde{A}_1$ and $\widetilde{B}_1$ are free element matrices of the subspaces $\mathcal{A}_1$ and $\mathcal{B}_1$.

Corollary. *We have*

$$d_{\text{sub}}(\mathcal{A},\mathcal{B}) \geq k+m-2\lambda. \quad (18)$$

4. BALANCED INCOMPLETE BLOCK DESIGNS AS NETWORK CODES

4.1. Constructing Multicomponent Network Codes

As is mentioned above, network codes with specified subspace distance d_{sub} consist of $k\times n$ matrices in row-reduced echelon form over the ground field $\mathbb{K}$ having pairwise subspace distances at least d_{sub}.

The subset of code matrices with the same multiindex is called a code component. It follows from (15) that the corresponding (reduced) free element matrices must form a rank code with rank distance $d_r \geq d_{\text{sub}}/2$.

The best code component has multiindex $\mathcal{I}=\{1,2,\ldots,k\}$. This code was proposed in [3] and is called the Silva–Kschischang–Koetter code (SKK code). The SKK code can be given as a set of basic $k\times n$ matrices of the form

$$\mathcal{C}_1 = \{(I_k \;\; M)\},$$

where I_k is the identity matrix of order k. The submatrix $M\in\mathcal{M}$ is a code matrix of a matrix rank code $\mathcal{M}$ consisting of matrices of size $k\times(n-k)$. Let d_r be the *rank distance*. The subspace distance is $d_{\text{sub}}=2d_r$. The matrix code $\mathcal{M}$ is constructed as an MRD code from a vector code with the following parameters: field $\mathbb{K}_{q^N}$, where $N=\max(k,n-k)$; length $m=\min(k,n-k)$; number of information symbols $K=m-d_r+1$; cardinality $|\mathcal{M}|=q^{NK}$ (see Sections 2.3 and 2.4).

To add to the SKK code a new component $\mathcal{C}_2$ with matrices of the same dimension, one can choose a multiindex satisfying condition (18), namely, $2k-2\lambda\geq d_{\text{sub}}$. Choose, for example, $\mathcal{J}=\{1,k+1,\ldots,2k-1\}$. Then $\lambda=1$. Free element matrices of this component are of the form

$$\widetilde{C}_1 = \begin{pmatrix} \overbrace{\boxtimes\boxtimes\ldots\boxtimes}^{k-1} & \overbrace{\boxtimes\ldots\boxtimes}^{n-2k+1} \\ \overbrace{0\ldots0}^{k-1} & \overbrace{\boxtimes\ldots\boxtimes}^{n-2k+1} \\ \cdots\cdots\cdots\cdots & \cdots\cdots \\ \overbrace{0\ldots0}^{k-1} & \overbrace{\boxtimes\ldots\boxtimes}^{n-2k+1} \\ \overbrace{0\ldots0}^{k-1} & \overbrace{\boxtimes\ldots\boxtimes}^{n-2k+1} \end{pmatrix}.$$

They should be chosen as code matrices of a restricted rank code (see Section 2.6).

In general, construction of a multicomponent network code reduces to choosing a sequence of multiindices. We propose a suboptimal algorithm based on using balanced incomplete block designs.

By definition, a balanced incomplete block design is an arrangement of n different elements in b blocks such that each block contains exactly k different elements, each element appears in r different blocks, and each pair of the distinct elements a_i, a_j appears exactly in λ blocks.

In network coding, different elements are integers $\{1,\ 2,\ \ldots,\ n\}$, treated as indices of columns of a basic matrix. A block is a set of k distinct integers. A block $\mathcal{B}$ is treated as a multiindex of size k. The integer k is the number of rows of the basic matrix.

The network code consists of b components, which are defined by different blocks (multiindices).

The parameter λ defines the subspace distance between subspaces from distinct components: $d_{\text{sub}}(\mathcal{B}_i, \mathcal{B}_j) = d_{\text{sub}} = 2k - 2\lambda$. In turn, the reduced free element matrices inside a component must form a matrix code with rank distance $d_r \geq d_{\text{sub}}/2 = k - \lambda$. Such codes are constructed as matrix representations of subcodes of restricted vector codes.

Many balanced incomplete block designs are presented in the book [17]. We give two simple examples.

4.2. Examples of Multicomponent Codes

A code of seven components. We show by examples how to construct a multicomponent code. First, construct a code of seven components. Consider a balanced incomplete block design with parameters ($n = 7$, $b = 7$, $r = 3$, $k = 3$, $\lambda = 1$). Write down $b = 7$ multiindices for matrices in row-reduced echelon form of size $(k \times n) = 3 \times 7$ as the set of indices in blocks $\mathcal{B}_i$ and also the corresponding basic matrices and reduced free element matrices:

$$\mathcal{B}_1 = \begin{Bmatrix} 1 \\ 2 \\ 3 \end{Bmatrix} \rightarrow A_1 = \begin{pmatrix} 1 & 0 & 0 & \boxtimes & \boxtimes & \boxtimes & \boxtimes \\ 0 & 1 & 0 & \boxtimes & \boxtimes & \boxtimes & \boxtimes \\ 0 & 0 & 1 & \boxtimes & \boxtimes & \boxtimes & \boxtimes \end{pmatrix} \rightarrow \widetilde{A}_{1\text{red}} = \begin{pmatrix} \boxtimes & \boxtimes & \boxtimes & \boxtimes \\ \boxtimes & \boxtimes & \boxtimes & \boxtimes \\ \boxtimes & \boxtimes & \boxtimes & \boxtimes \end{pmatrix},$$

$$\mathcal{B}_2 = \begin{Bmatrix} 1 \\ 4 \\ 5 \end{Bmatrix} \rightarrow A_2 = \begin{pmatrix} 1 & \boxtimes & \boxtimes & 0 & 0 & \boxtimes & \boxtimes \\ 0 & 0 & 0 & 1 & 0 & \boxtimes & \boxtimes \\ 0 & 0 & 0 & 0 & 1 & \boxtimes & \boxtimes \end{pmatrix} \rightarrow \widetilde{A}_{2\text{red}} = \begin{pmatrix} \boxtimes & \boxtimes & \boxtimes & \boxtimes \\ 0 & 0 & \boxtimes & \boxtimes \\ 0 & 0 & \boxtimes & \boxtimes \end{pmatrix},$$

$$\mathcal{B}_3 = \begin{Bmatrix} 1 \\ 6 \\ 7 \end{Bmatrix} \rightarrow A_3 = \begin{pmatrix} 1 & \boxtimes & \boxtimes & \boxtimes & \boxtimes & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \rightarrow \widetilde{A}_{3\text{red}} = \begin{pmatrix} \boxtimes & \boxtimes & \boxtimes & \boxtimes \end{pmatrix},$$

$$\mathcal{B}_4 = \begin{Bmatrix} 2 \\ 4 \\ 6 \end{Bmatrix} \rightarrow A_4 = \begin{pmatrix} 0 & 1 & \boxtimes & 0 & \boxtimes & 0 & \boxtimes \\ 0 & 0 & 0 & 1 & \boxtimes & 0 & \boxtimes \\ 0 & 0 & 0 & 0 & 0 & 1 & \boxtimes \end{pmatrix} \rightarrow \widetilde{A}_{4\text{red}} = \begin{pmatrix} \boxtimes & \boxtimes & \boxtimes \\ 0 & \boxtimes & \boxtimes \\ 0 & 0 & \boxtimes \end{pmatrix},$$

$$\mathcal{B}_5 = \begin{Bmatrix} 2 \\ 5 \\ 7 \end{Bmatrix} \rightarrow A_5 = \begin{pmatrix} 0 & 1 & \boxtimes & \boxtimes & 0 & \boxtimes & 0 \\ 0 & 0 & 0 & 0 & 1 & \boxtimes & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \rightarrow \widetilde{A}_{5\text{red}} = \begin{pmatrix} \boxtimes & \boxtimes & \boxtimes \\ 0 & 0 & \boxtimes \end{pmatrix},$$

$$\mathcal{B}_6 = \begin{Bmatrix} 3 \\ 4 \\ 7 \end{Bmatrix} \rightarrow A_6 = \begin{pmatrix} 0 & 0 & 1 & 0 & \boxtimes & \boxtimes & 0 \\ 0 & 0 & 0 & 1 & \boxtimes & \boxtimes & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \rightarrow \widetilde{A}_{6\text{red}} = \begin{pmatrix} \boxtimes & \boxtimes \\ \boxtimes & \boxtimes \end{pmatrix},$$

$$\mathcal{B}_7 = \begin{Bmatrix} 3 \\ 5 \\ 6 \end{Bmatrix} \rightarrow A_7 = \begin{pmatrix} 0 & 0 & 1 & \boxtimes & 0 & 0 & \boxtimes \\ 0 & 0 & 0 & 0 & 1 & 0 & \boxtimes \\ 0 & 0 & 0 & 0 & 0 & 1 & \boxtimes \end{pmatrix} \rightarrow \widetilde{A}_{7\text{red}} = \begin{pmatrix} \boxtimes & \boxtimes \\ 0 & \boxtimes \\ 0 & \boxtimes \end{pmatrix},$$

where $\boxtimes$ denotes free elements to be chosen.

The subspace distance between components is $d_{\text{sub}} = 2k - 2\lambda = 4$. Therefore, the rank distance of rank codes inside components must be $d_r = d_{\text{sub}}/2 = 2$. For the matrix code $A_{i,\text{red}}$ of each component, we will specify parameters of a restricted *vector* code from which the matrix code is obtained. These parameters are extension field $\mathbb{K}_{q^N}$, length m of the vector code, number K of information symbols, restrictions, and cardinality.

- Component $\mathcal{B}_1$. The code $A_{1\text{red}}$ is the SKK code. Field $\mathbb{K}_{q^N} = \mathbb{K}_{q^4}$, length of the vector code $m = 3$, number of information symbols $K = m - d_r + 1 = 2$, no restrictions, cardinality $q^{NK} = q^8$.
- Component $\mathcal{B}_2$. Code $A_{2\text{red}}$. Field $\mathbb{K}_{q^N} = \mathbb{K}_{q^4}$, length of the vector code $m = 3$, number of information symbols $K = m - d_r + 1 = 2$, information symbols take values in a subspace of dimension $\widehat{N} = 2$, cardinality $q^{\widehat{N}K} = q^4$.
- Component $\mathcal{B}_3$. Code $A_{3\text{red}}$. Field $\mathbb{K}_{q^N} = \mathbb{K}_{q^4}$, length of the vector code $m = 1$, number of information symbols $K = m - d_r + 1 = 0$, information symbols, cardinality $q^{\widehat{N}K} = 1$. The component $\mathcal{B}_3$ has a single basic matrix.
- Component $\mathcal{B}_4$. Code $A_{4\text{red}}$. Field $\mathbb{K}_{q^N} = \mathbb{K}_{q^3}$, length of the vector code $m = 3$, number of information symbols $K = m - d_r + 1 = 2$, one information symbol takes values in a 2-dimensional subspace and the other in a 1-dimensional subspace, cardinality $q^2 q^1 = q^3$.
- Component $\mathcal{B}_5$. Code $A_{5\text{red}}$. Field $\mathbb{K}_{q^N} = \mathbb{K}_{q^3}$, length of the vector code $m = 2$, number of information symbols $K = m - d_r + 1 = 1$, the information symbol take values in a 1-dimensional subspace, cardinality $q^1 = q$.
- Component $\mathcal{B}_6$. Code $A_{6\text{red}}$. Field $\mathbb{K}_{q^N} = \mathbb{K}_{q^2}$, length of the vector code $m = 2$, number of information symbols $K = m - d_r + 1 = 1$, the information symbol take values in $\mathbb{K}_{q^2}$, cardinality q^2.
- Component $\mathcal{B}_7$. Code $A_{7\text{red}}$. Field $\mathbb{K}_{q^N} = \mathbb{K}_{q^3}$, length of the vector code $m = 2$, number of information symbols $K = m - d_r + 1 = 1$, the information symbol take values in a 1-dimensional subspace, cardinality $q^1 = q$.

We have constructed a $[7, |\mathcal{C}|, 4, 3]$ code $\mathcal{C}$ of length $n = 7$ with subspace distance $d_{\text{sub}} = 4$, dimension $k = 3$, and cardinality $|\mathcal{C}| = q^8 + q^4 + q^3 + q^2 + 2q + 1$. An upper bound for the cardinality is $M_{\max} = q^8 + q^6 + q^5 + q^4 + q^3 + q^2 + 1$ (see (3)).

A code of thirteen components. We use a similar approach to construct a multicomponent code of thirteen components. From Table 1 in the book [17], choose a block design with parameters $n = b = 13$, $r = k = 4$, and $\lambda = 1$. The block design is defined by the following $b = 13$ blocks (multiindices):

$$\begin{aligned}
&\mathcal{B}_1 = \{1,2,3,4\}, && \mathcal{B}_2 = \{1,5,6,7\}, && \mathcal{B}_3 = \{1,8,9,10\}, && \mathcal{B}_4 = \{1,11,12,13\},\\
&\mathcal{B}_5 = \{2,5,8,11\}, && \mathcal{B}_6 = \{2,6,9,12\}, && \mathcal{B}_7 = \{2,7,10,13\}, && \mathcal{B}_8 = \{3,5,9,13\},\\
&\mathcal{B}_9 = \{3,6,10,11\}, && \mathcal{B}_{10} = \{3,7,8,12\}, && \mathcal{B}_{11} = \{4,5,10,12\}, && \mathcal{B}_{12} = \{4,6,8,13\},\\
&\mathcal{B}_{13} = \{4,7,9,11\}.
\end{aligned}$$

Accordingly, a network code $\mathcal{C}$ consists of thirteen components $\mathcal{C}_i$, $i = 1, \ldots, 13$. The subspace distance between subspaces from distinct components for this block design is $d_{\text{sub}} = 2k - 2\lambda = 6$. To provide the same distance for the whole code, distinct matrices (14) from the same component should belong to a matrix rank code with rank distance $d_r = 3$. Such a code can be obtained if we construct in advance a proper subcode of a *vector* code.

Consider, for example, the component $\mathcal{C}_3$ with multiindex $\mathcal{B}_3 = \{1,8,9,10\}$. The matrix $\widetilde{A}_3$ is of the form

$$\widetilde{A}_3 = \begin{pmatrix}
\boxtimes & \boxtimes & \boxtimes & \boxtimes & \boxtimes & \boxtimes & \boxtimes & \boxtimes & \boxtimes \\
0 & 0 & 0 & 0 & 0 & 0 & \boxtimes & \boxtimes & \boxtimes \\
0 & 0 & 0 & 0 & 0 & 0 & \boxtimes & \boxtimes & \boxtimes \\
0 & 0 & 0 & 0 & 0 & 0 & \boxtimes & \boxtimes & \boxtimes
\end{pmatrix}.$$

If the first 6 columns are all-zero, then the rank of the matrix $\widetilde{A}_3$ is equal to the rank of the submatrix consisting of the last 3 columns. In matrix representation, this submatrix corresponds to a vector of length 3 over the field $\mathbb{K}_{q^4}$. Construct an MRD $[3,1,3]$ code over the field $\mathbb{K}_{q^4}$. In matrix representation, we will get the maximal number $q^4 - 1$ of submatrices of rank 3.

However, if at least one of the first 6 elements of the first row is nonzero, then the rank of $\widetilde{A}_3$ equals 1 plus the rank of the 3×3 submatrix consisting of entries located at the intersection of the last 3 rows and last 3 columns. The rank of this submatrix should be not less than 2. In vector representation, this leads to an MRD $[3, 2, 2]$ code over the field $\mathbb{K}_{q^3}$. Hence, in matrix representation, we construct $q^{3\cdot 2} - 1 = q^6 - 1$ matrices of rank 2 or greater. This is compatible with the number of submatrices of rank 1 at the first 6 elements of the first row. We conclude that $|\mathcal{C}_3| = q^6$.

Careful choice of a subcode for each component allows us to maximize the code cardinality. For the above code, we have the following results:

$$|\mathcal{C}_1| = q^{18}, \quad |\mathcal{C}_2| = q^{12}, \quad |\mathcal{C}_3| = q^6, \quad |\mathcal{C}_4| = 1, \quad |\mathcal{C}_5| = q^6, \quad |\mathcal{C}_6| = q^4, \quad |\mathcal{C}_7| = q^2,$$
$$|\mathcal{C}_8| = q^3, \quad |\mathcal{C}_9| = q^4, \quad |\mathcal{C}_{10}| = q^5, \quad |\mathcal{C}_{11}| = q^3, \quad |\mathcal{C}_{12}| = q^4, \quad |\mathcal{C}_{13}| = q^5.$$

We have constructed a $[13, |\mathcal{C}|, 6, 4]$ code $\mathcal{C}$ of length $n = 13$ with subspace distance $d_{\text{sub}} = 6$, dimension $k = 4$, and cardinality $|\mathcal{C}| = q^{18} + q^{12} + 2q^6 + 2q^5 + 3q^4 + 2q^3 + q^2 + 1$. An upper bound for the cardinality is $M_{\max} = q^{18} + q^{15} + q^{14} + q^{12} + q^{11} + q^{10} + q^9 + q^8 + q^7 + q^6 + q^4 + q^3 + 1$ (see (3)).

5. CONCLUSION

A new class of rank subcodes (restricted rank codes) is developed. Based on this class, principles for constructing multicomponent codes for random network coding are found. The code cardinality equals the sum of component cardinalities. Code constructions use combinatorial balanced incomplete block designs and matrices in row-reduced echelon form. Parameters are chosen in such a way that the subspace distance between distinct components is not less than the subspace distance inside each component. Examples of codes with seven and thirteen components are presented.

REFERENCES

1. Wang, H., Xing, C., and Safavi-Naini, R., Linear Autentication Codes: Bounds and Constructions, *IEEE Trans. Inform. Theory*, 2003, vol. 49, no. 4, pp. 866–873.

2. Koetter, R. and Kschischang, F.R., Coding for Errors and Erasures in Random Network Coding, *IEEE Trans. Inform. Theory*, 2008, vol. 54, no. 8, pp. 3579–3591.

3. Silva, D., Kschischang, F.R., and Kötter, R., A Rank-Metric Approach to Error Control in Random Network Coding, *IEEE Trans. Inform. Theory*, 2008, vol. 54, no. 9, pp. 3951–3967.

4. Gabidulin, E.M., Theory of Codes with Maximum Rank Distance, *Probl. Peredachi Inf.*, 1985, vol. 21, no. 1, pp. 3–16 [*Probl. Inf. Trans.* (Engl. Transl.), 1985, vol. 21, no. 1, pp. 1–12].

5. Gabidulin, E.M. and Bossert, M., Codes for Network Coding, in *Proc. 2008 IEEE Int. Sympos. on Information Theory (ISIT'2008), Toronto, Canada*, 2008, pp. 867–870.

6. Gabidulin, E.M. and Bossert, M., Algebraic Codes for Network Coding, *Probl. Peredachi Inf.*, 2009, vol. 45, no. 4, pp. 54–68 [*Probl. Inf. Trans.* (Engl. Transl.), 2009, vol. 45, no. 4, pp. 343–356].

7. Gabidulin, E.M. and Pilipchuk, N.I., Multicomponent Network Coding, in *Proc. 7th Int. Workshop on Coding and Cryptography (WCC'2011), Paris, France, 2011*, pp. 443–452.

8. Gabidulin, E.M. and Pilipchuk, N.I., New Multicomponent Network Codes Based on Block Designs, in *Proc. Int. Mathematical Conf. "50 years of IITP," Moscow, 2011*, Moscow: Inst. Inf. Trans. Probl., 2011 (CD).

9. Skachek, V., Recursive Code Construction for Random Networks, *IEEE Trans. Inform. Theory*, 2010, vol. 56, no. 3, pp. 1378–1382.

10. Gadouleau, M. and Yan, Z., Construction and Covering Properties of Constant-Dimension Codes, in *Proc. 2009 IEEE Int. Sympos. on Information Theory (ISIT'2009), Seoul, Korea, 2009*, pp. 2221–2225.

11. Etzion, T. and Silberstein, N., Error-Correcting Codes in Projective Space via Rank-Metric Codes and Ferrers Diagrams, *IEEE Trans. Inform. Theory*, 2009, vol. 55, no. 7, pp. 2909–2919.

12. Etzion, T. and Silberstein, N., Codes and Designs Related to Lifted MRD Codes, `arXiv:1102.2593v4 [cs.IT]`, 2011.

13. Silberstein, N. and Etzion, T., Large Constant Dimension Codes and Lexicodes, *Adv. Math. Commun.*, 2011, vol. 5, no. 2, pp. 177–189.

14. Silberstein, N. and Etzion, T., Codes and Designs Related to Lifted MRD Codes, in *Proc. 2011 IEEE Int. Sympos. on Information Theory (ISIT'2011), St. Petersburg, Russia, 2011*, pp. 2288–2292.

15. Pilipchuk, N.I., Gabidulin, E.M., and Afanasiev, V.B., Decoding Multicomponent Codes Based on Rank Subcodes, in *Proc. 13th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT'2012), Pomorie, Bulgaria, 2012*, pp. 275–281.

16. Andrews, G.E., *The Theory of Partitions*, Reading, MA: Addison-Wesley, 1976. Translated under the title *Teoriya razbienii*, Moscow: Nauka, 1982.

17. Hall, M., Jr., *Combinatorial Theory*, Waltham: Blaisdell, 1967. Translated under the title *Kombinatorika*, Moscow: Mir, 1970.

18. Tarokh, V., Jafarkhani, H., and Calderbank, A.R., Space-Time Codes for High Data Rate Wireless Communication: Performance Criterion and Code Construction, *IEEE Trans. Inform. Theory*, 1998, vol. 44, no. 2, pp. 744–765.

19. Gabidulin, E.M., Bossert, M., and Lusina, P., Space-Time Codes Based on Rank Codes, in *Proc. 2000 IEEE Int. Symp. on Information Theory (ISIT'2000), Sorrento, Italy*, p. 283.

20. Gabidulin, E.M., Paramonov, A.V., and Tretjakov, O.V., Ideals over a Non-commutative Ring and Their Application in Cryptology, *Advances in Cryptology (Proc. EUROCRYPT'91: Workshop on the Theory and Application of Cryptographic Techniques, Brighton, UK, 1991)*, Davies, D.W., Ed., Lect. Notes Comp. Sci., vol. 547, Berlin: Springer, 1991, pp. 482–489.

21. Gabidulin, E.M., Pilipchuk, N.I., and Bossert, M., Decoding of Random Network Codes, *Probl. Peredachi Inf.*, 2010, vol. 46, no. 4, pp. 33–55 [*Probl. Inf. Trans.* (Engl. Transl.), 2010, vol. 46, no. 4, pp. 300–320].

22. Gabidulin, E.M., A Fast Matrix Decoding Algorithm for Rank-Error-Correcting Codes, *Proc. 1st French–Soviet Workshop on Algebraic Coding, Paris, France, 1991*, Cohen, G.D., Litsyn, S., Lobstein, A., and Zémor, G., Eds., Lect. Notes Comp. Sci., vol. 573, Berlin: Springer, 1992, pp. 126–133.

23. Paramonov, A.V. and Tretjakov, O.V., An Analogue of Berlekamp–Massey Algorithm for Decoding Codes in Rank Metric, in *Proc. Moscow Inst. Physics and Technology*, Moscow, 1991.

24. Sidorenko, V., Richter, G., and Bossert, M., Linearized Shift-Register Synthesis, *IEEE Trans. Inform. Theory*, 2011, vol. 57, no. 9, pp. 6025–6032.

25. Loidreau, P., A Welch–Berlekamp Like Algorithm for Decoding Gabidulin Codes, *Proc. 4th Int. Workshop on Coding and Cryptography (WCC'2005), Bergen, Norway, 2005*, Itrehus, Ø., Ed., Lect. Notes Comp. Sci., vol. 3969. Berlin: Springer, 2006, pp. 36–45.

26. Wachter, A.V., Afanasiev, V.B., and Sidorenko, V.R., Fast Decoding of Gabidulin Codes, in *Proc. 7th Int. Workshop on Coding and Cryptography (WCC'2011), Paris, France, 2011*, pp. 433–442.

27. Sidorenko, V., Schmidt, G., Gabidulin, E.M., Bossert, M., and Afanasiev, V.B., On Polyalphabetic Block Codes, in *Proc. 2005 IEEE ITSOC Information Theory Workshop on Coding and Complexity (ITW'2005), Rotorua, New Zealand, 2005*, pp. 207–210.