Multicomponent Network Coding

Ernst M. Gabidulin, Nina Pilipchuk

Multicomponent Network Coding

Ernst M. Gabidulin and Nina I. Pilipchuk

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

Abstract. In this paper, we propose so-called *multicomponent* codes with the prescribed subspace metric distance. This class is a generalization of the Silva-Kötter-Kschischang construction (SKK codes). Component constructions are chosen in such a manner that subspace distance between components would be not less than subspace distance of each component. Iterative decoding algorithm is proposed. A few examples are given.

Keywords: Network coding, subspace distance, rank-metric codes, decoding

1 Introduction

Network coding is a new area. A subspace approach [1] for network coding allows to overcome many previous restrictions on network configurations. Codes for network coding are proposed in several papers (see, [1] - [6]). A construction based on linearized polynomials was generalized in [4]. The lifting construction of Gabidulin's rank-metric code in the matrix representation was proposed by Wang et al. in [7] several years earlier in the context of authentication codes. It was independently reopened for network coding in [1].

This paper is devoted to constructing *multicomponent* codes with a specific subspace-metric distance. Our goal is to increase code cardinality which is an important performance for application background. We use the channel model from [1]. A special case where subspaces from the different components intersect only by 0-dimensional subspace ($\rho = 0$) was analyzed in [3]. Here, more general construction is presented ($\rho \neq 0$). The iterative decoding algorithm is constructed.

2 Definitions and notations

Let $\mathbb{F}_q$ be a finite field of q elements. Denote by $W_{N,q}$ a fixed N-dimensional vector space over the field $\mathbb{F}_q$. Let $\mathcal{P}(W_{N,q})$ be the set of all subspaces of $W_{N,q}$. The dimension of an element $V \in \mathcal{P}(W_{N,q})$ is denoted as $\dim(V)$. There exist subspaces of dimension $0, 1, \ldots, N$. An m-dimensional subspace V consists of q^m vectors of length N over the base field $\mathbb{F}_q$. It can be considered as the *row spanned* subspace of a $m \times N$ matrix $M(V)$ over $\mathbb{F}_q$ of full rank m. We refer to the matrix $M(V)$ as a *basis generator* matrix of V.

The set $\mathcal{P}(W_{N,q})$ is considered as the alphabet, or, as the signal space. We define two operations on the set $\mathcal{P}(W_{N,q})$. The *sum* of two subspaces $U \in \mathcal{P}(W_{N,q})$ and $V \in \mathcal{P}(W_{N,q})$ is defined as the unique subspace $C \in \mathcal{P}(W_{N,q})$ of the *minimal* dimension containing both U and V as subspaces. The sum is denoted as $C = U \oplus V$. If subspaces U and V are represented by their generator matrices $M(U)$ and $M(V)$, then the subspace $C = U \oplus V$ coincides with the row spanned subspace of a block matrix

$$M(C) = \begin{bmatrix} M(U) \\ M(V) \end{bmatrix}.$$

Given generator matrices $M(U)$ and $M(V)$, one can calculate $\dim(C)$ as

$$\dim(C) = \mathrm{Rk}(M(C)) = \mathrm{Rk}\left(\begin{bmatrix} M(U) \\ M(V) \end{bmatrix} \right).$$

The *product*, or, *intersection* of two subspaces $U \in \mathcal{P}(W_{N,q})$ and $V \in \mathcal{P}(W_{N,q})$ is defined as the unique subspace $C \in \mathcal{P}(W_{N,q})$ of the *maximal* dimension, which is contained both in U and in V. The product is denoted as $C = U \cap V$. In [1], the following metric on $\mathcal{P}(W_{N,q})$ is introduced. The *subspace distance* between two subspaces U and V is defined as follows:

$$d(U, V) = \dim(U \oplus V) - \dim(U \cap V). \tag{1}$$

The distance function takes values $\{0, 1, 2, \ldots, N\}$.

Any subset $\mathcal{C} \subseteq \mathcal{P}(W_{N,q})$ is called a *code*. The size of a code $\mathcal{C}$ is denoted by $|\mathcal{C}|$. The minimum subspace distance of $\mathcal{C}$ is denoted by $d(\mathcal{C}) = \min\{d(U, V) : U, V \in \mathcal{C}, U \neq V\}$. Given a metric the main problem of any coding theory are constructions of codes with a given distance. In [1] several families of subspace distance codes are presented, each codeword has the same dimension.

We need also another distance between matrices. Let A and B be two matrices of identical size. The *rank distance* $d_r(A, B)$ is defined as the rank of their difference: $d_r(A, B) = \mathrm{Rk}(A - B)$. If $\mathcal{M}$ is a matrix code, then a *rank code distance* $d_r(\mathcal{M})$ is defined as the minimal pairwise distance: $d_r(\mathcal{M}) = \min\{\mathrm{Rk}(A - B) : A, B \in \mathcal{M},\ A \neq B\}$.

3 Constructions of multicomponent *ρ-intersecting* codes

Let $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{P}(W_{N,q})$ be codes of subspace-metric distance $d_1,\ d_2$, respectively. Codes are said to be *ρ-intersecting*, if $\max\limits_{U \in \mathcal{C}_1,\ V \in \mathcal{C}_1} \dim(U \cap V) = \rho$.

Denote by $r_1 = \min(\dim(U) : U \in \mathcal{C}_1)$, $r_2 = \min(\dim(V) : V \in \mathcal{C}_2)$.

Lemma 1. *Let component codes $\mathcal{C}_1,\ \mathcal{C}_2$ be ρ-intersecting codes. Let $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$ be the code obtained as the union of component codes. We have:*

1. *The cardinality of $\mathcal{C}$ equals $|\mathcal{C}| = |\mathcal{C}_1| + |\mathcal{C}_2|$.*
2. *Subspace-metric distance of $\mathcal{C}$ equals $d(\mathcal{C}) = \min(d_1, d_2, r_1 + r_2 - 2\rho)$.*

Proof. The first statement is evident because codes $\mathcal{C}_1,\ \mathcal{C}_2$ have no common members. If $U_1, U_2 \in \mathcal{C}_1$, then $d(U_1, U_2) \geq d_1$. If $V_1, V_2 \in \mathcal{C}_2$, then $d(V_1, V_2) \geq d_2$. If $U \in \mathcal{C}_1,\ V \in \mathcal{C}_2$, then $d(U, V) = \dim(U)+\dim(V)-2\dim(U\cap V) \geq r_1+r_2-2\rho$. This proofs the second statement. □

Let us recall the lifting construction from [1].

Lemma 2 (Lifting construction). *Let $\mathcal{M}(m, N-m) = \mathcal{M}$ be a matrix code consisting of $m \times (N-m)$ matrices over $\mathbb{F}_q$. Let $d_r(\mathcal{M})$ be* rank-metric distance *of this code. Let a* subspace-metric *code $\mathcal{C}$ be defined in terms of basis generator matrices as a set of $m \times N$ basic matrices over $\mathbb{F}_q$ of the form*

$$\mathcal{C} = \left\{ \left[I_m \ M \right] \mid M \in \mathcal{M} \right\},$$

where I_m is the identity matrix of order m. Then subspace-metric distance $d(\mathcal{C}) = 2d_r(\mathcal{M})$.

A code $\mathcal{C}$ is called a Silva–Kötter–Kschischang code, or, SKK code. We will use codes with a *all zero prefix matrix* :

$$\mathcal{C} = \left\{ \left[0_m^v \ I_m \ M \right] \mid M \in \mathcal{M} \right\}, \tag{2}$$

where 0_m^v is the all zero matrix of size $m \times v$.

The union of several pairwise ρ-intersecting component codes is a multicomponent code. Let $N = m_1 + m_2 + \cdots + m_k$ be a partition of the integer N. Let I_{m_1} be the identity matrix of order m_1. Let $\mathcal{M}_1 = \mathcal{M}_1(m_1, N-m_1)$ be a rank-metric code consisting of matrices in $\mathbb{F}_q$ of size $m_1 \times (N-m_1)$ with rank-distance $d_{r,1} \leq \min(m_1, N-m_1)$. Define the first subspace-metric component code $\mathcal{C}_1$ in terms of the set of basic $m_1 \times N$ generator matrices as follows:

$$\mathcal{C}_1 = \left\{ \left[I_{m_1} \ M_1 \right] \mid M_1 \in \mathcal{M}_1 \right\}. \tag{3}$$

This is a SKK code. All members of $\mathcal{C}_1$ are of dimension m_1. Therefore the minimal dimension is $r_1 = m_1$. The subspace-metric code distance is equal to $d_1 = 2d_{r,1}$ by Lemma 2. Let $a_1 = \max\{N-m_1, m_1\},\ b_1 = \min\{N-m_1, m_1\}$. The cardinality is

$$|\mathcal{C}_1| = q^{a_1(b_1-d_{r,1}+1)}.$$

Similarly, let $O_{m_2}^{v_1}$ be the all zero matrix of size $m_2 \times v_1$, I_{m_2} be the identity matrix of order m_2. Assume that $m_1 - m_2 + 1 \leq v_1 \leq m_1$. Let $\mathcal{M}_2$ be a rank-metric code consisting of matrices in $\mathbb{F}_q$ of size $m_2 \times (N-v_1-m_2)$ with rank-distance $d_{r,2} \leq \min(m_1, N-v_1-m_2)$. Define the second subspace-metric component code $\mathcal{C}_2$ in terms of the set of basic $m_2 \times N$ generator matrices as

$$\mathcal{C}_2 = \left\{ \left[O_{m_2}^{v_1} \ I_{m_2} \ M_2 \right] \mid M_2 \in \mathcal{M}_2 \right\}. \tag{4}$$

This code differ from a SKK code by the zero prefix matrix $O_{m_2}^{v_1}$. All members of $\mathcal{C}_2$ are of dimension m_2. Therefore the minimal dimension is $r_2 = m_2$. It has

subspace distance $d_2 = 2d_{r,2}$ by Lemma 2. Let $a_2 = \max\{N - v_1 - m_2, m_2\},\ b_2 = \min\{N - v_1 - m_2, m_2\}$. The cardinality is

$$|\mathcal{C}_2| = q^{a_2(b_2 - d_{r,2}+1)}.$$

In turn, the maximal dimension of the pairwise intersection of the codes $\mathcal{C}_1$ and $\mathcal{C}_2$ is $\rho = m_1 - v_1$. Therefore the subspace distance between these codes is equal to $d(\mathcal{C}_1, \mathcal{C}_2) = m_1 + m_2 - 2\rho = m_2 - m_1 + 2v_1$. We obtain

$$d(\mathcal{C}_1 \cup \mathcal{C}_2) = \min\{2d_{r,1},\ 2d_{r,2},\ m_2 - m_1 + 2v_1\}.$$

If we continue to the $(k-1)$th step, we define

$$\mathcal{C}_{k-1} = \left\{ \left[O_{m_{k-1}}^{v_1+v_2+\cdots+v_{k-2}}\ I_{m_{k-1}}\ M_{k-1} \right] \mid M_{k-1} \in \mathcal{M}_{k-1} \right\}, \tag{5}$$

where $m_{k-2} - m_{k-1} + 1 \le v_{k-2} \le m_{k-2}$ and $\mathcal{M}_{k-1}$ is a rank-metric code consisting of matrices in $\mathbb{F}_q$ of size $m_{k-1} \times (N - v_1 - v_2 - \cdots - v_{k-2} - m_{k-1})$ with rank-distance $d_{r,k-1} \le \min(m_{k-1}, N - v_1 - v_2 - \cdots - v_{k-2} - m_{k-1})$. Let $a_{k-1} = \max\{N - v_1 - v_2 - \cdots - v_{k-2} - m_{k-1}, m_{k-1}\},\ b_{k-1} = \min\{N - v_1 - v_2 - \cdots - v_{k-2} - m_{k-1}, m_{k-1}\}$. The cardinality is

$$|\mathcal{C}_{k-1}| = q^{a_{k-1}(b_{k-1} - d_{r,k-1}+1)}.$$

The last kth component code consists of the only m_k-dimensional subspace generated by a basic $m_k \times N$ matrix of the form

$$\mathcal{C}_k = \left[O_{m_k}^{N-m_k}\ I_{m_k} \right]. \tag{6}$$

Consider the code $\mathcal{C}$ which is the union of components codes above: $\mathcal{C} = \bigcup_{i=1}^{k} \mathcal{C}_i$. We have proved the following theorem.

Theorem 1. *The cardinality of $\mathcal{C}$ is equal to $|\mathcal{C}| = \sum_{i=1}^{k} |\mathcal{C}_i|$. The code $\mathcal{C}$ has subspace-metric distance*

$$d(\mathcal{C}) = \min\{ \min_{1 \le i \le k-1} (m_{i+1} - m_i + 2v_i), \min_{1 \le i \le k-1} \{2d_{r,i}\} \}. \tag{7}$$

4 Choice of parameters

Multicomponent codes depend on parameters $v_i,\ i = 1, 2, \ldots, k$. These parameters have an influence on cardinality of component codes and on distance between components. Increasing the v decreases the cardinality of the corresponding component but increases distance between this and previous components.

Example 1. Let $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$ be a two-component code with parameters $m_1 = 5,\ m_2 = 3,\ N = 11$. Let $v_1 = m_1 = 5$.

$$
\begin{array}{ccccccccccccccccccccc}
1 & 0 & 0 & 0 & 0 & m_{11} & m_{12} & m_{13} & m_{14} & m_{15} & m_{16} \\
0 & 1 & 0 & 0 & 0 & m_{21} & m_{22} & m_{23} & m_{24} & m_{25} & m_{26} \\
0 & 0 & 1 & 0 & 0 & m_{31} & m_{32} & m_{33} & m_{34} & m_{35} & m_{36} \\
0 & 0 & 0 & 1 & 0 & m_{41} & m_{42} & m_{43} & m_{44} & m_{45} & m_{46} \\
0 & 0 & 0 & 0 & 1 & m_{51} & m_{52} & m_{53} & m_{54} & m_{55} & m_{56} \\
- & - \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & a_{11} & a_{12} & a_{13} \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & a_{21} & a_{22} & a_{23} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & a_{31} & a_{32} & a_{33}
\end{array}
$$

The upper part is a subspace code $\mathcal{C}_1$. It can have subspace distance in the interval $2 \le d(\mathcal{C}_1) \le 10$. The lower part is a subspace code $\mathcal{C}_2$. It can have subspace distance in the interval $2 \le d(\mathcal{C}_2) \le 6$.
Subspace distance of the code $\mathcal{C} = \mathcal{C}_1 + \mathcal{C}_2$ locates in the interval $2 \le d(\mathcal{C}) = d(\mathcal{C}_1 \cup \mathcal{C}_2) \le 6$.
Subspace distance between $\mathcal{C}_1$ and $\mathcal{C}_2$ is equal to $m_1 + m_2 = 8$.
Cardinality of the code $\mathcal{C}_1$ equals $q^{(N-m_1)k_1}$, where $k_1 = m_1 - d_{r1} + 1$.
Cardinality of the code $\mathcal{C}_2$ equals $q^{(N-m_1-m_2)k_2}$, where $k_2 = m_2 - d_{r2} + 1$.

Let $d_{r1} = d_{r2} = 3$. Then $k_1 = m_1 - d_r + 1 = 3$, $k_2 = m_2 - d_r + 1 = 1$. Cardinality of the code $\mathcal{C}_1$ equals $2^{6 \cdot 3} = 2^{18}$. Cardinality of the code $\mathcal{C}_2$ equals $2^{3 \cdot 1} = 2^3$. One can see $|\mathcal{C}_2| \ll |\mathcal{C}_1|$. Subspace code distance is $d(\mathcal{C}) = 6$.

We see that the first component code has the maximal cardinality. The cardinality of next components decreases exponentially. To increase cardinality let us change the parameter v_1 to $v_1 = m_1 - 1 = 4$.

The two-component code $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$ has parameters $m_1 = 5,\ m_2 = 3,\ N = 11,\ v_1 = 4$.

$$
\begin{array}{ccccccccccccccccccccc}
1 & 0 & 0 & 0 & 0 & m_{11} & m_{12} & m_{13} & m_{14} & m_{15} & m_{16} \\
0 & 1 & 0 & 0 & 0 & m_{21} & m_{22} & m_{23} & m_{24} & m_{25} & m_{26} \\
0 & 0 & 1 & 0 & 0 & m_{31} & m_{32} & m_{33} & m_{34} & m_{35} & m_{36} \\
0 & 0 & 0 & 1 & 0 & m_{41} & m_{42} & m_{43} & m_{44} & m_{45} & m_{46} \\
0 & 0 & 0 & 0 & 1 & m_{51} & m_{52} & m_{53} & m_{54} & m_{55} & m_{56} \\
- & - \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & a_{11} & a_{12} & a_{13} & a_{14} \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & a_{21} & a_{22} & a_{23} & a_{24} \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & a_{31} & a_{32} & a_{33} & a_{34}
\end{array}
$$

Subspace distance between $\mathcal{C}_1$ and $\mathcal{C}_2$ equals $m_1 + m_2 - 2 = 6$. Now cardinality of the first code $\mathcal{C}_1$ is the same as before, that is $\mid \mathcal{C}_1 \mid = 2^{18}$, cardinality of the second code $|\mathcal{C}_2| = 2^{4 \cdot 1} = 2^4$, that is twice more than before. Subspace code distance is as before: $d(\mathcal{C}) = 6$. We can not set v_1 less without decreasing subspace code distance.

In general, consider the case where the first code $\mathcal{C}_1$ is presented by matrices $\widetilde{M_1} = [I_{m_1} M_1]$, the second code is presented by matrices $\widetilde{M_2} = [O_{m_2}^{v_1} I_{m_2} M_2]$,

$O_{m_2}^{v_1}$ is the all zero matrix of size $m_2 \times v_1$. Let us obtain an optimal value of v_1 using the following condition: the value of subspace distance of any component code is identical and is equal to the value of subspace distance between components. For any component code this value equals $2d_r$, where d_r is rank code distance. Denote by $\langle C \rangle$ the subspace spanned by rows of a matrix C. For a two-component code, the value of subspace distance can be obtained as

$$\begin{aligned} d(\langle C_1 \rangle, \langle C_2 \rangle) &= 2\mathrm{Rk}\left(\begin{bmatrix} \widetilde{M_1} \\ \widetilde{M_2} \end{bmatrix}\right) - \mathrm{Rk}(\widetilde{M_1}) - \mathrm{Rk}(\widetilde{M_2}) \\ &= 2(v_1 + m_2) - m_1 - m_2 = 2v_1 - m_1 + m_2. \end{aligned}$$

Our condition is satisfied if $2v_1 - m_1 + m_2 \geq 2d_r$. Therefore $v_1 = d_r + \lceil \frac{m_1 - m_2}{2} \rceil$.

Example 2. Let $N = km$ and $m_1 = m_2 = \cdots = m_k = m$. Choose $v_1 = v_2 = \cdots = v_{k-1} = m$. This is the case analyzed in [3]. Here, we can choose k component codes. Let $\mathcal{M}_1 = \mathcal{M}_1(m, (k-1)m), \mathcal{M}_2 = \mathcal{M}_2(m, (k-2)m), \ldots, \mathcal{M}_{k-1} = \mathcal{M}_{k-1}(m, m)$ be MRD codes with the same *rank-metric* distance d_r. Then the construction above gives a code $\mathcal{C}$ of cardinality

$$|\mathcal{C}| = \sum_{p=0}^{k-1} q^{m(m-d_r+1)p} = \frac{q^{m(m-d_r+1)k} - 1}{q^{m(m-d_r+1)} - 1}$$

and with *subspace-metric* distance $d(\mathcal{C}) = 2d_r$. In particular, if a matrix code $\mathcal{M}$ is chosen with maximal possible rank distance $d_r = m$, then the code is an optimal constant-dimension constant-distance code proposed in [2].

Example 3. Let $N = km$ and $m_1 = m_2 = \cdots = m_k = m$. These parameters are as above but we choose $v_1 = v_2 = \cdots = v_{k-1} = d_r$. The *subspace-metric* distance remains the same: $d(\mathcal{C}) = 2d_r$, but we can define $s + 1 > k$ component codes, where $s = \lfloor (k-1)m/d_r \rfloor$. In this case $\mathcal{M}_1 = \mathcal{M}_1(m, (k-1)m), \mathcal{M}_2 = \mathcal{M}_2(m, (k-1)m - d_r), \ldots, \mathcal{M}_s = \mathcal{M}_s(m, \lfloor (k-1)m/d_r \rfloor)$ be MRD codes with the same *rank-metric* distance d_r. Then the code $\mathcal{C}$ cardinality is

$$|\mathcal{C}| = \sum_{p=0}^{s} q^{(km-m-pd_r)(m-d_r+1)} + 1.$$

Example 4. Multicomponent codes $\mathcal{C}$ with subspace distance $d(\mathcal{C}) = 4$ can be constructed with additional components. We demonstrate this by an example. Let the dimension of code subspaces be $m = 4$, length $N = 10$ and $q = 2$. Consider the following seven code components:

$$\mathcal{C}_1 = \left\{ \begin{bmatrix} I_2 & 0 & M_{11} & M_{12} & M_{13} \\ 0 & I_2 & M_{21} & M_{22} & M_{23} \end{bmatrix} \right\} \quad \mathcal{C}_2 = \left\{ \begin{bmatrix} I_2 & L_1 & 0 & F_{12} & F_{13} \\ 0 & 0 & I_2 & F_{22} & F_{23} \end{bmatrix} \right\}$$

$$\mathcal{C}_3 = \left\{ \begin{bmatrix} 0 & I_2 & 0 & G_{12} & G_{13} \\ 0 & 0 & I_2 & G_{22} & G_{23} \end{bmatrix} \right\} \quad \mathcal{C}_4 = \left\{ \begin{bmatrix} 0 & I_2 & L_2 & 0 & E_1 \\ 0 & 0 & 0 & I_2 & E_2 \end{bmatrix} \right\}$$

$$\mathcal{C}_5 = \left\{ \begin{bmatrix} 0 & 0 & I_2 & 0 & H_1 \\ 0 & 0 & 0 & I_2 & H_2 \end{bmatrix} \right\} \quad \mathcal{C}_6 = \left\{ \begin{bmatrix} 0 & 0 & I_2 & L_3 & 0 \\ 0 & 0 & 0 & 0 & I_2 \end{bmatrix} \right\} \quad \mathcal{C}_7 = \left\{ \begin{bmatrix} 0 & 0 & 0 & I_2 & 0 \\ 0 & 0 & 0 & 0 & I_2 \end{bmatrix} \right\}$$

Matrices $M_{ij},\ F_{ij},\ G_{ij},\ L_i,\ E_i,\ H_i$ of size 2×2 will be chosen later. But one can see that for all such matrices, the subspace distance between any couple of matrices from *different* components is at least 4. Therefore matrices above must be chosen in such a manner that the subspace distance between any couple of matrices from the same component would be not less than 4. Yo provide this, it is enough: (1) in the component $\mathcal{C}_1$ matrices $M_{11} \dots M_{21}$ all together form a code of 6×4 matrices with *rank* distance $d_r = 2$, $|\mathcal{C}_1| = 2^{6 \cdot 3} = 262144$; (2) in the component $\mathcal{C}_2$ $\{L_1\}$ must be a rank-distance code of 2×2 matrices with $d_r = 2$, $|\{L_1\}| = 2^2$; $\{F_{12} \dots F_{23}\}$ must be a rank-distance code of 4×4 matrices with $d_r = 2$, $|\{F_{12} \dots F_{23}| = 2^{4 \cdot 3}\}$, $|\mathcal{C}_2| = 2^2 \cdot 2^{12} = 16384$; (3) in the component $\mathcal{C}_3$ matrices $G_{12} \dots G_{23}$ all together form a code of 4×4 matrices with *rank* distance $d_r = 2$, $|\mathcal{C}_3| = 2^{4 \cdot 3} = 4096$; (4) in the component $\mathcal{C}_4$ $\{L_2\}$ must be a rank-distance code of 2×2 matrices with $d_r = 2$, $|\{L_2\}| = 2^2$; $\{E_1 \dots E_2\}$ must be a rank-distance code of 4×2 matrices with $d_r = 2$, $|\{E_1 \dots E_2\}| = 2^4$, $|\mathcal{C}_4| = 2^2 \cdot 2^4 = 64$; (5) in the component $\mathcal{C}_5$ matrices $H_1 \dots H_2$ all together form a code of 4×2 matrices with *rank* distance $d_r = 2$, $|\mathcal{C}_5| = 2^4 = 16$; (6) in the component $\mathcal{C}_6$ $\{L_3\}$ must be a rank-distance code of 2×2 matrices with $d_r = 2$, $|\{L_3\}| = 2^2$, $|\mathcal{C}_6| = 4$. The component $\mathcal{C}_7$ consists of the only matrix.

The cardinality of the constructed code $\mathcal{C} = \cup_{i=1}^{7} \mathcal{C}_i$ is equal to $|\mathcal{C}| = 262144 + 16384 + 4096 + 64 + 16 + 4 + 1 = 282709$. Note that the code constructed by Theorem 1 would consist of components $\mathcal{C}_1,\ \mathcal{C}_3,\ \mathcal{C}_5,\ \mathcal{C}_7$ with cardinality 266257.

This approach can be generalized to other values of subspace distances.

Example 5. To compare our results with known results, we have borrowed the table from [6] and add one extra column with cardinalities of multicomponent codes. There is no comparison with results of [5] because their constructions are based on q-cyclic MDR codes but such codes exist only for length coinciding with degree of the field extension. It follows from the table that multicomponent codes at least as good as other constructions, sometimes better.

Table 1. Cardinalities of SKK codes, Skachek codes, Gadouleau–Yan codes, and multicomponent codes in $\mathcal{P}(W_{10,2})$ for $2 \le m \le 5$

m	d_{sub}	SKK	Skachek	Gadouleau–Yan	**Multicomp**
2	4	256	340	320	**341**
3	4	16384	16640	17408	**17473**
	6	128	144	144	**145**
4	4	262144	262144	278544	**282709**
	6	4096	4096	4112	**4113**
	8	64	64	65	**65**
5	4	1048576	1048576	1056769	**1060873**
	6	32768	32768	32769	**32801**
	8	1024	1024	1025	**1025**
	10	32	32	33	**33**

5 Iterative decoding algorithm

Let us construct an iterative decoding algorithm for these multicomponent codes.

Example 6. Suppose, we construct a subspace code $\mathcal{C} = \{X_1,\ X_2\}$ of length m consisting of two subspace only. The first subspace is represented by the matrix $X_1 = I_m$, the second subspace is represented by the matrix $X_2 = O_m$.

Assume that the channel is described by the equation [1]

$$Y = AX + BZ, \tag{8}$$

where $X \in \mathcal{C}$, A is a matrix of random transformations of a signal matrix X, BZ is a random matrix of errors. We know the received matrix Y and want to decide what a matrix X was sent.

Let a transmitted matrix be $X_1 = I_m$. Then the received matrix is

$$Y = AX_1 + BZ = A + BZ$$

Let a transmitted matrix be $X_2 = O_m$. Then the received matrix is

$$Y = AX_2 + BZ = BZ.$$

The decoder calculates a distance between the received subspace $\langle Y \rangle$ and each of the subspaces $\langle X_1 \rangle$ and $\langle X_2 \rangle$ correspondingly:

$$d_1 = d(\langle Y \rangle, \langle X_1 \rangle) = 2\mathrm{Rk}\left(\begin{bmatrix} Y \\ I_m \end{bmatrix}\right) - \mathrm{Rk}(Y) - \mathrm{Rk}(I_m) = 2m - \mathrm{Rk}(Y) - m = m - \mathrm{Rk}(Y),$$

$$d_2 = d(\langle Y \rangle, \langle X_2 \rangle) = 2\mathrm{Rk}\left(\begin{bmatrix} Y \\ O_m \end{bmatrix}\right) - \mathrm{Rk}(Y) - \mathrm{Rk}(O_m) = 2\mathrm{Rk}(Y) - \mathrm{Rk}(Y) = \mathrm{Rk}(Y).$$

If $d_1 < d_2 (\mathrm{Rk}(Y) > m/2)$, then the decoder gives the solution $X = X_1 = I_m$. If $d_1 \geq d_2$ $(\mathrm{Rk}(Y) \leq m/2)$, then the decoder gives the solution $X = X_2 = O_m$.

Example 7. We consider the code $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$ with subspace distance $2m$ between component codes as a union of two subcodes $\mathcal{C}_1,\ \mathcal{C}_2$. Here

$$\mathcal{C}_1 = \left\{X : X = \begin{bmatrix} I_m\ M \end{bmatrix},\ M \in \mathcal{C}\right\}$$

– a subcode, $\mathcal{C}$ – a matrix subcode of size $m \times m$. Let

$$\mathcal{C}_2 = \left\{X : X = \begin{bmatrix} O_m\ I_m \end{bmatrix}\right\}$$

be another code with cardinality 1.

Let the received matrix be

$$Y = AX + BZ = \left[\widehat{A}\ y\right],$$

where $\widehat{A}$ is the submatrix with m columns. The decoding procedure consists of two stages. At the first stage the decoder recognizes if $X \in \mathcal{C}_1$, or, $X \in \mathcal{C}_2$. To decide, the decoder uses the submatrix $\widehat{A}$ of the received matrix Y. The problem is reduced to the problem of Example 6: to recognize if the subspace $\langle \widehat{A} \rangle$ corresponds to $\langle I_m \rangle$, or, to $\langle O_m \rangle$. To answer this question, the decoder calculates the rank of the matrix $\mathrm{Rk}(\widehat{A})$:

– If $\mathrm{Rk}(\widehat{A}) > m/2$, that means $\langle Y \rangle$ corresponds to $\mathcal{C}_1$. Then the decoder uses SKK decoding procedure [1] and obtains $X = \left[I_m \; M \right]$ as a decoding result.
– If $\mathrm{Rk}(\widehat{A}) \leq m/2$, then the subspace $\langle Y \rangle$ corresponds to $\mathcal{C}_2$. Then the decoder takes the matrix $\left[O_m \; I_m \right]$ as a result of the decoding.

Example 8. We consider the two-component code $\mathcal{C}$ which is an union of two subcodes $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$, where

$$\mathcal{C}_1 = \left\{ X : X = \left[I_{m_1} \; M_1 \right] \right\},$$

$$\mathcal{C}_2 = \left\{ X : X = \left[O_{m_2}^{v_1} \; I_{m_2} \; M_2 \right] \right\}.$$

Assume that $m_2 \leq m_1$, $m_1 - m_2 + 1 \leq v_1 \leq m_2$.

Suppose, we received a matrix Y and have to solve the following problem: if X belongs to $\mathcal{C}_1$, or, X belongs to $\mathcal{C}_2$. Represent the received matrix as

$$Y = AX + BZ = \left[\widehat{A} \; y \right],$$

where $\widehat{A}$ is the submatrix with m_1 columns. All matrices of the code $\mathcal{C}_1$ have as the submatrix of the first m_1 columns the matrix I_{m_1}. All matrices of the code $\mathcal{C}_2$ have as the submatrix of the first m_1 columns the matrix

$$G = \begin{bmatrix} O_{m_1 - v_1}^{v_1} & I_{m_1 - v_1} \\ O_{m_2 - m_1 + v_1}^{v_1} & O_{m_2 - m_1 + v_1}^{m_1 - v_1} \end{bmatrix}.$$

The subspace distance between $\langle \widehat{A} \rangle$ and $\langle I_{m_1} \rangle$ equals

$$d_1 = d(\langle \widehat{A} \rangle, \langle I_{m_1} \rangle) = m_1 - \mathrm{Rk}(\widehat{A}).$$

The subspace distance between $\langle \widehat{A} \rangle$ and $\langle G \rangle$ equals

$$d_2 = d(\langle \widehat{A} \rangle, \langle G \rangle) = 2\mathrm{Rk}\left(\begin{bmatrix} \widehat{A} \\ G \end{bmatrix} \right) - \mathrm{Rk}(\widehat{A}) - \mathrm{Rk}(G).$$

We have

$$\mathrm{Rk}\left(\begin{bmatrix} \widehat{A} \\ G \end{bmatrix} \right) = \mathrm{Rk}(\widetilde{\widehat{A}}) + m_1 - v_1,$$

where $\widetilde{\widehat{A}}$ is the matrix $\widehat{A}$ without $m_1 - v_1$ right columns. Therefore

$$d_2 = d(\langle \widehat{A} \rangle, \langle G \rangle) = 2\mathrm{Rk}(\widetilde{\widehat{A}}) + 2(m_1 - v_1) - \mathrm{Rk}(\widehat{A}) - (m_1 - v_1).$$

Compare distances d_1 and d_2.

If $d_1 < d_2$, i.e. $v_1/2 < \mathrm{Rk}(\widetilde{\widehat{A}})$, then the solution is I_{m_1}, i.e. $X \in \mathcal{C}_1$.
Otherwise the solution is G, i.e. $X \in \mathcal{C}_2$.

Now suppose that we have a multicomponent *ρ-intersecting* subspace code $\mathcal{C}$ which is an union of s subcodes $\mathcal{C}_i$, $i = \overline{1,s}$. At the receiver we have the matrix Y, where

$$Y = AX + BZ$$

and X belongs to one of the component codes.

Step 1 is solving the problem: $X \in \mathcal{C}_1$ or $X \in \cup_{i=2}^{s}\mathcal{C}_i$? For our construction, this problem is equivalent to the problem: $X \in \mathcal{C}_1$ or $X \in \mathcal{C}_2$? We use results of Example 8 to solve this problem. If the solution is $X \in \mathcal{C}_1$, then we apply to Y SKK decoding to extract X.

Otherwise we go to Step 2: $X \in \mathcal{C}_2$ or $X \in \mathcal{C}_3$? Apply again results of Example 8 to solve this problem. Note that v_1 left columns in Y and in $\mathcal{C}_2$, $\mathcal{C}_3$ can be deleted without changing of results. If the solution is $X \in \mathcal{C}_2$, then we apply to shortened Y SKK decoding to extract X.

Otherwise we go to Step 3: $X \in \mathcal{C}_3$ or $X \in \mathcal{C}_4$? Apply again results of Example 8 to solve this problem. Note that $v_1 + v_2$ left columns in Y and in $\mathcal{C}_3$, $\mathcal{C}_4$ can be deleted without changing of results. Continue until the final solution.

6 Conclusion

A family of multicomponent *ρ-intersecting* subspace codes for network coding is presented. The optimal parameters are chosen under the following condition: any component subspace distance is equal to a subspace distance between components. The iterative decoding algorithm is constructed. The comparison with codes from the papers [3] - [6] is made. These codes are at least as good as other constructions from [6] (sometimes better) and always better than constructions from [3].

References

1. Silva D., Kschischang F.R., and Koetter R.: A Rank-Metric Approach to Error Control in Random Network Coding. IEEE Trans. On Inform. Theory. Vol. 54., No. 9, pp. 3951-3967 (2008)
2. Gabidulin E., Bossert M.: Codes for Network Coding. In: Proc. of the 2008 IEEE International Symposium on Information Theory (ISIT 2008), pp. 867-870. Toronto, ON, Canada, 6-11 July (2008)
3. Gabidulin E.M., and Bossert M.: A Family of Algebraic Codes for Network Coding. Probl. Inform. Transm. Vol. 45. No. 4, pp. 54–68 (2009)
4. Skachek V.: Recursive Code Construction for Random Networks. IEEE Trans. On Inform. Theory. V. 56. No. 3, pp. 1378-1382 (2010)
5. Etzion T., and Silberstein N.: Error-Correcting Codes in Projective Spaces Via Rank-Metric Codes and Ferrers Diagrams. IEEE Trans. On Inform. Theory. V. 55. No. 7, pp. 29092919 (2009).
6. Gadouleau M., and Yan Z.: Construction and Covering Properties of Constant-Dimension Codes. In: Proc. of the 2009 IEEE International Symposium on Information Theory (ISIT 2009), pp. 2221-2225. Nice, France, 24-29 June (2007)
7. Wang H. , Xing C., and Safavi-Naini R.: Linear authentication codes: bounds and constructions. IEEE Trans. On Inform. Theory. V. 49. No. 4, pp. 866873 (2003).