Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 275–281*

Decoding multicomponent codes based on rank subcodes [1]

N. I. Pilipchuk pilipchuk.nina@gmail.com
Moscow Institute of Physics and Technology (State University)
E. M. Gabidulin ernst_gabidulin@yahoo.com
Moscow Institute of Physics and Technology (State University)
V. B. Afanassiev afanv@iitp.ru
Institute of Information Transmission Problems of the Russian Academy of Sciences

Abstract. We consider decoding algorithm of multicomponent codes based on subspace rank subcodes [1]. These codes are constructed by combinatorial incomplete balanced block-scheme and are assigned to random network coding [2], [3], [4]. Examples are given.

1 Introduction

Multicomponent codes are an union of component codes of a definite minimal code distance having the same minimum distance between any two components. Cardinality of such code is a sum of cardinalities of all component codes. The first paper devoted to multicomponent codes with lifted code matrix construction [2] was published in 2009 [6]. These codes are a set of lifting construction matrix with extra zero matrices as prefix. The every code matrix is a concatenation of zero matrices, the unit matrix and a rank code matrix [5]. The other approach with so called Ferrets diagrams was used in [3]. Here, we give the new constructions of rank - metric subcodes [1] based on combinatorial incomplete balanced block-schemes.

2 Reduced echelon form

Let us recall random network codes by Silva–Kschischang–Koetter (SKK-codes) [2]. They are represented as a set of basis $k \times n$ matrices over the base field $\mathbb{F}_q$. The matrix is presented in so called lifting construction:

$$\mathcal{C} = \left\{ \begin{bmatrix} I_k & M \end{bmatrix} \right\}, \tag{1}$$

where I_k – unit matrix of order k, $M \in \mathcal{M}$ – $k \times (n-k)$ matrix of the rank code $\mathcal{M}$. Let d_r be *rank distance*, then subspace distance equals $d(\mathcal{C}) = 2d_r(\mathcal{M})$.

[1] This research is partially supported by the grant RFBR 12-07-00122-a

Consider more general form. Let X be a $k \times n$ matrix of rank k. By Gaussian procedure we get X as $k \times n$ matrix of rank k in *reduced echelon form.* The following conditions are satisfied:

- the leading element of a row is located on the right of the leading element of a preceding row;
- all leading element are units;
- all elements on the left of leading elements are zeros;
- each leading element is the only nonzero element in a column;
- all other elements are "*free parameters.*"

Suppose that the leading element of the first row is in a column number i_1, the leading element of the second row is in a column number i_2, and so on, the leading element of the last row is in a column number i_k, where $1 \leq i_1 < i_2 < \cdots < i_k \leq n$. The vector $\mathbf{i} = [i_1\ i_2\ \ldots\ i_k]$ is called identifier ID of this form, and the designated matrix is $X(\mathbf{i}, \mathbf{a})$, where $\mathbf{a}$ are "*free parameters*".

Example 1. *Let be* $n = 6, k = 3$, $ID = \mathbf{i} = [1\ 3\ 4]$, *then there are* 7 *free parameters* $a_{i,j}$ *over* $\mathbb{F}_q$ *in*

$$X(\mathbf{i}, \mathbf{a}) = \begin{bmatrix} 1 & a_{1,1} & 0 & 0 & a_{1,2} & a_{1,3} \\ 0 & 0 & 1 & 0 & a_{2,2} & a_{2,3} \\ 0 & 0 & 0 & 1 & a_{3,2} & a_{3,3} \end{bmatrix}.$$

3 Incomplete balanced block-schemes

By definition, incomplete balanced block-scheme is such a disposition where n different elements are in b blocks and the each block contains exactly k different elements, each element appears in â r different blocks and each pair of different elements a_i, a_j appears exactly in λ blocks.

Let $\mathcal{S} = \{1, 2, \ldots, n\}$ be a set of elements. Giving the parameters $k, r, \lambda \geq 1$ we construct a configuration, called 2 B-block, as a set of subsets. Each subset has k elements from $\mathcal{S}$. It is necessary to satisfy the following condition: the number r blocks, which contain definite i elements from $\mathcal{S}$, does not depend on value i, the number λ blocks, which contains different pairs i, j from $\mathcal{S}$ does not depend on their values.

These configurations are determined by the parameters (n, k, λ), or equivalently by (n, b, r, k, λ) where $bk = vr$ and $r(k-1) = \lambda(v-1)$ [8].

Multicomponent code with seven components

Let be $k = 3, n = 7, d_r = 2$. Construct 7 blocks as identifiers with the corresponding code matrices where a_i - free parameters.

$$B_1^\top = \begin{bmatrix}1\\2\\3\end{bmatrix} = \begin{pmatrix} 1 & 0 & 0 & a_1 & a_2 & a_3 & a_4 \\ 0 & 1 & 0 & a_5 & a_6 & a_7 & a_8 \\ 0 & 0 & 1 & a_9 & a_{10} & a_{11} & a_{12} \end{pmatrix}$$

$$B_2^\top = \begin{bmatrix}1\\4\\5\end{bmatrix} = \begin{pmatrix} 1 & a_1 & a_2 & 0 & 0 & a_3 & a_4 \\ 0 & 0 & 0 & 1 & 0 & a_5 & a_6 \\ 0 & 0 & 0 & 0 & 1 & a_7 & a_8 \end{pmatrix}$$

$$B_3^\top = \begin{bmatrix}1\\6\\7\end{bmatrix} = \begin{pmatrix} 1 & a_1 & a_2 & a_3 & a_4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$B_4^\top = \begin{bmatrix}2\\4\\6\end{bmatrix} = \begin{pmatrix} 0 & 1 & a_1 & 0 & a_2 & 0 & a_3 \\ 0 & 0 & 0 & 1 & a_4 & 0 & a_5 \\ 0 & 0 & 0 & 0 & 0 & 1 & a_6 \end{pmatrix}$$

$$B_5^\top = \begin{bmatrix}2\\5\\7\end{bmatrix} = \begin{pmatrix} 0 & 1 & a_1 & a_2 & 0 & a_3 & 0 \\ 0 & 0 & 0 & 0 & 1 & a_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$B_6^\top = \begin{bmatrix}3\\4\\7\end{bmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 & a_1 & a_2 & 0 \\ 0 & 0 & 0 & 1 & a_3 & a_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$B_7^\top = \begin{bmatrix}3\\5\\6\end{bmatrix} = \begin{pmatrix} 0 & 0 & 1 & a_1 & 0 & 0 & a_2 \\ 0 & 0 & 0 & 0 & 1 & 0 & a_3 \\ 0 & 0 & 0 & 0 & 0 & 1 & a_4 \end{pmatrix}.$$

Now we use disposition of free parameters to construct rank subcodes. Finally it will be multicomponent code with parameters $k = 3, n = 7, d_r = 2$, minimal subspace distance 4 of every component code and the same subspace distance between each pair of the components. The component code have the following number of code matrices: $256, 16, 1, 16, 2, 4, 2$. The total number is 297 code words, it is 16% more than the number of code words of the first component.

4 Code matrix of the first component

Let us construct code matrices of the first components with the parameters $q = 2$, $d_r = 2$, $k = n - d_r + 1 = 3 - 2 + 1 = 2$, a primitive polynomial $f(\lambda) = \lambda^4 + \lambda + 1$ and generator matrix

$$G = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{bmatrix}. \quad (2)$$

Information vectors have two components u_1, u_2, because $k = 2$. The code vector is

$$g = (u_1, u_2)G = (u_1 + u_2), (u_1\alpha + u_2\alpha^2), (u_1\alpha^2 + u_2\alpha^4) = (g_1, g_2, g_3).$$

The rank code matrix is

$$M_1 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}.$$

The code matrix of the first component is $X_1 = I_3 + M_1^T$, that is

$$X_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Binary vectors u_1 and u_2 have 2^4 values, so the first component has $2^8 = 256$ code matrices.

5 Code matrices of the second component

Let be the same parameters. Using identifier of the second component we have the following code matrix of the second component

$$X_2 = \begin{matrix} 1 & a_{11} & a_{12} & 0 & 0 & a_{13} & a_{14} \\ 0 & 0 & 0 & 1 & 0 & a_{23} & a_{24} \\ 0 & 0 & 0 & 0 & 1 & a_{33} & a_{34} \end{matrix}, \quad (3)$$

where $a_{11}, a_{12}, a_{13}, a_{14}, a_{23}, a_{24}, a_{33}, a_{34}$ – free parameters of the rank subcode. All other elements are zeros, that is $a_{21} = 0, a_{22} = 0, a_{31} = 0, a_{32} = 0$. The matrix of rank subcode is

$$M_1 = \begin{bmatrix} a_{11} & 0 & 0 \\ a_{12} & 0 & 0 \\ a_{13} & a_{23} & a_{33} \\ a_{14} & a_{24} & a_{34} \end{bmatrix}. \quad (4)$$

Giving basis $1, \alpha, \alpha^2, \alpha^3$ transform the second and the third columns of the matrix in vector form and equate them to g_2 and g_3 correspondingly. We will get equations for code vectors u_1, u_2

$0\times1+0\times\alpha+a_{23}\alpha^2+a_{24}\alpha^3 = u_1\alpha+u_2\alpha^2, 0\times1+0\times\alpha+a_{33}\alpha^2+a_{34}\alpha^3 = u_1\alpha^2+u_2\alpha^4$

and

$$u_1 = a_{33}\alpha^{11} + a_{34}\alpha^{12} + a_{23}\alpha^{13} + a_{24}\alpha^{14}, u_2 = a_{33}\alpha^{10} + a_{34}\alpha^{11} + a_{23}\alpha^{11} + a_{24}\alpha^{12}.$$

We have 4 elements of the code matrix, each element has two values 0 and 1. The total number of this rank subcode matrices is 16. For example let be $a_{23} = 1, a_{24} = 1, a_{33} = 1, a_{34} = 1$. Then $u_1 = \alpha^{13} + \alpha^{14} + \alpha^{11} + \alpha^{12} = \alpha^8$, $u_2 = \alpha^{11} + \alpha^{12} + \alpha^{10} + \alpha^{11} = \alpha^3$ and $g_1 = u_1 + u_2 = \alpha^{13}$, $g_2 = u_1\alpha + u_2\alpha^2 = \alpha^6$, $g_3 = u_1\alpha^2 + u_2\alpha^4 = \alpha^6$. The code vector is $g = \alpha^{13}\alpha^6\alpha^6$ The matrix of the subcode is

$$M_{16} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

6 Decoding

Insert the matrix M_{16}^T into the second component as it is shown by the identifier. We have

$$X_{16} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}. \tag{5}$$

The network channel (without adversaries) [2] is characterized by equation

$$Y = AX_{16}, \tag{6}$$

where for example

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}. \tag{7}$$

Let a received matrix be

$$Y = AX_{16} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{8}$$

Applying to Y Gauss elimination procedure we get

$$\widetilde{Y} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{9}$$

The positions of leading units in two first columns of the matrix $\widetilde{Y}$ indicate two column of the unit matrix. They are the first column and the fourth column. The position of the last column of the unit matrix we will determine using the identifier, it is the fifth. Present A as a sum of the unit matrix and a matrix L, where

$$L = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{10}$$

The last columns of the matrix $\widetilde{Y}$ is subcode matrix M_{16} multiplied by $A = I + L$:

$$M_{16} + LM_{16} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{11}$$

Use the transpose form of the matrices. Apply any of known fast rank decoding algorithms, for example [9]. Transform the matrix M_{16}^T in the $m_1m_2m_3$, multiply by L^T: $(m_1m_2m_3)L^T = (m_30m_3)$. Using m_3, write down the syndrome:

$$S_1 = m_3(101)\begin{pmatrix} 1 \\ \alpha^2 \\ \alpha^{12} \end{pmatrix} = m_3(1 + \alpha^{12}) = m_3\alpha^{11} \tag{12}$$

Transform the matrix $\widetilde{M}_{16}^T$ into the vector $y = (1\alpha^60)$ and calculate the syndrome:

$$S_1 = (1\alpha^60)\begin{pmatrix} 1 \\ \alpha^2 \\ \alpha^{12} \end{pmatrix} = 1 + \alpha^8 = \alpha^2 \tag{13}$$

Equate two expressions for S_1 and get $m_3\alpha^{11} = \alpha^2$, that is $m_3 = \alpha^6$. The mistake as vector is $e = (m_30m_3) = \alpha^60\alpha^6$. The real vector is $y + e = (1 + \alpha^6)\alpha^6\alpha^6 = \alpha^{13}\alpha^6\alpha^6$. The real subcode matrix is

$$M_{16} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \tag{14}$$

References

[1] E. M. Gabidulin, New Subcodes of Rank Codes, *This issue.*

[2] D. Silva, F. R. Kschischang, R. Koetter, A Rank-Metric Approach to Error Control in Random Network Coding, *IEEE Transactions on Information Theory,* **54** (9), (3951-3967), 2008.

[3] N. Etzion, N. Silberstein, Error-correcting Codes in Projective Space Via Rank-Metric Codes and Ferrers Diagrams, *IEEE Trans. Inform. Theory.* **55** (7), (2909-2919), 2009.

[4] E. M. Gabidulin, N, I. Pilipchuk, New Multicomponent Network Codes Based on Block Designs, *Proc. International Mathematical Conference "50 years of IPPI".* 2011. ISBN 978-5-901158-15-9.

[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, M. Bossert, Algebraic codes for network coding, *Problems of Information Transmission.* **45** (4), (343-356), 2009.

[7] E. M. Gabidulin, N, I. Pilipchuk, M. Bossert, Decoding of Random Network Codes, *Probl. Inform. Transm.* **46** (4), (273-295), 2010.

[8] M. Hall, *Combinatorial Theory.* Waitham (Massachusetts)- Toronto - London, 1967.

[9] A. 'Wachter, V. Afanasiev, V. R. Sidorenko, Fast decoding of Gabidulin codes. *Proc. of Seventh International Workshop on Coding and Cryptography*, (433-442). April 11-15, 2011, Paris, France.