Thirteenth International Workshop
on Algebraic and Combinatorial Coding Theory (ACCT)
June 15-21, 2012, Pomorie, Bulgaria

Decoding Multicomponent Codes Based on Rank Subcodes

N.I. Pilipchuk, E.M. Gabidulin, V.B. Afanassiev

Moscow Institute of Physics and Technology
(State University), Russia
Institute of Information Transmission Problems of the Russian
Academy of Sciences

Outline

1. **Our goal**
2. **Rank codes with restrictions**
3. **Reduced echelon form**
4. **Incomplete Balanced Block-Schemes**
5. **Multicomponent code with seven components**
6. **Encoding**
7. **Decoding**
8. **Conclusion**

Our goal

We construct multicomponent code based on subspace rank subcodes which is assigned to random network coding.

This code is a union of codes. Minimal code distance inside of every code component and minimum distance between any two components are the same.

We use reduced echelon form and combinatorial incomplete balanced block-scheme.

Cardinality of the multicomponent code is a sum of cardinalities of each code component.

We design encoding and decoding algorithms.

Rank codes with restrictions. Example

Let be $q = 2$, $n = 3$, $k = 2$, $d = 2$, $\alpha^3 + \alpha^2 + 1 = 0$. The generator matrix is

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

The code matrix is

$$M_{\text{restrict}}(\hat{\mathbf{u}}G) = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ 0 & a_{2,2} & a_{2,3} \\ 0 & a_{3,2} & a_{3,3} \end{bmatrix}.$$

Restrictions to $\hat{\mathbf{u}}$: $\hat{\mathbf{u}} = (u,\ u + \beta)$, $u \in GF(2^3)$, $\beta \in GF(2)$. $\hat{\mathbf{u}}G = (\beta\ u\alpha^6 + \beta\alpha^2\ u\alpha^5 + \beta\alpha^4)$. Cardinality is $|M| = 2^3 \cdot 2 = 2^4$.

Reduced echelon form

Silva–Kschischang–Koetter (SKK) codes have reduced echelon form of code matrices (lifting construction):

$$\mathcal{C} = \left\{ \left[I_k \quad M \right] \right\}, \tag{1}$$

where I_k – the unit matrix, $M \in \mathcal{M}$ – a rank code matrix.

The reduced echelon form satisfies to the conditions:

the leading element of the row is located on the right of the leading element of the preceding row;

all leading element are units;

all elements which located before the leading elements are zeros;

each leading element is the only nonzero element into its column.

Example

The reduced echelon form matrix contains "*leading units*" and "*zero*" elements. All other elements are "*free parameters*".

Let be i_j– a location of the leading units at the their columns, j - is a number of the unit matrix column. The vector $\mathbf{i} = [i_1\ i_2\ \ldots\ i_k]$ is identifier (ID) of this form.
Example 1. *Let be* $n = 6, k = 3$, $\mathbf{i} = [i_1 = 1;\ i_2 = 3;\ i_3 = 4]$, *then the matrix is*

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

There are 7 free parameters $a_{i,j}$ over $\mathbb{F}_q$. Thus, we have q^7 different 3-dimension subspaces with the same identifier.

Incomplete Balanced Block-Schemes

By definition, incomplete balanced block-scheme (called 2 B-) is a disposition where n different elements locate in b blocks and the each block contains exactly k different elements, each element appears in r different blocks and each pair of different elements a_i, a_j appears exactly in λ blocks.

n – number of all elements in the set ;

b – number of blocks;

r – number of blocks, which contain a given element;

k – number elements in each block;

λ – number of blocks, which contain a given pair of elements.

Multicomponent code with seven components

Let be $k = 3, n = 7, d_r = 2$. Construct code matrices using incomplete balanced block-scheme with parameters $n = v = b = 7$, $r = k = 3$, $\lambda = 1$.

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

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

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

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

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

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

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

where a - free parameters.

Now we will use disposition of free parameters to construct rank subcodes.

In the whole it will be seven component code with parameters $k = 3, n = 7, d_r = 2$.

Minimal subspace distance 4 for each component.

The same subspace distance between each pair of the components.

The code components have $256, 16, 1, 16, 2, 4, 2$ code matrices. The total number is 297 code words, it is 16% more than the first component has.

Encoding (Example)

The code matrix of the second component is

$$X_2 = \begin{matrix} 1 & a_{11} & a_{12} & 0 & 0 & a_{13} & a_{14} \\ 0 & 0 & 0 & 1 & 0 & a_{23} & a_{24} \\ 0 & 0 & 0 & 0 & 1 & a_{33} & a_{34} \end{matrix}, \tag{2}$$

where $a_{11}, a_{12}, a_{13}, a_{14}, a_{23}, a_{24}, a_{33}, a_{34}$ – free parameters of the rank subcode, $a_{21} = 0, a_{22} = 0, a_{31} = 0, a_{32} = 0.$

The matrix of the rank subcode is

$$M_1 = \begin{bmatrix} a_{11} & 0 & 0 \\ a_{12} & 0 & 0 \\ a_{13} & a_{23} & a_{33} \\ a_{14} & a_{24} & a_{34} \end{bmatrix}. \tag{3}$$

Let us use basis $1, \alpha, \alpha^2, \alpha^3$ and the primitive polynomial $f(\lambda) = \lambda^4 + \lambda + 1$.

The generator matrix is

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

The information vector has two components u_1, u_2 $(k = 2)$.

The code vector is

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

The code vector $g = (g_1, g_2, g_3)$ has three components.

Transform the second and the third column of the matrix in vectors and equate to g_2 and g_3 correspondingly.

We get equations for code vectors u_1, u_2.

$$0 \times 1 + 0 \times \alpha + a_{23}\alpha^2 + a_{24}\alpha^3 = u_1\alpha + u_2\alpha^2;$$
$$0 \times 1 + 0 \times \alpha + a_{33}\alpha^2 + a_{34}\alpha^3 = u_1\alpha^2 + u_2\alpha^4.$$

We obtained

$$\begin{aligned} u_1 &= a_{33}\alpha^{11} + a_{34}\alpha^{12} + a_{23}\alpha^{13} + a_{24}\alpha^{14}; \\ u_2 &= a_{33}\alpha^{10} + a_{34}\alpha^{11} + a_{23}\alpha^{11} + a_{24}\alpha^{12}. \end{aligned}$$

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 $2^4 = 16$.

Let be

$a_{23} = 1, a_{24} = 1, a_{33} = 1, a_{34} = 1$. Then

$$\begin{aligned} u_1 &= \alpha^{13} + \alpha^{14} + \alpha^{11} + \alpha^{12} = \alpha^8; \\ u_2 &= \alpha^{11} + \alpha^{12} + \alpha^{10} + \alpha^{11} = \alpha^3. \end{aligned}$$

$$
\begin{aligned}
g_1 &= u_1 + u_2 = \alpha^{13};\\
g_2 &= u_1\alpha + u_2\alpha^2 = \alpha^6;\\
g_3 &= u_1\alpha^2 + u_2\alpha^4 = \alpha^6.
\end{aligned}
$$

The code vector is

$g = \alpha^{13}\alpha^6\alpha^6.$

The matrix of the subcode is

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

Decoding

Now insert the matrix M^T into the second component using the identifier. We have the code matrix of the random network code

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

The network channel is characterized by the equation

$$Y = AX, \tag{6}$$

where A is a random matrix, for example,

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

The received matrix is

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

Begin decoding procedure.

1. Apply Gauss elimination procedure to Y . We get

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

2. Analyze positions of the leading units.

They are at the first column and the fourth column.

Using our identifier we find the fifth column as the third column of the unit matrix.

3. Now, we can obtain the matrix A by comparing the corrupted part of the 3×3 matrix with the unit matrix.

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 rest columns of the matrix $\widetilde{Y}$ is an corrupted rank code matrix, that is M multiplied by $A = I + L$:

$$\widetilde{M}^T = M + LM = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{11}$$

4. Using L we extract M.

Transform the matrix M^T in the vector $m_1 m_2 m_3$ and multiply by L^T: $(m_1 m_2 m_3) L^T = (m_3 0 m_3)$.

Using m_3, write down the syndrome :

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

Transform the matrix $\widetilde{M}^T$ into the vector $y = (1\alpha^6 0)$ and calculate the syndrome:

$$S_1 = (1\alpha^6 0) \begin{pmatrix} 1 \\ \alpha^2 \\ \alpha^{12} \end{pmatrix} = 1 + \alpha^8 = \alpha^2 \qquad (13)$$

Equate two expressions for S_1 and get $m_3\alpha^{11} = \alpha^2$, that is $m_3 = \alpha^6$.

The mistake as a vector is $e = (m_3 0 m_3) = \alpha^6 0 \alpha^6$.

The real vector is $y + e = (1 + \alpha^6)\alpha^6\alpha^6 = \alpha^{13}\alpha^6\alpha^6$.

The real rank subcode matrix is

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

Conclusion

- Multicomponent codes is an union of code component with equal minimal subspace code distance of each component. There is the same distance between each two components.

- Each component is based on rank subcode.

- These codes are assigned to random network coding.

- Coding algorithm uses incomplete balanced block-schemes.

- Cardinality of the multicomponent codes equals to a sum of cardinalities of all components.

- Decoding algorithm consists of two parts, the first part is Gauss elimination procedure and analysis, the second part is a standard decoding algorithm of rank codes.