New constructions of multicomponent codes

GABIDULIN E. ernst.gabidulin@gmail.com
Moscow Institute of Physics and Technology

PILIPCHUK N. pilipchuk.nina@gmail.com
Moscow Institute of Physics and Technology

Abstract. We have constructed a new class of multicomponent codes which have maximal cardinality at the following parameters:

- Code length: \( n = m + \delta \)
- Code distance: \( d = 2\delta \)
- Dimension: \( m = r\delta \)

where \( r \) is an integer. It was shown that these codes have maximal cardinality which coincides with Johnson upper bound I. Dual multicomponent codes were constructed correspondingly to these new codes. These dual codes are spreads.

1 Introduction

Let \( m \leq n \) be integers. Let \( \mathcal{M}_m^n \) be a set of matrices of size \( m \times n \) and of rank \( m \) over the field \( GF(q) \). Define \( \mathcal{R}(U) \) the row spanned subspace of the \( U \in \mathcal{M}_m^n \) matrix. The subspace distance between two subspaces \( \mathcal{R}(U) \) and \( \mathcal{R}(V) \) is defined as

\[
d(\mathcal{R}(U), \mathcal{R}(V)) = \dim(\mathcal{R}(U) \cup \mathcal{R}(V)) - \dim(\mathcal{R}(U) \cap \mathcal{R}(V)).
\]

The subspace distance between two subspaces of the same dimension is even. A network code of constant dimension \( m \) and cardinality \( A(n, d = 2\delta, m) \) with minimal subspace distance \( d = 2\delta \) is defined as a set of \( m \)-dimensional subspaces \( \mathcal{R}(U_1), \mathcal{R}(U_2), \ldots, \mathcal{R}(U_A) \), where \( d(\mathcal{R}(U_i), \mathcal{R}(U_j)) \geq 2\delta, i \neq j \) and the parameter \( \delta \leq m \). The main problem is the following: to construct a network code of maximal cardinality under given parameters \( \{n, d = 2\delta, m\} \).

2 Silva–Koetter–Kschischang (SKK) codes

Subspaces are often defined by means of their generator matrix. Rows of these matrices are a basis of the subspace. The generator matrices of SKK code [1] are presented as

\[
C_{skk} = \{U_i\} = \{ [I_m \ M_i] \},
\]

where \( I_m \) is the identity matrix of order \( m \), and \( M_i, i = 1, \ldots, A \), are matrices of \textbf{rank} code of size \( m \times (n - m) \) over the field \( GF(q) \) [5]. Subspace distance between \( \mathcal{R}(U_i) \) and \( \mathcal{R}(U_j) \) is equal to \( d(\mathcal{R}(U_i), \mathcal{R}(U_j)) = 2\text{Rk}(M_i - M_j) \).

\(^{1}\)The research is supported by RFBR (Project 15-07-08480)
Rank distance between two matrices $M_i, M_j$ is rank of their difference. There exists a linear rank code consisting of $m \times n$ matrices with minimal rank distance $\delta$ and cardinality $A = q^{a(b - \delta + 1)}$, where $a = \max\{m, (n - m)\}$ and $b = \min\{m, (n - m)\}$. Hence, the network SKK code has the following parameters: $n$ is length, $d = 2\delta$ is subspace distance, $m$ is dimension of code subspaces, $A = q^{a(b - \delta + 1)}$ is number of code subspaces.

3 Multicomponent code with zero prefix (MZP)

In 2008 year a class of multicomponent codes with maximal subspace distance $d = 2m$ was presented by Gabidulin and Bossert [2], [3]. The $s$-th component $C_{mzp}(s)$ ($s = 1, 2, \ldots, r$) consists of the following $m \times n$ matrices:

$$C_{mzp}(s) = \left\{ \begin{bmatrix} O_m \cdots O_m & I_m & M_s \end{bmatrix} \right\},$$

where $r \geq 2$. The first component ($s = 1$) has no zero prefix. It coincides with SKK code: $C_{mzp}(1) = C_{skk}$. The matrices $M_s$ are $m \times (n - m - (i - 1)m)$ matrices of a Gabidulin code with rank distance $\delta = m$. Consider a code with the following parameters: $n$ is code length, $m$ is dimension of the code subspace, $d = 2\delta$ is the subspace code distance. Denote $a_s = \max\{m, (n - m - (s - 1)\delta)\}$ and $b_s = \min\{m, (n - m - (s - 1)\delta)\}$. The cardinality of the $s$-th component of MZP code is equal to

$$A(s) = |C_{mzp}(s)| = q^{a_s(b_s - \delta + 1)}.\quad (1)$$

The total cardinality is equal to sum of cardinality of all components [4]:

$$C_{mzp} = \sum_{s=1}^{r} q^{a_s(b_s - \delta + 1)}.$$

**Example 1.** We construct MZP code at the following parameters: $n = 4\delta$, $d = 2\delta$, $m = 3\delta$. The first component is SKK code:

$$C(1) = \left\{ \begin{bmatrix} I_{3\delta} & M_{3\delta}^\delta \end{bmatrix} \right\} = \left\{ \begin{bmatrix} I_\delta & 0 & 0 & M_\delta^\delta(1) \\ 0 & I_\delta & 0 & M_\delta^\delta(2) \\ 0 & 0 & I_\delta & M_\delta^\delta(3) \end{bmatrix} \right\}. $$

The second component is

$$C(2) = \left\{ \begin{bmatrix} 0 & I_{3\delta} \end{bmatrix} \right\} = \left\{ \begin{bmatrix} 0 & I_\delta & 0 \\ 0 & 0 & I_\delta \\ 0 & 0 & 0 \end{bmatrix} \right\}. $$
The cardinality of this code is

\[ M_{\text{mzp}} = |C(1)| + |C(2)| = q^{3\delta} + 1. \]

The second component provides only one extra code matrix for these parameters.

4 Johnson upper bound I

4.1 Johnson theorem

Theorem 1. \([\text{Johnson I}]\) Let \( n, d = 2\delta, m \) be network code parameters. If

\[ (q^m - 1)^2 > (q^n - 1)(q^{m-\delta} - 1), \]

then

\[ A(n, d = 2\delta, m) \leq \left\lfloor \frac{(q^m - q^{m-\delta})(q^n - 1)}{(q^m - 1)^2 - (q^n - 1)(q^{m-\delta} - 1)} \right\rfloor. \]

The condition (2) is satisfied, if \( \delta = m \). In this case Johnson upper bound I \([11]\) coincides with Wang upper bound \([6]\):

\[ A(n, d = 2m, m) \leq \left\lfloor \frac{q^n - 1}{q^m - 1} \right\rfloor. \]

4.2 Corollaries

Corollary 1. For \( \delta \leq m \), the condition (2) is satisfied if and only if

\[ n \leq m + \delta. \]

Corollary 2. If \( n < m + \delta \), then the cardinality of a MZP code is

\[ A(n, d = 2\delta, m) = 1. \]

Corollary 3. If \( n = m + \delta \), then

\[ A(n, d = 2\delta, m) \leq \left\lfloor \frac{q^n - 1}{q^\delta - 1} \right\rfloor. \]

It is Johnson upper bound I. Wang upper bound for these parameters is much greater.

Corollary 4. If \( n = m + \delta \), then the dimension of a dual code is \( m' = n - m = \delta \). The cardinality is

\[ A(n, d = 2\delta, m') = A(n, d = 2\delta, \delta). \]

This estimation coincides with Wang upper bound for spreads. Their code distance is equal to double code dimension (maximal).
5 A new construction

We modify MZP code. We describe a new construction by means of an example.

Example 2. Let parameters be \( n = 4 \delta, d = 2 \delta, m = 3 \delta \). A new algorithm is used for the reconstruction of a MZP code. The first component of the new construction is SKK code as usually:

\[
\tilde{C}(1) = \{ [I_{3\delta} \hspace{1cm} M_{3\delta}^{\delta}] \} = \begin{bmatrix}
I_{\delta} & 0 & 0 & M_{\delta}^{\delta}(1) \\
0 & I_{\delta} & 0 & M_{\delta}^{\delta}(2) \\
0 & 0 & I_{\delta} & M_{\delta}^{\delta}(3)
\end{bmatrix}
\]

The second component is constructed by another way in comparison with the second component of the previous construction:

\[
\tilde{C}(2) = \begin{bmatrix}
I_{\delta} & 0 & A_{\delta}^{\delta}(1) & 0 \\
0 & I_{\delta} & A_{\delta}^{\delta}(2) & 0 \\
0 & 0 & 0 & I_{\delta}
\end{bmatrix}
\]

where \( A_{\delta}^{\delta}(1) \) and \( A_{\delta}^{\delta}(2) \) are \( \delta \times \delta \) matrices of rank codes with rank distance \( \delta \). The third component is the following:

\[
\tilde{C}(3) = \begin{bmatrix}
I_{\delta} & B_{\delta}^{\delta} & 0 & 0 \\
0 & 0 & I_{\delta} & 0 \\
0 & 0 & 0 & I_{\delta}
\end{bmatrix}
\]

where \( B_{\delta}^{\delta} \) is a \( \delta \times \delta \) matrix of a rank code with rank distance \( \delta \). The fourth component coincides with the second component of the previous construction:

\[
\tilde{C}(4) = C(2) = \begin{bmatrix}
0 & I_{\delta} & 0 & 0 \\
0 & 0 & I_{\delta} & 0 \\
0 & 0 & 0 & I_{\delta}
\end{bmatrix}
\]

The cardinality of the new modified code is greater then the cardinality in the former construction:

\[
M_{\text{mod}} = |\tilde{C}(1)| + |\tilde{C}(2)| + |\tilde{C}(3)| + |\tilde{C}(4)| = (q^{3\delta} + 1) + (q^{2\delta} + q^{\delta})
= \frac{q^{4\delta} - 1}{q^{\delta} - 1}.
\]
6 General case: \( m = r\delta \)

Let us use Johnson theorem restriction on code lengths and put \( n = m + \delta \), where \( m = r\delta \), \( r \) is an integer. We will construct new multicomponent codes which have maximal cardinality. Present components of the new multicomponent code. As usually the first component is SKK code. The \( s \)-th component \((s < r)\) is

\[
\widetilde{C}(s) = \begin{bmatrix}
I_{(r-s)\delta} & U_{(r-s)\delta} & 0_{(r-s)\delta} \\
0_{(r-s)\delta} & 0_{\delta} & I_{s\delta}
\end{bmatrix}
\]

The last \( r \)-th component is

\[
\widetilde{C}(r) = \begin{bmatrix} 0_{r\delta} & I_{r\delta} \end{bmatrix}.
\]

The cardinality of this code is equal to

\[
M_{\text{mod}} = |\tilde{C}(1)| + \cdots + |\tilde{C}(r-1)| + |\tilde{C}(r)| = \frac{q^{(r+1)\delta-1}}{q^{\delta-1}}.
\]

7 Dual codes – spreads

Consider codes which are dual to components of the new multicomponent code. We have the first component of the new code as

\[
\tilde{C}(1) = \begin{bmatrix} I_{r\delta} & M_{r\delta}^{\delta} \end{bmatrix}.
\]

The corresponding dual component is

\[
\tilde{C}^\perp(1) = \begin{bmatrix} -M_{r\delta}^{\perp} & I_{\delta} \end{bmatrix}.
\]

We have the \( s \)-th component \((s < r)\) of the new code

\[
\tilde{C}(s) = \begin{bmatrix}
I_{(r-s)\delta} & U_{(r-s)\delta} & 0 \\
0_{(r-s)\delta} & 0_{\delta} & I_{s\delta}
\end{bmatrix}.
\]

The corresponding dual component is as follows:

\[
\tilde{C}^\perp(s) = \begin{bmatrix} -(U^{\perp})_{\delta}^{(r-s)\delta} & I_{\delta} & 0_{\delta} \end{bmatrix}.
\]

We have the last \( r \)-th component as

\[
\tilde{C}(r) = \begin{bmatrix} 0_{r\delta} & I_{r\delta} \end{bmatrix}.
\]

The corresponding dual component is

\[
\tilde{C}^\perp(r) = \begin{bmatrix} I_{\delta} & 0_{\delta} \end{bmatrix}.
\]

The dual codes at the dimension \( \tilde{m} = \delta \) and the subspace distance \( d = 2\tilde{m} = 2\delta \) present spreads which have maximal cardinality [7] – [10].
8 Conclusion

We have constructed a new class of multicomponent codes which have maximal cardinality. It allows to extend the class of optimal codes which achieve Johnson upper bound \( I \) at the following parameters: \( n = m + \delta \). Johnson upper bound is more exact than Wang upper bound for these parameters. Correspondingly to the new class of codes we have constructed dual multicomponent codes which are spreads.

References


