Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 18-24, 2016, Albena, Bulgaria *pp. 162–167*

New constructions of multicomponent codes [1]

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: $n = m + \delta$ is code length, $d = 2\delta$ is code distance, $m = r\delta$ is dimension, 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 $\mathcal{R}(\mathbf{U})$ the row spanned subspace of the $\mathbf{U} \in \mathcal{M}_m^n$ matrix. The subspace distance between two subspaces $\mathcal{R}(\mathbf{U})$ and $\mathcal{R}(\mathbf{V})$ is defined as

$$d(\mathcal{R}(\mathbf{U}), \mathcal{R}(\mathbf{V})) = \dim\left(\mathcal{R}(\mathbf{U}) \uplus \mathcal{R}(\mathbf{V})\right) - \dim\left(\mathcal{R}(\mathbf{U}) \cap \mathcal{R}(\mathbf{V})\right).$$

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 $\mathcal{R}(\mathbf{U}_1), \mathcal{R}(\mathbf{U}_2), \ldots, \mathcal{R}(\mathbf{U}_A)$, where $d(\mathcal{R}(\mathbf{U}_i), \mathcal{R}(\mathbf{U}_j)) \geq 2\delta$, $i \neq j$ 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

$$\mathcal{C}_{\text{skk}} = \{\mathbf{U}_i\} = \left\{\begin{bmatrix}\mathbf{I}_m & \mathbf{M}_i\end{bmatrix}\right\},$$

where $\mathbf{I}_m$ is the identity matrix of order m, and $\mathbf{M}_i$, $i = 1, \ldots, A$, are matrices of ***rank*** code of size $m \times (n - m)$ over the field $GF(q)$ [5]. Subspace distance between $\mathcal{R}(\mathbf{U}_i)$ and $\mathcal{R}(\mathbf{U}_j)$ is equal to $d(\mathcal{R}(\mathbf{U}_i), \mathcal{R}(\mathbf{U}_j)) = 2\text{Rk}(\mathbf{M}_i - \mathbf{M}_j)$.

[1]The research is supported by RFBR (Project 15-07-08480)

Rank distance between two matrices $\mathbf{M}_i$, $\mathbf{M}_j$ is *rank* of their difference. There exists a linear rank code consisting of $m\times n$ matrices with minimal rank distance δ and cardinality $A = q^{a(b-\delta+1)}$, where $a = \max\{m, (n-m)\}$ $b = \min\{m, (n-m)\}$. 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 $C_{\mathrm{mzp}}(s)$ $(s = 1, 2, \ldots, r)$ consists of the following $m \times n$ matrices:

$$\mathcal{C}_{\mathrm{mzp}}(s) = \left\{ \left[\begin{array}{ccc} \underbrace{\mathbf{O}_m \ldots \mathbf{O}_m}_{s-1} & \mathbf{I}_m & \mathbf{M}_s \end{array} \right] \right\},$$

where $r \geq 2$. The first component $(s = 1)$ has no zero prefix. It coincides with SKK code: $\mathcal{C}_{\mathrm{mzp}}(1) = \mathcal{C}_{\mathrm{skk}}$. The matrices $\mathbf{M}_s$ 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

$$A(s) = |\mathcal{C}_{mzp}(s)| = q^{a_s(b_s-\delta+1)}. \tag{1}$$

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

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

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:*

$$\mathcal{C}(1) = \left\{ \left[\mathbf{I}_{3\delta} \quad \mathbf{M}_{3\delta}^{\delta} \right] \right\} = \left\{ \begin{bmatrix} \mathbf{I}_\delta & \mathbf{0} & \mathbf{0} & \mathbf{M}_\delta^\delta(1) \\ \mathbf{0} & \mathbf{I}_\delta & \mathbf{0} & \mathbf{M}_\delta^\delta(2) \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_\delta & \mathbf{M}_\delta^\delta(3) \end{bmatrix} \right\}.$$

The second component is

$$\mathcal{C}(2) = \left\{ \left[\mathbf{0}_{3\delta}^{\delta} \quad \mathbf{I}_{3\delta} \right] \right\} = \left\{ \begin{bmatrix} \mathbf{0} & \mathbf{I}_\delta & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_\delta & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_\delta \end{bmatrix} \right\}.$$

The cardinality of this code is

$$M_{mzp} = |\mathcal{C}(1)| + |\mathcal{C}(2)| = q^{3\delta} + 1.$$

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

4 Johnson upper bound I

4.1 Johnson theorem

Theorem 1. *[**Johnson I**] Let n, $d = 2\delta$, m be network code parameters. If*

$$(q^m - 1)^2 > (q^n - 1)(q^{m-\delta} - 1), \tag{2}$$

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:*

$$\widetilde{\mathcal{C}}(1) = \left\{ \begin{bmatrix} \mathbf{I}_{3\delta} & \mathbf{M}_{3\delta}^{\delta} \end{bmatrix} \right\} = \left\{ \begin{bmatrix} \mathbf{I}_\delta & \mathbf{0} & \mathbf{0} & \mathbf{M}_\delta^\delta(1) \\ \mathbf{0} & \mathbf{I}_\delta & \mathbf{0} & \mathbf{M}_\delta^\delta(2) \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_\delta & \mathbf{M}_\delta^\delta(3) \end{bmatrix} \right\}$$

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

$$\widetilde{\mathcal{C}}(2) = \left\{ \begin{bmatrix} \mathbf{I}_\delta & \mathbf{0} & \mathbf{A}_\delta^\delta(1) & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_\delta & \mathbf{A}_\delta^\delta(2) & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_\delta \end{bmatrix} \right\},$$

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

$$\widetilde{\mathcal{C}}(3) = \left\{ \begin{bmatrix} \mathbf{I}_\delta & \mathbf{B}_\delta^\delta & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_\delta & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_\delta \end{bmatrix} \right\},$$

where $\mathbf{B}_\delta^\delta$ is a $\delta \times \delta$ matrix of a rank code with rank distance δ. The fourth component coincides with the second component of the previous construction:

$$\widetilde{\mathcal{C}}(4) = \mathcal{C}(2) = \begin{bmatrix} \mathbf{0} & \mathbf{I}_\delta & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_\delta & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_\delta \end{bmatrix}.$$

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

$$M_{\text{mod}} = |\widetilde{\mathcal{C}}(1)| + |\widetilde{\mathcal{C}}(2)| + |\widetilde{\mathcal{C}}(3)| + |\widetilde{\mathcal{C}}(4)| = (q^{3\delta} + 1) + (q^{2\delta} + q^{\delta})$$

$$= \tfrac{q^{4\delta}-1}{q^{\delta}-1}.$$

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

$$\widetilde{\mathcal{C}}(s) = \left\{ \begin{bmatrix} \mathbf{I}_{(r-s)\delta} & \mathbf{U}^{\delta}_{(r-s)\delta} & \mathbf{0}^{s\delta}_{(r-s)\delta} \\ \mathbf{0}^{(r-s)\delta}_{\delta} & \mathbf{0}^{\delta}_{\delta} & \mathbf{I}_{s\delta} \end{bmatrix} \right\}$$

The last r-th component is

$$\widetilde{\mathcal{C}}(r) = \begin{bmatrix} \mathbf{0}^{\delta}_{r\delta} & \mathbf{I}_{r\delta} \end{bmatrix}.$$

The cardinality of this code is equal to

$$M_{\text{mod}} = |\widetilde{\mathcal{C}}(1)| + \cdots + |\widetilde{\mathcal{C}}(r-1)| + |\widetilde{\mathcal{C}}(r)| = \tfrac{q^{(r+1)\delta}-1}{q^{\delta}-1}.$$

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

$$\widetilde{\mathcal{C}}(1) = \left\{ \begin{bmatrix} \mathbf{I}_{r\delta} & \mathbf{M}^{\delta}_{r\delta} \end{bmatrix} \right\}.$$

The corresponding dual component is

$$\widetilde{\mathcal{C}}^{\perp}(1) = \left\{ \begin{bmatrix} -(\mathbf{M}^{\top})^{r\delta}_{\delta} & \mathbf{I}_{\delta} \end{bmatrix} \right\}.$$

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

$$\widetilde{\mathcal{C}}(s) = \left\{ \begin{bmatrix} \mathbf{I}_{(r-s)\delta} & \mathbf{U}^{\delta}_{(r-s)\delta} & \mathbf{0} \\ \mathbf{0}^{(r-1)\delta}_{\delta} & \mathbf{0}^{\delta}_{\delta} & \mathbf{I}_{s\delta} \end{bmatrix} \right\}.$$

The corresponding dual component is as follows:

$$\widetilde{\mathcal{C}}^{\perp}(s) = \left\{ \begin{bmatrix} -(\mathbf{U}^{\top})^{(r-s)\delta}_{\delta} & \mathbf{I}_{\delta} & \mathbf{0}^{s\delta}_{\delta} \end{bmatrix} \right\}.$$

We have the last r-th component as

$$\widetilde{\mathcal{C}}(r) = \begin{bmatrix} \mathbf{0}^{\delta}_{r\delta} & \mathbf{I}_{r\delta} \end{bmatrix}.$$

The corresponding dual component is

$$\widetilde{\mathcal{C}}^{\perp}(r) = \left\{ \begin{bmatrix} \mathbf{I}_{\delta} & \mathbf{0}^{r\delta}_{\delta} \end{bmatrix} \right\}.$$

The dual codes at the dimension $\widetilde{m} = \delta$ and the subspace distance $d = 2\widetilde{m} = 2\delta$ 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

[1] *Silva D., Koetter R., Kschischang F.R.* A Rank-Metric Approach to Error Control in Random Network Coding // IEEE Trans. Inform. Theory. 2008. V. 54. No. 9. P. 3951-3967.

[2] *Gabidulin E., Bossert M.* Codes for Network Coding // Proc.2008 IEEE Int. Sympos. on Information Theory (ISIT2008). Toronto, Canada. July 6-11, 2008. P.867-870.

[3] *Gabidulin E., Bossert M.* Algebraic codes for network coding// Probl. Inform. Transm. 2009. V. 45. No. 4. P. 54-68.

[4] *Gabidulin E., Pilipchuk N.* Efficiency of subspace network codes //Proceeding of MIPT. 2015.-V.7. No. 1. P.104-111.

[5] *Gabidulin E.* Theory of codes with maximal rank distance. Probl. Inform. Transm. 1985. V. 21. No. 1. P. 3-16.

[6] *Wang H., Xing C., Safavi-Naini R.* Linear Autentication Codes: Bounds and Constructions//IEEE Trans. Inform. Theory. 2003. V. 49.4. P.866-873.

[7] *Dembowski P.*. Finite geometries// Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44. Springer-Verlag, Berlin, 1968.

[8] *Beutelspacher A.* Partial spreads in finite projective spaces and partial designs// Math. Z. 1975. 145(3)P. 211229.

[9] *Drake D.A. , Freeman J.W.* Partial t-spreads and group constructible s, r, μ-nets //J. Geom. 1979. 13(2) P. 210-216.

[10] *Beutelspacher A.* Blocking sets and partial spreads in finite projective spaces// Geom. Dedicata. 1980. 9(4)P. 425449.

[11] *Xia T., Fu F.W.* Jonson type bounds on constant dimension codes //Designs, Codes and Cryptography 2009. V.50. 2. P.163-172.