International conference ACCT-2016

New constructions of multicomponent codes

Gabidulin E.M., Pilipchuk N.I.

Content

- Subspace codes
- Silva–Koetter–Kschischang (SKK) codes
- Multicomponent with zero prefix (MZP) codes
- Johnson bound I
- Corollaries
- Modified multicomponent codes
- Dual multicomponent codes
- Conclusion

Subspace codes

Let $m \leq n$ be integers. Let $\mathcal{M}_m^n$ be a set of matrices of size $m \times n$ 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

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

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 $\{n, d = 2\delta, m\}$.

Silva–Koetter–Kschischang (SKK) codes

A subspace is often defined by means of the generator matrix. Rows of this matrix is a basis of this subspace. The generator matrix of SKK code is presented as

$$\mathbf{U}_i = \begin{bmatrix} \mathbf{I}_m & \mathbf{M}_i \end{bmatrix},$$

where $\mathbf{I}_m$ is the identity matrix of order m, and $\mathbf{M}_i$ is a matrix of **rank** code of size $m \times (n-m)$ over the field $GF(q)$. This code consists of matrices of size $m \times (n-m)$ over the field $GF(q)$.

Subspace distance between $\mathcal{R}(\mathbf{U}_i)$ and $\mathcal{R}(\mathbf{U}_j)$ is equal to

$$d(\mathcal{R}(\mathbf{U}_i), \mathcal{R}(\mathbf{U}_j)) = 2\mathrm{Rk}(\mathbf{U}_i - \mathbf{U}_j).$$

Rank distance between two matrices is *rank* of their difference.

There exists a linear rank code consisting of $m \times n$ matrices with minimal rank distance δ and cardinality

$$M = q^{a(b-\delta+1)},$$

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,

$M = q^{a(b-\delta+1)}$ is number of code subspaces.

Multicomponent with zero prefix (MZP) codes

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

$$\mathcal{C}_{mzp,i} = \left\{ \left[\ \underbrace{\mathbf{O}_m \ldots \mathbf{O}_m}_{i-1} \ \ \mathbf{I}_m \ \ \mathbf{M}_i \ \right] \right\},$$

where $i = 1, \ldots, r$, and $r \geq 2$. The first component $\mathcal{C}_{mzp,1} = \mathcal{C}_{\mathsf{SKK}}$ coincides with SKK code, it has no a zero prefix.
The matrix $\mathbf{M}_i$ is a $m \times (n - m - (i-1)m)$ matrix of Gabidulin code with rank distance $\delta = m$.

Cardinality of MZP code at given parameters $\delta = m$ and $n = (r+1)m$ is equal to

$$M_{mzp} = |\mathcal{C}_{mzp}| = \frac{q^n - 1}{q^m - 1}.$$

This value coincides with Wang *upper* bound of cardinality (2003).

MZP codes. General case.

If $\delta < m$, then (i)-th component $\mathcal{C}_{mzp,i}$ is $m \times (n - m - (i-1)\delta)$ matrix:

$$\mathcal{C}_{mzp,i} = \left\{ \left[\begin{array}{ccccc} \mathbf{O}_\delta & \ldots & \mathbf{O}_\delta & \mathbf{I}_m & \mathbf{M}_i \end{array} \right] \right\},$$

where $i = 1, \ldots, r$, and $r \geq 2$. As usually, the first component coincides with SKK code.

Cardinality of MZP codes

Consider a code with the following parameters: n is code length, m is dimension of code subspace, $d_{\text{sub}} = 2\delta$ is code distance. Denote $a_i = \max\{m, (n-m-(i-1)\delta)\}$ and $b_i = \min\{m, (n-m-(i-1)\delta)\}$. The cardinality of the i-th component is equal to

$$|\mathcal{C}_{mzp,\,i}| = q^{a_i(b_i-\delta+1)}. \tag{1}$$

The total cardinality is equal to sum of cardinality of all components:

$$\mathcal{C}_{mzp} = \sum_{i=1}^{r} q^{a_i(b_i-\delta+1)}.$$

Johnson upper bound I

Let n, $d = 2\delta$, m be network code parameters.

If

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

then

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

Corollary 1

The condition is satisfied, if $\delta = m$. In this case Johnson upper bound coincides with Wang upper bound (2003):

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

Corollary 2

For $\delta < m$, the condition is satisfied **iff**

$$n \leq m + \delta.$$

If $n < m + \delta$, then the cardinality of a MZP code is

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

If $n = m + \delta$, then

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

Corollary 3

If $n = m+\delta$, then for a dual code the dimension 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 maximal that is twice more than code dimension.

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:

$$\mathcal{C}_1 = \left\{ \begin{bmatrix} \mathbf{I}_{3\delta} & \mathbf{M}_{3\delta}^{\delta} \end{bmatrix} \right\} = \left\{ \begin{bmatrix} \mathbf{I}_\delta & \mathbf{0} & \mathbf{0} & \mathbf{M}_{1,\delta}^{\delta} \\ \mathbf{0} & \mathbf{I}_\delta & \mathbf{0} & \mathbf{M}_{2,\delta}^{\delta} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_\delta & \mathbf{M}_{3,\delta}^{\delta} \end{bmatrix} \right\}.$$

The second component is

$$\mathcal{C}_2 = \left\{ \begin{bmatrix} \mathbf{0}_{3\delta}^{\delta} & \mathbf{I}_{3\delta} \end{bmatrix} \right\} = \left\{ \begin{bmatrix} \mathbf{0} & \mathbf{I}_\delta & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_\delta & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_\delta \end{bmatrix} \right\}.$$

The cardinality of this code is

$$M = |\mathcal{C}_1| + |\mathcal{C}_2| = q^{3\delta} + 1.$$

This estimation is only one code matrix more than the cardinality SKK code for these parameters.

Example 2. A new construction

Now, we use modified algorithm for a new construction. The first component is the same as before (SKK code):

$$\widetilde{\mathcal{C}}_1 = \left\{ \begin{bmatrix} \mathbf{I}_{3\delta} & \mathbf{M}^{\delta}_{3\delta} \end{bmatrix} \right\} = \left\{ \begin{bmatrix} \mathbf{I}_{\delta} & \mathbf{0} & \mathbf{0} & \mathbf{M}^{\delta}_{1,\delta} \\ \mathbf{0} & \mathbf{I}_{\delta} & \mathbf{0} & \mathbf{M}^{\delta}_{2,\delta} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_{\delta} & \mathbf{M}^{\delta}_{3,\delta} \end{bmatrix} \right\}.$$

The second component is

$$\widetilde{\mathcal{C}}_2 = \left\{ \begin{bmatrix} \mathbf{I}_{\delta} & \mathbf{0} & \mathbf{A}^{\delta}_{1,\delta} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{\delta} & \mathbf{A}^{\delta}_{2,\delta} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_{\delta} & \mathbf{I}_{\delta} \end{bmatrix} \right\}.$$

The third component is

$$\widetilde{\mathcal{C}}_3 = \left\{ \begin{bmatrix} \mathbf{I}_\delta & \mathbf{B}_\delta^\delta & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_\delta & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_\delta \end{bmatrix} \right\}.$$

The fourth component coincides with the second component of the former algorithm:

$$\widetilde{\mathcal{C}}_4 = \mathcal{C}_2 = \left\{ \begin{bmatrix} \mathbf{0}_{3\delta}^\delta & \mathbf{I}_{3\delta} \end{bmatrix} \right\}.$$

The cardinality of the new construction code is equal to

$$M_{\mathsf{mod}} = |\widetilde{\mathcal{C}}_1| + |\widetilde{\mathcal{C}}_2| + |\widetilde{\mathcal{C}}_3 + |\widetilde{\mathcal{C}}_4| = q^{3\delta} + q^{2\delta} + q^\delta + 1 = \frac{q^{4\delta} - 1}{q^\delta - 1}.$$

We have four components instead two. The cardinality is grater than it was before. It value coincides with Johnson upper bound for given parameters.

General case: $m = r\delta$

Let us consider a general case: $n = m + \delta$, $m = r\delta$, where r is an integer. Present new constructions of the multicomponent code.

The first component is SKK code (as usually):

$$\begin{aligned}\widetilde{\mathcal{C}}_1 &= \left\{\left[\mathbf{I}_{r\delta} \quad \mathbf{M}^{\delta}_{r\delta}\right]\right\} = \\ &= \left\{\begin{bmatrix} \mathbf{I}_\delta & \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & \mathbf{M}^{\delta}_{\delta}(1) \\ \mathbf{0} & \mathbf{I}_\delta & \mathbf{0} & \dots & \mathbf{0} & \mathbf{M}^{\delta}_{\delta}(2) \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{I}_\delta & \mathbf{0} & \mathbf{M}^{\delta}_{\delta}(r-1) \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \dots & \mathbf{I}_\delta & \mathbf{M}^{\delta}_{\delta}(r) \end{bmatrix}\right\}.\end{aligned}$$

The second component is

$$
\begin{aligned}
\widetilde{\mathcal{C}}_2 &= \left\{ \begin{bmatrix} \mathbf{I}_{(r-1)\delta} & \mathbf{A}^{\delta}_{(r-1)\delta} & \mathbf{0} \\ \mathbf{0}^{(r-1)\delta}_{\delta} & \mathbf{0}^{\delta}_{\delta} & \mathbf{I}_{\delta} \end{bmatrix} \right\} = \\
&= \left\{ \begin{bmatrix} \mathbf{I}_{\delta} & \mathbf{0} & \mathbf{0} & \dots & \mathbf{A}^{\delta}_{\delta}(1) & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{\delta} & \mathbf{0} & \dots & \mathbf{A}^{\delta}_{\delta}(2) & \mathbf{0} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_{\delta} & \mathbf{A}^{\delta}_{\delta}(r-1) & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{\delta} \end{bmatrix} \right\}.
\end{aligned}
$$

The s-th component ($s < r$) is

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

$$\cdots \;\; \cdots \;\; \cdots \;\; \cdots \;\; \cdots \;\; \cdots$$

The (r-1)-th component is

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

The r-th component is

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

The cardinality of this code is equal to $M_{\text{mod}} = \frac{q^n-1}{q^\delta-1}$.

Dual codes – spreads

Consider codes which are dual to components of the new multi-component code.

We have the first component of the new code as

$$\widetilde{\mathcal{C}}_1 \;=\; \left\{ \left[\mathbf{I}_{r\delta} \;\; \mathbf{M}^{\delta}_{r\delta} \right] \right\}$$

corresponding dual component is

$$\widetilde{\mathcal{C}}_1^{\perp} \;=\; \left\{ \left[-(\mathbf{M}^{\top})^{r\delta}_{\delta} \;\; \mathbf{I}_{\delta} \right] \right\}.$$

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

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

corresponding dual component is as follows

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

We have the last r-th component as

$$\widetilde{\mathcal{C}}_r = \left\{ \begin{bmatrix} \mathbf{0} & \mathbf{I}_\delta & \mathbf{0} & \dots & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_\delta & \dots & \mathbf{0} & \mathbf{0} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_\delta & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_\delta \end{bmatrix} \right\}$$

corresponding dual component is

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

The dual codes at the dimension $\widetilde{m} = \delta$ and the subspace distance $d = 2\widetilde{m} = 2\delta$ present spreads with maximal cardinality.

Conclusion

- There were 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 allows to extend the class of optimal codes which achieve Johnson upper bound I.

- Correspondingly to the new class we have constructed dual multicomponent codes, which have the following parameters: $\widetilde{m} = \delta$ is dimension, $d = 2\widetilde{m} = 2\delta$ is code distance. Such codes are called spreads.