Thirteenth International Workshop

on Algebraic and Combinatorial Coding Theory

(ACCT)

June 15-21, 2012, Pomorie, Bulgaria

New Subcodes of Rank Codes

Ernst M. Gabidulin

Moscow Institute of Physics and Technology

(State University), Russia

Outline

1. **Motivation**
2. **Rank codes: background**
3. **Subspaces of extension fields**
4. **Subcodes over general subspaces**
5. **Uniformly restricted rank codes**
6. **Irregularly restricted rank codes**
7. **Conclusion**

Motivation

Let

$$\mathbf{YX} + \mathbf{E},$$

$$\mathbf{X} = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1\ n-1} & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2\ n-1} & x_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ x_{N-1\ 1} & x_{N-1\ 2} & \cdots & x_{N-1\ n-1} & x_{N-1\ n} \\ x_{N1} & x_{N2} & \cdots & x_{N\ n-1} & x_{Nn} \end{pmatrix}$$

– a code matrix of a $(N \times n, k, d)$ rank code,

$$\mathbf{E} = \begin{pmatrix} e_{11} & e_{12} & \cdots & e_{1\ n-1} & e_{1n} \\ e_{21} & e_{22} & \cdots & e_{2\ n-1} & e_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ e_{N-1\ 1} & e_{N-1\ 2} & \cdots & e_{N-1\ n-1} & e_{N-1\ n} \\ e_{N1} & e_{N2} & \cdots & e_{N\ n-1} & e_{Nn} \end{pmatrix}$$

A code can correct all error matrices $\mathbf{E}$ up to rank $(d-1)/2$.

But sometimes we would like to do more.

1. In multichannel communications or in space time coding, each column can be treated as a channel.

It would be desirable first to correct Hamming errors in channels, then to correct rank errors in the whole matrix.

2. In network coding, several selected entries of $\mathbf{X}$ must have prescribed values (mostly, zeroes).

3. In cryptography, code matrices should look as random matrices.

4. ……

Problems: to construct matrices $\mathbf{X}$ with properties needed.

Solution (partial): subcodes of rank codes. Each column of $\mathbf{X}$ is treated as a member of some subspace.

Rank codes: matrix representation

$\mathbb{K}_q = \mathbb{K}$ – a ground field of q elements

$\mathbb{K}_{q^N}$ – an extension field of degree N.

$\mathbb{K}^{N\times n}$ – the space of matrices of size $N \times n$ over the ground field $\mathbb{K}$.

The norm of a matrix $G \in \mathbb{K}^{N\times n}$ is its rank $\mathsf{Rk}(G)$.

The rank distance $d(G_1, G_2)$ between matrices G_1, G_2 is defined as the rank of its difference: $d(G_1, G_2) = \mathsf{Rk}(G_1 - G_2)$.

A rank code $\mathcal{M}$ in matrix representation of rank distance d and size M denoted as $(N \times n, M, d)$ is any subset $\mathcal{M} \subseteq \mathbb{K}^{N\times n}$, where

$$M = |\mathcal{M}|; \quad d = \min(\mathsf{Rk}(G_i - G_j)), \quad G_i, G_j \in \mathcal{M}.$$

For $(N \times n, M, d)$-code, the Singleton-type bound is valid:

$$M \leq q^{N(n-d+1)}.$$

If the equality holds, then a code is known as *a maximal rank distance* code (MRD code).

Rank codes: vector representation

The space $\mathbb{K}_{q^N}^n$ of vectors of length n over *the extension* field $\mathbb{K}_{q^N}$ is considered. It is assumed that $n \leq N$.

The rank of a vector $\mathbf{g} \in \mathbb{K}_{q^N}^n$ is defined as the maximal number $r(\mathbf{g})$ of its coordinates which are linearly independent over the *ground* field $\mathbb{K}$.

The rank distance between vectors $\mathbf{g}_1, \mathbf{g}_2$ is the rank of its difference: $d(\mathbf{g}_1, \mathbf{g}_2) = r(\mathbf{g}_1 - \mathbf{g}_2)$.

A code $\mathcal{V} \subseteq \mathbb{K}_{q^N}^n$ is any subset.

The code distance $d(\mathcal{V}) = d$ is the minimum of pairwise distances.

A k-dimensional subspace of the whole space $\mathbb{K}_{q^N}^n$ with distance d is known as a linear (n, k, d)-code $\mathcal{V}$.

The Singleton-type bound is as follows:

$$k \leq n - d + 1.$$

Connections between matrix and vector representations

$\Omega = \{\omega_1, \omega_2, \ldots, \omega_N\}$ – any basis of the extension field $\mathbb{K}_{q^N}$ over the ground field $\mathbb{K}$.

A vector $\mathbf{x} = \begin{bmatrix} x_1 & \ldots & x_n \end{bmatrix} \in \mathbb{K}_{q^N}^n$ over the extension field $\mathbb{K}_{q^N}$ can be mapped into a $N \times n$ matrix $X(\mathbf{x})$ over the ground field $\mathbb{K}$:

$$\mathbf{x} \Leftrightarrow X(\mathbf{x}) = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ x_{N1} & x_{N2} & \cdots & x_{Nn} \end{bmatrix}.$$

The vector representation is more convenient to construct codes, to encode and to decode.

The matrix representation is useful in practical implementations.

Generator matrices of rank codes. Non systematic encoding.

Notation: $[i] \stackrel{def}{=} q^i$, when $i \geq 0$ and $[i] \stackrel{def}{=} q^{N+i}$ when $i < 0$. Let $n \leq N$.

A generator matrix of a MRD $[n, k, d]$ code is of the form

$$\mathbf{G} = \begin{pmatrix} g_1 & \cdots & g_n \\ g_1^{[1]} & \cdots & g_n^{[1]} \\ \cdots & \cdots & \cdots \\ g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{pmatrix},$$

where elements $g_1, \ldots, g_n \in \mathbb{K}_{q^N}$ are linearly independent over $\mathbb{K}_q$. Matrix $\mathbf{G}$ generates a the *rank code* $\mathcal{V}$.

The code $\mathcal{V}$ has minimum rank distance $d = n - k + 1$ and is an MRD-code. It can correct errors of rank up to $t = \lfloor (d-1)/2 \rfloor$.

Let $\mathbf{i} = (i_0\ i_1\ \ldots\ i_{k-1}) \in \mathbb{K}_{q^N}^k$ be an information vector.

Non-systematic encoding. The corresponding code vector is calculated as

$$\mathbf{g(i)} = \mathbf{i} \cdot \mathbf{G}.$$

Check matrices of rank codes. Systematic encoding.

Check matrices satisfy the equation

$$\mathbf{G}\mathbf{H}^{\top} = \mathbf{0}.$$

A parity-check matrix $\mathbf{H}$ of $\mathcal{V}$ has a structure:

$$\mathbf{H} = \begin{pmatrix} h_1 & \cdots & h_n \\ h_1^{[1]} & \cdots & h_n^{[1]} \\ \cdots & \cdots & \cdots \\ h_1^{[d-2]} & \cdots & h_n^{[d-2]} \end{pmatrix},$$

for some elements $h_1, \ldots, h_n \in \mathbb{K}_{q^m}$ linearly independent over $\mathbb{K}_q$.

Systematic encoding.
Let $\mathbf{i} = (i_0 \ i_1 \ \ldots \ i_{k-1}) \in \mathbb{K}_{q^N}^k$ be an information vector. The corresponding code vector is represented as

$$\mathbf{g}(\mathbf{i}) = (\mathbf{v} \ \mathbf{i}),$$

where $\mathbf{v} = (v_0 \ \ldots \ v_{d-2})$ denotes the parity-check vector.

The parity-check matrix is represented as $\mathbf{H} = (\mathbf{H}_1 \ \mathbf{H}_2)$, where $\mathbf{H}_1$ is the square non-singular submatrix of order $d-1$, $\mathbf{H}_2$ is the $(d-1) \times (n-d+1)$ submatrix. Then the parity-check part $\mathbf{v}$ of $\mathbf{g}(\mathbf{i})$ is calculated as

$$\mathbf{v} = -\mathbf{i}\mathbf{H}_2^\top \left(\mathbf{H}_1^\top\right)^{-1}.$$

Subspaces of the extension field

The extension field $\mathbb{K}_{q^N}$ is a linear space of dimension N over the ground field $\mathbb{K}$.

Let $\mathbf{b} = (b_1, \ldots, b_s), s \leq N$ be s elements of $\mathbb{K}_{q^N}$, linearly independent over $\mathbb{K}$.

Denote $V_{\mathbf{b}}(s)$ the linear subspace of dimension s spanned by $\mathbf{b}$.

Choose n subspaces $V_{\mathbf{b}_1}(s_1), V_{\mathbf{b}_2}(s_2), \ldots, V_{\mathbf{b}_n}(s_n)$.

Define a general subspace Φ as the direct product of n subspaces:

$$\Phi = V_{\mathbf{b}_1}(s_1) \bigotimes V_{\mathbf{b}_2}(s_2) \bigotimes \cdots \bigotimes V_{\mathbf{b}_n}(s_n).$$

Subcodes of rank codes over Φ

Let $\mathcal{V}$ be a MRD (n, k, d)-code.

A subcode of $\mathcal{V}$ over Φ is the intersection $\mathcal{V}_\Phi = \mathcal{V} \bigcap \Phi$.

If $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathcal{V}_\Phi \subset \mathcal{V}$, then

$$v_1 \in V_{\mathbf{b}_1}(s_1),\ v_2 \in V_{\mathbf{b}_2}(s_2), \ldots, v_n \in V_{\mathbf{b}_n}(s_n).$$

Problem: construct for a given Φ the subcode $\mathcal{V}_\Phi$ including fast encoding and fast decoding.

Uniformly restricted rank codes

E. M. Gabidulin, P. Loidreau, On subcodes of codes in rank metric, *Proc. 2005 IEEE Int. Sympos. on Information Theory (ISIT'2005).* Adelaide, Australia. September 4-9, 2005. (121-125).

E. M. Gabidulin, P. Loidreau, Properties of subspace subcodes of Gabidulin codes, *Advances in Mathematics of Communication.* **2** (2), (147-158), 2008.

In this case

$$\Phi = V_{\mathbf{b}}(s)^n.$$

A uniformly restricted subcode is isomorphic to a MRD $[s, s - d + 1, d]$-code.

For given $\mathbf{H}$, $\mathbf{b} = (\beta_1\ \beta_2\ \ldots\ \beta_s)$ and $s \times N$ matrix U over the ground field $\mathbb{K}_q$ define the mapping

$$\mathbf{b}U \ \Leftrightarrow\ (h_1\ h_2\ \ldots\ h_N)U^\top.$$

Construct the matrix

$$\mathbf{H}_\Phi = \begin{pmatrix} \beta_1^{[N]} & \ldots & \beta_1^{[N-d+2]} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \beta_s^{[N]} & \ldots & \beta_s^{[N-d+2]} \end{pmatrix}.$$

Consider it as a check matrix of the MRD $[s, s-d+1, d]$-code.

Let $\mathbf{G}_\Phi$ be the corresponding generator matrix.

Non systematic encoding. For a given information vector

$$\mathbf{j} = (j_1 \ \dots \ j_{s-d+1}),$$

calculate a local code vector

$$\mathbf{z}_\Phi(\mathbf{j}) = \mathbf{j}\mathbf{G}_\Phi = (z_1 \ \dots \ z_s).$$

To find $U^\top$ represent this vector as

$$(z_1 \ \dots \ z_s) = (h_1 \ h_2 \ \dots \ h_N)U^\top.$$

Use the obtained matrix $U^\top$ to calculate a code vector

$$\mathbf{g}_\Phi(\mathbf{j}) = \mathbf{b}U$$

of the uniformly restricted subcode. This construction attains the Singleton bound.

Example 1

Let $q = 2$. Let $\mathcal{V}$ be a MRD $(N, N-2, 3)$-code correcting 1-fold rank errors. Let $N = 2^m - 1,\ s = N - m$. Let

$$\Phi = V_{\mathbf{b}}(s)^N,$$

where $V_{\mathbf{b}}(s)$ is the Hamming code correcting single random errors.

A uniformly restricted rank code $\mathcal{V}_\Phi$ can correct all rank errors of rank 1 and all rank errors of the form

$$\mathbf{e} = (\varepsilon_1\alpha^{s_1}, \varepsilon_2\alpha^{s_2}, \ldots, \varepsilon_N\alpha^{s_N}), \quad \varepsilon_j \in \{0, 1\}, \quad s_j \in [0, N-1].$$

Irregularly restricted rank codes

Let $d-1$ subspaces $V_{\mathbf{b}_i}(s_i)$ may coincide with $\mathbb{K}_{q^N}$ (no restrictions for these positions).

Other positions are restricted.

The subspace Φ is of the form

$$\Phi = \left(\mathbb{K}_{q^N}\right)^{d-1} \otimes V_{\mathbf{b}_1}(s_1) \otimes V_{\mathbf{b}_2}(s_2) \otimes V_{\mathbf{b}_{n-d+1}}(s_{n-d+1}).$$

A code vector of a subspace subcode $\mathcal{V}_\Phi = \mathcal{V} \cap \Phi$ has a structure

$$(v_1 \ \ldots \ v_{d-1} \ c_1 \ldots c_{n-d+1}) = (\mathbf{v} \ \mathbf{c}),$$

where $\mathbf{v} = (v_1 \ \ldots \ v_{d-1})$ is the check part of the code vector, $\mathbf{c} = (c_1 \ldots c_{n-d+1})$ is the information part.

It must be

$$c_i \in V_{\mathbf{b}_i}(s_i), \ i = 1, \ldots, n-d+1.$$

In other words,

$$\mathbf{c} \in V_{\mathbf{b}_1}(s_1) \otimes V_{\mathbf{b}_2}(s_2) \otimes V_{\mathbf{b}_{n-d+1}}(s_{n-d+1}).$$

The Singleton bound is

$$|\mathcal{V}_\Phi| \leq q^{s_1+s_2+\cdots+s_{n-d+1}}.$$

Use the systematic encoding. The vector $\mathbf{c}$ is treated as an information vector.

The vector

$$\mathbf{v} = -\mathbf{c}\mathbf{H}_2^\top \left(\mathbf{H}_1^\top\right)^{-1}$$

is a parity-check vector.

The code vector is

$$\mathbf{g}_\Phi(\mathbf{c}) = (-\mathbf{c}\mathbf{H}_2^\top \left(\mathbf{H}_1^\top\right)^{-1} \quad \mathbf{c})$$

This construction attains the Singleton bound.

Example 2

An illustrative example. Let $N = 5,\ n = 4$. Construct for a network coding a rank code in matrix representation of rank distance $d = 2$ with code matrices of the form

$$\begin{pmatrix} m_{11} & m_{12} & m_{13} & m_{14} \\ m_{21} & m_{22} & m_{23} & m_{24} \\ m_{31} & m_{32} & m_{33} & m_{34} \\ m_{41} & m_{42} & 0 & 0 \\ m_{51} & 0 & 0 & 0 \end{pmatrix}.$$

We use an equivalent vector code with the check matrix

$$\mathbf{H} = (1\ \alpha\ \alpha^2\ \alpha^3).$$

A code vector of the irregularly restricted rank code has the form

$$\mathbf{g}(\mathbf{c}) = (-c_1\alpha - c_2\alpha^2 - c_3\alpha^3 \; c_1 \; c_2 \; c_3),$$

where

$$\begin{aligned} c_1 &= x_1 + x_2\alpha + x_3\alpha^2 + x_4\alpha^3, \\ c_2 &= y_1 + y_2\alpha + y_3\alpha^2, \\ c_3 &= z_1 + z_2\alpha + z_3\alpha^2, \end{aligned}$$

where x, y, z are information symbols.

Then convert the code vector $\mathbf{g}(\mathbf{c})$ into the corresponding code matrix $M(\mathbf{c})$.

Conclusion

Subspace subcodes of rank codes have applications in parallel channels whenever the errors occur along lines or columns.

They can also be used in the construction of Space-Time codes with optimal rate diversity trade-off.

Using subcodes in cryptography is under investigation.

Also implementation in network coding is not well known.

Many thanks
for your attention!