Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 157–161*

New subcodes of rank codes [1]

Ernst M. Gabidulin ernst_gabidulin@yahoo.com
Moscow Institute of Physics and Technology (State University)

Abstract. We investigate properties of subspace subcodes of a family of maximal rank distance (MRD) codes. We design systematic encoding and decoding algorithms for subspace subcodes.

1 Introduction

Subspace subcodes of rank codes have applications in the field of error-correction whenever information is stored under the form of bi-dimensional arrays (like in tape-recording or memory arrays for chips) and 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 [9, 10].

Using subcodes in the GPT cryptosystem [11] is under investigation.

Also implementation in network coding is not well known.

Section 2 contains some background. Section 3 introduces to the general definition of subcodes. Known constructions are presented in Section 4. New results are given in Section 5. Section 6 concludes the paper.

2 Rank codes

Let $\mathbb{K}_q$ be the finite field with q elements and let $\mathbb{K}_{q^N}$ be an extension field of degree N. We will also consider $\mathbb{K}_{q^N}$ as a N-dimensional vector space over $\mathbb{K}_q$.

Let $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{K}_{q^N}^n$. The rank of $\mathbf{x}$ over $\mathbb{K}_q$ is the maximal number of x_i which are linearly independent over $\mathbb{K}_q$. Equivalently, the rank of $\mathbf{x}$ over $\mathbb{K}_q$ is the rank of the $N \times n$ q-ary matrix obtained by extending the components of $\mathbf{x}$ over a basis of $\mathbb{K}_{q^N}/\mathbb{K}_q$.

The $\mathbb{K}_q$-rank of $\mathbf{x}$ is denoted by $\mathrm{Rk}(\mathbf{x})$.

A code $\mathcal{V}$ is a linear code of dimension k if it is a k-dimensional subspace of the space $\mathbb{K}_{q^N}^n$.

The minimum rank distance of a linear vector code $\mathcal{V}$ is defined by

$$d \stackrel{def}{=} \min_{\mathbf{v} \in \mathcal{V} \setminus \{0\}} (\mathrm{Rk}(\mathbf{v}))$$

[1] This research is partially supported by the grant RFBR 12-07-00122-a

Such a code is denoted as a $[n, k, d]$ code.

If $N \geq n$, then an equivalent of Singleton bound has a form

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

A linear code attaining the bound is called a *maximum rank distance* code (MRD-code).

Define $[i] \stackrel{def}{=} q^i$, when $i \geq 0$ and $[i] \stackrel{def}{=} q^{m+i}$ when $i < 0$. Let $n \leq N$. A generator matrix of a MRD $[n, k, d]$ code was proposed in [1] in the form

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

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

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

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

The code $\mathcal{V}$ has minimum rank distance $d = n - k + 1$ and is therefore an MRD-code. They 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

$$\mathbf{g}(\mathbf{i}) = \mathbf{i} \cdot \mathbf{G}. \tag{3}$$

Systematic encoding. The corresponding code vector is represented as

$$\mathbf{g}(\mathbf{i}) = (\mathbf{v}\ \mathbf{i}), \tag{4}$$

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

$$\mathbf{v} = -\mathbf{i}\mathbf{H}_2^\top \left(\mathbf{H}_1^\top\right)^{-1}. \tag{5}$$

Several polynomial-time decoding algorithms were designed, see [1–6].

3 Subspaces of the extension field and subspace subcodes

Consider the extension field $\mathbb{K}_{q^N}$ as a N-dimensional vector space over $\mathbb{K}_q$.

Let $\mathbf{b} = (b_1, \ldots, b_s), s \leq N$, be a set of s elements which are linearly independent over the ground field $\mathbb{K}_q$.

Let $V_{\mathbf{b}}(s)$ be the linear s-dimensional subspace spanned by $\mathbf{b}$.

Define the direct product of n possibly different subspaces as

$$\Phi = V_{\mathbf{b}_1,\ldots,\mathbf{b}_n}(s_1, s_2, \ldots, s_n) = V_{\mathbf{b}_1}(s_1) \otimes V_{\mathbf{b}_2}(s_2) \otimes V_{\mathbf{b}_n}(s_n).$$

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

A subspace subcode of the code $\mathcal{V}$ over the subspace Φ is defined as the intersection $\mathcal{V}_\Phi = \mathcal{V} \cap \Phi$.

Our goal: to construct subcodes $\mathcal{V}_\Phi$ for interesting Φ.

If Φ is the product of identical subspaces, then subcodes are called uniformly restricted rank codes. Otherwise they are called irregularly restricted rank codes.

4 Uniformly restricted rank codes

These subcodes were investigated in [7, 8]. In this case

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

It was shown that a uniformly restricted subcode is isomorphic to a MRD $[s, s-d+1, d]$-code. For given $\mathbf{b}$, $\mathbf{H}$ and $s \times n$ matrix U over the ground field $\mathbb{K}_q$ define the mapping

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

Let

$$\mathbf{H}_\Phi = \begin{pmatrix} \beta_1^{[N]} & \ldots & \beta_1^{[N-d+2]} \\ \ldots & \ldots & \ldots \\ \beta_s^{[N]} & \ldots & \beta_s^{[N-d+2]} \end{pmatrix} \tag{6}$$

be the parity-check matrix of the MRD $[s, s-d+1, d]$-code and $\mathbf{G}_\Phi$ the corresponding generator matrix. The non-systematic encoding is as follows. For a given information vector $\mathbf{j} = (j_1\ \ldots\ j_{s-d+1})$, calculate a local code vector $\mathbf{j}\mathbf{G}_\Phi = (z_1\ \ldots\ z_s)$. To find $U^\top$ represent this vector as

$$(z_1\ \ldots\ z_s) = (h_1\ h_2\ \ldots\ h_n)U^\top.$$

Use the obtained matrix $U^\top$ to calculate a code vector $\mathbf{b}U$ of the uniformly restricted subcode.

5 Irregularly restricted rank codes

Another interesting case is described as follows. Assume that $d-1$ subspaces $V_{\mathbf{b}_i}(s_i)$ coincide with $\mathbb{K}_q$, i.e., there are no restrictions for these positions. 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 $\mathbf{v} = (v_1 \ \ldots \ v_{d-1})$, $\mathbf{c} = (c_1 \ldots c_{n-d+1})$. 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

$$|\mathcal{V}_\Phi| \leq |\Phi| = q^{s_1+s_2+\cdots+s_{n-d+1}}. \tag{7}$$

To construct a subspace subcode with these restrictions, we use the systematic encoding (3)-(5). The vector $\mathbf{c}$ is treated as an information vector, while the vector $\mathbf{v} = -\mathbf{c}\mathbf{H}_2^\top \left(\mathbf{H}_1^\top\right)^{-1}$ as a parity-check vector. Note, that this construction attains the Singleton bound (7).

Subcodes with this restrictions can be used in constructions of multicomponent network codes [12–15].

6 Conclusion

A new class of subspace subcodes of rank codes is proposed. It is matched especially for network coding and cryptography applications. Still specific implementations need to be investigated in more details.

References

[1] E. M. Gabidulin, Theory of Codes with Maximum Rank Distance, *Probl. Inform. Transm.,* vol. 21, No. 1, pp. 1–12, July, 1985.

[2] E. M. Gabidulin, A Fast Matrix Decoding Algorithm for Rank-Error-Correcting, *Proc. 1st French–Soviet Workshop on Algebraic Coding,* Paris, France. July 22-24, 1991. Lecture Notes in Computer Science. **573**, (126-133) Berlin: Springer, 1992.

[3] A. V. Paramonov, O. V. Tretjakov, An Analogue of Berlekamp-Massey Algorithm for Decoding Codes in Rank Metric. *Proc. of MIPT,* 1991.

[4] G. Richter, S. Plass, Fast Decoding of Rank-Codes with Rank Errors and Column Erasures, *Intern. Symp. on Inform. Theory 2004, ISIT 2004,* (398), 2004.

[5] P. Loidreau, A Welch–Berlekamp Like Algorithm for Decoding Gabidulin Codes, *Proc. 4th Int. Workshop on Coding and Cryptography (WCC'2005),* Bergen, Norway. March 14-18, 2005. Lecture Notes in Computer Science. **3969**. Berlin: Springer, (36-45), 2006.

[6] A. Wachter, V. Afanasiev, V. R. Sidorenko, Fast decoding of Gabidulin codes. *Proc. of Seventh International Workshop on Coding and Cryptography*, (433-442). April 11-15, 2011, Paris, France.

[7] 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).

[8] E. M. Gabidulin, P. Loidreau, Properties of subspace subcodes of Gabidulin codes, *Adv. Mathematics of Communication.* **2** (2), (147-158), 2008.

[9] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, Space-Time Codes for High Data Rate Wireless Communication: Performance Criterion and Code Construction, *IEEE Trans. Inform. Theory.* **44** (2), (744-765), 1998.

[10] E. M. Gabidulin, M. Bossert, and P. Lusina, Space-Time Codes Based on Rank Codes, *Proc. 2000 IEEE Int. Sympos. on Information Theory (ISIT'2000).* Sorrento, Italy. June 25-30, 2000. (283).

[11] E. M. Gabidulin, A. V. Paramonov, O. V. Tretjakov, Ideals over a Non-commutative Ring and Their Application in Cryptology, *Advances in Cryptology – Eurocrypt '91.* Editor: Davies, D.W. Lecture Notes in Computer Science, **547,** (482–489), Berlin-Heidelberg: Springer-Verlag, 1991.

[12] D. Silva, F. R. Kschischang, R. Koetter, A Rank-Metric Approach to Error Control in Random Network Coding, *IEEE Trans. Inform. Theory.* **54** (9), (3951-3967), 2008.

[13] E. M. Gabidulin, M. Bossert, Algebraic codes for network coding, *Problems of Information Transmission.* **45** (4), (343-356), 2009.

[14] N. Etzion, N. Silberstein, Error-correcting Codes in Projective Space Via Rank-Metric Codes and Ferrers Diagrams, *IEEE Trans. Inform. Theory.* **55** (7), (2909-2919), 2009.

[15] E. M. Gabidulin, N, I. Pilipchuk, New Multicomponent Network Codes Based on Block Designs, *Proc. International Mathematical Conference "50 years of IPPI".* 2011. ISBN 978-5-901158-15-9.