Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 300–306*

On cardinality of network subspace codes [1]

Alexander Shishkin sisoid@frtk.ru
Ernst Gabidulin ernst_gabidulin@yahoo.com
Nina Pilipchuk pilipchuk.nina@gmail.com
Moscow Institute of Physics and Technology

Abstract. We analyze properties of different subspace network codes. Our study includes Silva-Koetter-Kshishang codes (SKK-codes), multicomponent codes with zero prefix (Gabidulin-Bossert codes), codes based on combinatorial block designs, Etzion-Silberstein codes (E-S codes) based on Ferrer's diagrams, and codes which use greedy search algorithm and restricted rank codes. We calculate cardinality values of these codes for different parameters and compare actual cardinality with the upper bound of subspace codes. The ratio of the actual cardinality to the upper bound is called code efficiency. It is shown that multicomponent codes have greater efficiency than SKK-codes for all parameters. In cases of minimal and maximum code distances the upper bound of cardinality is attained for some codes under consideration.

1 Introduction

Cardinality is a very important code characteristic: the greater is cardinality, the higher is transmission speed. Thus, the problem how to construct codes with large cardinality has received much attention in technical literature. A serious breakthrough in this direction was made in works by Koetter, Kshishang and Silva [1, 2]. The authors introduced so-called lifting construction of subspace codes, based on rank codes [3] and called them random network codes. Shortly after Gabidulin and Bossert generalized this construction using all-zero matrices as prefix [4,5]. They have created multicomponent codes which are an union of several codes at a definite minimal code distance. There is the same minimal distance between any two components. The cardinality of multicomponent code equals the sum of cardinalities of all components. It was shown that cardinality of multicomponent codes attains the upper bound for maximum code distance [5].

All subsequent years study in this direction is still actively pursued by many researchers in different countries. A lexicographic approach and Ferrer's diagrams were used by Etzion and Silberstein to build multicomponent codes with large cardinality [9,10]. Using combinatorial balanced incomplete block designs a new class of multicomponent network codes was built [6–8]. For intermediate code distances the cardinality of such codes is larger than the cardinality of

[1]This research is partially supported by RFBR grant (project No 12-07-00122-a).

codes with zero prefix. A new flexible construction of multicomponent codes was proposed in the work [11] where lexicographic approach and rank subcodes were used.

We give a comparative analysis of efficiency of network codes for the described constructions. The code efficiency is defined as the ratio of the actual cardinality to the upper bound at the following parameters: code length, subspace dimension and code distance.

In the next sections we introduce the upper bound of subspace codes cardinality as a function of the code parameters. Then we briefly describe different code constructions and calculate the cardinality values of these codes. On the basis of comparison we reveal the conditions when some code may be more efficient then others. Conclusion provides a summary review and indicates open issues.

2 Upper bound of codes cardinality

The upper bound of subspace codes cardinality was obtained in 2003 in the work [12]. It is a function of code length, subspace dimension and subspace distance:

$$M_{max} = \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-m+\delta}-1)}{(q^m-1)(q^{m-1}-1)\dots(q^{\delta}-1)}. \quad (1)$$

where $\delta = \frac{d_{sub}}{2}$, $d_{sub} = 2\delta$ - subspace distance, m - subspace dimension, n - code length.

Let us analyze the dependence of the upper bound M_{max} on the code length n for a given code dimension m and code distance $d_{sub} = 2\delta$. Fig.1 represents M_{max} as a function of code length n at $m = 4$ and $\delta = 1, 2, 3, 4$.

Note that Y-axis is logarithmic. As one can see, the value of M_{max} rises with the growth of n for fixed δ. Furthermore, there is almost a straight line $\lg(M_{max})$ as a function of n. For fixed n the function M_{max} rises with decreasing of code distance $d_{sub} = 2\delta$. The overall conclusion of this analysis is the following: the upper bound of code cardinality increases when the code length increases, and it decreases when the code distance increases.

3 Constructions of subspace network codes

The random network codes (SKK-codes) [2] represent a set of $k \times n$ matrices over the base field $GF(q)$:

$$\mathcal{C} = \left\{ \begin{bmatrix} I_k & M \end{bmatrix} \right\},$$

where I_k is the identity matrix of order k, submatrix M is the $k \times (n-k)$ rank code matrix over the field $GF(q)$. Let d_r be the rank distance of this code. Then subspace distance of the network code is equal to $d_{sub}(\mathcal{C}) = 2d_r$.

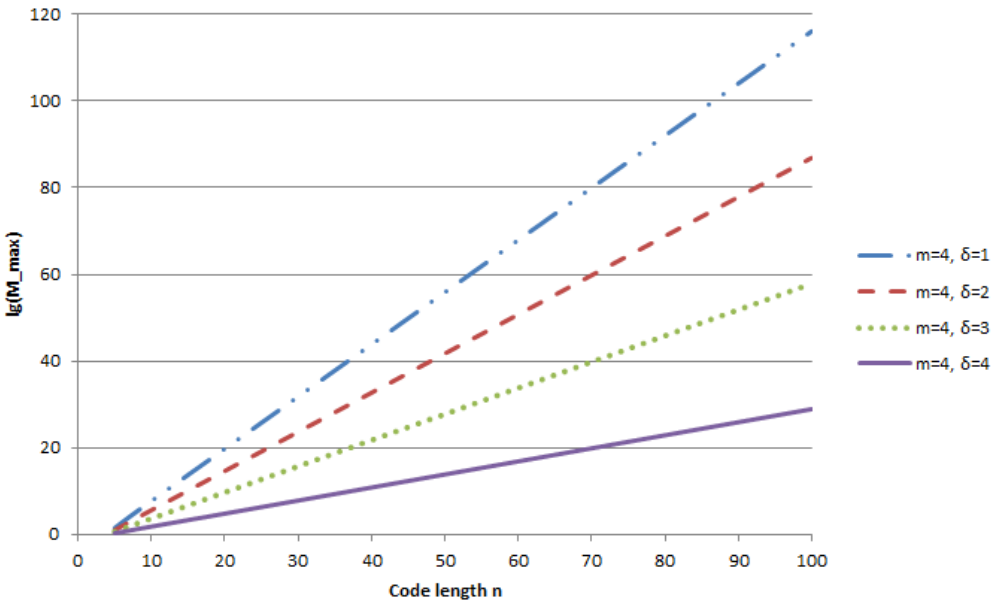

Figure 1: The dependence of M_{max} on code length n.

Gabidulin-Bossert codes with zero prefix [4] have a multicomponent structure. The first component is an SKK-code with the $k \times (n-k)$ rank code submatrix. The second component has all-zero matrix as a prefix of the whole code matrix. Number of rows in this all-zero matrix is equal to k while number of columns is equal to rank distance $d_r = \delta$. The identity matrix of order k follows the zero prefix and the leftmost positions in the network code matrix are occupied by $k \times (n-k-\delta)$ rank code matrix. The third code component contains two all-zero matrices as a prefix and so on for the remaining components. Number of components depends on the code length. The last component contains only zero prefix and an identity matrix when $(n-k)$ is divisible by δ.

In the works [9,10] Etzion and Silberstein introduced a greedy lexicographic search of the network code components among the the set of all binary vectors with the length n and Hamming weight m. This approach avoids the use of complex combinatorial circuits and gives considerable freedom to choose parameters of the network code. However, this approach does not guarantee that all subcodes in the multicomponent construction are linear rank codes and therefore the decoding algorithm may be too complicated.

There is another method to construct multicomponent codes. It uses incomplete balanced block designs [13]. These block designs define multiindeces which in turn define the location of the identity matrix columns in the network code matrix. Free elements of the code matrix are used for building rank subcodes [8]. Each multiindex corresponds to the code component. The first code

component corresponds to SKK-code. It has the greatest cardinality among all other components.

In the paper [11] a combined approach which takes advantage of both previous methods was introduced. It uses greedy search for the network code components and linear rank codes with restrictions as subcodes. On the first step for the set of all binary vectors-indices of length n and Hamming weight m the cardinality of corresponding rank subcodes is defined. Lexicographically the first vector-index corresponds to the SKK-code and it is used as the first code component. Then greedy search starts for the code component with the biggest cardinality among the remaining. If its subspace distance to all already added to code subspaces is not less than d_{sub} it is included into the code, and so on. This method has no limits on code parameters and allows decoding by means of standard algorithms. It does not exceed the cardinality of E-S codes.

4 Efficiency of subspace network codes

The code efficiency is defined as the ratio of its actual cardinality to the upper bound for fixed parameters. We introduce the notation: η_{skk} – SKK-code efficiency, η_0 – efficiency of the codes with zero prefixes, η_{es} – E-S codes efficiency, η_b – efficiency of the code based on block designs and η_c – efficiency of the code based on combined approach.

We analyze dependency of efficiency on the code length. Our calculations at $m = 3$, 4 and $\delta = 2$ are shown in the Table 1.

Table 1: Efficiency at different n.

n	7	9	15	31
η_{skk}, $m = 4$	0,650	0,624	0,615	0,615
η_{skk}, $m = 3$	0,672	0,660	0,656	0,656
η_0, $m = 4$	0,357	0,688	0,685	0,685
η_0, $m = 3$	0,693	0,702	0,700	0,700
η_b, $m = 3$	0,759	0,740	0,746	0,750
η_c, $m = 3$	0,759	0,750	0,746	0,750
η_c, $m = 4$	0,367	0,703	0,700	0,700

One can see that code efficiency weakly depends on code length. In the Table 2 we give our calculation results for dependence of efficiency on code distance, where code distance changes from minimum $\delta = 1$ to maximum $\delta = 4$. As can be seen from the table, η_{skk} rises with the growth of δ for fixed subspace dimension.

Table 2: Network codes efficiency for $m = 4$ and $m = 5$.

δ	1	2	3	4
η_{skk}, $n = 13, m = 4$	0,315	0,670	0,820	0,938
η_{skk}, $n = 10, m = 4$	0,312	0,619	0,823	0,938
η_0, $n = 13, m = 4$	0,329	0,675	0,833	0,998
η_0, $n = 10, m = 4$	0,333	0,629	0,826	0,953
η_{es}, $n = 9, m = 4$	-	0,716	-	-
η_{es}, $n = 10, m = 5$	-	-	0,803	-
η_b, $n = 13, m = 4$	1	-	0,835	-
η_b, $n = 10, m = 4$	1	0,670	-	-
η_c, $n = 10, m = 5$	1	0,673	0,802	0,912
η_c, $n = 13, m = 4$	1	0,700	0,835	0,998

Codes with zero prefix attain the maximum efficiency $\eta_0 = 1$ for $\delta = m$. Codes for $\delta = 1$ consist of all subspaces in the Grassmannian. For intermediate values of δ all multicomponent codes are more effective than SKK-codes. Similarly, codes based on block designs have higher efficiency than codes with zero prefix. E-S code has the highest efficiency for $\delta = 2$ and $\delta = 3$ while codes based on combined approach are rather efficient for all subspace distances.

5 Conclusion

- Cardinality of SKK-code and cardinality of multicomponent codes rises with the growth of code length. At the same time, code efficiency weakly depends on the code length.
- For all the considered codes efficiency clearly depends on the subspace distance: it rises with the growth of the subspace distance at the fixed values of other parameters.
- For codes with zero prefix the upper bound of cardinality attains in the case of maximum code distance. In the case of minimum code distance the upper bound of cardinality attains at complete block design.
- At intermediate subspace distances Etzion–Silberstein code shows the best efficiency at $n = 9$, $m = 4$, $\delta = 2$. At other parameters the maximal cardinality has the code [11], the code on the combinatorial design has the

same cardinality at the same parameters, then there is the code with zero prefix which is a little worse at intermediate subspace distances. Finally, SKK-code is characterized by minimal efficiency because it uses only one component of multicomponent codes.

- Therefore, we know how to construct codes with maximal cardinality for minimum and maximum code distances, however, how to construct codes with maximal cardinality at intermediate subspace distances is open problem.

References

[1] *Koetter R., Kschischang F. R.* Coding for errors and erasures in random network coding // IEEE Intern. Symp. on Inf. Theory. Proc. ISIT-07. – 2007. - P. 791-795.

[2] *D.Silva, F. R. Kschischang, R. Koetter* A Rank-Metric Approach to Error Control in Random Network Coding// IEEE Transactions on Information Theory, vol. 54, pp. 3951-3967, No. 9, Sept. 2008.

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

[4] *Gabidulin E.M., Bossert M.* Codes for Network Coding // IEEE Intern. Symposium on Inf. Theory. Proc. ISIT-08. – 2008. – P. 867-870.

[5] *Gabidulin E.M., Bossert M.* Algebraic codes for network coding // Probl. Inform. Transm. vol. 45, No. 4, pp. 54–68, 2009.

[6] *Gabidulin E.M., Pilipchuk N.I.* Multicomponent Network Coding // Proc. 7th Int. Workshop on Coding and Cryptography (WCC'2011), 2011.– P.443-452.

[7] *Gabidulin E.M., Pilipchuk N.I.* New Multicomponent Network Codes Based on Block Designs // Proc. Intern. Conf. "50 years PPI", 2011 (CD).

[8] *Gabidulin E.M., Pilipchuk N.I.* Rank subcodes in multicomponent network coding // Probl. Inform. Transm. vol. 49, No. 1, pp. 46–60, 2013.

[9] *Etzion T., Silberstein N.* Error-Correcting Codes in Projective Spaces via Rank-Metric Codes and Ferrers Diagrams // IEEE Transactions on Information Theory. — 2011. — V. 55, N. 7. — P. 2909–2919.

[10] *Etzion T., Silberstein N.* Large Constant Dimension Codes and Lexicodes // Advances in Mathematics of Communications. — 2011. — V. 5, N. 2. — P. 177–189.

[11] *Shishkin A.* A combined method of constructing multicomponent network codes // MIPT Proceedings. – 2014. V. 6. No. 2.

[12] *Wang H., Xing C., Safavi-Naini R.* Linear Autentication Codes: Bounds and Constructions // IEEE Trans. Inform. Theory, 2003, v. 49, No 4, pp. 866-873.

[13] *Hall M.* // Combinatorial Theory, 1967.