New Multicomponent Network Codes Based on Block Designs

Ernst M. Gabidulin, Nina I. Pilipchuk
Moscow Institute of Physics and Technology (State University)
Email: ernst.gabidulin@gmail.com, pilipchuk.nina@gmail.com

Abstract

We propose new *multicomponent* network codes based on block designs. They have the prescribed subspace metric distance. This class of codes is a generalization of the Silva-Kötter-Kschischang construction (SKK codes). Component constructions are chosen in such a manner that subspace distance between components would be not less than subspace distance of each component. A few examples are given.

Keywords: Network coding, subspace distance, lifted rank-metric codes

1 Introduction

Let $\mathbb{F}_q$ be a finite field of q elements. Let $\mathbb{F}_q^n$ be a fixed n-dimensional vector space over the field $\mathbb{F}_q$. Let $\mathcal{P}(n)$ be the set of all subspaces of $\mathbb{F}_q^n$. A k-dimensional subspace V consists of q^k vectors of length n over the base field $\mathbb{F}_q$. It can be considered as the *row spanned* subspace of a $k \times n$ matrix $M(V)$ over $\mathbb{F}_q$ of full rank k. We refer to the matrix $M(V)$ as a *basic generator* matrix of V.

For any two subspaces U and V in $\mathcal{P}(n)$, the distance function is defined by

$$\begin{aligned} d_{\text{sub}}(U, V) &= \dim(U \uplus V) - \dim(U \cap V) = \\ &= \dim U + \dim V - 2\dim(U \cap V) = \\ &= 2\dim(U \uplus V) - \dim U - \dim V. \end{aligned} \quad (1)$$

This distance function is known as the *subspace* distance.

Network coding is a new area of Information theory. A subspace approach for network coding is introduced in [1]. The set $\mathcal{P}(n)$ is considered as the alphabet, or, as the signal space. A Source represents k packets of length n as the basic generator matrix X of a subspace spanned by its rows. The Source transmits the matrix X to Destination. Intermediate nodes fulfill random transformations over rows of received matrix before retransmitting it to the next nodes. At last the Destination gets the transformed matrix Y. It is possible to recover the row spanned subspace of Y though the Destination does know intermediate transformations. If no corruption then the row spanned subspaces of Y and X are identical. If corruptions may exist then we have to use network coding.

A $[n, M, d_S]$ code with prescribed distance d_S and cardinality M is a set of subspaces $\{V_1, \ldots, V_M\}$ with basic matrices $\{X_1, \ldots, X_M\}$ such that $\min\limits_{i \neq j} d_{\text{sub}}(V_i, V_j) = d_S$.

If all subspaces V_i are of identical dimension k, then a code is called a $[n, M, d_S, k]$ *constant dimension code.*

The main problem is constructing $[n, M, d_S, k]$ and $[n, M, d_S]$ codes.

Codes for network coding are proposed in several papers (see, [1] - [5]). The lifting construction of Gabidulin‘s rank-metric code in the matrix representation was proposed by Wang et al. in [7] several years earlier in the context of authentication codes. It was independently reopened for network coding in [1]. Several constructions of $[n, M, d_s]$ codes are given in [2] and [3]. These codes are known now as Silva–Kötter–Kschischang codes (SKK codes, for brevity). A construction based on linearized polynomials was generalized in [4]. A connection between constant-rank codes and constant-dimension codes and new codes are presented in [5]. Use of the standard reduced row echelon form of basic $k \times n$ generator matrices for subspaces is proposed in [6]. Each form can be described by means of a n-vector with k *ones*. This vector is called the generator vector of the form. It allows to introduce codes similar to SKK codes (the Ferrers diagram rank-metric codes) though the general construction is unknown.

This paper is devoted to constructing new *multicomponent* codes with a specific subspace-metric distance. Our goal is to increase code cardinality which is an important performance for application background. Each component code consists of generator matrices with the same reduced row echelon form. Any two subspaces of this component must have the subspace distance d_S or greater.

On the other hand, components must be chosen in such a manner that subspace distance between different components would be not less than subspace distance of each component. Therefore the problem is to choose a set of the generator vectors. We propose to choose as sets block designs with suitable parameters. Our examples show that such codes may outperform known codes.

2 Network codes over subspaces of standard form

Recall that SKK codes are described as the set of $k \times n$ basic matrices over $\mathbb{F}_q$ of the form

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

where I_k is the identity matrix of order k. A submatrix $M \in \mathcal{M}$, where $\mathcal{M}$ is a matrix code consisting of $k \times (n-k)$ matrices over $\mathbb{F}_q$. Let $d_r(\mathcal{M})$ be *rank-metric distance* of this code.

Then subspace-metric distance $d(\mathcal{C}) = 2d_r(\mathcal{M})$.

On the other hand, code matrices can be considered as matrices in reduced row echelon form induced by the identity matrix I_k.

We consider below the general case of reduced row echelon form.

2.1 The reduced row echelon form of a subspace

Let X be a $k \times n$ generator matrix of a k-dimensional subspace. Apply to X the Gaussian elimination procedure. Then we get the $k \times n$ matrix with rank k in *reduced row echelon form.* The following conditions are satisfied [6]:

- The leading coefficient of a row is always to the right of the leading coefficient of the previous row.
- All leadings coefficients are *ones.*
- All entries of a row before the leading coefficient are *zeroes.*
- Every leading coefficient is the only nonzero entry in its column.

Therefore the matrix in reduced row echelon form contains as entries k leading coefficients "*ones*" and related "*zeroes*". All the other entries are called "*free parameters*". Denote the set of free parameters by $\mathbf{a}$.

Assume that the leading coefficient of the first row appears at the position i_1, of the second row – at the position i_2, of the last kth row – at the position i_k. We have $1 \le i_1 < i_2 < \cdots < i_k \le n$. Integers $i_1,\ i_2,\ \ldots,\ i_k$ define completely the structure of the generator matrix in *reduced row echelon form* including the set of free parameters $\mathbf{a}$.

The vector $\mathbf{i} = [i_1\ i_2\ \ldots\ i_k]$ is called the identifier (ID) of the reduced row echelon form. Denote the corresponding generator matrix by $X(\mathbf{i}, \mathbf{a})$.

Example 1. *Let $n = 6, k = 3$, $\mathbf{i} = [i_1\ i_2\ i_3] = [1\ 3\ 4]$. Then a generator matrix $X(\mathbf{i}, \mathbf{a})$ of this echelon form is as follows:*

$$X(\mathbf{i}, \mathbf{a}) = \begin{bmatrix} 1 & a_{1,1} & 0 & 0 & a_{1,2} & a_{1,3} \\ 0 & 0 & 1 & 0 & a_{2,2} & a_{2,3} \\ 0 & 0 & 0 & 1 & a_{3,2} & a_{3,3} \end{bmatrix}.$$

The matrix has 7 free parameters $a_{i,j}$. Entries $a_{i,j}$ can be chosen arbitrarily in $\mathbb{F}_q$. Therefore we have q^7 different 3-dimensional subspaces with the same ID $\mathbf{i} = [i_1\ i_2\ i_3] = [1\ 3\ 4]$.

In general, let $\mathbf{i} = [i_1\ i_2\ \dots\ i_k]$ be the ID of a reduced row echelon form. Calculate the number of free parameters and the structure of the matrix. We observe in the first row, that there exists between columns i_1 and i_2 exactly $f_1 = i_2 - i_1 - 1$ parameters; between columns i_2 and i_3 exactly $f_2 = i_3 - i_2 - 1$ parameters; $\dots$; between columns i_{k-1} and i_k exactly $f_{k-1} = i_k - i_{k-1} - 1$ parameters; after the column i_k exactly $f_k = n - i_k$ parameters. In common, the first row contains $n - k + 1 - i_1$ free parameters. Similarly, the second row contains between columns i_2 and i_3 exactly $f_2 = i_3 - i_2 - 1$ parameters; $\dots$; between columns i_{k-1} and i_k exactly $f_{k-1} = i_k - i_{k-1} - 1$ parameters; after the column i_k exactly $f_k = n - i_k$ parameters. In common, the second row contains $n - k + 2 - i_2$ free parameters. Sequentially, we find that the $(k-1)$th row contains between columns i_{k-1} and i_k exactly $f_{k-1} = i_k - i_{k-1} - 1$ parameters; after the column i_k exactly $f_k = n - i_k$ parameters. In common, $n - 1 - i_{k-1}$ free parameters. The last kth row contains $f_k = n - i_k$ free parameters. The whole number of free parameters is equal to

$$f = \sum_{i=1}^{k} f_i = nk - \frac{(k-1)k}{2} - i_1 - i_2 - \dots - i_k.$$

Consider the structure of free parameters. Let $F(\mathbf{i}, \mathbf{a})$ be the minimal submatrix of $X(\mathbf{i}, \mathbf{a})$, containing all free parameters. In common position, it has the following echelon form:

$$F(\mathbf{i}, \mathbf{a}) = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,k-1} & a_{1,k} \\ 0 & a_{2,2} & a_{2,3} & \cdots & a_{2,k-1} & a_{2,k} \\ 0 & 0 & a_{3,3} & \cdots & a_{3,k-1} & a_{3,k} \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_{k-1,k-1} & a_{k-1,k} \\ 0 & 0 & 0 & \cdots & 0 & a_{k,k} \end{bmatrix}, \tag{2}$$

where $a_{1,1}$ is a $1 \times f_1$ block of free parameters, $a_{i,2}$, $i = 1, 2$, are $1 \times f_2$ blocks of free parameters, $\dots$, $a_{i,k-1}$, $i = 1, 2, \dots, k-1$, are $1 \times f_{k-1}$ blocks of free parameters, $a_{i,k}$, $i = 1, 2, \dots, k$, are $1 \times f_k$ blocks of free parameters.

If $f_s = 0$ for some s, then the corresponding column block must be deleted.

2.2 Codes over matrices with a given reduced row echelon form

Assume that for a given $\mathbf{i}$ there exists a subset of free parameters $\mathcal{A}$ such that the matrix code $F(\mathbf{i}, \mathbf{a})$, $\mathbf{a} \in \mathcal{A}$ has *rank distance* d_r. Let code matrices be the set $\mathcal{C}(\mathbf{i}) = \{X(\mathbf{i}, \mathbf{a}),\ \mathbf{a} \in \mathcal{A}\}$. The subspace distance $d_S(\mathcal{C})$ of this code is given by the formula

$$d_S(\mathcal{C}) = 2d_r.$$

Proof is similar to proof for SKK codes [1].

For simplicity, consider the case $i_k \neq n$ and $k \leq n - k + 1 - i_1$. Then the size of $F(\mathbf{i}, \mathbf{a})$ is $k \times n - k + 1 - i_1$. It follows from Eq. (2) that this matrix contains

$$f = (k-1)f_1 + (k-2)f_2 + \dots + f_{k-1}$$

zero entries, which are not free parameters.

Theorem 1. *If $d_r \leq k$, then there exists a matrix code $F(\mathbf{i}, \mathbf{a})$ with rank distance d_r and cardinality*

$$M = q^{(n-k+1-i_1)(k-d_r+1)-f}.$$

Sketch of proof. Well known that without restrictions there exists a $k \times n-k+1-i_1$ matrix rank metric code of cardinality $\widetilde{M} = q^{(n-k+1-i_1)(k-d_r+1)}$. Restrictions in the form of f zero entries reduces cardinality to q^f times. Hence $M = \widetilde{M}/q^f = q^{(n-k+1-i_1)(k-d_r+1)-f}$. □

3 Block design constructions

3.1 Constructions of multicomponent codes

Let $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{P}(n)$ be codes of subspace-metric distance $d_1,\ d_2$, respectively. Codes are said to be *ρ-intersecting*, if $\max\limits_{U \in \mathcal{C}_1,\ V \in \mathcal{C}_1} \dim(U \cap V) = \rho$.

Denote by $r_1 = \min(\dim(U) : U \in \mathcal{C}_1)$, $r_2 = \min(\dim(V) : V \in \mathcal{C}_2)$.

Lemma 1. *Let component codes $\mathcal{C}_1,\ \mathcal{C}_2$ be ρ-intersecting codes. Let $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$ be the code obtained as the union of component codes. We have:*

1. *The cardinality of $\mathcal{C}$ equals $|\mathcal{C}| = |\mathcal{C}_1| + |\mathcal{C}_2|$.*

2. *Subspace-metric distance of $\mathcal{C}$ equals $d(\mathcal{C}) = \min(d_1, d_2, r_1 + r_2 - 2\rho)$.*

Proof. The first statement is evident because codes $\mathcal{C}_1,\ \mathcal{C}_2$ have no common members. If $U_1, U_2 \in \mathcal{C}_1$, then $d(U_1, U_2) \geq d_1$. If $V_1, V_2 \in \mathcal{C}_2$, then $d(V_1, V_2) \geq d_2$. If $U \in \mathcal{C}_1,\ V \in \mathcal{C}_2$, then $d(U, V) = \dim(U) + \dim(V) - 2\dim(U \cap V) \geq r_1 + r_2 - 2\rho$. This proofs the second statement. □ □

Let $\dim = \dim V = k$, $d_1 = d_2 = 2d_r$. The space distance between components is $2k - 2\rho$. We require $2k - 2\rho = 2d_r$, or, $\rho = k - d_r$. Let the ID of $\mathcal{C}_1$ be $\mathbf{i} = [i_1\ i_2\ \ldots\ i_k]$. Let the ID of $\mathcal{C}_2$ be $\mathbf{j} = [j_1\ j_2\ \ldots\ j_k]$. Then the number of common integers must be less than or equal to $\rho = k - d_r$. Hence we have to choose block designs with suitable parameters.

3.2 Block designs

3.3 Balanced incomplete block designs

Given a finite set $\mathcal{N} = \{1, 2, \ldots, n\}$ and integers $k, r, \lambda \geq 1$, we define a 2-design B to be a set of k-element subsets of $\mathcal{N}$, called blocks, such that the number r of blocks containing i in $\mathcal{N}$ is independent of i, and the number λ of blocks containing given distinct points i and j in $\mathcal{N}$ is also independent of the choices. Here n (the number of elements of $\mathcal{N}$), b (the number of blocks), k, r, and λ are the parameters of the design. In brief:

1. n – number of elements of $\mathcal{N}$;

2. b – number of blocks;

3. r – number of blocks containing a given element of $\mathcal{N}$;

4. k – number of elements in a block;

5. λ – number of blocks containing 2 (or more generally t) elements.

The design is called a (n, k, λ)-design or a (n, b, r, k, λ)-design.

Example 2. ***Block design constructions***
Let $k = 3, n = 7, d_r = 2$. Define 7 identifiers (ID) of reduced row echelon forms (blocks) as follows:

$$B_1^\top = \begin{bmatrix}1\\2\\3\end{bmatrix},\ B_2^\top = \begin{bmatrix}1\\4\\5\end{bmatrix},\ B_3^\top = \begin{bmatrix}1\\6\\7\end{bmatrix},\ B_4^\top = \begin{bmatrix}2\\4\\6\end{bmatrix},\ B_5^\top = \begin{bmatrix}2\\5\\7\end{bmatrix},\ B_6^\top = \begin{bmatrix}3\\4\\7\end{bmatrix},\ B_7^\top = \begin{bmatrix}3\\5\\6\end{bmatrix}.$$

Each block meets another one in exactly $\lambda = 1$ point. Thus we have a balanced incomplete block design with parameters $n = b = 7,\ r = k = 3,\ \lambda = 1$.
The number of matrices in each component is $256, 16, 1, 16, 2, 4, 2$, respectively. The whole code of subspace distance 4 contains 297 elements.

In general, blocks of a block design are used as identifiers of reduced row echelon forms.

3.4 Comparison with other codes

To compare our results with known results, we have borrowed the table from (Gadouleau M., and Yan Z.: Construction and Covering Properties of Constant-Dimension Codes. Proc. of the 2009 IEEE International Symposium on Information Theory (ISIT 2009), pp. 2221-2225. Nice, France,) and add one extra column with cardinalities of new multicomponent codes based on block designs.

Cardinalities of SKK codes, Skachek codes, Gadouleau–Yan codes, and multicomponent codes in $\mathcal{P}(10)$ for $2 \le k \le 5$

k	d_{sub}	*SKK*	*Skachek*	*Gadouleau − −Yan*	**Multicomp**
2	4	256	340	320	**341**
3	4	16384	16640	17408	**18441**
	6	128	144	144	**145**
4	4	262144	262144	278544	**283045**
	6	4096	4096	4112	**4113**
	8	64	64	65	**65**
5	4	1048576	1048576	1056769	**1060873**
	6	32768	32768	32769	**32801**
	8	1024	1024	1025	**1025**
	10	32	32	33	**33**

It follows from the table that multicomponent codes at least as good as other constructions, sometimes better.

4 Conclusion

A family of multicomponent network codes based on block designs is presented. The parameters are chosen under the following condition: any component subspace distance is equal to a subspace distance between components. These codes are at least as good as other constructions (sometimes better).

References

[1] Silva D., Kschischang F.R., and Koetter R.: A Rank-Metric Approach to Error Control in Random Network Coding. IEEE Trans. On Inform. Theory. Vol. 54., No. 9, pp. 3951-3967 (2008)

[2] Gabidulin E., Bossert M.: Codes for Network Coding. In: Proc. of the 2008 IEEE International Symposium on Information Theory (ISIT 2008), pp. 867-870. Toronto, ON, Canada, 6-11 July (2008)

[3] Gabidulin E.M., and Bossert M.: A Family of Algebraic Codes for Network Coding. Probl. Inform. Transm. Vol. 45. No. 4, pp. 54–68 (2009)

[4] Skachek V.: Recursive Code Construction for Random Networks. IEEE Trans. On Inform. Theory. V. 56. No. 3, pp. 1378-1382 (2010)

[5] Gadouleau M., and Yan Z.: Construction and Covering Properties of Constant-Dimension Codes. In: Proc. of the 2009 IEEE International Symposium on Information Theory (ISIT 2009), pp. 2221-2225. Nice, France, 24-29 June (2009)

[6] Etzion T., and Silberstein N.: Error-Correcting Codes in Projective Spaces Via Rank-Metric Codes and Ferrers Diagrams. IEEE Trans. on Inform. Theory. V. 55. No. 7, pp. 29092919 (2009).

[7] Wang H. , Xing C., and Safavi-Naini R.: Linear authentication codes: bounds and constructions. IEEE Trans. On Inform. Theory. V. 49. No. 4, pp. 866873 (2003).