6th International Conference on
Combinatorics, Cryptography, Computer Science and Computing
November. 17-18, 2021

Random network coding via new orbit codes based on tensor structures

Soleyman Askary
Nader Biranvand
Farrokh Shirjian[1]
Imam Ali Officers' University, Tehran, Iran

Abstract

Orbit codes, as special constant dimension codes, have attracted much attention due to their applications for error correction in random network coding. They arise as orbits of a subspace of $\mathbb{F}_q^n$ under the action of some subgroup of the finite general linear group $\mathrm{GL}_n(q)$. In this paper, We introduce the notion of tensor product operation for subspace codes and determine the parameters of such product codes. Furthermore, it is shown that the tensor product of two subspace codes, one of them being a partial spread, is also a partial spread. The properties wreathed tensor products of groups are then employed to select certain types of subspaces and their stabilizers, thereby providing a systematic way of constructing orbit codes with optimum parameters. The constructions presented in this paper improve significantly the constructions already obtained in [8] and [7].

Keywords: Random linear network coding, Algebraic coding theory, non-Abelian orbit code, Linear groups.
Mathematics Subject Classification [2010]: 11T71, 94B27, 94A60

1 Introduction

Throughput enhancement is one of the major research challenges in wireless communication systems. It is foreseen that network throughput requirements for wireless networks in the future will be much higher than nowadays. The frequency band is a limited resource, therefore sophisticated solutions are required to maximize the delivered data on this limited spectra. Random linear network coding, introduced in [1], is used to increase the information throughput by allowing the random linear combination of packets within a network; that is, each internal node of the network transmits random linear combinations of the received packets to adjacent nodes. Due the encoding method the receivers are able to reconstruct the original packets that have been injected into the network at its sources. Although this method is very effective but it is highly sensitive to the error propagation. Trying to solve this problem, Kötter and Kschischang [10] proposed a mathematical description of random network coding, called subspace codes, by considering messages as subspaces of some fixed vector space over a finite field. Te subspace codes have been extensively investigated in the literature, see for instance [4], [6].

An important class of subspace codes are orbit codes which are constant dimension codes that arise as an orbit of a subspace under the action of a subgroup of the general linear group. Orbit codes in which the intersection of any two distinct codewords is zero are called partial spreads. Orbit codes were first introduced in the area of network coding in [12], where the authors showed how the Reed-Solomon type codes introduced in [10] as well as the spread codes described in [11], can be seen as special instances of orbit codes. Orbit codes can be classified according to the groups used to construct the orbits. the authors in [8] and

[1] speaker

[5] recently considered Abelian non-cyclic orbit codes; that is, orbit codes which are generated by Abelian non-cyclic subgroups of the general linear group. Indeed, they presented a construction of an Abelian non-cyclic orbit code of length n over $\mathbb{F}_q$ with cardinality $q(q-1)$ and the minimum subspace distance $2k$, see [8]. Furthermore, they put forward the following open question as one of the main future research directions:

Question. [8] Find constructions of good (Abelian) non-cyclic orbit codes in the sense that increase the cardinality without decreasing the distance.

In this paper we answer the above question by giving new constructions of non-cyclic orbit codes with optimum parameters. Meanwhile, we introduce the notion of tensor product operation of subspace codes and prove the main properties (including the length, dimension, minimum distance etc.) of such product codes. Among other things, we prove that the tensor product of two subspace codes (resp. orbit codes), one of them being a partial spread, is always a partial spread. This gives a new way to construct new larger-size orbit codes from the known ones. We then apply this result to construct non-cyclic orbit codes which are partial spreads and they have large sizes.

We recall that a subspace code $\mathcal{C}$ of length n is simply a collection of subspaces in $\mathbb{F}_q^n$. The code is called a constant dimension code if all subspaces have the same dimension.

Definition 1.1. The subspace code $\mathcal{C}$ is called a partial spread of $\mathbb{F}_q^n$, if $\mathbf{U} \cap \mathbf{W} = 0$ for all $\mathbf{U}, \mathbf{W} \in \mathcal{C}$ such that $\mathbf{U} \neq \mathbf{W}$.

The minimum distance of a subspace code $\mathcal{C}$ is defined as

$$d(\mathcal{C}) = min\{d(\mathbf{U}, \mathbf{W}) : \mathbf{U}, \mathbf{W} \in \mathcal{C}, \mathbf{U} \neq \mathbf{W}\},$$

where

$$d(\mathbf{U}, \mathbf{W}) = dim(\mathbf{U}) + dim(\mathbf{W}) - 2dim(\mathbf{U} \cap \mathbf{W})$$

Consequently, if $\mathcal{C}$ is a constant dimension code of dimension k, then

$$d(\mathcal{C}) \leq min\{2k, 2(n-k)\}.$$

A constant dimension code of length n, dimension k and cardinality M will be called an $[n, M; k]$-code, and it is a $[n, M, d; k]$-code if its minimum distance is d.

Definition 1.2. [12] Let $\mathbf{G}$ be a subgroup of $\mathrm{GL}_n(q)$ and $\mathbf{U} \in \mathcal{G}_q(k, n)$. The orbit of the action of $\mathbf{G}$ on $\mathbf{U}$, which we denoted by $\mathcal{C}$, is called the *orbit code* generated by $\mathbf{G}$. Indeed, $\mathcal{C} = \{A\mathbf{U} : A \in \mathbf{G}\}$. Furthermore, the code $\mathcal{C}$ is called a cyclic (resp. Abelian, non-Abelian) orbit code, if the group $\mathbf{G}$ is cyclic (resp. Abelian, non-Abelian).

Definition 1.3. For $\mathcal{C}$ being an orbit code generated by $\mathbf{G}$ and $\mathbf{U} \in \mathcal{C}$, the stabilizer $Stab_{\mathbf{G}}(\mathbf{U})$ of $\mathbf{U}$ in $\mathbf{G}$ is defined as

$$Stab_{\mathbf{G}}(\mathbf{U}) = \{A \in \mathbf{G} : A\mathbf{U} = \mathbf{U}\}.$$

Lemma 1.4. *[9] Let $\mathbf{U} \in \mathcal{G}_q(k, n)$ and $\mathbf{G} \leq \mathrm{GL}_n(q)$ and $\mathcal{C} = \mathbf{G}.\mathbf{U}$. Then*

1. *the code $\mathcal{C}$ has the size $|\mathcal{C}| = \frac{|\mathbf{G}|}{|Stab_{\mathbf{G}}(\mathbf{U})|}$.*
2. *the minimum distance of the code $\mathcal{C}$ may obtain by the following formula:*

$$d(\mathcal{C}) = min\{dim(\mathbf{U}, A.\mathbf{U}) : A \in \mathbf{G} \text{ is a coset representative of } \mathrm{Stab}_{\mathbf{G}}(\mathbf{U}) \text{ in } \mathbf{G}\}.$$

2 Main Results

In this section we introduce the notion of tensor product of subspace codes and prove some of the main properties of tensor products of subspace codes. We then apply this to introduce some new ways to construct new orbit codes from the known orbit codes. Moreover, the proposed orbit codes obtain in this way are shown to be partial spreads.

Definition 2.1. [2, Definition 4.2] Let $\mathcal{C}_1 \subseteq \mathcal{G}_q(k_1, n_1)$ and $\mathcal{C}_2 \subseteq \mathcal{G}_q(k_2, n_2)$ be two subspace codes. The tensor product of $\mathcal{C}_1$ and $\mathcal{C}_2$, denoted by $\mathcal{C}_1 \otimes \mathcal{C}_2$, is defined as

$$\mathcal{C}_1 \otimes \mathcal{C}_2 = \{(\mathbf{U} \otimes \mathbf{W}) : \mathbf{U} \in \mathcal{C}_1, \mathbf{W} \in \mathcal{C}_2\}.$$

Theorem 2.2. *[2, Theorem 4.3] For $i = 1, 2$, let $\mathcal{C}_i \subseteq \mathcal{G}_q(k_i, n_i)$ is a $[n_i, M_i, d_i; k_i]$-subspace code. Then $\mathcal{C} = \mathcal{C}_1 \otimes \mathcal{C}_2$ is also a subspace code with parameters $[n_1 n_2, M_1 M_2, d; k_1 k_2]$ where $d = 2(k_1 k_2 - d_1^{max} d_2^{max})$ in which $d_i^{max} = max\{dim(\mathbf{U} \cap \mathbf{W}) : \mathbf{U}, \mathbf{W} \in \mathcal{C}_i\}$.*

In [7], the authors introduced the sum operation of subspace codes as

$$\mathcal{C}_1 + \mathcal{C}_2 := \{\mathbf{U} + \mathbf{W} : \mathbf{U} \in \mathcal{C}_1, \mathbf{W} \in \mathcal{C}_2\}.$$

However, it is rarely that the sum of two partial spreads be a partial spread again. The following example illustrates this fact.

Example 2.3. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two subspace codes which are partial spreads. Moreover, let $\mathbf{U}_1 \in \mathcal{C}_1$ and $\mathbf{W}_1, \mathbf{W}_2 \in \mathcal{C}_2$. We then have

$$\mathbf{U}_1 + \mathbf{W}_1 \in \mathcal{C}_1 + \mathcal{C}_2,$$

and

$$\mathbf{U}_1 + \mathbf{W}_2 \in \mathcal{C}_1 + \mathcal{C}_2,$$

with $\mathbf{U}_1 \subseteq (\mathbf{U}_1 + \mathbf{W}_1) \cap (\mathbf{U}_1 + \mathbf{W}_2)$. So the two codewords have non-trivial intersection. This in turn implies that $\mathcal{C}_1 + \mathcal{C}_2$ is not a partial spread.

In contrast to the sum operation of codes introduced in [7], we show that the tensor product operation of two subspace codes, with one of them being a partial spread, is always a partial spread.

Theorem 2.4. *[2, Theorem 4.5] For $i = 1, 2$, let $\mathcal{C}_i \in \mathcal{G}(k_i, n_i)$ be two subspace codes one of them being a partial spread. Then $\mathcal{C}_1 \otimes \mathcal{C}_2$ is also a partial spread with size $|\mathcal{C}_1| \times |\mathcal{C}_2|$.*

Given a partial spread orbit code of dimension k, the tensor operation allow us to construct further partial spreads of dimension k with larger sizes. It is deduced from the Aschbacher theorem that if $\mathbf{V} = \mathbf{U} \otimes \cdots \otimes \mathbf{U}$ is a tensor product decomposition of a n-dimensional vector space $\mathbf{V}$ into m copies of a k-dimensional subspace $\mathbf{U}$, then the stabilizer of $\mathbf{V}$ is of the form $\mathrm{GL}_k(q) \wr S_m$ where $n = k^m$. In the sequel we give another method to construct large orbit codes from the smaller known ones. The special feature of this method is that it increases the code size without changing the minimum distance and hence provides a new approach to construct large partial spreads. This answers the question posed in [8].

Theorem 2.5. *[3, Theorem 4.8] Let $\mathbf{V} = \mathbf{U} \otimes \cdots \otimes \mathbf{U}$ be a tensor decomposition into m spaces $\mathbf{U}$ of dimension k, where $k^m = n$, $k \geq m$ and let $\mathbf{W}_1 \leq \mathbf{U}$ be of dimension $k_1 \leq k$ such that the orbit code $\mathcal{C} = G.\mathbf{W}_1$ has parameters $[k, r, d; k_1]$ for some subgroup $G \leq \mathrm{GL}_k(q)$. Assume furthermore that $v_i's$, with $2 \leq i \leq m$, are pairwise linearly independent vectors of $\mathbf{U}$ such that the corresponding orbit codes $\mathcal{C}_i = \mathrm{GL}_k(q).\langle v_i \rangle$ have parameters $[k, (q^k - 1)/(q - 1), 2; 1]$ for $2 \leq i \leq m$. Then the action of the wreathed tensor product group $G \circ (\mathrm{GL}_k(q) \wr S_{m-1})$ on the tensor subspace $\mathbf{W}_1 \otimes \langle v_2 \rangle \otimes \cdots \otimes \langle v_m \rangle$ induces a non-Abelian orbit code $\mathcal{D}$ with parameters $[n, r(\frac{q^k-1}{q-1})^{m-1}, d; k_1]$.*

Note that for any composite number $n = k^m$, the code of length n constructed via the above methods is larger than the construction obtained in [8] which was of length n and of size $q(q - 1)$.

References

[1] R. Ahlswede, N. Cai, S.-Y.R. Li, R.W. Yeung, Network information flow. *IEEE Trans. Inf. Theory* 46(4), (2000), 1204–1216.

[2] S. Askary, N. Biranvand, F. Shirjian, New constructions of orbit codes based on tensor structures, submitted for publication.

[3] S. Askary, N. Biranvand, F. Shirjian, New constructions of orbit codes based on imprimitive wreath products and wreathed tensor products, submitted for publication.

[4] F. Bardestani, A. Iranmanesh, Cyclic orbit codes with the normalizer of a Singer subgroup. *J. Sci. Islamic Republic Iran* 26(1), (2015) 49–55.

[5] G. Bastos, R.P. Junior, M. Guerreiro, Abelian Noncyclic Orbit Codes and Multishot Subspace Codes. *Adv. Math. Commun.*, 14, (2020) 631–650.

[6] E. Ben-Sasson, T. Etzion, A. Gabizon, N. Raviv, Subspace polynomials and cyclic subspace codes. *IEEE Trans. Inf. Theory* 62(3), (2016) 1157–1165 .

[7] Sd. Chen, Jy. Liang, New Constructions of Orbit Codes Based on the Operations of Orbit Codes. *Acta Math. Appl. Sin. Engl. Ser.* 36, (2020) 803–815.

[8] J-J. Climent, V. Requena, X. Soler-Escriva, A construction of Abelian non-cyclic orbit codes. *Cryptogr. Commun.* 11, (2019) 839–852.

[9] H. Gluesing-Luerssen, K. Morrison, C. Troha, Cyclic orbit codes and stabilizer subfields. *Adv. Math. Commun.* 9(2), (2015) 177–197.

[10] R. Kotter, F.R. Kschischang, Coding for errors and erasures in random network coding. *IEEE Trans. Inf. Theory* 54(8), (2008) 3579–3591.

[11] F. Manganiello, E. Gorla, J. Rosenthal, Spread codes and spread decoding in network coding. In: *Proceedings of the 2008 IEEE international symposium on information theory (ISIT 2008)*, pp. 881-885, Toronto, Canada. IEEE (2008).

[12] A.-L. Trautmann, F. Manganiello, J. Rosenthal, Orbit codes – a new concept in the area of network coding. In: *Proceedings of the 2010 IEEE information theory workshop (ITW 2010)*, Dublin, Ireland. IEEE (2010).

Email: s.asgary95@gmail.com
Email: nabiranvand@gmail.com
Email: farrokh.shirjian@modares.ac.ir