Journal of Sciences, Islamic Republic of Iran 26(1): 49 - 55 (2015) http://jsciences.ut.ac.ir
University of Tehran, ISSN 1016-1104

Cyclic Orbit Codes with the Normalizer of a Singer Subgroup

F. Bardestani and A. Iranmanesh*

Department of pure Mathematics, Faculty of Mathematical Sciences, Tarbiat Modares University, Tehran, Islamic Republic of Iran

Received: 16 November 2014 / Revised: 3 January 2015 / Accepted: 17 February 2015

Abstract

An algebraic construction for constant dimension subspace codes is called orbit code. It arises as the orbits under the action of a subgroup of the general linear group on subspaces in an ambient space. In particular orbit codes of a Singer subgroup of the general linear group has investigated recently. In this paper, we consider the normalizer of a Singer subgroup of the general linear group and its orbit codes. Several properties of these codes are considered.

Key words: Linear network coding; Constant dimension codes; Group action; Orbit codes.

* Corresponding author:Tel: +982182883493; Fax:+982188009730; Email:iranmana@modares.ac.ir

Introduction

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 i.e., the middle nodes combine packets linearly, where they choose the coefficients for linear combinations randomly within a finite field. 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. In 2008, Kötter and Kschischang developed an algebraic approach to overcome this deficiency [9]. They suggested an error correcting network code as a family of subspaces of an ambient space F^n. This pioneering article initiate intensive research effort on subspace codes, particularly for construction of large error-correcting codes with efficient encoding and decoding algorithms. In 2009, Etzion and Silberstein presented a construction of subspace codes with large distance and cardinality which is based on rank-metric codes [4]. In [5], Etzion and Vardy introduced the concept of a cyclic subspace code and present several optimal cyclic subspace codes.

In [13], Trautmann et al., used group action and present an algebraic construction for subspace codes named orbit code. Especially by considering the group action of a certain group (Singer subgroup), they presented an algebraic construction for cyclic subspace codes.

In [6], Gluesing-Luerssen et al., introduced the notion of Stabilizer subfield and investigate the cardinality and distance of the orbit codes of the Singer subgroup.

While the orbit codes of a Singer subgroup are not large but taking the unions of them is a nice idea to obtain large cyclic subspace codes for a given minimum distance. The normalizer of a Singer subgroup is a candidate to have an algebraic structure for some certain unions of the orbits of the Singer subgroup.

In 2013, Braun et al., presented a nontrivial q-analog of Steiner systems, which also form an optimal cyclic code. This code has the normalizer of the Singer subgroup as its automorphism group [2].

In this paper, we will study the orbits of the normalizer of a Singer subgroup, which are a class of cyclic subspace codes. The structure of the orbits of this normalizer is closely related to the orbits of the Singer subgroup.

Notation and preliminary results

A subspace code of length n is defined as a collection of subspaces in $\mathrm{F}_q{}^n$, where F_q is a finite field. If all the subspaces have the same dimension k the code is called constant dimension code. The subspace distance between two subspaces is defined as follows [9]:

$$d_s(\mathrm{U},\mathrm{V}) := \dim(\mathrm{U}) + \dim(\mathrm{V}) - 2\dim(\mathrm{U} \cap \mathrm{V})$$

Therefore, the minimum distance of a code C is defined as:

$$d_{\min}(\mathrm{C}) := \min\{d_s(\mathrm{U},\mathrm{V}) \mid \mathrm{U},\mathrm{V} \in \mathrm{C}, \mathrm{U} \neq \mathrm{V}\}.$$

As a consequence, if C is a constant dimension code, then $\mathrm{d}_{\min}\ \mathrm{C}) \leq 2k$.

The dual of the subspace code C is denoted by $\mathrm{C}^{\perp}$ and is defined as $\mathrm{C}^{\perp} := \{\mathrm{U}^{\perp} \mid \mathrm{U} \in \mathrm{C}\}$. Since $d_s(\mathrm{U}^{\perp},\mathrm{V}^{\perp}) = d_s(\mathrm{U},\mathrm{V})$,

then $d_{\min}(\mathrm{C}) = d_{\min}\ \mathrm{C}^{\perp}$ [13].

The set of all k-dimensional subspaces of $\mathrm{F}_q{}^n$ is called Grassmannian, denoted by $\mathrm{G}(k,n)$. It is well known that:

$$|\mathrm{G}(k,n)| = \begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{\prod_{i=n-k+1}^{i=n}(q^i-1)}{\prod_{i=1}^{i=k}(q^i-1)}.$$

Let $\mathrm{GL}(n,q)$ be the general linear group , an orbit code, is defined as the orbit of the natural action of a subgroup G of $\mathrm{GL}(n,q)$ on the Grassmannian [13]. More precisely let $U \in Mat_{k\times n}(\mathrm{F}_q)$ be a full-rank matrix such that $\mathrm{U} := \mathrm{rowspace}(U)$ and g be an element of G . We can define, $\mathrm{U}.g := \mathrm{rowspace}(Ug)$, then an orbit code by G and starting point U is denoted by $Orbit_G(\mathrm{U})$, so $Orbit_G(\mathrm{U}) := \{\mathrm{U}.g \mid g \in G\}$. Let $\mathrm{Stab}_G(\mathrm{U}) := \{g \in G \mid \mathrm{U}.g = \mathrm{U}\}$ be the stabilizer of the action, then simple facts in group theory leads that $|Orbit_G(\mathrm{U})| = \dfrac{|G|}{|\mathrm{Stab}_G(\mathrm{U})|}$

and since $d_s(\mathrm{U}g, \mathrm{U}g') = d_s(\mathrm{U}, \mathrm{U}g'g^{-1})$,

then:

$$d_{\min}(Orbit_G(\mathrm{U})) := \min\{d_s(\mathrm{U},\mathrm{U}g)\,|\, g\in G\setminus \mathrm{Stab}_G(\mathrm{U})\}.$$

Let C_1 and C_2 be two subspace codes of length n such that $\mathrm{C}_1=\phi(\mathrm{C}_2)$ where $\phi\in \mathrm{GL}(n,q)$, then C_1 and C_2 are called linearly isometric or simply isometric. It is easy to see that isometric codes have the same minimum distance and cardinality [13]. Since orbit codes are a class of subspace codes, the isometry between them is defined in the same way. In [10], it is proved that two conjugate subgroups lead isometric orbit codes. For more information about isometry in subspace codes, the reader is refered to [12].

If $\mathrm{C}=Orbit_G(\mathrm{U})$, we say C is a code with parameters $[n,k,|\mathrm{C}|,d_{\min}(\mathrm{C})]$, we may omit $|\mathrm{C}|$, where the cardinality is not the point. With these parameters it is easy to see that the dual code $\mathrm{C}^{\perp}$ is an $[n,n-k,|\mathrm{C}|,d_{\min}(\mathrm{C})]$ orbit code. The related orbit code to a cyclic subgroup of $\mathrm{GL}(n,q)$ is called a cyclic orbit code.

An element of order q^n-1 in $\mathrm{GL}(n,q)$ is called a Singer cycle. Since the multiplicative group of the field F_{q^n} is cyclic of order q^n-1 and we can take its generator as an element of $\mathrm{GL}(n,q)$, so for every n and every q there is a Singer cycle in $\mathrm{GL}(n,q)$. A cyclic group generated by a Singer cycle called a Singer subgroup. There are several ways to describe a Singer subgroup, for example, let $p(x)$ be a primitive polynomial of degree n over F_q, and M_p be its companion matrix, then $\langle M_p\rangle$ is a Singer subgroup of $\mathrm{GL}(n,q)$ [13].

We recall that if $p(x)=p_0+p_1x+...p_{n-1}x^{n-1}$, then

$$M_p=\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ -p_0 & -p_1 & \cdots & -p_{n-1} \end{pmatrix}.$$

Since the extension field F_{q^n} is a vector space of dimension n over F_q, we may consider F_{q^n}. as the vector space. Fix α as a primitive element of F_{q^n}, then $C_\alpha=\langle\alpha\rangle=\mathrm{F}^*_{q^n}$ is a Singer subgroup of $\mathrm{GL}(n,q)$. Since all Singer subgroups are conjugate, in order to investigate orbits of a Singer subgroup, without loosing generality we investigate the orbits of C_α.

A collection of subspaces with this property that if $\{0,\alpha^{x_i}\ |i=1,..2^k-1\}$ is a codeword, then $\{0,\alpha^{x_i+1}\ |i=1,..2^k-1\}$ is also a codeword which is called a cyclic subspace code [5]. Whence one of the several interesting properties for $Orbit_{C_\alpha}(\mathrm{U})$, is that every $\bigcup Orbit_{C_\alpha}(\mathrm{U}_t)$ is a cyclic subspace code.

According to the definition of isometric subspace codes, the auotomorphism group of $Orbit_{C_\alpha}(\mathrm{U})$ is contained C_α. Recall that the Frobenius automorphism $\sigma:\mathrm{F}_{q^n}\to\mathrm{F}_{q^n}$ is defined by $\sigma(x):=x^q$ for all $x\in\mathrm{F}_{q^n}$. We mention, the following example which shows, in general $Aut(Orbit_{C_\alpha}(\mathrm{U}))\neq C_\alpha$.

Example 1.1 Consider primitive polynomial $p(x)=x^7+x+1$. Let $\alpha\in\mathrm{F}_{2^7}$ be a root of $p(x)$ and $\mathrm{U}=\{0,1,\alpha^8,\alpha^{24},\alpha^{56},\alpha^{120},\alpha^{121},\alpha^{123}\}$ be a subspace of F_{2^7}, then $\mathrm{U}\sigma=\mathrm{U}\alpha^{-8}$, so $\sigma\in Aut(Orbit_{C_\alpha}(\mathrm{U}))$, while $\sigma\notin C_\alpha$.

In the next section, we will focus on the normalizer of a Singer subgroup and the related orbits.

Results and Discussion

Let G be a subgroup of $\mathrm{GL}(n,q)$, the normalizer of G in $\mathrm{GL}(n,q)$ is the set of all elements in $\mathrm{GL}(n,q)$ such that commute with G . That is:

$$N_{\mathrm{GL}}(G):=\{n\in\mathrm{GL}(n,q)\,|nG=Gn\}.$$

Let $n\in N_{\mathrm{GL}}(G)$, then it is well known that $\langle G,n\rangle=G.\langle n\rangle$ is a subgroup of $\mathrm{GL}(n,q)$. It is straightforward to see that :

$$Orbit_{G.\langle n\rangle}(\mathrm{U})=\bigcup_{i=0}^{i=|n|} Orbit_G(\mathrm{U}n^i).$$

By this method, if we consider $G=C_\alpha$, then we obtain a union of cyclic subspace codes as an orbit code. Through the paper, we denote the normalizer of the

Singer subgroup C_α in $\mathrm{GL}(n,q)$ by N_α. Galois group $Gal(\mathrm{F}_{q^n}/\mathrm{F}_q)$ is a cyclic group which is generated by the Frobenius automorphism σ of order n. We mention a well known construction for N_α as a semidirect product [7]. We recall the definition of a semidirect product as the following:

Definition 2.1. Let H and K be two arbitrary groups and $\varphi: H \to K$ be a homomorphism (denote the image of every h under φ by φ_h). On the Cartesian product $H \times K$ define, the following operation:

$$(h_1, \mathrm{k}_1)(h_2, k_2) = (h_1 h_2, (k_1 \varphi_{h_2}) k_2).$$

The set $H \times K$ with this operation is a group, which is called the semidirect product of H and K, denoted by H **ã** K **.**

Theorem 2.2. [7] N_α has order $n(q^n - 1)$ and is isomorphic to the semidirect product of the Galois group $Gal(\mathrm{F}_{q^n}/\mathrm{F}_q)$ and C_α.

As a consequence of Theorem 2.2, $N_\alpha = C_\alpha . \langle \sigma \rangle$ and $Orbit_{N_\alpha}(\mathrm{U}) = \bigcup_{i=0}^{s} Orbit_{C_\alpha}(\mathrm{U}\sigma^i)$, where s is the smallest integer such that $Orbit_{C_\alpha}(\mathrm{U}) = Orbit_{C_\alpha}(\mathrm{U}\sigma^s)$. It turns that the orbit of N_α is the union of cyclic subspace codes and so is cyclic too.

We mention two other important results which can be found in [2] and [3].

Lemma 2.3. [2; Lemma 4] The normalizer N_α of a Singer subgroup is self-normalizing in $\mathrm{GL}(n,q)$, that is $N_{\mathrm{GL}}(N_\alpha) = N_\alpha$.

The following theorem mentions when the normalizer of a Singer subgroup is a maximal subgroup

Theorem 2.4. [3] Let n be an odd prime. Then the normalizer of a Singer subgroup is a maximal subgroup of $\mathrm{GL}(n,q)$.

As a consequence of Theorem 2.4, if $n > 2$ is a prime, then $Aut(Orbit_{N_\alpha}(\mathrm{U})) = N_\alpha$ and we have the following result:

Theorem 2.5. Suppose that $n \geq 3$ is a prime. Let N_α be the normalizer of a Singer subgroup in $\mathrm{GL}(n,q)$. Then distinct orbit codes by N_α are nonisomorphic.

Proof. Let $Orbit_{N_\alpha}(\mathrm{U})$ and $Orbit_{N_\alpha}(\mathrm{U}')$ be two distinct orbit codes, and there is $g \in \mathrm{GL}(n,q)$ such that $Orbit_{N_\alpha}(\mathrm{U}) = (Orbit_{N_\alpha}(\mathrm{U}'))g.$ Then for every $n \in N_\alpha$, we have:

$$(Orbit_{N_\alpha}(\mathrm{U}'))gng^{-1} = (Orbit_{N_\alpha}(\mathrm{U}))ng^{-1} = (Orbit_{N_\alpha}(\mathrm{U}))g^{-1} = Orbit_{N_\alpha}(\mathrm{U}'),$$

that is $gng^{-1} \in N_\alpha$ and hence $g \in N_{\mathrm{GL}}(N_\alpha) = N_\alpha.$ It follows that $Orbit_{N_\alpha}(\mathrm{U}) = Orbit_{N_\alpha}(\mathrm{U}')$, which is a contradiction.

Remark 2.6. Let U be an arbitrary k -dimensional subspace of F_{q^n} according to [6], there exist a k -dimensional subspace U' such that $1 \in \mathrm{U}'$ and $Orbit_{C_\alpha}(\mathrm{U}) = Orbit_{C_\alpha}(\mathrm{U}').$ Then

$$Orbit_{C_\alpha}(\mathrm{U}\sigma^i) = (Orbit_{C_\alpha}(\mathrm{U}))\sigma^i \Rightarrow Orbit_{C_\alpha}(\mathrm{U}\sigma^i) = Orbit_{C_\alpha}(\mathrm{U}'\sigma^i)$$

So $Orbit_{N_\alpha}\left(\mathrm{U}\right) = Orbit_{N_\alpha}(\mathrm{U}')$. Therefore we can restrict ourselves to the subspaces U that contain the identity $1 \in \mathrm{F}_{q^n}$.

According to the above remark, if $\mathrm{U} \neq \mathrm{U}\sigma$, then since $\sigma(1) = 1$, $d_{\min}(Orbit_{N_\alpha}(\mathrm{U})) \leq 2(k-1).$

A spread code in $\mathrm{G}(k,n)$ is a set of subspaces of dimension k such that they pairwise intersect only trivially and they cover the whole vector space $\mathrm{F}_q{}^n$. Spread code is optimal since its minimum distance is $2k$ and its cardinality is $\dfrac{q^n - 1}{q^k - 1}$ [12]. By Corollary 3.8 in [6], an $Orbit_{C_\alpha}(\mathrm{U})$ is a spread code if and only if $\mathrm{U} \equiv \mathrm{F}_{q^k}$. Then since $\sigma(\mathrm{F}_{q^k}) = \mathrm{F}_{q^k}$, $Orbit_{N_\alpha}(\mathrm{F}_{q^k}) = Orbit_{C_\alpha}(\mathrm{F}_{q^k})$. Therefore an interesting case is to focus on orbit codes by N_α with parameters, $\left[n, k, 2\left(k-1\right)\right]$.

In the following examples, we mention several orbits $Orbit_{N_\alpha}(\mathrm{U})$ with parameters $[n,k,2(k-1)]$, where $|Orbit_{N_\alpha}(\mathrm{U})| \neq |Orbit_{C_\alpha}(\mathrm{U})|$:

Example 2.7. Let $\mathrm{U}=\langle 1,\alpha^2,\alpha^{19}\rangle$ be a subspace of F_{2^n} where $n\in\{12\cdots 20\}$. Then $Orbit_{N_\alpha}(\mathrm{U})$ is a code with parameters $[n,3,n(2^n-1),4]$.

Example 2.8.

1) Let $\mathrm{U}=\langle 1,\alpha^5,\alpha^{93}\rangle$, then $Orbit_{N_\alpha}(\mathrm{U})$ is a $[8,3,2(2^8-1),4]-$code.

2) Let $\mathrm{U}=\langle 1,\alpha^1,\alpha^{47}\rangle$, then $Orbit_{N_\alpha}(\mathrm{U})$ is a $[9,3,9(2^9-1),4]$-code.

3) Let $\mathrm{U}=\langle 1,\alpha,\alpha^7,\alpha^{87}\rangle$, then $Orbit_{N_\alpha}(\mathrm{U})$ is a $[13,4,13(2^{13}-1),6]$-code.

4) Let $\mathrm{U}=\langle 1,\alpha^5,\alpha^7,\alpha^{87}\rangle$, then $Orbit_{N_\alpha}(\mathrm{U})$ is a $[17,4,17(2^{17}-1),6]$-code.

Remark 2.9. Let r divides n and F_{q^r} be the largest subfield in F_{q^n} such that U is a vector space over F_{q^r}. In [6], the authors called F_{q^r}, the best friend for U. Consider $\mathrm{U}=\overset{t-1}{\underset{i=0}{\oplus}}\alpha^{il}\mathrm{F}_{q^r}$, then $d_{\min}(Orbit_{C_\alpha}(\mathrm{U}))=2r$ [6]. In fact this result is based on this property that for every α^J, $\mathrm{U}\alpha^J$ is a vector sapcae over F_{q^r} too. It is obvious that this is not true for every element of $\mathrm{GL}(n,q)$. However, since $(\overset{t-1}{\underset{i=0}{\oplus}}\alpha^{il}\mathrm{F}_{q^r})\sigma=\overset{t-1}{\underset{i=0}{\oplus}}\alpha^{ilq}\mathrm{F}_{q^r}$, for every $g\in N_\alpha$, $\mathrm{U}g$ is a vector space over F_{q^r} therefore we have proved the following theorem:

Theorem 2.10. Let r divides n and $\mathrm{U}=\overset{t-1}{\underset{i=0}{\oplus}}\alpha^{il}\mathrm{F}_{q^r}$ be a nontrivial subspace of F_{q^n}, where $l<\frac{q^n-1}{q^r-1}$. If $\mathrm{U}\neq\mathrm{F}_{q^n}$, then $d_{\min}(Orbit_{N_\alpha}(\mathrm{U}))=2r$.

Example 2.11. Let $n=10$, $\mathrm{U}_1=\mathrm{F}_{2^2}\oplus\alpha^3\mathrm{F}_{2^2}$ and $\mathrm{U}_2=\mathrm{F}_{2^2}\oplus\alpha^5\mathrm{F}_{2^2}$, then for $i=1,2$ we have, $d_{\min}(Orbit_{N_\alpha}(\mathrm{U}_i))=4$. Also $|Orbit_{N_\alpha}(\mathrm{U}_1)|=2\frac{2^{10}-1}{2^2-1}$ and $|Orbit_{N_\alpha}(\mathrm{U}_2)|=10\frac{2^{10}-1}{2^2-1}$.

In [6], the authors proved that when n is a prime, $\mathrm{Stab}_{C_\alpha}(\mathrm{U})=\mathrm{F}_q^*$ and so $|Orbit_{C_\alpha}(\mathrm{U})|=\frac{q^n-1}{q-1}$. Hence we have the following result:

Lemma 2.12. If n is a prime, then $Orbit_{\mathrm{N}_\alpha}(\mathrm{U})=Orbit_{C_\alpha}(\mathrm{U})$. or $|Orbit_{N_\alpha}(\mathrm{U})|=n(\frac{q^n-1}{q-1})$.

Let $\mathrm{F}_q=\mathrm{F}_2$, if $n=5$ and $k=2$, then $d_{\min}(Orbit_{N_\alpha}(\mathrm{U}))=2=2(k-1)$. However as a consequence of the above lemma, in the following Corollary, we will prove that, if $n\geq 7$ is a prime, then there is not $Orbit_{N_\alpha}(\mathrm{U})$ with parameters $[n,\frac{n-1}{2},n(2^n-1),2(\frac{n-1}{2}-1)]$:

Corollary 2.13. Let $n\geq 7$ be a prime number, $\mathrm{F}_q=\mathrm{F}_2$ and $k=\frac{n-1}{2}$, then $Orbit_{N_\alpha}(\mathrm{U})=Orbit_{C_\alpha}(\mathrm{U})$ or $d_{\min}(Orbit_{N_\alpha}(\mathrm{U}))\leq 2(k-2)$.

Proof. Supppose $Orbit_{N_\alpha}(\mathrm{U})\neq Orbit_{C_\alpha}(\mathrm{U})$ and $d_{\min}(Orbit_{N_\alpha}(\mathrm{U}))=2(k-1)$. Then Singelton bound for subspace codes [9; Theorem 9], leads that:

$$n(2^n-1)\leq\begin{bmatrix} n-(2k-4)/2 \\ \max\{n,n-k\}\end{bmatrix}_2,$$

therefore

$$(2k+1)(2^{2k+1}-1)\leq\frac{(2^{k+3}-1)(2^{k+2}-1)}{3}.$$

On the other hand if $k\geq 3$, then $(2^{k+3}-1)(2^{k+2}-1)\leq 2^4(2^{2k+1}-1)$, thus for $n\geq 7$,

$$(2^{k+3}-1)(2^{k+2}-1)<3(2k+1)(2^{2k+1}-1),$$

which is a contradiction.

Consider $n=8$, $q=2$ and $\mathrm{U}=\langle 1,\alpha^{17},\alpha^{34}\rangle$, then

$Orbit_{N_\alpha}(\mathrm{U}) = Orbit_{C_\alpha}(\mathrm{U})$. In general it is an interesting question that when the Frobenius automorphism is a shift α^J on the elements of U? In the other words, when $Orbit_{N_\alpha}(\mathrm{U})$ is not equal to $Orbit_{C_\alpha}(\mathrm{U})$. In the following theorem, we give an answer to this question:

Theorem 2.14. Let $2^n - 1$ be a prime, $n \geq 5$ and $\dim(\mathrm{U}) = k$, such that $k \neq \log_2(n+1)$, and $\mathrm{U} \neq \mathrm{U}\sigma$, then $|Orbit_{N_\alpha}(\mathrm{U})| = n(2^n - 1)$.

Proof. Since $2^n - 1$ is a prime, then n is a prime, therefore by Lemma 2.12, if we suppose $|Orbit_{N_\alpha}(\mathrm{U})| \neq n(2^n - 1)$, then $Orbit_{N_\alpha}(\mathrm{U}) = Orbit_{C_\alpha}(\mathrm{U})$. Since $\mathrm{U} \neq \mathrm{U}\sigma$, we have, $\mathrm{U}\sigma = \mathrm{U}\alpha^J$ for some $J \neq 0$. Suppose $\mathrm{U} = \{0, 1, \alpha^{x_i} \ | i = 1, \ldots, 2^k - 2\}$ and denote the powers of the elements of $\mathrm{U} \setminus \{0\}$ by X_{U}:

$$X_{\mathrm{U}} = \{0, x_i \ | i = 1, 2, \ldots, 2^k - 2\}.$$

It is obvious that $X_{\mathrm{U}} \subset Z_{2^n}$ and all the operations over the elements are done module $2^n - 1$. We have

$$X_{\mathrm{U}\alpha^J} = \{J, x_i + J \ | i = 1, 2, \ldots, 2^k - 2\}$$
$$= X_{\mathrm{U}\sigma} = \{0, 2x_i \ | i = 1, 2, \ldots, 2^k - 2\}.$$

Let $x_1 + J = 0$, if $2x_1 = J$, then $3J = 0$. Since $2^n - 1 \neq 3$ and is a prime number, then $J = 0$, a contradiction. Suppose $2x_1 = x_2 + J$, so $x_2 = 3x_1$. If $2x_2 = J$, then $J = 0$, which is a contradiction. Therefore $2x_2 = x_3 + J$ so $x_3 = 7x_1$. In general suppose $x_i = (2^i - 1)x_1$, then

$$2x_i = J = -x_1 \Leftrightarrow (2^{i+1} - 1) = 0 \Leftrightarrow n | \, i + 1.$$

Since $k \neq log_q(n+1)$, then $n + 1 \neq q^k$ and we have the following two cases which we obtain a contradiction in both of them:

Case 1. If $n + 1 > 2^k$, then there is not an element x_i such that $2x_i = J$ and it is a contradiction.

Case 2. If $2^k > n + 1$, then for all $1 \leq i \leq n - 1$, $x_i = (2^i - 1)x_1$. Since n is a prime, then $n \neq 2^k - 2$, hence there is at least two elemets in the following equal sets:

$$\{x_i + J \mid i = n, \ldots, 2^k - 2\} = \{2x_i \mid i = n, \ldots 2^k - 2\}.$$

If $x_n + J = 2x_n$, then $x_n = J$ and for all $n \leq i \leq 2^i - 2$, $x_i + J \neq 2x_i$. Let $x_{n+1} + J = 2x_{n+2}$, then we have

$$x_{n+1} + J = 2x_{n+2}, x_{n+2} + J = 2x_{n+3}, \ldots, x_{n+i} + J = 2x_{n+1}.$$

Therefore it is easy to see that $x_{n+1} = J$ which is a contradiction. If we suppose that there is not any i such that $x_i + J = 2x_i$, then we have $x_n + J = 2x_{n+1}$ and in the same way we have, $x_n = J$ which is a contradiction and the proof is completed.

By Example 2.7 (2), we can see that the converse of the above theorem is not true.

Remark 2.15. In the proof of Theorem 2.14, if $n + 1 = 2^k$, then $X_{\mathrm{U}} = \{0, x_i \ | i = 1, 2, \ldots, 2^k - 2\}$ where for $1 \leq i \leq 2^k - 2$ we have $x_i = (2^i - 1)x_1$. This gives the structure of the subspace U, which $Orbit_{N_\alpha}(\mathrm{U}) = Orbit_{C_\alpha}(\mathrm{U})$.

We know that if $\frac{q^n - 1}{q - 1}$ is a prime number, then n is a prime, so $|Orbit_{C_\alpha}(\mathrm{U})| = \frac{q^n - 1}{q - 1}$, also if $q \neq 2$, then for every k we have $k \neq \log_q(n+1)$, therefore we can prove the following theorem:

Theorem 2.16. Let $\frac{q^n - 1}{q - 1}$ be a prime number, $n \geq 5$ and $q \neq 2$. Then $|Orbit_{N_\alpha}(\mathrm{U})| = n\frac{q^n - 1}{q - 1}$.

Proof. Since the proof is similar to Theorem 2.14, we omit it.

Conclusion

We considered orbit codes of the normalizer of a Singer subgroup. The structure of this normalizer leads a close relation between its orbits and the orbits of the Singer subgroup. Since these orbits are union of the cyclic subspace codes, they are cyclic subspace codes as well. Despite the orbits of the normalizer of a Singer subgroup are not large, taking the union of these orbits is suitable to form large cyclic subspace codes. For further work the main aid is to use the normalizer of the

Singer subgroup to construct optimal subspace codes. Also we will consider the normalizer of an irreducible cyclic subgroup of the general linear group and investigate its orbits.

Acknowledgement

The authors are grateful to the referee for the useful comments which improved the presentation of manuscript. This work was partially supported by the Center of Excellence of Algebraic Hyperstructures and its Applications of Tarbiat Modares University (CEAHA). Partial support by the Iran Telecommunication Research Center is gratefully acknowledged by the first author (FB).

References

1. Ahlswede R., Cai N., Li S.-Y.R., Yeung R.W. Network information flow. *IEEE Trans. Inform. Theory,* **46**: 1204-1216 (2000).
2. Braun M., Etzion T., Ostergard P., Vardy A., Wasserman A. Existence of q-analogs of Steiner systems. **arXiv**:1304-1462 (2013).
3. Dye R.H. Maximal subgroups of symplectic groups stabilizing spreads. II.*J. London Math. Soc,* **40**(2): 215-226 (1989).
4. Etzion T., Silberstein N. Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams. *IEEE Trans. Inform. Theory,* **IT-55**: 2909-2919 (2009).
5. Etzion T., Vardy A. Error-correcting codes in projective geometry. *IEEE Trans. Inform. Theory,* **IT-57**: 1165-1173 (2011).
6. Gluesing-Luerssen H., Morrison K., Troha C. Cyclic orbit codes and stabilizer subfields. **arXiv**:1403.1218 (2014).
7. Huppert B. Endliche Gruppen. I. Springer-Verlag, Berlin (1967).
8. Kohnert A., Kurz S., Construction of large constant dimension codes with a prescribed minimum distance. *Mathematical Methods in Computer Science, Springer, Berlin,* 31-42 (2008),
9. Kötter R., Kschischang F.R. Coding for errors and erasures in random network coding. *IEEE Trans. Inform. Theory,* **54**(8): 3579-3591 (2008).
10. Manganiello F., Trautmann A.-L., Rosenthal J. On conjugacy classes of subgroups of the general linear group and cyclic orbit codes. *In Proceedings of the 2011 IEEE International Symposium on Information Theory,* **31**(5): 1916-1920 (2011).
11. Rosenthal J., Trautman A.-L. A complete characterization of irreducible cyclic orbit codes and their Plucker embedding. *Des. Codes Cryptogr.,* 275-289 (2013).

12. Trautmann A.-L., Isometry and automorphisms of constant dimension codes. **arXiv**:1205.5465 [cs.IT] (2012).

13. Trautmann A.-L., Manganiello F., Braun M., and Rosenthal J. Cyclic orbit codes. *IEEE Trans. Inform. Theory*, **59**(11): 7386–7404 (2013).