The Construction of Orbit Codes Based on Singular Linear Space over Finite Fields

You Gao[1,*], Min-Yao Niu[1], Gang Wang[2]

[1] *College of Science, Civil Aviation University of China, Tianjin, 300300, P.R.China*

[2] *Chern Institute of Mathematics and LPMC, Nankai University, Tianjin, 300071, P. R. China*

Abstract: Orbit code is a class of constant dimension code which is defined as orbit of a subgroup of the general linear group $GL_n(\mathbb{F}_q)$, acting on the set of all the subspaces of vector space $\mathbb{F}_q^n$. In this paper, the construction of orbit codes based on the singular general linear group $GL_{n+l,n}(\mathbb{F}_q)$ acting on the set of all the subspaces of type (m,k) in singular linear spaces $\mathbb{F}_q^{n+l}$ is given. We give a characterization of orbit code constructed in singular linear space $\mathbb{F}_q^{n+l}$, and then give some basic properties of the constructed orbit codes. Finally two examples about our orbit codes for understanding these properties explicitly are presented.

Keywords: Random network coding, Constant dimension codes, Orbit codes, Singular general linear group, Singular linear space.

§1 Introduction

Random network coding, introduced by Ahlswede et al. in [1], describes a method for attaining a maximum information flow in a non-coherent network with several sources and sinks. The main feature of the network is that the nodes form random linear combinations of the incoming packets (vectors) and transmit the resulting packets further to their neighboring nodes. As a result, the receiver nodes (sinks) of the network will obtain linear combinations of the packets that have been injected into the network at its sources. This method is very effective in disseminating the information throughout the network.

In real-world applications, networks may be disrupted by noise, erasures et al. In order to overcome this deficiency, and since linear spaces are

*Corresponding author.
E-mail addresses: gao_you@263.net.

invariant under linear combinations, Koetter and Kschischang [2] developed an algebraic approach to random network coding by considering messages as subspaces of some fixed vector space $\mathbb{F}_q^n$. It is helpful (e.g. for decoding) to constrain oneself to subspaces of a fixed dimension, in which case we talk about constant dimension codes. Thus, codewords are subspaces of $\mathbb{F}_q^n$, and a code is a collection of such subspaces. Transmitting information through the network is thus reformulated in terms of transmitting subspaces. This motivates some scholars' interest in such codes. A. Elsenhans et al. in [3] showed a connection to the theory q-analogues of a combinatorial object. T. Etzion et al. in [4] proposed a method to design error-correcting codes in the projective space and in [5] investigated certain basic aspects of "coding theory in projective space."

Orbit code is a class of constant dimension code which is defined as the orbit of a subgroup of the general linear group $GL_n(\mathbb{F}_q)$, acting on the set of all the subspaces of vector space $\mathbb{F}_q^n$. The concept of defining codes as orbits of certain groups traces back to Slepian [6] where Euclidian spaces were considered and the corresponding codes are called group codes. In the network coding setting, A. L. Trautmann et al. [7] defined such codes as orbit codes. Firstly, the set of all the subspaces of $\mathbb{F}_q^n$ of dimension k is called Grassmann vatiety, denoted by $\mathcal{G}(k,n)$.

Definition 1.1. [7] Let $\mathcal{U} \in \mathcal{G}(k,n)$ be fixed, $\mathfrak{G}$ is the subgroup of $GL_n(\mathbb{F}_q)$, then

$$\mathbb{C} = \{\mathcal{U} \cdot A | A \in \mathfrak{G}\}$$

is called an orbit code. An orbit code is cyclic if the defining group is cyclic.

For vectors $x = (x_1, x_2, \cdots, x_n)$ and $y = (y_1, y_2, \cdots, y_n)$ in $\mathbb{F}_q^n$, the standard inner product is defined to be $x \cdot y = \sum_{i=1}^{n} x_i y_i$. For $\mathcal{U} \in \mathcal{G}(k,n)$, the orthogonal subspace $\mathcal{U}^\perp$ of $\mathcal{U}$ is defined as $\mathcal{U}^\perp = \{x \in \mathbb{F}_q^n | x \cdot y = 0, y \in \mathcal{U}\}$. Then we give the definition of the dual code of $\mathbb{C} \subseteq \mathcal{G}(k,n)$.

Definition 1.2. [7] If $\mathbb{C} \subseteq \mathcal{G}(k,n)$ is a constant dimension code, one defines the dual code of $\mathbb{C}$ as

$$\mathbb{C}^\perp = \{\mathcal{U}^\perp \in \mathcal{G}(n-k,n) | \mathcal{U} \in \mathbb{C}\}.$$

Orbit codes have useful algebraic structure, e.g. for the computation of the distance of an orbit code it is enough to compute the distance between the starting point and any of its orbit elements. This is analogous to linear block codes where the minimum distance of the codes can be derived from the weight of the non-zero codewords. The importance of this class of codes is underlined by the fact that several of the known algebra construction of constant dimension codes can be seen as orbit codes. E.g. the Reed-Solomon-like codes as well as the spread codes described in [7] can be seen as orbit codes.

In [7], A. L. Trautmann et al. introduced orbit codes, a new class of constant dimension codes for random network coding and defined that these codes can be described as the discrete orbit under a natural group action within the finite Grassmann variety $\mathcal{G}(k,n)$. In [8], J. Rosenthal et al. gave a complete characterization of orbit codes that are generated by an irreducible cyclic group. In [9], A. L. Trautmann investigated the Plücker embedding of cyclic orbit codes and showed how to efficiently compute the Grassmann coordinates of these codewords. In [10], A. L. Trautmann et al. showed how orbit codes can be seen as an analog of linear codes in block coding case. In [11], H. Gluesing-Luerssen et al. presented a detailed study of cyclic orbit codes based on the stabilizer subfield.

The structure of the paper is the following. In the section 2, the concept and a part of anzahl formulas of singular linear space $\mathbb{F}_q^{n+l}$ over a finite field $\mathbb{F}_q$ are introduced. In the section 3, the orbit codes based on the subspaces of type (m,k) in singular linear space $\mathbb{F}_q^{n+l}$ over $\mathbb{F}_q$ under the action of a subgroup of the singular general linear group $GL_{n+l,n}(\mathbb{F}_q)$ are presented and three explicit examples of our orbit codes are listed. In the section 4, a conclusion is given for this paper.

§2 Preliminaries

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a prime power. For two non-negative integers n and l, $\mathbb{F}_q^{n+l}$ denotes the $(n+l)$-dimensional row vector space over $\mathbb{F}_q$. It is easy to verify that the set of all the $(n+l)\times(n+l)$ nonsingular matrices over $\mathbb{F}_q$ of the form

$$\begin{pmatrix} T_{11} & T_{12} \\ 0 & T_{22} \end{pmatrix},$$

where T_{11} and T_{22} are nonsingular $n \times n$ and $l \times l$ matrices, respectively, forms a group under martix multiplication. This group is called the singular general linear group of degree $n+l$ over $\mathbb{F}_q$ and denoted by $GL_{n+l,n}(\mathbb{F}_q)$. If $l = 0$(resp. $n = 0$), $GL_{n,n} = GL_n(\mathbb{F}_q)$(resp. $GL_{l,0} = GL_l(\mathbb{F}_q)$) is the general linear group of degree n(resp. l) over $\mathbb{F}_q$. Moreover, the set of all the $k \times (n+l)$ matrices over $\mathbb{F}_q$ is denoted by $\mathrm{Mat}_{k\times(n+l)}$.

Now let P be an m-dimensional row vector space of $\mathbb{F}_q^{n+l}$, then we write $\dim P = m$. Let $v_1, v_2, ..., v_m$ be a basis of P. We notice that $v_1, v_2, ..., v_m$ are vectors of $\mathbb{F}_q^{n+l}$. We usually use the $m \times (n+l)$ matrix to represent

the vector subspace P, write $P = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix}$, i.e, we use the same letter P to denote a matrix which represents the vector subspace P, and call the matrix P a matrix representation of the vector subspace P. It should be noted that a matrix representing an m-dimensional vector subspace of $\mathbb{F}_q^{n+l}$ is an $m \times (n+l)$ matrix of rank m.

In fact, let $\mathrm{T} \in GL_{n+l,n}(\mathbb{F}_q)$, $(x_1, ..., x_n, x_{n+1}, ..., x_{n+l}) \in \mathbb{F}_q^{n+l}$. There is an action of $GL_{n+l,n}(\mathbb{F}_q)$ on $\mathbb{F}_q^{n+l}$ defined as follows:

$$\mathbb{F}_q^{n+l} \times GL_{n+l,n}(\mathbb{F}_q) \to \mathbb{F}_q^{n+l}$$

$$((x_1, \cdots, x_n, x_{n+1}, \cdots, x_{n+l}), T) \mapsto (x_1, \cdots, x_n, \cdots, x_{n+l})T.$$

The above action induces an action of $GL_{n+l,n}(\mathbb{F}_q)$ on the set of $m \times (n+l)$ matrices over $\mathbb{F}_q$ and also on the set of m-dimensional vector subspaces of $\mathbb{F}_q^{n+l}$; i.e., a subspace P is carried by $T \in GL_{n+l,n}(\mathbb{F}_q)$ to the subspace PT. The vector space $\mathbb{F}_q^{n+l}$, together with the above group action of the singular general linear group $\mathrm{T} \in GL_{n+l,n}(\mathbb{F}_q)$, is called the $(n+l)$-dimensional singular linear space over $\mathbb{F}_q$ [12].

For $1 \leq i \leq n+l$, let e_i be the row vector in $\mathbb{F}_q^{n+l}$ whose i-th coordinate is 1 and all other coordinates are 0. Denote by E the l-dimensional vector subspace of $\mathbb{F}_q^{n+l}$ generated by $e_{n+1}, e_{n+2}, \cdots, e_{n+l}$. We call an m-dimensional vector subspace P of $\mathbb{F}_q^{n+l}$ is called a subspace of type (m,k) if $\dim(P \cap E) = k$. The collection of all the subspaces of type $(m,0)$ in $\mathbb{F}_q^{n+l}$, $0 \leq m \leq n$, is called attenuated space [13].

Let q be a prime power, and let m_1, m_2 be two integers. For brevity we use the Gaussian coefficient [14]

$$\begin{bmatrix} m_2 \\ m_1 \end{bmatrix}_q = \frac{\prod_{t=m_2-m_1+1}^{m_2} (q^t - 1)}{\prod_{t=1}^{m_1} (q^t - 1)}.$$

By convenience $\begin{bmatrix} m_2 \\ 0 \end{bmatrix}_q = 1$ and $\begin{bmatrix} m_2 \\ m_1 \end{bmatrix}_q = 0$ whenever $m_1 < 0$ or $m_2 < m_1$.

Let $\mathcal{M}(m,k;n+l,n)$ denote the set of all the subspaces of type (m,k) in $\mathbb{F}_q^{n+l}$, and let $N(m,k;n+l,n)$ denote the size of $\mathcal{M}(m,k;n+l,n)$.

Lemma 2.1. [12] Subspace of type (m,k) exists in the $(n+l)$-dimensional singular linear space $\mathbb{F}_q^{n+l}$ if and only if

$$0 \leq k \leq l \text{ and } 0 \leq m-k \leq n.$$

Moreover, if $\mathcal{M}(m,k;n+l,n)$ is non-empty, then the set of all the subspaces of type (m,k) in $\mathbb{F}_q^{n+l}$ forms an orbit under the action of $GL_{n+l,n}(\mathbb{F}_q)$, and

$$N(m,k;n+l,n) = q^{(m-k)(l-k)} \begin{bmatrix} n \\ m-k \end{bmatrix}_q \begin{bmatrix} l \\ k \end{bmatrix}_q .$$

§3 Orbit codes based on singular linear space $\mathbb{F}_q^{n+l}$

In [15], the authors introduced suborbits of subspaces of type (m,k) under finite singular general linear groups, and calculated the length of each suborbits. In this section, based on their works, we construct the codes which can be described as the discrete orbits based on the singular general linear group $GL_{n+l,n}(\mathbb{F}_q)$ acting on a subset of the subspaces of type (m,k) in singular linear space $\mathbb{F}_q^{n+l}$, and give some basic properties.

Let us start with a fact. The results may be found in [15]. Assume that P represent the subspace of type (m,k) in singular linear space $\mathbb{F}_q^{n+l}$, and A, B denote matrices which represent the subspace P of type (m,k). Then there is an $m \times m$ nonsingular matrix $U \in GL_{m,m-k}(\mathbb{F}_q)$, such that

$$A = UB,$$

and U have the following form

$$\begin{pmatrix} U_{11} & U_{12} \\ 0 & U_{22} \end{pmatrix}.$$

Define the subspace distance on $\mathcal{M}(m,k;n+l,n)$ as follows:

$$\begin{aligned} d_s(P,Q) &= \dim(P) + \dim(Q) - 2\dim(P \cap Q) \\ &= 2(m - \dim(P \cap Q)) \\ &= 2\mathrm{rank}\begin{pmatrix} P \\ Q \end{pmatrix} - 2m, \end{aligned}$$

$\forall P, Q \in \mathcal{M}(m,k;n+l,n)$. The subspace distance above is indeed a metric [4].

In this paper, a constant dimension code $\mathbb{C}(m,k)$ is a non-empty subset of $\mathcal{M}(m,k;n+l,n)$. The minimum distance is defined by the usual way, i.e., $d_s(\mathbb{C}(m,k)) = \min\{d_s(c_1,c_2) \mid c_1 \neq c_2, c_1, c_2 \in \mathbb{C}(m,k)\}$. Then $\mathbb{C}(m,k) \subseteq$

$\mathcal{M}(m,k;n+l,n)$, if $\mathbb{C}(m,k)$ has the minimum distance $d_s(\mathbb{C}(m,k))$ and the size $|\mathbb{C}(m,k)|$, is called an $[n+l, d_s(\mathbb{C}(m,k)), |\mathbb{C}(m,k)|, (m,k)]$-code.

Let $P \in \mathcal{M}(m,k;n+l,n)$ be a subspace of type (m,k) in $\mathbb{F}_q^{n+l}$ and the same letter P denote the matrix representation of the subspace P. For any $A \in GL_{n+l,n}(\mathbb{F}_q)$, define

$$P \cdot A = \text{rowspace}(P \cdot A).$$

Lemma 3.1. Let $X \in \mathcal{M}(m,k;n+l,n)$, and suppose

$$P = \begin{pmatrix} P_{11} & P_{12} \\ 0 & P_{22} \end{pmatrix}, Q = \begin{pmatrix} Q_{11} & Q_{12} \\ 0 & Q_{22} \end{pmatrix}$$

are two matrices representation of the subspace X, where rank P_{11} = rank $Q_{11} = m-k$, rankP_{22} = rank$Q_{22} = k$. Then for any $A \in GL_{n+l,n}(\mathbb{F}_q)$,

$$\text{rowspace}(PA) = \text{rowspace}(QA).$$

Proof. Since rowspace(P) = rowspace$(Q) = X$, the same as [15, Theorem 2.1, proof], we can suppose that there is a matrix $T \in GL_{m,m-k}(\mathbb{F}_q)$ such that $P = TQ$, and T have the form

$$\begin{pmatrix} T_{11} & T_{12} \\ 0 & T_{22} \end{pmatrix}.$$

Then

$$\begin{aligned} \text{rowspace}(PA) &= \text{rowspace}(TQA) \\ &= \text{rowspace}(QA). \end{aligned}$$

By Lemma 3.1, we deduce immediately the operation defined above is independent of the representation of P.

We can now define an action of $GL_{n+l,n}(\mathbb{F}_q)$ on the set of all the subspaces of type (m,k) in singular linear space $\mathbb{F}_q^{n+l}$ as follows:

$$\begin{aligned} \mathcal{M}(m,k;n+l,n) \times GL_{n+l,n}(\mathbb{F}_q) &\to \mathcal{M}(m,k;n+l,n) \\ (P,A) &\mapsto P \cdot A. \end{aligned}$$

Theorem 3.2. The subspace distance on $\mathcal{M}(m,k;n+l,n)$, i.e., $\forall P, Q \in \mathcal{M}(m,k;n+l,n)$, $d_s(P,Q) = \dim P + \dim Q - 2\dim(P \cap Q)$ is $GL_{n+l,n}(\mathbb{F}_q)$-invariant.

Proof.

$$\begin{aligned} d_s(PA,QA) &= \dim(PA) + \dim(QA) - 2\dim(PA \cap QA) \\ &= 2(m - \dim(PA \cap QA)) \\ &= 2\text{rank}\begin{pmatrix} PA \\ QA \end{pmatrix} - 2m \\ &= 2\text{rank}\begin{pmatrix} P \\ Q \end{pmatrix} - 2m \\ &= d_s(P,Q), \end{aligned}$$

where $P, Q \in \mathcal{M}(m, k; n+l, n)$, $A \in GL_{n+l,n}(\mathbb{F}_q)$. P, Q also denote the matrix representations of the subspaces P, Q of type (m, k) in singular linear space $\mathbb{F}_q^{n+l}$.

Based on the Theorem 3.2, it may be easy to calculate the minimum distance of orbit codes constructed in singular linear space $\mathbb{F}_q^{n+l}$.

Definition 3.3. For $P \in \mathcal{M}(m, k; n+l, n)$, the stabilizer group of P in the singular general linear group $GL_{n+l,n}(\mathbb{F}_q)$ is defined as follows:

$$\mathrm{Stab}(P) = \{A \in GL_{n+l,n}(\mathbb{F}_q) \mid P \cdot A = P\}.$$

Remark. According to the definition 3.3, we can give a relation of equivalence for $A, B \in GL_{n+l,n}(\mathbb{F}_q)$,

$$A \sim B \Leftrightarrow \exists S \in \mathrm{Stab}(P), \text{ such that } A = SB.$$

Theorem 3.4. For $P \in \mathcal{M}(m, k; n+l, n)$, then

$$\mathcal{M}(m, k; n+l, n) \cong GL_{n+l,n}(\mathbb{F}_q)/\mathrm{Stab}(P).$$

Proof. For $P \in \mathcal{M}(m, k; n+l, n)$, we use the same letter P to represent the matrix representation of subspace P. We prove that the following map is bijective:

$$\begin{aligned} \varphi : GL_{n+l,n}(\mathbb{F}_q)/\mathrm{Stab}(P) &\longrightarrow \mathcal{M}(m, k; n+l, n) \\ [M] &\mapsto \mathrm{rowspace}(PM), \end{aligned}$$

where $[M]$ denotes the class in $GL_{n+l,n}(\mathbb{F}_q)/\mathrm{Stab}(P)$ for which $M \in GL_{n+l,n}(\mathbb{F}_q)$ is a representative.

Consider $Q \in \mathcal{M}(m, k; n+l, n)$ and $Q \in \mathrm{Mat}_{m\times(n+l)}$ such that $Q = \mathrm{rowspace}(Q)$. Then the map is surjective since for any full-rank matrix $Q \in \mathrm{Mat}_{m\times(n+l)}(\mathbb{F}_q)$ there exists a $M \in GL_{n+l,n}(\mathbb{F}_q)$ such that $Q = PM$.

Let $M_1, M_2 \in GL_{n+l,n}(\mathbb{F}_q)$. We show that the row space of PM_1 is equal to the row space of PM_2 if and only if $[M_1] = [M_2] \in GL_{n+l,n}(\mathbb{F}_q)/\mathrm{Stab}(P)$:

$$\begin{aligned} &\mathrm{rowspace}(PM_1) = \mathrm{rowspace}(PM_2) \\ &\Leftrightarrow \exists M \in Gl_m(\mathbb{F}_q) \text{ such that } PM_1 = MPM_2 \\ &\Leftrightarrow P = MPM_2M_1^{-1} \\ &\Leftrightarrow \mathrm{rowspace}(P) = \mathrm{rowspace}(PM_2M_1^{-1}) \\ &\Leftrightarrow M_2M_1^{-1} \in \mathrm{Stab}(P) \\ &\Leftrightarrow \exists S \in \mathrm{Stab}(P) \text{ such that } M_2 = SM_1 \\ &\Leftrightarrow [M_1] = [M_2]. \end{aligned}$$

This proves that φ is also injective, hence it is a bijection.

Example 1. Consider the case of

$$P = \text{rowspace}\begin{pmatrix} I^{(m-k)} & 0 & 0 & 0 \\ 0 & 0 & I^{(k)} & 0 \end{pmatrix}.$$

We can prove

$$\text{Stab}(P) = \{\begin{pmatrix} I^{(m-k)} & 0 & 0 & 0 \\ A_{21} & A_{22} & A_{23} & A_{24} \\ 0 & 0 & I^{(k)} & 0 \\ A_{41} & A_{42} & A_{43} & A_{44} \end{pmatrix} | A_{22} \in GL_{n-m-k}(\mathbb{F}_q), A_{44} \in GL_{l-k}(\mathbb{F}_q)\}.$$

Proposition 3.5. If $P, Q \in \mathcal{M}(m,k;n+l,n)$, then $\text{Stab}(P)$ is conjugate to $\text{Stab}(Q)$, and $|\text{Stab}(P)| = |\text{Stab}(Q)|$.

Proof. Let $A \in GL_{n+l,n}(\mathbb{F}_q)$ such that $P = QA$, then

$$\begin{aligned} S \in \text{Stab}(P) &\Leftrightarrow P \cdot S = P \\ &\Leftrightarrow QAS = QA \\ &\Leftrightarrow ASA^{-1} \in \text{Stab}(Q). \end{aligned}$$

Then $\text{Stab}(P)$ is conjugate to $\text{Stab}(Q)$, and $|\text{Stab}(P)| = |\text{Stab}(Q)|$.

Because of this property, it is enough to choose a representative P when we calculate the number of the orbits formed by the subspaces of type (m,k) in singular linear space $\mathbb{F}_q^{n+l}$ under the action of $GL_{n+l,n}(\mathbb{F}_q)$.

Definition 3.6. For $P \in \mathcal{M}(m,k;n+l,n)$ is fixed, and G is a subgroup of $GL_{n+l,n}(\mathbb{F}_q)$. Then

$$\mathbb{C}(m,k) = \{P \cdot A | A \in G\}$$

is called an orbit code based on the subspaces of type (m,k) in singular linear space $\mathbb{F}_q^{n+l}$ under the action of a subgroup of the singular general linear group $GL_{n+l,n}(\mathbb{F}_q)$. Furthermore, if G is a cyclic subgroup of the singular general linear group $GL_{n+l,n}(\mathbb{F}_q)$, orbit code $\mathbb{C}(m,k)$ is called cyclic orbit code based on singular linear space $\mathbb{F}_q^{n+l}$.

Lemma 3.7. For $\mathbb{C}(m,k) = \{P \cdot A | A \in G\}$ is an orbit code as defined in Definition 3.6. Then the cardinality of $\mathbb{C}(m,k)$ is

$$|\mathbb{C}(m,k)| = \frac{|G|}{|\text{Stab}(P) \cap G|}.$$

The minimum distance of $\mathbb{C}(m,k)$ is

$$d_s(\mathbb{C}(m,k)) = \min_{A \in G \setminus \text{Stab}(P)} d_s(P, PA).$$

Moreover,

$$d_s(P, PA_1) = d_s(P, PA_2), \text{ if } A_1 \sim A_2.$$

Proof. Based on [15, Theorem 2.5], it is easy to verify that the cardinality of orbit code $\mathbb{C}(m,k)$ is $\frac{|G|}{|\mathrm{Stab}(P)\cap G|}$. By the definition of the minimum distance of orbit code $\mathbb{C}(m,k)$ and the transitivity of $GL_{n+l,n}(\mathbb{F}_q)$ on the set of subspaces of the same type (m,k), $\forall Q_1, Q_2 \in \mathbb{C}(m,k)$, we have

$$d_s(Q_1, Q_2) = d_s(PA_1, PA_2) = d_s(P, PA_2A_1^{-1}),$$

for some $A_1, A_2 \in G$, and $A_2A_1^{-1} \in G$.
If $A_1 \sim A_2$, then $\exists S \in \mathrm{Stab}(P)$, such that $A_1 = SA_2$. Thus $d_s(P, PA_1) = d_s(P, PSA_2) = d_s(P, PA_2)$.

Next we will give the definition of complementary codes for the orbit codes based on singular linear space $\mathbb{F}_q^{n+l}$.

Firstly, we present a fact. By the transitivity of $GL_{n+l,n}(\mathbb{F}_q)$ on the set of subspaces of the same type (m,k), we may pick the subspace P of type (m,k) as the following form

$$\mathrm{P} = \begin{pmatrix} I^{(m-k)} & 0^{(m-k,n-m+k)} & 0 & 0 \\ 0 & 0 & I^{(k)} & 0^{(k,l-k)} \end{pmatrix}.$$

For $P \in \mathbb{C}(m,k)$, the orthogonal subspace $P^\perp$ of P is defined as $P^\perp = \{x \in \mathbb{F}_q^{n+l} | x \cdot y = 0, y \in P\}$. Then we give the definition of the dual code of the orbit code $\mathbb{C}(m,k) \subseteq \mathcal{M}(m,k;n+l,n)$.

Definition 3.8. Given an orbit code $\mathbb{C}(m,k) \subseteq \mathcal{M}(m,k;n+l,n)$, define the dual code of $\mathbb{C}(m,k)$ in singular linear space $\mathbb{F}_q^{n+l}$ as

$$\mathbb{C}^\perp(m,k) = \{P^\perp | P \in \mathbb{C}(m,k)\},$$

where the form of $P^\perp$ is:

$$P^\perp = \begin{pmatrix} 0 & I^{(n-m+k)} & 0 & 0 \\ 0 & 0 & 0 & I^{(l-k)} \end{pmatrix} \in \mathcal{M}(n+l-m, l-k; n+l, n).$$

The dual codes of the orbit codes based on singular linear space $\mathbb{F}_q^{n+l}$ have a nice property.

Theorem 3.9. The dual code $\mathbb{C}^\perp(m,k)$ of orbit code $\mathbb{C}(m,k)$ based on singular linear space $\mathbb{F}_q^{n+l}$ is again an orbit code.

Proof. Let $P \in \mathcal{M}(m,k;n+l,n)$ be fixed in $\mathbb{F}_q^{n+l}$, and $\mathbb{C}(m,k) = \{P \cdot A | A \in G\}$ is an orbit code based on singular linear space $\mathbb{F}_q^{n+l}$. There, we define a new action on $\mathcal{M}(m,k;n+l,n)$ under a subgroup of the singular general linear group $Gl_{n+l,n}(\mathbb{F}_q)$ as follows:

$$P^\perp \circ A^{-1} = P^\perp \cdot (A^{-1})^T,$$

where $P^{\perp} \in \mathcal{M}(n+l-m, l-k; n+l, n), A \in G \subseteq Gl_{n+l,n}(\mathbb{F}_q)$.

Obviously, $\{A^{-1}|A \in G\}$ is a subgroup of $Gl_{n+l,n}(\mathbb{F}_q)$. It is easy to verify that $(P \cdot A)^{\perp} = P^{\perp} \circ A^{-1} = P^{\perp} \cdot (A^{-1})^T$, so the set $\{P^{\perp} \circ A^{-1}|P^{\perp} \in \mathcal{M}(n+l-m, l-k; n+l, n),\ A^{-1} \in G\}$ is also an orbit code based on singular linear space $\mathbb{F}_q^{n+l}$.

The construction of dual codes for the orbit codes based on singular linear space $\mathbb{F}_q^{n+l}$ is clear, so we will calculate the parameters of the dual codes. We give the conclusion.

Remark. If $\mathbb{C}(m,k)$ is an orbit code based on singular linear space $\mathbb{F}_q^{n+l}$ and its parameters are $[n+l, M, 2\delta, (m,k)]$, thus $\mathbb{C}^{\perp}(m,k)$ is an $[n+l, M, 2\delta, (n+l-m, l-k)]$-code.

Above property of the orbit codes based on singular linear space $\mathbb{F}_q^{n+l}$ is nice, and next we will introduce another nice property for these codes.

Theorem 3.10. Given an orbit code $\mathbb{C}(m,k) = \{P \cdot A|A \in G\}$, then there is an isometry orbit code in singular linear space $\mathbb{F}_q^{n+l}$,

$$\widetilde{\mathbb{C}}(m,k) = \{\text{rowspace}\begin{pmatrix} I^{(m-k)} & 0^{(m-k,n-m+k)} & 0 & 0 \\ 0 & 0 & I^{(k)} & 0^{(k,l-k)} \end{pmatrix} \cdot A|A \in \widetilde{G}\},$$

for some $\widetilde{G}$.

Particularly, $|\mathbb{C}(m,k)| = |\widetilde{\mathbb{C}}(m,k)|$, and $d_s(\mathbb{C}(m,k)) = d_s(\widetilde{\mathbb{C}}(m,k))$.

Proof. Let P be an $m \times (n+l)$ matrix over $\mathbb{F}_q$ and be also a matrix representation of P. The same as [15, Theorem 2.1, proof], suppose that $B \in GL_{n+l,n}(\mathbb{F}_q)$, such that

$$PB = \begin{pmatrix} I^{(m-k)} & 0^{(m-k,n-m+k)} & 0 & 0 \\ 0 & 0 & I^{(k)} & 0^{(k,l-k)} \end{pmatrix}$$

Define

$$\widetilde{G} = \{B^{-1}AB|A \in G\},$$

then

$$\widetilde{\mathbb{C}}(m,k) = \{\text{rowspace}\begin{pmatrix} I^{(m-k)} & 0^{(m-k,n-m+k)} & 0 & 0 \\ 0 & 0 & I^{(k)} & 0^{(k,l-k)} \end{pmatrix} \cdot D|D \in \widetilde{G}\}$$

has the desired property.

Example 2. Let $P = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$, $PB = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$,

thus $B = \{\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} |a_{31}+a_{41} = 0, a_{32}+a_{42} = 0, a_{33}+a_{43} = 1, a_{34}+a_{44} = 0\}$,

so the isometric orbit code of orbit code $\mathbb{C}(3,1)$ is

$$\widetilde{\mathbb{C}}(3,1) = \{\text{rowspace}(\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot D) | D \in \widetilde{G}\},$$

where $\widetilde{G} = \{B^{-1}AB | A \in G\}$.

Finally we present an example about our orbit code in singular linear space $\mathbb{F}_q^{n+l}$ for understanding these properties explicitly.

Example 3. Let $n = 4$, $l = 2$, $m = 3$, $k = 1$. And

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

The matrix representation of the subspace $P \in \mathcal{M}(3,1;6,4)$ is

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

The stabilizer group of P is

$$\text{Stab}(P) = \{\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} & a_{36} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} & a_{46} \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} | a_{3i}, a_{4i} \in \mathbb{F}_q, i = 1, ..., 6\}.$$

It is easy to verify that G, G^2, G^3, G^4 are different, and order(G)=4.

Therefore $\mathbb{C}(3,1) = \{P \cdot \langle G \rangle\} = \{P, PG, PG^2, PG^3\}$ is an orbit code based on singular linear space $\mathbb{F}_2^6$, and is also a cyclic orbit code where the acting group is $\langle G \rangle$. By calculating, we get $d_s(\mathbb{C}(3,1)) = 2$, so the parameters of this orbit code are $[6,2,4,(3,1)]$. The parameters of dual code $\mathbb{C}^{\perp}(3,1)$ for this orbit code $\mathbb{C}(3,1)$ are $[6,2,4,(3,1)]$.

§4 Conclusions

We give a detailed study of the orbit codes in singular linear space $\mathbb{F}_q^{n+l}$. These codes can be described as the discrete orbits based on the singular

general linear group $GL_{n+l,n}(\mathbb{F}_q)$ acting on the set of all the subspaces of type (m,k) in singular linear spaces $\mathbb{F}_q^{n+l}$. The basic properties (e.g. the dual codes and the isometry orbit codes et.al) of our orbit codes are presented. Finally an example about our orbit codes for understanding these properties explicitly is provided.

Acknowledgements

This work is supported by the National Natural Science Foundation of China under Grant No.11701558.

References

[1] R. Ahlswede, N. Cai, S. Y. R. Li and R. W. Yeung. Network information flow. IEEE Trans. Inform. Theory, vol. 46, no. 4, pp. 1204-1216, 2000.

[2] R. Koetter and F. R. Kschischang. Coding for errors and erasures in random network coding. IEEE Trans. Inform. Theory. vol. 54, no. 8, pp. 3579-3591, 2008.

[3] A. Elsenhans, A. Kohnert and A. Wassermann. Construction of codes for network coding. In Proc. 19th Int. Symp. Math. Theorey Netw. Syst., pp. 1811-1814, Budapest, Hungary, 2010.

[4] T. Etzion and N. Silberstein. Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams. IEEE Trans. Inform. Theory. vol. 55, no. 7, pp. 2909-2919, 2009.

[5] T. Etzion and A. Vardy. Error-correcting codes in projective spaces. IEEE Trans. Inform. Theory. vol. 57, no. 2, pp. 1165-1173, 2011.

[6] D. Slepian. Group codes for the Graussian channel. Bell Labs. Tech. Journal., vol. 47, no. 4, pp. 575-602, 1968.

[7] A. L. Trautmann, F. Manganiello and J. Rosenthal. Orbit codes-A new concept in the area of network coding. in Proc. IEEE Inform. Theory Workshop, Dublin, Ireland, vol, 23. no. 3, pp. 1-4, 2010.

[8] J. Rosenthal and A. L. Trautmann. A complete characterization of irreducible cyclic orbit codes and their Plücker embedding. Des. Codes Cryptogr., vol. 66, no. 1-3, pp. 275-289, 2013.

[9] A. L. Trautmann. Plücker embedding of cyclic orbit codes. in Proc. 20th Int. Symp. Math. Theory Networks Syst., Melbourne, Australia, vol. 59, no. 11, pp. 7386-7404, 2012.

[10] A. L. Trautmann, F. Manganiello, M. Braun and J. Rosenthal. Cyclic orbit codes. IEEE Trans. Inform. Theory. vol. 59, no. 11, pp. 7386-7404, 2013.

[11] H. Gluesing-Luerssen, K. Morrison and C. Troha. Cyclic orbit codes and stabilizer subfields. Advances in Mathematics of Communications., vol. 9, no. 2, pp. 177-197, 2017.

[12] K. Wang, J. Guo and F. Li. Singular linear space and its applications. Finite Fields Appl. vol. 17, no. 5, pp. 395-406, 2011.

[13] K. Wang, J. Guo and F. Li. Association schemes based on attenuated spaces. European J. Combin., vol. 31, no. 1, pp. 297-305, 2010.

[14] Z. Wan. Geometry of classical groups over finite fifids. Second Edition., Science Press, Beijing, New York, 2002.

[15] K. Wang, J. Guo and F. Li. Suborbits of subspaces of type (m, k) under finite singular general linear groups. Linear Algebra and its Application, vol. 431, no. 8, pp. 1360-1366, 2009.