IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received December 25, 2020, accepted January 20, 2021, date of publication January 25, 2021, date of current version January 29, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3054377

Constructions of Orbit Codes Based on Unitary Spaces Over Finite Fields

SHANGDI CHEN AND QIN XU
College of Science, Civil Aviation University of China, Tianjin 300300, China

Corresponding author: Shangdi Chen (11csd@163.com)

This work was supported by the projects of Natural Science from Fundamental Research of the Central Universities Civil Aviation University of China under Grant 3122019152 and Grant 31220199192.

ABSTRACT Orbit codes, as special constant dimension codes, have attracted much attention due to their applications for error correction in random network coding. This paper is devoted to constructing large orbit codes by making full use of unitary space. Firstly, we construct a cyclic unitary group of order $q^{2n} - 1$ by means of the companion matrix of a primitive polynomial over finite fields $\mathbb{F}_{q^2}$, and so the corresponding code is unitary cyclic orbit code. As a special application, a new quaternary orbit code (6, 63, 4, 3) is given. Secondly, we obtain orbit codes with large size using the external direct product of unitary groups acting on the direct sum of subspaces. Finally, a table is given for illustrating our codes improve upon those constructed by Trautmann *et al.* and Poroch *et al.*

INDEX TERMS Constant dimension codes, orbit codes, unitary space, unitary group, primitive polynomials.

I. INTRODUCTION

Random network coding plays an important role in coding theory for its high efficiency in transmitting the information. However, it has a deficiency of highly sensitive to error propagation. In order to overcome this deficiency, Kotter and Kschischang [1] proposed an algebraic approach to random network coding by considering messages as subspaces of some fixed vector space and showed how constant dimension codes can used in random network coding for correction of errors and erasures.

Different approaches of constructing constant dimension codes have been investigated in recent years. In [2], Silva *et al.* pointed out that lifted maximum rank distance codes can result in asymptotically optimal constant dimension codes, and can be decoded efficiently. Xu and Chen [3] presented an effective construction which can be seen as a generalization of the lifted maximum rank distance codes. Heinlein [4] generalized the upper bounds of for constant dimension codes which contain lifted maximum rank distance codes. In [5], Luerssen and Troha proposed a new construction coming from Corollary 39 in [6] which was named as the linkage construction. Li [7] combined the linkage construction and echelon Ferrers [8] to obtain some new lower bounds of constant dimension codes.

This paper at hand is most closely related to references [9]–[19]. All these papers study orbit codes, which are constant dimension codes that arise as an orbit of a subgroup of the general linear group acting on a subspace in $\mathbb{F}_q^{(n)}$. Orbit codes were first introduced in [9], where the authors showed spread codes can be seen as special instances of orbit codes. In [10], Rosenthal and Trautmann gave the complete characterization of orbit codes generated by irreducible cyclic groups. At the same time, Trautmann *et al.* [11] described cyclic orbit codes and proposed a decoding algorithm for cyclic orbit codes arising from irreducible cyclic groups. Luerssen *et al.* [12] presented a detailed study of cyclic orbit codes based on the stabilizer subfields. Trautmann [13] investigated how message encoding can be done for Desarguesian spread and cyclic orbit codes. Climent and Requena [14] gave a construction of an abelian non-cyclic orbit code and it is partial spread [15].

Recently, Poroch and Talebi [16] determined product of symplectic groups and its orbit codes, and a decoding algorithm of this code was considered. Gao and Niu [17] constructed orbit codes based on the subspaces of type (m, k) in singular linear spaces over finite fields and derived some basic properties of these codes. Chen and Liang [18] gave some methods of constructing large orbit codes from known

The associate editor coordinating the review of this manuscript and approving it for publication was Sun-Yuan Hsieh.

orbit codes by fully applying the sub-orbits of permutation groups. Chen and Liang [19] presented a new construction of abelian non-cyclic orbit code by making use of the companion matrix of a primitive polynomial over finite fields and a spread code was obtained.

Compared with the research results of orbit codes in Grassmannian, there are few research results of orbit codes based on typical spaces in the geometry of classical groups over finite fields with good combinatorial structures (see wan [20]). Our main motivation is to study how to construct unitary orbit codes which arise as an orbit of a totally isotropic subspace in unitary space under a unitary subgroup of the general linear group. In this paper, we firstly construct a cyclic unitary group of order $q^{2n}-1$ by using the companion matrix of a primitive polynomial over finite fields $\mathbb{F}_{q^2}$, and so the corresponding code is unitary cyclic orbit code (see Construction 1). Based on this code, orbit codes with larger size are derived using the external direct product of unitary groups acting on the direct sum of subspaces (see Construction 2). Finally, a comparison is made with the orbit codes constructed by Trautmann *et al.* [11] in Grassmannian and Poroch and Talebi [16] based on symplectic spaces over finite fields. What is important is that our codes improve upon those constructed in [11], [16] from TABLE 1. A new series of orbit codes with good error-correcting performance is obtained.

TABLE 1. **The comparison.**

	M	d_S
Trautmann et al.	$lcm\{q^{n_1}-1, q^{n_2}-1\}$	$2k-2d$
Poroch et al.	q^n-1	$2n-2d$
our results	$q^{2n}-1$	$2n-2d$

The rest of the paper is organized as follows. In Section 2, the relevant concepts of orbit codes and unitary spaces are introduced. In Section 3, the concrete construction of unitary cyclic orbit codes based on the subspaces of type $(n, 0)$ in unitary space $\mathbb{F}_{q^2}^{(2n)}$ is provided and the related parameters are computed. In Section 4, orbit codes with larger size are given. In Section 5, a conclusion is made for this paper.

II. PRELIMINARIES

Let us first recall some basic facts about constant dimension codes and orbit codes.

Let $\mathbb{F}_q$ be the finite field with q elements (where q is a prime power), and $\mathbb{F}_q^{(n)}$ denotes the n-dimensional row vector space over $\mathbb{F}_q$.

Definition 1: ([1]) Given a nonnegative integer $k \leq n$, the set of all k-dimensional subspaces of $\mathbb{F}_q^{(n)}$ is called the Grassmannian and is denoted by $\mathcal{G}_q(k, n)$.

The cardinality of $\mathcal{G}_q(k, n)$ is given by the Gaussian coefficient

$$|\mathcal{G}_q(k,n)| = \begin{bmatrix} n \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^{n-i}-1}{q^{k-i}-1}.$$

For any two subspaces $\mathcal{U}, \mathcal{V} \in \mathcal{G}_q(k, n)$, their subspace distance is defined by

$$\begin{aligned} d_S(\mathcal{U}, \mathcal{V}) &= \dim \mathcal{U} + \dim \mathcal{V} - 2\dim(\mathcal{U} \cap \mathcal{V}) \\ &= 2(k - \dim(\mathcal{U} \cap \mathcal{V})). \end{aligned} \tag{1}$$

Definition 2: ([1]) A constant dimension code of length n is simply a subset $\mathcal{C}$ of $\mathcal{G}_q(k, n)$. The minimum distance of $\mathcal{C}$ is defined as

$$d_S(\mathcal{C}) = \min\{d_S(\mathcal{U}, \mathcal{V}) | \mathcal{U}, \mathcal{V} \in \mathcal{C}, \mathcal{U} \neq \mathcal{V}\}.$$

A constant dimension code $\mathcal{C}$ of length n, dimension k, size $M(= |\mathcal{C}|)$ and distance d_S is referred to a $(n, M, d_S, k)_q$-code. The size M measures the efficiency of the code, the distance d_S is a measure of the error-correcting capability of the code. It would be nice if both M and d_S could be as large as possible.

A k-dimensional subspace $\mathcal{U}$ of $\mathbb{F}_q^{(n)}$ can be represented by a $k \times n$ generator matrix U whose rows form a basis of $\mathcal{U}$, i.e.,

$$\mathcal{U} = rs(U) := rowspace(U) \in \mathcal{G}_q(k, n).$$

The subspace distance on $\mathcal{G}_q(k, n)$ is also given by

$$d_S(\mathcal{U}, \mathcal{V}) = 2rank \begin{bmatrix} U \\ V \end{bmatrix} - 2k \tag{2}$$

for any $\mathcal{U}, \mathcal{V} \in \mathcal{G}_q(k, n)$ and some respective matrix representations U and V.

We focus on constant dimension codes arising from group actions, which are simply called orbit codes and which were introduced in [9].

The set of all invertible $n \times n$ matrices over $\mathbb{F}_q$ form a group with respect matrix multiplication, called the general linear group of degree n, is denoted by $GL_n(\mathbb{F}_q)$. Elements of $GL_n(\mathbb{F}_q)$ can be seen as linear transformations of $\mathbb{F}_q^{(n)}$. Multiplication by elements of $GL_n(\mathbb{F}_q)$ defines a group action from the right on $\mathcal{G}_q(k, n)$ by

$$\begin{aligned} \mathcal{G}_q(k,n) \times GL_n(\mathbb{F}_q) &\to \mathcal{G}_q(k,n) \\ (\mathcal{U}, A) &\mapsto \mathcal{U}A. \end{aligned}$$

Definition 3: ([9]) Let $\mathcal{U} \in \mathcal{G}_q(k, n)$ and G a subgroup of $GL_n(\mathbb{F}_q)$, then

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

is called an orbit code. Furthermore, the code $\mathcal{C}$ is said to be a cyclic orbit code if G is cyclic group.

Next we introduce the relative contents of unitary spaces over finite fields.

Let $\mathbb{F}_{q^2}$ be the finite field with q^2 elements (where q is a prime power). $\mathbb{F}_{q^2}$ has an involutive automorphism, i.e., an automorphism of order 2

$$\eta : \alpha \mapsto \overline{\alpha} = \alpha^q$$

and the fixed field of η is $\mathbb{F}_q$. A matrix H_n over $\mathbb{F}_{q^2}$ is said to be Hermitian, if ${}^t\overline{H_n} = H_n$.

Any $n \times n$ nonsingular Hermitian matrix over $\mathbb{F}_{q^2}$ is necessarily cogredient to the $n \times n$ identity matrix. And it is also cogredient to

$$H_{2v} = \begin{bmatrix} 0 & I^{(v)} \\ I^{(v)} & 0 \end{bmatrix}$$

or

$$H_{2v+1} = \begin{bmatrix} 0 & I^{(v)} & 0 \\ I^{(v)} & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

where v is the index of H_{2v} and H_{2v+1}.

Definition 4: ([20]) All $n \times n$ matrices over $\mathbb{F}_{q^2}$ satisfying $UH_n{}^t\overline{U} = H_n$ form a group with respect matrix multiplication, called the unitary group of degree n with respect to H_n, is denoted by $U_n(\mathbb{F}_{q^2})$. i.e.,

$$U_n(\mathbb{F}_{q^2}) = \{U \in GL_n(\mathbb{F}_{q^2}) | UH_n{}^t\overline{U} = H_n\}.$$

Definition 5: ([20]) $\mathbb{F}_{q^2}^{(n)}$ denotes the n-dimensional row vector space over $\mathbb{F}_{q^2}$. There is an action of $U_n(\mathbb{F}_{q^2})$ on $\mathbb{F}_{q^2}^{(n)}$ defined as follows

$$\begin{aligned} \mathbb{F}_{q^2}^{(n)} \times U_n(\mathbb{F}_{q^2}) &\rightarrow \mathbb{F}_{q^2}^{(n)} \\ ((x_1, x_2, \cdots, x_n), U) &\mapsto (x_1, x_2, \cdots, x_n)U. \end{aligned}$$

The vector space $\mathbb{F}_{q^2}^{(n)}$, with the above action of the unitary group $U_n(\mathbb{F}_{q^2})$, is called the n-dimensional unitary space over $\mathbb{F}_{q^2}$.

Let $\mathcal{U}$ be an m-dimensional vector subspace of $\mathbb{F}_{q^2}^{(n)}$, $U \in \mathbb{F}_{q^2}^{m \times n}$ is the matrix representation of $\mathcal{U}$, i.e., U is a $m \times n$ matrix of rank m whose rows form a basis of $\mathcal{U}$. For an $n \times n$ nonsingular Hermitian matrix H_n, it is clear that $UH_n{}^t\overline{U}$ is Hermitian. If $UH_n{}^t\overline{U}$ is of rank r, we say that $\mathcal{U}$ is a subspace of type (m, r) with respect to H_n. Clearly $r \leq m \leq n$. In Particular, subspaces of type $(m, 0)$ with respect to H_n are called m-dimensional totally isotropic subspaces with respect to H_n.

Denote by $\mathcal{M}(m, 0; n)$ the set of subspaces of $\mathbb{F}_{q^2}^{(n)}$ of type $(m, 0)$ with respect to H_n. Moreover, $\mathcal{U} \in \mathcal{M}(m, 0; n)$ if and only if $UH_n{}^t\overline{U} = 0$.

Theorem 1: ([21]) There is an embedding of $GL_n(\mathbb{F}_{q^2})$ in $U_{2n}(\mathbb{F}_{q^2})$. Moreover, if $h \in GL_n(\mathbb{F}_{q^2})$ and if H is the matrix representing h with respect to some basis, then there is a basis of $\mathbb{F}_{q^2}^{(2n)}$ such that h maps to the block matrix

$$\begin{bmatrix} H & 0 \\ 0 & {}^t\overline{(H^{-1})} \end{bmatrix}.$$

III. CONSTRUCTIONS OF CYCLIC ORBIT CODES BASE ON TOTALLY ISOTROPIC SUBSPACES IN UNITARY SPACE

In this section, we mainly give a construction of cyclic orbit codes based on n-dimensional totally isotropic subspaces in unitary space $\mathbb{F}_{q^2}^{(2n)}$. We begin by giving the following lemma.

Lemma 1: ([11, *Lemma* 32]) Let $g(x) = x^n + d_{n-1}x^{n-1} + \cdots + d_1x + d_0$ be an irreducible polynomial of degree n over $\mathbb{F}_{q^2}$, the companion matrix M_g of $g(x)$ is given by

$$M_g = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -d_0 & -d_1 & -d_2 & \cdots & -d_{n-1} \end{bmatrix} \in \mathbb{F}_{q^2}^{n \times n}.$$

Suppose that $\beta \in \mathbb{F}_{q^{2n}}$ be a root of $g(x)$, then

1) β is an irreducible element of $\mathbb{F}_{q^{2n}}$ and $\mathbb{F}_{q^{2n}}$ can be represented by

$$\mathbb{F}_{q^{2n}} \cong \mathbb{F}_{q^2}[x]/(g(x)) \cong \mathbb{F}_{q^2}[\beta] \cong \mathbb{F}_{q^2}[M_g].$$

2) The map

$$\begin{aligned} \varphi^{(n)} : \mathbb{F}_{q^2}^{(n)} &\rightarrow \mathbb{F}_{q^{2n}} \cong \mathbb{F}_{q^2}[\beta] \\ (u_1, u_2, \cdots, u_n) &\mapsto \sum_{i=0}^{n-1} u_{i+1}\beta^i \end{aligned}$$

is a vector space isomorphism. Furthermore, for all $u \in \mathbb{F}_{q^2}^{(n)}$ we get

$$\varphi^{(n)}(uM_g) = \varphi^{(n)}(u)\beta. \tag{3}$$

According to Lemma 1 and some known facts on primitive polynomials over finite fields [22], we have the following corollary.

Corollary 1: Let $g(x) \in \mathbb{F}_{q^2}[x]$ be a primitive polynomial of degree n, M_g, β and $\varphi^{(n)}$ are defined as in Lemma 1, it follows that

1) $g(M_g) = 0$, $g(x)$ is both a characteristic polynomial and minimal polynomial of M_g.
2) $ord(M_g) = ord(g(x)) = q^{2n} - 1$.
3) β is a primitive element of $\mathbb{F}_{q^2}^{(n)}$, i.e.,

$$\mathbb{F}_{q^{2n}}^* = \langle\beta\rangle = \{\beta^i | i = 0, 1, \cdots, q^{2n} - 2\}.$$

4) For all non-zero element $v \in \mathbb{F}_{q^2}^{(n)}$, there exists $i \in Z_{q^{2n}-1}$ such that

$$\varphi^{(n)}(v) = \beta^i.$$

In order to construct cyclic unitary subgroups of $GL_{2n}(\mathbb{F}_{q^2})$, we consider the following matrix of $GL_{2n}(\mathbb{F}_{q^2})$:

$$A = \begin{bmatrix} M_g & 0 \\ 0 & {}^t\overline{(M_g{}^{-1})} \end{bmatrix} \in \mathbb{F}_{q^2}^{2n \times 2n}, \tag{4}$$

where $g(x) \in \mathbb{F}_{q^2}[x]$ is a primitive polynomial of degree n and M_g is the companion matrix of $g(x)$.

Lemma 2: For the matrix $\underline{A\ \text{given}}$ by (4), let $h(x)$ be the characteristic polynomial of ${}^t\overline{(M_g^{-1})}$ over $\mathbb{F}_{q^2}$, then

1) $A \in U_{2n}(\mathbb{F}_{q^2})$ and $ord(A) = q^{2n} - 1$.
2) $h(x)$ is a primitive polynomial of degree n.

3) There exists $\varepsilon \in Z_{q^{2n}-1}$ such that $\overline{{}^t(M_g{}^{-1})} = M_h{}^{\varepsilon}$, where M_h is the companion matrix of $h(x)$.

Proof: 1) According to Theorem 1 and $AH_n{}^t\overline{A} = H_n$, where

$$H_n = \begin{bmatrix} 0 & I^{(n)} \\ I^{(n)} & 0 \end{bmatrix}.$$

We obtain $A \in U_{2n}(\mathbb{F}_{q^2})$. Since

$$\begin{aligned} ord(\overline{{}^t(M_g{}^{-1})}) &= ord(M_g) = ord(g(x)) \\ &= q^{2n} - 1, \end{aligned}$$

it follows that

$$\begin{aligned} ord(A) &= lcm\{ord(M_g), ord(\overline{{}^t(M_g{}^{-1})})\} \\ &= lcm\{q^{2n} - 1,\ q^{2n} - 1\} \\ &= q^{2n} - 1. \end{aligned}$$

2) Suppose that $h(x)$ be not irreducible, we can assume that

$$h(x) = f_1(x)f_2(x)\cdots f_k(x),$$

where $f_i(x) \in \mathbb{F}_{q^2}[x]$ is irreducible, $k \geq 2$. For any $i = 1, 2, \cdots, k$, we have

$$1 \leq deg(f_i(x)) < n, \quad ord(f_i(x)) < q^{2n} - 1.$$

Since $h(\overline{{}^t(M_g{}^{-1})}) = 0$, it follows that there exists i such that

$$f_i(\overline{{}^t(M_g{}^{-1})}) = 0,$$

which contradicts to $ord(\overline{{}^t(M_g{}^{-1})}) = q^{2n} - 1$. Hence, $h(x)$ is an irreducible polynomial of degree n. Since

$$h(\overline{{}^t(M_g{}^{-1})}) = 0$$

and

$$ord(\overline{{}^t(M_g{}^{-1})}) = q^{2n} - 1,$$

thus $h(x)$ is a primitive polynomial of degree n.

3) Since $h(x)$ is a primitive polynomial, and

$$h(\overline{{}^t(M_g{}^{-1})}) = 0, \quad h(M_h{}^{\varepsilon}) = 0,$$

it follows that there exists $\varepsilon \in Z_{q^{2n}-1}$ such that

$$\overline{{}^t(M_g{}^{-1})} = M_h{}^{\varepsilon}.$$

■

Construction 1: Consider the group $G = \langle A \rangle$, then

$$G = \left\{ \begin{bmatrix} M_g{}^l & 0 \\ 0 & (\overline{{}^t(M_g{}^{-1})})^l \end{bmatrix} | l = 0, 1, \cdots, q^{2n} - 2 \right\},$$

that is, G is a cyclic unitary group of order $q^{2n} - 1$. Let

$$\mathcal{V} = rs[V_1\ V_2] \in \mathcal{M}(n, 0; 2n),$$

where $V = [V_1\ \ V_2]$ is the matrix representation of subspace $\mathcal{V}$ and $V_1, V_2 \in \mathbb{F}_{q^2}^{n\times n}$. Let

$$\begin{aligned} \mathcal{C}(n, 0, 2n) &= \mathcal{V}\langle A \rangle \\ &= \{\mathcal{V}A^l | l = 0, 1, \cdots, q^{2n} - 2\} \\ &= \{rs[V_1M_g{}^l\ V_2(\overline{{}^t(M_g{}^{-1})})^l]| \\ &\qquad l = 0, 1, \cdots, q^{2n} - 2\}. \end{aligned} \tag{5}$$

Then $\mathcal{C}(n, 0, 2n)$ is the unitary cyclic orbit code generated by the action of group G on subspace $\mathcal{V}$. The code $\mathcal{C}(n, 0, 2n)$ has size

$$|\mathcal{C}(n, 0, 2n)| = \frac{ord(A)}{|Stab_A(\mathcal{V})|},$$

where $Stab_A(\mathcal{V}) = \{A^l | \mathcal{V}A^l = \mathcal{V}, 0 \leq l < q^{2n} - 1\}$, and the minimum distance

$$d_S(\mathcal{C}(n, 0, 2n)) = \min_{1\leq l\leq q^{2n}-2} \{d_S(\mathcal{V}, \mathcal{V}A^l)\}.$$

The following Lemma is convenient for calculating the minimum distance of $\mathcal{C}(n, 0, 2n)$.

Lemma 3: Let β_1, β_2 be primitive elements of $\mathbb{F}_{q^2}^{(n)}$, suppose that

$$\begin{aligned} &\varphi^{(n,n)} : \mathbb{F}_{q^2}^{(2n)} \to \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}} \\ &(v_{i_1}, \cdots, v_{i_{2n}}) \mapsto (\varphi_1^{(n)}(v_{i_1}, \cdots, v_{i_n}), \varphi_2^{(n)}(v_{i_{n+1}}, \cdots, v_{i_{2n}})), \end{aligned}$$

where

$$\begin{aligned} \varphi_1^{(n)} : \mathbb{F}_{q^2}^{(n)} &\to \mathbb{F}_{q^{2n}} \cong \mathbb{F}_{q^2}[\beta_1] \\ (v_{i_1}, \cdots, v_{i_n}) &\mapsto \sum_{j=0}^{n-1} v_{i_{j+1}}\beta_1^j \end{aligned}$$

and

$$\begin{aligned} \varphi_2^{(n)} : \mathbb{F}_{q^2}^{(n)} &\to \mathbb{F}_{q^{2n}} \cong \mathbb{F}_{q^2}[\beta_2] \\ (v_{i_{n+1}}, \cdots, v_{i_{2n}}) &\mapsto \sum_{j=n}^{2n-1} v_{i_{j+1}}\beta_2^j \end{aligned}$$

It follows that

1) $\varphi^{(n,n)}$ is a vector space isomorphism.
2) For any non-zero element $v_i = (v_{i_1}, \cdots, v_{i_{2n}}) \in \mathbb{F}_{q^2}^{(2n)}$, there exists $k_i, k_i{}' \in Z_{q^{2n}-1}$ such that

$$\varphi^{(n,n)}(v_i) = \begin{cases} (\beta_1^{k_i}, \beta_2^{k_i{}'}), & if\, \varphi_i^{(n)}(v_i) \neq 0, \\ (\beta_1^{k_i}, 0), & if\, v_{i_{n+1}} = \cdots = v_{i_{2n}}, \\ (0, \beta_2^{k_i{}'}), & if\, v_{i_1} = \cdots = v_{i_n}. \end{cases}$$

Moreover, $u_i = v_iA^l$ for some $u_i, v_i \in \mathbb{F}_{q^2}^{(2n)} \backslash \{0\}$ if and only if

$$\varphi^{(n,n)}(u_i) = \begin{cases} (\beta_1^{k_i+l}, \beta_2^{k_i{}'+l+\varepsilon}), & if\, \varphi_i^{(n)}(v_i) \neq 0, \\ (\beta_1^{k_i+l}, 0), & if\, v_{i_{n+1}} = \cdots = v_{i_{2n}}, \\ (0, \beta_2^{k_i{}'+l+\varepsilon}), & if\, v_{i_1} = \cdots = v_{i_n}. \end{cases}$$

where $\varepsilon \in Z_{q^{2n}-1}$ such that $\overline{{}^t(M_g{}^{-1})} = M_h{}^{\varepsilon}$.

Proof: 1) If β_1, β_2 are irreducible elements of $\mathbb{F}_{q^2}^{(n)}$, then by Lemma 1, $\varphi_1^{(n)}, \varphi_2^{(n)}$ are vector space isomorphisms. Moreover, according to (3), we get

$$\varphi_1^{(n)}((v_{i_1}, \cdots, v_{i_n})M_g) = \varphi_1^{(n)}(v_{i_1}, \cdots, v_{i_n})\beta_1.$$

$$\varphi_2^{(n)}((v_{i_{n+1}},\cdots,v_{i_{2n}})^t\overline{(M_g{}^{-1})}) = \varphi_2^{(n)}(v_{i_{n+1}},\cdots,v_{i_{2n}})\beta_2^{\varepsilon}.$$

Therefore, $\varphi^{(n,n)}$ is a vector space isomorphism.

2) For any $v_i = (v_{i_1},\cdots,v_{i_{2n}}) \in \mathbb{F}_{q^2}^{(2n)}\backslash\{0\}$, we then have

$$\begin{aligned}\varphi^{(n,n)}(v_iA^l) &= \varphi^{(n,n)}(((v_{i_1},\cdots,v_{i_n})M_g{}^l),\\ &\quad ((v_{i_{n+1}},\cdots,v_{i_{2n}})({}^t\overline{(M_g{}^{-1})})^l))\\ &= (\varphi_1^{(n)}((v_{i_1},\cdots,v_{i_n})M_g{}^l),\\ &\quad \varphi_2^{(n)}((v_{i_{n+1}},\cdots,v_{i_{2n}})({}^t\overline{(M_g{}^{-1})})^l)\\ &= (\varphi_1^{(n)}((v_{i_1},\cdots,v_{i_n})M_g{}^l),\\ &\quad \varphi_2^{(n)}((v_{i_{n+1}},\cdots,v_{i_{2n}})M_h{}^{l+\varepsilon}))\\ &= (\varphi_1^{(n)}(v_{i_1},\cdots,v_{i_n})\beta_1^l,\\ &\quad \varphi_2^{(n)}(v_{i_{n+1}},\cdots,v_{i_{2n}})\beta_2^{l+\varepsilon}).\end{aligned}$$

In Particular, if β_1, β_2 are primitive elements of $\mathbb{F}_{q^2}^{(n)}$, we obtain the desired result by Corollary 1. ■

Lemma 4: Let $\mathcal{V} = \{0, v_1, \cdots, v_{q^{2n}-1}\} \in \mathcal{M}(n, 0; 2n)$ and $\mathcal{V} = \bigcup_{i=1}^{3} W_i$, where

$$\begin{aligned}W_1 &= \{v_i \in \mathbb{F}_{q^2}^{(2n)}\backslash\{0\} |\ \varphi^{(n,n)}(v_i) = (\beta_1^{k_i}, \beta_2^{k_i{}'})\},\\ W_2 &= \{v_i \in \mathbb{F}_{q^2}^{(2n)}\backslash\{0\} |\ \varphi^{(n,n)}(v_i) = (\beta_1^{k_i}, 0)\},\\ W_3 &= \{v_i \in \mathbb{F}_{q^2}^{(2n)}\backslash\{0\} |\ \varphi^{(n,n)}(v_i) = (0, \beta_2^{k_i{}'})\}.\end{aligned}$$

For any $v_s, v_t \in \mathcal{V}$, if

$$v_sA^l = v_t \quad \forall l \in \{1, 2, \cdots, q^{2n} - 2\},$$

it follows that $v_s, v_t \in W_1,\ or\ v_s, v_t \in W_2,\ or\ v_s, v_t \in W_3$.

Proof: Let

$$\begin{aligned}\Phi_1 : \mathbb{F}_{q^2}^{(2n)} &\to \mathbb{F}_{q^2}^{(n)}\\ (v_{i_1},\cdots,v_{i_n},v_{i_{n+1}},\cdots,v_{i_{2n}}) &\mapsto (v_{i_1},\cdots,v_{i_n})\end{aligned}$$

and

$$\begin{aligned}\Phi_2 : \mathbb{F}_{q^2}^{(2n)} &\to \mathbb{F}_{q^2}^{(n)}\\ (v_{i_1},\cdots,v_{i_n},v_{i_{n+1}},\cdots,v_{i_{2n}}) &\mapsto (v_{i_{n+1}},\cdots,v_{i_{2n}}).\end{aligned}$$

For any $v_s \in \mathcal{V}$, we have

$$\Phi_1(v_sA^l) = \Phi_1(v_s)M_g{}^l,$$

and

$$\Phi_2(v_sA^l) = \Phi_2(v_s)({}^t\overline{(M_g{}^{-1})})^l.$$

Suppose that $v_s \in W_1$, then $\Phi_1(v_s) \neq 0, \Phi_2(v_s) \neq 0$. It follows that

$$\Phi_1(v_sA^l) \neq 0, \quad \Phi_2(v_sA^l) \neq 0,$$

which implies that $v_sA^l \in W_1$, that is, $v_t \in W_1$. Other cases can be proved similarly. ■

For derive the following theorem, we recall that a multiset is a generalization of the notion of set in which members are allowed to appear more than once. We will denote multisets by $\{\{\cdots\}\}$. The number of times an element x appears in the multiset X, denoted by $m_X(x)$, is call its multiplicity (see [11]).

Theorem 2: Let $\mathcal{V} = \{0, v_1, \cdots, v_{q^{2n}-1}\} \in \mathcal{M}(n, 0; 2n)$, consider the difference sets

$$\begin{aligned}D_1 &= \{\{(\lambda_{(s,t)}\ mod\ (q^{2n}-1), \lambda'_{(s,t)}\ mod\ (q^{2n}-1))|\\ &\qquad v_s, v_t \in W_1, s \neq t, \lambda_{(s,t)} + \varepsilon \equiv \lambda'_{(s,t)} mod(q^{2n}-1)\}\},\\ D_2 &= \{\{(\lambda_{(s,t)}\ mod\ (q^{2n}-1), l)|\ v_s, v_t \in W_2, s \neq t,\\ &\qquad l = 1, \cdots, q^{2n}-1, \lambda_{(s,t)} \equiv l\ mod\ (q^{2n}-1)\}\},\\ D_3 &= \{\{(l, \lambda'_{(s,t)}\ mod\ (q^{2n}-1))|\ v_s, v_t \in W_3, s \neq t,\\ &\qquad l = 1, \cdots, q^{2n}-1, l + \varepsilon \equiv \lambda'_{(s,t)}\ mod\ (q^{2n}-1)\}\}\end{aligned}$$

and

$$D = \bigcup_{i=1}^{3} D_i.$$

where $\lambda_{(s,t)} = k_s - k_t,\ \lambda'_{(s,t)} = k_s{}' - k_t{}'$. Suppose that

$$d = \log_{q^2}(\max\{m_D(\lambda_1, \lambda_2)|(\lambda_1, \lambda_2) \in D\} + 1).$$

where $m_D(\lambda_1, \lambda_2)$ denote the number of times pair (λ_1, λ_2) appears in the multiset D. If $d < n$, then $\mathcal{C}(n, 0, 2n)$ is an $(2n, q^{2n} - 1, 2n - 2d, n)$ unitary cyclic orbit code. In particular, if $D = \emptyset$, $\mathcal{C}(n, 0, 2n)$ is a partial spread in $\mathbb{F}_{q^2}^{(2n)}$.

Proof: First we compute the minimal distance of $\mathcal{C}(n, 0, 2n)$, which is

$$\min\{d_S(\mathcal{V}, \mathcal{V}A^l)\}, \quad \forall l = 1, \cdots, q^{2n} - 1.$$

By (1), we should consider the value of

$$dim(\mathcal{V} \cap \mathcal{V}A^l),$$

for all $1 \leq l \leq q^{2n} - 1$. Let $v_s \in \mathcal{V}$, then $v_s \in \mathcal{V}A^l$ if and only if there exists $v_t \in \mathcal{V}$ such that

$$v_s = v_tA^l.$$

In the sense of isomorphism, it follows that

$$\varphi^{(n,n)}(v_s) = \varphi^{(n,n)}(v_tA^l).$$

According to Lemma 4, $\{W_i|i = 1, 2, 3\}$ is a partition of $\mathcal{V}$. We will consider three cases.

Case 1. If $v_s \in W_1$, then $v_s \in W_1A^l$ if and only if there exists $v_t \in W_1$ such that

$$(\beta_1^{k_s}, \beta_2^{k_s{}'}) = (\beta_1^{k_t+l}, \beta_2^{k_t{}'+l+\varepsilon}),$$

for any $t \in \{1, \cdots, q^{2n} - 1\}$. Equivalently,

$$k_s \equiv k_t + l\ mod\ (q^{2n} - 1)$$

and

$$k_s{}' \equiv k_t{}' + l + \varepsilon\ mod\ (q^{2n} - 1).$$

That is,

$$\lambda_{(s,t)} \equiv l\ mod\ (q^{2n} - 1)$$

and

$$\lambda'_{(s,t)} \equiv l + \varepsilon \ mod \ (q^{2n} - 1),$$

and it follows that

$$\lambda_{(s,t)} + \varepsilon \equiv \lambda'_{(s,t)} \ mod \ (q^{2n} - 1).$$

Therefore,

$$(\lambda_{(s,t)} \ mod \ (q^{2n} - 1), \lambda'_{(s,t)} \ mod \ (q^{2n} - 1)) \in D_1.$$

Case 2. If $v_s \in W_2$, then $v_s \in W_2 A^l$ if and only if there exists $v_t \in W_2$ such that

$$(\beta_1^{k_s}, 0) = (\beta_1^{k_t + l}, 0),$$

for any $t \in \{1, \cdots, q^{2n} - 1\}$. Equivalently,

$$k_s \equiv k_t + l \ mod \ (q^{2n} - 1),$$

and then

$$\lambda_{(s,t)} \equiv l \ mod \ (q^{2n} - 1).$$

Hence,

$$(\lambda_{(s,t)} \ mod \ (q^{2n} - 1), l) \in D_2.$$

Case 3. If $v_s \in W_3$, then $v_s \in W_3 A^l$ if and only if there exists $v_t \in W_3$ such that

$$(0, \beta_2^{k_s'}) = (0, \beta_2^{k_t' + l + \varepsilon}),$$

for any $t \in \{1, \cdots, q^{2n} - 1\}$. Equivalently,

$$k_s' \equiv k_t' + l + \varepsilon \ mod \ (q^{2n} - 1),$$

and we have that

$$\lambda'_{(s,t)} \equiv l + \varepsilon \ mod \ (q^{2n} - 1).$$

Thus,

$$(l, \lambda'_{(s,t)} \ mod \ (q^{2n} - 1)) \in D_3.$$

Since $\max\{m_D(\lambda_1, \lambda_2) | (\lambda_1, \lambda_2) \in D\} = q^{2d} - 1$, we then have

$$|\mathcal{V} \cap \mathcal{V}A^l| \leq q^{2d},$$

for any $l \in \{1, \cdots, q^{2n} - 2\}$. This shows that

$$dim(\mathcal{V} \cap \mathcal{V}A^l) \leq d. \tag{6}$$

Using (1),

$$d_S(\mathcal{V}, \mathcal{V}A^l) \geq 2n - 2d.$$

Therefore,

$$d_S(\mathcal{C}(n, 0, 2n)) = 2n - 2d.$$

Note that if $d < n$, then $\mathcal{V}A^l$ are distinct for any $l \in \{1, \cdots, q^{2n} - 2\}$. It follows that

$$Stab_A(\mathcal{V}) = \{I_{2n}\}.$$

Therefore,

$$|\mathcal{C}(n, 0, 2n)| = q^{2n} - 1.$$

In particular, if $D = \emptyset$, we have that

$$\mathcal{V} \cap \mathcal{V}A^l = \{0\},$$

for any $l \in \{1, \cdots, q^{2n} - 2\}$, and thus

$$d_S(\mathcal{C}(n, 0, 2n)) = 2n.$$

Hence, $\mathcal{C}(n, 0, 2n)$ is a partial spread in $\mathbb{F}_{q^2}^{(2n)}$. ■

Corollary 2: Let $d = n$ in Theorem 2. Suppose that

$$D' = \{\{(\lambda_1, \lambda_2) \in D | m_D(\lambda_1, \lambda_2) < q^{2n} - 1\}\}$$

and

$$d' = \log_{q^2}(\max\{m_{D'}(\lambda_1, \lambda_2) | (\lambda_1, \lambda_2) \in D'\} + 1),$$

where $\lambda_1 \equiv l_i \, mod \, (q^{2n} - 1)$, for $i = 1, 2, \cdots, s$. Then $\mathcal{C}(n, 0, 2n)$ is an unitary cyclic orbit code of size $\gcd(lcm\{l_1, l_2, \cdots, l_s\}, q^{2n} - 1)$ and minimal distance $2n - 2d'$.

Proof: Assume that (λ_1, λ_2) such that

$$m_D(\lambda_1, \lambda_2) = q^{2n} - 1,$$

we obtain

$$\mathcal{V} = \mathcal{V}A^{l_i}, \quad \lambda_1 \equiv l_i \ mod \ (q^{2n} - 1),$$

for $i = 1, 2, \cdots, s$. This leads to

$$\begin{aligned} Stab_A(\mathcal{V}) &= \langle A^{l_1}, A^{l_2}, \cdots, A^{l_s} \rangle \\ &= \langle A^{lcm\{l_1, l_2, \cdots, l_s\}} \rangle, \end{aligned}$$

and

$$|Stab_A(\mathcal{V})| = \frac{q^{2n} - 1}{\gcd(lcm\{l_1, l_2, \cdots, l_s\}, q^{2n} - 1)}.$$

Therefore,

$$|\mathcal{C}(n, 0, 2n)| = \gcd(lcm\{l_1, l_2, \cdots, l_s\}, q^{2n} - 1).$$

Since the minimum distance of $\mathcal{C}(n, 0, 2n)$ is only taken between two distinct vector spaces, it follows that

$$|\mathcal{V} \cap \mathcal{V}A^l| < q^{2n},$$

for any $l \in \{1, \cdots, q^{2n} - 2\}$. We can assume, therefore, that

$$D' = \{\{(\lambda_1, \lambda_2) \in D | m_D(\lambda_1, \lambda_2) < q^{2n} - 1\}\}$$

and

$$\max\{m_{D'}(\lambda_1, \lambda_2) | (\lambda_1, \lambda_2) \in D'\} = q^{2d'} - 1.$$

As we have done in the proof of Theorem 2, we conclude that

$$d_S(\mathcal{C}(n, 0, 2n)) = 2n - 2d'.$$

■

Example 1: Consider field

$$\mathbb{F}_{2^6} = \mathbb{F}_2[x]/(x^6 + x + 1).$$

Let β be a root of $x^6 + x + 1 = 0$, and let $g(x)$ be a minimal polynomial of β over $\mathbb{F}_4$. Since $x^6 + x + 1$ is a primitive polynomial of degree 6 over $\mathbb{F}_2$, it follows from Corollary 1 that β is a primitive element of $\mathbb{F}_{2^6}$. We then have

$$\begin{aligned} g(x) &= (x-\beta)(x-\beta^4)(x-\beta^{4^2}) \\ &= x^3 - x^2 + (\beta^5+\beta^4+\beta^3+\beta)x^2 \\ &\quad - (\beta^5+\beta^4+\beta^3+\beta+1). \end{aligned}$$

Set $\lambda = \beta^5+\beta^4+\beta^3+\beta$, then $\lambda^2 = \lambda + 1$. Note that λ is a root of irreducible polynomial x^2+x+1 over $\mathbb{F}_2$, and thus

$$\begin{aligned} \mathbb{F}_4 &= \mathbb{F}_2[x]/(x^2+x+1) \\ &= \{c_0 + c_1\lambda \mid c_0, c_1 \in \mathbb{F}_2\}. \end{aligned}$$

Therefore, $g(x) = x^3 + x^2 + \lambda x + \lambda + 1$ is a primitive polynomial of degree 3 over $\mathbb{F}_4$.

The companion matrix of $g(x)$ is the matrix

$$M_g = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \lambda+1 & \lambda & 1 \end{bmatrix},$$

it follows that

$${}^t(M_g{}^{-1}) = \begin{bmatrix} \lambda+1 & 1 & 0 \\ \lambda & 0 & 1 \\ \lambda & 0 & 0 \end{bmatrix}.$$

By $\alpha \mapsto \overline{\alpha} = \alpha^2$, we get

$${}^t\overline{(M_g{}^{-1})} = \begin{bmatrix} \lambda & 1 & 0 \\ \lambda+1 & 0 & 1 \\ \lambda+1 & 0 & 0 \end{bmatrix}.$$

Let $h(x)$ be the characteristic polynomial of ${}^t\overline{(M_g^{-1})}$, then

$$h(x) = x^3 + \lambda x^2 + (\lambda+1)x + \lambda + 1$$

and $h(x)$ is a primitive polynomial of degree 3 over $\mathbb{F}_4$.

Suppose that

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ \lambda+1 & \lambda & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda & 1 & 0 \\ 0 & 0 & 0 & \lambda+1 & 0 & 1 \\ 0 & 0 & 0 & \lambda+1 & 0 & 0 \end{bmatrix} \in U_6(\mathbb{F}_4),$$

and

$$\mathcal{V} = rs \begin{bmatrix} \lambda+1 & 0 & 1 & \lambda+1 & 0 & 1 \\ 0 & \lambda & 1 & 0 & \lambda & 1 \\ \lambda+1 & 1 & 0 & \lambda+1 & 1 & 0 \end{bmatrix} \in \mathcal{M}(3,0,6).$$

Then $\langle A \rangle$ is a cyclic unitary group of order 63. Since $\mathcal{V}A^l$ are distinct for any $l \in \{0, 1, \cdots, 62\}$, it follows that

$$\begin{aligned} Stab_A(\mathcal{V}) &= \{A^l \mid \mathcal{V}A^l = \mathcal{V}, 0 \le l < 63\} \\ &= \{I_6\}. \end{aligned}$$

Let

$$\mathcal{C}(3,0,6) = \{\mathcal{V}A^l \mid l = 0, 1, \cdots, 62\},$$

we have that

$$|\mathcal{C}(3,0,6)| = \frac{ord(A)}{|Stab_A(\mathcal{V})|} = 63.$$

Since $\mathcal{V} \neq \mathcal{V}A^l$, it follows that

$$3 < rank \begin{bmatrix} V \\ VA^l \end{bmatrix} \le 6$$

and we can calculate that

$$rank \begin{bmatrix} V \\ VA^l \end{bmatrix} = 5 \text{ or } 6,$$

for any $l \in \{0, 1, \cdots, 62\}$. Using (2), we get

$$rank \begin{bmatrix} V \\ VA^l \end{bmatrix} = 6 - dim(\mathcal{V} \cap \mathcal{V}A^l).$$

This lead to $dim(\mathcal{V} \cap \mathcal{V}A^l) \le 1$, and $d = 1$. By Theorem 2, thus

$$d_S(\mathcal{C}(3,0,6)) = 6 - 2d = 4.$$

Therefore, $\mathcal{C}(3,0,6)$ is an $(6, 63, 4, 3)$ unitary cyclic orbit code. ■

IV. CONSTRUCTIONS OF ORBIT CODES USING THE EXTERNAL DIRECT PRODUCT OF UNITARY GROUPS

In this section, we present a construction of how to use the external direct product of unitary groups to construct orbit codes with longer length. We need the following notation.

Definition 6: Let $U_{2n_i}(\mathbb{F}_{q^2})(i = 1, 2, \cdots, m)$ be m unitary groups. Suppose that

$$\begin{aligned} G &= U_{2n_1}(\mathbb{F}_{q^2}) \times U_{2n_2}(\mathbb{F}_{q^2}) \times \cdots \times U_{2n_m}(\mathbb{F}_{q^2}) \\ &= \{(A_1, A_2, \cdots, A_m) \mid A_i \in U_{2n_i}(\mathbb{F}_{q^2})\} \end{aligned}$$

and define the multiplication in G as follows

$$AB = (A_1B_1, \cdots, A_mB_m),$$

where

$$A = (A_1, \cdots, A_m), B = (B_1, \cdots, B_m) \in G,$$

then G form a group with respect matrix multiplication as defined above, called the external direct product of groups $U_{2n_1}(\mathbb{F}_{q^2}), \cdots, U_{2n_m}(\mathbb{F}_{q^2})$.

Construction 2: For $i = 1, 2, \cdots, m$, let $\mathcal{V}_i = rs(V_i) \in \mathcal{M}(n_i, 0, 2n_i)$, $G_i = \langle A_i \rangle \in U_{2n_i}(\mathbb{F}_{q^2})$ and

$$\mathcal{C}(n_i, 0, 2n_i) = \mathcal{V}_i G_i,$$

where $V_i \in \mathbb{F}_{q^2}^{n_i \times 2n_i}$. Suppose that

$$\mathcal{V} = \mathcal{V}_1 \oplus \mathcal{V}_2 \oplus \cdots \oplus \mathcal{V}_m \in \mathcal{M}(n, 0, 2n)$$

and

$$G = G_1 \times G_2 \times \cdots \times G_m \le GL_{2n}(\mathbb{F}_{q^2}).$$

Let $d_i = \log_{q^2}(\max\{m_{D_i}(\lambda_1, \lambda_2) \mid (\lambda_1, \lambda_2) \in D_i\} + 1)$ and $d_i < n_i$, where $n = \sum_{i=1}^{m} n_i$. Then

$$\mathcal{C}(n, 0, 2n) = \mathcal{V}G$$

is an $(2n, M, d_S, n)$ unitary orbit code, where $M = \prod_{i=1}^{m}(q^{2n_i} - 1)$, $d_S \geq \min_{i\in\{1,\cdots,m\}}\{2n_i - 2d_i\}$.

Proof: According to Theorem 2, $\mathcal{C}(n_i, 0, 2n_i)$ is an $(2n_i, q^{2n_i} - 1, 2n_i - 2d_i, n_i)$ unitary cyclic orbit code.

Now we consider $G = \{(A_1, \cdots, A_m) | A_i \in G_i\}$, and define A by

$$\begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_m \end{bmatrix},$$

for $A = (A_1, \cdots, A_m) \in G$. Since $G_i \in U_{2n_i}(\mathbb{F}_{q^2})(i = 1, \cdots, m)$ is finite group, it follows that

$$|G| = \prod_{i=1}^{m} |G_i| = \prod_{i=1}^{m}(q^{2n_i} - 1),$$

and hence G is an unitary group of order $\prod_{i=1}^{m}(q^{2n_i}-1)$. Suppose that

$$\begin{aligned} \mathcal{V} &= \mathcal{V}_1 \oplus \cdots \oplus \mathcal{V}_m \\ &= rs \begin{bmatrix} V_1 & & \\ & \ddots & \\ & & V_m \end{bmatrix} \in \mathcal{M}(n, 0, 2n), \end{aligned}$$

where V_i is the matrix representation of subspace $\mathcal{V}_i$, and then

$$\mathcal{V}A^l = rs \begin{bmatrix} V_1A_1^l & & \\ & \ddots & \\ & & V_mA_m^l \end{bmatrix}.$$

Note that $V_i \neq V_iA_i^l$ for any $l \in \{1, 2, \cdots, q^{2n_i} - 2\}$, we then have

$$Stab_{G_i}(\mathcal{V}_i) = \{I_{2n_i}\}.$$

This leads to

$$\begin{aligned} Stab_G(\mathcal{V}) &= Stab_{G_1}(\mathcal{V}_1) \times \cdots \times Stab_{G_m}(\mathcal{V}_m) \\ &= \{I_{2n_1}\} \times \cdots \times \{I_{2n_m}\} \\ &= \{I_{2n}\}. \end{aligned}$$

Therefore,

$$|\mathcal{C}(n, 0, 2n)| = \frac{|G|}{|Stab_G(\mathcal{V})|} = \prod_{i=1}^{m}(q^{2n_i} - 1).$$

By (2) and (6), we have

$$\begin{aligned} rank \begin{bmatrix} V_i \\ V_iA_i^l \end{bmatrix} &= 2n_i - dim(\mathcal{V}_i \cap \mathcal{V}_iA_i^l) \\ &\geq 2n_i - 2d_i. \end{aligned}$$

for any $1 \leq l < q^{2n_i} - 1$.

For $1 \leq l < \prod_{i=1}^{m}(q^{2n_i} - 1) - 1$, then there exist $\gamma_i \in \{0, 1, \cdots, q^{2n_i} - 2\}$ such that

$$l = \gamma_i \ mod\ (q^{2n_i} - 1) \quad and \quad \gamma_i \neq 0.$$

Furthermore, we obtain

$$\begin{aligned} d_S(\mathcal{V}, \mathcal{V}A^l) &= 2rank \begin{bmatrix} V \\ VA^l \end{bmatrix} - 2n \\ &= 2rank \begin{bmatrix} V_1 & & \\ & \ddots & \\ & & V_m \\ V_1A_1^l & & \\ & \ddots & \\ & & V_mA_m^l \end{bmatrix} - 2n \\ &= 2(rank \begin{bmatrix} V_i \\ V_iA_i^l \end{bmatrix} + \sum_{\substack{j=1 \\ j\neq i}}^{m} rank \begin{bmatrix} V_j \\ V_jA_j^l \end{bmatrix}) - 2n \\ &\geq 2(2n_i - d_i + \sum_{j=1}^{m} n_j - n_i) - 2n \\ &= 2(n + n_i - d_i) - 2n \\ &= 2n_i - 2d_i = d_S(\mathcal{C}(n_i, 0, 2n_i)). \end{aligned}$$

Therefore,

$$d_S(\mathcal{C}(n, 0, 2n)) \geq \min_{i\in\{1,\cdots,m\}}\{2n_i - 2d_i\}.$$

■

As a straightforward corollary of Construction 2, we have the following result.

Corollary 3: In Construction 2, let $\mathcal{V}_1 = \cdots = \mathcal{V}_m$, $A_1 = \cdots = A_m$, then $\mathcal{C}(n, 0, 2n)$ is a non-cyclic orbit code of size $(q^{2n_1} - 1)^m$ and minimal distance $2m(n_1 - d_1)$.

Proof: Since $A_1 = \cdots = A_m$, it imply that $n_1 = \cdots = n_m$, we now assume that $n = mn_1$, then

$$\gcd(q^{2n_1} - 1, \cdots, q^{2n_m} - 1) = q^{2n_1} - 1 \neq 1.$$

and hence G is a non-cyclic unitary group of order $(q^{2n_1}-1)^m$. It follows that

$$|\mathcal{C}(n, 0, 2n)| = (q^{2n_1} - 1)^m.$$

For $1 \leq l < q^{2n_1} - 1$, we have

$$\begin{aligned} d_S(\mathcal{V}, \mathcal{V}A^l) &= 2rank \begin{bmatrix} V_1 & & \\ & \ddots & \\ & & V_m \\ V_1A_1^l & & \\ & \ddots & \\ & & V_mA_m^l \end{bmatrix} - 2n \\ &= 2rank(\begin{bmatrix} V_1 \\ V_1A_1^l \end{bmatrix} + \cdots + \begin{bmatrix} V_1 \\ V_1A_1^l \end{bmatrix}) - 2mn_1 \\ &= m(2rank \begin{bmatrix} V_1 \\ V_1A_1^l \end{bmatrix} - 2n_1) \\ &\geq md_S(\mathcal{C}(n_1, 0, 2n_1)). \end{aligned}$$

Since there exists $1 \leq l_0 < q^{2n_1} - 1$ such that

$$d_S(\mathcal{V}, \mathcal{V}A^{l_0}) = d_S(\mathcal{C}(n_1, 0, 2n_1)),$$

and thus

$$d_S(\mathcal{C}(n, 0, 2n)) = 2m(n_1 - d_1).$$

■

Trautmann *et al.* [11] investigated cyclic orbit codes in the Grassmannian in detail. Poroch and Talebi [16] constructed orbit codes based on the Lagrangian Grassmannian in symplectic spaces over finite fields. The TABLE 1 gives a comparison with codes from [11], [16] and this paper. We can see that our codes have larger size without decreasing the distance. In summary, our proposed codes have better error-correcting performance than [11], [16].

V. CONCLUSION

We present two constructions of orbit codes based on totally isotropic subspaces in unitary spaces $\mathbb{F}_{q^2}^{(n)}$ over finite fields in this paper. Our results improves Poroch *et al.* in two directions: Firstly, the size of cyclic orbit code can be increased up to $q^{2n} - 1$ without decreasing the minimum distance $2n - 2d$ in Theorem 2; secondly, we enlarge the code size $\prod_{i=1}^{m}(q^{2n_i} - 1)$ using the external direct product of unitary groups in Construction 2. We hope these construction methods can provide some inspirations for constructing other constant dimension codes. For further research, we are looking forward to finding efficient decoding algorithms of these codes in the paper. Furthermore, an open question is to find systematic ways to take unions of cyclic orbit codes without decreasing the distance.

REFERENCES

[1] R. Koetter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3579–3591, Aug. 2008.

[2] D. Silva, F. R. Kschischang, and R. Koetter, "A rank-metric approach to error control in random network coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 3951–3967, Sep. 2008.

[3] L. Xu and H. Chen, "New constant-dimension subspace codes from maximum rank distance codes," *IEEE Trans. Inf. Theory*, vol. 64, no. 9, pp. 6315–6319, Sep. 2018.

[4] D. Heinlein, "New LMRD code bounds for constant dimension codes and improved constructions," *IEEE Trans. Inf. Theory*, vol. 65, no. 8, pp. 4822–4830, Aug. 2019.

[5] H. G. Luerssen and C. Troha, "Construction of subspace codes through linkage," *Adv. Math. Commun.*, vol. 10, no. 3, pp. 525–540, 2017.

[6] N. Silberstein and A.-L. Trautmann, "Subspace codes based on graph matchings, Ferrers diagrams, and pending blocks," *IEEE Trans. Inf. Theory*, vol. 61, no. 7, pp. 3937–3953, Jul. 2015.

[7] F. Li, "Construction of constant dimension subspace codes by modifying linkage construction," *IEEE Trans. Inf. Theory*, vol. 66, no. 5, pp. 2760–2764, May 2020.

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

[9] A.-L. Trautmann, F. Manganiello, and J. Rosenthal, "Orbit codes—A new concept in the area of network coding," in *Proc. IEEE Inf. Theory Workshop*, Aug. 2010, pp. 1–4.

[10] J. Rosenthal and A.-L. Trautmann, "A complete characterization of irreducible cyclic orbit codes and their Plücker embedding," *Des., Codes Cryptogr.*, vol. 66, nos. 1–3, pp. 275–289, Jan. 2013.

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

[12] H. G. Luerssen, K. Morrison, and C. Troha, "Cyclic orbit codes and stabilizer subfields," *Adv. Math. Commun.*, vol. 9, no. 2, pp. 177–197, 2015.

[13] A.-L. Horlemann-Trautmann, "Message encoding and retrieval for spread and cyclic orbit codes," *Des., Codes Cryptogr.*, vol. 86, no. 2, pp. 365–386, Feb. 2018.

[14] J. J. Climent and V. Requena, "A construction of Abelian non-cyclic orbit codes," *Cryptogr. Commun.*, vol. 11, no. 4, pp. 839–852, Sep. 2019.

[15] E. Gorla and A. Ravagnani, "Partial spreads in random network coding," *Finite Fields Appl.*, vol. 26, pp. 104–115, Mar. 2014.

[16] M. H. Poroch and A. A. Talebi, "Product of symplectic groups and its cyclic orbit code," *Discrete Math., Algorithms Appl.*, vol. 11, no. 5, Oct. 2019, Art. no. 1950061.

[17] Y. Gao and M. Y. Niu, "The construction of orbit codes based on singular linear space over finite fields," *J. Combinat. Math. Combinat. Comput.*, vol. 108, pp. 245–257, Feb. 2019.

[18] S.-D. Chen and J.-Y. Liang, "New constructions of orbit codes based on the operations of orbit codes," *Acta Mathematicae Applicatae Sinica, English Ser.*, vol. 36, no. 4, pp. 803–815, Oct. 2020.

[19] S. Chen and J. Liang, "Construction of spread codes based on Abelian non-cyclic orbit codes," *Linear Algebra Appl.*, vol. 608, pp. 54–67, Jan. 2021.

[20] Z. X. Wan, *Geometry of Classical Group Over Finite Fields*. Beijing, China: Science Press, 2002.

[21] T. Brookfield, *Overgroups of a Linear Singer Cyclic in Classical Groups*. Birmingham, U.K.: School Mathematics Univ. of Birmingham, 2014.

[22] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*. London, U.K.: Cambridge Univ. Press, 2003.

SHANGDI CHEN received the Ph.D. degree from the Institute of Mathematics, Zhejiang University, Zhejiang, China, in 2004. Since March 2004, he has been working with the Civil Aviation University of China, where he is currently a Professor with the College of Science. He is involved in several national natural science foundation projects. His research interests include algebraic graph theory, coding, and cryptography.

QIN XU is currently pursuing the degree with the College of Science, Civil Aviation University of China. Her research interests include algebraic coding and cryptography.