ORBIT CODES FROM FORMS ON VECTOR SPACES OVER A FINITE FIELD

Angela Aguglia

Dipartimento di Meccanica, Matematica e Management
Politecnico di Bari
Bari, I-70126, Italy

Antonio Cossidente

Dipartimento di Matematica, Informatica ed Economia
Università degli Studi della Basilicata
Potenza, I-85100, Italy

Giuseppe Marino

Dipartimento di Matematica e Applicazioni “Renato Caccioppoli”
Università degli Studi di Napoli “Federico II”
Napoli, I-80138, Italy

Francesco Pavese*

Dipartimento di Meccanica, Matematica e Management
Politecnico di Bari
Bari, I-70126, Italy

Alessandro Siciliano

Dipartimento di Matematica, Informatica ed Economia
Università degli Studi della Basilicata
Potenza, I-85100, Italy

(Communicated by Ferruh Özbudak)

Abstract. In this paper we construct different families of orbit codes in the vector spaces of the symmetric bilinear forms, quadratic forms and Hermitian forms on an n-dimensional vector space over the finite field $\mathbb{F}_q$. All these codes admit the general linear group $\mathrm{GL}(n,q)$ as a transitive automorphism group.

1. Introduction

In [1] Ahlswede, Cai, Li and Yeung, random linear network coding was introduced as a powerful tool for data communication in point-to-point networks on which a number of information sources are multicasted to certain sets of destinations and the information sources are mutually independent [29, 30]. A mathematical description of random network coding was given in [35] where codewords are subspaces of some fixed vector space and a code is a collection of such subspaces.

More formally, let $V = V(n,q)$ denote the n-dimensional vector space over the finite field $\mathbb{F}_q$ with q elements, and $\mathrm{PG}(V)$ be the partially ordered set with respect

2020 *Mathematics Subject Classification:* Primary: 05B25; Secondary: 15A63,94B25.

Key words and phrases: Orbit code; Constant dimension code; Subspace code.

The research was supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM)..

* Corresponding author: Francesco Pavese.

to the inclusion relation of all subspaces of V. It is well-known that $\mathrm{PG}(V)$ is a metric space with respect to the *subspace distance* defined by

$$d(U,W) = \dim(U) + \dim(W) - 2\dim(U \cap W).$$

A *subspace code of length n over $\mathbb{F}_q$* is a nonempty subset $\mathcal{X}$ of $\mathrm{PG}(V)$, and the elements of $\mathcal{X}$ are the *codewords* of $\mathcal{X}$. The *minimum distance* of $\mathcal{X}$ is given by $d(\mathcal{X}) = \min\{d(U,W) : U,W \in \mathcal{X}, U \neq W\}$.

In view of their application in random network coding, subspace codes have been intensely studied in recent years (see for instance [31, 39, 13, 28] and references therein). One of the main problems of subspace coding asks for the maximum possible cardinality of a subspace code of length n over $\mathbb{F}_q$ with minimum distance at least d and the classification of the corresponding optimal codes.

An important class of subspace codes are those whose codewords have constant dimension k. If $\mathcal{X}$ is such a code then $\mathcal{X}$ is called a *constant dimension code* (or *k-dimensional subspace code*) with parameters $(n, |\mathcal{X}|, d, k)_q$, where n is the dimension of the vector space V, d is the minimum distance of $\mathcal{X}$ and k is the dimension of the codewords. Constant dimension codes are useful for error correction in random linear network communication. The errors in this scenario can either be dimension deletions or dimension insertions. The maximum cardinality of an $(n,*,d,k)_q$ constant dimension code is denoted by $\mathcal{A}_q(n,d;k)$. The upper bound on $\mathcal{A}_q(n,d;k)$ are usually the q–analog of the bounds obtained for the well studied constant weight codes. In particular the following upper bound has been proved in [19] and [50]:

$$(1) \qquad \mathcal{A}_q(n,d;k) \leq \left\lfloor \frac{q^n-1}{q^k-1} \left\lfloor \frac{q^{n-1}-1}{q^{k-1}-1} \cdots \left\lfloor \frac{q^{n-k+d/2}-1}{q^{d/2}-1} \right\rfloor \cdots \right\rfloor \right\rfloor .$$

Note that for $k \leq n-k$, starting from a suitable set of $k \times (n-k)$–matrices with entries in $\mathbb{F}_q$, known as MRD–codes, by means of the so–called *lifting process*, one can construct an $(n, q^{(n-k)(k-d+1)}, 2d, k)_q$ constant dimension code [42, 21]. Although the size of these codes matches the term of highest order of (1), there are many constructions that give rise to larger codes. With respect to the best known constructions, or lower bounds for $\mathcal{A}_q(n,d;k)$, we only mention the *Echelon-Ferrers constructions* [20, 41], the *linkage constructions* [24, 15] and constructions obtained with geometrical techniques [10, 11, 12, 14]. These approaches give for many parameters the largest codes known so far. The currently best known lower and upper bounds for $\mathcal{A}_q(n,d;k)$ can be found at the online tables http://subspacecodes.uni-bayreuth.de and the associated survey [25].

Examples of constant dimension codes are the so called orbit codes. A subspace code is an *orbit code* if it can be written as UG, where U is a subspace of V and G is a subgroup of the general semilinear group $\Gamma\mathrm{L}(V)$. The group G is said to be a *generating subgroup* of the code. By [45, Proposition 3.11], if a code has G as a generating subgroup, then G is a subgroup of the automorphism group of the code. These codes were introduced in [47], and since then they have been further investigated by many authors [8, 27, 44, 40]. It is well known that $\mathrm{GL}(V)$ contains exactly one conjugacy class of cyclic subgroups, acting regularly on $V \setminus \{0\}$ and isomorphic to $\mathbb{F}_{q^n} \setminus \{0\}$, i.e., the *Singer groups*. Constant dimension codes that are obtained by glueing together distinct orbit codes having as generating subgroup a Singer group are also called *cyclic codes*. Stimulated by the fact that, for small parameters, there are examples of large or optimal subspace codes that are cyclic codes [34, 19, 5], particular attention has been devoted to the construction of cyclic codes [44, 23, 3, 38, 7]. Some of the largest k-dimensional cyclic subspace codes obtained have parameters $(N, (q^n-1)\frac{q^N-1}{q-1}+\frac{q^N-1}{q^k-1}, 2k-2, k)_q$, where N is the degree of the splitting field of certain q-polynomials over $\mathbb{F}_{q^n}$ of degree q^k [7]. Typically, the known cyclic codes admit a group of order at most $N(q^N-1)$, that is the normalizer of a Singer group, but their size is far behind the theoretical upper bound. In [8] the authors study an abelian non–cyclic group of order $q(q-1)^2$ in order to obtain an orbit code with parameters $(n, q(q-1), 2k, k)_q$.

In this paper we aim at establishing new techniques for the construction of orbit codes. To this end we consider $\mathcal{S}(V)$, $\mathcal{Q}(V)$ and $\mathcal{H}(V)$, the set of all symmetric, quadratic and Hermitian forms on $V = V(n,q)$ (in the Hermitian case, $q = q_0^2$). Then each of these sets is a vector space, say $\widetilde{V}$, over $\mathbb{F}_q$ (in the Hermitian case over $\mathbb{F}_{q_0}$), and $\mathrm{GL}(V)$ is a subgroup of $\mathrm{GL}(\widetilde{V})$. In particular, $\mathrm{GL}(V)$ acts on the forms by preserving the rank. In all cases, we construct orbit codes whose generating subgroup is $\mathrm{GL}(V)$. In order to do that we use the cyclic model of a finite dimensional vector space over $\mathbb{F}_q$, see [9, 26]. More precisely we obtain:

- an orbit code in $\mathrm{PG}(\mathcal{S}(V))$ with parameters
$$\left(\frac{n(n+1)}{2}, \frac{q^{n(n-1)/2}\prod_{i=1}^{n-1}(q^i-1)}{n}, 2(n-j), n\right)_q,$$
where $j < n$ is the greatest divisor of n;
- a $\left(15, \frac{q^{10}\prod_{i=1}^{4}(q^i-1)}{5}, 8, 5\right)_q$ orbit code in $\mathrm{PG}(\mathcal{Q}(V))$, where $V = V(5,q)$;
- an orbit code in $\mathrm{PG}(\mathcal{H}(V))$ with parameters
$$\left(n^2, \frac{q^{n(n-1)/2}\prod_{i=1}^{n-1}(q^i-1)}{n}, 2(n-j), n\right)_{q_0},$$
where $j < n$ is the greatest divisor of n, whenever n is odd and $q = q_0^2$.

We remark that the generating subgroups of these codes have order $q^{n(n-1)/2}\prod_{i=1}^{n}(q^i-1)$. Moreover, if n is a prime, then the leading order term of the size of these orbit codes is $q^{n(n-1)}/n$, while the term of highest order in the upper bound (1) equals $q^{n(n-1)}$. Therefore, as functions of q they have the same order. This implies that, when n is a prime and q approaches infinity, the size of these orbit codes is not very far from the theoretical upper bound.

The paper is structured as follows: in Section 2 we collect some preliminary facts about symmetric, quadratic and Hermitian forms on V, the cyclic representation of a finite dimensional vector space over $\mathbb{F}_q$ and q-circulant matrices. In Section 3, 4 and 5 we describe the orbit codes in the cyclic model of the vector space of the symmetric, quadratic and Hermitian forms respectively.

2. Preliminaries

Let $V = V(n,q)$ be an n-dimensional vector space over $\mathbb{F}_q$ and let $(v_0, \dots, v_{n-1})$ be an ordered basis of V. If $g \in \mathrm{GL}(V)$, let M_g be the matrix of g with respect to $(v_0, \dots, v_{n-1})$.

A *symmetric bilinear form* on V is a function $f : V \times V \to \mathbb{F}_q$ that satisfies the identities
$$f\left(\sum_i x_i v_i, \sum_j y_j w_j\right) = \sum_{i,j} x_i f(v_i, w_j) y_j,$$

and $f(v,w)=f(w,v)$, for all scalars $x_i, y_j \in \mathbb{F}_q$ and all vectors $v_i, w_j, v, w \in V$. The set $\mathcal{S}(V)$ of all symmetric bilinear forms on V is an $n(n+1)/2$-dimensional vector space over $\mathbb{F}_q$. The *radical* of $f \in \mathcal{S}(V)$ is the subspace of V consisting of all vectors v satisfying $f(v,v')=0$ for every $v' \in V$, and we denote it by $\mathrm{Rad}\, f$. We say that f is *non-degenerate* if $\mathrm{Rad}\, f = \{0\}$. The *rank of* f, denoted by $\mathrm{rk} f$, is $n - \dim_{\mathbb{F}_q} \mathrm{Rad}\, f$. For any $f \in \mathcal{S}(V)$, the $n \times n$ symmetric matrix $A_f = (f(v_i, v_j))$ is called the *Gram matrix of f with respect to the basis* $(v_0, \ldots, v_{n-1})$. We denote by $\mathcal{S}(n,q)$ the set of all $n \times n$ symmetric $\mathbb{F}_q$-matrices. The map $f \in \mathcal{S}(V) \mapsto A_f \in \mathcal{S}(n,q)$ is an isomorphism and $\mathrm{rk} f = \mathrm{rank}\, A_f$. Therefore, non-degenerate symmetric bilinear forms correspond to non-singular symmetric matrices, and conversely. Let $\mathrm{GL}(\mathcal{S}(V))$ denote the *general linear group* of $\mathcal{S}(V)$, that is the group of all invertible linear transformations of $\mathcal{S}(V)$. By [48, Theorem 5.4], the subgroup of $\mathrm{GL}(\mathcal{S}(V))$ which acts on $\mathcal{S}(V)$ by preserving the rank is isomorphic to $\mathrm{GL}(V)$. If $f \in \mathcal{S}(V)$ and $g \in \mathrm{GL}(V)$ then the element f^g of $\mathcal{S}(V)$ is that whose Gram matrix is $M_g^t A_f M_g$. Here, and in the sequel, ^{t} denotes transposition.

A *quadratic form* on V is a function $Q : V \to \mathbb{F}_q$ such that $Q(av) = a^2 Q(v)$, for every $a \in \mathbb{F}_q$, $v \in V$ and $\beta : (u,v) \in V \times V \mapsto Q(u+v) - Q(u) - Q(v) \in \mathbb{F}_q$ is a bilinear form on V; β is called the *polar form* of Q. A non-zero vector v is *singular* if $Q(v) = 0$ and a subspace U is *totally singular* if $Q(u) = 0$, for all $u \in U$. A quadratic form is said to be *non-singular* if each non-zero vector of $\mathrm{Rad}\, \beta$ is non-singular. The *Witt index* of Q is the common dimension of the maximal totally singular subspaces. The set $\mathcal{Q}(V)$ of all quadratic forms on V is a vector space over $\mathbb{F}_q$ of dimension $n(n+1)/2$. If $g \in \mathrm{GL}(V)$ and $Q \in \mathcal{Q}(V)$, then Q^g is the quadratic form defined by $Q^g(v) = Q(gv)$, for every $v \in V$.

Let $q = q_0^2$. A *Hermitian form* on V is a function $h : V \times V \to \mathbb{F}_q$ satisfying

$$h\left(\sum_i x_i v_i, \sum_j y_j w_j\right) = \sum_{i,j} x_i h(v_i, w_j) y_j^{q_0},$$

and $h(v,w) = (h(w,v))^{q_0}$, for all $x_i, y_j \in \mathbb{F}_q$ and for all $v_i, w_j, v, w \in V$. The set $\mathcal{H}(V)$ of all Hermitian forms on V is an n^2-dimensional vector space over $\mathbb{F}_{q_0}$. The *radical* $\mathrm{Rad}\, h$ of $h \in \mathcal{H}(V)$ is the subspace of V consisting of all vectors v such that $h(v,v') = 0$, for every $v' \in V$. The form h is said to be *non-degenerate* if $\mathrm{Rad}\, h = \{0\}$, and the *rank of* h, denoted by $\mathrm{rk}\, h$, is $n - \dim_{\mathbb{F}_q} \mathrm{Rad}\, h$. If $h \in \mathcal{H}(V)$, the $n \times n$ Hermitian matrix $A_h = (h(v_i, v_j))$ is called the *Gram matrix of h with respect to the basis* $\{v_1, \ldots, v_n\}$. Let $\mathcal{H}(n,q)$ be the set of all $n \times n$ Hermitian matrices over $\mathbb{F}_q$. The map $h \in \mathcal{H}(V) \mapsto A_h \in \mathcal{H}(n,q)$ is an isomorphism and $\mathrm{rk}\, h = \mathrm{rank}\, A_h$. Therefore, non-degenerate Hermitian forms correspond to non-singular Hermitian matrices, and conversely. Let $\mathrm{GL}(\mathcal{H}(V))$ denote the *general linear group* of the n^2-dimensional $\mathbb{F}_{q_0}$-vector space $\mathcal{H}(V)$. By [48, Theorem 6.4], the subgroup of $\mathrm{GL}(\mathcal{H}(V))$ acting on $\mathcal{H}(V)$ by preserving the rank is $\mathrm{GL}(V)$. If $h \in \mathcal{H}(V)$ and $g \in \mathrm{GL}(V)$ then the element $h^g \in \mathcal{H}(V)$ is that whose Gram matrix is $M_g^t A_h \overline{M}_g$, where $\overline{M}_g$ is the matrix obtained by raising each entry of M_g to the q_0-th power.

A *correlation* of $\mathrm{PG}(V)$ is a collineation from $\mathrm{PG}(V)$ to its dual. The correlation ϕ with underlying matrix A and field automorphism θ acts on $\mathrm{PG}(V)$ by mapping $P = (x_0, \ldots, x_{n-1})^t$ to the hyperplane represented by the column vector $(a_0, \ldots, a_{n-1})^t = A(x_0^\theta, \ldots, x_{n-1}^\theta)^t$. For completeness, we recall that the correlation

ϕ^* from the dual of $\mathrm{PG}(V)$ to $\mathrm{PG}(V)$, with underlying matrix A and field automorphism θ, maps the hyperplane Π with projective coordinates $(a_0, \ldots, a_{n-1})^t$ on the projective point with coordinates $A^{-t}(a_0^\theta, \ldots, a_{n-1}^\theta)^t$. Therefore, the product of two correlations is a collineation of $\mathrm{PG}(V)$. A correlation of order two is called *polarity.* It is well-known that any correlation of $\mathrm{PG}(V)$ arises from a non-degenerate sesquilinear form on V, and polarities arise from either an alternating or a symmetric or a Hermitian form.

For further details on symmetric bilinear forms, polarities, correlations, quadratic forms and Hermitian forms, the interested reader is referred to [17] and [46].

Embed $V = V(n,q)$ in $\widehat{V} = V(n,q^n)$ by extending the scalars to $\mathbb{F}_{q^n}$. It is known [9, 18] that, for any given primitive element ω of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, there is an $\mathbb{F}_{q^n}$-basis $(s_0, \ldots, s_{n-1})_w$ of $\widehat{V}$ such that

$$V = \left\{ \sum_{i=0}^{n-1} x^{q^i} s_i : x \in \mathbb{F}_{q^n} \right\}. \tag{2}$$

The ordered basis $(s_0, \ldots, s_{n-1})_w$ is called a *Singer basis* for V in $\widehat{V}$ and the representation (2) of V, or equivalently the set $\{(x, x^q, \ldots, x^{q^{n-1}}) : x \in \mathbb{F}_{q^n}\} \subset \mathbb{F}_{q^n}^n$, is the so-called *cyclic model of* V in $\widehat{V}$ [22].

A *q-circulant $n \times n$ matrix over* $\mathbb{F}_{q^n}$ is a matrix of the form

$$D_{\mathbf{a}} = D_{(a_0,a_1,\ldots,a_{n-1})} = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1}^q & a_0^q & \cdots & a_{n-2}^q \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & a_0^{q^{n-1}} \end{pmatrix},$$

with $a_i \in \mathbb{F}_{q^n}$; we say that the matrix $D_{\mathbf{a}}$ is *generated by the array* $\mathbf{a} = (a_0, \ldots, a_{n-1})$. The set of all q-circulant $n \times n$ matrices over $\mathbb{F}_{q^n}$ forms the *Dickson matrix algebra* $\mathcal{D}_n(\mathbb{F}_{q^n})$ and the set of all invertible matrices in $\mathcal{D}_n(\mathbb{F}_{q^n})$ forms the *Betti-Mathieu group* $\mathcal{I}_n(\mathbb{F}_{q^n})$ [4, 6]. It is known that $\mathcal{D}_n(\mathbb{F}_{q^n}) \simeq \mathrm{End}(V)$ and $\mathcal{I}_n(\mathbb{F}_{q^n}) \simeq \mathrm{GL}(V)$ [37, 49]. Therefore, for any $g \in \mathrm{GL}(V)$ the matrix of g with respect to the Singer basis $(s_0, \ldots, s_{n-1})_w$ is a non-singular q-circulant matrix $D_{\mathbf{g}}$ [16, 18]. In addition, the non-singular Moore matrix

$$E_n = \begin{pmatrix} 1 & w & \cdots & w^{n-1} \\ 1 & w^q & \cdots & w^{(n-1)q} \\ \vdots & \vdots & & \vdots \\ 1 & w^{q^{n-1}} & \cdots & w^{(n-1)q^{n-1}} \end{pmatrix} \tag{3}$$

is the matrix of the change of basis from $(v_0, \ldots, v_{n-1})$ to $(s_0, \ldots, s_{n-1})$ [16]. Then $D_{\mathbf{g}} = E_n M_g E_n^{-1}$.

A *Singer cycle* of $\mathrm{GL}(V)$ is an element of order $q^n - 1$. It is known that any primitive element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ defines a Singer cycle of $V = V(n,q)$ [32, 43]. Let σ be the Singer cycle defined by the primitive element ω associated with the Singer basis $(s_0, \ldots, s_{n-1})_w$. Then, with respect to this basis, σ has q-circulant matrix $\mathrm{diag}(\omega, \omega^q, \ldots, \omega^{q^{n-1}})$ [9].

Let $\tau \in \mathrm{GL}(V)$ whose q-circulant matrix is

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}. \tag{4}$$

Observe that τ acts on the *Singer cyclic group* $S = \langle \sigma \rangle$ by mapping $\mathrm{diag}(\omega, \omega^q, \dots, \omega^{q^{n-1}})$ to $\mathrm{diag}(\omega^q, \dots, \omega^{q^{n-1}}, \omega)$. Let C be the cyclic group of order n generated by τ. Then $S \rtimes C$ is the normalizer of S in $\mathrm{GL}(V)$ [32].

In $\mathcal{D}_n(\mathbb{F}_{q^n})$, let $\mathcal{SD}_n(\mathbb{F}_{q^n})$ be the set of all symmetric q-circulant matrices. The isomorphism between the set of all bilinear forms on V and $\mathcal{D}_n(\mathbb{F}_{q^n})$ described in [16, Proposition 2.6], induces the isomorphism $\mathcal{S}(V) \simeq \mathcal{SD}_n(\mathbb{F}_{q^n})$. Therefore, we may identify any $f \in \mathcal{S}(V)$ with its symmetric q-circulant Gram matrix $D_{\mathbf{f}} = E^{-1} A_f E^{-1} \in \mathcal{SD}_n(\mathbb{F}_{q^n})$, with respect to the fixed Singer basis $(s_0, \dots, s_{n-1})_w$. If $g \in \mathrm{GL}(V)$ with q-circulant matrix $D_{\mathbf{g}}$, then the q-circulant Gram matrix of $f^g \in \mathcal{S}(V)$ is $D_{\mathbf{g}}^t D_{\mathbf{f}} D_{\mathbf{g}} \in \mathcal{SD}_n(\mathbb{F}_{q^n})$.

Let n be odd and $q = q_0^2$. A q-circulant matrix generated by the array

$$\left(a_0, a_1, \dots, a_{\frac{n-1}{2}-1}, b, a_{\frac{n-1}{2}-1}^{q_0^{n+2}}, \dots, a_1^{q_0^{2n-3}}, a_0^{q_0^{2n-1}}\right),$$

with $a_i \in \mathbb{F}_{q^n}$ and $b \in \mathbb{F}_{q_0^n}$ is said to be a *q-circulant pseudo-Hermitian matrix*. We denote by $\mathcal{HD}_n(\mathbb{F}_{q^n})$ the set of these matrices. Analogously to the symmetric case, it can be seen that $\mathcal{H}(V) \simeq \mathcal{H}(n,q) \simeq \mathcal{HD}_n(\mathbb{F}_{q^n})$. Therefore, we may identify any $h \in \mathcal{H}(V)$ with its q-circulant Gram matrix $D_{\mathbf{h}} = E^{-1} A_h E^{-1} \in \mathcal{HD}_n(\mathbb{F}_{q^n})$, with respect to the fixed Singer basis. If $g \in \mathrm{GL}(V)$, then the q-circulant Gram matrix of $h^g \in \mathcal{H}(V)$ is $D_{\mathbf{g}}^t D_{\mathbf{h}} \overline{D}_{\mathbf{g}} \in \mathcal{HD}_n(\mathbb{F}_{q^n})$.

Throughout the paper let $\mathrm{Tr}_{q^n/q}$ denote the trace map from $\mathbb{F}_{q^n}$ onto $\mathbb{F}_q$,

$$\mathrm{Tr}_{q^n/q} : x \in \mathbb{F}_{q^n} \longmapsto \sum_{i=0}^{n-1} x^{q^i} \in \mathbb{F}_q.$$

and let $\mathrm{N}_{q^n/q}$ denote the norm map from $\mathbb{F}_{q^n}$ onto $\mathbb{F}_q$,

$$\mathrm{N}_{q^n/q} : x \in \mathbb{F}_{q^n} \longmapsto x^{q^{n-1}+\dots+q+1} \in \mathbb{F}_q.$$

Also, we will denote by $\mathbf{x}$ the vector $(x, x^q, \dots, x^{q^{n-1}})$ of the cyclic model of V in $\widehat{V}$, and by $\mathbf{e}_i$ the vector $(0, \dots, 0, 1, 0, \dots, 0)$, $0 \le i \le n-1$, where 1 is in the i-th position and 0 elsewhere. Finally, we will index rows and columns of any $n \times n$ matrix M by elements in $\{0, \dots, n-1\}$ and $\{0, \dots, n-1\}$, and we will denote by $M_{(i)}$ and $M^{(j)}$ its i-th row and j-th column, respectively.

3. ORBIT CODES FROM SYMMETRIC BILINEAR FORMS

Let f_a be the symmetric bilinear form on V whose q-circulant Gram matrix in the Singer basis $(s_0, \dots, s_{n-1})_w$ is

$$D_a = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a^q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a^{q^{n-1}} \end{pmatrix},$$

for some $a \in \mathbb{F}_{q^n}$. Hence, the set

$$U_1 = \{f_a : a \in \mathbb{F}_{q^n}\}$$

is an n-dimensional $\mathbb{F}_q$-vector subspace of $\mathcal{S}(V)$.

Theorem 3.1. *The stabilizer of U_1 in $\mathrm{GL}(V)$ is $S \rtimes C$, where S is the Singer cyclic group of $\mathrm{GL}(V)$ generated by σ and C is the cyclic group generated by τ.*

Proof. Let $g \in \mathrm{GL}(V)$ with q-circulant matrix $D_{\mathbf{g}}$ generated by $(g_0, g_1, \ldots, g_{n-1})$ with respect to the Singer basis $(s_0, \ldots, s_{n-1})_w$. Then $D_{\mathbf{g}}^t$ is generated by $(h_0, h_1, \ldots, h_{n-1}) = (g_0, g_{n-1}^q, \ldots, g_1^{q^{n-1}})$. Let f_a be any element in U_1. Then, the q-circulant Gram matrix of f_a^g is generated by the array $(D_{\mathbf{g}}^t D_a D_{\mathbf{g}})_{(0)}$.

The l-th entry of $(D_{\mathbf{g}}^t D_a D_{\mathbf{g}})_{(0)}$, for $0 \le l \le n-1$, is given by the inner product $(D_{\mathbf{g}}^t D_a)_{(0)} \cdot D_{\mathbf{g}}^{(l)}$, with $D_{\mathbf{g}}^{(l)} = (g_{n-l}^{q^l}, g_{n-l+1}^{q^l}, \ldots, g_{n-l-1}^{q^l})$, where subscripts are taken modulo n. As

$$(D_{\mathbf{g}}^t D_a)_{(0)} = \left(h_0 a, h_1 a^q, \ldots, h_{n-1} a^{q^{n-1}}\right),$$

the l-th entry of $(D_{\mathbf{g}}^t D_a D_{\mathbf{g}})_{(0)}$ is

$$\sum_{i=0}^{n-1} h_i h_{n-l+i}^{q^l} a^{q^i}.$$

Since we are assuming that g fixes U_1, we must have

$$\sum_{i=0}^{n-1} h_i h_{i-l}^{q^l} a^{q^i} = 0 \tag{5}$$

for $1 \le l \le n-1$. As equation (5) holds for all $a \in \mathbb{F}_{q^n}$, we get

$$0 = h_i h_{i-l}^{q^l} = g_{n-i}^{q^i} g_{l-i}^{q^i},$$

for $0 \le i \le n-1$ and $1 \le l \le n-1$. This is equivalent to

$$g_i g_{i-l} = 0, \tag{6}$$

for $0 \le i \le n-1$ and $1 \le l \le n-1$.

As $D_{\mathbf{g}} \in \mathcal{I}_n(\mathbb{F}_{q^n})$, then $(g_0, g_1, \ldots, g_{n-1}) \neq (0, \ldots, 0)$. So, by applying a suitable element in C, we may assume $g_0 \neq 0$. Equation (6) implies $g_{-l} = 0$, for $1 \le l \le n-1$. By considering subscripts modulo n, we see that the only possible non-zero entry in $(g_0, \ldots, g_{n-1})$ is g_0, that is $g \in S$. Therefore the stabilizer of U_1 in $\mathrm{GL}(V)$ has the prescribed form. □

For any $g \in \mathrm{GL}(V)$, set $U_1^g = \{f_a^g : a \in \mathbb{F}_{q^n}\}$. Let $\mathcal{U}_1$ be the orbit code $\mathcal{U}_1 = U_1 \mathrm{GL}(V) = \{U_1^g : g \in \mathrm{GL}(V)\}$. From Theorem 3.1 and the Orbit-Stabilizer Theorem [2, p.16] we get the following result.

Corollary 1. *The size of $\mathcal{U}_1$ is*

$$\frac{q^{n(n-1)/2} \prod_{i=1}^{n-1} (q^i - 1)}{n}.$$

Lemma 3.2. *Let $f_a, f_b \in U_1$ with associated polarities $\widehat{\delta}_a$ and $\widehat{\delta}_b$ of $\mathrm{PG}(\widehat{V})$. Then the (linear) collineation $\psi = \widehat{\delta}_b \cdot \widehat{\delta}_a$ of $\mathrm{PG}(\widehat{V})$ is represented by the q-circulant matrix generated by the array $(ab^{-1}, 0, \ldots, 0)$.*

Proof. It suffices to consider $\widehat{\delta}_a$ and $\widehat{\delta}_b$ as correlations of $\mathrm{PG}(\widehat{V})$ acting on it via the corresponding q-circulant matrices D_a and D_b with respect to the Singer basis. □

It is immediate to see that ψ fixes each point $\langle \mathbf{e}_i \rangle$, for $i = 0, \dots, n-1$.

Theorem 3.3. *Let $g \in \mathrm{GL}(V)$, with $g \notin S \rtimes C$, and $q-$circulant matrix $D_{\mathbf{g}}$ with respect to the Singer basis $(s_0, s_1, \dots, s_{n-1})_w$. Let $D_{\mathbf{k}} = D_{\mathbf{g}}^{-t}$ the inverse transpose of $D_{\mathbf{g}}$, where $\mathbf{k} = (k_0, \dots, k_{n-1})$. Suppose that exactly $l+1$ entries of $\mathbf{k}$ are non-zero, say $k_{i_0}, k_{i_1}, \dots, k_{i_l}$, with $0 \le i_0 < i_1 < \dots < i_l \le n-1$. Then the subspaces U_1 and U_1^g meet either trivially or in a j-dimensional $\mathbb{F}_q$-subspace, where $j = \gcd(n, i_1 - i_0, \dots, i_l - i_0)$.*

Proof. Assume that U_1 and U_1^g do not meet trivially, and let $f_a \in U_1 \cap U_1^g$ for some non-zero $a \in \mathbb{F}_{q^n}$. Let $f_b \in U_1 \cap U_1^g$ with $b \in \mathbb{F}_{q^n} \setminus \{0, a\}$. Note that $\mathbf{e}_i^{g^{-1}} = (k_{n-i}^{q^i}, \dots, k_{n-i-1}^{q^i})$, which is the i-th column of $D_{\mathbf{g}}^{-1}$. As $f_a, f_b \in U_1$, by Lemma 3.2, the linear collineation $\psi = \widehat{\delta}_a \cdot \widehat{\delta}_b$ of $\mathrm{PG}(\widehat{V})$ fixes $\langle \mathbf{e}_i \rangle$ and $\langle \mathbf{e}_i^{g^{-1}} \rangle$, for all $i = 0, \dots, n-1$.

Assume first that all entries k_i are non-zero. Then $\left\{ \langle \mathbf{e}_0 \rangle, \dots, \langle \mathbf{e}_{n-1} \rangle, \langle \mathbf{e}_0^{g^{-1}} \rangle \right\}$ is a projective frame in $\mathrm{PG}(\widehat{V})$. Therefore ψ is the identity on $\mathrm{PG}(\widehat{V})$. From Lemma 3.2 it follows that $ab^{-1} \in \mathbb{F}_q \setminus \{0\}$, that is $U_1 \cap U_1^g = \langle f_a \rangle_{\mathbb{F}_q}$.

Assume now that exactly $l+1 < n$ entries of $(k_0, \dots, k_{n-1})$ are non-zero, say $k_{i_0}, k_{i_1}, \dots, k_{i_l}$, with $0 \le i_0 < i_1 < \dots < i_l \le n-1$. As the cyclic subgroup $C = \langle \tau \rangle$ fixes U_1 we may assume $k_0 \ne 0$, i.e. $i_0 = 0$. Then $\left\{ \langle \mathbf{e}_0 \rangle, \langle \mathbf{e}_{i_1} \rangle, \dots, \langle \mathbf{e}_{i_l} \rangle, \langle \mathbf{e}_0^{g^{-1}} \rangle \right\}$ is a projective frame in the subspace Γ spanned by $\langle \mathbf{e}_0 \rangle, \langle \mathbf{e}_{i_1} \rangle, \dots, \langle \mathbf{e}_{i_l} \rangle$. From the above argument we see that ψ induces the identity on Γ. Therefore $ab^{-1} = (ab^{-1})^{q^{i_m}}$, for $m = 1, \dots, l$, that is $ab^{-1} \in \mathbb{F}_{q^j}$, with $j = \gcd(n, i_1, \dots, i_l)$. This implies that U_1 and U_1^g intersect in a j-dimensional $\mathbb{F}_q$-subspace. □

Corollary 2. *For each $g \in \mathrm{GL}(V)$, $g \notin S \rtimes C$, the subspaces U_1 and U_1^g have at most q^j elements in common, where $j < n$ is the greatest divisor of n.*

Theorem 3.4. *Let $j < n$ be the greatest divisor of n. Then the set $\mathcal{U}_1$ is an orbit code with parameters*

$$\left(\frac{n(n+1)}{2}, \frac{q^{n(n-1)/2} \prod_{i=1}^{n-1} (q^i - 1)}{n}, 2(n-j), n \right)_q .$$

Moreover, $\mathrm{GL}(V)$ acts transitively on it.

Proof. The result follows from Corollaries 1 and 2. □

Example 1. Let $n = 4$. For any given $a \in \mathbb{F}_{q^4}$ the matrix of the symmetric bilinear form f_a in the Singer basis $(s_0, \dots, s_{n-1})_w$ is

$$D_a = \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & a^q & 0 & 0 \\ 0 & 0 & a^{q^2} & 0 \\ 0 & 0 & 0 & a^{q^3} \end{pmatrix} .$$

Hence the $\mathbb{F}_q$-subspace U_1 of V can be identified with the $\mathbb{F}_q$-subspace $\{D_a : a \in \mathbb{F}_{q^4}\}$ in the Dickson matrix algebra $\mathcal{D}_4(\mathbb{F}_{q^4})$, and the codewords of $\mathcal{U}_1$ are the subspaces

$\{D_{\mathbf{g}}^t D_a D_{\mathbf{g}} : a \in \mathbb{F}_{q^n}\}$ for any non-singular q-circulant matrix

$$D_{\mathbf{g}} = D_{(g_0,g_1,g_2,g_3)} = \begin{pmatrix} g_0 & g_1 & g_2 & g_3 \\ g_3^q & g_0^q & g_1^q & g_2^q \\ g_2^{q^2} & g_3^{q^2} & g_0^{q^2} & g_1^{q^2} \\ g_1^{q^3} & g_2^{q^3} & g_2^{q^3} & g_0^{q^3} \end{pmatrix}.$$

Note that $D_{\mathbf{g}}^t D_a D_{\mathbf{g}} = D_{\mathbf{h}}$, with $\mathbf{h} = (h_0, \dots, h_{n-1})$ where $h_l = \sum_{i=0}^{3} g_{3-i}^{q^i} g_{l-i}^{q^i} a^{q^i}$; here subscripts are taken modulo n.

Remark 1. The representation of U_1 and of the orbit code $\mathcal{U}_1$ over $\mathbb{F}_q$ is obtained by considering the matrix E_n of the change of basis from $(v_0, \dots, v_{n-1})$ to $(s_0, \dots, s_{r-1})_w$. The q-ary representation of U_1 is the subspace $\{E_n^t D_a E_n : a \in \mathbb{F}_{q^n}\}$ of $\mathcal{S}(n,q)$, and the codewords of $\mathcal{U}_1 = U_1 \mathrm{GL}(V)$ are the subspaces $\{(D_{\mathbf{g}} E_n)^t D_a (D_{\mathbf{g}} E_n) : a \in \mathbb{F}_{q^n}\}$, for all $D_{\mathbf{g}} \in \mathcal{I}_n(\mathbb{F}_{q^n})$. By using the isomorphism

$$\begin{array}{rccc} \nu : & \mathcal{S}(n,q) & \rightarrow & V(n(n+1)/2, q) \\ & (a_{i\,j}) & \mapsto & (a_{i,j})_{0 \le i \le j \le n-1} \end{array} \tag{7}$$

one can easily obtain the representation of the codewords of $\mathcal{U}_1$ as vectors of length $n(n+1)/2$ over $\mathbb{F}_q$.

4. Orbit codes from quadratic forms

In this section we assume $n = 2k+1$ to be an odd integer. For any $a \in \mathbb{F}_{q^n}$ and $\mathbf{x} = (x, x^q, \dots, x^{q^{n-1}})$, the map

$$Q_a(\mathbf{x}) = \mathrm{Tr}_{q^n/q}\left(a x^{q^k+1}\right)$$

is a quadratic form on V whose associated polar form is

$$\beta_a(\mathbf{x}, \mathbf{y}) = \mathrm{Tr}_{q^n/q}\left(a x y^{q^k} + a x^{q^k} y\right). \tag{8}$$

It is easy to see that each quadratic form Q_a of V is the restriction on V of the quadratic form $\widehat{Q}_a(\mathbf{X}) = \sum_{i=0}^{n-1} a^{q^i} X_i X_{i+k}$ on $\widehat{V}$, where $\mathbf{X} = (X_0, \dots, X_{n-1})$. Also we denote by $\widehat{\beta}_a$ the extension of β_a on $\widehat{V}$.

Lemma 4.1. *For any non-zero $a \in \mathbb{F}_{q^n}$, Q_a is a non-degenerate quadratic form on V.*

Proof. Let $\mathbf{x} = (x, x^q, \dots, x^{q^{n-1}}) \in \mathrm{Rad}\,\beta_a$. Then

$$\mathrm{Tr}_{q^n/q}\left(y\left(a x^{q^k} + a^{q^{k+1}} x^{q^{k+1}}\right)\right) = 0,$$

for all $y \in \mathbb{F}_{q^n}$. As the left hand side is a polynomial in the unknown y of degree at most q^{n-1} with q^n roots, we get

$$a x^{q^k} + a^{q^{k+1}} x^{q^{k+1}} = 0. \tag{9}$$

If q is odd then β_a is symmetric and we have $Q_a(\mathbf{x}) = \beta_a(\mathbf{x}, \mathbf{x})/2$. Therefore Q_a is non-degenerate if and only if $\mathrm{Rad}\,\beta_a = \{0\}$. The above equation implies

$$\mathrm{N}_{q^n/q}(a^{q^{k+1}-1}) = (-1)^n \mathrm{N}_{q^n/q}\left(\frac{1}{x^{q^k(q-1)}}\right) = -1,$$

as n is odd and $\mathrm{N}_{q^n/q}(x^{q^k(q-1)}) = 1$. On the other hand, since $q^{k+1} - 1 = (q-1)(q^k + q^{k-1} + \dots + 1)$ we get $\mathrm{N}_{q^n/q}(a^{q^{k+1}-1}) = 1$; a contradiction.

If q is even then β_a is alternating with $\mathrm{Rad}\,\beta_a$ nontrivially as n is odd. Therefore Q_a is non-degenerate if and only if $\mathrm{Ker}(Q_a|_{\mathrm{Rad}\,\beta_a}) = \{0\}$. Let $x \in \mathbb{F}_{q^n} \setminus \{0\}$ such that $\mathbf{x} \in \mathrm{Rad}\,\beta_a$. By raising (9) to the q^{k+1}-th power, we get

$$a^{q^{k+1}}x + a^q x^q = 0.$$

Hence

$$\left(\frac{x}{a^{q\frac{q^k-1}{q-1}}}\right)^{q-1} = 1,$$

i.e., $x = ca^{q\frac{q^k-1}{q-1}}$, for some non-zero $c \in \mathbb{F}_q$. Therefore, $\mathbf{x}$ is singular if and only if

$$Q_a(\mathbf{x}) = \mathrm{Tr}_{q^n/q}(ax^{q^k+1}) = c^2\mathrm{Tr}_{q^n/q}\left(a^{q\frac{q^{2k}-1}{q-1}+1}\right) = c^2 n\mathrm{N}_{q^n/q}(a) = 0$$

if and only if $a = 0$. □

From the previous lemma, the Witt index of Q_a is k and $\langle \mathbf{e}_i : i = 0, \dots, k-1\rangle$ is a totally singular subspace of $\widehat{Q}_a$, for all $a \in \mathbb{F}_{q^n} \setminus \{0\}$.

Let U_2 be the following set

$$U_2 = \{Q_a : a \in \mathbb{F}_{q^n}\}. \tag{10}$$

Then U_2 is an n-dimensional $\mathbb{F}_q$-subspace of $\mathcal{Q}(V)$. Straightforward computations show that $Q_a^\sigma = Q_{a\omega^{q^k+1}}$ and $Q_a^\tau = Q_{a^q}$, for all $a \in \mathbb{F}_{q^n} \setminus \{0\}$. Therefore the group $S \rtimes C$ fixes U_2.

Theorem 4.2. *The stabilizer of U_2 in $\mathrm{GL}(V)$ is $S \rtimes C$, where S is the Singer cyclic group of $\mathrm{GL}(V)$ generated by σ and C is the cyclic group generated by τ.*

Proof. The result was proved in [11] for $n = 3$. Therefore, we assume $n \geq 5$, that is $k > 1$. For any $Q_a \in U_2$, $a \neq 0$, the associated polar form is β_a defined by (8). Let B_a be the q-circulant Gram matrix of β_a with respect to the Singer basis $(s_0, \dots, s_{n-1})_w$. Then B_a is generated by the array $(0, \dots, 0, a, a^{q^{k+1}}, 0, \dots, 0)$, where a is in the k-th position. If $g \in \mathrm{GL}(V)$ fixes U_2, then it fixes also the set $\{\beta_a : a \in \mathbb{F}_{q^n}\}$. We use the same notation and arguments as in the proof of Theorem 3.1. Assume that $D_{\mathbf{g}}^t$ is generated by the array $(g_0, g_1, \dots, g_{n-1})$.

Since the q-circulant Gram matrix of β_a^g is generated by the array $(D_{\mathbf{g}}^t B_a D_{\mathbf{g}})_{(0)}$, the l-th entry, with $0 \leq l \leq n-1$, in $(D_{\mathbf{g}}^t B_a D_{\mathbf{g}})_{(0)}$ is given by the inner product $(D_{\mathbf{g}}^t B_a)_{(0)} \cdot D_{\mathbf{g}}^{(l)}$, with $D_{\mathbf{g}}^{(l)} = (g_{n-l}^{q^l}, g_{n-l+1}^{q^l}, \dots, g_{n-l-1}^{q^l})^t$, where subscripts are taken modulo n. As

$$(D_{\mathbf{g}}^t B_a)_{(0)} = (g_k a + g_{k+1}a^{q^{k+1}}, g_{k+1}a^q + g_{k+2}a^{q^{k+2}}, \dots, g_{k-1}a^{q^{n-1}} + g_k a^{q^k}),$$

the l-th entry of $(D_{\mathbf{g}}^t B_a D_{\mathbf{g}})_{(0)}$ is

$$\sum_{i=0}^{n-1}(g_{k+i}a^{q^i} + g_{k+1+i}a^{q^{k+1+i}})g_{n-l+i}^{q^l} = \sum_{i=0}^{n-1}(g_i g_{n-l+k+i}^{q^l} + g_{k+i}g_{n-l+i}^{q^l})a^{q^i}. \tag{11}$$

Since B_a is symmetric and g fixes U_2, we have

$$\sum_{i=0}^{n-1}(g_{k+i}g_{n-l+i}^{q^l} + g_i g_{n-l+k+i}^{q^l})a^{q^i} = 0$$

for $0 \leq l \leq k-1$ and all $a \in \mathbb{F}_{q^n}$. This implies

$$g_i g_{k-l+i}^{q^l} + g_{k+i}g_{n-l+i}^{q^l} = 0, \tag{12}$$

for $0 \le i \le n-1$ and $0 \le l \le k-1$. As $D^t_{\mathbf{g}}$ is non-singular, we may apply a suitable element in C, and hence assume $g_0 \neq 0$. Note that if the element g_0 appears in the equation (12), then either $i \in \{0, k+1\}$ or $i - l \in \{0, k+1\}$. In the former case, we have

$$\begin{cases} g_0 g_{k-l}^{q^l} + g_k g_{n-l}^{q^l} &= 0 \\ g_{k+1} g_{n-l}^{q^l} + g_0 g_{k+1-l}^{q^l} &= 0 \end{cases}, \quad \text{for } l = 0, \dots, k-1,$$

i.e.

$$\begin{cases} g_0 g_{1+l}^{q^l} + g_k g_{k+2+l}^{q^l} &= 0 \\ g_0 g_{2+l}^{q^l} + g_{k+1} g_{k+2+l}^{q^l} &= 0 \end{cases}, \quad \text{for } l = 0, \dots, k-1. \tag{13}$$

In the case $i - l \in \{0, k+1\}$, we have

$$\begin{cases} g_0^{q^i} g_{k+i} + g_k^{q^i} g_i &= 0 \quad \text{for } i = 0, \dots, k-1, \\ g_0^{q^{i+k}} g_i + g_{k+1}^{q^{i+k}} g_{k+i} &= 0 \quad \text{for } i = k+1, \dots, 2k. \end{cases} \tag{14}$$

Let q be odd. By putting $i = 0$ and $i = k+1$ in the first and in the second equation of (14), respectively, we get $g_k = g_{k+1} = 0$. Hence, from (13) and (14), we have $g_m = 0$ for $m = 1, \dots, k-1, k+2, \dots, n-1$, that is $g \in S$.

Let q be even. By applying a suitable element of S we may assume $g_0 = 1$. As $k > 1$, Equations (13) and (14) give

$$\begin{cases} g_{1+l}^{q^l} &= g_k g_{k+2+l}^{q^l} \\ g_{2+l}^{q^l} &= g_{k+1} g_{k+2+l}^{q^l} \end{cases}, \quad \text{for } l = 0, \dots, k-1, \tag{15}$$

and

$$\begin{cases} g_{k+i} &= g_k^{q^i} g_i \quad \text{for } i = 0, \dots, k-1, \\ g_i &= g_{k+1}^{q^{i+k}} g_{k+i} \quad \text{for } i = k+1, \dots, 2k. \end{cases} \tag{16}$$

Assume $g_k = 0$. Then $g_i = 0$ for $i = 1, \dots, 2k-1$, and $g_{2k} = 0$ from the second equation of (16), as $g_{k-1} = 0$. Therefore, $g \in S$.

Assume $g_{k+1} = 0$. Then $g_i = 0$ for $i = 2, \dots, 2k$, and $g_1 = 0$ from the first of (15), as $g_k = 0$. Therefore, $g \in S$.

Assume by contradiction that $g_k \neq 0 \neq g_{k+1}$. From (15) with $l = k-1$ we get

$$\begin{cases} g_k^{q^{k-1}} &= g_k \\ g_{k+1}^{q^{k-1}} &= g_{k+1} \end{cases}.$$

From the first of (13) with $l = 0$ we get $g_1 = g_k g_{k+2}$, which plugged in (16) with $i = k+2$ gives $g_{k+2} = g_{k+1}^q g_k g_{k+2}$. From (16) with $i = 1$ follows $g_1 \neq 0$, whence $g_{k+2} \neq 0$. Therefore, $g_{k+1}^q g_k = 1$, i.e. $g_k = (g_{k+1}^{-1})^q$. From the first equation of (15) we get

$$g_{1+l}^{q^l} g_{k+1}^q = g_{k+2+l}^{q^l}, \qquad \text{for } l = 0, \dots, k-1,$$

which for $l = 1$ gives $g_2^q g_{k+1}^q = g_{k+3}^q$, that is $g_2 g_{k+1} = g_{k+3}$, where $g_2 \neq 0$ from (16) with $i = 2$. By comparing this equation with (16) with $i = k+3$ we see that $g_{k+1} \in \mathbb{F}_q$, as n is odd. Thus, $g_k = g_{k+1}^{-1} \in \mathbb{F}_q$, and substituting this in (16) we have

$$g_i = g_{k+1} g_{k+i}, \tag{17}$$

for $i = 0, \dots, k-1, k+1, \dots, 2k$. Finally, induction on i in Eq. (17) provides

$$\begin{cases} g_i &= g_{k+1}^{2i} \\ g_{k+i+1} &= g_{k+1}^{2i+1} \end{cases}, \quad \text{for } i = 0, \dots, k-1,$$

that is,

$$\left\{\begin{array}{rcl} g_i & = & \alpha^{2i} \\ g_{k+i+1} & = & \alpha^{2i+1} \end{array}\right., \quad \text{for } i=0,\ldots,k-1,$$

for some non-zero $\alpha \in \mathbb{F}_q$, and $g_k = \alpha^{-1}$. Substituting once again these equalities in the second of (15) with $l = k-2$, we get $\alpha^n = 1$. Since g fixes U_2 setwise, also αg does. Therefore, we may assume that $D^t_{\mathbf{g}}$ is the q-circulant matrix generated by the array $(g_0, \ldots, g_{2k})$, where

$$\left\{\begin{array}{rcl} g_i & = & \alpha^{2i+1} \\ g_{k+i+1} & = & \alpha^{2i+2} \end{array}\right., \quad \text{for } i=0,\ldots,k-1, \text{ and } g_k = 1.$$

By taking into account that $g_i \in \mathbb{F}_q$, for $i \in \{0, \ldots, n-1\}$ and using (11), the k-th entry of $(D^t_{\mathbf{g}} B_a D_{\mathbf{g}})_{(0)}$ is

$$\begin{array}{rcl} \sum_{i=0}^{n-1} (g_i^2 + g_{k+i}g_{k+i+1})a^{q^i} & = & \sum_{i=0}^{k-1} (g_i^2 + g_{k+i}g_{k+i+1})a^{q^i} + (g_k^2 + g_{2k}g_0)a^{q^k} + \\ & & \sum_{i=k+1}^{n-1} (g_i^2 + g_{k+i}g_{k+i+1})a^{q^i} \\ & = & (\alpha^2+\alpha^2)a + \sum_{i=1}^{k-1} (\alpha^{4i+2} + \alpha^{2(i-1)+2}\alpha^{2i+2})a^{q^i} + \\ & & (1+\alpha^{2(k-1)+2}\alpha)a^{q^k} + \sum_{i=0}^{k-2} (\alpha^{4i+4} + \alpha^{2i+1}\alpha^{2(i+1)+1})a^{q^{k+i+1}} \\ & & +(\alpha^{4k} + \alpha^{2k-1})a^{q^{2k}}. \end{array}$$

As q is even and $\alpha^n = 1$, we see that the k-th entry of $(D^t_{\mathbf{g}} B_a D_{\mathbf{g}})_{(0)}$ is zero. On the other hand, since g fixes U_2, the q-circulant Gram matrix $D^t_{\mathbf{g}} B_a D_{\mathbf{g}}$ is associated with the polar form β_b, for some $b \in \mathbb{F}_{q^n} \setminus \{0\}$. This gives a contradiction. Hence, $g_k = g_{k+1} = 0$, and $g \in S$. This completes the proof. □

Remark 2. *In the particular case when n is a prime, Theorem 4.2 follows from a result of Kantor* [33].

Let us consider the orbit code $\mathcal{U}_2 = U_2\mathrm{GL}(V) = \{U_2^g : g \in \mathrm{GL}(V)\}$. From Theorem 4.2 and the Orbit-Stabilizer Theorem [2, p.16], we obtain the following result.

Corollary 3. *The size of $\mathcal{U}_2$ is*

$$\frac{q^{n(n-1)/2}\prod_{i=1}^{n-1}(q^i-1)}{n}.$$

Remark 3. *In the case $n = 3$, the orbit code $\mathcal{U}_2$ has minimum distance 4 and the group* $\mathrm{GL}(3, q)$ *acts transitively on it* [11].

At this point the main goal is the determination of the minimum distance of $\mathcal{U}_2$. We will do this in the case $n = 5$ by using geometric arguments, while this computation remains an open problem for $n > 5$ odd. However, before to do that we consider it appropriate to give here the representation over $\mathbb{F}_q$ of the subspace U_2 and of the set $\mathcal{U}_2$. If $(u_0, \ldots, u_{n-1})$ is an ordered basis for $V = V(n, q)$, and $v \in V$, write $v = x_0u_0 + \ldots + x_{n-1}u_{n-1} \in V$. Then, for any $Q \in \mathcal{Q}(V)$ we have

$$Q(v) = \sum_{i \leq j} a_{ij}x_ix_j,$$

for some $a_{ij} \in \mathbb{F}_q$, so Q can be identified with the homogeneous polynomial $\sum_{i \leq j} a_{ij}X_iX_j$ of degree two in the n coordinates X_i of V relative to the given basis; by abuse of notation we will denote this polynomial by $Q(\mathbf{X})$. Let $\mathcal{Q}(n, q)$ be the set of all the homogeneous polynomials of degree two over $\mathbb{F}_q$ in the variables X_i, $i = 0, \dots, n-1$. It is evident that $\{Q_{ij}(\mathbf{X}) = X_i X_j : 0 \le i \le j \le n-1\}$, is a basis for $\mathcal{Q}(n,q)$. Let C_{ij} be the $n \times n$ matrix over $\mathbb{F}_q$ whose all entries are all 0 but the (i,j)-entry which is 1. Then we may write $X_i X_j = \mathbf{X}^t C_{ij} \mathbf{X}$. If $Q \in \mathcal{Q}(V)$ corresponds to the polynomial $Q(\mathbf{X}) = \sum_{i \le j} a_{ij} X_i X_j$ in the given basis, then $Q(\mathbf{X})$ can be written as $\mathbf{X}^t C \mathbf{X} = \sum_{i \le j} a_{ij} \mathbf{X}^t C_{ij} \mathbf{X}$. Conversely, given any upper-triangular matrix C, then $\mathbf{X}^t C \mathbf{X} \in \mathcal{Q}(n,q)$, i.e. $Q(\mathbf{X}) = \mathbf{X}^t C \mathbf{X}$ is a quadratic form of $\mathbb{F}_q^n$. We denote by $\mathcal{T}(n,q)$ the set of all the upper triangular matrices over $\mathbb{F}_q$. It is evident that $\{C_{ij} : 0 \le i \le j \le n-1\}$ is a basis for $\mathcal{T}(n,q)$ and the map

$$\nu_{\{u_0,\dots,u_{n-1}\}} : \begin{array}{ccc} \mathcal{Q}(V) & \to & \mathcal{T}(n,q) \\ Q & \mapsto & (a_{ij})_{i \le j} \end{array} \tag{18}$$

is an isomorphism. To get the action of $A \in \mathrm{GL}(n,q)$ on $\mathcal{Q}(n,q)$ it suffices to know the action of A on $Q_{ij}(\mathbf{X})$ and then to extend it by linearity. To do this we need to write $Q_{ij}^A(\mathbf{X})$ in a matrix form. As $Q_{ij}(\mathbf{X}) = \mathbf{X}^t C_{ij} \mathbf{X}$, we first compute $C_{ij}^A = A^t C_{ij} A$ and then define the upper-triangular matrix $T(C_{ij}^A)$ as follows:

$$[T(C_{ij}^A)](k,l) = \begin{cases} C_{ij}^A(k,k) & \text{if } k = l; \\ C_{ij}^A(k,l) + C_{ij}^A(l,k) & \text{if } k < l; \\ 0 & \text{if } k > l. \end{cases}$$

It turns out that the coefficient of $X_k X_l$ in the polynomial $Q_{ij}^A(\mathbf{X})$ is precisely the (k,l)-entry of the matrix $T(C_{ij}^A)$.

We are now in position to give the q-ary representation of the subspace U_2 and the set $\mathcal{U}_2$. For $n = 2k+1$ and any $a \in \mathbb{F}_{q^n}$, the quadratic form $Q_a(\mathbf{x}) = \mathrm{Tr}_{q^n/q}\left(a x^{q^k+1}\right)$ can be written as $\mathbf{x}^t C_a \mathbf{x}$ where $\mathbf{x} = (x, x^q, \dots, x^{q^{n-1}})$, $x \in \mathbb{F}_{q^n}$, and

$$C_a = \begin{pmatrix} 0 & \cdots & 0 & a & a^{q^{k+1}} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & a^q & a^{q^{k+2}} & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & a^{q^k} \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix};$$

Therefore the $\mathbb{F}_q$-subspace U_2 can be identified with the $\mathbb{F}_q$-subspace $\{C_a : a \in \mathbb{F}_{q^n}\}$ of $\mathcal{T}(n,q^n)$, and the elements of $\mathcal{U}_2$ with the subspaces $\{T(C_a^{D_{\mathbf{g}}}) : a \in \mathbb{F}_{q^n}\}$, for all $D_{\mathbf{g}} \in \mathcal{I}_n(q^n)$. As we did for U_1 and $\mathcal{U}_1$, the representation of U_2 and $\mathcal{U}_2$ over $\mathbb{F}_q$ is obtained by considering the matrix E_n of the change of basis from $(v_0, \dots, v_{n-1})$ to the Singer basis $(s_0, \dots, s_{r-1})_w$. Therefore, the subspace U_2 can be identified with the $\mathbb{F}_q$-subspace $\{T(C_a^{E_n}) : a \in \mathbb{F}_{q^n}\}$ of $\mathcal{T}(n,q)$, and the elements of $\mathcal{U}_2 = U_2\mathrm{GL}(V)$ can be identified with the subspaces $\{T(D_a^{D_{\mathbf{g}} E_n}) : a \in \mathbb{F}_{q^n}\}$, for all $D_{\mathbf{g}} \in \mathcal{I}_n(\mathbb{F}_{q^n})$. At this point one can easily obtain the representation of the elements of $\mathcal{U}_2$ as subspaces of $\mathbb{F}_q^{n(n+1)/2}$.

Now set $V = V(5,q)$. In what follows we show that the orbit code $\mathcal{U}_2$ of $\mathcal{Q}(V)$ has minimum distance 8.

Lemma 4.3. *Let $a \in \mathbb{F}_{q^c} \setminus \mathbb{F}_q$ and let ℓ_a be the line of $\mathrm{PG}(\widehat{V})$ spanned by $\langle(a - a^q, a^{q^3} - a, 0, 0, 0)\rangle$ and $\langle(0, 0, a^{q^3} - a^q, a^q - a, 0)\rangle$. For any $x \in \mathbb{F}_{q^c} \setminus \mathbb{F}_q$, let δ_x denote* *the polarity of* $\mathrm{PG}(\widehat{V})$ *defined by the extension* $\widehat{\beta}_x$ *on* $\widehat{V}$ *of the polar form* β_x *of* Q_x*. Then, for each point* $P = \langle v \rangle \in \ell_a$*, the hyperplanes* P^{δ_x} *and* P^{δ_y} *coincide if and only if* $y = cx$*, for some* $c \in \mathbb{F}_q \setminus \{0\}$*.*

Proof. Let $v = (a_0, a_1, a_2, a_3, 0) = (\lambda(a - a^q), \lambda(a^{q^3} - a), \mu(a^{q^3} - a^q), \mu(a^q - a), 0)$, where $\lambda, \mu \in \mathbb{F}_{q^c}$ are not both zero. For any $x \in \mathbb{F}_{q^c} \setminus \mathbb{F}_q$, the hyperplane P^{δ_x} has equation

$$(xa_2 + x^{q^3} a_3)X_0 + x^q a_3 X_1 + x a_0 X_2 + (x^{q^3} a_0 + x^q a_1)X_3 + (x^{q^4} a_1 + x^{q^2} a_2)X_4 = 0.$$

The two hyperplanes P^{δ_x} and P^{δ_y} coincide if and only if the matrix

$$\begin{pmatrix} xa_2 + x^{q^3} a_3 & x^q a_3 & x a_0 & x^{q^3} a_0 + x^q a_1 & x^{q^4} a_1 + x^{q^2} a_2 \\ ya_2 + y^{q^3} a_3 & y^q a_3 & y a_0 & y^{q^3} a_0 + y^q a_1 & y^{q^4} a_1 + y^{q^2} a_2 \end{pmatrix}$$

has rank 1. This happens if and only if $y = cx$ for some $c \in \mathbb{F}_q \setminus \{0\}$. □

Theorem 4.4. *For any* $g \in \mathrm{GL}(V)$*,* $g \notin S \rtimes C$*, the subspaces* U_2 *and* U_2^g *meet either trivially or in a* 1*-dimensional* $\mathbb{F}_q$*-subspace.*

Proof. Throughout the proof, we will use the fact that every plane of $\mathrm{PG}(\widehat{V})$ containing two lines which are totally singular for a non-degenerate quadratic form contains no further singular point.

Let $g \in \mathrm{GL}(V)$, $g \notin S \rtimes C$ and assume that $(D_{\mathbf{g}}^{-1})^t$ is generated by the array $(k_0, \dots, k_4)$. Then

$$\mathbf{e}_i^{g^{-1}} = (k_{5-i}^{q^i}, k_{5-i+1}^{q^i}, \dots, k_{5-i-1}^{q^i})$$

for $i = 0, \dots, 4$, where indices are taken modulo 5.

For any $i = 0, \dots, 4$, the line $r_i = \langle \mathbf{e}_i, \mathbf{e}_{i+1} \rangle$ of $\mathrm{PG}(\widehat{V})$ is totally singular for each $\widehat{Q}_a \in U_2$, i.e. $\widehat{Q}_a|_{r_i} = 0$ and the lines $r_i^{g^{-1}} = \langle \mathbf{e}_i^{g^{-1}}, \mathbf{e}_{i+1}^{g^{-1}} \rangle$ are totally singular for the non-degenerate quadratic form $\widehat{Q}_a^g$. Note that the semilinear transformation $\bar{\tau}$ of $\widehat{V}$ with matrix (4) and associated automorphism $\alpha \in \mathbb{F}_{q^n} \mapsto \alpha^q \in \mathbb{F}_{q^n}$ fixes the cyclic model of V pointwise, maps r_i and $r_i^{g^{-1}}$ into r_{i+1} and $r_{i+1}^{g^{-1}}$, respectively.

Let $Q \in U_2 \cap U_2^g$. Suppose there is $Q' \in U_2 \cap U_2^g$, $Q' \notin \langle Q \rangle_{\mathbb{F}_q}$. By applying a suitable element in the Singer group S, we may assume $Q = Q_1$. Then $Q' = Q_a$, for some $a \in \mathbb{F}_{q^c} \setminus \mathbb{F}_q$. Thus the lines r_i and $r_i^{g^{-1}}$ are totally singular for both $\widehat{Q}_1$ and $\widehat{Q}_a$, for $i = 0, \dots, 4$. If $r_i^{g^{-1}} = r_j$, for some $j \in \{0, 1, 2, 3, 4\}$, then

$$r_{i+1}^{g^{-1}} = (r_i^{\bar{\tau}})^{g^{-1}} = (r_i^{g^{-1}})^{\bar{\tau}} = r_j^{\bar{\tau}} = r_{j+1}$$

and hence $\bigcup_{i=0}^4 r_i = \bigcup_{i=0}^4 r_i^{g^{-1}}$. Therefore $g^{-1} \in \mathrm{GL}(V)$ fixes $\{\langle \mathbf{e}_i \rangle : 0 \le i \le 4\}$ setwise, contradicting $g \notin S \rtimes C$. In particular observe that

$$\langle \mathbf{e}_i^{g^{-1}} \rangle \notin \{\langle \mathbf{e}_j \rangle : 1 \le j \le 4\}.$$

Let Π_4 be the hyperplane of $\mathrm{PG}(\widehat{V})$ with equation $X_4 = 0$. Assume that $r_i^{g^{-1}} = \langle \mathbf{e}_i^{g^{-1}}, \mathbf{e}_{i+1}^{g^{-1}} \rangle \subset \Pi_4$, for some $i = 0, \dots, 4$. Then $\mathbf{e}_i^{g^{-1}} = (w_0, w_1, w_2, 0, 0)$ and $\mathbf{e}_{i+1}^{g^{-1}} = (0, w_0^q, w_1^q, w_2^q, 0)$, for some $w_0, w_1, w_2 \in \mathbb{F}_{q^c}$ not all zero. Some computations show that $\widehat{Q}_1 \cap \widehat{Q}_a \cap \Pi_4 = r_0 \cup r_1 \cup r_2 \cup \ell_a$ and hence $r_i^{g^{-1}}$ should coincide with ℓ_a. This implies that $w_2 = w_0 = 0$, i.e., $r_i^{g^{-1}} = r_1$, a contradiction. Therefore, $r_i^{g^{-1}}$ is not contained in Π_4, for all $i = 0, \dots, 4$ and similarly the lines $r_i^{g^{-1}}$, $i = 0, \dots, 4$ are not contained in the hyperplanes $\Pi_j : X_j = 0$, for all $j = 0, \dots, 4$, since $\Pi_j^{\bar{\tau}} = \Pi_{j+1}$.

Let P be the point $r_i^{g^{-1}} \cap \Pi_4$. Note that P is a singular point for both $\widehat{Q}_1$ and $\widehat{Q}_a$, whence $P \in r_0 \cup r_1 \cup r_2 \cup \ell_a$.

Assume first $P = \langle \mathbf{e}_i^{g^{-1}} \rangle$, for some $i = 0, \ldots, 4$. If $\mathbf{e}_i^{g^{-1}} \in r_j \setminus \{\langle \mathbf{e}_j \rangle, \langle \mathbf{e}_{j+1} \rangle\}$, for some $j = 0, 1, 2$, then $\mathbf{e}_{i+1}^{g^{-1}} \in r_{j+1}$. This implies that $r_i^{g^{-1}}$ is contained in the plane $\langle r_j, r_{j+1} \rangle$ with $r_j \neq r_i^{g^{-1}} \neq r_{j+1}$, a contradiction. On the other hand, if $\mathbf{e}_i^{g^{-1}} \in \ell_a$, since $\langle \mathbf{e}_i^{g^{-1}} \rangle = r_i^{g^{-1}} \cap r_{i-1}^{g^{-1}}$, the hyperplane spanned by $r_i^{g^{-1}}$, $r_{i-1}^{g^{-1}}$ and ℓ_a should coincide with both P^{δ_1} and P^{δ_a}, contradicting Lemma 4.3. Then $P \neq \langle \mathbf{e}_i^{g^{-1}} \rangle$, $0 \leq i \leq 4$.

Note that at least one among $r_i^{g^{-1}}$ and $r_{i+1}^{g^{-1}}$ must intersect $r_0 \cup r_1 \cup r_2$. Therefore, up to the action of $\langle \bar{\tau} \rangle$, we may assume that $P = r_i^{g^{-1}} \cap \Pi_4 \in r_0$. Then $P^{\bar{\tau}^j} \in r_j$, for $j = 0, \ldots, 4$. We now show that both $\left(r_i^{g^{-1}}\right)^{\bar{\tau}^3}$ and $\left(r_i^{g^{-1}}\right)^{\bar{\tau}^4}$ meet ℓ_a. If $\left(r_i^{g^{-1}}\right)^{\bar{\tau}^3}$ meets r_0, then $\left(r_i^{g-1}\right)^{\bar{\tau}^3}$ should be contained in the hyperplane Π_2 spanned by r_0, r_3, r_4. Similarly, if $\left(r_i^{g^{-1}}\right)^{\bar{\tau}^3}$ meets r_1, then $\left(r_i^{g-1}\right)^{\bar{\tau}^3}$ should be contained in the hyperplane Π_0 spanned by r_1, r_2, r_3. If $\left(r_i^{g^{-1}}\right)^{\bar{\tau}^3}$ meets r_2, then the plane spanned by $\left(r_i^{g^{-1}}\right)^{\bar{\tau}^3}$ and $\left(r_i^{g^{-1}}\right)^{\bar{\tau}^2}$ should contain the further totally singular line r_2. In all these cases we get a contradiction. It follows that $\left(r_i^{g^{-1}}\right)^{\bar{\tau}^3}$ meets ℓ_a. Similarly $\left(r_i^{g^{-1}}\right)^{\bar{\tau}^4}$ intersects ℓ_a. This implies that the plane spanned by $\left(r_i^{g^{-1}}\right)^{\bar{\tau}^3}$ and $\left(r_i^{g^{-1}}\right)^{\bar{\tau}^4}$ would contain the further totally singular line ℓ_a, a contradiction. □

Theorem 4.5. *The set $\mathcal{U}_2 = U_2\mathrm{GL}(V)$ is an orbit code with parameters*

$$\left(15, \frac{q^{10}\prod_{i=1}^{4}(q^i-1)}{5}, 8, 5\right)_q .$$

Moreover, $\mathrm{GL}(V)$ *acts transitively on it.*

Proof. The result follows from Corollary 3 and Theorem 4.4. □

4.1. A GEOMETRIC INTERPRETATION. In this section we set $\theta_m = (q^m-1)/(q-1)$.

For any quadratic form Q on $V = V(n,q)$, $n = 2k+1$, the *quadric defined by* Q is the set $\mathfrak{Q}$ of points of $\mathrm{PG}(V)$ arising from the singular vectors of Q. We refer to the quadric defined by a non-singular quadratic form of V as a *parabolic quadric of* $\mathrm{PG}(V)$. For any set of k linearly independent quadratic forms $Q_1, \ldots, Q_r$ on V, let $\mathcal{L}$ be the subspace of $\mathcal{Q}(V)$ spanned by $Q_1, \ldots, Q_r$. The set of points $\mathcal{Z}_{\mathcal{L}} = \cap_{i=1}^{r}\mathfrak{Q}_i$ is contained in any quadric defined by an element of $\mathcal{L}$, and it is called the *base locus of* $\mathcal{L}$.

In [36], Kestenband proved that in $\mathcal{Q}(V)$, with $V = V(n,q)$ and both n and q odd, there exists an n-dimensional subspace $\mathcal{B}$ such that all its elements are non-degenerate and with the property that the parabolic quadrics defined by any r linearly independent elements of $\mathcal{B}$, $0 \leq r \leq n$, share θ_{n-r} singular points. In particular, the quadrics defined by any $n-2$ independent elements in $\mathcal{B}$ intersect in a $(q+1)$-cap of $\mathrm{PG}(V)$ [36, Theorem 1], where a $(q+1)$-*cap* of $\mathrm{PG}(V)$ is a set of $q+1$

points no three of which are collinear. Consider the following incidence structure: the *points* are the points of $\mathrm{PG}(V)$, the *lines* are the $(q+1)$-caps whose points are the common singular points of any $n-2$ independent elements in $\mathcal{B}$, and *incidence* is defined by inclusion. This incidence structure is a projective geometry Π isomorphic to $\mathrm{PG}(V)$ [36, Theorem 2]. In particular, the quadrics defined by the forms in $\mathcal{B}$ play the role of hyperplanes in Π, and the r-dimensional subspaces, $0 \leq r \leq n$, are the intersections of the quadrics defined by $n-1-r$ linearly independent elements from $\mathcal{B}$. However, no construction for the projective geometry Π was ruled out in [36] for n odd and q even. In this section, we fill this gap by showing that the incidence geometry Π can be constructed for any q by using the subspace U_2 defined by (10).

Lemma 4.6. *Let $\mathcal{L}$ be a r-dimensional subspace in $\mathcal{Q}(V)$ and let $\mathcal{Z}_{\mathcal{L}}$ be the base locus of $\mathcal{L}$. Then, every point P of* $\mathrm{PG}(V)$ *not in $\mathcal{Z}_{\mathcal{L}}$ lies in exactly θ_{r-1} quadrics defined by the quadratic forms of a $(r-1)$-dimensional subspace contained in $\mathcal{L}$.*

Proof. Let $\mathcal{L}$ be generated by the quadratic forms $Q_1, \ldots, Q_r$ on V, and let $P = \langle \mathbf{X} \rangle \notin \mathcal{Z}_{\mathcal{L}}$, with $\mathbf{X} = (X_0, \ldots, X_{n-1})$. As $(Q_1(\mathbf{X}), \ldots, Q_r(\mathbf{X})) \neq (0, \ldots, 0)$, the equation

$$\lambda_1 Q_1(\mathbf{X}) + \cdots + \lambda_k Q_r(\mathbf{X}) = 0 \tag{19}$$

is not trivial. It is then clear that the solutions $(\bar{\lambda}_1, \ldots, \bar{\lambda}_k)$ of (19) form a $(r-1)$-dimensional $\mathbb{F}_q$-vector space. □

Lemma 4.7. *Let $\mathcal{B}$ be an n-dimensional subspace of $\mathcal{Q}(V)$ such that each non-zero element is non-singular. Then the base locus of any r-dimensional subspace of $\mathcal{B}$ consists of θ_{n-r} points.*

Proof. Let $\mathcal{L}$ be a r-dimensional subspace of $\mathcal{B}$ and let $\mathcal{Z}_{\mathcal{L}}$ be its base locus. We count in two different ways the pairs $(P, \mathfrak{Q})$, where P is a point of $\mathrm{PG}(n-1,q) \setminus \mathcal{Z}_{\mathcal{L}}$, $\mathfrak{Q}$ is a quadric defined by a non-zero element of $\mathcal{L}$ and P is on $\mathfrak{Q}$. By using Lemma 4.6, we get

$$(\theta_n - |\mathcal{Z}_{\mathcal{L}}|)\, \theta_{r-1} = \theta_r\, (\theta_{n-1} - |\mathcal{Z}_{\mathcal{L}}|)\,.$$

This yields $|\mathcal{Z}_{\mathcal{L}}| = \theta_{n-r}$. □

Theorem 4.8. *Let $\mathcal{B}$ be an n-dimensional subspace of $\mathcal{Q}(V)$, such that each non-zero element is non-singular. Then the base locus of any $(n-2)$-dimensional subspace of $\mathcal{B}$ is a $(q+1)$-cap in* $\mathrm{PG}(V)$.

Proof. If $n = 3$, the quadric defined by a non-singular quadratic form consists of $q+1$ points of $\mathrm{PG}(2,q)$ no three of which are collinear [26]. Hence the theorem holds true in this case.

Assume $n > 3$. From Lemma 4.7 the base locus of $\mathcal{B}$ is empty, and, by Lemma 4.6, every point of $\mathrm{PG}(V)$ is contained in precisely the θ_{n-1} quadrics defined by the forms of an $(n-1)$-dimensional subspace contained in $\mathcal{B}$.

Let R and T be two distinct points of $\mathrm{PG}(V)$ and $\mathcal{L}_{R,T}$ be the $(n-2)$-dimensional subspace of $\mathcal{B}$ consisting of elements having both R and T as singular points. Note that the base locus of $\mathcal{L}_{R,T}$ consists of $q+1$ points by Lemma 4.7. Hence, two possibilities arise: either the line $\ell = \langle R, T \rangle$ is contained in the base locus of $\mathcal{L}_{R,T}$ or it does not. In the former case there are θ_{n-2} quadrics defined by members of $\mathcal{B}$ containing ℓ, whereas in the latter case there are θ_{n-3} quadrics defined by members of $\mathcal{B}$ containing ℓ. We denote by n_1 and n_2 the number of lines which are contained in θ_{n-2} and θ_{n-3} quadrics defined by members of $\mathcal{B}$, respectively. Clearly $n_1+n_2=\theta_n\theta_{n-1}/(q+1)$, which is the number of lines of $\mathrm{PG}(V)$. We recall that a parabolic quadric contains $\theta_{n-1}\theta_{n-3}/(q+1)$ lines [46, p.174].

We count in two different ways the pairs $(\ell,\mathfrak{Q})$, where ℓ is a line of $\mathrm{PG}(V)$ and $\mathfrak{Q}$ is a quadric defined by an element of $\mathcal{B}$ containing ℓ:

$$\begin{array}{rcl}\theta_n\frac{\theta_{n-1}\theta_{n-3}}{q+1} & = & n_1\theta_{n-2}+n_2\theta_{n-3}\\ & = & n_1(q^{n-3}+\theta_{n-3})+n_2\theta_{n-3}\\ & = & n_1q^{n-3}+(n_1+n_2)\theta_{n-3}\\ & = & n_1q^{n-3}+\frac{\theta_n\theta_{n-1}}{q+1}\theta_{n-3},\end{array}$$

which yields $n_1=0$. The result then follows. □

The subspace U_2 of $\mathcal{Q}(V)$ defined in Section 3, satisfies the hypothesis of Theorem 4.8 for any q and hence has the property that the base locus of any of its $(n-2)$-dimensional subspaces is a $(q+1)$-cap of the ambient projective space. Therefore we have the following result.

Theorem 4.9. *Let $\mathcal{P}$ denote the set of points of $\mathrm{PG}(V)$, $V=V(n,q)$, n odd. Then, in $\mathrm{PG}(V)$ there exists a family $\mathcal{K}$ of $(q+1)$-caps and an incidence relation $\mathcal{I}$ such that the incidence geometry $\Pi=(\mathcal{P},\mathcal{K},\mathcal{I})$ is isomorphic to $\mathrm{PG}(V)$.*

5. Orbit codes from Hermitian forms

For the whole section n is odd, $q=q_0^2$ and $\mathbf{x}=(x,x^q,\dots,x^{q^{n-1}})$, $x\in\mathbb{F}_{q^n}$.

Proposition 1. *The map*

$$h_a(\mathbf{x},\mathbf{y})=\mathrm{Tr}_{q^n/q}(axy^{q_0^n})$$

is a Hermitian form on V, for all $a\in\mathbb{F}_{q_0^n}$. Moreover, if $a\neq 0$, then h_a is non–degenerate.

Proof. We have

$$\begin{array}{rcl}h_a(\mathbf{y},\mathbf{x}) & = & ayx^{q_0^n}+a^qy^qx^{q_0^nq}+\dots+a^{q^{\frac{n-1}{2}}}y^{q^{\frac{n-1}{2}}}x^{q_0^nq^{\frac{n-1}{2}}}+\cdots\\ & = & ayx^{q_0^n}+a^qy^qx^{q_0^nq}+\dots+a^{q_0^{n-1}}y^{q_0^{n-1}}x^{q_0^{2n-1}}+\dots\end{array}$$

Therefore, $(h_a(\mathbf{y},\mathbf{x}))^{q_0}=\mathrm{Tr}_{q^n/q}(axy^{q_0^n})=h_a(\mathbf{x},\mathbf{y})$. The q-circulant Gram matrix of h_a, say H_a, is generated by the array $(0,\dots,0,a,0,\dots,0)$, with a in the $(n-1)/2$-th position. It is then clear that h_a is non–degenerate for $a\neq 0$. □

We set

$$U_3=\{h_a : a\in\mathbb{F}_{q_0^n}\}.$$

It easily seen that U_3 is an n-dimensional $\mathbb{F}_{q_0}$-vector subspace of $\mathcal{H}(V)$. Some computations show that the group $S\rtimes C$ fixes U_3. By arguing as in the proof of Theorem 3.1 the following result is obtained.

Theorem 5.1. *The stabilizer of U_3 in $\mathrm{GL}(V)$ is $S\rtimes C$, where S is the Singer cyclic group of $\mathrm{GL}(V)$ generated by σ and C is the cyclic group generated by τ.*

Corollary 4. *The set $\mathcal{U}_3=U_3\mathrm{GL}(V)$ has size*

$$\frac{q^{n(n-1)/2}\prod_{i=1}^{n-1}(q^i-1)}{n}.$$

The set $\mathcal{U}_3$ is an orbit code in $\mathcal{H}(V)$. In what follows we determine its minimum distance. Any Hermitian form $h_a \in U_3$ can be naturally extended to a semilinear map $\widehat{h}_a$ on $\widehat{V}$. Since the associated automorphism of $\widehat{h}_a$ is $\theta : x \in \mathbb{F}_{q^n} \mapsto x^{q_0} \in \mathbb{F}_{q^n}$, $\widehat{h}_a$ is not a Hermitian form. Note that $\widehat{h}_a$ is non-degenerate and hence it defines a correlation of $\mathrm{PG}(\widehat{V})$, with matrix H_a and companion automorphism θ. Therefore, $\widehat{h}_a$ maps the point $\langle (x_0, \ldots, x_{n-1}) \rangle$ into the hyperplane of equation

$$a x_{(n-1)/2}^{q_0} X_0 + a^{{q_0}^2} x_{(n+1)/2}^{q_0} X_1 + \cdots + a^{{q_0}^{n-2}} x_{(n-3)/2}^{q_0} X_{n-1} = 0,$$

where exponents and indices are taken modulo n.

Lemma 5.2. *Let $h_a, h_b \in U_3$ and $\widehat{h}_a, \widehat{h}_b$ be the corresponding correlations of* $\mathrm{PG}(\widehat{V})$, *respectively. Then the collineation $\psi = \widehat{h}_b \cdot \widehat{h}_a$ of $\mathrm{PG}(\widehat{V})$ is given by*

$$\begin{array}{llcl} \psi : & \mathrm{PG}(\widehat{V}) & \to & \mathrm{PG}(\widehat{V}) \\ & \langle (x_0, \ldots, x_{n-1}) \rangle & \mapsto & \langle (ab^{-1} x_{n-1}^{{q_0}^2}, (ab^{-1})^{{q_0}^2} x_0^{{q_0}^2}, \ldots, (ab^{-1})^{{q_0}^{2n-2}} x_{n-2}^{{q_0}^2}) \rangle, \end{array}$$

where exponents are taken modulo n.

Proof. Straightforward calculations show that the collineation ψ is represented by the q-circulant matrix $H_b^{-t} \overline{H}_a = H_{b^{-1}a}$ (which is generated by the array $(0, \ldots, 0, b^{-1}a, 0, \ldots, 0)$) and has θ^2 as a companion automorphism. □

Consider the following n-dimensional $\mathbb{F}_{q_0}$-vector space

$$V_0 = \{(x, x^{{q_0}^2}, \ldots, x^{{q_0}^{2n-2}}) : x \in \mathbb{F}_{q_0^n}\} \subset V.$$

The restriction ψ_0 of the collineation ψ to $\mathrm{PG}(V_0)$ is the projectivity given by

$$\begin{array}{lcl} \mathrm{PG}(V_0) & \to & \mathrm{PG}(V_0) \\ \langle (x, x^{{q_0}^2}, \ldots, x^{{q_0}^{2n-2}}) \rangle & \mapsto & \langle (ab^{-1}x, (ab^{-1})^{{q_0}^2} x^{{q_0}^2}, \ldots, (ab^{-1})^{{q_0}^{2n-2}} x^{{q_0}^{2n-2}}) \rangle. \end{array}$$

The projectivity ψ_0 naturally extends to the projectivity $\widehat{\psi}_0$ of $\mathrm{PG}(\widehat{V})$, whose q-circulant matrix is generated by the array $(ab^{-1}, 0, \ldots, 0)$. In addition, $\widehat{\psi}_0$ fixes each $\langle \mathbf{e}_i \rangle$, for $i = 0, \ldots, n-1$.

Theorem 5.3. *Let $g \in \mathrm{GL}(V)$, with $g \notin S \rtimes C$. Suppose that $D_{\mathbf{g}}^{-t}$ is generated by the array $(k_0, \ldots, k_{n-1})$ and that exactly $l+1 > 0$ entries of $(k_0, \ldots, k_{n-1})$ are non-zero, say $k_{i_0}, k_{i_1}, \ldots, k_{i_l}$, with $0 \le i_0 < i_1 < \ldots < i_l \le n-1$. Then the $\mathbb{F}_{q_0}$-vector subspaces U_3 and U_3^g meet either trivially or in a j-dimensional $\mathbb{F}_{q_0}$-subspace, where $j = \gcd(n, i_1 - i_0, \ldots, i_l - i_0)$.*

Proof. Assume that U_3 and U_3^g do not meet trivially, and let $h_a \in U_3 \cap U_3^g$, for some non-zero $a \in \mathbb{F}_{q_0^n}$. Let $h_b \in U_3 \cap U_3^g$, with $b \in \mathbb{F}_{q_0^n} \setminus \{0, a\}$. Note that $(D_{\mathbf{g}}^{-1})^{(i)} = \mathbf{e}_i^{g^{-1}} = (k_{n-i}^{q^i}, \ldots, k_{n-i-1}^{q^i})$. As $h_a, h_b \in U_3$, by Lemma 5.2, the linear collineation $\widehat{\psi}_0$ of $\mathrm{PG}(\widehat{V})$ fixes $\langle \mathbf{e}_i \rangle$ and $\langle \mathbf{e}_i^{g^{-1}} \rangle$, $0 \le i \le n-1$.

Assume first that $k_i \neq 0$ for all $i = 0, \ldots, n-1$. Then $\left\{ \langle \mathbf{e}_0 \rangle, \ldots, \langle \mathbf{e}_{n-1} \rangle, \langle \mathbf{e}_0^{g^{-1}} \rangle \right\}$ is a projective frame in $\mathrm{PG}(\widehat{V})$. Therefore $\widehat{\psi}_0$ is the identity. A similar argument as in Lemma 3.2 implies that $ab^{-1} = (ab^{-1})^{q_0^2}$. Since $ab^{-1} \in \mathbb{F}_{q_0^n}$, with n odd, then $ab^{-1} \in \mathbb{F}_{q_0} \setminus \{0\}$. Hence $U_3 \cap U_3^g = \langle h_a \rangle_{\mathbb{F}_{q_0}}$.

Assume now that $l+1 < n$ entries of $(k_0, \ldots, k_{n-1})$ are non-zero, say $k_{i_0}, k_{i_1}, \ldots, k_{i_l}$, with $0 \le i_0 < i_1 < \ldots < i_l \le n-1$. As the cyclic subgroup $\langle \tau \rangle$ fixes U_3, we may assume $k_0 \neq 0$, i.e., $i_0 = 0$. Then $\left\{ \langle \mathbf{e}_0 \rangle, \langle \mathbf{e}_{i_1} \rangle, \ldots, \langle \mathbf{e}_{i_l} \rangle, \langle \mathbf{e}_0^{g^{-1}} \rangle \right\}$ is a projective frame of the subspace Γ of $\mathrm{PG}(\widehat{V})$ spanned by $\langle \mathbf{e}_0\rangle, \langle \mathbf{e}_{i_1}\rangle, \ldots, \langle \mathbf{e}_{i_l}\rangle, \langle \mathbf{e}_0^{g^{-1}}\rangle$ and $\widehat{\psi}_0$ induces the identity on Γ. Therefore $ab^{-1} = (ab^{-1})^{q_0^{2im}}$, $1 \le m \le l$. It follows that $ab^{-1} \in \mathbb{F}_{q_0{}^j} \setminus \{0\}$, with $j = \gcd(n, 2i_1, \ldots, 2i_l) = \gcd(n, i_1, \ldots, i_l)$. This implies that U_3 and U_3^g intersect in a j-dimensional $\mathbb{F}_{q_0}$-subspace. □

Corollary 5. *For each $g \in \mathrm{GL}(V)$, $g \notin S \rtimes C$, the $\mathbb{F}_{q_0}$-subspaces U_3 and U_3^g have at most q_0^j elements in common, where $j < n$ is the greatest divisor of n.*

Theorem 5.4. *Let $j < n$ be the greatest divisor of n. Then $\mathcal{U}_3$ is an orbit code with parameters*

$$\left(n^2, \frac{q^{n(n-1)/2}\prod_{i=1}^{n-1}(q^i-1)}{n}, 2(n-j), n\right)_{q_0}.$$

Moreover, $\mathrm{GL}(V)$ *acts transitively on it.*

Proof. From Corollary 5, any two distinct elements of $\mathcal{U}_3$ meet either trivially or in a j-dimensional $\mathbb{F}_{q_0}$-subspace. □

Example 2. Let $n = 5$ and $q = q_0^2$. For any given $a \in \mathbb{F}_{q_0^5}$ the matrix of the Hermitian form h_a in the Singer basis $(s_0, \ldots, s_{n-1})_w$ is

$$D_a = \begin{pmatrix} 0 & 0 & a & 0 & 0 \\ 0 & 0 & 0 & a^{q_0^2} & 0 \\ 0 & 0 & 0 & 0 & a^{q_0^4} \\ a^{q_0} & 0 & 0 & 0 & 0 \\ 0 & a^{q_0^3} & 0 & 0 & 0 \end{pmatrix}.$$

Hence the $\mathbb{F}_q$-subspace U_3 of V can be identified with the $\mathbb{F}_{q_0}$-subspace $\{D_a : a \in \mathbb{F}_{q_0^5}\}$ in the Dickson matrix algebra $\mathcal{D}_5(\mathbb{F}_{q^5})$, and the codewords of $\mathcal{U}_3$ are the subspaces $\{D_{\mathbf{g}}^t D_a D_{\mathbf{g}} : a \in \mathbb{F}_{q_0^5}\}$ for any non-singular q-circulant matrix

$$D_{\mathbf{g}} = D_{(g_0,g_1,g_2,g_3,g_4)} = \begin{pmatrix} g_0 & g_1 & g_2 & g_3 & g_4 \\ g_4^q & g_0^q & g_1^q & g_2^q & g_3^q \\ g_3^{q^2} & g_4^{q^2} & g_0^{q^2} & g_1^{q^2} & g_2^{q^2} \\ g_2^{q^3} & g_3^{q^3} & g_4^{q^3} & g_0^{q^3} & g_1^{q^3} \\ g_1^{q^4} & g_2^{q^4} & g_3^{q^4} & g_4^{q^4} & g_0^{q^4} \end{pmatrix},$$

with $g_i \in \mathbb{F}_{q^5}$. Note that $D_{\mathbf{g}}^t D_a D_{\mathbf{g}} = D_{\mathbf{h}}$, with $\mathbf{h} = (h_0, \ldots, h_{n-1})$ where $h_l = \sum_{i=0}^5 g_{6-i} g_{3+l-i}^{q^i} a^{q^i}$.

Remark 4. The representation of U_3 and of the orbit code $\mathcal{U}_3$ as vectors of length n^2 over $\mathbb{F}_{q_0}$ are obtained by considering the matrix E_n of the change of basis from $(v_0, \ldots, v_{n-1})$ to the Singer basis $(s_0, \ldots, s_{r-1})_w$. The representation of U_3 into the q_0-vector space $\mathcal{H}(n,q)$ is the subspace $\{E_n^t D_a E_n : a \in \mathbb{F}_{q_0}\}$, and the codewords of $\mathcal{U}_3 = U_3\mathrm{GL}(V)$ are the subspaces $\{(D_{\mathbf{g}}E_n)^t D_a (D_{\mathbf{g}}E_n) : a \in \mathbb{F}_{q_0}\}$, for all $D_{\mathbf{g}} \in \mathcal{I}_n(\mathbb{F}_{q^n})$. Let $\{1, \zeta\}$ be a basis of $\mathbb{F}_q$ over $\mathbb{F}_{q_0}$. We write $x = x^{(1)} + x^{(2)}\zeta$, for any $x \in \mathbb{F}_{q_0^2}$. Then it is easy to see there exists a bijection from the $\mathcal{H}(n,q)$ and $V(n^2, q_0)$.

Remark 5. In the case $n = 5$, the orbit code $\mathcal{U}_2$ can be extended in such a way that the subspace distance is preserved by adding $(q^2+1)(q^2+q+1)$ codewords that are orbits of a suitable subgroup of $\mathrm{GL}(3,q)$, see [11]. So, it seems plausible that each of the orbit codes constructed in this paper could be enlarged by adding orbits of subspaces under the action of a suitable subgroup of GL(V).

References

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

[2] M. Aschbacher, *Finite Group Theory*, Cambridge Studies in Advanced Mathematics, 10. Cambridge University Press, Cambridge, 1986.

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

[4] O. Bottema, On the Betti-Mathieu group, *Nieuw Arch. Wisk.*, **16** (1930), 46–50.

[5] M. Braun, T. Etzion, P. R. J. Östergård, A. Vardy and A. Wassermann, Existence of q–analogs of Steiner systems, *Forum Math. Pi*, **4** (2016), e7, 14 pp.

[6] L. Carlitz, A Note on the Betti-Mathieu group, *Portugaliae mathematica*, **22** (1963), 121–125.

[7] B. Chen and H. Liu, Constructions of cyclic constant dimension codes, *Des. Codes Cryptogr.*, **86** (2018), 1267–1279.

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

[9] B. N. Cooperstein, External flats to varieties in PG($M_{n,n}$(GF(q))), *Linear Algebra Appl.*, **267** (1997), 175–186.

[10] A. Cossidente and F. Pavese, On subspace codes, *Des. Codes Cryptogr.*, **78** (2016), 527–531.

[11] A. Cossidente and F. Pavese, Veronese subspace codes, *Des. Codes Cryptogr.*, **81** (2016), 445–457.

[12] A. Cossidente and F. Pavese, Subspace codes in PG($2n-1,q$), *Combinatorica*, **37** (2017), 1073–1095.

[13] A. Cossidente, F. Pavese and L. Storme, Geometrical aspects of subspace codes, in *Network Coding and Subspace Designs*, 107–129, Signals Commun. Technol., Springer, Cham, 2018.

[14] A. Cossidente, F. Pavese and L. Storme, Optimal subspace codes in PG($4,q$), *Adv. Math. Commun.,* **13** (2019), 393–404.

[15] A. Cossidente, S. Kurz, G. Marino and F. Pavese, Combining subspace codes, preprint, arXiv:1911.03387.

[16] B. Csajbók and A. Siciliano, Puncturing maximum rank distance codes, *J. Algebraic Combin.*, **49** (2019), 507–534.

[17] P. Dembowski, *Finite Geometries*, Springer-Verlag, Berlin-New York, 1968.

[18] N. Durante and A. Siciliano, Non-linear maximum rank distance codes in the cyclic model for the field reduction of finite geometries, *Electron. J. Combin.*, **24** (2017), 18 pp.

[19] T. Etzion and A. Vardy, Error-correcting codes in projective space, *IEEE Trans. Inform. Theory*, **57** (2011), 1165–1173.

[20] T. Etzion and N. Silberstein, Error-correcting codes in projective spaces via rank- metric codes and Ferrers diagrams, *IEEE Trans. Inform. Theory*, **55** (2009), 2909–2919.

[21] T. Etzion and N. Silberstein, Codes and designs related to lifted MRD codes, *IEEE Trans. Inform. Theory*, **59** (2013), 1004–1017.

[22] G. Faina, G. Kiss, S. Marcugini and F. Pambianco, The cyclic model for PG($n-1,q$) and a construction of arcs, *European J. Combin.*, **23** (2002), 31–35.

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

[24] H. Gluesing-Luerssen and C. Troha, Construction of subspace codes through linkage, *Adv. Math. Commun.*, **10** (2016), 525–540.

[25] D. Heinlein, M. Kiermaier, S. Kurz and A. Wassermann, Tables of subspace codes, preprint, arXiv:1601.02864, 2016.

[26] J. W. P. Hirschfeld, *Projective Geometries Over Finite Fields*, 2nd ed., Clarendon Press, Oxford, 1998.

[27] A.-L. Horlemann-Trautmann, Message encoding and retrieval for spread and cyclic orbit codes, *Des. Codes Cryptogr.*, **86** (2018), 365–386.

[28] T. Honold, M. Kiermaier and S. Kurz, Partial spreads and vector space partitions, in *Network Coding and Subspace Designs*, 131–170, Signals Commun. Technol., Springer, Cham, 2018.

[29] T. Ho, R. Koetter, M. Médard, D. R. Karger and M. Effros, The benefits of coding over routing in a randomized setting, in *Proceedings of the 2003 IEEE international symposium on information theory (ISIT 2003)*, Yokohama, Japan. IEEE, (2003), p442.

[30] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi and B. Leong, A random linear network coding approach to multicast, *IEEE Trans. Inform. Theory*, **52** (2006), 4413–4430.

[31] A. L. Horlemann-Trautmann and J. Rosenthal, Constructions of constant dimension codes, in *Network Coding and Subspace Designs*, 25–42, Signals Commun. Technol., Springer, Cham, 2018.

[32] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin-New York, 1967.

[33] W. M. Kantor, Linear groups containing a Singer cycle, *J. Algebra*, **62** (1980), 232–234.

[34] A. Kohnert and S. Kurz, Construction of large constant-dimension codes with a prescribed minimum distance, *Lecture Notes in Computer Science*, **5393** (2008), 31–42.

[35] R. Kötter and F. R. Kschischang, Coding for errors and erasures in random network coding, *IEEE Trans. Inform. Theory*, **54** (2008), 3579–3591.

[36] B. C. Kestenband, Finite projective geometries that are incidence structures of caps, *Linear Algebra Appl.*, **48** (1982), 303–313.

[37] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997.

[38] K. Otal and F. Özbudak, Cyclic subspace codes via subspace polynomials, *Des. Codes Cryptogr.*, **85** (2017), 191–204.

[39] K. Otal and F. Özbudak, Constructions of cyclic subspace codes and maximum rank distance codes, in *Network Coding and Subspace Designs*, 43–66, Signals Commun. Technol., Springer, Cham, 2018.

[40] M. H. Poroch and A. A. Talebi, Product of symplectic groups and its cyclic orbit code, *Discrete Math. Algorithms Appl.*, **11** (2019), 1950061, 25 pp.

[41] N. Silberstein and A.-L. Trautmann, Subspace codes based on graph matchings, Ferrers diagrams, and pending blocks, *IEEE Trans. Inform. Theory*, **61** (2015), 3937–3953.

[42] D. Silva, F. R. Kschischang and R. Koetter, A rank-metric approach to error control in random network coding, *IEEE Trans. Inform. Theory*, **54** (2008), 3951–3967.

[43] J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.*, **43** (1938), 377–385.

[44] A.-L. Trautmann, F. Manganiello, M. Braun and J. Rosenthal, Cyclic orbit codes, *IEEE Trans. Inf. Theory*, **59** (2013), 7386–7404.

[45] A.-L. Trautmann, Isometry and automorphisms of constant dimension codes, *Adv. Math. Commun.*, **7** (2013), 147–160.

[46] D. E. Taylor, *The Geometry of the Classical Groups*, Sigma Series in Pure Mathematics, 9. Heldermann Verlag, Berlin, 1992.

[47] 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*, Dublin, Ireland, 2010, 1–4.

[48] Z.-X. Wan, *Geometry of matrices*, World Scientific Publishing Co. NJ, 1996.

[49] B. Wu and Z. Liu, Linearized polynomials over finite fields revisited, *Finite Fields Appl.*, **22** (2013), 79–100.

[50] S.-T. Xia and F.-W. Fu, Johnson type bounds on constant dimension codes, *Des. Codes Cryptogr.*, **50** (2009), 163–172.

Received April 2020; revised July 2020.

E-mail address: angela.aguglia@poliba.it
E-mail address: antonio.cossidente@unibas.it
E-mail address: giuseppe.marino@unina.it
E-mail address: francesco.pavese@poliba.it
E-mail address: alessandro.siciliano@unibas.it