An Orbital Construction of Optimum Distance Flag Codes

Clementa Alonso-González[1], Miguel Ángel Navarro-Pérez[1],
Xaro Soler-Escrivà[1]

Friday 6th November, 2020

Abstract

Flag codes are multishot network codes consisting of sequences of nested subspaces (flags) of a vector space $\mathbb{F}_q^n$, where q is a prime power and $\mathbb{F}_q$, the finite field of size q. In this paper we study the construction on $\mathbb{F}_q^{2k}$ of full flag codes having maximum distance (*optimum distance full flag codes*) that can be endowed with an orbital structure provided by the action of a subgroup of the general linear group. More precisely, starting from a subspace code of dimension k and maximum distance with a given orbital description, we provide sufficient conditions to get an optimum distance full flag code on $\mathbb{F}_q^{2k}$ having an orbital structure directly induced by the previous one. In particular, we exhibit a specific orbital construction with the best possible size from an orbital construction of a planar spread on $\mathbb{F}_q^{2k}$ that strongly depends on the characteristic of the field.

Keywords: Network coding, spreads, subspace codes, orbit codes, flag codes, general linear group.

1 Introduction

Random linear network coding is a powerful tool for data transmission over noisy and lossy networks. First introduced in [6], this network operates with *packets*, consisting of n symbols of a finite field $\mathbb{F}_q$ (for a prime power q), which can be interpreted as vectors in the vector space $\mathbb{F}_q^n$. The intermediate nodes of the network transmit random linear combinations of the packets they receive. The seminal paper in this area is [9], where Kötter and Kschischang realized that the vector subspace generated by the packets sent by the source is preserved in the

---

[1]Dpt. de Matemàtiques, Universitat d'Alacant, Sant Vicent del Raspeig, Ap. Correus 99, E – 03080 Alacant.
E-mail adresses: `clementa.alonso@ua.es`, `miguelangel.np@ua.es`, `xaro.soler@ua.es`.

network. Thus, they proposed to encode the information in vector subspaces of $\mathbb{F}_q^n$ and defined the *subspace channel*. In this setting, a *subspace code* is just a non-empy subset of the *projective space* $\mathcal{P}_q(n)$, which is the collection of all vector subspaces of $\mathbb{F}_q^n$. Since then, the study of these codes has led to many papers in recent years (see for instance [4] and the references inside). Most of this research focuses on the study of *constant dimension codes*, that is, subspace codes in which all subspaces have the same dimension (we refer the reader to [17] for a survey on constructions of these codes). A leading family of constant dimension codes are *spread codes* (or just *spreads*), since they attain the maximum possible distance and the largest size for that distance. A spread of $\mathbb{F}_q^n$ is a collection of subspaces of $\mathbb{F}_q^n$, all of the same dimension, which partition the ambient space. Such a family of subspaces exists if, and only if, their dimension divides n [14]. Within the scope of network coding, spread codes were introduced in [11]. Another interesting family of constant dimension codes is the one of *orbit codes*. First defined in [15], these codes appear as orbits of subspaces under the action of a subgroup of the general linear group, $GL(n, q)$. Many of the known families of constant dimension codes are, in fact, orbit codes [15]. Due to their orbital structure, the size of these codes clearly depends on the order of the acting group and their minimum distance can be computed in a simpler manner [16].

Subspace codes are also known as *one-shot subspace codes* since they use the subspace channel only once. In contrast, when the subspace channel is used many times, we talk about *multishot subspace codes* [13]. When the parameters q and n cannot be increased, multishot subspace codes arise as an interesting substitute of the standard subspace codes in order to improve efficiency. In this context, an *r-shot subspace code* over $\mathcal{P}_q(n)$ is a non-empty subset of $\mathcal{P}_q(n)^r$ and a *codeword* is just an r-tuple of subspaces of $\mathcal{P}_q(n)$, which is sent through the subspace channel using r shots.

In this paper, we focus on a special type of multishot subspace codes, in which the codewords are sequences of nested subspaces in $\mathcal{P}_q(n)$, that is, *flags*. The use of flags in network coding was introduced in [10], where the authors developed a network channel model for flags and provided constructions of flag codes using group actions. Later on, flag codes having maximum distance, called *optimum distance flag codes*, have been studied in [2, 3]. In [2], these flag codes are characterized in terms of the constant dimension codes used at each shot and, for $n = 2k$, it is proved that optimum distance full flag codes with the largest size are exactly those having a spread at the k-th shot. In the same paper, the authors provide a precise construction of these codes as well as a decoding algorithm.

The main objective of the present paper is to provide an orbital construction of optimum distance full flag codes on $\mathbb{F}_q^{2k}$ with the best size. Taking into account the results obtained in [2], we want to do this by extending to flags the orbital expression appearing in [15] of a specific planar spread $\mathcal{S}$ under the action of a particular group $\mathbf{G}$. In a general setting, given a subspace code of dimension k and maximum distance equipped with an orbital structure provided by the action

of a given subgroup of $GL(2k, q)$, we investigate how this action can be extended to the full flag variety on $\mathbb{F}_q^{2k}$ in such a way we obtain optimum distance full flag codes with an orbital structure directly inherited from the one fixed at dimension k. In particular, we conclude that the action of the chosen group $\mathbf{G}$ on the planar spread $\mathcal{S}$ cannot be properly extended to the flag codes level. Nevertheless, we find a suitable subgroup $\mathbf{H}$ of $\mathbf{G}$ whose action on $\mathcal{S}$ also works for full flags on $\mathbb{F}_q^{2k}$. This action, in addition, allows us to construct optimum distance full flag codes with the largest size and a number of orbits that deeply depends on the parity of the characteristic of the field $\mathbb{F}_q$.

The article is organized as follows. In Section 2 we summarize all the basic background we need on finite fields and subspace codes. Section 3 begins with a brief review of known results on flag codes, which leads to the study of some properties of orbit flag codes. We give sufficient conditions to obtain optimum distance orbit full flag codes on $\mathbb{F}_q^{2k}$ from orbit codes of dimension k with maximum distance. Moreover, we show that, under these conditions, such codes codes directly inherit the orbital structure fixed at dimension k. Section 4 is devoted to present a specific orbital construction of optimum distance full flag codes on $\mathbb{F}_q^{2k}$ with the best size. Taking $\mathcal{S}$ and $\mathbf{G}$ as in the preceding paragraph, we find a suitable subgroup $\mathbf{H}$ of $\mathbf{G}$, whose action on $\mathcal{S}$ can be extended to flags in the appropriate manner. In particular, by translation of the problem to the spread of lines of $\mathbb{F}_{q^k}^2$, we show that this group $\mathbf{H}$ provides a nice orbital description of the spread $\mathcal{S}$ strongly depending on the characteristic of the field. This orbital description of $\mathcal{S}$ naturally induces an orbital construction of optimum distance full flag codes with the best size as union of at most two orbits.

2 Preliminaries

In this section we collect some definitions and known results we will need later on. First, we give some background on finite fields; then we briefly review some concepts and facts on subspace codes and two special families of them: spread codes and orbit codes.

2.1 Finite fields

We recall some known facts about finite fields that can be found in [12].

Let q be a prime power. We denote the finite field of q elements by $\mathbb{F}_q$. Given a positive integer k, a generator α of the multiplicative cyclic group $\mathbb{F}_{q^k}^*$ is said to be a *primitive element* of the field $\mathbb{F}_{q^k}$. In this case, the multiplicative order of α is $q^k - 1$. Moreover, if $p(x) = x^k + \sum_{i=0}^{k-1} p_i x^i$ is the minimal polynomial of α over $\mathbb{F}_q$, we say that $p(x)$ is a *primitive polynomial* and we have the following isomorphisms of fields

$$\mathbb{F}_{q^k} \cong \mathbb{F}_q[x]/(p(x)) \cong \mathbb{F}_q[\alpha].$$

It turns out that the finite field $\mathbb{F}_{q^k}$ can be realized as $\mathbb{F}_{q^k} \cong \mathbb{F}_q[\alpha] = \{0\} \cup \langle\alpha\rangle$.

On the other hand, the *companion matrix* P of $p(x)$ over $\mathbb{F}_q$ is defined as the following $k \times k$ matrix

$$P = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -p_0 & -p_1 & -p_2 & \cdots & -p_{k-1} \end{pmatrix}.$$

The characteristic polynomial of P is $p(x)$. Therefore, the eigenvalues of P are precisely the zeros of $p(x)$, that is, the elements $\alpha, \alpha^q, \ldots, \alpha^{q^{k-1}}$. In particular, it follows that $\det(P) = \alpha^{1+q+q^2+\cdots+q^{k-1}} = \alpha^t$, where $t = \frac{q^k-1}{q-1}$. Moreover, the $\mathbb{F}_q$-algebra $\mathbb{F}_q[P]$ is isomorphic to the finite field $\mathbb{F}_{q^k}$, since the map

$$\begin{array}{cccc} \phi: & \mathbb{F}_q[\alpha] & \longrightarrow & \mathbb{F}_q[P] \\ & \sum_{i=0}^{k-1} a_i \alpha^i & \longmapsto & \sum_{i=0}^{k-1} a_i P^i \end{array} \tag{1}$$

is a field isomorphism mapping α into P. As a consequence, P is a primitive element of the field $\mathbb{F}_q[P]$, that is, P has multiplicative order $q^k - 1$ and $\mathbb{F}_q[P] = \{0\} \cup \langle P \rangle$.

2.2 Subspace codes, spreads and orbit codes

Given the finite field $\mathbb{F}_q$ and a positive integer n, the set of all vector subspaces of $\mathbb{F}_q^n$, denoted by $\mathcal{P}_q(n)$, is a metric space with respect to the subspace distance defined by

$$d_S(\mathcal{U}, \mathcal{V}) = \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2\dim(\mathcal{U} \cap \mathcal{V}) \tag{2}$$

for all $\mathcal{U}, \mathcal{V} \in \mathcal{P}_q(n)$. For any integer $k \in \{0, \ldots, n\}$, the set of all k-dimensional vector subspaces of $\mathbb{F}_q^n$ is called the *Grassmann variety* (or simply the *Grassmannian*) of dimension k and it is denoted by $\mathcal{G}_q(k, n)$. Thus, it follows that $\mathcal{P}_q(n) = \cup_{k=0}^n \mathcal{G}_q(k, n)$.

A *subspace code* is a non-empty set $\mathcal{C}$ of $\mathcal{P}_q(n)$ and the *minimum (subspace) distance* of $\mathcal{C}$ is defined as

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

Notice that $d_S(\mathcal{C}) > 0$ whenever $|\mathcal{C}| > 1$. If $|\mathcal{C}| = 1$, we put $d_S(\mathcal{C}) = 0$. A subspace code $\mathcal{C}$ is said to be a *constant dimension code* if $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$, for some dimension $k \in \{1, \ldots, n-1\}$. The minimum distance of such a code is an even integer and it is upper-bounded by $d_S(\mathcal{C}) \leqslant \min\{2k, 2(n-k)\}$. This bound is attained by codes in which the intersection of every two different subspaces has dimension equal to $\max\{0, 2k - n\}$ (see [9] for all the basics on subspace codes and constant dimension codes). Now, we introduce the concepts of spread and orbit codes, which are the families of constant dimension codes that we need in this paper.

4

2.2.1 Spreads

A k-dimensional *spread* of $\mathbb{F}_q^n$, or a *k-spread*, is a set of elements of $\mathcal{G}_q(k, n)$ that pairwise intersect trivially and cover the whole space $\mathbb{F}_q^n$. Spreads are geometrical objects (see [5, 14]) that can be used as constant dimension codes. In this case, we speak of *spread codes*. Spreads in $\mathcal{G}_q(k, n)$ exist if, and only if, k divides n. One can easily compute the minimum distance of a k-spread code of $\mathbb{F}_q^n$ as $2k$ and its cardinality as $(q^n - 1)/(q^k - 1)$ (see [5, 11]). It follows that spreads are an interesting type of constant dimension codes since they have the maximum possible distance and the best possible size for that distance. We will focus on *planar spreads*, that is, spreads where the sum of any two different elements covers the whole space $\mathbb{F}_q^n$. Equivalently, a planar spread is a k-spread of $\mathbb{F}_q^{2k}$.

We will use a concrete construction of planar spreads of $\mathbb{F}_q^{2k}$ inspired in the general construction of spreads due to Segre [14] and first used in the network coding setting in [11]. To do this, we use the matrix representation of a k-dimensional subspace $\mathcal{U} \in \mathcal{G}_q(k, n)$. A *generator matrix* $U \in \mathrm{Mat}_{k \times n}(\mathbb{F}_q)$ of $\mathcal{U}$, is a full-rank matrix whose rows form a basis of $\mathcal{U}$. Hence, $\mathcal{U} = \mathrm{rowsp}(U) = \{xU \mid x \in \mathbb{F}_q^k\}$.

Let P be the companion matrix of a primitive polynomial $p(x) \in \mathbb{F}_q[x]$ of degree k. If we denote by $0_k, I_k \in \mathrm{Mat}_{k \times k}(\mathbb{F}_q)$ respectively to the $k \times k$ zero and identity matrices, then the collection of subspaces

$$\mathcal{S} = \left\{ \mathrm{rowsp}(0_k | I_k), \mathrm{rowsp}(I_k | 0_k), \mathrm{rowsp}(I_k | P^i) \mid i = 0, \ldots, q^k - 2 \right\} \qquad (3)$$

is a planar spread code of $\mathbb{F}_q^{2k}$ (see [11]). In the same paper, the authors gave another way to view this spread by using the field isomorphism ϕ given in (1). Notice that the following map, which is called *field reduction map*, is a natural embedding of the Grassmannian of lines of $\mathbb{F}_{q^k}^2$ into $\mathcal{G}_q(k, 2k)$:

$$\begin{array}{cccc} \varphi : & \mathcal{G}_{q^k}(1, 2) & \longrightarrow & \mathcal{G}_q(k, 2k) \\ & \mathrm{rowsp}(x_1, x_2) & \longmapsto & \mathrm{rowsp}(\phi(x_1) | \phi(x_2)). \end{array} \qquad (4)$$

Clearly, $\mathcal{G}_{q^k}(1, 2)$ is a planar spread of $\mathbb{F}_{q^k}^2$ and, as proved in [11], $\varphi(\mathcal{G}_{q^k}(1, 2)) = \mathcal{S}$ is a planar spread of $\mathbb{F}_q^{2k}$. We will make use of this bijective map between $\mathcal{G}_{q^k}(1, 2)$ and $\mathcal{S}$ in the following sections.

2.2.2 Orbit codes

Constant dimension codes arising from group actions are called *orbit codes* and were introduced in [15]. In order to define them, we consider the general linear group of degree n over $\mathbb{F}_q$, denoted by $GL(n, q)$, composed of all invertible matrices of $\mathrm{Mat}_{n \times n}(\mathbb{F}_q)$. Now, given a full-rank matrix $U \in \mathrm{Mat}_{k \times n}(\mathbb{F}_q)$ and the subspace $\mathcal{U} = \mathrm{rowsp}(U) \in \mathcal{G}_q(k, n)$, one has the following group action on the

Grassmann variety:

$$\begin{array}{rcc} \mathcal{G}_q(k,n) \times GL(n,q) & \longrightarrow & \mathcal{G}_q(k,n) \\ (\mathcal{U}, A) & \longmapsto & \mathcal{U} \cdot A = \mathrm{rowsp}(UA). \end{array}$$

This operation is well-defined since it is independent from the generator matrix we choose for $\mathcal{U}$ (see [15]).

This action allows to construct constant dimension codes starting from a given subspace. To be precise, if $\mathcal{U}$ is a k-dimensional subspace of $\mathbb{F}_q^n$, its orbit under the action of some subgroup $\mathbf{T}$ on $\mathcal{G}_q(k,n)$ is a constant dimension code that we denote by

$$\mathrm{Orb}_{\mathbf{T}}(\mathcal{U}) = \{\mathcal{U} \cdot A \mid A \in \mathbf{T}\} \subseteq \mathcal{G}_q(k,n).$$

Codes constructed in this way are called *orbit codes*. The stabilizer of $\mathcal{U}$ under the action of $\mathbf{T}$ is the subgroup $\mathrm{Stab}_{\mathbf{T}}(\mathcal{U}) = \{A \in \mathbf{T} \mid \mathcal{U} \cdot A = \mathcal{U}\}$ and the size of the orbit code $\mathrm{Orb}_{\mathbf{T}}(\mathcal{U})$ is

$$|\mathrm{Orb}_{\mathbf{T}}(\mathcal{U})| = \frac{|\mathbf{T}|}{|\mathrm{Stab}_{\mathbf{T}}(\mathcal{U})|}.$$

Moreover, the minimum distance of $\mathrm{Orb}_{\mathbf{T}}(\mathcal{U})$ can be computed as

$$d_S(\mathrm{Orb}_{\mathbf{T}}(\mathcal{U})) = \min\{d_S(\mathcal{U}, \mathcal{U} \cdot A) \mid A \in \mathbf{T} \setminus \mathrm{Stab}_{\mathbf{T}}(\mathcal{U})\}.$$

The reader is referred to [15, 16] for a general background on orbit codes.

In [15] the authors suggest an orbital description of the planar spread $\mathcal{S}$ provided in (3). Let us recall it. For the rest of the paper, we fix $\mathcal{U}_k = \mathrm{rowsp}(I_k|0_k)$, that is, the standard k-dimensional vector subspace of $\mathbb{F}_q^{2k}$. If P is the companion matrix considered in (3), then

$$\mathcal{S} = \mathrm{Orb}_{\mathbf{G}}(\mathcal{U}_k) = \{\mathcal{U}_k \cdot A \mid A \in \mathbf{G}\} \subseteq \mathcal{G}_q(k, 2k), \tag{5}$$

where $\mathbf{G}$ is the following subgroup of $GL(2k, q)$

$$\mathbf{G} = \left\langle \begin{pmatrix} 0_k & I_k \\ I_k & 0_k \end{pmatrix}, \begin{pmatrix} I_k & P^i \\ 0_k & I_k \end{pmatrix} \ \middle| \ i = 0, \dots, q^k - 2 \right\rangle. \tag{6}$$

This orbital construction of $\mathcal{S}$, as the orbit of $\mathcal{U}_k$ under the action of the group $\mathbf{G}$, will be crucial in this paper.

3 Flag codes

Flag varieties on the vector space $\mathbb{F}_q^n$ are classical geometrical concepts that can be seen as an extension of Grassmann varieties. In the setting of network coding, the use of flags was introduced in [10]. We start the section by reviewing some known results on flag codes. Next, we will focus on studying some properties

of orbit flag codes. From there, we will give sufficient conditions to build orbit full flag codes on $\mathbb{F}_q^{2k}$ with the best possible distance from orbit codes in $\mathcal{G}(k, 2k)$ attaining the maximum distance. Finally, we show how to increase the cardinality of these flag codes by considering the union of orbits under the action of the same group.

3.1 Background on flag codes

A *flag* of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_q^n$, with $0 < t_1 < \cdots < t_r < n$, is an element $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ of $\mathcal{G}_q(t_1, n) \times \cdots \times \mathcal{G}_q(t_r, n) \subseteq \mathcal{P}_q(n)^r$ such that

$$\{0\} \subsetneq \mathcal{F}_1 \subsetneq \cdots \subsetneq \mathcal{F}_r \subsetneq \mathbb{F}_q^n.$$

We say that $\mathcal{F}_i$ is the *i-th subspace* of the flag $\mathcal{F}$. When the type vector is $(1, 2, \ldots, n-1)$, we speak about *full flags*. The *flag variety* of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_q^n$ is the space of flags of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_q^n$ and will be denoted by $\mathcal{F}_q((t_1, \ldots, t_r), n)$. It can be naturally endowed with a metric by extending the subspace distance provided in (2). Given $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ and $\mathcal{F}' = (\mathcal{F}'_1, \ldots, \mathcal{F}'_r)$ two flags in $\mathcal{F}_q((t_1, \ldots, t_r), n)$, the *flag distance* between $\mathcal{F}$ and $\mathcal{F}'$ is

$$d_f(\mathcal{F}, \mathcal{F}') = \sum_{i=1}^{r} d_S(\mathcal{F}_i, \mathcal{F}'_i).$$

A *flag code of type* $(t_1, \ldots, t_r)$ on $\mathbb{F}_q^n$ is a non-empty subset $\mathcal{C}$ of $\mathcal{F}_q((t_1, \ldots, t_r), n)$. The *minimum distance* of the flag code $\mathcal{C}$ is given by

$$d_f(\mathcal{C}) = \min\{d_f(\mathcal{F}, \mathcal{F}') \mid \mathcal{F}, \mathcal{F}' \in \mathcal{C}, \ \mathcal{F} \neq \mathcal{F}'\}.$$

If $|\mathcal{C}| = 1$, we put $d_f(\mathcal{C}) = 0$. Notice that $d_f(\mathcal{C})$ is upper bounded by (see [2])

$$d_f(\mathcal{C}) \leqslant 2 \left(\sum_{t_i \leqslant \lfloor \frac{n}{2} \rfloor} t_i + \sum_{t_i > \lfloor \frac{n}{2} \rfloor} (n - t_i) \right). \tag{7}$$

Flag codes attaining the bound (7) are called *optimum distance flag codes* and have been studied in [2, 3]. The *i-projected code* $\mathcal{C}_i$ of $\mathcal{C}$ is the constant dimension code given by the set of i-th subspaces of flags in $\mathcal{C}$, that is,

$$\mathcal{C}_i = \{\mathcal{F}_i \mid (\mathcal{F}_1, \ldots, \mathcal{F}_i, \ldots, \mathcal{F}_r) \in \mathcal{C}\} \subseteq \mathcal{G}_q(t_i, n),$$

for $i = 1, \ldots, r$ (see [2]). Notice that $1 \leqslant |\mathcal{C}_i| \leqslant |\mathcal{C}|$ for all $i = 1, \ldots, r$.

Having projected codes with the maximum possible distance is a necessary condition in order to obtain optimum distance flag codes, but it is not enough as it was proved in [2]. For this reason, in that paper, the concept of *disjointness* was introduced. The flag code $\mathcal{C}$ is said to be *disjoint* if $|\mathcal{C}_1| = \cdots = |\mathcal{C}_r| = |\mathcal{C}|$. Using this definition, one has the following characterization of optimum distance flag codes.

Theorem 3.1. *[2, Th. 3.11] Let $\mathcal{C}$ be a flag code of type $(t_1, \ldots, t_r)$. The following statements are equivalent:*

(i) *The code $\mathcal{C}$ is an optimum distance flag code.*

(ii) *The code $\mathcal{C}$ is disjoint and every projected code $\mathcal{C}_i$ attains the maximum possible distance.*

In [2] it is proved that, for $n = 2k$, optimum distance full flag codes with the largest size are exactly those having a planar spread as a projected code.

Theorem 3.2. *[2, Cor. 4.3] Let $\mathcal{C}$ be an optimum distance full flag code on $\mathbb{F}_q^{2k}$. Then $|\mathcal{C}| \leqslant q^k + 1$. Equality holds if, and only if, the k-projected code of $\mathcal{C}$ is a planar spread of $\mathbb{F}_q^{2k}$.*

3.2 Orbit flag codes

Since flags are sequences of subspaces of $\mathbb{F}_q^n$, the group action given in Section 2.2.2 on the Grassmannian can be easily extended to the space $\mathcal{F}_q((t_1, \ldots, t_r), n)$. Hence, given a flag $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_q^n$ and a subgroup $\mathbf{T}$ of $GL(n, q)$, the *orbit flag code* generated by $\mathcal{F}$ under the action of $\mathbf{T}$ is

$$\mathrm{Orb}_{\mathbf{T}}(\mathcal{F}) = \{\mathcal{F} \cdot A \mid A \in \mathbf{T}\} = \{(\mathcal{F}_1 \cdot A, \ldots, \mathcal{F}_r \cdot A) \mid A \in \mathbf{T}\} \subseteq \mathcal{F}_q((t_1, \ldots, t_r), n).$$

It follows that the size of an orbit flag code can be computed as

$$|\mathrm{Orb}_{\mathbf{T}}(\mathcal{F})| = \frac{|\mathbf{T}|}{|\mathrm{Stab}_{\mathbf{T}}(\mathcal{F})|},$$

where $\mathrm{Stab}_{\mathbf{T}}(\mathcal{F}) = \{A \in \mathbf{T} \mid \mathcal{F} \cdot A = \mathcal{F}\}$ denotes the stabilizer subgroup of the flag $\mathcal{F}$ under the action of $\mathbf{T}$ and its minimum distance is

$$d_f(\mathrm{Orb}_{\mathbf{T}}(\mathcal{F})) = \min\{d_f(\mathcal{F}, \mathcal{F} \cdot A) \mid A \in \mathbf{T} \setminus \mathrm{Stab}_{\mathbf{T}}(\mathcal{F})\}.$$

In this context, the projected codes of the orbit flag code $\mathrm{Orb}_{\mathbf{T}}(\mathcal{F})$ are orbit subspace codes and can be written as

$$\mathrm{Orb}_{\mathbf{T}}(\mathcal{F})_i = \mathrm{Orb}_{\mathbf{T}}(\mathcal{F}_i) \subseteq \mathcal{G}_q(t_i, n), \ i = 1, \ldots, r.$$

The next result states the relationship between the stabilizer subgroup of a flag and the ones of its subspaces under the action of the same group. The proof is straightforward.

Lemma 3.3. *With the previous notation, it holds*

$$\mathrm{Stab}_{\mathbf{T}}(\mathcal{F}) = \bigcap_{i=1}^{r} \mathrm{Stab}_{\mathbf{T}}(\mathcal{F}_i).$$

Remember that we say that a flag code is disjoint if its cardinality coincides with the ones of its projected codes. Since in the orbital scenario the cardinality of a code is extremely related with the order of the stabilizer subgroup, the previous lemma allows us to establish a stronger equivalence for disjointness. The proof is clear and we omit it.

Proposition 3.4. *Given a flag $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_q^n$ and a subgroup $\mathbf{T}$ of $GL(n, q)$, the following statements are equivalent:*

a) $\mathrm{Orb}_{\mathbf{T}}(\mathcal{F})$ *is a disjoint flag code.*

b) $\mathrm{Stab}_{\mathbf{T}}(\mathcal{F}) = \mathrm{Stab}_{\mathbf{T}}(\mathcal{F}_1) = \cdots = \mathrm{Stab}_{\mathbf{T}}(\mathcal{F}_r)$.

c) $\mathrm{Stab}_{\mathbf{T}}(\mathcal{F}_1) = \cdots = \mathrm{Stab}_{\mathbf{T}}(\mathcal{F}_r)$.

As stated in Section 2.2.2, the orbit of $\mathcal{U}_k = \mathrm{rowsp}(I_k | 0_k)$ under the action of the group $\mathbf{G}$ defined in (6) provides the planar spread $\mathcal{S}$ of $\mathbb{F}_q^{2k}$ (see (5)). Our intention is to study the extension of this action to full flags on $\mathbb{F}_q^{2k}$ in order to construct optimum distance orbit full flag codes with $\mathcal{S}$ as a projected code. Notice that, by means of Theorem 3.2, such codes would attain the maximum possible size as well. On the other hand, optimum distance flag codes are, in particular, disjoint (see Theorem 3.1). Hence, according to Proposition 3.4, we would need $\mathbf{G}$ to provide equal stabilizer subgroups when acting on every subspace of a suitable flag. Taking into account that the spread $\mathcal{S}$ is a subspace code with maximum distance, the next result gives us a necessary condition for our purpose valid for any subgroup of $GL(2k, q)$.

Proposition 3.5. *Let $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_{2k-1})$ be a full flag on $\mathbb{F}_q^{2k}$ and $\mathbf{T}$ a subgroup of $GL(2k, q)$ such that $\mathrm{Orb}_{\mathbf{T}}(\mathcal{F}_k)$ has maximum distance. Then $\mathrm{Stab}_{\mathbf{T}}(\mathcal{F}_i) \subseteq \mathrm{Stab}_{\mathbf{T}}(\mathcal{F}_k)$, for all $i \in \{1, \ldots, 2k-1\}$.*

Proof. Consider $A \in \mathbf{T}$ such that $\mathcal{F}_i = \mathcal{F}_i \cdot A$ for some $i \in \{1, \ldots, 2k-1\}$. Since $\mathcal{F}_k, \mathcal{F}_k \cdot A \in \mathrm{Orb}_{\mathbf{T}}(\mathcal{F}_k)$, we know that $d_S(\mathcal{F}_k, \mathcal{F}_k \cdot A) = 2k$, whenever $\mathcal{F}_k \neq \mathcal{F}_k \cdot A$. Then, either $\mathcal{F}_k \cap \mathcal{F}_k \cdot A = \{0\}$ or $\mathcal{F}_k = \mathcal{F}_k \cdot A$. Hence,

- if $1 \leqslant i \leqslant k$, we obtain that $\{0\} \neq \mathcal{F}_i = \mathcal{F}_i \cap \mathcal{F}_i \cdot A \subseteq \mathcal{F}_k \cap \mathcal{F}_k \cdot A$. Thus, $\mathcal{F}_k = \mathcal{F}_k \cdot A$.

- If $k < i \leqslant 2k-1$, the i-dimensional subspace $\mathcal{F}_i = \mathcal{F}_i \cdot A$ contains both $\mathcal{F}_k$ and $\mathcal{F}_k \cdot A$ and hence, $\mathcal{F}_k = \mathcal{F}_k \cdot A$. Otherwise, $\mathcal{F}_i$ would contain the whole space $\mathbb{F}_q^{2k} = \mathcal{F}_k \oplus \mathcal{F}_k \cdot A$, which is not possible.

Therefore, $\mathrm{Stab}_{\mathbf{T}}(\mathcal{F}_i) \subseteq \mathrm{Stab}_{\mathbf{T}}(\mathcal{F}_k)$ for all $i = 1, \ldots, 2k-1$. ∎

As a consequence of the previous results, we can enunciate a sufficient condition to build optimum distance orbit full flag codes on $\mathbb{F}_q^{2k}$ from constant dimension codes in $\mathcal{G}(k, 2k)$ attaining the maximum distance.

9

Proposition 3.6. *Let $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_{2k-1})$ be a full flag on $\mathbb{F}_q^{2k}$ and $\mathbf{T}$ a subgroup of $GL(2k, q)$ such that $\mathrm{Orb}_{\mathbf{T}}(\mathcal{F}_k)$ has maximum distance.*

If $\mathrm{Stab}_{\mathbf{T}}(\mathcal{F}_k) \subseteq \mathrm{Stab}_{\mathbf{T}}(\mathcal{F}_i)$, for all $i \in \{1, \ldots, 2k-1\}$, then $\mathrm{Orb}_{\mathbf{T}}(\mathcal{F})$ is an optimum distance full flag code of cardinality $|\mathrm{Orb}_{\mathbf{T}}(\mathcal{F}_k)|$.

Proof. If $\mathrm{Stab}_{\mathbf{T}}(\mathcal{F}_k) \subseteq \mathrm{Stab}_{\mathbf{T}}(\mathcal{F}_i)$, for all $i \in \{1, \ldots, 2k-1\}$, then $\mathbf{T}$ provides equal stabilizers when acting on all subspaces of $\mathcal{F}$, by Proposition 3.5. Hence, by means of Proposition 3.4, we obtain that $\mathrm{Orb}_{\mathbf{T}}(\mathcal{F})$ is a disjoint full flag code.

Now, we will show that $\mathrm{Orb}_{\mathbf{T}}(\mathcal{F})_i = \mathrm{Orb}_{\mathbf{T}}(\mathcal{F}_i)$ has the maximum possible distance, that is,

$$d_S(\mathrm{Orb}_{\mathbf{T}}(\mathcal{F}_i)) = \begin{cases} 2i & \text{if } i \leqslant k, \\ 2(2k-i) & \text{if } i > k. \end{cases}$$

Arguing by contradiction, suppose that for some dimension $1 \leqslant i \leqslant 2k-1$, the maximum possible distance is not attained. Hence, there must exist a matrix $A \in \mathbf{T} \setminus \mathrm{Stab}_{\mathbf{T}}(\mathcal{F}_i)$ such that

$$\begin{cases} \dim(\mathcal{F}_i \cap \mathcal{F}_i \cdot A) > 0 & \text{if } i \leqslant k, \\ \dim(\mathcal{F}_i \cap \mathcal{F}_i \cdot A) > 2(i-k) & \text{if } i > k. \end{cases}$$

In any case, A does not stabilize $\mathcal{F}_k$, since $\mathrm{Stab}_{\mathbf{T}}(\mathcal{F}_k) = \mathrm{Stab}_{\mathbf{T}}(\mathcal{F}_i)$. Thus, $d_S(\mathcal{F}_k, \mathcal{F}_k \cdot A) = d_S(\mathrm{Orb}_{\mathbf{T}}(\mathcal{F}_k)) = 2k$. This implies that $\mathcal{F}_k \cap \mathcal{F}_k \cdot A = \{0\}$ and $\mathcal{F}_k \oplus \mathcal{F}_k \cdot A = \mathbb{F}_q^{2k}$. Therefore,

- If $i \in \{1, \ldots k\}$, then $0 < \dim(\mathcal{F}_i \cap \mathcal{F}_i \cdot A) \leqslant \dim(\mathcal{F}_k \cap \mathcal{F}_k \cdot A) = 0$.

- If $i \in \{k, \ldots 2k-1\}$, then $\mathbb{F}_q^{2k} = \mathcal{F}_k \oplus \mathcal{F}_k \cdot A \subseteq \mathcal{F}_i + \mathcal{F}_i \cdot A$ and thus $\dim(\mathcal{F}_i \cap \mathcal{F}_i \cdot A) = 2(i-k)$.

Both cases lead us to a contradiction. We conclude that $\mathrm{Orb}_{\mathbf{T}}(\mathcal{F}_i)$ must have the maximum possible distance for all dimensions $i = 1, \ldots, 2k-1$, as stated.

Consequently, $\mathrm{Orb}_{\mathbf{T}}(\mathcal{F})$ is an optimum distance full flag code by Theorem 3.1. ∎

The following result is a particular case of the previous proposition.

Corollary 3.7. *Let $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_{2k-1})$ be a full flag on $\mathbb{F}_q^{2k}$ and $\mathbf{T}$ a subgroup of $GL(2k, q)$ such that $\mathrm{Orb}_{\mathbf{T}}(\mathcal{F}_k)$ has maximum distance.*

If $\mathrm{Stab}_{\mathbf{T}}(\mathcal{F}_k) = \{I_{2k}\}$, then $\mathrm{Orb}_{\mathbf{T}}(\mathcal{F})$ is an optimum distance full flag code.

From Proposition 3.6, we have that, under some condition on the stabilizers, if we start from an orbit subspace code of dimension k and maximum distance, the same action induces an optimum distance orbit full flag code with the same cardinality. This result is also true if we place as a starting code a constant dimension code of maximum distance consisting of more than one orbit. In other words, the orbital structure, the cardinality and the property of attaining the maximum distance of the starting subspace code of dimension k will be directly translated to the flag code level. We denote by $\dot{\cup}$ the disjoint union of sets.

Theorem 3.8. *Let $\{\mathcal{F}^j = (\mathcal{F}^j_1, \ldots, \mathcal{F}^j_{2k-1})\}^m_{j=1}$ be a set of full flags on $\mathbb{F}^{2k}_q$ and $\mathbf{T}$ a subgroup of $GL(2k, q)$ such that the subspaces $\mathcal{F}^1_k, \ldots, \mathcal{F}^m_k$ lie in different orbits of the action of $\mathbf{T}$ on $\mathcal{G}_q(k, 2k)$ and the union $\dot{\cup}^m_{j=1}\mathrm{Orb}_\mathbf{T}(\mathcal{F}^j_k)$ is a constant dimension code of maximum distance.*

If $\mathrm{Stab}_\mathbf{T}(\mathcal{F}^j_k) \subseteq \mathrm{Stab}_\mathbf{T}(\mathcal{F}^j_i)$, for all $i \in \{1, \ldots, 2k-1\}$ and for all $j \in \{1, \ldots, m\}$, then the union $\dot{\cup}^m_{j=1}\mathrm{Orb}_\mathbf{T}(\mathcal{F}^j)$ is an optimum distance full flag code with size $\sum^m_{j=1}|\mathrm{Orb}_\mathbf{T}(\mathcal{F}^j_k)|$.

Proof. By Proposition 3.6, we know that $\mathrm{Orb}_\mathbf{T}(\mathcal{F}^j)$ is an optimum distance full flag code, for $j = 1, \ldots, m$. Moreover, since the subspaces $\mathcal{F}^1_k, \ldots, \mathcal{F}^m_k$ lie in different orbits, there is no common subspace in different constant dimension codes $\mathrm{Orb}_\mathbf{T}(\mathcal{F}^j_k)$. Therefore, the union $\cup^m_{j=1}\mathrm{Orb}_\mathbf{T}(\mathcal{F}^j)$ contains exactly

$$\sum^m_{j=1}|\mathrm{Orb}_\mathbf{T}(\mathcal{F}^j)| = \sum^m_{j=1}|\mathrm{Orb}_\mathbf{T}(\mathcal{F}^j_k)|$$

flags. Hence, it suffices to show that, given A_1, $A_2 \in \mathbf{T}$ and $j_1, j_2 \in \{1, \ldots, m\}$ with $j_1 \neq j_2$, the distance between the flags $\mathcal{F}^{j_1} \cdot A_1$ and $\mathcal{F}^{j_2} \cdot A_2$ is maximum.

Notice that $\mathcal{F}^{j_1}_k \cdot A_1 \in \mathrm{Orb}_\mathbf{T}(\mathcal{F}^{j_1}_k)$ and $\mathcal{F}^{j_2}_k \cdot A_2 \in \mathrm{Orb}_\mathbf{T}(\mathcal{F}^{j_2}_k)$. Hence $\mathcal{F}^{j_1}_k \cdot A_1 \neq \mathcal{F}^{j_2}_k \cdot A_2$ and $d_S(\mathcal{F}^{j_1}_k \cdot A_1, \mathcal{F}^{j_2}_k \cdot A_2) = 2k$, by hypothesis. In other words, $\mathcal{F}^{j_1}_k \cdot A_1 \cap \mathcal{F}^{j_2}_k \cdot A_2 = \{0\}$ and $\mathcal{F}^{j_1}_k \cdot A_1 \oplus \mathcal{F}^{j_2}_k \cdot A_2 = \mathbb{F}^{2k}_q$. Then, it holds

$$\mathcal{F}^{j_1}_i \cdot A_1 \cap \mathcal{F}^{j_2}_i \cdot A_2 \subseteq \mathcal{F}^{j_1}_k \cdot A_1 \cap \mathcal{F}^{j_2}_k \cdot A_2 = \{0\}, \quad \text{for } 1 \leqslant i \leqslant k,$$

and

$$\mathbb{F}^{2k}_q = \mathcal{F}^{j_1}_k \cdot A_1 \oplus \mathcal{F}^{j_2}_k \cdot A_2 \subseteq \mathcal{F}^{j_1}_i \cdot A_1 + \mathcal{F}^{j_2}_i \cdot A_2, \quad \text{for } k+1 \leqslant i \leqslant 2k-1.$$

In both cases, $\mathcal{F}^{j_1}_i \cdot A_1 \cap \mathcal{F}^{j_2}_i \cdot A_2$ has the minimum possible dimension. It follows that $d_S(\mathcal{F}^{j_1}_i \cdot A_1, \mathcal{F}^{j_2}_i \cdot A_2)$ is the maximum possible distance, for all $i \in \{1, \ldots, 2k-1\}$. Therefore, $d_f(\mathcal{F}^{j_1} \cdot A_1, \mathcal{F}^{j_2} \cdot A_2)$ is the maximum possible distance between full flags on $\mathbb{F}^{2k}_q$, which finishes the proof. ∎

The previous result allows us to build optimum distance full flag codes on $\mathbb{F}^{2k}_q$ of higher cardinality as union of orbits under the action of the same group. Recall that, by means of Theorem 3.2, optimum distance full flag codes on $\mathbb{F}^{2k}_q$ with the maximum possible size are the ones with a k-spread as a projected code. Hence, given the acting group $\mathbf{T}$, the number of orbits needed to get full flag codes attaining both the maximum distance and cardinality coincides with the number of orbits in which $\mathbf{T}$ partitions the planar spread we use as a starting k-projected code.

Coming back to the action of the group $\mathbf{G}$ defined in (6), notice that if $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_{2k-1})$ is a full flag on $\mathbb{F}^{2k}_q$ with $\mathcal{F}_k \in \mathcal{S}$, where $\mathcal{S}$ is the planar spread defined in (3), the group $\mathbf{G}$ satisfies the first hypothesis of Proposition 3.6, since

$\mathrm{Orb}_{\mathbf{G}}(\mathcal{F}_k) = \mathcal{S}$. Hence, we just need $\mathrm{Stab}_{\mathbf{G}}(\mathcal{F}_k)$ to be a subgroup of any other $\mathrm{Stab}_{\mathbf{G}}(\mathcal{F}_i)$ in order to have that $\mathrm{Orb}_{\mathbf{G}}(\mathcal{F})$ is an optimum distance full flag code. However, the next example shows that $\mathbf{G}$ does not give equal stabilizers in general.

Example 3.9. Denote by $\mathcal{F} = (\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3)$ the standard full flag on $\mathbb{F}_2^4$, that is, the i-th subspace $\mathcal{F}_i$ of $\mathcal{F}$ is spanned by the first i rows of the 4×4 identity matrix. Let P be the companion matrix of the primitive polynomial $p(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ and consider the matrix group $\mathbf{G} \leqslant GL(4, 2)$ defined in (6). The orbit full flag code $\mathrm{Orb}_{\mathbf{G}}(\mathcal{F})$ has projected codes $\mathrm{Orb}_{\mathbf{G}}(\mathcal{F})_i = \mathrm{Orb}_{\mathbf{G}}(\mathcal{F}_i)$, for $i = 1, 2, 3$. In particular, since $\mathcal{F}_2 = \mathrm{rowsp}(I_2 \mid 0_2) = \mathcal{U}_2$, it follows by (5) that $\mathrm{Orb}_{\mathbf{G}}(\mathcal{F}_2) = \mathcal{S}$ is the planar spread given in (3). Moreover, $\mathrm{Orb}_{\mathbf{G}}(\mathcal{F}_1)$ and $\mathrm{Orb}_{\mathbf{G}}(\mathcal{F}_3)$ are collections of lines and hyperplanes of $\mathbb{F}_2^4$ respectively. Hence, all the projected codes of $\mathrm{Orb}_{\mathbf{G}}(\mathcal{F})$ attain the maximum possible distance. However, $\mathrm{Orb}_{\mathbf{G}}(\mathcal{F})$ is not an optimum distance full flag code. It suffices to consider the following matrix $A \in \mathbf{G}$:

$$A = \begin{pmatrix} P & 0_2 \\ 0_2 & P^2 \end{pmatrix} = \begin{pmatrix} 0_2 & I_2 \\ I_2 & 0_2 \end{pmatrix} \begin{pmatrix} I_2 & P^2 \\ 0_2 & I_2 \end{pmatrix} \begin{pmatrix} 0_2 & I_2 \\ I_2 & 0_2 \end{pmatrix} \begin{pmatrix} I_2 & P \\ 0_2 & I_2 \end{pmatrix} \begin{pmatrix} 0_2 & I_2 \\ I_2 & 0_2 \end{pmatrix} \begin{pmatrix} I_2 & P^2 \\ 0_2 & I_2 \end{pmatrix}$$

and the flag $\mathcal{F} \cdot A \in \mathrm{Orb}_{\mathbf{G}}(\mathcal{F})$. One has

$$\begin{aligned} \mathcal{F}_1 \cdot A &= \mathrm{rowsp} \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix} &\neq \mathcal{F}_1, \\ \mathcal{F}_2 \cdot A &= \mathrm{rowsp} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} &= \mathcal{F}_2, \end{aligned}$$

Then $A \in \mathrm{Stab}_{\mathbf{G}}(\mathcal{F}_2) \setminus \mathrm{Stab}_{\mathbf{G}}(\mathcal{F}_1)$. This shows that the flag code $\mathrm{Orb}_{\mathbf{G}}(\mathcal{F})$ is not disjoint by Proposition 3.4. Consequently $\mathrm{Orb}_{\mathbf{G}}(\mathcal{F})$ is not an optimum distance flag code.

Remark 3.10. In the light of Corollary 3.7, we see that, given a full flag $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_{2k-1})$ on $\mathbb{F}_q^{2k}$ with $\mathcal{F}_k \in \mathcal{S}$ and a subgroup $\mathbf{T}$ of $\mathbf{G}$, if the stabilizer of $\mathcal{F}_k$ under the action of $\mathbf{T}$ is trivial, then $\mathrm{Orb}_{\mathbf{T}}(\mathcal{F})$ is automatically an optimum distance flag code of size $|\mathbf{T}|$. Moreover, if $|\mathbf{T}| = |\mathcal{S}| = q^k + 1$, then $\mathbf{T}$ acts regularly (that is, transitively and providing trivial stabilizers) on $\mathcal{S}$ and the full flag orbit code $\mathrm{Orb}_{\mathbf{T}}(\mathcal{F})$ has $\mathcal{S}$ as its k-projected code. Consequently, $\mathrm{Orb}_{\mathbf{T}}(\mathcal{F})$ is an optimum distance full flag code with the best size. Nevertheless, take into account that the action of a subgroup $\mathbf{T}$ of $\mathbf{G}$ on $\mathcal{F}$ still could give optimum distance orbit full flag codes as long as the stabilizer subgroups of all the subspaces of the flag $\mathcal{F}$ coincide (Propositions 3.5 and 3.6). Therefore, by Theorem 3.8, if $|\mathbf{T}| = |\mathcal{S}|$ but the stabilizer subgroup of $\mathbf{T}$ on $\mathcal{F}_k$ is not trivial, we will need to increase the number of orbits to get an optimum distance flag code of size $|\mathcal{S}|$.

The following section is devoted to explore the existence of subgroups of $\mathbf{G}$ of order $q^k + 1$ whose action on a full flag $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_{2k-1})$ on $\mathbb{F}_q^{2k}$ with $\mathcal{F}_k \in \mathcal{S}$, provides disjoint full flag codes having $\mathcal{S}$ as its k-projected code as union of the minimum number of orbits.

4 An orbital construction of optimum distance flag codes

Let us fix $n = 2k$. The purpose of this section is to provide an orbital construction of optimum distance full flag codes on $\mathbb{F}_q^{2k}$ with the best size, $q^k + 1$, by using a subgroup of the group $\mathbf{G}$ defined in (6). To achieve this goal, we will proceed in several steps. First, we will deepen the structure of the group $\mathbf{G}$ in order to find a suitable subgroup $\mathbf{H}$. Secondly, this subgroup choice will give an orbital description of the Grassmannian of lines of $\mathbb{F}_{q^k}^2$ that induces an orbital construction of the planar spread $\mathcal{S}$ of $\mathbb{F}_q^{2k}$ defined in (3). Finally, by using Propositions 3.5, 3.6 and Theorem 3.8 we will prove that it is possible to extend the previous construction to flags giving rise to an orbital construction of optimum distance flag codes with the best size.

4.1 Obtaining a suitable subgroup

Although $\mathbf{G}$ is a subgroup of $GL(2k, q)$, the field isomorphism ϕ given in (1) induces the following group monomorphism ψ, which allows us to work on $GL(2, q^k)$:

$$
\begin{array}{rccc}
\psi: & GL(2, q^k) & \longrightarrow & GL(2k, q) \\
 & \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & \begin{pmatrix} \phi(a) & \phi(b) \\ \phi(c) & \phi(d) \end{pmatrix}.
\end{array}
\tag{8}
$$

In particular, one has that

$$
\psi \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & I_k \\ I_k & 0 \end{pmatrix} \text{ and } \psi \begin{pmatrix} 1 & \alpha^i \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} I_k & P^i \\ 0 & I_k \end{pmatrix},
$$

for $i = 0, \ldots, q^k - 2$. Thus, if we consider the group

$$
\bar{\mathbf{G}} = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & \alpha^i \\ 0 & 1 \end{pmatrix} \,\middle|\, i = 0, \ldots, q^k - 2 \right\rangle \leqslant GL(2, q^k),
$$

it is clear that $\psi(\bar{\mathbf{G}}) = \mathbf{G}$ and therefore $\bar{\mathbf{G}}$ and $\mathbf{G}$ are isomorphic groups.

The following statements show that $\bar{\mathbf{G}}$ is extremely related to the *special linear group* $SL(2, q^k)$, which consists of all matrices of $GL(2, q^k)$ with determinant 1.

Proposition 4.1. *[1, Proposition 2, page 57] If α is a generator of the multiplicative cyclic group $\mathbb{F}_{q^k}^*$, then*

$$
SL(2, q^k) = \left\langle \begin{pmatrix} 1 & \alpha^i \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \alpha^i & 1 \end{pmatrix} \,\middle|\, i = 0, \ldots, q^k - 2 \right\rangle
$$

Proposition 4.2. *The group $SL(2, q^k)$ is a subgroup of $\bar{\mathbf{G}}$. Moreover, if $\operatorname{char}(\mathbb{F}_q) = 2$, then $\bar{\mathbf{G}} = SL(2, q^k)$. In case of $\operatorname{char}(\mathbb{F}_q) \neq 2$, one has that $\bar{\mathbf{G}}$ is the semidirect product $\bar{\mathbf{G}} = SL(2, q^k) \rtimes \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle.$*

Proof. Observe that

$$\begin{pmatrix} 1 & 0 \\ \alpha^i & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & \alpha^i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

for all $0 \leqslant i \leqslant q^k - 2$. Thus $SL(2, q^k)$ is a subgroup of $\bar{\mathbf{G}}$ by Proposition 4.1. On the other hand, it is clear that $\begin{pmatrix} 1 & \alpha^i \\ 0 & 1 \end{pmatrix} \in SL(2, q^k)$, for all $0 \leqslant i \leqslant q^k - 2$. Moreover, if $\mathrm{char}(\mathbb{F}_q) = 2$, then $\det \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = 1$. Therefore $\bar{\mathbf{G}} = SL(2, q^k)$ in this case. If $\mathrm{char}(\mathbb{F}_q) \neq 2$, then the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ has multiplicative order two and it normalizes the subgroup $SL(2, q^k) \leqslant \bar{\mathbf{G}}$. Hence $\bar{\mathbf{G}}$ is the semidirect product of $\left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$ acting by conjugation on $SL(2, q^k)$. ∎

Now, recall the natural embedding φ of the Grassmannian of lines of $\mathbb{F}_{q^k}^2$ into $\mathcal{G}_q(k, 2k)$ defined in (4). Since $\varphi(\mathcal{G}_{q^k}(1, 2)) = \mathcal{S}$, the action of $\bar{\mathbf{G}}$ on $\mathcal{G}_{q^k}(1, 2)$ is equivalent to the action of $\mathbf{G}$ on $\mathcal{S}$ in the following sense: given $\bar{A} \in \bar{\mathbf{G}}$ and a line $l \in \mathcal{G}_{q^k}(1, 2)$ given by $l = \mathrm{rowsp}(x_1, x_2)$, it follows that

$$\varphi(l \cdot \bar{A}) = \varphi(\mathrm{rowsp}(x_1, x_2) \cdot \bar{A}) = \varphi(\mathrm{rowsp}(x_1, x_2)) \cdot \psi(\bar{A}) = \varphi(l) \cdot \psi(\bar{A}). \quad (9)$$

This way, we can work with the action of $\bar{\mathbf{G}}$ (or subgroups of $\bar{\mathbf{G}}$) on $\mathcal{G}_{q^k}(1, 2)$ by simplicity and then easily translate it to the action of $\mathbf{G}$ (or subgroups of $\mathbf{G}$) on $\mathcal{S}$ via φ. In particular, $\varphi(\mathrm{rowsp}(1, 0)) = \mathcal{U}_k$ and using (9) we obtain

$$\begin{aligned} \mathcal{S} = \mathrm{Orb}_{\mathbf{G}}(\mathcal{U}_k) &= \{\mathcal{U}_k \cdot A \mid A \in \mathbf{G}\} \\ &= \{\varphi(\mathrm{rowsp}(1, 0)) \cdot \psi(\bar{A}) \mid \bar{A} \in \bar{\mathbf{G}}\} \\ &= \{\varphi(\mathrm{rowsp}(1, 0) \cdot \bar{A}) \mid \bar{A} \in \bar{\mathbf{G}}\} \\ &= \varphi(\mathrm{Orb}_{\bar{\mathbf{G}}}(\mathrm{rowsp}(1, 0))). \end{aligned}$$

Consequently,

$$\mathcal{G}_{q^k}(1, 2) = \mathrm{Orb}_{\bar{\mathbf{G}}}(\mathrm{rowsp}(1, 0)) \quad (10)$$

since φ is injective. Thus, given that $\bar{\mathbf{G}}$ acts transitively on $\mathcal{G}_{q^k}(1, 2)$, we wonder if there is any subgroup of $\bar{\mathbf{G}}$ acting regularly on $\mathcal{G}_{q^k}(1, 2)$. To this end, we study first the existence of subgroups of order $q^k + 1$ in $\bar{\mathbf{G}}$.

Remark 4.3. Observe that we can restrict our study to subgroups of $SL(2, q^k)$. In case the characteristic is even, it is clear by Proposition 4.2. On the other hand, for odd characteristic, notice that the matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ has determinant equal to one. Hence,

$$\begin{aligned} \mathcal{G}_{q^k}(1, 2) &= \{\mathrm{rowsp}(0, 1), \mathrm{rowsp}(1, 0), \mathrm{rowsp}(1, \alpha^i) \mid i = 1, \ldots q^k - 2\} \\ &= \mathrm{Orb}_{SL(2, q^k)}(\mathrm{rowsp}(1, 0)) \end{aligned}$$

in both cases.

At this point, we take into account the existence of *Singer subgroups* of $SL(2, q^k)$ whose order is precisely $q^k + 1$. Singer subgroups of classical linear groups are well-known in finite group theory (see [7, 8] for instance). In general, a Singer subgroup of $GL(n, q)$ is a cyclic subgroup of order $q^n - 1$ generated by a *Singer cycle* or *cyclic projectivity* (see [5]). In our context and from [8], Singer subgroups of $GL(2, q^k)$ can be constructed in the following way. Let us consider a primitive element $\omega \in \mathbb{F}_{q^{2k}}$ and the companion matrix $M \in GL(2, q^k)$ of the minimal polynomial of ω over $\mathbb{F}_{q^k}$. The matrix M is called a *Singer cycle* of $GL(2, q^k)$ and any conjugate subgroup of $\langle M \rangle$ is said to be a *Singer subgroup* of $GL(2, q^k)$. Recall from Section 2.1 that the multiplicative order of M is equal to $q^{2k} - 1$ and that we have the field isomorphism

$$\mathbb{F}_{q^{2k}} \cong \mathbb{F}_{q^k}[M] = \{0\} \cup \langle M \rangle.$$

As a consequence, the group $\langle M \rangle$ acts regularly by multiplication on the elements of $\mathbb{F}_{q^{2k}}^* \cong \langle M \rangle$, which can be identified with the set of non-zero vectors of $\mathbb{F}_{q^k}^2$.

The intersection of a Singer subgroup of $GL(2, q^k)$ with $SL(2, q^k)$ is called a *Singer subgroup* of $SL(2, q^k)$. As it is stated in Section 2.1, the eigenvalues of M are ω and ω^{q^k} and $\det(M) = \omega^{q^k+1}$. Therefore, $\det(M^{q^k-1}) = \det(M)^{q^k-1} = 1$, since the multiplicative order of ω is $q^{2k} - 1$. Consequently, the group

$$\bar{\mathbf{H}} = \langle M \rangle \cap SL(2, q^k) = \langle M^{q^k-1} \rangle \tag{11}$$

is a Singer subgroup of $SL(2, q^k)$ and its order is $q^k + 1$. From now on, we fix this group $\bar{\mathbf{H}}$. Throughout the following section, we will study how $\bar{\mathbf{H}}$ acts on the set of lines of $\mathbb{F}_{q^k}^2$.

4.2   An orbital description of the spread of lines

As it was stated in (10), we know that $\mathcal{G}_{q^k}(1, 2) = \mathrm{Orb}_{\bar{\mathbf{G}}}(\mathrm{rowsp}(1, 0))$. Since $|\mathcal{G}_{q^k}(1, 2)| = |\bar{\mathbf{H}}| = q^k + 1$, it seems quite natural to wonder if $\bar{\mathbf{H}}$ acts regularly on $\mathcal{G}_{q^k}(1, 2)$. As we will see, this is true for even characteristic whereas for odd characteristic this action is not transitive and we obtain $\mathcal{G}_{q^k}(1, 2)$ as the union of exactly two orbits.

To do this, let us come back to the group $\langle M \rangle \subset GL(2, q^k)$ for a while and study its action on $\mathcal{G}_{q^k}(1, 2)$. Next we see that the set of matrices in $\langle M \rangle$ stabilizing an arbitrary line is exactly the group of scalar matrices.

Lemma 4.4. *Let l be an arbitrary line of $\mathcal{G}_{q^k}(1, 2)$. It holds that*

$$\mathrm{Stab}_{\langle M \rangle}(l) = \{aI_2 \mid a \in \mathbb{F}_{q^k}^*\}.$$

Proof. Let $A \in \mathrm{Stab}_{\langle M \rangle}(l)$ and consider a non-zero vector $(x_1, x_2) \in \mathbb{F}_{q^k}^2$ such that $l = \mathrm{rowsp}(x_1, x_2)$. Thus, $(x_1, x_2)A = a(x_1, x_2)$, for some $a \in \mathbb{F}_{q^k}^*$. Equivalently, $(x_1, x_2)(A - aI_2) = (0, 0)$. But $A - aI_2 \in \mathbb{F}_{q^k}[M]$, which is a field, and thus the only non-invertible matrix is the null matrix. It follows that $A = aI_2$ and the result is true since the other inclusion is trivial. ∎

From the definition of $\bar{\mathbf{H}}$ (see (11)), one has that $\mathrm{Stab}_{\bar{\mathbf{H}}}(l) = \mathrm{Stab}_{\langle M \rangle}(l) \cap SL(2, q^k)$ for any arbitrary line l in $\mathcal{G}_{q^k}(1, 2)$. Consequently, the next result follows directly from the previous lemma.

Lemma 4.5. *Let l be an arbitrary line of $\mathcal{G}_{q^k}(1, 2)$. It holds that*

$$\mathrm{Stab}_{\bar{\mathbf{H}}}(l) = \{aI_2 \mid a \in \mathbb{F}_{q^k}^*, \ a^2 = 1\} = \{I_2, -I_2\}.$$

Remark 4.6. Note that the stabilizer subgroups of $\bar{\mathbf{H}}$ on all the lines in $\mathcal{G}_{q^k}(1, 2)$ coincide. Moreover, if the field characteristic is even, this stabilizer is the trivial group. On the other hand, for odd characteristic, it consists of two elements, each of one fixing the whole set $\mathcal{G}_{q^k}(1, 2)$.

Proposition 4.7. *If $\mathrm{char}(\mathbb{F}_q) = 2$, then the group $\bar{\mathbf{H}}$ acts regularly on $\mathcal{G}_{q^k}(1, 2)$. If $\mathrm{char}(\mathbb{F}_q) \neq 2$, there are exactly two orbits of the action of $\bar{\mathbf{H}}$ on $\mathcal{G}_{q^k}(1, 2)$, each of them contains $\frac{q^k+1}{2}$ elements.*

Proof. If the field characteristic is even, the result is clear. Assume that $\mathrm{char}(\mathbb{F}_q) \neq 2$. From Lemma 4.5, we have that $\mathrm{Stab}_{\bar{\mathbf{H}}}(l) = \langle -I_2 \rangle$, for any line $l \in \mathcal{G}_{q^k}(1, 2)$. Hence, $\mathrm{Orb}_{\bar{\mathbf{H}}}(l)$ contains exactly $\frac{q^k+1}{2}$ lines and $\mathcal{G}_{q^k}(1, 2)$ is partitioned into two orbits with the same cardinality. ∎

In view of the previous result, the Grassmannian $\mathcal{G}_{q^k}(1, 2)$ can be described as a unique orbit in even characteristic. For odd characteristic, it is enough to consider a couple of lines lying in different orbits to describe $\mathcal{G}_{q^k}(1, 2)$ as the union of their respective orbits. As an example of this construction, the next result gives a specific partition of $\mathcal{G}_{q^k}(1, 2)$ in odd characteristic.

Proposition 4.8. *If $\mathrm{char}(\mathbb{F}_q) \neq 2$, then*

$$\mathcal{G}_{q^k}(1, 2) = \mathrm{Orb}_{\bar{\mathbf{H}}}(\mathrm{rowsp}(1, 0)) \ \dot{\cup} \ \mathrm{Orb}_{\bar{\mathbf{H}}}(\mathrm{rowsp}(0, 1)).$$

Proof. By means of Proposition 4.7, to prove the statement, it suffices to show that $\mathrm{Orb}_{\bar{\mathbf{H}}}(\mathrm{rowsp}(1, 0))$ and $\mathrm{Orb}_{\bar{\mathbf{H}}}(\mathrm{rowsp}(0, 1))$ are different orbits.

Arguing by contradiction, assume that $\mathrm{rowsp}(0, 1) \in \mathrm{Orb}_{\bar{\mathbf{H}}}(\mathrm{rowsp}(1, 0))$. Thus, there exist $A \in \bar{\mathbf{H}}$ such that $\mathrm{rowsp}(0, 1) = \mathrm{rowsp}(1, 0) \cdot A$, that is, the first row of A must be of the form $(0, a)$ for some $a \in \mathbb{F}_{q^k}^*$. On the other hand, recall that the first row of the companion matrix M is $(0, 1)$. It follows that the first row of $A - aM$ is the zero vector. But $A - aM \in \mathbb{F}_{q^k}[M]$, which is a field. Thus the

null matrix is the only non-invertible matrix on it. Therefore, $A = aM$ and, in particular, $A^{\frac{q^{2k}-1}{2}} = (aM)^{\frac{q^{2k}-1}{2}}$. Now, since $q^k - 1$ is an even number, we can put

$$A^{\frac{q^{2k}-1}{2}} = (A^{q^k+1})^{\frac{q^k-1}{2}} = I_2,$$

since $A \in \bar{\mathbf{H}}$ and $|\bar{\mathbf{H}}| = q^k + 1$. In contrast,

$$(aM)^{\frac{q^{2k}-1}{2}} = a^{\frac{q^{2k}-1}{2}} M^{\frac{q^{2k}-1}{2}} = (a^{q^k-1})^{\frac{q^k+1}{2}} M^{\frac{q^{2k}-1}{2}} = M^{\frac{q^{2k}-1}{2}}$$

since a is a element of the group $\mathbb{F}_{q^k}^*$. We conclude that $M^{\frac{q^{2k}-1}{2}} = I_2$, which is a contradiction since the order of M is $q^{2k} - 1$. ∎

Remark 4.9. At this point, a natural question is if, for odd characteristic, there exist any other subgroup of order $q^k + 1$ of $\bar{\mathbf{G}}$ providing the spread of lines of $\mathbb{F}_{q^k}^2$ as the unique orbit of a regular action. The answer to this question is that it is not true in general. For instance, if $q = 3$ and $k = 2$, we have checked by using GAP, that there is no subgroup of order $q^k + 1 = 10$ of $\bar{\mathbf{G}} \cong SL(2, 9) \rtimes C_2$ acting transitively on $\mathcal{G}_9(1, 2)$ (by C_2 we denote the cyclic group of order 2).

4.3 From the spread of lines to the planar spread $\mathcal{S}$

Now, we will translate the orbital structure of $\mathcal{G}_{q^k}(1, 2)$ under the action of $\bar{\mathbf{H}}$, studied in the previous section, to the planar spread $\mathcal{S}$ of $\mathbb{F}_q^{2k}$ defined in (3). To do so, we will use the field reduction map φ defined in (4) and the group monomorphism ψ defined in (8). Let us consider $\mathbf{H} = \psi(\bar{\mathbf{H}})$, the subgroup of $\mathbf{G}$ isomorphic to $\bar{\mathbf{H}}$ via ψ.

With this notation, the following lemma states that all subspaces in $\mathcal{S}$ have the same stabilizer subgroup under the action of $\mathbf{H}$.

Lemma 4.10. *Let $\mathcal{L}$ be an arbitrary subspace in $\mathcal{S}$. It holds that*

$$\mathrm{Stab}_{\mathbf{H}}(\mathcal{L}) = \{I_{2k}, -I_{2k}\}.$$

Proof. Since $\mathcal{S} = \varphi(\mathcal{G}_{q^k}(1, 2))$, there exists a line $l \in \mathcal{G}_{q^k}(1, 2)$ such that $\varphi(l) = \mathcal{L}$. Now, using the equivalence of the action provided in (9), it is clear that $\mathrm{Stab}_{\mathbf{H}}(\mathcal{L}) = \psi(\mathrm{Stab}_{\bar{\mathbf{H}}}(l))$. Thus, the result follows from Lemma 4.5. ∎

Now, the orbital structure of the planar spread $\mathcal{S}$ under the action of $\mathbf{H}$ can be described straightforwardly:

Theorem 4.11. *If $\mathrm{char}(\mathbb{F}_q) = 2$, then $\mathbf{H}$ acts regularly on $\mathcal{S}$. If $\mathrm{char}(\mathbb{F}_q) \neq 2$, then there are exactly two orbits of the action of $\mathbf{H}$ on $\mathcal{S}$, each of them with the same cardinality $\frac{q^k+1}{2}$.*

Proof. Assume that $\text{char}(\mathbb{F}_q) = 2$ and consider an arbitrary subspace $\mathcal{L} \in \mathcal{S}$. Since $\mathcal{S} = \varphi(\mathcal{G}_{q^k}(1,2))$, there exists a line $l \in \mathcal{G}_{q^k}(1,2)$ such that $\varphi(l) = \mathcal{L}$. Now, Proposition 4.7 states that $\mathcal{G}_{q^k}(1,2) = \text{Orb}_{\bar{\mathbf{H}}}(l)$ and we can use (9) to see that

$$\mathcal{S} = \varphi(\mathcal{G}_{q^k}(1,2)) = \varphi(\text{Orb}_{\bar{H}}(l)) = \{\varphi(l \cdot \bar{A}) \mid \bar{A} \in \bar{\mathbf{H}}\} = \{\mathcal{L} \cdot A \mid A \in \mathbf{H}\} = \text{Orb}_{\mathbf{H}}(\mathcal{L}).$$

Suppose now that $\text{char}(\mathbb{F}_q) \neq 2$. By Proposition 4.7, we know that

$$\mathcal{G}_{q^k}(1,2) = \text{Orb}_{\bar{\mathbf{H}}}(l_1) \mathbin{\dot{\cup}} \text{Orb}_{\bar{\mathbf{H}}}(l_2),$$

where $l_1, l_2 \in \mathcal{G}_{q^k}(1,2)$ lie in different orbits under the action of $\bar{\mathbf{H}}$. Let $\mathcal{L}_1, \mathcal{L}_2 \in \mathcal{S}$ such that $\varphi(l_1) = \mathcal{L}_1$ and $\varphi(l_2) = \mathcal{L}_2$. Then, we have that

$$\varphi(\text{Orb}_{\bar{\mathbf{H}}}(l_i)) = \{\varphi(l_i \cdot \bar{A}) \mid \bar{A} \in \bar{\mathbf{H}}\} = \{\mathcal{L}_i \cdot A \mid A \in \mathbf{H}\} = \text{Orb}_{\mathbf{H}}(\mathcal{L}_i),$$

for $i = 1, 2$. In particular, $\text{Orb}_{\mathbf{H}}(\mathcal{L}_i)$ has $\frac{q^k+1}{2}$ elements since φ is injective. Moreover,

$$\begin{aligned} \mathcal{S} = \varphi(\mathcal{G}_{q^k}(1,2)) &= \varphi(\text{Orb}_{\bar{\mathbf{H}}}(l_1) \mathbin{\dot{\cup}} \text{Orb}_{\bar{\mathbf{H}}}(l_2)) \\ &= \varphi(\text{Orb}_{\bar{\mathbf{H}}}(l_1)) \mathbin{\dot{\cup}} \varphi(\text{Orb}_{\bar{\mathbf{H}}}(l_2)) = \text{Orb}_{\mathbf{H}}(\mathcal{L}_1) \mathbin{\dot{\cup}} \text{Orb}_{\mathbf{H}}(\mathcal{L}_2). \end{aligned}$$

∎

Recall that $\mathcal{U}_k = \text{rowsp}(I_k|0_k) \in \mathcal{G}_q(k, 2k)$. Now we denote $\mathcal{V}_k = \text{rowsp}(0_k|I_k) \in \mathcal{G}_q(k, 2k)$. Since $\varphi(\text{rowsp}(1,0)) = \mathcal{U}_k$ and $\varphi(\text{rowsp}(0,1)) = \mathcal{V}_k$, by (9) and Proposition 4.8, in odd characteristic we have a nice orbital description of the spread $\mathcal{S}$.

Proposition 4.12. *If* $\text{char}(\mathbb{F}_q) \neq 2$, *then* $\mathcal{S} = \text{Orb}_{\mathbf{H}}(\mathcal{U}_k) \mathbin{\dot{\cup}} \text{Orb}_{\mathbf{H}}(\mathcal{V}_k)$.

Remark 4.13. By Remark 4.9 and using the equivalent action provided by (9), for odd characteristic, it is not possible, in general, to obtain $\mathcal{S}$ as the only orbit of the regular action of a subgroup (of order $q^k + 1$) of $\mathbf{G}$.

4.4   From the planar spread $\mathcal{S}$ to flags

In this section we will focus on how to extend the action of $\mathbf{H}$ on k-dimensional subspaces given in Section 4.3 to full flags on $\mathbb{F}_q^{2k}$, in order to obtain flag codes with the maximum distance having the spread $\mathcal{S}$ defined in (3) as its k-projected code. The following results show that $\mathbf{H}$ always provides optimum distance full flag codes of the best size as the union of at most two orbits.

Theorem 4.14. *Let* $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_{2k-1})$ *be a full flag on* $\mathbb{F}_q^{2k}$ *such that* $\mathcal{F}_k \in \mathcal{S}$.
  If $\text{char}(\mathbb{F}_q) = 2$, *then* $\text{Orb}_{\mathbf{H}}(\mathcal{F})$ *is an optimum distance full flag code with the largest possible size, which is* $q^k + 1$.
  If $\text{char}(\mathbb{F}_q) \neq 2$, *then* $\text{Orb}_{\mathbf{H}}(\mathcal{F})$ *is an optimum distance full flag code with size* $\frac{q^k+1}{2}$.

Proof. Since $\mathcal{F}_k \in \mathcal{S}$, it is clear that $\mathrm{Orb}_{\mathbf{H}}(\mathcal{F}_k)$ has maximum distance. Moreover, Lemma 4.10 states that $\mathrm{Stab}_{\mathbf{H}}(\mathcal{F}_k)$ stabilizes $\mathcal{F}_i$ for all $i = 1, \ldots, 2k - 1$. Therefore, Proposition 3.6 allows us to conclude that $\mathrm{Orb}_{\mathbf{H}}(\mathcal{F})$ is an optimum distance full flag code of cardinality $|\mathrm{Orb}_{\mathbf{H}}(\mathcal{F})| = |\mathrm{Orb}_{\mathbf{H}}(\mathcal{F}_k)|$. Finally, this cardinality is given by Theorem 4.11. ∎

For odd characteristic, we can give an optimum distance full flag code of the largest possible size by considering the union of two orbit flag codes constructed as in Theorem 4.14 and using Theorem 3.8.

Proposition 4.15. *Assume that* $\mathrm{char}(\mathbb{F}_q) \neq 2$. *Let* $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_{2k-1})$ *and* $\mathcal{F}' = (\mathcal{F}'_1, \ldots, \mathcal{F}'_{2k-1})$ *be two full flags on* $\mathbb{F}_q^{2k}$ *such that* $\mathcal{F}_k, \mathcal{F}'_k \in \mathcal{S}$ *lie in different orbits of the action of* $\mathbf{H}$ *on* $\mathcal{S}$. *Then the full flag code*

$$\mathcal{C} = \mathrm{Orb}_{\mathbf{H}}(\mathcal{F}) \mathbin{\dot{\cup}} \mathrm{Orb}_{\mathbf{H}}(\mathcal{F}')$$

is an optimum distance flag code with the largest possible size, that is, $q^k + 1$.

Proof. Notice that, by Lemma 4.10, we can use Theorem 3.8 to conclude that $\mathcal{C}$ is an optimum distance full flag code of size $|\mathrm{Orb}_{\mathbf{H}}(\mathcal{F}_k)| + |\mathrm{Orb}_{\mathbf{H}}(\mathcal{F}'_k)|$, which is $q^k + 1$ by Theorem 4.11. ∎

As a consequence, we can directly translate the orbital description of the spread $\mathcal{S}$ given in Proposition 4.12 to obtain a specific construction of an optimum distance full flag code with the largest possible size on fields of odd characteristic:

Corollary 4.16. *Assume that* $\mathrm{char}(\mathbb{F}_q) \neq 2$. *Let* $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_{2k-1})$ *and* $\mathcal{F}' = (\mathcal{F}'_1, \ldots, \mathcal{F}'_{2k-1})$ *be two full flags on* $\mathbb{F}_q^{2k}$ *such that* $\mathcal{F}_k = \mathcal{U}_k$ *and* $\mathcal{F}'_k = \mathcal{V}_k$. *Then the full flag code*

$$\mathcal{C} = \mathrm{Orb}_{\mathbf{H}}(\mathcal{F}) \mathbin{\dot{\cup}} \mathrm{Orb}_{\mathbf{H}}(\mathcal{F}')$$

is an optimum distance flag code with the largest possible size, that is, $q^k + 1$.

Remark 4.17. The main goal of this paper was to provide an orbital construction of optimum distance full flag codes on $\mathbb{F}_q^{2k}$ having the spread $\mathcal{S}$ as its k-projected code by using some subgroup of the group $\mathbf{G}$. By Theorem 3.2, these flag codes have both maximum distance and cardinality. For the case, $q = 3$ and $k = 2$, we have checked by using GAP that no subgroup $\mathbf{N}$ of $\mathbf{G}$ such that $\mathcal{S} = \mathrm{Orb}_{\mathbf{N}}(\mathcal{U}_2)$ is able to extend its action to the standard full flag on $\mathbb{F}_3^4$ providing an optimum distance flag code as a single orbit. Hence, for odd characteristic, it is not possible to give a general construction of orbit full flag code, under the action of a subgroup of $\mathbf{G}$, with the maximum distance and the best size for that distance. Consequently, the action of our subgroup $\mathbf{H}$ allows us to achieve our objective with the lowest possible number of orbits.

5   Conclusions

In this paper we have adressed the construction of optimum distance full flag codes having an orbital structure. To do this, we have stated first some useful properties of orbit flag codes under the action of an arbitrary subgroup of $GL(n, q)$. For the particular case $n = 2k$, we have given sufficient conditions to obtain optimum distance orbit full flag codes on $\mathbb{F}_q^{2k}$, starting from orbit codes of dimension k and maximum distance.

Moreover, we have shown how, under these conditions, these starting orbit codes completely drive our construction in the following sense: their property of being of maximum distance, as well as their cardinality and orbital structure, are perfectly translated to the flag codes level. As a consequence, the cardinality of optimum distance full flag codes constructed in this way can be increased by considering a starting subspace code of dimension k consisting of more than one orbit. Besides, we have presented a specific orbital construction of optimum distance full flag codes on $\mathbb{F}_q^{2k}$ with the best size using at most two orbits.

References

[1] J. L. Alperin and R. B. Bell, *Groups and Representations.* Graduate Texts in Mathematics, Vol. 162. Springer, New York, 1995.

[2] C. Alonso-González, M. A. Navarro-Pérez and X. Soler-Escrivà, *Flag Codes from Planar Spreads in Network Coding*, To appear in Finite Fields and Their Applications, https://doi.org/10.1016/j.ffa.2020.101745.

[3] C. Alonso-González, M. A. Navarro-Pérez and X. Soler-Escrivà, *Optimum Distance Flag Codes from Spreads via Perfect Matchings in Gaphs*, https://arxiv.org/abs/2005.09370v2 (preprint).

[4] M. Greferath, M. O. Pavčević, N. Silberstein and M. A. Vázquez-Castro, *Network Coding and Subspace Designs*, Springer, 2018.

[5] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields.* Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second edition, 1998.

[6] T. Ho, R. Kötter, M. Médard, D. Karger and M. Effros, *The Benefits of Coding over Routing in a Randomized Setting*, in: IEEE International Symposium on Information Theory, Proceedings (ISIT), Yokohama, Japan, 2003, p. 442.

[7] M. D. Hestenes, *Singer Groups*, Canadian Journal of Mathematics, Vol. XXII, 3 (1970), pp. 492-513.

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

[9] R. Kötter and F. Kschischang, *Coding for Errors and Erasures in Random Network Coding*, in: IEEE Transactions on Information Theory, Vol. 54 (2008) 3579-3591.

[10] D. Liebhold, G. Nebe and A. Vazquez-Castro, *Network Coding with Flags*, Designs, Codes and Cryptography, Vol. 86 (2) (2018) 269-284.

[11] F. Manganiello, E. Gorla and J. Rosenthal, *Spread Codes and Spread Decoding in Network Coding*, in: IEEE International Symposium on Information Theory, Proceedings (ISIT), Toronto, Canada, 2008, pp. 851-855.

[12] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*. Cambridge University Press, Cambridge, London, 1994. Revised edition.

[13] R. W. Nóbrega and B. F. Uchôa-Filho, *Multishot Codes for Network Coding: Bounds and a Multilevel Construction*, in: 2009 IEEE International Symposium on Information Theory, Proceedings (ISIT), Seoul, South Korea, 2009, pp. 428-432.

[14] B. Segre, *Teoria di Galois, Fibrazioni Proiettive e Geometrie non Desarguesiane*, Annali di Matematica Pura ed Applicata, Vol. 64 (1964), 1-76.

[15] A.-L. Trautmann, F. Manganiello and J. Rosenthal, *Orbit Codes - A New Concept in the Area of Network Coding* in: 2010 IEEE Information Theory Workshop, ITW 2010 - Proceedings, Dublin, Ireland, 2010, pp. 1-4.

[16] A.-L. Trautmann, F. Manganiello, M. Braun and J. Rosenthal, *Cyclic Orbit Codes* in: IEEE Trans. Inform. Theory, Vol. 59 (11) (2013) 7386-7404.

[17] A.-L. Trautmann and J. Rosenthal, *Constructions of Constant Dimension Codes*, in: M. Greferath et al. (Eds.), Network Coding and Subspace Designs, E-Springer International Publishing AG, 2018, pp. 25-42.