This is a previous version of the article published in Designs, Codes and Cryptography. 2021. https://doi.org/10.1007/s10623-021-00920-5

Cyclic Orbit Flag Codes

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

February 2, 2021

Abstract

In network coding, a flag code is a set of sequences of nested subspaces of $\mathbb{F}_q^n$, being $\mathbb{F}_q$ the finite field with q elements. Flag codes defined as orbits of a cyclic subgroup of the general linear group acting on flags of $\mathbb{F}_q^n$ are called *cyclic orbit flag codes*. Inspired by the ideas in [10], we determine the cardinality of a cyclic orbit flag code and provide bounds for its distance with the help of the largest subfield over which all the subspaces of a flag are vector spaces (the *best friend* of the flag). Special attention is paid to two specific families of cyclic orbit flag codes attaining the extreme possible values of the distance: *Galois cyclic orbit flag codes* and *optimum distance cyclic orbit flag codes*. We study in detail both classes of codes and analyze the parameters of the respective subcodes that still have a cyclic orbital structure.

Keywords: Network coding, flag codes, cyclic orbit flag codes.

1 Introduction

Network coding is a strong tool for effective data transmission in a network modelled as a directed acyclic multigraph with several sources and sinks. In [1], it was proved that the information flow of the network may be improved if the intermediate nodes are able to perform random linear combinations of the received inputs instead of simply routing them. Random network coding was introduced in [12], and an algebraic approach to it was presented in [13]. In that work, the authors propose transmitting information by using vector subspaces of $\mathbb{F}_q^n$ and define *subspace codes* as a class of codes well suited for error correction. In case all the codewords in a subspace code have the same dimension, it is said to be a *constant dimension code*. The seminal paper [13] has lately led to many lines of research on subspace codes addressed either to the construction of subspace codes with the best size fixed the minimum distance or to find algebraic constructions of subspace codes with good parameters (see [25] and references therein).

In [24], Trautmann *et al.* introduced the concept of *orbit codes* as subspace codes obtained from the action of subgroups of the general linear group $\mathrm{GL}(n, q)$

[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.

on the set of subspaces of $\mathbb{F}_q^n$. When the acting group is cyclic, we speak about *cyclic orbit codes*. This family of codes has awaken a lot of interest due to the simplicity of their algebraic structure and to the existence of efficient encoding/decoding algorithms. We refer the reader to [5, 6, 8, 9, 10, 19, 21, 23, 24, 26] for some of the more recent papers.

Taking into account that $\mathbb{F}_q^n$ and the field extension $\mathbb{F}_{q^n}$ are isomorphic as $\mathbb{F}_q$-vector spaces, in [10], the authors consider subspace codes as collections of $\mathbb{F}_q$-vector subspaces of $\mathbb{F}_{q^n}$ and study orbit codes arising from the natural action of the multiplicative subgroups of $\mathbb{F}_{q^n}^*$ (cyclic groups as well) on $\mathbb{F}_q$-vector spaces. Fixed a generating subspace $\mathcal{U}$ of the cyclic orbit code $\mathrm{Orb}(\mathcal{U})$, their main tool is the *best friend* of $\mathcal{U}$, that is, the largest subfield of $\mathbb{F}_{q^n}$ over which $\mathcal{U}$ is a vector space. This concept is closely related with the stabilizer of $\mathcal{U}$, specially when the acting group is $\mathbb{F}_{q^n}^*$. The best friend allows the authors to give relevant information about the cardinality, distance and other features of cyclic orbit codes.

Flag codes were introduced in [15] as a generalization of constant dimension codes in network coding. In a flag code of constant type, codewords are given by sequences of nested subspaces (flags) of prescribed dimensions. In that paper, the multiplicative action of $\mathrm{GL}(n,q)$ is naturally extended from subspaces to flags and several constructions of *orbit flag codes* are provided. In [3, 4], flag codes attaining the maximum possible distance (*optimum distance flag codes*) are characterized and obtained without regard to their possible orbital structure whereas in [2] an orbital construction of them is proposed.

In this work we follow the approach of Gluesing-Luerssen *et al.* in [10]. Inspired by their ideas, we consider flags on $\mathbb{F}_{q^n}$ given by nested $\mathbb{F}_q$-subspaces of the field $\mathbb{F}_{q^n}$ and focus on *cyclic orbit flag codes* constructed as orbits of subgroups of $\mathbb{F}_{q^n}^*$. We generalize the concept of the best friend of a subspace to the flags framework by defining the *best friend* of a flag as the largest subfield of $\mathbb{F}_{q^m}$ over which every subspace in a flag is a vector space. As it occurs in the constant dimension codes scenario, the knowledge of the best friend of a generating flag allows us to easily determine the size of the cyclic orbit code as well as to give estimates for its distance. In particular, we pay special attention to two specific families of cyclic orbit flag codes attaining the extreme possible values of the distance. We introduce first the concept of *Galois cyclic flag codes* as the cyclic orbit codes generated by sequences of nested subfields of $\mathbb{F}_{q^n}$. Despite the fact that these codes have the minimum possible distance (fixed the best friend), they present a nice gear of nested spreads compatible with the action of $\mathbb{F}_{q^n}^*$. Moreover, if one consider the subcodes of Galois cyclic flag codes that keep cyclic orbital structure, we can improve their distance in a controlled manner and reach even the maximum possible one. By the way, we also determine which dimensions in the type vector of a general generating flag are compatible with attaining the maximum distance, having a fixed best friend and being orbits under the action of subgroups of $\mathbb{F}_{q^n}^*$. In other words, we study *optimum distance cyclic orbit flag codes* and their orbital cyclic subcodes.

The text is organized as follows. In Section 2, the reader can find the general background on subspace codes. Particular care is devoted to the study of cyclic orbit (subspace) codes developed in [10]. In Section 3, cyclic orbit flag codes

are introduced. We also generalize the notions of stabilizer subfield and best friend to the flag codes setting by exhibiting the relationship between these two concepts and the corresponding ones for subspace codes. In Section 4, the cardinality and bounds for the distance of a cyclic orbit flag code with a given best friend are provided. We finish by introducing Galois cyclic flag codes and optimum distance cyclic flag codes with a prescribed best friend. We study their parameters and properties as well as the ones of respective subcodes coming also from the action of subgroups of $\mathbb{F}_{q^n}^*$.

2 Preliminaries

Fix $\mathbb{F}_q$ the finite field of q elements where q is a primer power. For any natural number $n \geqslant 1$, $\mathbb{F}_q^n$ represents the n-dimensional vector space over $\mathbb{F}_q$. Given $1 \leqslant k < n$, the *Grassmannian* $\mathcal{G}_q(k,n)$ is the set of k-dimensional subspaces of $\mathbb{F}_q^n$ and we write $\mathcal{P}_q(n)$ to denote the *projective geometry* of $\mathbb{F}_q^n$, that is, the set of all the subspaces of $\mathbb{F}_q^n$. The set $\mathcal{P}_q(n)$ can be considered as a metric space with the *subspace distance* (see [13]) defined as

$$d_S(\mathcal{U},\mathcal{V}) = \dim(\mathcal{U}+\mathcal{V}) - \dim(\mathcal{U}\cap\mathcal{V}). \tag{1}$$

A *subspace code* $\mathcal{C}$ of length n is a nonempty subset of $\mathcal{P}_q(n)$ and its *minimum subspace distance* is defined as

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

A subspace code in which every codeword has the same dimension, say k, is called *constant dimension code* of dimension k and length n (see [25] and references therein). The subspace distance between two subspaces $\mathcal{U}$ and $\mathcal{V}$ of dimension k is given by

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

Consequently, the minimum distance of a constant dimension code of dimension k is upper bounded by

$$d_S(\mathcal{C}) \leqslant \begin{cases} 2k & \text{if} \quad 2k \leqslant n, \\ 2(n-k) & \text{if} \quad 2k > n. \end{cases} \tag{2}$$

These bounds for the distance are attained by constant dimension codes in which every pair of codewords intersects with the minimum possible dimension. For dimensions k up to $\lfloor \frac{n}{2} \rfloor$, constant dimension codes attaining the previous bound are known as *partial spread codes* and their cardinality is, at most, $\lfloor \frac{q^n-1}{q^k-1} \rfloor$. In contrast, a constant dimension code that attains the bound in (2) and has dimension $k > \lfloor \frac{n}{2} \rfloor$, cannot contain more than $\lfloor \frac{q^n-1}{q^{n-k}-1} \rfloor$ elements.

A *spread code* in $\mathcal{G}_q(k,n)$, or just a *k-spread*, is a partition of $\mathbb{F}_q^n$ into k-dimensional subspaces. In other words, a spread is a partial spread that covers $\mathbb{F}_q^n$. Spreads are classical objects coming from Finite Geometry and it is well known that k-spreads exist if, and only if, k divides n (see [22]). As a

consequence, the size of every k-spread is $\frac{q^n-1}{q^k-1}$. For further information related to spread codes in the network coding framework, we refer the reader to [11, 16, 17, 25].

There are constant dimension codes that can be obtained as orbits of the action of subgroups of the general linear group $\mathrm{GL}(n,q)$ on the Grassmannian of the corresponding dimension. In this case, we speak about *orbit codes*, which were introduced for the first time in [24]. Given a k-dimensional subspace $\mathcal{U}$ of $\mathbb{F}_q^n$ and a subgroup G of $\mathrm{GL}(n,q)$, the orbit of $\mathcal{U}$ under the action of G is the constant dimension code given by $\mathrm{Orb}_G(\mathcal{U}) = \{\mathcal{U}\cdot A \mid A \in G\}$, where $\mathcal{U}\cdot A = \mathrm{rowsp}(UA)$ for any full-rank generator matrix U of $\mathcal{U}$. The *stabilizer* of $\mathcal{U}$ under the action of G is the subgroup $\mathrm{Stab}_G(\mathcal{U}) = \{A \in G \mid \mathcal{U}\cdot A = \mathcal{U}\}$. Clearly,

$$|\mathrm{Orb}_G(\mathcal{U})| = \frac{|G|}{|\mathrm{Stab}_G(\mathcal{U})|}$$

and its minimum distance is given by

$$d_S(\mathrm{Orb}_G(\mathcal{U})) = \min\{d_s(\mathcal{U},\mathcal{U}\cdot A) \mid A \in G \setminus \mathrm{Stab}_G(\mathcal{U})\}.$$

If the group G is cyclic, the code $\mathrm{Orb}_G(\mathcal{U})$ is called *cyclic orbit code*. This special family of orbit codes was widely studied in [10, 18, 20, 23]. In particular, using the fact that $\mathbb{F}_q^n$ and $\mathbb{F}_{q^n}$ are isomorphic as $\mathbb{F}_q$-vector spaces, Trautmann *et al.* provide in [23] the following construction of a k-spread as a cyclic orbit code. Take a divisor k of n and let α denote a primitive element of $\mathbb{F}_{q^n}$, i.e, a generator of the multiplicative group $\mathbb{F}_{q^n}^*$. If we put $c = \frac{q^n-1}{q^k-1}$, then it is clear that $\langle\alpha^c\rangle$ is the unique subgroup of order q^k-1 of $\mathbb{F}_{q^n}^*$ and that $\langle\alpha^c\rangle\cup\{0\} = \mathbb{F}_{q^k}$. As proved in [23, Th. 31], the stabilizer of $\mathbb{F}_{q^k}$ under the action of the cyclic group $\langle\alpha\rangle$ is precisely the subgroup $\langle\alpha^c\rangle$ and the orbit

$$\mathcal{S} = \mathrm{Orb}_{\langle\alpha\rangle}(\mathbb{F}_{q^k}) = \{\mathbb{F}_{q^k}\alpha^i \mid i = 0,\ldots,c-1\} \tag{3}$$

is a k-spread of $\mathbb{F}_{q^n}$.

In [10], Gluesing-Luerssen *et al.* generalize the construction in (3) for any $\beta \in \mathbb{F}_{q^n}^*$ by introducing the concept of *β-cyclic orbit code generated by a subspace* $\mathcal{U}$ of $\mathbb{F}_{q^n}$ and study these codes by specifying the largest subfield over which the subspace $\mathcal{U}$ is a vector space. Let us recall some definitions and results from that work that we will use along this paper.

Consider any nonzero element β in the finite field $\mathbb{F}_{q^n}$ and the natural multiplicative action of the group $\langle\beta\rangle$ on $\mathbb{F}_q$-vector subspaces of $\mathbb{F}_{q^n}$. Orbits of this action are called *β-cyclic orbit codes*. To be precise, if $1 \leqslant k < n$ and $\mathcal{U} \subset \mathbb{F}_{q^n}$ is a k-dimensional subspace over $\mathbb{F}_q$, the *β-cyclic orbit code generated by $\mathcal{U}$* is the constant dimension code in the Grassmannian $\mathcal{G}_q(k,n)$ given by

$$\mathrm{Orb}_\beta(\mathcal{U}) = \{\mathcal{U}\beta^i \mid 0 \leqslant i \leqslant |\beta| - 1\},$$

where $|\beta|$ denotes the *multiplicative order* of β (for further information on these orbits, see [7]). The *stabilizer* of the subspace $\mathcal{U}$ under the action of $\langle\beta\rangle$ is the cyclic subgroup defined as $\mathrm{Stab}_\beta(\mathcal{U}) = \{\beta^i \in \langle\beta\rangle \mid \mathcal{U}\beta^i = \mathcal{U}\}$ and the *stabilizer subfield* $\mathrm{Stab}_\beta^+(\mathcal{U})$ of $\mathcal{U}$ (with respect to β) is the smallest subfield of $\mathbb{F}_{q^n}$ containing both $\mathbb{F}_q$ and $\mathrm{Stab}_\beta(\mathcal{U})$.

Remark 2.1. When the acting group is $\mathbb{F}_{q^n}^*$, following the notation in [10], we simply write by $\mathrm{Orb}(\mathcal{U})$ and call it the *cyclic orbit code generated by* $\mathcal{U}$. In this situation, we also remove the subscript β and write $\mathrm{Stab}(\mathcal{U})$ and $\mathrm{Stab}^+(\mathcal{U})$ to the denote the stabilizer and the stabilizer subfield of $\mathcal{U}$ respectively.

Concerning the cardinality of a β-cyclic orbit code, there exists a nice relationship between $|\mathrm{Orb}_\beta(\mathcal{U})|$ and the dimension of the generating subspace $\mathcal{U}$. More precisely, in [10, Prop. 3.7], the authors showed that, if $\mathcal{U}$ is a k-dimensional subspace of $\mathbb{F}_{q^n}$, then

$$|\beta^{q^k-1}| = \frac{|\beta|}{\gcd(|\beta|, q^k-1)} \text{ divides } |\mathrm{Orb}_\beta(\mathcal{U})|. \tag{4}$$

Moreover, the equality $|\mathrm{Orb}_\beta(\mathcal{U})| = \frac{|\beta|}{q^k-1}$ holds if, and only if, $\mathcal{U}$ is a vector space over $\mathbb{F}_{q^k}$. More precisely, if $1 \in \mathcal{U}$, for every divisor k of n, the code $\mathrm{Orb}(\mathcal{U})$ is a k-spread if, and only if, $\mathcal{U} = \mathbb{F}_{q^k}$. Therefore, the spread defined in (3) arises as the cyclic orbit code $\mathrm{Orb}(\mathbb{F}_{q^k})$ in this context.

A subfield $\mathbb{F}_{q^m}$ of $\mathbb{F}_{q^n}$ is said to be a *friend* of a subspace $\mathcal{U} \subset \mathbb{F}_{q^n}$ if $\mathcal{U}$ is an $\mathbb{F}_{q^m}$-vector space. In that case, if t is the dimension of $\mathcal{U}$ as $\mathbb{F}_{q^m}$-vector space, we have that $\dim_{\mathbb{F}_q}(\mathcal{U}) = mt$. Moreover, if $\{u_1, \ldots, u_t\} \subseteq \mathcal{U}$ is a basis of $\mathcal{U}$ over $\mathbb{F}_{q^m}$, then it holds

$$\mathcal{U} = \mathbb{F}_{q^m} u_1 \oplus \cdots \oplus \mathbb{F}_{q^m} u_t.$$

Note that every subspace $\mathcal{U}$ is a vector space over $\mathrm{Stab}_\beta^+(\mathcal{U})$. In other words, the stabilizer subfield is a friend of $\mathcal{U}$. The largest friend of $\mathcal{U}$ is called its *best friend* (see [10]). The concepts of stabilizer subfield and best friend of a subspace turn to be same in the following situation in which, in addition, the knowledge of the best friend of $\mathcal{U}$ provides straightforwardly the cardinality of the cyclic orbit code as well as a lower bound for its distance.

Proposition 2.2. *([10, Prop. 3.3, 3.12, 3.13 and 4.1]) If $\mathcal{U}$ is a subspace of $\mathbb{F}_{q^n}$, then its stabilizer subfield satisfies*

$$\mathrm{Stab}^+(\mathcal{U}) = \mathrm{Stab}(\mathcal{U}) \cup \{0\}$$

and it contains every friend of $\mathcal{U}$. As a consequence, the field $\mathrm{Stab}^+(\mathcal{U})$ is the best friend of the subspace $\mathcal{U}$. In particular, if $\mathrm{Stab}^+(\mathcal{U}) = \mathbb{F}_{q^m}$, then

$$|\mathrm{Orb}(\mathcal{U})| = \frac{q^n-1}{q^m-1}.$$

Moreover, the value $2m$ divides the distance between every pair of subspaces in $\mathrm{Orb}(\mathcal{U})$ and, hence, we have that $d_S(\mathrm{Orb}(\mathcal{U})) \geqslant 2m$. Besides, if $1 \in \mathcal{U}$, we have the inclusion $\mathrm{Stab}^+(\mathcal{U}) \subseteq \mathcal{U}$.

3 Cyclic orbit flag codes

In classical linear algebra, a flag variety on the field extension $\mathbb{F}_{q^n}$ is a homogeneous space that generalizes the Grassmann variety and whose points are flags.

The use of flags in network coding was proposed for the first time in [15]. We start this section by recalling some basic background on flag codes. Next, we will focus on the family of flag codes that are orbits under the action of a cyclic group on the flag variety. Finally, we introduce the concepts of stabilizer subfield and best friend of a flag, following the ideas in [10], in order to deepen the structure and properties of the family of cyclic orbit flag codes.

3.1 Flag codes

Definition 3.1. A *flag* $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ on $\mathbb{F}_{q^n}$ is a sequence of nested $\mathbb{F}_q$-vector subspaces of $\mathbb{F}_{q^n}$, i.e., such that

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

The subspace $\mathcal{F}_i$ is said to be the *i-th subspace* of $\mathcal{F}$. The type of $\mathcal{F}$ is the vector $(\dim(\mathcal{F}_1), \ldots, \dim(\mathcal{F}_r))$. In case the type vector is $(1, 2, \ldots, n-1)$, we say that $\mathcal{F}$ is a *full flag*.

The *flag variety* $\mathcal{F}_q((t_1, \ldots, t_r), n)$ is the set of flags of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_{q^n}$. This variety can naturally be equipped with a metric by extending the subspace distance defined in (1). Given two flags $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ and $\mathcal{F}' = (\mathcal{F}'_1, \ldots, \mathcal{F}'_r)$ in $\mathcal{F}_q((t_1, \ldots, t_r), n)$, their *flag distance* is

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

Definition 3.2. A *flag code* of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_{q^n}$ is a nonempty subset $\mathcal{C} \subseteq \mathcal{F}_q((t_1, \ldots, t_r), n)$. Its *minimum distance* is given by

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

and, in case $|\mathcal{C}| = 1$, we put $d_f(\mathcal{C}) = 0$.

For each dimension t_i in the type vector of a flag code $\mathcal{C}$, we can associate to it the constant dimension code in the Grassmannian $\mathcal{G}_q(t_i, n)$ consisting of the set of the i-th subspaces of flags in $\mathcal{C}$. This set is called the *i-projected code* of $\mathcal{C}$ and we denote it by $\mathcal{C}_i$. It is clear that $|\mathcal{C}_i| \leqslant |\mathcal{C}|$ for every $i = 1, \ldots, r$. In case $|\mathcal{C}_1| = \cdots = |\mathcal{C}_r| = |\mathcal{C}|$, we say that $\mathcal{C}$ is *disjoint*. As shown in [3], the property of being disjoint is necessary in order to have flag codes that achieve the maximum possible flag distance. For type $(t_1, \ldots, t_r)$, that maximum distance is

$$2\left(\sum_{t_i \leqslant \lfloor \frac{n}{2} \rfloor} t_i + \sum_{t_i > \lfloor \frac{t}{2} \rfloor} (n - t_i)\right) \tag{5}$$

and flag codes attaining it are called *optimum distance flag codes*. In [3, 4] the reader can find constructions of this class of codes as well as the following characterization of them.

Theorem 3.3. *[3, Th. 3.11] A flag code is an optimum distance flag code if, and only if, it is disjoint and every projected code attains the maximum possible distance for its dimension.*

As in the case of subspace codes, one can build families of flag codes through the action of a group. This approach already appears in [15], where the authors generalize the action of $\mathrm{GL}(n,q)$ on subspaces of $\mathbb{F}_q^n$ to flags and provide several constructions of flag codes as orbits of the action of specific upper unitriangular matrix groups on the full flag variety.

In the next section, following the ideas developed in [10] for subspace codes, we introduce the concept of *cyclic orbit flag code* as the orbit of the multiplicative action of subgroups of $\mathbb{F}_{q^n}^*$ on flags on $\mathbb{F}_{q^n}$.

3.2 Cyclic orbit flag codes

Given a nonzero element β in the field $\mathbb{F}_{q^n}$, we can extend the natural action of the cyclic group $\langle\beta\rangle$ on $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^n}$ to flags on $\mathbb{F}_{q^n}$ as follows. If $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ is a flag of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_{q^n}$, we define the flag $\mathcal{F}\beta$ as

$$\mathcal{F}\beta = (\mathcal{F}_1\beta, \ldots, \mathcal{F}_r\beta).$$

The set

$$\mathrm{Orb}_\beta(\mathcal{F}) = \{\mathcal{F}\beta^j \mid 0 \leqslant j \leqslant |\beta| - 1\}. \tag{6}$$

is called the *β-cyclic orbit flag code* generated by $\mathcal{F}$. The *stabilizer* of the flag $\mathcal{F}$ (w.r.t. β) is the subgroup of $\langle\beta\rangle$ given by

$$\mathrm{Stab}_\beta(\mathcal{F}) = \{\beta^j \in \langle\beta\rangle \mid \mathcal{F}\beta^j = \mathcal{F}\}.$$

When the acting group is $\mathbb{F}_{q^n}^*$, we do not specify it and simply write $\mathrm{Orb}(\mathcal{F})$ to denote the *cyclic orbit flag code generated by $\mathcal{F}$*. We also drop the subscript in $\mathrm{Stab}(\mathcal{F})$. Observe that every $\mathrm{Orb}_\beta(\mathcal{F})$ is a subcode of $\mathrm{Orb}(\mathcal{F})$. Furthermore, it holds

$$\mathrm{Stab}_\beta(\mathcal{F}) = \langle\beta\rangle \cap \mathrm{Stab}(\mathcal{F}).$$

As in the subspace codes framework, the orbital structure simplifies the computation of the code parameters: the cardinality of the flag code in (6) is given by

$$|\mathrm{Orb}_\beta(\mathcal{F})| = \frac{|\beta|}{|\mathrm{Stab}_\beta(\mathcal{F})|} = \frac{|\beta|}{|\langle\beta\rangle \cap \mathrm{Stab}(\mathcal{F})|} \tag{7}$$

and its minimum distance can be computed as

$$d_f(\mathrm{Orb}_\beta(\mathcal{F})) = \min\{d_f(\mathcal{F}, \mathcal{F}\beta^j) \mid \beta^j \notin \mathrm{Stab}_\beta(\mathcal{F})\}.$$

Remark 3.4. Notice that the projected codes associated to $\mathrm{Orb}_\beta(\mathcal{F})$ are β-cyclic orbit (subspace) codes as well. More precisely, for every $1 \leqslant i \leqslant r$, we have

$$(\mathrm{Orb}_\beta(\mathcal{F}))_i = \mathrm{Orb}_\beta(\mathcal{F}_i).$$

Moreover, as for any other group action, it holds a clear relationship between the stabilizer of the flag $\mathcal{F}$ and the ones of its subspaces:

$$\mathrm{Stab}_\beta(\mathcal{F}) = \bigcap_{i=1}^{r} \mathrm{Stab}_\beta(\mathcal{F}_i). \tag{8}$$

This equality leads to a direct link between the cardinality of a β-cyclic orbit flag code, the ones of its projected codes, and the dimensions on the generating flag type vector.

Proposition 3.5. *Let $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ be a flag of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_{q^n}$ and $\beta \in \mathbb{F}_{q^n}^*$. Then $|\mathrm{Orb}_\beta(\mathcal{F}_i)|$ divides $|\mathrm{Orb}_\beta(\mathcal{F})|$, for $1 \leqslant i \leqslant r$. In particular,*

$$\mathrm{lcm}\left\{|\beta^{q^{t_i}-1}| \mid 1 \leqslant i \leqslant r\right\} \text{ divides } |\mathrm{Orb}_\beta(\mathcal{F})|.$$

Proof. Recall that $|\mathrm{Orb}_\beta(\mathcal{F})| = \frac{|\beta|}{|\mathrm{Stab}_\beta(\mathcal{F})|}$ and $|\mathrm{Orb}_\beta(\mathcal{F}_i)| = \frac{|\beta|}{|\mathrm{Stab}_\beta(\mathcal{F}_i)|}$, for every $1 \leqslant i \leqslant r$. Moreover, by means of (8), we have that $|\mathrm{Stab}_\beta(\mathcal{F})|$ divides $|\mathrm{Stab}_\beta(\mathcal{F}_i)|$ for every value of i. Hence, the cardinality of $\mathrm{Orb}_\beta(\mathcal{F}_i)$ must divide $|\mathrm{Orb}_\beta(\mathcal{F})|$, for $1 \leqslant i \leqslant r$. The last part of the statement follows directly from this fact along with (4). ∎

3.3 Stabilizer subfield and best friend of a flag code

The following definition extends the concept of stabilizer subfield of a subspace defined in [10] to the flag codes setting.

Definition 3.6. Let $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ be a flag of type $(t_1, \ldots, t_r)$ on the field $\mathbb{F}_{q^n}$ and $\beta \in \mathbb{F}_{q^n}^*$. We define the *stabilizer subfield* of the flag $\mathcal{F}$ (w.r.t. β) as the smallest subfield $\mathrm{Stab}_\beta^+(\mathcal{F})$ of $\mathbb{F}_{q^n}$ containing both $\mathbb{F}_q$ and $\mathrm{Stab}_\beta(\mathcal{F})$.

As before, if β is a primitive element of $\mathbb{F}_{q^n}$, we just write $\mathrm{Stab}^+(\mathcal{F})$. In this case, the stabilizer subfield of a flag admits the following nice description:

Proposition 3.7. *Let $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ be a flag on $\mathbb{F}_{q^n}$. It holds*

$$\mathrm{Stab}^+(\mathcal{F}) = \mathrm{Stab}(\mathcal{F}) \cup \{0\} = \bigcap_{i=1}^{r} \mathrm{Stab}^+(\mathcal{F}_i)$$

and every i-th subspace $\mathcal{F}_i$ of the flag $\mathcal{F}$ is a vector space over $\mathrm{Stab}^+(\mathcal{F})$. Moreover, if $1 \in \mathcal{F}_1$, the stabilizer subfield $\mathrm{Stab}^+(\mathcal{F})$ is contained in every subspace of $\mathcal{F}$.

Proof. By application of Proposition 2.2, one has that $\mathrm{Stab}^+(\mathcal{F}_i) = \mathrm{Stab}(\mathcal{F}_i) \cup \{0\}$ for every $1 \leqslant i \leqslant r$. Now, by means of (8), we conclude that

$$\begin{array}{rcl} \mathrm{Stab}(\mathcal{F}) \cup \{0\} & = & (\bigcap_{i=1}^{r} \mathrm{Stab}(\mathcal{F}_i)) \cup \{0\} \\ & = & (\bigcap_{i=1}^{r} \mathrm{Stab}(\mathcal{F}_i) \cup \{0\}) \quad = \quad \bigcap_{i=1}^{r} \mathrm{Stab}^+(\mathcal{F}_i). \end{array} \tag{9}$$

This proves that $\mathrm{Stab}(\mathcal{F}) \cup \{0\}$ is a field and then it is the stabilizer subfield of the flag $\mathcal{F}$. Moreover, it is a subfield of every $\mathrm{Stab}^+(\mathcal{F}_i)$. Hence, it is clear that the subspace $\mathcal{F}_i$ is a vector space over $\mathrm{Stab}^+(\mathcal{F})$. Besides, if $1 \in \mathcal{F}_1$, by using Proposition 2.2, we obtain

$$\mathrm{Stab}^+(\mathcal{F}) \subseteq \mathrm{Stab}^+(\mathcal{F}_1) \subseteq \mathcal{F}_1 \subset \mathcal{F}_2 \subset \cdots \subset \mathcal{F}_r.$$

∎

Notice that the condition $1 \in \mathcal{F}_1$ in Proposition 3.7 is by no means restrictive when the acting group is $\mathbb{F}_{q^n}^*$. In fact, we can always find a generating flag fulfilling this property. It suffices to see that, given an arbitrary flag $\mathcal{F}$, for every nonzero element $\beta \in \mathcal{F}_1$, the flag $\mathcal{F}\beta^{-1}$ clearly satisfies the required condition. Moreover, since β is an element in the field $\mathbb{F}_{q^n}^*$, both flags $\mathcal{F}$ and $\mathcal{F}\beta^{-1}$ generate the same cyclic orbit flag code $\mathrm{Orb}(\mathcal{F}) = \mathrm{Orb}(\mathcal{F}\beta^{-1})$.

Remark 3.8. Clearly, if $\beta \in \mathbb{F}_{q^n}^*$, it holds $\mathrm{Stab}_\beta(\mathcal{F}) \subseteq \mathrm{Stab}(\mathcal{F})$ and, hence, $\mathrm{Stab}_\beta^+(\mathcal{F}) \subseteq \mathrm{Stab}^+(\mathcal{F})$. As a consequence, every $\mathcal{F}_i$ is a vector space over the field $\mathrm{Stab}_\beta^+(\mathcal{F})$ as well as over all its subfields. Moreover, if $1 \in \mathcal{F}_1$, then $\mathrm{Stab}_\beta^+(\mathcal{F}) \subseteq \mathcal{F}_i$ for $1 \leqslant i \leqslant r$.

As it occurs for constant dimension codes, the inclusion $\mathrm{Stab}_\beta^+(\mathcal{F}) \subseteq \mathrm{Stab}^+(\mathcal{F})$ may be strict. Let us provide an example from a length-two flag inspired by [10, Example 3.6].

Example 3.9. Consider the flag $\mathcal{F} = (\mathbb{F}_{3^2}, \mathbb{F}_{3^4})$ on the field $\mathbb{F}_{3^8}$ and let α be a primitive element of $\mathbb{F}_{3^8}$. Observe that $\mathrm{Stab}^+(\mathbb{F}_{3^2}) = \mathbb{F}_{3^2}$ and $\mathrm{Stab}^+(\mathbb{F}_{3^4}) = \mathbb{F}_{3^4}$. Hence, by Proposition 3.7, it follows that $\mathrm{Stab}^+(\mathcal{F}) = \mathbb{F}_{3^2} \cap \mathbb{F}_{3^4} = \mathbb{F}_{3^2}$. Let us now choose $\beta = \alpha^{1312}$, which have multiplicative order equal to 5. Observe that $\mathrm{Stab}_\beta(\mathcal{F}) \subseteq \langle\beta\rangle$ and also $\mathrm{Stab}_\beta(\mathcal{F}) \subseteq \mathrm{Stab}_\beta^+(\mathcal{F})^* \subseteq \mathrm{Stab}^+(\mathcal{F})^* = \mathbb{F}_{3^2}^*$. As the orders of $\langle\beta\rangle$ and $\mathbb{F}_{3^2}^*$ are coprime, we have that $\mathrm{Stab}_\beta(\mathcal{F}) = \{1\}$. This implies that $\mathrm{Stab}_\beta^+(\mathcal{F}) = \mathbb{F}_3$.

There are remarkable connections between the cardinality of a β-cyclic orbit flag code and the generating flag when one has a divisor of n among the dimensions of the type vector.

Proposition 3.10. *Let $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ be a flag of type $(t_1, \ldots, t_t)$ on $\mathbb{F}_{q^n}$. Assume that m is a divisor of n such that $m = t_i$ for some $i \in \{1, \ldots, r\}$ and consider the subfield $\mathbb{F}_{q^m}$ of $\mathbb{F}_{q^n}$. Take an element $\beta \in \mathbb{F}_{q^n}^*$ such that $\mathbb{F}_{q^m}^* \subseteq \langle\beta\rangle$. Then:*

(1) The value $\frac{|\beta|}{q^m-1}$ divides $|\mathrm{Orb}_\beta(\mathcal{F})|$.

(2) We have $|\mathrm{Orb}_\beta(\mathcal{F})| = \frac{|\beta|}{q^m-1}$ if, and only if, each subspace $\mathcal{F}_j$ is a vector space over $\mathbb{F}_{q^m}$. In particular, $t_1 = m$.

Proof. As $\mathbb{F}_{q^m}^* \subseteq \langle\beta\rangle$, we have that $q^m - 1$ must divide $|\beta|$. This implies that $|\beta^{q^{t_i}-1}| = |\beta^{q^m-1}| = \frac{|\beta|}{q^m-1}$ and (1) follows directly from Proposition 3.5.

To prove (2), observe that $|\mathrm{Orb}_\beta(\mathcal{F})| = \frac{|\beta|}{q^m-1}$ holds if, and only if, $\mathrm{Stab}_\beta(\mathcal{F})$ is a subgroup of order q^m-1 of $\langle\beta\rangle$. By the uniqueness of subgroups of a cyclic group, it follows that $\mathrm{Stab}_\beta(\mathcal{F}) = \mathbb{F}_{q^m}^*$. Hence, the field $\mathrm{Stab}_\beta^+(\mathcal{F}) = \mathbb{F}_{q^m}$ is a subfield of $\mathrm{Stab}^+(\mathcal{F})$ and, by means of Remark 3.8, every subspace $\mathcal{F}_j$ has structure of $\mathbb{F}_{q^m}$-vector space. In particular, no dimension smaller than m can appear in the type vector, i.e., $t_1 = m$.

Conversely, assume that every $\mathcal{F}_j$ is a vector space over $\mathbb{F}_{q^m}$ for $j \in \{1,\dots,r\}$. In particular, $\mathcal{F}_1 = \mathbb{F}_{q^m}\gamma$ for some $\gamma \in \mathbb{F}_{q^n}^*$. As a consequence, multiplication by elements in $\mathbb{F}_{q^m}^* \subseteq \langle\beta\rangle$ is closed on every subspace $\mathcal{F}_j$. Hence, we have $\mathbb{F}_{q^m}^* \subseteq \mathrm{Stab}_\beta(\mathcal{F}_j)$ for $1 \leqslant j \leqslant r$ and, by means of (8), it holds $\mathbb{F}_{q^m}^* \subseteq \mathrm{Stab}_\beta(\mathcal{F})$. On the other hand, notice that $\mathrm{Stab}_\beta(\mathcal{F}) \subseteq \mathrm{Stab}_\beta(\mathcal{F}_1) = \mathbb{F}_{q^m}^*$. Thus, it follows that $\mathrm{Stab}_\beta(\mathcal{F}) = \mathbb{F}_{q^m}^*$ and $|\mathrm{Orb}_\beta(\mathcal{F})| = \frac{|\beta|}{q^m-1}$, as we wanted to prove. ∎

The second statement in Proposition 3.10 turns out specially interesting in the case of cyclic orbit codes, that is, when the acting group is $\mathbb{F}_{q^n}^*$.

Corollary 3.11. *Let $\mathcal{F} = (\mathcal{F}_1,\dots,\mathcal{F}_r)$ be a flag of type $(t_1,\dots,t_r)$ on $\mathbb{F}_{q^n}$. Assume that m is a divisor of n such that $m = t_i$ for some $i \in \{1,\dots,r\}$. If $|\mathrm{Orb}(\mathcal{F})| = \frac{q^n-1}{q^m-1}$, then $m = t_1$ and the constant dimension code $\mathrm{Orb}(\mathcal{F}_1)$ is the m-spread $\mathrm{Orb}(\mathbb{F}_{q^m})$. Moreover, the value m divides t_j, for $j \in \{1,\dots,r\}$.*

Proof. By means of Proposition 3.10, it is clear that the first dimension in the type vector is $t_1 = m$ and it divides every t_i. Moreover, $\mathcal{F}_1$ must be a one-dimensional vector space over $\mathbb{F}_{q^m}$, that is, it is of the form $\mathcal{F}_1 = \mathbb{F}_{q^m}\gamma$ for some $\gamma \in \mathbb{F}_{q^n}^*$. As a result, the first projected code $\mathrm{Orb}(\mathcal{F}_1) = \mathrm{Orb}(\mathbb{F}_{q^m})$ is the m-spread defined in (3). ∎

Remark 3.12. In the conditions of the previous corollary, if we require the subspace $\mathcal{F}_1$ to contain the element $1 \in \mathbb{F}_{q^n}$, not only do we obtain that $\mathrm{Orb}(\mathcal{F}_1) = \mathrm{Orb}(\mathbb{F}_{q^m})$ but also the equality $\mathcal{F}_1 = \mathbb{F}_{q^m}$.

In view of Propositions 3.7 and 3.10, it also makes sense the extension to flags of the concept of best friend introduced in [10].

Definition 3.13. Consider a flag $\mathcal{F}$ on $\mathbb{F}_{q^n}$. A subfield $\mathbb{F}_{q^m}$ of $\mathbb{F}_{q^n}$ is said to be a *friend* of the flag $\mathcal{F}$ if all its subspaces are $\mathbb{F}_{q^m}$-vector spaces. In other words, a subfield of $\mathbb{F}_{q^n}$ is a friend of the flag $\mathcal{F}$ if it is a friend of all its subspaces. We call *best friend* of the flag $\mathcal{F}$ to its largest friend.

The next result states a necessary condition on the type vector of flags having a given subfield of $\mathbb{F}_{q^n}$ as a friend. The proof is straightforward.

Lemma 3.14. *Let $\mathcal{F} = (\mathcal{F}_1,\dots,\mathcal{F}_r)$ be a flag of type $(t_1,\dots,t_r)$ on $\mathbb{F}_{q^n}$. If $\mathbb{F}_{q^m}$ is a friend of $\mathcal{F}$ then m divides $\gcd(t_1,\dots,t_r,n)$.*

Remark 3.15. If follows that the best friend of a flag of type $(t_1,\dots,t_r)$ with $\gcd(t_1,\dots,t_r,n) = 1$, in particular a full flag, is the ground field $\mathbb{F}_q$.

Beyond conditions on the type vector, we can always characterize the best friend of an arbitrary flag in terms of the ones of its subspaces. To do so, we generalize Proposition 2.2 to the flag codes scenario.

Proposition 3.16. *Let $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ be a flag on $\mathbb{F}_{q^n}$. Then $\mathrm{Stab}^+(\mathcal{F})$ is the best friend of the flag $\mathcal{F}$ and it contains any other friend $\mathbb{F}_{q^m}$ of $\mathcal{F}$. Moreover, if $1 \in \mathcal{F}_1$, then we have that $\mathbb{F}_{q^m} \subseteq \mathrm{Stab}^+(\mathcal{F}) \subseteq \mathcal{F}_1$.*

Proof. Let us prove that $\mathrm{Stab}^+(\mathcal{F})$ is the largest friend of $\mathcal{F}$, i.e., its best friend. To do so, assume that a subfield $\mathbb{F}_{q^m}$ of $\mathbb{F}_{q^n}$ is a friend of the flag $\mathcal{F}$. By definition of friend of a flag, we know that multiplication by elements in $\mathbb{F}_{q^m}$ is closed in every subspace $\mathcal{F}_i$ of the flag. As a consequence, $\mathbb{F}_{q^m}^*$ is a subgroup of $\mathrm{Stab}(\mathcal{F})$ and we can conclude that $\mathbb{F}_{q^m}$ is contained in $\mathrm{Stab}(\mathcal{F}) \cup \{0\} = \mathrm{Stab}^+(\mathcal{F})$. This proves that the stabilizer subfield of $\mathcal{F}$ is its best friend. Finally, by using the condition $1 \in \mathcal{F}_1$ together with Proposition 3.7, we obtain the inclusion

$$\mathbb{F}_{q^m} \subseteq \mathrm{Stab}^+(\mathcal{F}) \subseteq \mathrm{Stab}^+(\mathcal{F}_1) \subseteq \mathcal{F}_1.$$

∎

Remark 3.17. Observe that all flags in the code $\mathrm{Orb}(\mathcal{F})$ have the same best friend. In particular, since $\mathrm{Orb}_\beta(\mathcal{F}) \subseteq \mathrm{Orb}(\mathcal{F})$, flags in a β-cyclic orbit flag code have all the same best friend for every $\beta \in \mathbb{F}_{q^n}^*$. Hence, we say that $\mathrm{Stab}^+(\mathcal{F})$ is the best friend of every $\mathrm{Orb}_\beta(\mathcal{F})$.

As stated in the proof of Proposition 3.7, (see equation (9)), the stabilizer subfield of the cyclic flag code $\mathrm{Orb}(\mathcal{F})$ can be computed as the intersection of the ones of its projected codes. Combining this with Proposition 3.16, we obtain the next result.

Corollary 3.18. *Let $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ be a flag on $\mathbb{F}_{q^n}$. Then its best friend is the intersection of the ones of its subspaces. Moreover, if $1 \in \mathcal{F}_1$, every friend of the flag $\mathcal{F}$ is contained in $\mathcal{F}_1$.*

It is clear that the best friend of a flag is a subfield of the ones of its subspaces. However, while the subspaces in a flag are nested, their respective best friends might not form a sequence of nested subfields as we can see in the following example.

Example 3.19. Take q a prime power and the flag of type $(2, 3)$ on $\mathbb{F}_{q^4}$ given by $\mathcal{F} = (\mathbb{F}_{q^2}, \mathbb{F}_{q^2} + \mathbb{F}_q\alpha)$, where α denotes a primitive element of $\mathbb{F}_{q^4}$. In this case, the best friend of $\mathcal{F}_1$ is precisely $\mathbb{F}_{q^2}$ whereas, since $\gcd(3, 4) = 1$, the best friend of $\mathcal{F}_2$ is the ground field $\mathbb{F}_q$.

As it happens in the subspace codes setting, knowing the best friend of a cyclic orbit flag code gives relevant information about the code parameters as we will see below.

4 Cyclic orbit flag codes with fixed best friend

This section is devoted to the study of cyclic orbit flag codes on $\mathbb{F}_{q^n}$ generated by flags with the subfied $\mathbb{F}_{q^m}$ as their best friend. From now on, the integer m will denote a divisor of n. Let us first see how the close relationship between the best friend of a flag and its stabilizer allows us to compute the size of the generated cyclic or β-cyclic orbit flag code. The next result follows from (7) and Proposition 3.16.

Proposition 4.1. *Let $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ be a flag on $\mathbb{F}_{q^n}$ and $\beta \in \mathbb{F}_{q^n}^*$. Assume that $\mathbb{F}_{q^m}$ is the best friend of $\mathcal{F}$. Then*

$$|\mathrm{Orb}_\beta(\mathcal{F})| = \frac{|\beta|}{|\langle\beta\rangle \cap \mathbb{F}_{q^m}^*|}.$$

In particular, if β is a primitive element of $\mathbb{F}_{q^n}$, it holds $|\mathrm{Orb}(\mathcal{F})| = \frac{q^n-1}{q^m-1}$.

Remark 4.2. It is well known that any orbit coming from the action of a group can be partitioned into a set of orbits when we restrict the action to a subgroup. These orbits may have different cardinality in general. However, the cardinality of the code $\mathrm{Orb}_\beta(\mathcal{F})$ just depends on $|\beta|$ and the best friend of $\mathcal{F}$. Moreover, since all the flags in $\mathrm{Orb}(\mathcal{F})$ have the same best friend, we have that $|\mathrm{Orb}_\beta(\mathcal{F}')| = |\mathrm{Orb}_\beta(\mathcal{F})|$ for every $\mathcal{F}' \in \mathrm{Orb}(\mathcal{F})$. We conclude that, for any $\beta \in \mathbb{F}_{q^n}^*$ the code $\mathrm{Orb}(\mathcal{F})$ can be partitioned into a set of β-cyclic subcodes, all of them with the same cardinality.

Proposition 4.1 leads to a characterization of β-cyclic orbit flag codes whose size coincides with the order or the acting group.

Corollary 4.3. *Let $\mathcal{F}$ be a flag on $\mathbb{F}_{q^n}$ with $\mathbb{F}_{q^m}$ as its best friend and consider $\beta \in \mathbb{F}_{q^n}^*$. Then $|\mathrm{Orb}_\beta(\mathcal{F})| = |\beta|$ if, and only if $|\beta|$ and $q^m - 1$ are coprime. In particular, this equality always holds if $q = 2$ and $m = 1$.*

Having the subfield $\mathbb{F}_{q^m}$ as best friend yields a condition on the type vector of a flag, as well as a description of the structure of all the flags in its β-cyclic orbit flag code in terms of $\mathbb{F}_{q^m}$. Let $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ be a flag of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_{q^n}$ with $\mathbb{F}_{q^m}$ as its best friend. Hence, $\mathbb{F}_{q^m}$ must be a friend of all its subspaces and m divides every dimension in the type vector. Consequently, we can write $t_i = ms_i$ for $i = 1, \ldots, r$, where $1 \leqslant s_1 < s_2 < \cdots < s_r < s = \frac{n}{m}$. On the other hand, the nested structure of the flag $\mathcal{F}$ allows us to find linearly independent elements $a_1, \ldots, a_{s_r} \in \mathbb{F}_{q^n}$ (over $\mathbb{F}_{q^m}$) such that, for every $1 \leqslant i \leqslant r$, we have

$$\mathcal{F}_i = \bigoplus_{j=1}^{s_i} \mathbb{F}_{q^m} a_j.$$

In particular, observe that if m is a dimension in the type vector, then $s_1 = 1$ and the cyclic orbit code $\mathrm{Orb}(\mathcal{F}_1)$ is the m-spread of $\mathbb{F}_{q^n}$ described in (3). Moreover, if $1 \in \mathcal{F}_1$, this subspace must be the subfield $\mathbb{F}_{q^m}$.

Concerning the distance of β-cyclic orbit flag codes, as in the constant dimension codes framework, we can also deduce some estimates from the knowledge of the best friend.

Proposition 4.4. *Let $\mathcal{F}$ be a flag of type $(ms_1, \ldots, ms_r)$ on $\mathbb{F}_{q^n}$ with the subfield $\mathbb{F}_{q^m}$ as its best friend and take $\beta \in \mathbb{F}_{q^n}^*$. Then $d_f(\mathrm{Orb}_\beta(\mathcal{F})) = 0$ if, and only if, $\beta \in \mathbb{F}_{q^m}^*$. Out of this case, $2m$ divides $d_f(\mathrm{Orb}_\beta(\mathcal{F}))$ and it holds*

$$2m \leqslant d_f(\mathrm{Orb}_\beta(\mathcal{F})) \leqslant 2m \left(\sum_{s_i \leqslant \lfloor \frac{s}{2} \rfloor} s_i + \sum_{s_i > \lfloor \frac{s}{2} \rfloor} (s - s_i) \right). \tag{10}$$

Proof. Assume that $d_f(\mathrm{Orb}_\beta(\mathcal{F})) = 0$ or, equivalently, that $\mathrm{Orb}_\beta(\mathcal{F}) = \{\mathcal{F}\}$. This happens if, and only if, β stabilizes the flag $\mathcal{F}$, i.e., if $\beta \in \mathrm{Stab}(\mathcal{F}) = \mathbb{F}_{q^m}^*$.

Take now $\beta \in \mathbb{F}_{q^n}^* \setminus \mathbb{F}_{q^m}^*$. By the definition of best friend of the flag $\mathcal{F}$, it follows that $\mathbb{F}_{q^m}$ is a friend of every subspace $\mathcal{F}_i$. This implies that, for every $1 \leqslant i \leqslant r$, subspaces in $\mathrm{Orb}_\beta(\mathcal{F}_i)$ are vector spaces over $\mathbb{F}_{q^m}$. Take a flag $\mathcal{F}'$ in $\mathrm{Orb}_\beta(\mathcal{F}) \setminus \{\mathcal{F}\}$. Since, for every $1 \leqslant i \leqslant r$, both $\mathcal{F}_i$, $\mathcal{F}'_i$, and hence $\mathcal{F}_i \cap \mathcal{F}'_i$, are vector spaces over $\mathbb{F}_{q^m}$, the value m divides their dimensions (over $\mathbb{F}_q$). Taking into account that $d_S(\mathcal{F}_i, \mathcal{F}'_i) = 2(\dim(\mathcal{F}_i) - \dim(\mathcal{F}_i \cap \mathcal{F}'_i))$, we conclude that $2m$ divides $d_S(\mathcal{F}_i, \mathcal{F}'_i)$ for every $1 \leqslant i \leqslant r$. Consequently, the value $2m$ also divides $d_f(\mathcal{F}, \mathcal{F}') = \sum_{i=1}^r d_S(\mathcal{F}, \mathcal{F}')$, for every choice of $\mathcal{F}' \in \mathrm{Orb}_\beta(\mathcal{F}) \setminus \{\mathcal{F}\}$. In particular, $2m$ divides $d_f(\mathrm{Orb}_\beta(\mathcal{F}))$ and it is a lower bound for it. At the same time, if we consider the general upper bound for the distance of flag codes of type $(ms_1, \ldots, ms_r)$ on $\mathbb{F}_{q^n}$ given in (5), taking into account that $n = ms$, we obtain the result. ∎

Remark 4.5. Notice that for every $\beta \in \mathbb{F}_{q^n}^*$, it holds $\mathrm{Orb}_\beta(\mathcal{F}) \subseteq \mathrm{Orb}(\mathcal{F})$. Then it follows $d_f(\mathrm{Orb}_\beta(\mathcal{F})) \geqslant d_f(\mathrm{Orb}(\mathcal{F}))$ except for $\beta \in \mathrm{Stab}(\mathcal{F}) = \mathbb{F}_{q^m}^*$. However, not every β allows us to improve the distance with respect to the one of $\mathrm{Orb}(\mathcal{F})$. We can appreciate this fact in the next example.

Example 4.6. Take q a prime power and α a primitive element of $\mathbb{F}_{q^6}$. Consider $\mathcal{F}$ a flag of type $(1, 4)$ on $\mathbb{F}_{q^6}$ with subspaces

$$\mathcal{F}_1 = \mathbb{F}_q \text{ and } \mathcal{F}_2 = \mathbb{F}_{q^2} + \mathbb{F}_{q^2}\alpha.$$

Notice that, since $\gcd(1, 4, 6) = 1$, by application of Lemma 3.14, $\mathbb{F}_q$ is the best friend of $\mathcal{F}$. Clearly, it is the best friend of $\mathcal{F}_1$ as well. Concerning $\mathcal{F}_2$, observe that $\mathbb{F}_{q^2}$ is one of its friends. Hence, its best friend is a subfield of $\mathbb{F}_{q^6}$ containing $\mathbb{F}_{q^2}$. We conclude that $\mathbb{F}_{q^2}$ is the best friend of $\mathcal{F}_2$. The cyclic orbit flag code $\mathrm{Orb}(\mathcal{F})$ contains exactly $\frac{q^6-1}{q-1}$ flags and we have $d_f(\mathrm{Orb}(\mathcal{F})) = 2$. It suffices to see that, for every $\beta \in \mathbb{F}_{q^2}^* \setminus \mathbb{F}_q^* \subset \mathbb{F}_{q^6}^*$, it holds $\mathcal{F}_2 = \mathcal{F}_2\beta$ and

$$d_f(\mathcal{F}, \mathcal{F}\beta) = d_S(\mathcal{F}_1, \mathcal{F}_1\beta) = 2.$$

Observe that this is the minimum possible distance fixed the best friend $\mathbb{F}_q$. Now, if we consider the subgroup $\langle\gamma\rangle = \mathbb{F}_{q^2}^*$, the subcode $\mathrm{Orb}_\gamma(\mathcal{F})$ has cardinality $\frac{q^2-1}{q-1} = q + 1$ and the same argument above gives that $d_f(\mathrm{Orb}_\gamma(\mathcal{F})) = 2$. In this case, $\mathrm{Orb}_\gamma(\mathcal{F})$ does not have a better distance than $\mathrm{Orb}(\mathcal{F})$. Take now $\delta \in \mathbb{F}_{q^6}^*$ a generator of $\mathbb{F}_{q^3}^*$, then the δ-cyclic flag code generated by $\mathcal{F}$ contains $\frac{q^3-1}{q-1} = q^2 + q + 1$ flags. To compute its distance, observe that

$$\mathrm{Stab}_\delta(\mathcal{F}_2) = \langle\delta\rangle \cap \mathbb{F}_{q^2}^* = \mathbb{F}_{q^3}^* \cap \mathbb{F}_{q^2}^* = \mathbb{F}_q^* = \mathrm{Stab}_\delta(\mathcal{F}_1) = \mathrm{Stab}_\delta(\mathcal{F}).$$

Hence, for every $\delta^i \notin \mathrm{Stab}_\delta(\mathcal{F})$ it holds $\mathcal{F}_j \neq \mathcal{F}_j\delta^i$, for $j = 1, 2$. On the one hand, we have $d_S(\mathbb{F}_q, \mathbb{F}_q\delta^i) = 2$. On the other hand, as $\mathbb{F}_{q^2}$ is the best friend of $\mathcal{F}_2$, the value $d_S(\mathcal{F}_2, \mathcal{F}_2\delta^i)$ is a multiple of 4. Since the maximum possible distance between 4-dimensional subspaces of $\mathbb{F}_{q^6}$ is precisely $2(6-4) = 4$, it follows that $d_S(\mathcal{F}_2, \mathcal{F}_2\delta^i) = 4$. As a result, $d_f(\mathcal{F}, \mathcal{F}\delta^i) = 6$ for all $\delta^i \in \langle\delta\rangle \setminus \mathrm{Stab}_\delta(\mathcal{F})$ and we conclude that

$$d_f(\mathrm{Orb}_\delta(\mathcal{F})) = 6 > 2 = d_f(\mathrm{Orb}(\mathcal{F})).$$

Remark 4.7. Observe that the upper bound for the distance given in (10) coincides with the general bound for the flag distance given in (5). However, in Subsection 4.2, we will see that, in our scenario, not every type vector is compatible with attaining this upper bound. On the other hand, the lower bound for the distance of a β-cyclic flag code having $\mathbb{F}_{q^m}$ as its best friend obtained in (10) coincides with the one given in Proposition 2.2 for cyclic (subspace) codes having the same best friend. The previous example shows that this lower bound can also be attained by β-cyclic obit flag codes of length at least two. Let us see another situation where the generating flag has a special form.

Example 4.8. Let $\mathcal{F} = (\mathbb{F}_{3^2}, \mathbb{F}_{3^4})$ be the flag of type $(2, 4)$ on $\mathbb{F}_{3^8}$ defined in Example 3.9 and consider the cyclic orbit flag code $\mathrm{Orb}(\mathcal{F})$. Observe that, as stated in 3.9, the best friend of the flag $\mathcal{F}$ is the subfield $\mathbb{F}_{3^2}$. Moreover, $\mathrm{Stab}(\mathcal{F}) = \mathrm{Stab}(\mathcal{F}_1) = \mathbb{F}_{3^2}$ and $\mathrm{Stab}(\mathcal{F}_2) = \mathbb{F}_{3^4}$. Now, if α denotes a primitive element of $\mathbb{F}_{3^8}$, the power α^{82} is also a primitive element of the subfield $\mathbb{F}_{3^4}$. Hence, α^{82} clearly lies in $\mathbb{F}_{3^4}^* \setminus \mathbb{F}_{3^2}^*$. As a result, the flags $\mathcal{F}$ and $\mathcal{F}\alpha^{82}$ are different codewords in $\mathrm{Orb}(\mathcal{F})$ whereas we have the subspaces equality $\mathcal{F}_2 = \mathcal{F}_2\alpha^{82}$. It follows that

$$d_f(\mathrm{Orb}(\mathcal{F})) \leqslant d_f(\mathcal{F}, \mathcal{F}\alpha^{82}) = d_S(\mathbb{F}_{3^2}, \mathbb{F}_{3^2}\alpha^{82}) = 4,$$

which is the minimum possible distance between subspaces of dimension one over $\mathbb{F}_{3^2}$. Hence, we conclude that $d_f(\mathrm{Orb}(\mathcal{F})) = 4$.

Notice that in the previous example the two subspaces of the generating flag are nested subfields of a given finite field. This example gives rise to the definition of a family of cyclic orbit flag codes inspired by the towers of subfields of $\mathbb{F}_{q^n}$.

4.1 Galois cyclic flag codes

Let $1 \leqslant t_1 < \cdots < t_r < n$ be a sequence of divisors of n such that t_i divides t_{i+1}, for $1 \leqslant i \leqslant r-1$.

Definition 4.9. We define the *Galois flag* of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_{q^n}$ as the flag given by the sequence of nested subfields $(\mathbb{F}_{q^{t_1}}, \ldots, \mathbb{F}_{q^{t_r}})$. For every $\beta \in \mathbb{F}_{q^n}^*$, the β-cyclic orbit flag code generated by this flag is called the *Galois β-cyclic flag code* of type $(t_1, \ldots, t_r)$. When β is primitive, we just say *Galois cyclic flag code.*

Remark 4.10. Notice that, for each subgroup $\langle\beta\rangle \subseteq \mathbb{F}_{q^n}^*$, there is just one Galois β-cyclic flag code for each type vector satisfying the condition above. In contrast, the Galois β-cyclic flag code of a fixed type can be generated by different flags consisting of sequences of subspaces, not necessarily fields. Nevertheless, if we impose the condition $1 \in \mathcal{F}_1$, only the Galois flag of type $(t_1, \ldots, t_r)$ can generate the Galois β-cyclic flag code of this type.

Given the Galois flag $\mathcal{F}$ of type vector $(t_1, \ldots, t_r)$, it is clear that its i-th subspace is its own best friend. Hence, contrary to what happens for general flags (see Example 3.19), the best friends of the Galois flag subspaces form a

sequence of nested subfieds. As a consequence, the first subfield $\mathbb{F}_{q^{t_1}}$ is the best friend of the Galois flag of type $(t_1, \ldots, t_r)$ and, in order to construct Galois β-cyclic flag codes with the subfield $\mathbb{F}_{q^m}$ as its best friend, it suffices to consider a sequence of suitable divisors $(t_1, \ldots, t_r)$ starting at $t_1 = m$.

Let us start focusing on Galois cyclic flag codes (β primitive). According to Proposition 4.1, the cardinality of the Galois cyclic flag code of type $(t_1, \ldots, t_r)$ is $c_1 = (q^n - 1)/(q^{t_1} - 1)$ whereas its distance is $2t_1$. In particular, its i-projected code contains exactly $c_i = (q^n - 1)/(q^{t_i} - 1)$ subspaces and has subspace distance equal to $2t_i$. In spite of the fact that the distance of Galois cyclic flag codes is the smallest possible for cyclic orbit flag codes with a fixed best friend, the kaleidoscopic algebraic structure of nested spreads inside them is remarkable and deserves to be pointed out.

Theorem 4.11. *Let $\mathcal{F} = (\mathbb{F}_{q^{t_1}}, \ldots, \mathbb{F}_{q^{t_r}})$ be the Galois flag of type $(t_1, \ldots, t_r)$ on the field $\mathbb{F}_{q^n}$ and $\mathrm{Orb}(\mathcal{F})$ the associated Galois cyclic flag code. Consider α and α_i respective primitive elements of the fields $\mathbb{F}_{q^n}$ and $\mathbb{F}_{q^{t_i}}$, for $1 \leqslant i \leqslant r$. Then it holds:*

(1) Each projected code of $\mathrm{Orb}(\mathcal{F})$ is a t_i-spread of $\mathbb{F}_{q^n}$.

(2) The α_j-cyclic orbit code $\mathrm{Orb}_{\alpha_j}(\mathbb{F}_{q^{t_i}}\alpha^l)$ is a t_i-spread of the subspace $\mathbb{F}_{q^{t_j}}\alpha^l$, for every $i < j \leqslant r$ and $0 \leqslant l \leqslant c_j - 1$, where $c_j = (q^n - 1)/(q^{t_j} - 1)$.

Proof. Observe that, by the definition of Galois cyclic flag code, the i-projected code $\mathrm{Orb}(\mathcal{F}_i) = \mathrm{Orb}(\mathbb{F}_{q^{t_i}})$ is the t_i-spread of the field $\mathbb{F}_{q^n}$ described in (3). The same argument allows us to state that, for every $i < j \leqslant r$, the α_j-cyclic orbit code $\mathrm{Orb}_{\alpha_j}(\mathbb{F}_{q^{t_i}})$ is a t_i-spread of $\mathbb{F}_{q^{t_j}}$ as well. Moreover, since the subspace distance is invariant by the multiplicative action of $\mathbb{F}_{q^n}^* = \langle\alpha\rangle$ on subspaces, we have that $\mathrm{Orb}_{\alpha_j}(\mathbb{F}_{q^{t_i}}\alpha^l)$ is also a t_i-spread of the vector space $\mathbb{F}_{q^{t_j}}\alpha^l$, for every $0 \leqslant l \leqslant q^n - 2$. Now, taking into account that α^{c_j} is a primitive element of $\mathbb{F}_{q^{t_j}}$, we have that $\langle\alpha_j\rangle = \langle\alpha^{c_j}\rangle = \mathbb{F}_{q^{t_j}}^*$ and $\mathbb{F}_{q^{t_j}} = \mathbb{F}_{q^{t_j}}\alpha^{c_j}$. This fact allows us to restrict ourselves to exponents $0 \leqslant l \leqslant c_j - 1$. ∎

Remark 4.12. Note that Theorem 4.11, describes a striking cyclic spreads gear. First, every projected code of a Galois cyclic flag code is a spread. Then, every codeword in the j-projected code $\mathrm{Orb}(\mathbb{F}_{q^{t_j}})$, i.e., every subspace of the form $\mathbb{F}_{q^{t_j}}\alpha^l$, is partitioned into the subspaces of the α_j-cyclic orbit code $\mathrm{Orb}_{\alpha_j}(\mathbb{F}_{q^{t_i}}\alpha^l)$ if $i < j \leqslant r$. Thereby, we have that $\mathrm{Orb}_{\alpha_j}(\mathbb{F}_{q^{t_i}}\alpha^l)$ is a t_i-spread of $\mathbb{F}_{q^{t_j}}\alpha^l$ for every value $0 \leqslant l \leqslant c_j - 1$ and also a partial spread of dimension t_i of the field $\mathbb{F}_{q^n}$. Finally, the union of all these orbits

$$\dot{\bigcup_{l=0}^{c_j-1}} \mathrm{Orb}_{\alpha_j}(\mathbb{F}_{q^{t_i}}\alpha^l)$$

gives us back the t_i-spread $\mathrm{Orb}(\mathbb{F}_{q^{t_i}}) = \mathrm{Orb}(\mathcal{F}_i)$. In other words, Galois cyclic flag codes provide collections of nested spreads that respect the orbital structure induced by the action of $\langle\alpha\rangle$ on flags.

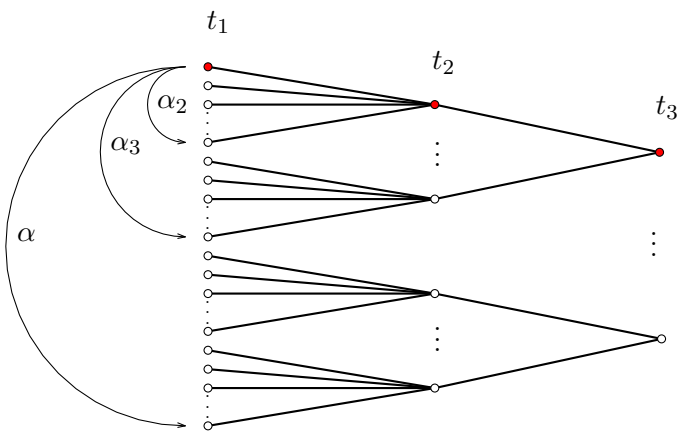

Figure 1: Nested spread structure of a Galois cyclic flag code

The previous figure represents the structure of the Galois cyclic flag code of a given type (t_1, t_2, t_3). Vertices are subspaces, (directed) edges denote inclusions (from left to right) and flags are given by directed paths in the graph. Each column in the graph is a projected code and, by Theorem 4.11, all of them are spreads of $\mathbb{F}_q^n$ of the corresponding dimensions. In addition, every subspace in the graph is partitioned into the set of its left adjacent vertices. On the other hand, the Galois flag $\mathcal{F} = (\mathbb{F}_{q^{t_1}}, \mathbb{F}_{q^{t_2}}, \mathbb{F}_{q^{t_3}})$ is represented by the sequence of red vertices. Since $\mathrm{Stab}(\mathcal{F}) = \mathbb{F}_{q^{t_1}}^* = \langle \alpha_1 \rangle$, the code $\mathrm{Orb}_{\alpha_1}(\mathcal{F})$ consists of the single element $\mathcal{F}$. In contrast, for $i = 2, 3$, the code $\mathrm{Orb}_{\alpha_i}(\mathcal{F})$ is given by the set of flags in the graph marked by the round arrow labeled with α_i.

Take now an element $\beta \in \mathbb{F}_{q^n}^*$. Let $\mathcal{F}$ be the Galois flag of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_{q^n}$ and consider the Galois β-cyclic flag code $\mathrm{Orb}_\beta(\mathcal{F})$. Since $\mathbb{F}_{q^{t_1}}$ is the best friend of $\mathcal{F}$, it follows that $\mathrm{Stab}_\beta(\mathcal{F}) = \langle \beta \rangle \cap \mathbb{F}_{q^{t_1}}^*$. Moreover, for every value of $1 \leqslant i \leqslant r$, it holds $\mathrm{Stab}_\beta(\mathcal{F}_i) = \langle \beta \rangle \cap \mathbb{F}_{q^{t_i}}^*$. As a result, we have the following sequence of nested subgroups of $\langle \beta \rangle$

$$\mathrm{Stab}_\beta(\mathcal{F}) = \mathrm{Stab}_\beta(\mathcal{F}_1) \subseteq \mathrm{Stab}_\beta(\mathcal{F}_2) \subseteq \cdots \subseteq \mathrm{Stab}_\beta(\mathcal{F}_r) \subseteq \langle \beta \rangle. \tag{11}$$

By means of Proposition 4.1, the cardinality of $\mathrm{Orb}_\beta(\mathcal{F})$ and the one of its i-projected code, for every $1 \leqslant i \leqslant r$, are respectively

$$|\mathrm{Orb}_\beta(\mathcal{F})| = \frac{|\beta|}{|\langle \beta \rangle \cap \mathbb{F}_{q^{t_1}}^*|} \text{ and } |\mathrm{Orb}_\beta(\mathcal{F}_i)| = \frac{|\beta|}{|\langle \beta \rangle \cap \mathbb{F}_{q^{t_i}}^*|}.$$

Furthermore, from Theorem 4.11, and taking into account that $\mathrm{Orb}_\beta(\mathcal{F}) \subseteq \mathrm{Orb}(\mathcal{F})$, we can derive the following result for the projected codes of a Galois β-cyclic flag code.

Corollary 4.13. *Let $\mathcal{F} = (\mathbb{F}_{q^{t_1}}, \ldots, \mathbb{F}_{q^{t_r}})$ be the Galois flag of type $(t_1, \ldots, t_r)$ on the field $\mathbb{F}_{q^n}$ and take a nonzero element $\beta \in \mathbb{F}_{q^n}$. For each $1 \leqslant i \leqslant r$,*

we write β_i to denote a generator of the cyclic subgroup $\langle \beta_i \rangle = \mathrm{Stab}_\beta(\mathbb{F}_{q^{t_i}}) = \langle \beta \rangle \cap \mathbb{F}_{q^{t_i}}^*$. Then the following statements hold:

(1) The projected code $\mathrm{Orb}_\beta(\mathcal{F}_i)$ is a partial spread of dimension t_i of $\mathbb{F}_{q^n}$.

(2) The β_j-cyclic orbit code $\mathrm{Orb}_{\beta_j}(\mathbb{F}_{q^{t_i}}\beta^l)$ is a partial spread of dimension t_i of the subspace $\mathbb{F}_{q^{t_j}}\beta^l$, for every $i < j \leqslant r$ and $0 \leqslant l \leqslant |\beta_j| - 1$.

Concerning the distance of Galois β-cyclic flag codes, since they are subcodes of the Galois cyclic flag code of the same type, their distance might be better than $2t_1$, apart from the case of the trivial subcode consisting just of the Galois flag, which has distance equal to zero. Actually, it is possible to determine the exact distance of a Galois β-cyclic flag code by checking the relationship between the subgroup $\langle \beta \rangle$ and the subfields $\mathbb{F}_{q^{t_i}}$ and vice versa, that is, if we choose a permitted distance, we can find a suitable subgroup (possibly not unique) to build a β-cyclic orbit Galois attaining such a distance. We state the precise conditions in the following result:

Theorem 4.14. *Let $\mathcal{F}$ be the Galois flag of type $(t_1, \ldots, t_r)$ and consider an element $\beta \in \mathbb{F}_{q^n}^*$. Then $d_f(\mathrm{Orb}_\beta(\mathcal{F})) \in \{0, 2t_1, 2(t_1+t_2), \ldots, 2(t_1+t_2+\cdots+t_r)\}$. Moreover,*

(1) $d_f(\mathrm{Orb}_\beta(\mathcal{F})) = 0$ if, and only if, $\mathrm{Stab}_\beta(\mathcal{F}_1) = \mathrm{Stab}_\beta(\mathcal{F}_r) = \langle \beta \rangle$.

(2) $d_f(\mathrm{Orb}_\beta(\mathcal{F})) = 2\sum_{i=1}^{r} t_i$ if, and only if, $\mathrm{Stab}_\beta(\mathcal{F}_1) = \mathrm{Stab}_\beta(\mathcal{F}_r) \neq \langle \beta \rangle$.

(3) $d_f(\mathrm{Orb}_\beta(\mathcal{F})) = 2\sum_{i=1}^{j-1} t_i$ if, and only if, $\mathrm{Stab}_\beta(\mathcal{F}_1) \neq \mathrm{Stab}_\beta(\mathcal{F}_r)$ and $j \in \{2, \ldots, r\}$ is the minimum index such that $\mathrm{Stab}_\beta(\mathcal{F}_1) \subsetneq \mathrm{Stab}_\beta(\mathcal{F}_j)$.

Proof. Recall that for every choice of β, the projected codes of $\mathrm{Orb}_\beta(\mathcal{F})$ are partial spreads. As a result, for every $0 \leqslant l \leqslant |\beta| - 1$, we have that $d_S(\mathcal{F}_j, \mathcal{F}_j\beta^l) \in \{0, 2t_j\}$. Moreover, $d_S(\mathcal{F}_j, \mathcal{F}_j\beta^l) = 0$ holds if, and only if, $\beta^l \in \mathrm{Stab}_\beta(\mathcal{F}_j)$. In this case, since $\mathrm{Stab}_\beta(\mathcal{F}_j) \subseteq \cdots \subseteq \mathrm{Stab}_\beta(\mathcal{F}_r)$ by (11), we have $d_S(\mathcal{F}_i, \mathcal{F}_i\beta^l) = 0$, for every $j \leqslant i \leqslant r$. Hence, distances between flags in $\mathrm{Orb}_\beta(\mathcal{F})$ belong to the set $\{0, 2t_1, 2(t_1 + t_2), \ldots, 2(t_1 + t_2 + \cdots + t_r)\}$. Let us see that all of them can be reached, by showing (1), (2) and (3).

(1) As proved in Proposition 4.4, we have $d_f(\mathrm{Orb}_\beta(\mathcal{F})) = 0$ if, and only if, $\beta \in \mathbb{F}_{q^{t_1}}^* = \mathrm{Stab}(\mathcal{F})$ or, by using (8), $\beta \in \mathrm{Stab}(\mathcal{F}_i)$ for all $1 \leqslant i \leqslant r$. Since $\mathrm{Stab}_\beta(\mathcal{F}_i) = \langle \beta \rangle \cap \mathrm{Stab}(\mathcal{F}_i)$ is always a subgroup of $\langle \beta \rangle$, the previous condition is equivalent to $\mathrm{Stab}_\beta(\mathcal{F}_i) = \langle \beta \rangle$, for every $1 \leqslant i \leqslant r$. Hence, by (11), we just need to check the equality $\mathrm{Stab}_\beta(\mathcal{F}_1) = \mathrm{Stab}_\beta(\mathcal{F}_r) = \langle \beta \rangle$.

In the remaining cases, $\mathrm{Stab}_\beta(\mathcal{F})$ must be a proper subgroup of $\langle \beta \rangle$.

(2) Assume now that $d_f(\mathrm{Orb}_\beta(\mathcal{F})) = 2\sum_{i=1}^{r} t_i$. Hence, for every $\beta^l \in \langle \beta \rangle \setminus \mathrm{Stab}_\beta(\mathcal{F})$, it must hold $d_S(\mathcal{F}_i, \mathcal{F}_i\beta^l) = 2t_i$, for all $1 \leqslant i \leqslant r$. This happens if, and only if, $\beta^l \notin \mathrm{Stab}_\beta(\mathcal{F}_i)$ for every $1 \leqslant i \leqslant r$. As a consequence, $\mathrm{Stab}_\beta(\mathcal{F}_i) \subseteq \mathrm{Stab}_\beta(\mathcal{F})$. On the other hand, by (8), we conclude that $\mathrm{Stab}_\beta(\mathcal{F}) = \mathrm{Stab}_\beta(\mathcal{F}_i)$ for every $1 \leqslant i \leqslant r$. Again, since these stabilizer subgroups are nested, this condition is equivalent to $\mathrm{Stab}_\beta(\mathcal{F}_1) = \mathrm{Stab}_\beta(\mathcal{F}_r)$.

(3) Consider the case $d_f(\mathrm{Orb}_\beta(\mathcal{F})) = 2\sum_{i=1}^{j-1} t_i$ for some $2 \leqslant j \leqslant r$. In other words, there exists some $\beta^l \in \langle\beta\rangle \setminus \mathrm{Stab}_\beta(\mathcal{F})$ such that

$$d_f(\mathrm{Orb}_\beta(\mathcal{F})) = d_f(\mathcal{F}, \mathcal{F}\beta^l) = 2\sum_{i=1}^{j-1} t_i.$$

This happens if, and only if

$$d_S(\mathcal{F}_i, \mathcal{F}_i\beta^l) = \begin{cases} 2t_i & \text{if} \quad 1 \leqslant i \leqslant j-1, \\ 0 & \text{if} \quad j \leqslant i \leqslant r, \end{cases}$$

or equivalently, if $\beta^l \in \langle\beta\rangle \setminus \mathrm{Stab}_\beta(\mathcal{F}_i)$ for $1 \leqslant i \leqslant j-1$, and $\beta^l \in \mathrm{Stab}_\beta(\mathcal{F}_i)$ for $j \leqslant i \leqslant r$. Hence, we conclude

$$\mathrm{Stab}_\beta(\mathcal{F}) = \mathrm{Stab}_\beta(\mathcal{F}_1) = \cdots = \mathrm{Stab}_\beta(\mathcal{F}_{j-1}) \subsetneq \mathrm{Stab}_\beta(\mathcal{F}_j).$$

∎

Graphically, Galois β-cyclic flag codes can be represented as subgraphs of the graph in Figure 1. In the next picture, flags in a Galois β-cyclic flag code are marked with black lines. In contrast, directed paths containing dotted edges represent flags in $\mathrm{Orb}(\mathcal{F}) \setminus \mathrm{Orb}_\beta(\mathcal{F})$. The index j in Theorem 4.14 states that no flags in the code share subspaces of dimensions t_i, for $1 \leqslant i \leqslant j-1$, whereas there exist different flags having the same j-th subspace. At left, and example of Galois β-cyclic flag code with distance $2t_1$ ($j = 2$). At right, the corresponding index and distance are $j = 3$ and $2(t_1 + t_2)$, respectively.

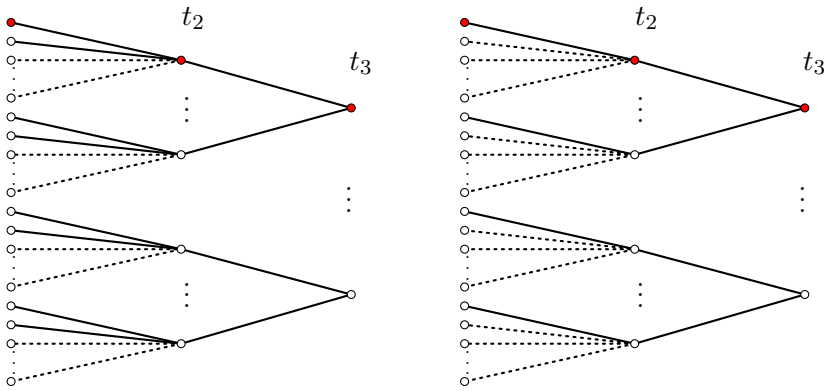

Figure 2: Two different Galois β-cyclic of type (t_1, t_2, t_3).

Observe that Theorem 4.14 allows us to provide specific constructions of Galois β-cyclic flag codes with a prescribed distance just by choosing a suitable element $\beta \in \mathbb{F}_{q^n}^*$. Moreover, since $\mathbb{F}_{q^n}^* = \langle\alpha\rangle$, being α a primitive element of $\mathbb{F}_{q^n}$, we can translate the above conditions on the stabilizers (w.r.t. β) in terms of suitable powers of α as follows. Given $\beta \in \mathbb{F}_{q^n}^*$, we can write $|\beta| = (q^n - 1)/l$ for some divisor l of $q^n - 1$. Hence, by the uniqueness of subgroups of a given order of the cyclic group $\mathbb{F}_{q^n}^*$, it is clear that $\langle\beta\rangle = \langle\alpha^l\rangle$. In particular, if

$c_i = (q^n-1)/(q^{t_i}-1)$, we have that $\mathbb{F}_{q^{t_i}}^* = \langle \alpha^{c_i} \rangle$, for every $1 \leqslant i \leqslant r$. As a consequence, it holds $\mathrm{Stab}_\beta(\mathbb{F}_{q^{t_i}}) = \langle \beta \rangle \cap \mathbb{F}_{q^{t_i}}^* = \langle \alpha^l \rangle \cap \langle \alpha^{c_i} \rangle = \langle \alpha^{l_i} \rangle$, where $l_i = \mathrm{lcm}(l, c_i)$. Moreover, given that each c_{i+1} divides c_i, then l_{i+1} divides l_i, for every $1 \leqslant i \leqslant r-1$, and the sequence of nested stabilizers given in (11) becomes

$$\langle \alpha^{l_1} \rangle \subseteq \langle \alpha^{l_2} \rangle \subseteq \cdots \subseteq \langle \alpha^{l_r} \rangle \subseteq \langle \alpha^{l} \rangle.$$

Now, since $l, c_1, \ldots, c_r$ divide $q^n - 1$, every exponent l_i divides $q^n - 1$ as well. Hence, the order of each stabilizer is $|\mathrm{Stab}_\beta(\mathbb{F}_{q^{t_i}})| = |\alpha^{l_i}| = \frac{q^n-1}{l_i}$, for every $1 \leqslant i \leqslant r$. We can reformulate Theorem 4.14 as follows:

Theorem 4.15. *Let $\mathcal{F}$ be the Galois flag of type $(t_1, \ldots, t_r)$ and consider $\beta \in \mathbb{F}_{q^n}^*$ such that $\langle \beta \rangle = \langle \alpha^l \rangle$ for some divisor l of $q^n - 1$. It holds:*

(1) $d_f(\mathrm{Orb}_\beta(\mathcal{F})) = 0$ if, and only if, $l_1 = l_r = l$.

(2) $d_f(\mathrm{Orb}_\beta(\mathcal{F})) = 2\sum_{i=1}^{r} t_i$ if, and only if, $l_1 = l_r \neq l$.

(3) $d_f(\mathrm{Orb}_\beta(\mathcal{F})) = 2\sum_{i=1}^{j-1} t_i$ if, and only if, $l_1 \neq l_r$ and $2 \leqslant j \leqslant r$ is the minimum index such that $l_1 \neq l_j$

Example 4.16. Take $\mathcal{F}$ the Galois flag of type $(2, 4, 8)$ on $\mathbb{F}_{2^{16}}$ and let α be a primitive element of $\mathbb{F}_{2^{16}}$. The following table shows the parameters of all possible Galois β-cyclic flag codes of this type. The sizes of the stabilizer subgroups (w.r.t. β) of the fields $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ are given, together with the cardinality and distance (just denoted by d_β) of $\mathrm{Orb}_\beta(\mathcal{F})$.

β	$\lvert\beta\rvert$	$\lvert\mathrm{Stab}_\beta(\mathbb{F}_{2^2})\rvert$	$\lvert\mathrm{Stab}_\beta(\mathbb{F}_{2^4})\rvert$	$\lvert\mathrm{Stab}_\beta(\mathbb{F}_{2^8})\rvert$	$\lvert\mathrm{Orb}_\beta(\mathcal{F})\rvert$	d_β
α	65535	3	15	255	21845	4
α^3	21845	1	5	85	21845	4
α^5	13107	3	3	51	4369	12
α^{15}	4369	1	1	17	4369	12
α^{17}	3855	3	15	15	1285	4
α^{51}	1285	1	5	5	1285	4
α^{85}	771	3	3	3	257	28
α^{255}	257	1	1	1	257	28
α^{257}	255	3	15	255	85	4
α^{771}	85	1	5	85	85	4
α^{1285}	51	3	3	51	17	12
α^{3855}	17	1	1	17	17	12
α^{4369}	15	3	15	15	5	4
α^{13107}	5	1	5	5	5	4
α^{21845}	3	3	3	3	1	0
1	1	1	1	1	1	0

Table 1: Parameters of all Galois β-cyclic flag codes of type $(2, 4, 8)$ on $\mathbb{F}_{2^{16}}$.

Clearly, different subgroups of $\mathbb{F}_{q^n}^*$ can provide the same code. For instance, the subgroup $\langle \alpha^3 \rangle$ gives the Galois cyclic flag code $\mathrm{Orb}(\mathcal{F})$. We have also $\mathrm{Orb}_{\alpha^5}(\mathcal{F}) = \mathrm{Orb}_{\alpha^{15}}(\mathcal{F})$ or $\mathrm{Orb}_{\alpha^{85}}(\mathcal{F}) = \mathrm{Orb}_{\alpha^{255}}(\mathcal{F})$, among other possibilities.

Remark 4.17. As proved in the previous theorem, the Galois β-cyclic code of type $(t_1, \ldots, t_r)$ attains the maximum possible distance for its type if, and only if, it holds

$$\mathrm{Stab}_\beta(\mathcal{F}_1) = \mathrm{Stab}_\beta(\mathcal{F}_r) \subsetneq \langle \beta \rangle. \tag{12}$$

In other words, if condition (12) is satisfied, we can build an optimum distance flag code with $\mathbb{F}_{q^{t_1}}$ as its best friend. This fact drives us to investigate cyclic orbit flag codes with the maximum possible distance and fixed best friend when the generating flag is not necessarily a Galois flag.

4.2 Optimum distance cyclic orbit flag codes

This subsection is devoted to the study of flag codes on $\mathbb{F}_{q^n}$ reaching the maximum distance and being also β-cyclic orbit flag codes with a prescribed best friend $\mathbb{F}_{q^m}$. To tackle this problem, we have to take into account first that, in particular, optimum distance flag codes must be disjoint as proved in [3]. Recall that a flag code $\mathcal{C}$ of type $(t_1, \ldots, t_r)$ is said to be *disjoint* if $|\mathcal{C}| = |\mathcal{C}_1| = \cdots = |\mathcal{C}_r|$. In our specific context, we have that a β-cyclic flag code $\mathrm{Orb}_\beta(\mathcal{F})$ is disjoint if, and only if,

$$\frac{|\beta|}{|\mathrm{Stab}_\beta(\mathcal{F})|} = \frac{|\beta|}{|\mathrm{Stab}_\beta(\mathcal{F}_1)|} = \cdots = \frac{|\beta|}{|\mathrm{Stab}_\beta(\mathcal{F}_r)|}$$

or, equivalently, if all the stabilizers $\mathrm{Stab}_\beta(\mathcal{F}), \mathrm{Stab}_\beta(\mathcal{F}_1), \ldots, \mathrm{Stab}_\beta(\mathcal{F}_r)$ have the same order. In fact, by the uniqueness of subgroups of a cyclic group, all these stabilizers must coincide. Moreover, by using (8), we have the next result:

Proposition 4.18. *The following statements are equivalent:*

(1) $\mathrm{Orb}_\beta(\mathcal{F})$ *is a disjoint flag code,*

(2) $\mathrm{Stab}_\beta(\mathcal{F}) = \mathrm{Stab}_\beta(\mathcal{F}_1) = \cdots = \mathrm{Stab}_\beta(\mathcal{F}_r)$.

(3) $\mathrm{Stab}_\beta(\mathcal{F}_1) = \cdots = \mathrm{Stab}_\beta(\mathcal{F}_r)$.

In light of Propositions 3.7 and 3.16, the best friend of a flag $\mathcal{F}$ can be computed as $\mathrm{Stab}^+(\mathcal{F}) = \mathrm{Stab}(\mathcal{F}) \cup \{0\}$. Similarly, the best friend of its subspaces are given by $\mathrm{Stab}^+(\mathcal{F}_i) = \mathrm{Stab}(\mathcal{F}_i) \cup \{0\}$. The next result leads directly a characterization of disjoint β-cyclic orbit flag codes in terms of β and the best friends of the generating flag and its subspaces.

Proposition 4.19. *Let $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ be a flag on $\mathbb{F}_{q^n}$ with $\mathbb{F}_{q^m}$ as its best friend and take $\beta \in \mathbb{F}_{q^n}^*$. If $\mathbb{F}_{q^{m_i}}$ denotes the best friend of $\mathcal{F}_i$, then the β-cyclic orbit code $\mathrm{Orb}_\beta(\mathcal{F})$ is disjoint if, and only if*

$$\langle \beta \rangle \cap \mathbb{F}_{q^m}^* = \langle \beta \rangle \cap \mathbb{F}_{q^{m_1}}^* = \cdots = \langle \beta \rangle \cap \mathbb{F}_{q^{m_r}}^*.$$

In particular, the cyclic orbit flag code $\mathrm{Orb}(\mathcal{F})$ is disjoint if, and only if, all the subspaces in the flag have the field $\mathbb{F}_{q^m}$ as their best friend.

Proof. By means of Proposition 4.18, the code $\mathrm{Orb}_\beta(\mathcal{F})$ is disjoint if, and only if, for every $1 \leqslant i \leqslant r$, it holds $\mathrm{Stab}_\beta(\mathcal{F}_i) = \mathrm{Stab}_\beta(\mathcal{F})$. Since $\mathrm{Stab}_\beta(\mathcal{F}_i) = \langle\beta\rangle \cap \mathbb{F}_{q^{m_i}}^*$, for every $1 \leqslant i \leqslant r$, and $\mathrm{Stab}_\beta(\mathcal{F}) = \langle\beta\rangle \cap \mathbb{F}_{q^m}^*$, the result follows. In the particular case of β primitive, then it must hold $\mathrm{Stab}(\mathcal{F}_i) = \mathbb{F}_{q^m}^*$, i.e., the best friend of each $\mathcal{F}_i$ coincides with the one of $\mathcal{F}$. ∎

Observe that it is possible to give a tighter lower bound for the distance of disjoint β-cyclic orbit flag codes with $\mathbb{F}_q^m$ as best friend. In order to avoid codes with distance equal to zero, throughout the rest of the section we only consider elements $\beta \in \mathbb{F}_{q^n}^* \setminus \mathbb{F}_{q^m}^*$.

Proposition 4.20. *Let $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ be a flag on $\mathbb{F}_{q^n}$ with the subfield $\mathbb{F}_{q^m}$ as its best friend and $\beta \in \mathbb{F}_{q^n}^*$. If the code $\mathrm{Orb}_\beta(\mathcal{F})$ is disjoint, then $2mr \leqslant d_f(\mathrm{Orb}_\beta(\mathcal{F}))$.*

Proof. Let $\mathcal{F}'$ be a flag in $\mathrm{Orb}_\beta(\mathcal{F})$ with $\mathcal{F}' \neq \mathcal{F}$. As $\mathrm{Orb}_\beta(\mathcal{F})$ is a disjoint flag code, we have that $\mathcal{F}_i \neq \mathcal{F}'_i$ for every $1 \leqslant i \leqslant r$. Hence, by means of Proposition 2.2, for every $1 \leqslant i \leqslant r$, we have that $d_S(\mathcal{F}_i, \mathcal{F}'_i) \geqslant 2m$. We conclude that $d_f(\mathcal{F}, \mathcal{F}') \geqslant 2mr$, for every $\mathcal{F}' \in \mathrm{Orb}_\beta(\mathcal{F}) \setminus \{\mathcal{F}\}$, and the result holds. ∎

As shown in Proposition 4.1, the cardinality of a β-cyclic flag code $\mathrm{Orb}_\beta(\mathcal{F})$ with $\mathbb{F}_{q^m}^*$ as its best friend is completely determined. Moreover, we know that $\langle\beta\rangle = \langle\alpha^l\rangle$, for the divisor l of $q^n - 1$ such that $|\beta| = \frac{q^n-1}{l}$. Similarly, $\mathbb{F}_{q^m}^* = \langle\alpha^{\frac{q^n-1}{q^m-1}}\rangle$. Moreover, it holds

$$\mathrm{Stab}_\beta(\mathcal{F}) = \langle\alpha^{\mathrm{lcm}(l, \frac{q^n-1}{q^m-1})}\rangle \text{ and } |\mathrm{Stab}_\beta(\mathcal{F})| = \frac{q^n-1}{\mathrm{lcm}(l, \frac{q^n-1}{q^m-1})}.$$

As a result,

$$|\mathrm{Orb}_\beta(\mathcal{F})| = \frac{\mathrm{lcm}\left(l, \frac{q^n-1}{q^m-1}\right)}{l}. \tag{13}$$

Using this notation, the next result follows.

Theorem 4.21. *Let $\mathcal{F}$ be a flag on $\mathbb{F}_{q^n}$ with best friend $\mathbb{F}_{q^m}$. Take $\beta \in \mathbb{F}_{q^n}^*$ and write $\langle\beta\rangle = \langle\alpha^l\rangle$ with l a divisor of $q^n - 1$. If $\mathrm{Orb}_\beta(\mathcal{F})$ is an optimum distance flag code and t is a dimension in the type vector of $\mathcal{F}$, then m divides t and it must hold*

$$\frac{\mathrm{lcm}(l, \frac{q^n-1}{q^m-1})}{l} \leqslant \begin{cases} \left\lfloor \frac{q^n-1}{q^t-1} \right\rfloor & \text{if } \ 2t \leqslant n, \\ \left\lfloor \frac{q^n-1}{q^{n-t}-1} \right\rfloor & \text{if } \ 2t > n. \end{cases}$$

Proof. Consider a flag $\mathcal{F}$ on $\mathbb{F}_{q^n}$ with the subfield $\mathbb{F}_{q^m}$ as its best friend and assume that the code $\mathrm{Orb}_\beta(\mathcal{F})$ is an optimum distance flag code. Hence, by application of Lemma 3.14, m must divide every dimension in the type vector. Moreover, by means of Theorem 3.3, all the projected codes attain the maximum possible distance for their dimension and $\mathrm{Orb}_\beta(\mathcal{F})$ is disjoint. In other words, the cardinality of every projected code coincides with $|\mathrm{Orb}_\beta(\mathcal{F})|$. In particular, this value has to satisfy the bounds for the cardinality of constant dimension codes of maximum distance given in Section 2 for dimensions in the type vector. As a result, if t is a dimension in the type vector, it must hold:

(1) If $2t \leqslant n$, then $|\mathrm{Orb}_\beta(\mathcal{F})| \leqslant \left\lfloor \frac{q^n-1}{q^t-1} \right\rfloor$ and

(2) if $2t > n$, then $|\mathrm{Orb}_\beta(\mathcal{F})| \leqslant \left\lfloor \frac{q^n-1}{q^{n-t}-1} \right\rfloor$.

Moreover, assuming $\langle \beta \rangle = \langle \alpha^l \rangle$ for some divisor l of $q^n - 1$, by using (13), the result holds. ∎

Remark 4.22. Observe that a dimension t satisfies the necessary condition provided in Theorem 4.21 if, and only if, the dimension $n-t$ does it as well. This is due to the fact that the upper bound for the cardinality of constant dimension codes with maximum distance of dimensions t and $n-t$ of $\mathbb{F}_{q^n}$ coincide. Moreover, these upper bounds decrease as dimensions get closer to $n/2$. Hence, central dimensions are allowed for a smaller number elements $\beta \in \mathbb{F}_{q^n}^*$ than the other ones. In contrast, extreme dimensions, that is, m and $n-m$, are allowed for every subgroup of $\mathbb{F}_{q^n}^*$. In fact, when the acting group is $\mathbb{F}_{q^n}^*$, we can derive the following corollary.

Corollary 4.23. *Assume that the cyclic orbit code* $\mathrm{Orb}(\mathcal{F})$ *is an optimum distance flag code on* $\mathbb{F}_{q^n}$ *with the subfield* $\mathbb{F}_{q^m}$ *as its best friend. Then one of the following statements holds:*

(1) $\mathrm{Orb}(\mathcal{F})$ *is a constant dimension code of dimension either* m *or* $n-m$.

(2) $\mathrm{Orb}(\mathcal{F})$ *has type vector* $(m, n-m)$.

In any of the three cases above, the code $\mathrm{Orb}(\mathcal{F})$ *has the largest possible size, that is,* $\frac{q^n-1}{q^m-1}$.

Proof. This result follows by application of Theorem 3.3 when β is a primitive element of $\mathbb{F}_{q^n}^*$. In this case, the cardinality of every projected code is $\frac{q^n-1}{q^m-1}$. Moreover, if t is a dimension in the type vector, it has to be a multiple of m. Observe that, both m and $n-m$ satisfy the necessary condition given in Theorem 4.21. On the other hand, this condition is violated by any other multiple of m. Hence, only dimensions m or $n-m$ could appear in the type vector of $\mathcal{F}$. As a result, optimum distance cyclic orbit flag codes with $\mathbb{F}_{q^m}$ as their best friend could only be constructed for type vectors equal to (m), $(n-m)$ or $(m, n-m)$. For these three type vectors, the cardinality of $\mathrm{Orb}(\mathcal{F})$, which is also $\frac{q^n-1}{q^m-1}$, coincides with the largest possible size of constant dimension codes with maximum distance for both dimensions m and $n-m$. Hence, it is the best size for optimum distance flag codes with any of these type vectors. ∎

Apart from the case where the type vector is $(m, n-m)$, we see that optimum distance cyclic orbit flag codes with $\mathbb{F}_{q^m}$ as their best friend are actually cyclic orbit (subspace) codes of dimension either m or $n-m$. In case the dimension is m, the code $\mathrm{Orb}(\mathcal{F})$ is, in addition, the m-spread $\mathrm{Orb}(\mathbb{F}_{q^m})$ of $\mathbb{F}_{q^n}$.

From Theorem 4.21 and Corollary 4.23, one can deduce that not every type vector is compatible with attaining the maximum possible distance once we have fixed the best friend of the generating flag of a β-cyclic orbit flag code. The following examples exhibit this fact.

Example 4.24. Let $\mathcal{F}$ be a flag on $\mathbb{F}_{2^{12}}$ with the subfield $\mathbb{F}_{2^2}$ as its best friend. This condition implies that the dimensions in the type vector of $\mathcal{F}$ must be even integers. Notice that $|\mathbb{F}_{2^{12}}^*| = 2^{12} - 1 = 4095 = 273 \cdot 15$ and $\langle \alpha^{15} \rangle$ is the only subgroup of $\mathbb{F}_{2^{12}}^*$ of order 273. On the other hand, we have $\mathbb{F}_{2^2}^* = \langle \alpha^{1365} \rangle$. Since $\operatorname{lcm}(15, 1365) = 1365$, we have $|\mathrm{Orb}_\beta(\mathcal{F})| = \frac{1365}{15} = 91$, for every $\beta \in \langle \alpha^{15} \rangle$. Now, assume that $\mathrm{Orb}_\beta(\mathcal{F})$ is an optimum distance flag code. If we compare its size with the upper bounds for the cardinality of constant dimension codes of $\mathbb{F}_{2^{12}}$ with maximum distance, we conclude that the dimension 6 cannot appear in the type vector of $\mathrm{Orb}_\beta(\mathcal{F})$ since $\frac{2^{12}-1}{2^6-1} = 65 < 91$. In contrast, dimensions $2, 4, 8$ and 10 satisfy the necessary condition given in Theorem 4.21.

Example 4.25. Consider a flag $\mathcal{F}$ on $\mathbb{F}_{q^n}$ with the subfield $\mathbb{F}_{q^m}$ as its best friend and let α denote a primitive element of $\mathbb{F}_{q^n}$. The tables below illustrate which dimensions are susceptible to appear in the type vector of the optimum distance β-cyclic orbit flag code generated by $\mathcal{F}$ for different choices of β and specific values of q, n and m.

β	$\lvert\beta\rvert$	$\langle\beta\rangle \cap \mathbb{F}_{q^m}^*$	$\lvert\mathrm{Orb}_\beta(\mathcal{F})\rvert$	Allowed dimensions	Max. distance
α	6560	$\mathbb{F}_3^*$	3280	1, 7	4
α^2	3280	$\mathbb{F}_3^*$	1640	1, 7	4
α^4	1640	$\mathbb{F}_3^*$	820	1, 2, 6, 7	12
α^5	1312	$\mathbb{F}_3^*$	656	1, 2, 6, 7	12
α^8	820	$\mathbb{F}_3^*$	410	1, 2, 6, 7	12
α^{10}	656	$\mathbb{F}_3^*$	328	1, 2, 6, 7	12
α^{16}	410	$\mathbb{F}_3^*$	205	1, 2, 3, 5, 6, 7	24
α^{20}	328	$\mathbb{F}_3^*$	164	1, 2, 3, 5, 6, 7	24
α^{32}	205	$\{1\}$	205	1, 2, 3, 5, 6, 7	24
α^{40}	164	$\mathbb{F}_3^*$	82	1, 2, 3, 4, 5, 6, 7	32
α^{41}	160	$\mathbb{F}_3^*$	80	1, 2, 3, 4, 5, 6, 7	32
α^{80}	82	$\mathbb{F}_3^*$	41	1, 2, 3, 4, 5, 6, 7	32
α^{82}	80	$\mathbb{F}_3^*$	40	1, 2, 3, 4, 5, 6, 7	32
α^{160}	41	$\{1\}$	41	1, 2, 3, 4, 5, 6, 7	32
α^{164}	40	$\mathbb{F}_3^*$	20	1, 2, 3, 4, 5, 6, 7	32
α^{205}	32	$\mathbb{F}_3^*$	16	1, 2, 3, 4, 5, 6, 7	32
α^{328}	20	$\mathbb{F}_3^*$	10	1, 2, 3, 4, 5, 6, 7	32
α^{410}	16	$\mathbb{F}_3^*$	8	1, 2, 3, 4, 5, 6, 7	32
α^{656}	10	$\mathbb{F}_3^*$	5	1, 2, 3, 4, 5, 6, 7	32
α^{820}	8	$\mathbb{F}_3^*$	4	1, 2, 3, 4, 5, 6, 7	32
α^{1312}	5	$\{1\}$	5	1, 2, 3, 4, 5, 6, 7	32
α^{1640}	4	$\mathbb{F}_3^*$	2	1, 2, 3, 4, 5, 6, 7	32
α^{3280}	2	$\mathbb{F}_3^*$	1	1, 2, 3, 4, 5, 6, 7	0
1	1	$\{1\}$	1	1, 2, 3, 4, 5, 6, 7	0

Table 2: Values for $q = 3$, $n = 8$, $m = 1$ and all subgroups of $\mathbb{F}_{3^8}^*$.

As it occurs when considering Galois β-cyclic flag codes, in these tables we can see that different subgroups of $\mathbb{F}_{q^n}^*$ (hence, subgroups with different order) can provide the same β-cyclic orbit flag code. Furthermore, there are different subgroups providing in turn different orbits but sharing the set of allowed dimensions and, as a consequence, also sharing the maximum possible value for the distance. For instance, in Table 3, both subgroups $\langle \alpha^3 \rangle$ and $\langle \alpha^9 \rangle$

give us the same orbit. On the other hand, the orbits under the action of $\langle\alpha^5\rangle$ and $\langle\alpha^7\rangle$ have different cardinality (thus, they are different codes) but their sets of allowed dimensions are equal.

β	$\lvert\beta\rvert$	$\langle\beta\rangle \cap \mathbb{F}_{q^m}^*$	$\lvert\mathrm{Orb}_\beta(\mathcal{F})\rvert$	Allowed dimensions	Max. distance
α	4095	$\mathbb{F}_{2^2}^*$	1365	2, 10	8
α^3	1365	$\mathbb{F}_{2^2}^*$	455	2, 10	8
α^5	819	$\mathbb{F}_{2^2}^*$	273	2, 4, 8, 10	24
α^7	585	$\mathbb{F}_{2^2}^*$	195	2, 4, 8, 10	24
α^9	455	$\{1\}$	455	2, 10	8
α^{13}	315	$\mathbb{F}_{2^2}^*$	105	2, 4, 8, 10	24
α^{15}	273	$\mathbb{F}_{2^2}^*$	91	2, 4, 8, 10	24
α^{21}	195	$\mathbb{F}_{2^2}^*$	65	2, 4, 6, 8, 10	36
α^{35}	117	$\mathbb{F}_{2^2}^*$	39	2, 4, 6, 8, 10	36
α^{39}	105	$\mathbb{F}_{2^2}^*$	35	2, 4, 6, 8, 10	36
α^{45}	91	$\{1\}$	91	2, 4, 8, 10	24
α^{63}	65	$\{1\}$	65	2, 4, 6, 8, 10	36
α^{65}	63	$\mathbb{F}_{2^2}^*$	21	2, 4, 6, 8, 10	36
α^{91}	45	$\mathbb{F}_{2^2}^*$	15	2, 4, 6, 8, 10	36
α^{105}	39	$\mathbb{F}_{2^2}^*$	13	2, 4, 6, 8, 10	36
α^{117}	35	$\{1\}$	35	2, 4, 6, 8, 10	36
α^{195}	21	$\mathbb{F}_{2^2}^*$	7	2, 4, 6, 8, 10	36
α^{273}	15	$\mathbb{F}_{2^2}^*$	5	2, 4, 6, 8, 10	36
α^{315}	13	$\{1\}$	13	2, 4, 6, 8, 10	36
α^{455}	9	$\mathbb{F}_{2^2}^*$	3	2, 4, 6, 8, 10	36
α^{585}	7	$\{1\}$	7	2, 4, 6, 8, 10	36
α^{819}	5	$\{1\}$	5	2, 4, 6, 8, 10	36
α^{1365}	3	$\mathbb{F}_{2^2}^*$	1	2, 4, 6, 8, 10	0
1	1	$\{1\}$	1	2, 4, 6, 8, 10	0

Table 3: Values for $q = 2$, $n = 12$, $m = 2$ and all subgroups of $\mathbb{F}_{2^{12}}^*$.

Remark 4.26. Observe that results 4.21 and 4.23 give us necessary conditions on the type vector for the existence of optimum distance β-cyclic orbit flag codes but the problem of constucting them remains open. In Subsection 4.1 we have characterized optimum distance Galois β-cyclic flag codes and built them by providing a suitable subgroup $\langle\beta\rangle$ of $\mathbb{F}_{q^n}^*$. Recall that in that case, the allowed dimensions correspond to the divisors appearing in the type vector of the generating Galois flag. Looking at Table 3, for instance, we can obtain optimum distance Galois β-cyclic flag codes of types $(2, 4)$ and $(2, 6)$.

Apart from optimum distance cyclic flag codes of Galois type, as far as we know, there are only two constructions of optimum distance flag codes given by the action of a cyclic subgroup of $\mathbb{F}_{q^n}$. One of them can be found in [14, Prop. 2.5], where the author, for every prime power q, provide a cyclic orbit full flag code on $\mathbb{F}_{q^3}$ (hence, of type $(1, 2)$) with maximum distance as a matching code obtained from the action of $\mathbb{F}_{q^3}^*$. The same argument allows us to build optimum distance cyclic orbit flag codes with best friend $\mathbb{F}_q$ of type $(1, n-1)$ as matching codes for every $n \geqslant 3$. On the other hand, in [2], the authors present a construction of an optimum distance orbit full flag code on $\mathbb{F}_{q^{2k}}$ arising from

the action of a subgroup of $\mathrm{GL}(2k, q)$ that is a cyclic group generated by the companion matrix of a primitive polynomial of degree $2k$ in $\mathbb{F}_q[x]$. Observe that this action can be naturally translated into our scenario by identifying such a companion matrix with a primitive element of $\mathbb{F}_{q^{2k}}$, as it was pointed out in [23, Lemma 21].

5 Conclusions and future work

We have introduced the concept of cyclic orbit flag code as a generalization of cyclic orbit (subspace) code to the flag codes setting. Following the viewpoint of [10], we analyze the structure and properties of this family of codes by defining the best friend of a flag. This approach allows us to easily compute the cardinality of the code and to provide bounds for its distance.

In particular, we explore families of codes attaining the extreme possible values for the distance. For the minimum one, we introduce the family of Galois cyclic flag codes, whose elements present a rich structure of nested spreads compatible with the action of $\mathbb{F}_{q^n}^*$ on flags. We also study the subcodes of Galois cyclic flag codes whose structure is also orbital cyclic, the Galois β-cyclic flag codes, and show that we can improve the distance of such codes by choosing a suitable β to attain even the maximum possible one. On the other hand, concerning optimum distance flag codes with a fixed best friend, we have provided a necessary condition on the type vector of orbit flag codes that attain the maximum possible distance and arise also from the action of subgroups of $\mathbb{F}_{q^n}^*$.

In future work we want to come up with other constructions of β-cyclic orbit flag codes as well as to study conditions and properties of cyclic obit codes with a prescribed distance not necessarily being the maximum one. Despite the study of union of cyclic and β-cyclic orbit flag codes has not been addressed in this paper, it would be also interesting to tackle this problem. In addition, we would like to exploit the structure of cyclic orbit flag codes in order to determine efficient decoding algorithms taking advantage of the ones already designed for cyclic orbit (subspace) codes in [23].

References

[1] R. Ahlswede, N. Cai, R. Li and R. W. Yeung, *Network Informatin Flow*, IEEE Transactions on Information Theory, Vol. 46 (2000), 1204-1216.

[2] C. Alonso-González, M. A. Navarro-Pérez and X. Soler-Escrivà, *An orbital construction of Optimum Distance Flag Codes* https://arxiv.org/abs/2011.02724 (preprint).

[3] C. Alonso-González, M. A. Navarro-Pérez and X. Soler-Escrivà, *Flag Codes from Planar Spreads in Network Coding*, Finite Fields and Their Applications, Vol. 68 (2020), 101745.

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

[5] E. Ben-Sasson, T. Etzion, A. Gabizon, and N. Raviv, *Subspace Polynomials and Cyclic Subspace Codes*, IEEE Transactions on Information Theory, Vol. 62 (2016), 1157–1165.

[6] B. Chen and H. Liu, *Constructions of cyclic constant dimension codes*, Designs, Codes and Cryptography, Vol. 86(6), (2018), 1267–1279.

[7] K. Drudge. *On the Orbits of Singer Groups and Their Subgroups*, The Electronic Journal of Combinatorics, Vol. 9 (2002), #R15.

[8] T. Etzion and A. Vardy, *Error-correcting codes in projective space*, IEEE Transactions on Information Theory, Vol. 57 (2011), 1165–1173.

[9] H. Gluesing-Luerssen and H. Lehman, *Distance Distributions of Cyclic Orbit Codes*, Designs, Codes and Cryptography, (2021), https://doi.org/10.1007/s10623-020-00823-x.

[10] H. Gluesing-Luerssen, K. Morrison and C. Troha, *Cyclic Orbit Codes and Stabilizer Subfields*, Advances in Mathematics of Communications, 9 (2015), 2, 177-197.

[11] E. Gorla, F. Manganiello and J. Rosenthal, *An Algebraic Approach for Decoding Spread Codes*, Advances in Mathematics of Communications, 6 (2012), 4, 443-466.

[12] 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 Transactions on Information Theory, Vol. 52 (2006), 4413-4430.

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

[14] S. Kurz, *Bounds for Flag Codes*, https://arxiv.org/abs/2005.04768 (preprint).

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

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

[17] F. Manganiello and A.-L. Trautmann, *Spread Decoding in Extension Fields*, Finite Fields and Their Applications, Vol. 25 (2014), 94-105.

[18] F. Manganiello, A.-L. Trautmann and J. Rosenthal, *On Conjugacy Classes of Subgroups of the General Linear Group and Cyclic Orbit Codes*; in: Proceedings of the 2011 IEEE International Symposium on Information Theory (ISIT), Saint Pettersburg, 2011, pp. 1916–1920.

[19] K. Otal and F. Özbudak, *Cyclic Subspace Codes via Subspace Polynomials*, Designs, Codes and Cryptography, Vol. 85(2), 2017, 191-204.

[20] J. Rosenthal and A.-L. Trautmann, *A Complete Characterization of Irreducible Cyclic Orbit Codes and their Plücker Embedding*, Designs, Codes and Cryptography, Vol. 66 (2013), 275–289.

[21] R. M. Roth, N. Raviv and I. Tamo, *Construction of Sidon Spaces With Applications to Coding*, IEEE Transactions on Information Theory, Vol. 64, no. 6, pp. 4412-4422, 2018.

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

[23] A.-L. Trautmann, F. Manganiello, M. Braun and J. Rosenthal, *Cyclic Orbit Codes*, IEEE Transactions on Information Theory, Vol. 59, no. 11, pp. 7386-7404, 2013.

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

[25] 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.

[26] W. Zhao and X. Tang. *A Characterization of Cyclic Subspace Codes via Subspace Polynomials*, Finite Fields and Their Applications, Vol. 57 (2019), 1–12.