Article

On Generalized Galois Cyclic Orbit Flag Codes

Clementa Alonso-González [ID] and Miguel Ángel Navarro-Pérez *[ID]

Departement de Matemàtiques, Universitat d'Alacant, Ap. Correus 99, E-03080 Alacant, Spain; clementa.alonso@ua.es

Abstract: Flag codes that are orbits of a cyclic subgroup of the general linear group acting on flags of a vector space over a finite field, are called *cyclic orbit flag codes*. In this paper, we present a new contribution to the study of such codes, by focusing this time on the generating flag. More precisely, we examine those ones whose generating flag has at least one subfield among its subspaces. In this situation, two important families arise: the already known *Galois flag codes*, in case we have just fields, or the *generalized Galois flag codes* in other case. We investigate the parameters and properties of the latter ones and explore the relationship with their underlying Galois flag code.

Keywords: network coding; flag codes; cyclic orbit flag codes; Galois flags

1. Introduction

Network coding represents a procedure to data transfer within a network that is a directed multigraph without cycles, where the information travels from one or several senders to several receivers. In [1], it was proved that the efficiency of the network increases if the intermediate nodes are allowed to perform linear combinations of the received information vectors. We speak about *random network coding* whenever the underlying network topology is unknown. Due to the fact that vector subspaces are invariant under linear combinations, they are proposed as suitable codewords in [2], giving raise to the concept of *subspace codes*. When all the subspaces have a fixed dimension, we get *constant dimension codes* (see [3] and references inside).

In [4], the authors build subspace codes as orbits under the action of subgroups of the general linear group $GL(n, q)$ on the set of subspaces of $\mathbb{F}_q^n$, i.e., *orbit codes*. In particular, when the acting group is cyclic, we obtain the so-called *cyclic orbit codes*, widely studied in the last times (see [4–12], for instance). In particular, the paper [9] is of special interest for our purposes. There the authors treat *β-cyclic orbit codes* as collections of $\mathbb{F}_q$-vector subspaces of $\mathbb{F}_{q^n}$ that are orbits under the natural action of a subgroup $\langle \beta \rangle$ of $\mathbb{F}_{q^n}^*$ on $\mathbb{F}_q$-vector spaces (if β is primitive, the corresponding orbit is called just *cyclic orbit code*). In that paper, an interesting tool is introduced to analyze *β*-cyclic orbit codes: the *best friend* of the code, that is, the largest subfield of $\mathbb{F}_{q^n}$ over which the *generating subspace* is a vector space.

In the context of constant dimension codes, each codeword, i.e., a subspace, is sent in a single use of the channel. In [13], the authors introduce *multishot (subspace) codes* as a generalization of subspace codes. In this setting, a codeword is a sequence of subspaces of $\mathbb{F}_q^n$ of length $r \geqslant 1$ and requires r channel uses to be sent. As a particular case of multishot codes, we have the family of *flag codes*. The codewords in a flag code are flags, that is, sequences of nested subspaces of prescribed dimensions. In the network coding context, they appeared for the first time in the paper [14]. In that work, the authors proposed an adequate channel for flag codes. Moreover, they use the multiplicative action of $GL(n, q)$ on flags to provide different constructions of *orbit flag codes*. This seminal work has led to other recent related papers (see [15–22], for instance).

In [16], inspired by the ideas in [9], a study of *β-cyclic orbit flag codes* is undertaken. More precisely, the authors consider flags on $\mathbb{F}_{q^n}$ given by nested $\mathbb{F}_q$-subspaces of the field $\mathbb{F}_{q^n}$ constructed as orbits of subgroups $\langle \beta \rangle \subseteq \mathbb{F}_{q^n}^*$, and coin the concept of *best friend* of a

cyclic flag code as the largest subfield of $\mathbb{F}_{q^n}$ over which every subspace in the *generating flag* is a vector space. The knowledge of the best friend turns out to be extremely useful to determine the parameters of the code as well as other features, such as the necessary conditions on the type vector to reach the maximum distance. As a particular case, they present the family of *Galois flag codes*, those β-cyclic orbit flag codes generated by sequences of nested subfields of $\mathbb{F}_{q^n}$. For that class of codes it is possible to precisely establish a nice correspondence between the set of attainable distances and the subgroups of $\mathbb{F}_{q^n}^*$. Out of this family, the problem of giving constructions of cyclic orbit flag codes with a prescribed minimum distance is widely open. In fact, the authors also point out that the difficulty of that problem lies on the compatible choice of suitable generating flags and acting subgroups.

The current paper is a new contribution in this line, where we extend the study performed in [16] by focusing on the generating flag. More precisely, we examine β-cyclic orbit flag codes whose generating flag has at least one subfield among its subspaces. We distinguish two situations: either all the subspaces are fields, then we have the already known *Galois flag codes*, or there is also at least one subspace not being a field. The last case entails the definition of a new kind of β-cyclic orbit flag codes called *generalized Galois flag codes*. The subsequence of subfields in a generalized Galois flag determines its *underlying Galois flag*. Here we study to what extent this underlying tower of subfields drives the properties and parameters of generalized Galois flag codes. Moreover, we provide precise constructions of these codes with a given underlying Galois flag and discuss in which cases the maximum possible distance can be attained.

The text is structured as follows. In Section 2, we remember the basics on subspace codes as well as some notions and results related to cyclic orbit (subspace) codes developed in [9]. In Section 3, we recall, on the one hand, some background on flag codes and the most important facts on cyclic orbit flag codes that appear in [16]. On the other hand, we present some new results on the interplay of type vectors, best friend and the flag distance parameter. The family of generalized β-Galois flag codes is introduced here as an extension of the β-Galois flag codes. We discuss in which way the properties of a generalized Galois flag code are conducted by its underlying Galois flag code. Section 4 is devoted to provide a systematic construction of generalized β-Galois flag codes with a prescribed underlying β-Galois flag code by using generating flags written in a particular regular form. In Sections 4.1–4.3 we analyze the particular properties of the previous construction in case β is primitive, and describe a decoding algorithm over the erasure channel taking advantage of such properties. In Section 4.4, we address the case when β is not primitive and present some specific results.

2. Preliminaries

Consider q a prime power and $\mathbb{F}_q$ the finite field with q elements. We denote by $\mathbb{F}_q^n$ the n-dimensional vector space over $\mathbb{F}_q$ for any natural number $n \geqslant 1$ and by $\mathcal{P}_q(n)$ the set of all the subspaces of $\mathbb{F}_q^n$. For every $0 \leqslant k \leqslant n$, the set of k-dimensional subspaces of $\mathbb{F}_q^n$, that is, the *Grassmannian*, will be denoted by $\mathcal{G}_q(k,n)$. The set $\mathcal{P}_q(n)$ can be equipped with a metric called the *subspace distance*: for any pair $\mathcal{U}, \mathcal{V} \in \mathcal{P}_q(n)$, we set

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

In particular, the subspace distance between two subspaces $\mathcal{U}, \mathcal{V} \in \mathcal{G}_q(k,n)$ becomes

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

A *constant dimension code* $\mathcal{C}$ of dimension k and length n is a nonempty subset of $\mathcal{G}_q(k,n)$ whose *minimum subspace distance* is given by

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

If $|\mathcal{C}| = 1$, we put $d_S(\mathcal{C}) = 0$. For further details on this family of codes, consult [3] and the references inside.

It is clear that the minimum distance of a constant dimension code $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ is attained when the intersection of every pair of codewords has the minimum possible dimension. In this case, we have that

$$d_S(\mathcal{C}) \leqslant \begin{cases} 2k & \text{if } 2k \leqslant n, \\ 2(n-k) & \text{if } 2k > n. \end{cases} \tag{3}$$

A constant dimension code with dimension $k \leqslant \lfloor \frac{n}{2} \rfloor$ attaining the previous bound is called *partial spread code*. A partial spread code being also a partition of $\mathbb{F}_q^n$ into k-dimensional subspaces is known as a *spread code* or just a *k-spread*. In [23], it is proved that k-spread exists if, and only if, k divides n. As a result, the size of any k-spread is exactly $\frac{q^n-1}{q^k-1}$. See [3,24–26] for more information concerning spread codes in the network coding setting.

Among all the special families of constant dimension codes, here we are interested in *orbit codes*, that is, those that arise as orbits of the action of subgroups of the general linear group $\mathrm{GL}(n, q)$ on the Grassmannian. This family of codes was introduced in [4]. More precisely, fixed a k-dimensional subspace $\mathcal{U} \subset \mathbb{F}_q^n$ and a subgroup $G \subseteq \mathrm{GL}(n, q)$, 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 $\mathrm{Stab}_G(\mathcal{U}) = \{A \in G \mid \mathcal{U} \cdot A = \mathcal{U}\}$. As a consequence,

$$|\mathrm{Orb}_G(\mathcal{U})| = \frac{|G|}{|\mathrm{Stab}_G(\mathcal{U})|} \tag{4}$$

and the minimum distance can be computed as

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

Whenever the acting group G is cyclic, the orbit $\mathrm{Orb}_G(\mathcal{U})$ is called *cyclic orbit code*. The works [9,12,27,28] are devoted to the study of this family of codes. In the current paper we are specially interested in the viewpoint developed in [9,12] where, taking advantage of the natural $\mathbb{F}_q$-linear isomorphism between $\mathbb{F}_q^n$ and $\mathbb{F}_{q^n}$, cyclic orbit codes are seen as collections of subspaces in $\mathbb{F}_{q^n}$. More precisely, in [9] the authors consider a nonzero element β and define *β-cyclic orbit codes* as orbits of the group $\langle \beta \rangle$ on $\mathbb{F}_q$-vector subspaces of $\mathbb{F}_{q^n}$. In particular, 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 following set of $\mathbb{F}_q$-subspaces of dimension k

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

where $|\beta|$ denotes the *multiplicative order* of β. The *stabilizer* of the subspace $\mathcal{U}$ under the action of $\langle \beta \rangle$ is the cyclic subgroup $\mathrm{Stab}_\beta(\mathcal{U}) = \{\beta^i \mid \mathcal{U}\beta^i = \mathcal{U}\}$. An important example of such kind of codes, already developed in [12], is the following k-spread code, where k is a divisor of n and α is a primitive element of $\mathbb{F}_{q^n}$:

$$\mathrm{Orb}_{\langle \alpha \rangle}(\mathbb{F}_{q^k}) = \{\mathbb{F}_{q^k}\alpha^i \mid i = 0, \dots, q^n - 2\}. \tag{5}$$

Remark 1. *Following the notation used in [9], when the acting group is $\mathbb{F}_{q^n}^*$, we simply denote the corresponding orbit by $\mathrm{Orb}(\mathcal{U})$ and call it just the cyclic orbit code generated by $\mathcal{U}$. In this situation, we also remove the subscript β and write $\mathrm{Stab}(\mathcal{U})$ to denote the stabilizer of $\mathcal{U}$.*

Concerning the cardinality and distance of a β-cyclic orbit code, in [9] the authors study these parameters with the aid of the *best friend* of the generating subspace. This concept is closely linked to the stabilizer of the subspace. Let us recall the definition.

Definition 1. *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. The largest friend of $\mathcal{U}$ is called its best friend.*

The knowledge of the best friend of a subspace $\mathcal{U}$ provides straightforwardly the cardinality of the cyclic orbit code as well as a lower bound for its distance.

Proposition 1 ([9], Propositions 3.3, 3.12, 3.13 and 4.1). *Let $\mathcal{U}$ be a subspace of $\mathbb{F}_{q^n}$ with the subfield $\mathbb{F}_{q^m}$ as its best friend. 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 $d_S(\mathrm{Orb}(\mathcal{U})) \geqslant 2m$.

We finish this section recalling a construction of cyclic orbit codes with prescribed distance and cardinality from the choice of a subspace $\mathcal{U}$ written in a specific regular form.

Proposition 2 ([9], Proposition 4.3). *Consider the subspace $\mathcal{U} = \bigoplus_{i=0}^{t-1} \mathbb{F}_{q^m} \alpha^{li}$ for some $1 \leqslant l < \frac{q^n-1}{q^m-1}$ such that $\mathbb{F}_{q^m}$ is the best friend of $\mathcal{U}$. Then $d_S(\mathrm{Orb}(\mathcal{U})) = 2m$.*

It is clear that the subfield $\mathbb{F}_{q^m}$ is a friend of a subspace $\mathcal{U}$ written as in previous proposition, although it is not necessarily its best friend. In fact, there are just two possibilities for the best friend of $\mathcal{U}$.

Proposition 3 ([9], Proposition 4.4). *Given the subspace $\mathcal{U} = \bigoplus_{i=0}^{t-1} \mathbb{F}_{q^m} \alpha^{li}$ for some $1 \leqslant l < \frac{q^n-1}{q^m-1}$. If $f(x)$ is the minimal polynomial of α^l over $\mathbb{F}_{q^m}$, then its degree is at least t and*

$$\mathcal{U} = \mathbb{F}_{q^{mt}} \iff \deg(f) = t \iff \alpha^l \in \mathrm{Stab}(\mathcal{U}) \iff \mathbb{F}_{q^m} \text{ is not the best friend of } \mathcal{U}.$$

We will come back to this family of subspaces and to the β-cyclic orbit codes generated by them in Section 4, where we provide a specific construction of generalized Galois cyclic orbit flag codes by using subspaces written as in Proposition 2.

3. Cyclic Orbit Flag Codes

Part of this section is dedicated to gather the basic background on flag codes that already appears in [14,19,22], and to recall the main definitions and results that pertain to the particular class of cyclic orbit flag codes introduced in [16]. In Section 3.3, we present new results concerning the interdependence between the minimum distance of a β-cyclic orbit flag code, its best friend and the set of dimensions appearing in the type vector. In addition, the class of generalized Galois flag codes is introduced in Section 3.4.2.

3.1. Flags and Flag Codes

A *flag* $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ on the extension field $\mathbb{F}_{q^n}$ is a sequence of nested $\mathbb{F}_q$-vector subspaces

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

The subspace $\mathcal{F}_i$ is called the *i-th subspace* of $\mathcal{F}$ and the *type* of $\mathcal{F}$ is the vector $(\dim(\mathcal{F}_1), \ldots, \dim(\mathcal{F}_r))$. When the type vector is $(1, 2, \ldots, n-1)$, we say that $\mathcal{F}$ is a *full flag*. Given two different flags $\mathcal{F}, \mathcal{F}'$ on $\mathbb{F}_{q^n}$, we say that $\mathcal{F}'$ is a *subflag* of $\mathcal{F}$ if each subspace of $\mathcal{F}'$ is a also subspace of $\mathcal{F}$.

The *flag variety* of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_{q^n}$ is the set of flags of this type and will be denoted by $\mathcal{F}_q((t_1, \ldots, t_r), n)$. Note that $\mathcal{F}_q((t_1, \ldots, t_r), n)$ embeds in the product of Grassmannians $\mathcal{G}_q(t_1, n) \times \cdots \times \mathcal{G}_q(t_r, n)$ and, hence, this variety can be endowed with a

metric that extends 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 2. *A flag code $\mathcal{C}$ of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_{q^n}$ is a nonempty subset of $\mathcal{F}_q((t_1, \ldots, t_r), n)$. The minimum distance of $\mathcal{C}$ is given by*

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

whenever $\mathcal{C}$ has more that two elements. In case $|\mathcal{C}| = 1$, we put $d_f(\mathcal{C}) = 0$. For type $(t_1, \ldots, t_r)$, it always holds

$$d_f(\mathcal{C}) \leqslant 2 \left(\sum_{t_i \leqslant \lfloor \frac{n}{2} \rfloor} t_i + \sum_{t_i > \lfloor \frac{n}{2} \rfloor} (n - t_i) \right). \tag{6}$$

There are constant dimension codes intrinsically correlated with a flag code $\mathcal{C}$ that play an important role in the study of parameters and properties of $\mathcal{C}$.

Definition 3. *Given a flag code $\mathcal{C}$ of type $(t_1, \ldots, t_r)$, the i-projected code of $\mathcal{C}$ is the set*

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

Remark 2. *Concerning the relationship between the size of a flag code and the ones of its projected codes, 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. Under this condition, it is possible to establish also a clear connection between the minimum distance of a given flag code and the ones of its projected codes. More precisely, if $\mathcal{C}$ is a disjoint flag code, then*

$$d_f(\mathcal{C}) \geqslant \sum_{i=1}^{r} d_S(\mathcal{C}_i).$$

In [15], the authors introduced a family of flag codes such that the distance and size of the projected codes completely determine the ones of the corresponding flag code.

Definition 4. *A flag code $\mathcal{C}$ is consistent if the following conditions hold:*

(1) $\mathcal{C}$ is disjoint.

(2) $d_f(\mathcal{C}) = \sum_{i=1}^{r} d_S(\mathcal{C}_i)$.

In the same paper, the authors develop a decoding algorithm for consistent flag codes over the erasure channel and provide important families of such a class of codes. Among them, we can find the one of *optimum distance flag codes*. This class of flag codes has been already studied in [17,19,21,22]. In these works, the reader can find specific constructions of them as well as the following characterization.

Theorem 1 ([19], Theorem 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.*

We will come back to this ideas in Section 4.3 in order to adapt the consistent flag codes decoding algorithm designed in [15] to the constructions proposed in the present paper.

3.2. Cyclic Orbit Flag Codes

Let us recall the concept of *cyclic orbit flag code* as the orbit of the multiplicative action of (cyclic) subgroups of $\mathbb{F}_{q^n}^*$ on flags on $\mathbb{F}_{q^n}$. This concept of cyclic orbit flag code was first introduced in [16] following the approach of [9] for cyclic orbit subspace codes.

The cyclic group $\mathbb{F}_{q^n}^*$ acts on flags on $\mathbb{F}_{q^n}$ as follows: given $\beta \in \mathbb{F}_{q^n}^*$ and a flag $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ of type $(t_1, \ldots, t_r)$, the flag $\mathcal{F}\beta$ is

$$\mathcal{F}\beta = (\mathcal{F}_1\beta, \ldots, \mathcal{F}_r\beta) \tag{7}$$

and the orbit

$$\mathrm{Orb}_\beta(\mathcal{F}) = \{\mathcal{F}\beta^j \mid 0 \leqslant j \leqslant |\beta| - 1\} \tag{8}$$

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

$$\mathrm{Stab}_\beta(\mathcal{F}) = \{\beta^j \mid \mathcal{F}\beta^j = \mathcal{F}\}. \tag{9}$$

If β is primitive, that is, if the acting group is $\mathbb{F}_{q^n}^*$, we 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, for every $\beta \in \mathbb{F}_{q^n}^*$, it holds $\mathrm{Stab}_\beta(\mathcal{F}) = \langle \beta \rangle \cap \mathrm{Stab}(\mathcal{F})$.

We can take advantage of the orbital structure to compute the code parameters: the cardinality of $\mathrm{Orb}_\beta(\mathcal{F})$ is given by

$$|\mathrm{Orb}_\beta(\mathcal{F})| = \frac{|\beta|}{|\mathrm{Stab}_\beta(\mathcal{F})|} = \frac{|\beta|}{|\langle \beta \rangle \cap \mathrm{Stab}(\mathcal{F})|} \tag{10}$$

and its minimum distance can be calculated as

$$d_f(\mathrm{Orb}_\beta(\mathcal{F})) = \min\{d_f(\mathcal{F}, \mathcal{F}\beta^j) \mid \beta^j \notin \mathrm{Stab}_\beta(\mathcal{F})\}. \tag{11}$$

Remark 3. *Concerning the projected codes associated with $\mathrm{Orb}_\beta(\mathcal{F})$, there are important facts to point out. First of all, note that the projected codes of a β-cyclic orbit flag codes are also β-cyclic orbit (subspace) codes. More precisely, for every $1 \leqslant i \leqslant r$, we have*

$$(\mathrm{Orb}_\beta(\mathcal{F}))_i = \mathrm{Orb}_\beta(\mathcal{F}_i). \tag{12}$$

Moreover, the straightforward stabilizers relationship

$$\mathrm{Stab}_\beta(\mathcal{F}) = \bigcap_{i=1}^r \mathrm{Stab}_\beta(\mathcal{F}_i) \tag{13}$$

leads to a nice rapport between cardinalities: for every $1 \leqslant i \leqslant r$, we have that $|\mathrm{Orb}_\beta(\mathcal{F}_i)|$ divides $|\mathrm{Orb}_\beta(\mathcal{F})|$ ([16], Proposition 3.6).

Coming back to the computation of the values $|\mathrm{Orb}_\beta(\mathcal{F})|$ and $d_f(\mathrm{Orb}_\beta(\mathcal{F}))$, in [16], it is shown that the knowledge of a specific subfield associated with $\mathcal{F}$ allows us to obtain them directly. Let us recall the concept of best friend of a flag introduced in [16] by generalization of the concept of a subspace best friend given in [9].

Definition 5. *A subfield $\mathbb{F}_{q^m}$ of $\mathbb{F}_{q^n}$ is said to be a friend of a flag $\mathcal{F}$ on $\mathbb{F}_{q^n}$ if all the subspaces of $\mathcal{F}$ are $\mathbb{F}_{q^m}$-vector spaces, that is, if it is a friend of all of them. The best friend of the flag $\mathcal{F}$ is its biggest friend.*

From this definition it clearly holds that the type vector of a flag has to satisfy a necessary condition whenever the best friend is fixed. Furthermore, as it occurs when we work with the stabilizer subgroup, there are important connections between the best friend of a flag and the ones of its subspaces.

Proposition 4 ([16], Lemma 3.14, Proposition 3.16, Corollary 3.18). *Let $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ be a flag of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_{q^n}$. If $\mathbb{F}_{q^m}$ is a friend of $\mathcal{F}$, then m divides $\gcd(t_1, \ldots, t_r, n)$. Moreover, if $\mathbb{F}_{q^m}$ is the best friend of $\mathcal{F}$, then it is the intersection of the ones of $\mathcal{F}_i$, for every $i = 1, \ldots, r$, and we also have that $\mathbb{F}_{q^m} = \mathrm{Stab}(\mathcal{F}) \cup \{0\}$.*

Remark 4. *Note that, if $1 \in \mathcal{F}_1$, then every friend of the flag $\mathcal{F}$ is contained in $\mathcal{F}_1$. Moreover, all the flags in $\mathrm{Orb}_\beta(\mathcal{F})$ have the same best friend, allowing us to speak about the best friend of a β-cyclic orbit flag code. Now, if $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ is a flag of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_{q^n}$ with $\mathbb{F}_{q^m}$ as its best friend, $\mathbb{F}_{q^m}$ must be a friend of all its subspaces and we can write $t_i = ms_i$ for $i = 1, \ldots, r$, where $1 \leqslant s_1 < \cdots < s_r < s = \frac{n}{m}$. Finally, we can 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*

$$\mathcal{F}_i = \bigoplus_{j=1}^{s_i} \mathbb{F}_{q^m} a_j. \tag{14}$$

In case 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 (5). Moreover, if $1 \in \mathcal{F}_1$, this subspace is exactly the subfield $\mathbb{F}_{q^m}$.

Let us recall how the knowledge of the best friend of a β-cyclic orbit flag code provides relevant information about the code parameters.

Proposition 5 ([16]). *Let $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ be a flag on $\mathbb{F}_{q^n}$ and assume that $\mathbb{F}_{q^m}$ is its best friend. Then*

$$|\mathrm{Orb}_\beta(\mathcal{F})| = \frac{|\beta|}{|\langle \beta \rangle \cap \mathbb{F}_{q^m}^*|}. \tag{15}$$

Moreover, the value 2m divides $d_f(\mathrm{Orb}_\beta(\mathcal{F}))$ and, if the the type vector of $\mathcal{F}$ is $(ms_1, \ldots, ms_r)$, then it holds

$$2m \leqslant d_f(\mathrm{Orb}(\mathcal{F})) \leqslant 2m \left(\sum_{s_i \leqslant \lfloor \frac{s}{2} \rfloor} s_i + \sum_{s_i > \lfloor \frac{s}{2} \rfloor} (s - s_i) \right), \tag{16}$$

whenever $\beta \notin \mathbb{F}_{q^m}^*$. On the other hand, if $\beta \in \mathbb{F}_{q^m}^*$, then $d_f(\mathrm{Orb}_\beta(\mathcal{F})) = 0$.

Remark 5. *From (15) and (16), it is clear that both size and cardinality depend on the generating flag (hence on its best friend), the acting subgroup and the type vector. In particular, once we have fixed the best friend $\mathbb{F}_{q^m}$, we obtain the maximum possible orbit size if β is a primitive element of $\mathbb{F}_{q^n}$. In this case, it holds $|\mathrm{Orb}(\mathcal{F})| = \frac{q^n - 1}{q^m - 1}$. However, if we take $\beta \in \mathbb{F}_{q^m}^*$, we obtain the minimum possible cardinality since $\mathrm{Orb}_\beta(\mathcal{F}) = \{\mathcal{F}\}$.*

3.3. Flag Distances, Best Friend and Type Vectors Interplay

From the bounds provided in (16) we know that, fixed the subfield $\mathbb{F}_{q^m}$ as best friend of a flag code $\mathcal{C}$ of type $(ms_1, \ldots, ms_r)$, the possible values for the distance between flags in $\mathcal{C}$ are multiples of $2m$ in the interval

$$\left[2m, 2m \left(\sum_{s_i \leqslant \lfloor \frac{s}{2} \rfloor} s_i + \sum_{s_i > \lfloor \frac{s}{2} \rfloor} (s - s_i) \right) \right]. \tag{17}$$

Nevertheless, in the orbital flag codes setting it is very important to point out that not every possible flag distance value is compatible with every type vector. In general, the greater the flag distance, the more conditions over the corresponding type vector we will have to impose. The simplest case comes from considering cyclic flag codes of length one. In ([9], Lemma 4.1), it was already shown that a cyclic (subspace) code with best friend $\mathbb{F}_{q^m}$ has, at least, distance $2m$ and constructions attaining this extreme value of the distance

were also provided in ([9], Proposition 4.3). However, when we work with flags of length $r \geqslant 2$, not even the minimum value of the distance, which is $2m$ as well, can be obtained for every type vector. This is a consequence of the link between the flag distance and the number of subspaces in a flag $\mathcal{F}$ having the same best friend than $\mathcal{F}$. Let us explain this relationship in the following result.

Theorem 2. *Let $\mathcal{F}$ be a flag on $\mathbb{F}_{q^n}$ with the subfield $\mathbb{F}_{q^m}$ as its best friend and take $\beta \in \mathbb{F}_{q^n}^* \setminus \mathbb{F}_{q^m}^*$.*

(1) If there are $1 \leqslant j \leqslant r$ subspaces of $\mathcal{F}$ with $\mathbb{F}_{q^m}$ as their best friend, then $d_f(\mathrm{Orb}_\beta(\mathcal{F})) \geqslant 2mj$.

(2) If $d_f(\mathrm{Orb}_\beta(\mathcal{F})) = 2m$, then $\mathbb{F}_{q^m}$ is the best friend of exactly one subspace of $\mathcal{F}$.

Proof. Let us prove (1). Assume that there exist j subspaces, say $\mathcal{F}_{i_1}, \dots, \mathcal{F}_{i_j}$, of $\mathcal{F}$ having $\mathbb{F}_{q^m}$ as their best friend. Then it suffices to see that, if $\beta^l \notin \mathrm{Stab}_\beta(\mathcal{F}) = \langle \beta \rangle \cap \mathbb{F}_{q^m}^*$, then β^l does not stabilize the subspaces $\mathcal{F}_{i_1}, \dots, \mathcal{F}_{i_j}$. Consequently, we have

$$d_f(\mathcal{F}, \mathcal{F}\beta^l) \geqslant \sum_{k=1}^{j} d_S(\mathcal{F}_{i_k}, \mathcal{F}_{i_k}\beta^l) \geqslant 2mj.$$

To prove (2), let us start assuming that there are at least two different subspaces $\mathcal{F}_i$ and $\mathcal{F}_j$ in $\mathcal{F}$ with $\mathbb{F}_{q^m}$ as their best friend. By (1) we have that $d_f(\mathrm{Orb}_\beta(\mathcal{F})) \geqslant 4m > 2m$. On the other hand, suppose that no subspace in $\mathcal{F}$ has $\mathbb{F}_{q^m}$ as its best friend. In this case, for every $1 \leqslant i \leqslant r$, we put $\mathbb{F}_{q^{m_i}}$ the best friend of $\mathcal{F}_i$ and, since $\mathbb{F}_{q^m} = \bigcap_{i=1}^{r} \mathbb{F}_{q^{m_i}}$, we have that m is a proper divisor of every m_i. In particular, $m < m_i$, for every $1 \leqslant i \leqslant r$. Now, for every $\beta^l \notin \mathrm{Stab}_\beta(\mathcal{F})$, we have at least one index $1 \leqslant i \leqslant r$ such that $\beta^l \notin \mathrm{Stab}_\beta(\mathcal{F}_i)$. Hence,

$$d_f(\mathcal{F}, \mathcal{F}\beta^l) \geqslant d_S(\mathcal{F}_i, \mathcal{F}_i\beta^l) \geqslant 2m_i > 2m.$$

Thus, $d_f(\mathcal{C}) > 2m$. □

Remark 6. *Note that the converses of statements (2) and (1) in the previous result are not necessarily true. Take, for instance, $\mathcal{F} = (\mathbb{F}_{q^2}, \mathbb{F}_{q^4}, \mathbb{F}_{q^8})$ on $\mathbb{F}_{q^{16}}$, which has best friend $\mathbb{F}_{q^2}$. Let us consider $\beta = \alpha^5$ where $\langle \alpha \rangle = \mathbb{F}_{q^{16}}^*$. Then we have just one subspace of $\mathcal{F}$ with best friend $\mathbb{F}_{q^2}$ whereas $d_f(\mathrm{Orb}_\beta(\mathcal{F})) = 12 = 2 \cdot 3 \cdot 2 \geqslant 4$. At the same time there are not three subspaces in $\mathcal{F}$ sharing its best friend.*

The previous theorem allows us to discard some type vectors if we work with the minimum value of the distance when the best friend is $\mathbb{F}_{q^m}$.

Corollary 1. *Let $\mathcal{F}$ be a flag of type $(ms_1, \dots, ms_r)$ on $\mathbb{F}_{q^n}$ with best friend $\mathbb{F}_{q^m}$ and take $\beta \in \mathbb{F}_{q^n}^* \setminus \mathbb{F}_{q^m}^*$. If $d_f(\mathrm{Orb}_\beta(\mathcal{F})) = 2m$, then $\gcd(s_j, \frac{n}{m}) \neq 1$ for, at least $r - 1$ indices $1 \leqslant j \leqslant r$.*

Proof. By means of Theorem 2, we know that there is exactly one subspace of $\mathcal{F}$ having best friend $\mathbb{F}_{q^m}$, say $\mathcal{F}_i$. Now, for each $j \neq i$, we put $\mathbb{F}_{q^{m_j}}$ the best friend of $\mathcal{F}_j$. In particular, we know that m is a proper divisor of every m_j. Let us write $m_j = ma_j$, with $a_j > 1$ for every $j \neq i$. In addition, $m_j = ma_j$ divides both $\dim(\mathcal{F}_j) = ms_j$ and n. Hence, $1 < a_j$ divides both s_j and $\frac{n}{m}$. We conclude that $\gcd(s_j, \frac{n}{m}) > 1$ for all $1 \leqslant j \leqslant r$, $j \neq i$. □

Example 1. *If $n = 16$ and we fix $\mathbb{F}_{q^2}$ as the best friend of our flags, the minimum distance value 4 cannot be obtained for type $(4, 6, 10)$ since $\gcd(3, 8) = \gcd(5, 8) = 1$. In contrast, this value would be attainable for type $(4, 6, 8)$, for instance. Using the same argument, if we take $n = 14$, and consider a flag $\mathcal{F}$ on $\mathbb{F}_{q^{14}}$ having the subfield $\mathbb{F}_{q^2}$ as its best friend, we can conclude that β-cyclic orbit flag codes generated by $\mathcal{F}$ will never give distance 4, unless $\mathcal{F}$ is the flag of length one $\mathcal{F} = (\mathbb{F}_{q^2})$.*

We have seen that, fixed the best friend $\mathbb{F}_{q^m}$, the minimum value of the distance $2m$ can only be obtained by codes $\mathrm{Orb}_\beta(\mathcal{F})$ in which $\mathcal{F}$ has exactly one subspace with $\mathbb{F}_{q^m}$ as its best friend as well. On the other end, as said in Theorem 1, a flag code $\mathcal{C}$ attains the maximum possible distance for its type if, and only if, it is disjoint and all its projected codes attain the respective maximum (subspace) distance. Recall that a flag code $\mathcal{C}$ of length r on $\mathbb{F}_{q^n}$ is disjoint if it holds

$$|\mathcal{C}_1| = \cdots = |\mathcal{C}_r| = |\mathcal{C}|. \tag{18}$$

In ([16], Proposition 4.19) the authors prove that for cyclic orbit flag codes (β primitive) this condition is equivalent to say that each subspace of $\mathcal{F}$ has the same best friend (then the best friend of $\mathcal{F}$). Summing up, we can also draw conditions on the type vector in the case of cyclic orbit flag codes having $\mathbb{F}_{q^m}$ as their best friend and the largest possible distance, that is, the upper value of the range in (17).

Proposition 6 ([16], 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, $\frac{q^n-1}{q^m-1}$.*

Using Theorem 2, we obtain the next construction of cyclic orbit flag codes with the best possible distance for the above mentioned cases.

Proposition 7. *Let* $\mathcal{F} = (\mathcal{F}_1, \mathcal{F}_2)$ *a flag of type $(n, n - m)$ on* $\mathbb{F}_{q^n}$. *If* $\mathcal{F}_1$ *and* $\mathcal{F}_2$ *have the subfield* $\mathbb{F}_{q^m}$ *as their best friend, then the cyclic orbit codes* $\mathrm{Orb}(\mathcal{F}_1)$, $\mathrm{Orb}(\mathcal{F}_2)$ *and* $\mathrm{Orb}(\mathcal{F})$ *have the maximum possible distance.*

Proof. The result holds for $\mathrm{Orb}(\mathcal{F}_1) = \mathrm{Orb}(\mathbb{F}_{q^m})$ by means of (5). For $\mathrm{Orb}(\mathcal{F}_2)$, it suffices to see that, if $\mathbb{F}_q^m$ is the best friend of $\mathcal{F}_2$, then $d_S(\mathrm{Orb}(\mathcal{F}_2)) = 2m$, which is the maximum possible distance for dimension $n - m$. Last, by means of Theorem 2, we conclude that $d_f(\mathrm{Orb}(\mathcal{F})) = 4m$, i.e., the maximum possible distance for type $(m, n - m)$. $\square$

Remark 7. *In the case of β-cyclic orbit flag codes with β non primitive, in ([16], Prop. 4.19) it is proved that the code* $\mathrm{Orb}_\beta(\mathcal{F})$ *is disjoint if, and only if,*

$$\langle\beta\rangle \cap \mathbb{F}_{q^m}^* = \langle\beta\rangle \cap \mathbb{F}_{q^{m_1}}^* = \cdots = \langle\beta\rangle \cap \mathbb{F}_{q^{m_r}}^*. \tag{19}$$

Note that to have (19) it is not necessary that all the subspaces of $\mathcal{F}$ share the same best friend, contrary to what happens if β primitive (see part (2) on Example 2). Moreover, in ([16], Theorem 4.21) the authors give also conditions on the type vector of $\mathcal{F}$ of an optimum distance β-cyclic flag code with fixed best friend if β is not primitive. In Table 1 present some examples extracted from ([16], Table 3) where they determine the set of allowed dimensions in the type vector, depending on the size of the acting subgroup $\langle\beta\rangle$ of $\mathbb{F}_{2^{12}}^* = \langle\alpha\rangle$, when the best friend is $\mathbb{F}_{2^2}$.

Table 1. Admissible dimensions for $q = 2$, $n = 12$, $m = 2$.

β	$|\beta|$	$\langle\beta\rangle \cap \mathbb{F}_{q^m}^*$	$|\mathrm{Orb}_\beta(\mathcal{F})|$	Allowed Dimensions	Max. Distance
α	4095	$\mathbb{F}_{2^2}^*$	1365	2, 10	8
α^5	819	$\mathbb{F}_{2^2}^*$	273	2, 4, 8, 10	24
α^9	455	$\{1\}$	455	2, 10	8
α^{63}	65	$\{1\}$	65	2, 4, 6, 8, 10	36

Concerning the explicit construction of such codes, in [17,21], the authors follow the approach of [12] to build optimum distance flag codes under the action of (subgroups of) Singer groups of the special linear group and the general linear group, respectively, by placing a suitable spread among the projected codes. In our framework, this idea corresponds to the choice a generating flag that has certain subfield among its subspaces. Let us exhibit some concrete examples.

Example 2. *Let us work in $\mathbb{F}_{2^{12}}$ and fix $\mathbb{F}_{q^2}$ as best friend of all our flags.*

(1) *Take $\mathcal{F} = (\mathbb{F}_{2^2}, \mathcal{F}_2, \mathbb{F}_{2^6}, \mathcal{F}_4, \mathcal{F}_5)$ of type $(2,4,6,8,10)$ and consider $\beta = \alpha^{63}$, then the orbit $\mathrm{Orb}_\beta(\mathcal{F})$ is an optimum distance flag code of cardinality 65 (see [17]), which is the maximum possible size for an optimum distance flag code of this type. With the same notation, the orbit $\mathrm{Orb}_\beta((\mathbb{F}_{2^2}, \mathcal{F}_2, \mathcal{F}_4, \mathcal{F}_5))$ is an optimum distance flag code, in this case of type $(2,4,8,10)$, of the same size.*

(2) *On the other hand, following the ideas in [21], if we consider the flag $\mathcal{F}' = (\mathbb{F}_{2^2}, \mathbb{F}_{2^4}, \mathcal{F}'_3, \mathcal{F}'_4)$ of type $(2,4,8,10)$ such that $\mathbb{F}_{2^4}$ is the best friend of $\mathcal{F}'_3$, and take $\beta = \alpha^5$, then the orbit $\mathrm{Orb}_\beta(\mathcal{F}')$ is an optimum distance flag code with cardinality 273. Note that in this example the subspaces $\mathcal{F}'_1$ and $\mathcal{F}'_3$ do not share their best friend even thought $\mathrm{Orb}_\beta(\mathcal{F}')$ is disjoint.*

These examples lead us to study β-cyclic orbit codes when we place one or more subfields in the generating flag.

3.4. Generating Flags with Subfields as Their Subspaces

In this subsection we focus on β-cyclic orbit flag codes generated by flags having at least one subfield among their subspaces. We distinguish two situations: either every subspace in the generating flag is a subfield or there is also one subspace that is not a subfield.

3.4.1. Galois Flag Codes

Let us start with β-cyclic orbit flag codes generated by flags having just subfields of $\mathbb{F}_{q^n}$ as subspaces, that is, generated by the so-called *Galois flags*. This particular class of β-cyclic orbit flag codes was introduced in [16]. Let us recall the definition. Consider a sequence of integers $1 \leqslant t_1 < \cdots < t_r < n$ such that all of them are divisors of n and t_i divides t_{i+1}, for $1 \leqslant i \leqslant r-1$.

Definition 6. *The* Galois flag *of type $(t_1, \ldots, t_r)$ on $\mathbb{F}_{q^n}$ is the flag given by the sequence of nested subfields $(\mathbb{F}_{q^{t_1}}, \ldots, \mathbb{F}_{q^{t_r}})$. Given $\beta \in \mathbb{F}_{q^n}^*$, the β-cyclic orbit flag code generated by this Galois flag is called the β-Galois cyclic orbit flag code, or just β-Galois flag code, for short, of type $(t_1, \ldots, t_r)$.*

In the Galois flag $\mathcal{F}$ of type vector $(t_1, \ldots, t_r)$, clearly the i-th subspace has the subfield $\mathbb{F}_{q^{t_i}}$ as best friend. Hence, the first subfield $\mathbb{F}_{q^{t_1}}$ is the best friend of any β-Galois flag code of type $(t_1, \ldots, t_r)$. For β primitive we have the following straightforward result.

Proposition 8 ([16])**.** *Let $\mathcal{C}$ be the Galois flag code of type $(t_1, \ldots, t_r)$, then the cardinality of this flag code is $|\mathcal{C}| = (q^n - 1)/(q^{t_1} - 1)$ and its distance is $d_f(\mathcal{C}) = 2t_1$. Its i-th projected code $\mathcal{C}_i$ has size $|\mathcal{C}_i| = (q^n - 1)/(q^{t_i} - 1)$ and distance $2t_i$.*

Remark 8. *Note that, if we take the Galois flag $\mathcal{F}$ of type $(t_1, \ldots, t_r)$, the distance $d_f(\mathrm{Orb}(\mathcal{F})) = 2t_1$ is the lowest possible one for cyclic orbit flag codes with $\mathbb{F}_{q^{t_1}}$ as best friend, according to (6) (in case $|\mathcal{C}| > 1$). In fact, there is a precise set of attainable distances for the different orbits $\mathrm{Orb}_\beta(\mathcal{F})$ when we consider the action of subgroups $\langle \beta \rangle \subseteq \mathbb{F}_{q^n}^*$. Furthermore, as proved in [16], we can always select β in a controlled manner such that the code $\mathrm{Orb}_\beta(\mathcal{F})$ reaches any distance value in the set of possible distances. This choice is made by checking the relationship between the subgroup $\langle \beta \rangle$ and the subfields $\mathbb{F}_{q^{t_i}}$. Let us recall the precise result.*

Theorem 3 ([16], 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*

$$d_f(\mathrm{Orb}_\beta(\mathcal{F})) \in \{0, 2t_1, 2(t_1 + t_2), \ldots, 2(t_1 + t_2 + \cdots + t_r)\}. \tag{20}$$

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 $\mathrm{Stab}_\beta(\mathcal{F}_1) \subsetneq \mathrm{Stab}_\beta(\mathcal{F}_j)$.*

In view of the previous result, it is worth highlighting that, given a Galois flag $\mathcal{F}$, the range of attainable distances by the codes $\mathrm{Orb}_\beta(\mathcal{F})$ follows a concrete pattern in terms of the dimensions in the type vector (see (20)). On the other hand, we have the possibility to gradually improve the distance of $\mathrm{Orb}(\mathcal{F})$ by selecting the orbit $\mathrm{Orb}_\beta(\mathcal{F})$ for an appropriate β, even if this choice could involve a loss of size. This nice behaviour gives rise to think that Galois codes could constitute an appropriate "skeleton" to support a more general family of β-cyclic orbit flag codes whose properties, in turn, might be driven by them. To explore this idea, in the following section we introduce a new family of codes.

3.4.2. Generalized Galois Flag Codes

Let us take now generating flags having at least one subspace that is a subfield and at least another one that is not. This condition gives length at least two. Note also that, all the fields in a flag $\mathcal{F}$ constitute a Galois subflag.

Definition 7. *We say that a flag $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_k)$ of type $(s_1, \ldots, s_k)$ generalizes the Galois flag of type $(t_1, \ldots, t_r)$ if $\{t_1, \ldots, t_r\} \subsetneq \{s_1, \ldots, s_k\}$ and the following conditions are satisfied:*

(1) *The subflag of $\mathcal{F}$ of type $(t_1, \ldots, t_r)$ is the Galois flag of this type,*

(2) *there is at least one subspace of $\mathcal{F}$ that is not a field.*

Remark 9. *Observe that the second condition in Definition 7 excludes Galois flags from our study of generalized Galois flags. Even more, according to the previous definition, a generalized Galois flag is just a flag having at least one field and one subspace that is not a field among its subspaces. Besides, in the conditions of the previous definition, $\mathcal{F}$ clearly generalizes every subflag of the Galois flag of type $(t_1, \ldots, t_r)$ as well. We pay special attention to the longest Galois subflag of $\mathcal{F}$.*

Definition 8. *Let $\mathcal{F}$ be a generalized Galois flag. Its longest Galois subflag is called its underlying Galois subflag.*

Observe that the underlying Galois subflag of a generalized Galois flag always exists and, due to the nested structure of flags, it is unique.

Definition 9. *Given $\mathcal{F}$ a generalized Galois flag and $\beta \in \mathbb{F}_{q^n}^*$, the β-cyclic orbit flag code generated by $\mathcal{F}$ is called a generalized β-Galois (cyclic orbit) flag code. If $\mathcal{F}'$ is the underlying Galois subflag of $\mathcal{F}$, then we say that $\mathrm{Orb}_\beta(\mathcal{F}')$ is the underlying β-Galois flag code of $\mathrm{Orb}_\beta(\mathcal{F})$.*

Let us see some examples reflecting different situations related to this new class of flag codes.

Example 3. *Take $n = 8$ and primitive elements $\alpha \in \mathbb{F}_{q^8}$, $\gamma \in \mathbb{F}_{q^4}$. The sequences*

$$\mathcal{F} = (\mathbb{F}_{q^2}, \mathbb{F}_{q^4}, \mathbb{F}_{q^4} \oplus \mathbb{F}_q^2 \alpha) \ \text{ and } \ \mathcal{F}' = (\mathbb{F}_{q^2}, \mathbb{F}_{q^2} \oplus \mathbb{F}_q \gamma, \mathbb{F}_{q^4})$$

are generalized flags of type $(2, 4, 6)$ and $(2, 3, 4)$ on $\mathbb{F}_{q^8}$, respectively, with common underlying Galois subflag $(\mathbb{F}_{q^2}, \mathbb{F}_{q^4})$. Now, for any $\beta \in \mathbb{F}_{q^n}^*$, the best friend of the β-Galois flag code $\mathrm{Orb}_\beta((\mathbb{F}_{q^2}, \mathbb{F}_{q^4}))$ is the field $\mathbb{F}_{q^2}$ and this property also holds for the generalized β-Galois flag code $\mathrm{Orb}(\mathcal{F})$. However, the best friend of $\mathrm{Orb}(\mathcal{F}')$ is $\mathbb{F}_q$, which is a field not appearing in $\mathcal{F}'$.

Remark 10. *Given a generalized β-Galois flag code $\mathcal{C}$ of type $(s_1, \ldots, s_k)$ with underlying Galois subflag $(\mathbb{F}_{q^{t_1}}, \ldots, \mathbb{F}_{q^{t_r}})$, if the subfield $\mathbb{F}_{q^m}$ is the best friend of $\mathcal{C}$, then it holds $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^{t_1}}$.*

Concerning the attainable distance values for this class of codes, contrary what happens with Galois flag codes whose set of reachable distances is completely determined by the type, different situations can arise.

Example 4. *Take $n = 4$ and consider a generalized Galois flag $\mathcal{F}$ of type $(1, 2, 3)$ with underlying Galois subflag $(\mathbb{F}_q)$. In this case, the set of attainable values for $d_f(\mathrm{Orb}_\beta(\mathcal{F}))$ is exactly the same as for general flag codes of this type on $\mathbb{F}_{q^4}$, that is, any even integer between 0 and 8. However, for the same choice of the parameters, flags generalizing the Galois flag $(\mathbb{F}_q, \mathbb{F}_{q^2})$,, i.e., those of the form*

$$\mathcal{F}' = (\mathbb{F}_q, \mathbb{F}_{q^2}, \mathcal{F}'_3),$$

for some subspace $\mathcal{F}'_3$ of dimension 3 of $\mathbb{F}_{q^4}$, present a restriction on the set of possible distances. Let us prove that the value $d_f(\mathrm{Orb}_\beta(\mathcal{F}')) = 6$ cannot be obtained for any $\beta \in \mathbb{F}_{q^4}^*$. Observe that the projected code $\mathrm{Orb}_\beta(\mathbb{F}_{q^2})$ is a partial spread of dimension 2 of $\mathbb{F}_{q^4}$. Hence, when computing the distance

$$d_f(\mathcal{F}', \mathcal{F}'\beta^i) = d_S(\mathbb{F}_q, \mathbb{F}_q\beta^i) + d_S(\mathbb{F}_{q^2}, \mathbb{F}_{q^2}\beta^i) + d_S(\mathcal{F}'_3, \mathcal{F}'_3\beta^i),$$

we have that

$$d_S(\mathbb{F}_{q^2}, \mathbb{F}_{q^2}\beta^i) = \begin{cases} 0 & \text{if } \beta \in \mathbb{F}_{q^2}^*, \\ 4 & \text{otherwise.} \end{cases}$$

Moreover, if $d_S(\mathbb{F}_{q^2}, \mathbb{F}_{q^2}\beta^i) = 0$, then it holds $d_f(\mathcal{F}', \mathcal{F}'\beta^i) \leqslant 4$. On the other hand, if $d_S(\mathbb{F}_{q^2}, \mathbb{F}_{q^2}\beta^i) = 4$, we have $\dim(\mathbb{F}_{q^2} \cap \mathbb{F}_{q^2}\beta^i) = 0$ or, equivalently, $\dim(\mathbb{F}_{q^2} \oplus \mathbb{F}_{q^2}\beta^i) = 4$. Hence, for this precise β^i, we get

$$\dim(\mathbb{F}_q \cap \mathbb{F}_q\beta^i) = 0 \ \text{ and } \ \dim(\mathcal{F}'_3 + \mathcal{F}'_3\beta^i) = 4.$$

In both cases, we can conclude $d_S(\mathbb{F}_q, \mathbb{F}_q\beta^i) = d_S(\mathcal{F}'_3, \mathcal{F}'_3\beta^i) = 2$. As a consequence, it holds $d_f(\mathcal{F}', \mathcal{F}'\beta^i) = 8$. Thus, the value $d = 6$ cannot be obtained if we consider flags of type $(1, 2, 3)$ on $\mathbb{F}_{q^4}$ generalizing $(\mathbb{F}_q, \mathbb{F}_{q^2})$.

The situation exhibited in the last example is a direct consequence of the presence of certain subfields of $\mathbb{F}_{q^n}$ as subspaces of a generalized Galois flag $\mathcal{F}$. In other words, its underlying Galois subflag affects, in some sense, the value $d_f(\mathrm{Orb}_\beta(\mathcal{F}))$. The next result establish some conditions on the minimum distance of generalized β-Galois flag codes that allow us to discard some values of the distance.

Theorem 4. *Let $\mathcal{F}$ be a generalized Galois flag of type $(s_1, \ldots, s_k)$ on $\mathbb{F}_{q^n}$ with underlying Galois subflag $(\mathbb{F}_{q^{t_1}}, \ldots, \mathbb{F}_{q^{t_r}})$ and take $\beta \in \mathbb{F}_{q^n}^*$. Consider $i \in \{1, \ldots, r\}$. Then the following statements hold:*

(1)   If $\beta \in \mathbb{F}_{q^{t_i}}^*$, then $d_S(\mathcal{F}_l, \mathcal{F}_l\beta) = 0$, for all $s_l \in \{t_i, \ldots, t_r\}$.

(2)   If $\beta \notin \mathbb{F}_{q^{t_i}}^*$, then $d_S(\mathcal{F}_l, \mathcal{F}_l\beta) = 2s_l$ for all $s_1 \leqslant s_l \leqslant t_i$.

Proof.

(1)   Assume that $\beta \in \mathbb{F}_{q^{t_i}}^*$. Hence, $\beta \in \mathbb{F}_{q^{t_j}}^*$, for every $i \leqslant j \leqslant r$. In other words, we have $\mathbb{F}_{q^{t_j}} \beta = \mathbb{F}_{q^{t_j}}$, i.e., $d_S(\mathbb{F}_{q^{t_j}}, \mathbb{F}_{q^{t_j}} \beta) = 0$ for all $i \leqslant j \leqslant r$.

(2)   Take now $\beta \notin \mathbb{F}_{q^{t_i}}^* = \operatorname{Stab}(\mathbb{F}_{q^{t_i}})$. In this case, $\mathbb{F}_{q^{t_i}}$ and $\mathbb{F}_{q^{t_i}} \beta$ are different subspaces in the t_i-spread $\operatorname{Orb}(\mathbb{F}_{q^{t_i}})$ and we have that $\dim(\mathbb{F}_{q^{t_i}} \cap \mathbb{F}_{q^{t_i}} \beta) = 0$. Thus, for every dimension $s_l \leqslant t_i$ in the type vector, we have $\dim(\mathcal{F}_l \cap \mathcal{F}_l \beta) = 0$ and then $d_S(\mathcal{F}_l, \mathcal{F}_l \beta) = 2s_l$. □

According to this result, it is clear that some combinations of subspace distances are automatically discarded when we compute the minimum distance of a generalized β-Galois flag code. Even thought we do not have a pattern to compute the distance values as it occurs for Galois flag codes (see (20), by means of Theorem 4, we can state some required conditions for potential distance values between flags on a generalized β-Galois flag code.

Definition 10. *Take a flag $\mathcal{F}$ of type $(s_1, \ldots, s_k)$ on $\mathbb{F}_{q^n}$ generalizing the Galois flag $(\mathbb{F}_{q^{t_1}}, \ldots, \mathbb{F}_{q^{t_r}})$ and an element $\beta \in \mathbb{F}_{q^n}^*$. We say that an even integer d is a potential value for $d_f(\operatorname{Orb}_\beta(\mathcal{F}))$ if it can be obtained as a sum of subspace distances of dimensions $s_1, \ldots, s_k$ satisfying:*

(1)   *For dimensions t_i, only distances 0 or $2t_i$ are considered.*

(2)   *If we sum $2t_i$ for dimension t_i, then all the distances for lower dimensions in the type vector are maximum as well.*

(3)   *If for some dimension t_i we have distance 0, then the same happens for dimensions t_j, with $i \leqslant j \leqslant r$.*

Remark 11. *Notice that, according to Definition 10, and as suggested in Example 4, having the field $\mathbb{F}_q$ as the first subspace of a flag does not affect to the set of potential distance values since every β-cyclic code of dimension 1 of $\mathbb{F}_{q^n}$ (generated or not by $\mathbb{F}_q$) has distance either 0 or 2. On the other hand, as also mentioned in Example 4, some distances cannot be attained when we have other fields among the subspaces of the generating flag. For instance, the single value $d = 6$ is discarded for $n = 4$, type $(1, 2, 3)$ and underlying Galois subflag of type $(1, 2)$.*

The next example shows that, in general, many values of the flag distance are not compatible with the underlying structure of nested fields.

Example 5. *Fix $n = 16$ and the type vector $(2, 4, 5, 6, 8)$. In general, every even integer $0 \leqslant d \leqslant 50$ is a possible value for the flag distance for this choice of the parameters. Nevertheless, if $\mathcal{F}$ is a generalized Galois flag of type $(2, 4, 5, 6, 8)$ with underlying Galois subflag of type $(2, 4, 8)$, then for every $\beta \in \mathbb{F}_{q^n}^*$, the set of potential values for $\operatorname{Orb}_\beta(\mathcal{F})$ is*

$$\{0, 2, 4, 6, 8, 10, 22, 50\}.$$

In other words, intermediate distances $12 \leqslant d \leqslant 20$ and $24 \leqslant d \leqslant 48$ cannot be obtained when the starting flag contains fields as its subspaces of dimensions 2, 4 and 8. For more details on the computation of the set of distance values, we refer the reader to [18] where, using the notion of distance vectors, a deeper study on the flag distance parameter and its behaviour is presented. For instance, if we obtain the maximum (subspace) distance for dimension 4, that is, distance 8, then we just have two possibilities for the flag distance: either 22 or 50, corresponding to distance vectors

$$(4, \mathbf{8}, 6, 4, 0) \quad \text{and} \quad (4, \mathbf{8}, 10, 12, 16),$$

which are completely determined by distances either 0 or 16 for dimension 8, respectively, (see [18], Theorem 3.9).

At this point, we can assert that the distance of a generalized Galois flag code is strongly influenced by its underlying Galois code. Hence, it is quite natural to wonder if generalized β-Galois flag codes behave as well as Galois flag codes in the following sense:

($*$) *Given a generalized Galois flag $\mathcal{F}$ and a potential value d for the distance defined in Definition 10, can we always find a suitable subgroup $\langle \beta \rangle \subseteq \mathbb{F}_{q^n}^*$ such that $d_f(\mathrm{Orb}_\beta(\mathcal{F})) = d$?*

In the following section we prove that the answer to the previous question is negative by exhibiting a specific family of generalized Galois flags.

4. A Construction of Generalized Galois Flag Codes

This section is devoted to build generalized Galois flags written in a regular form that allows us to provide constructions of β-cyclic orbit flag codes with a prescribed best friend. In Sections 4.1–4.3, we focus on the particular case of β primitive due to the fact that the obtained cyclic orbit codes present important properties that deserve to be underlined. Finally, Section 4.4 is devoted to deal with the β-cyclic case and, in particular, to give an answer to the question ($*$) formulated in the previous section.

Recall that, according to the definition of best friend, we can express all the subspaces of a given flag as vector spaces over its best friend (see (14)). In our case, we will consider a specific family of flags, whose subspaces are written in the regular form used in Proposition 2. Let us describe the form of such flags and obtain the parameters of cyclic orbit flag codes generated by them.

Fix $\mathbb{F}_{q^m}$ a subfield of $\mathbb{F}_{q^n}$ and consider a primitive element α of $\mathbb{F}_{q^n}$. For each positive integer l such that $1 \leqslant l < \frac{q^n-1}{q^m-1}$, let L be the degree of the minimal polynomial of α^l over $\mathbb{F}_{q^m}$. Observe that L is also the degree of the field extension $\mathbb{F}_{q^{mL}}/\mathbb{F}_{q^m}$, that is, $L = [\mathbb{F}_{q^{mL}} : \mathbb{F}_{q^m}]$. Hence, L divides $[\mathbb{F}_{q^n} : \mathbb{F}_{q^m}] = n/m = s$ and, we have that $L \leqslant s$. In addition, the set $\{1, \alpha^l, \alpha^{2l}, \ldots, \alpha^{(L-1)l}\}$ is a basis of the field extension $\mathbb{F}_{q^{mL}}/\mathbb{F}_{q^m}$. Thus, we can write

$$\bigoplus_{j=0}^{L-1} \mathbb{F}_{q^m} \alpha^{jl} = \mathbb{F}_{q^m}[\alpha^l] \cong \mathbb{F}_{q^{mL}}. \tag{21}$$

Now, for every $i = 1, \ldots, L$, the vector space

$$\mathcal{U}_i = \bigoplus_{j=0}^{i-1} \mathbb{F}_{q^m} \alpha^{jl} \tag{22}$$

has dimension mi (over $\mathbb{F}_q$) and, as stated in Section 2, it is a field if, and only if, either $i = 1$ or $i = L$. Hence, the sequence $(\mathcal{U}_1, \ldots, \mathcal{U}_L)$ forms a generalized Galois flag of type $(m, 2m, \ldots, mL)$ with underlying Galois subflag $(\mathbb{F}_{q^m}, \mathbb{F}_{q^{mL}})$.

Remark 12. *Observe that we cannot define a direct sum of this shape with more than L terms, since every power of α^l is always an element in $\mathcal{U}_L = \mathbb{F}_{q^m}[\alpha^l] \cong \mathbb{F}_{q^{mL}}$. Hence, this regular form allows us to construct flag codes on $\mathbb{F}_{q^n}$ of length $r \leqslant L$. Moreover, in case $L = s$, as $\mathcal{U}_L = \mathbb{F}_{q^n}$, we just get $r \leqslant L - 1 = s - 1$.*

The following two sections (Sections 4.1 and 4.2) are devoted to describe a construction of generalized Galois flag codes having $\mathbb{F}_{q^m}$ as their best friend. We perform it in two steps. First, we use flags in the regular form just described above in order to obtain a "basic" construction of generalized Galois flag codes where the underlying Galois flag code has, at most, length 2. Then, we propose a procedure to overcome this restriction and present another construction of generalized Galois flag code having a prescribed underlying Galois flag code by suitably "weaving" several basic generalized Galois flag codes.

4.1. Basic Constructions

By means of Proposition 3, we can easily determine the best friend of the subspaces $\mathcal{U}_i$ defined in (22): it is the subfield $\mathbb{F}_{q^m}$, for $1 \leqslant i \leqslant L - 1$ whereas the subspace $\mathcal{U}_L = \mathbb{F}_{q^{mL}}$ is its own best friend. This fact implies that we will find one or two fields among the subspaces $\mathcal{U}_i$, according to Remark 12. Since the case of length $r = 1$ corresponds to constant dimension codes (already studied in [9]), from now on, we will assume $r \geqslant 2$. Now, we know that for every type vector given by multiples of m, say $(ms_1, \ldots, ms_r)$, where $1 \leqslant s_1 < \cdots < s_r \leqslant L$, we select the subspaces defined in (22) corresponding, respectively, to these dimensions, that is,

$$\mathcal{F}_i = \mathcal{U}_{s_i} = \bigoplus_{j=0}^{s_i-1} \mathbb{F}_{q^m} \alpha^{lj}, \ 1 \leqslant i \leqslant r. \tag{23}$$

With this notation, the next result holds.

Theorem 5. *Let α be a primitive element of $\mathbb{F}_{q^n}$, l a positive integer with $1 \leqslant l < \frac{q^n - 1}{q^m - 1}$ and L the degree of the minimal polynomial of α^l over $\mathbb{F}_{q^m}$. Consider the flag $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ of type $(ms_1, \ldots, ms_r)$ on $\mathbb{F}_{q^n}$ with subspaces defined in (23). Hence, the code $\mathrm{Orb}(\mathcal{F})$ has best friend $\mathbb{F}_{q^m}$ and, in particular, its cardinality is $(q^n - 1)/(q^m - 1)$. Moreover,*

(1) If $s_r < L$, the code $\mathrm{Orb}(\mathcal{F})$ is consistent with distance $d_f(\mathrm{Orb}(\mathcal{F})) = 2mr$.

(2) If $s_r = L$, we have that $d_f(\mathrm{Orb}(\mathcal{F})) = 2m(r - 1)$ and we can write

$$\mathrm{Orb}(\mathcal{F}) = \dot{\bigcup}_{i=0}^{c-1} \mathrm{Orb}_{\alpha^c}(\mathcal{F}\alpha^i),$$

with $c = \frac{q^n - 1}{q^{mL} - 1}$.

Proof. Recall that, by means of Proposition 3, the best friend of every subspace in $\mathcal{F}$ is either $\mathbb{F}_{q^m}$ or $\mathbb{F}_{q^{mL}}$. Since $r \geqslant 2$, there is at least one subspace with $\mathbb{F}_{q^m}$ as best friend and, automatically, this subfield is the best friend of the flag $\mathcal{F}$. As a consequence, by Proposition 5, the cardinality of $\mathrm{Orb}(\mathcal{F})$ is $(q^n - 1)/(q^m - 1)$.

Now, suppose that $s_r < L$. In this case, every dimension in the type vector is $ms_i \leqslant ms_r < mL$ and every subspace in the flag $\mathcal{F}$ has the subfield $\mathbb{F}_{q^m}$ as its best friend. Hence, the code is disjoint and, by means of Theorem 2, we have $d_f(\mathrm{Orb}(\mathcal{F})) \geqslant 2mr$. Moreover, notice that, for every $1 \leqslant i \leqslant r$, the subspace $\mathcal{F}_i \cap \mathcal{F}_i \alpha^l = \bigoplus_{j=1}^{s_i-1} \mathbb{F}_{q^m} \alpha^{lj}$ has dimension $m(s_i - 1)$ over $\mathbb{F}_q$ and then $d_S(\mathrm{Orb}(\mathcal{F}_i)) = d_S(\mathcal{F}_i, \mathcal{F}_i \alpha^l) = 2m$. Hence, it holds

$$d_f(\mathcal{C}) \leqslant d_f(\mathcal{F}, \mathcal{F}\alpha^l) = \sum_{i=1}^{r} d_S(\mathcal{F}_i, \mathcal{F}_i \alpha^l) = 2mr$$

and we conclude $d_f(\mathcal{C}) = 2mr$. Moreover, the value coincides with the sum of the ones of its r projected codes (each one of them with distance $2m$). Hence, our code is consistent (see Definition 4).

Assume now that $s_r = L$. Then $\mathrm{Orb}(\mathcal{F})$ is not disjoint since the subspace $\mathcal{F}_r = \mathbb{F}_{q^{mL}}$ is its own best friend. However, since $\mathcal{F}_1, \ldots, \mathcal{F}_{r-1}$ have the same best friend $\mathbb{F}_{q^m}$, Theorem 2 ensures that $d_f(\mathrm{Orb}(\mathcal{F})) \geqslant 2m(r - 1)$. On the other hand, observe that $\alpha^l \in \mathbb{F}_q^{mL} \setminus \mathbb{F}_{q^m}^*$ stabilizes $\mathcal{F}_r$ but $d_S(\mathcal{F}_i, \mathcal{F}_i \alpha^l) = 2m$ for every $1 \leqslant i < r$. Hence, we have $d_f(\mathrm{Orb}(\mathcal{F})) = d_f(\mathcal{F}, \mathcal{F}\alpha^l) = 2m(r - 1)$.

Concerning the structure of this cyclic orbit flag code, it is clear that

$$\bigcup_{i=0}^{c-1} \mathrm{Orb}_{\alpha^c}(\mathcal{F}\alpha^i) \subseteq \mathrm{Orb}(\mathcal{F}).$$

Let us see that both sets have the same cardinality. To do so, observe that α^c is a primitive element of $\mathbb{F}_{q^{mL}}$. Hence, for every $1 \leqslant i \leqslant r$, it holds

$$\text{Stab}_{\alpha^c}(\mathcal{F}\alpha^i) = \mathbb{F}^*_{q^{mL}} \cap \text{Stab}(\mathcal{F}\alpha^i) = \mathbb{F}^*_{q^{mL}} \cap \mathbb{F}^*_{q^m} = \mathbb{F}^*_{q^m}.$$

As a consequence, we have $|\text{Orb}_{\alpha^c}(\mathcal{F}\alpha^i)| = \frac{q^{mL}-1}{q^m-1}$. Now, we prove that all these orbits are different. To do so, for every choice $0 \leqslant i \leqslant c-1$, observe that flags in $\text{Orb}_{\alpha^c}(\mathcal{F}\alpha^i)$ have the same last subspace $\mathcal{F}_r \alpha^i = \mathbb{F}_{q^{mL}}\alpha^i$ since α^c stabilizes $\mathcal{F}_r = \mathbb{F}_{q^{mL}} = \{0\} \cup \langle \alpha^c \rangle$. Moreover, the last projected code

$$\text{Orb}(\mathcal{F}_r) = \{\mathbb{F}_{q^{mL}}\alpha^i \mid 0 \leqslant i \leqslant c-1\}$$

of $\text{Orb}(\mathcal{F})$ is precisely the mL-spread $\text{Orb}(\mathbb{F}_{q^{mL}})$ of $\mathbb{F}_{q^n}$. Hence, for every choice $0 \leqslant i < j \leqslant c-1$, subspaces $\mathbb{F}_{q^{mL}}\alpha^i$ and $\mathbb{F}_{q^{mL}}\alpha^j$ are different. Therefore, all the orbits $\text{Orb}_{\alpha^c}(\mathcal{F}\alpha^i)$ are different and the cardinality of their union is exactly

$$c \cdot \frac{q^{mL}-1}{q^m-1} = \frac{q^n-1}{q^{mL}-1} \cdot \frac{q^{mL}-1}{q^m-1} = \frac{q^n-1}{q^m-1} = |\mathcal{C}|.$$

$\square$

From Theorem 5, and making a suitable choice of the type vector, we derive some constructions of our interest.

Corollary 2. *Consider the flag $\mathcal{F}$ of type $(ms_1, \ldots, ms_r)$ with $r \geqslant 2$ defined in (23). If $L < s$, then:*

(1)   the code $\text{Orb}(\mathcal{F})$ is a Galois flag code if, and only if, the type vector is (m, mL).

(2) $\text{Orb}(\mathcal{F})$ is a generalized Galois flag code if, and only if,

$$\varnothing \neq \{1, L\} \cap \{s_1, \ldots, s_r\} \neq \{1, L\}.$$

Proof. In the first place, if $L < s$, it is clear that $\mathcal{F}$ is a Galois flag if it just have subfields of $\mathbb{F}_{q^n}$ as its subspaces. According to expression (23), just subspaces of dimensions m and mL are fields. Moreover, since $r \geqslant 2$, the result follows. $\square$

Corollary 3. *Take the flag $\mathcal{F}$ of type $(ms_1, \ldots, ms_r)$ defined in (23) and assume $r \geqslant 2$ and $L = s$, then:*

(1) $\text{Orb}(\mathcal{F})$ is a generalized Galois flag code if, and only if, $s_1 = 1$.

(2)   In particular, if $s_1 = 1$ and $s_2 = L - 1$, then $\text{Orb}(\mathcal{F})$ is an optimum distance generalized Galois flag code of type $(m, n - m)$ with the largest possible size.

Proof. In this case, the only subfield of $\mathbb{F}_{q^n}$ written in the regular form (22) is $\mathbb{F}_{q^m}$ and the first statement follows straightforwardly. For the second one, it suffices to notice that the subspaces $\mathcal{F}_1 = \mathcal{U}_1 = \mathbb{F}_{q^m}$ and $\mathcal{F}_2 = \mathcal{U}_{L-1}$ are of dimensions m and $n - m$ and have $\mathbb{F}_{q^m}$ as their best friend. Hence, the result holds by means of Proposition 7. $\square$

At this point, we have all the ingredients to perfectly describe the structure of any cyclic orbit flag code $\text{Orb}(\mathcal{F})$ given in Theorem 5, in case its distance is either the minimum or the maximum possible one. This result is closely related with to discussion in Section 3.3 about the interdependence of distance values and type vectors, for this particular family of codes.

Theorem 6. *Let α be a primitive element of $\mathbb{F}_{q^n}$, l a positive integer such that $1 \leqslant l < \frac{q^n-1}{q^m-1}$, and L the degree of the minimal polynomial of α^l over $\mathbb{F}_{q^m}$. Consider $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ the flag of type $(ms_1, ms_2, \ldots, ms_r)$ on $\mathbb{F}_{q^n}$ of length $r \geqslant 2$ with subspaces defined as in (23). If $s = n/m$, then:*

(1) *The code $\mathrm{Orb}(\mathcal{F})$ has distance equal to $2m$ if, and only if, its type vector is (ms_1, mL) for some $1 \leqslant s_1 < L < s$. Moreover, if $s_1 = 1$, then $\mathrm{Orb}(\mathcal{F})$ is the Galois flag code of type (m, mL).*

(2) *The code $\mathrm{Orb}(\mathcal{F})$ is an optimum distance flag code if, and only if, $L = s$ and its type vector is $(m, m(L-1))$. In this case, $\mathrm{Orb}(\mathcal{F})$ is a generalized Galois flag code that attains the largest possible size.*

Proof. We divide the proof into two parts.

(1) By means of Theorem 2, if the orbit $\mathrm{Orb}(\mathcal{F})$ has distance $2m$, then there is exactly one subspace of $\mathcal{F}$ with $\mathbb{F}_{q^m}$ as its best friend. Since subspaces defined in (23) have the subfield $\mathbb{F}_{q^m}$ as their best friend except if they are fields, we conclude that the last subspace of the generating flag must be the field $\mathbb{F}_{q^{mL}} = \mathbb{F}_{q^m}[\alpha^l]$. Thus, L cannot be s and it holds $L < s$. Its first subspace can be any other subspace $\mathcal{F}_1$ of dimension $ms_1 < mL$.

To prove the converse, just note that the distance between $(\mathcal{F}_1, \mathbb{F}_{q^{mL}})$ and $(\mathcal{F}_1, \mathbb{F}_{q^{mL}})\alpha^l$ is $2m$, which is the minimum distance for cyclic orbit flag codes with $\mathbb{F}_{q^m}$ as their best friend.

To finish, if $s_1 = 1$, the only possibility for $\mathcal{F}$ is to be the Galois flag of type (m, mL) and the result holds.

(2) On the other hand, if $\mathrm{Orb}(\mathcal{F})$ is an optimum distance cyclic orbit flag code with $\mathbb{F}_{q^m}$ as its best friend, by means of Proposition 6, and assuming $r \geqslant 2$, its type vector must be $(m, n-m)$. Hence, we need mL to be at least $n - m = m(s-1)$. In other words, L must be greater or equal than $s - 1$. However, L has to divide s. If $L = s - 1$, the only possibility is $s = 2$ and the only type vector consisting of multiples of m is (m), which has length one. Thus, it must hold $L = s$. The converse is also true by application of Corollary 2.

□

Remark 13. *Concerning the first statement of the previous result, it is important to point out that if we consider a generating flag not necessarily written in the regular form described in (23), it is possible to attain the distance $2m$ with no other field among the subspaces of the generating flag than the best friend of the flag. Recall that, for general flags, even if we fix the field $\mathbb{F}_{q^m}$ as the first subspace, there are three possibilities for the best friend of each one of its subspaces: the field $\mathbb{F}_{q^m}$, the subspace itself (in case it is a field) or an intermediate extension field over $\mathbb{F}_{q^m}$. The next example contemplates this situation.*

Example 6. *Fix $n = 16$ and consider a generalized Galois flag $\mathcal{F} = (\mathcal{F}_1, \mathcal{F}_2)$ with type vector $(2, 8)$ such that*

$$
\begin{aligned}
\mathcal{F}_1 &= \mathbb{F}_{q^2}, \\
\mathcal{F}_2 &= \mathbb{F}_{q^2} \oplus \mathbb{F}_{q^2}\beta \oplus \mathbb{F}_{q^2}\alpha \oplus \mathbb{F}_{q^2}\beta\alpha = \mathbb{F}_{q^4} \oplus \mathbb{F}_{q^4}\alpha,
\end{aligned}
$$

where α denotes a primitive element of $\mathbb{F}_{q^{16}}$ and $\beta = \alpha^{(q^{16}-1)/(q^4-1)}$ is a primitive element of the subfield $\mathbb{F}_{q^4}$. Observe that $\mathbb{F}_{q^4}$ is a friend of $\mathcal{F}_2$. Even more, it is its best friend by means of Proposition 3, since the degree of the minimal polynomial of α over $\mathbb{F}_{q^4}$ is $16/4 = 4$. According to this, $\mathbb{F}_{q^2}$ is the best friend of the cyclic orbit flag code $\mathrm{Orb}(\mathcal{F})$. Moreover, we have that $d_f(\mathcal{F}, \mathcal{F}\beta) = d_S(\mathcal{F}_1, \mathcal{F}_1\beta) = 4$ is the minimum possible distance for cyclic orbit flag codes with $\mathbb{F}_{q^2}$ as its best friend. However, $\mathrm{Orb}(\mathcal{F})$ is not the Galois flag code of type $(2, 8)$, since $\mathcal{F}$ is the only flag in the code with its first subspace containing the element $1 \in \mathbb{F}_{q^{16}}$ but $\mathcal{F}_2$ is not a field.

Observe now that, taking again the flag $\mathcal{F} = (\mathcal{F}_1, \mathcal{F}_2)$ as in the previous example, we have the subfield $\mathbb{F}_{q^4}$ as an intermediate subspace. In other words, the sequence

$$\mathcal{F}' = (\mathbb{F}_{q^2}, \mathbb{F}_{q^4}, \mathbb{F}_{q^4} \oplus \mathbb{F}_{q^4}\alpha)$$

forms a generalized Galois flag longer than $\mathcal{F}$. Notice that the field $\mathbb{F}_{q^4}$ can be written in regular form as a vector space over $\mathbb{F}_{q^2}$ as $\mathbb{F}_{q^2} \oplus \mathbb{F}_{q^2}\beta$. Moreover, the subspace $\mathbb{F}_{q^4} \oplus \mathbb{F}_{q^4}\alpha$ is, at the same time, written in regular form as a vector space over $\mathbb{F}_{q^4}$. Inspired by this idea, we will describe a general procedure that allows us to obtain generalized Galois flags codes, written in regular form over suitably chained subfields.

4.2. Weaving Basic Generalized Galois Flag Codes

The previous basic construction (Theorem 5) presents a limitation on the number of subfields that can appear as subspaces of the generating flag. In this subsection, we focus on a systematic construction of generalized Galois flag codes with a prescribed underlying Galois subflag. More precisely, if $m_1, m_2, \ldots, m_k$ are divisors of n such that m_i divides m_{i+1}, for every $1 \leqslant i \leqslant k$, we work on the construction of generalized Galois flag codes with $(\mathbb{F}_{q^{m_1}}, \ldots, \mathbb{F}_{q^{m_k}})$ as underlying Galois subflag.

As a matter of notation, through this section we will write $m_{k+1} = n$. Let α be a primitive element of $\mathbb{F}_{q^n}$ and put $c_i = \frac{q^n - 1}{q^{m_i} - 1}$, for $1 \leqslant i \leqslant k+1$. It turns out that each power $\alpha_i = \alpha^{c_i}$ is a primitive element of the corresponding subfield $\mathbb{F}_{q^{m_i}}$. For every $2 \leqslant i \leqslant k+1$, the degree of the minimal polynomial of α_i over $\mathbb{F}_{q^{m_{i-1}}}$ is $L_i = \frac{m_i}{m_{i-1}}$. With this notation, we consider k flags $\mathcal{F}^1, \ldots, \mathcal{F}^k$ on $\mathbb{F}_{q^n}$, whose subspaces are given by

$$\mathcal{F}_j^i = \bigoplus_{l=0}^{j-1} \mathbb{F}_{q^{m_i}} \alpha_{i+1}^l, \tag{24}$$

for $1 \leqslant j \leqslant L_{i+1} - 1$ and $1 \leqslant i \leqslant k$. Observe that, for every $1 \leqslant i \leqslant k$, we have that $\mathcal{F}_1^i = \mathbb{F}_{q^{m_i}}$ and the dimension of $\mathcal{F}_j^i$ (as an $\mathbb{F}_q$-vector space) is jm_i. Hence, the type vector of $\mathcal{F}^i$ is given by all the multiples of m_i smaller than m_{i+1}, that is, $(m_i, 2m_i, \ldots, m_{i+1} - m_i)$. As a consequence of Theorem 5, the next result holds.

Corollary 4. *Let $\mathcal{F}^i$ be the flag defined in (24) for every $1 \leqslant i \leqslant k$. Then the generalized Galois flag code $\mathrm{Orb}(\mathcal{F}^i)$ is consistent with distance $2(m_{i+1} - m_i)$ and has the field $\mathbb{F}_{q^{m_i}}$ as its best friend.*

Proof. For every $1 \leqslant i \leqslant k$, we apply Theorem 5 (part (1)) to the generalized Galois flag code $\mathrm{Orb}(\mathcal{F}^i)$ and conclude that it is a consistent flag code with distance equal to $2m_i(L_{i+1} - 1) = 2(m_{i+1} - m_i)$. $\square$

Observe that we have constructed a collection of orbit flag codes with respective generating flags in regular form over their best friend. The first subspace of each flag $\mathcal{F}^i$ is precisely its best friend and contains the last subspace of the previous flag, since

$$\mathcal{F}_{L_{i+1}-1}^i \subseteq \mathbb{F}_{q^{m_i}}[\alpha_{i+1}] = \mathbb{F}_{q^{m_{i+1}}} = \mathcal{F}_1^{i+1},$$

for every value $1 \leqslant i \leqslant k-1$. By means of this property, we can consider a generating generalized Galois flag having all the subfields $\{\mathbb{F}_{q^{m_i}}\}_{i=1}^k$ among its subspaces just by taking

$$\mathcal{F} = (\mathcal{F}_1^1, \ldots, \mathcal{F}_{L_1-1}^1, \mathcal{F}_1^2, \ldots, \mathcal{F}_{L_2-1}^2, \ldots, \mathcal{F}_1^k, \ldots, \mathcal{F}_{L_k-1}^k), \tag{25}$$

whose type vector is $(m_1, \ldots, m_2 - m_1, m_2, \ldots, m_3 - m_2, m_3, \ldots, m_k, \ldots, n - m_k)$. In this way, by weaving the independent basic constructions described in Corollary 4, we get a generalized Galois flag code with the prescribed tower of subfields $(\mathbb{F}_{q^{m_1}}, \ldots, \mathbb{F}_{q^{m_k}})$ as its underlying Galois subflag.

Proposition 9. *Let $\mathcal{F}$ be the generalized Galois flag on $\mathbb{F}_{q^n}$ given in (25). Then the generalized Galois flag code $\mathrm{Orb}(\mathcal{F})$ generalizes the Galois flag of type $(m_1, \ldots, m_r)$. Its cardinality is $\frac{q^n - 1}{q^{m_1} - 1}$ and its minimum distance, $2(m_2 - m_1)$.*

Proof. By construction, it is clear that the subspace of dimension m_i of $\mathcal{F}$ is the field $\mathbb{F}_{q^{m_i}}$, for every $1 \leqslant i \leqslant k$. Moreover, subspaces of dimensions $m_i, \ldots, m_{i+1} - m_i$ have the subfield $\mathbb{F}_{q^{m_i}}$ as its best friend. As a result, the best friend of the flag $\mathcal{F}$ coincides with its first subspace, that is, $\mathbb{F}_{q^{m_1}}$. This fact leads to the statement about the cardinality. Let us compute now the minimum distance of the code. First, by means of Theorem 2, since there are exactly $L_2 - 1$ subspaces of $\mathcal{F}$ with $\mathbb{F}_{q^{m_1}}$ as their best friend, we conclude that $d_s(\mathrm{Orb}(\mathcal{F})) \geqslant 2m_1(L_2 - 1) = 2(m_2 - m_1)$. Moreover, observe that α_2 stabilizes every subspace of the flag $\mathcal{F}$ containing $\mathbb{F}_{q^{m_2}} = \{0\} \cup \langle \alpha_2 \rangle$. Hence, $d_f(\mathrm{Orb}(\mathcal{F})) \leqslant d_f(\mathcal{F}, \mathcal{F}\alpha_2) = d_f(\mathcal{F}^1, \mathcal{F}^1\alpha_2) = 2m(L_2 - 1) = 2(m_2 - m_1)$ since, for every $1 \leqslant j \leqslant L_2 - 1$, the subspace $\mathcal{F}_j^1 \cap \mathcal{F}_j^1 \alpha = \bigoplus_{l=1}^{j-1} \mathbb{F}_{q^m} \alpha_2^l$ has dimension $m(j-1)$. We conclude that $d_f(\mathrm{Orb}(\mathcal{F})) = 2(m_2 - m_1)$. $\square$

Remark 14. *Note that weaving our basic constructions allows us to give generalized Galois flag codes with any given underlying Galois subflag in a systematic way. Another interesting fact to point out is that the best friends of the subspaces in the generalized Galois flag $\mathcal{F}$ defined in (25) form a nested sequence of subfields. This does not happen in general for arbitrary generalized Galois flag codes and it helps us to easily determine the cardinality and distance of the code $\mathrm{Orb}(\mathcal{F})$ as well as to give bounds for the distance when we consider its β-cyclic subcodes, as we will see in Section 4.4. On the negative side, contrary to what happens with the basic construction, the waved one is not consistent since it is not even disjoint.*

4.3. Decoding Our Constructions over the Erasure Channel

The use of flags in network coding was originally introduced by Liebhold et al. in [14]. In that paper, a channel model for flags was presented and some constructions, together with their decoding algorithms (over the erasure channel) were provided. In [15], a decoding algorithm over the erasure channel for consistent flag codes is presented. In particular, such an algorithm can be applied to the basic construction given in Theorem 5, part (1). Although the rest of constructions in this paper are not consistent, we can adapt the decoding process in [15] to them. To do so, let us briefly recall some concepts related to the notion of *correctability*.

Assume that we have sent a flag $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_r)$ and hence, the receiver gets a sequence of nested subspaces $\mathcal{X} = (\mathcal{X}_1, \ldots, \mathcal{X}_r)$ that, when working over an erasure channel, must satisfy $\mathcal{X}_i \subseteq \mathcal{F}_i$, for all $1 \leqslant i \leqslant r$. In this context, each value $e_i = d_S(\mathcal{F}_i, \mathcal{X}_i) = \dim(\mathcal{F}_i) - \dim(\mathcal{X}_i)$ is called *number of erasures at the i-th shot* whereas $e = d_f(\mathcal{F}, \mathcal{X}) = \sum_{i=1}^r e_i$ is the *total number of erasures*. We say that the total number of erasures e is *correctable* (by minimum distance) by a flag code $\mathcal{C}$ whenever $e \leqslant \lfloor \frac{d_f(\mathcal{C}) - 1}{2} \rfloor$. Analogously, we also say that the value e_i is correctable by the projected code $\mathcal{C}_i$ if $e_i \leqslant \lfloor \frac{d_S(\mathcal{C}_i) - 1}{2} \rfloor$.

Let us fix the flag code $\mathcal{C}$ as the one presented in Theorem 5, part (2). Recall that such a code has distance $2m(r-1)$ and r projected codes of distance $2m$. Following the ideas of ([15], Proposition 8), we state the next result.

Proposition 10. *If the total number of erasures e is correctable by the generalized Galois flag code $\mathcal{C}$, then there exists some $1 \leqslant i \leqslant r - 1$ such that the value e_i is also correctable by the corresponding projected code $\mathcal{C}_i$.*

Proof. Assume that no value e_i is correctable for every $1 \leqslant i \leqslant r - 1$. Equivalently, we have that $e_i \geqslant m$ for every $1 \leqslant i \leqslant r - 1$. As a consequence, we have that

$$e = \sum_{i=1}^{r} e_i \geqslant m(r-1) + e_r \geqslant m(r-1),$$

which is a contradiction, since $\mathcal{C}$ can correct up to $m(r-1) - 1$ erasures. □

Now, if $\mathcal{C}'$ denotes the generalized Galois flag code obtained by the weaved construction given in Proposition 9 and $m_1 = m$, then we have $d_f(\mathcal{C}') = 2(m_2 - m) = 2m(L_2 - 1)$. Moreover, $d_S(\mathcal{C}'_i) = 2m$ holds for the first $L_2 - 1$ projected codes. Hence, the same argument in the proof of Proposition 10 can be used to show that a correctable total number of erasures can be detected and corrected by one of the first $L_2 - 1$ projected codes of $\mathcal{C}$.

Proposition 11. *If the total number of erasures e is correctable by $\mathcal{C}'$, then there exists some $1 \leqslant i \leqslant L_2 - 1$ such that e_i is correctable by the projected code $\mathcal{C}'_i$.*

Moreover, in both situations, every projected code has the same distance, which is $2m$. Hence, the number of erasures at any shot is correctable whenever it holds $e_i \leqslant m - 1$. We can easily identify if an erasure is correctable just by checking the dimension of every received subspace $\mathcal{X}_i$. The next proposition is valid for both a generalized Galois flag codes $\mathcal{C}$ and $\mathcal{C}'$.

Proposition 12. *The number of erasures e_i is correctable by the constant dimension code $\mathcal{C}_i$ (resp. $\mathcal{C}'_i$) if, and only if, $\dim(\mathcal{X}_i) \geqslant \dim(\mathcal{F}_i) - m + 1$.*

Proof. Assume that we send a flag $\mathcal{F} \in \mathcal{C}$ (resp. in $\mathcal{C}'$) and a stuttering flag $\mathcal{X}$ is received. Then e_i is correctable by $\mathcal{C}_i$ (resp. $\mathcal{C}'_i$) if, and only if, it holds

$$\dim(\mathcal{F}_i) - \dim(\mathcal{X}_i) = d_S(\mathcal{F}_i, \mathcal{X}_i) = e_i \leqslant m - 1$$

or equivalently, if $\dim(\mathcal{X}_i) \geqslant \dim(\mathcal{F}_i) - m + 1$. □

Remark 15. *Observe that neither $\mathcal{C}$ nor $\mathcal{C}'$ are disjoint flag codes. However, Proposition 10 (resp. Proposition 11) allows us to decode at least one of the received subspaces $\mathcal{X}_i$ into the sent one $\mathcal{F}_i$ for an index i satisfying $|\mathcal{C}_i| = |\mathcal{C}|$ (resp. $|\mathcal{C}'_i| = |\mathcal{C}'|$). Hence, after having recovered $\mathcal{F}_i$, one can easily obtain the sent flag $\mathcal{F}$ as the unique flag in $\mathcal{C}$ (resp. $\mathcal{C}'$) having $\mathcal{F}_i$ as its i-th subspace.*

4.4. The β-Cyclic Case

In this part of the paper, we consider orbits under the action of proper subgroups of $\mathbb{F}_{q^n}^*$ generated by the flag $\mathcal{F}$ given in (25), which has underlying Galois subflag $(\mathbb{F}_{q^{m_1}}, \mathbb{F}_{q^{m_2}}, \dots, \mathbb{F}_{q^{m_k}})$. In other words, for every $\beta \in \mathbb{F}_{q^n}^*$, we study the generalized β-Galois flag code $\mathrm{Orb}_\beta(\mathcal{F})$. Recall that this code has type $(m_1, \dots, m_2 - m_1, m_2, \dots, m_3 - m_2, m_3, \dots, m_k, \dots, n - m_k)$ and it has the following particularity: the best friends of the subspaces of $\mathcal{F}$ are nested. More precisely, the subfield $\mathbb{F}_{q^{m_i}}$ is the best friend of the subspaces of dimensions $m_i, \dots, m_{i+1} - m_i$ in the flag, for every $1 \leqslant i \leqslant k$, where $m_{k+1} = n$. This property makes our flag $\mathcal{F}$ be closer to the Galois flag of type $(m_1, \dots, m_k)$ than other flags that also generalize it. As a result, we can give lower and upper bounds for the distance of $\mathrm{Orb}_\beta(\mathcal{F})$ by studying the sequence of subgroups

$$\langle \beta \rangle \cap \mathbb{F}_{q^{m_1}}^* \subseteq \langle \beta \rangle \cap \mathbb{F}_{q^{m_2}}^* \subseteq \cdots \subseteq \langle \beta \rangle \cap \mathbb{F}_{q^{m_k}}^*.$$

In particular, we consider two possibilities: either all these subgroups coincide or some inclusion is strict. In the latest case, we are specially interested in the first index $1 < i \leqslant k$

such that $\langle \beta \rangle \cap \mathbb{F}^*_{q^{m_1}} \neq \langle \beta \rangle \cap \mathbb{F}^*_{q^{m_i}}$. Moreover, we exclude those elements $\beta \in \mathbb{F}^*_{q^{m_1}}$ since they provide trivial orbit flag codes with distance equal to zero.

Theorem 7. *Let $\mathcal{F}$ be the generalized Galois flag given in (25) and $\beta \in \mathbb{F}^*_{q^n} \setminus \mathbb{F}^*_{q^{m_1}}$. For every $1 \leqslant i \leqslant k$, we write $M_i = \sum_{j=1}^{i-1} m_{j+1}(L_{j+1} - 1)$.*

(1) If $\langle \beta \rangle \cap \mathbb{F}^*_{q^{m_1}} = \langle \beta \rangle \cap \mathbb{F}^*_{q^{m_k}}$, then

$$2m_k(L_{k+1} - 1) + M_k \leqslant d_f(\mathrm{Orb}_\beta(\mathcal{F})) \leqslant m_k \left\lfloor \frac{L_{k+1}^2}{2} \right\rfloor + M_k.$$

(2) Otherwise, consider the minimum $1 < i \leqslant k$ such that $\langle \beta \rangle \cap \mathbb{F}^*_{q^{m_1}} \subsetneq \langle \beta \rangle \cap \mathbb{F}^*_{q^{m_i}}$. Then it holds:

$$2m_{i-1}(L_i - 1) + M_{i-1} \leqslant d_f(\mathrm{Orb}_\beta(\mathcal{F})) \leqslant m_{i-1} \left\lfloor \frac{L_i^2}{2} \right\rfloor + M_{i-1}.$$

Proof. Assume that $\langle \beta \rangle \cap \mathbb{F}^*_{q^{m_1}} = \langle \beta \rangle \cap \mathbb{F}^*_{q^{m_k}}$. Let us compute the distance $d_f(\mathcal{F}, \mathcal{F}\beta^l)$, for every element $\beta^l \notin \mathrm{Stab}_\beta(\mathcal{F}) = \langle \beta \rangle \cap \mathbb{F}^*_{q^{m_1}}$. Since $\langle \beta \rangle \cap \mathbb{F}^*_{q^{m_1}} = \langle \beta \rangle \cap \mathbb{F}^*_{q^{m_k}}$, this power β^l does not stabilize any subspace in the flag $\mathcal{F}$. In particular, observe that $\mathbb{F}_{q^{m_k}}$ and $\mathbb{F}_{q^{m_k}}\beta^l$ are different subspaces in the spread $\mathrm{Orb}(\mathbb{F}_{q^{m_k}})$. In other words, it holds $d_S(\mathbb{F}_{q^{m_k}}, \mathbb{F}_{q^{m_k}}\beta^l) = 2m_k$ and, by means of Theorem 4, every subspace distance between subspaces of $\mathcal{F}$ and $\mathcal{F}\beta^l$ of dimensions lower than m_k is maximum as well, i.e., twice the corresponding dimension. Hence, for dimensions up to $m_k - m_{k-1} = m_{k-1}(L_k - 1)$, we obtain the sum of subspace distances:

$$
\begin{aligned}
\sum_{j=1}^{k-1} \left(2m_j + \cdots + 2m_j(L_{j+1} - 1) \right) &= \sum_{j=1}^{k-1} 2m_j \left(1 + \cdots + (L_{j+1} - 1) \right) \\
&= \sum_{j=1}^{k-1} m_j L_{j+1}(L_{j+1} - 1) \\
&= \sum_{j=1}^{k-1} m_{j+1}(L_{j+1} - 1) = M_k.
\end{aligned}
$$

Moreover, since subspaces of dimensions $m_k, \ldots, n - m_k = m_k(L_{k+1} - 1)$ have $\mathbb{F}_{q^{m_k}}$ as their best friend, if d represents the flag distance between the subflags of type $m_k(1, \ldots, L_{k+1} - 1)$ of $\mathcal{F}$ and $\mathcal{F}\beta^l$ and, by means of (16), we have:

$$2m_k(L_{k+1} - 1) \leqslant d \leqslant m_k \left\lfloor \frac{L_{k+1}^2}{2} \right\rfloor.$$

Combining these two facts, we get the desired lower and upper bounds for $d_f(\mathcal{F}, \mathcal{F}\beta^l)$, if $\beta^l \notin \mathrm{Stab}_\beta(\mathcal{F})$. In particular, these bounds are also valid for $d_f(\mathrm{Orb}_\beta(\mathcal{F}))$.

To prove (2), suppose that $\langle \beta \rangle \cap \mathbb{F}_{q^{m_1}} \neq \langle \beta \rangle \cap \mathbb{F}_{q^{m_k}}$ and then take the minimum $1 < i \leqslant k$ such that $\langle \beta \rangle \cap \mathbb{F}_{q^{m_1}} \subsetneq \langle \beta \rangle \cap \mathbb{F}_{q^{m_i}}$. In this case, we can always find an element $\beta^l \in \mathbb{F}^*_{q^{m_i}} \setminus \mathbb{F}^*_{q^{m_1}}$. This power β^l stabilizes every subspace in $\mathcal{F}$ having the subfield $\mathbb{F}_{q^{m_i}}$ as a friend, i.e., all those of dimensions at least m_i. This means that these dimensions do not contribute to the computation of $d_f(\mathcal{F}, \mathcal{F}\beta^l)$. On the other hand, since $\langle \beta \rangle \cap \mathbb{F}_{q^{m_1}} = \cdots = \langle \beta \rangle \cap \mathbb{F}_{q^{m_{i-1}}}$, then $\mathbb{F}_{q^{m_{i-1}}} \neq \mathbb{F}_{q^{m_{i-1}}}\beta^l$ are different spread elements and the distance between them is $2m_{i-1}$. As before, by means of Theorem 4, all the subspace distances are maximum for dimensions up to m_i. In particular, the distance between the subflags of type $(m_1, \ldots, m_i - m_{i-1})$ of $\mathcal{F}$ and $\mathcal{F}\beta^l$ is exactly

$$\sum_{j=1}^{i-2} m_{j+1}(L_{j+1} - 1) = M_{i-1}.$$

Besides, observe that the subspaces of dimensions $m_{i-1}, \ldots, m_i - m_{i-1}$ of $\mathcal{F}$ and $\mathcal{F}\beta^l$ are $\mathbb{F}_{q^{m_{i-1}}}$-subspaces of $\mathbb{F}_{q^{m_i}}$. Hence, if d denotes the distance between the corresponding subflags of $\mathcal{F}$ and $\mathcal{F}\beta^l$, by (16), we have

$$2m_{i-1}(L_i - 1) \leqslant d \leqslant m_{i-1} \left\lfloor \frac{L_i^2}{2} \right\rfloor.$$

As a result, we conclude

$$2m_{i-1}(L_i - 1) + M_{i-1} \leqslant d_f(\mathcal{F}, \mathcal{F}\beta^l) \leqslant m_{i-1} \left\lfloor \frac{L_i^2}{2} \right\rfloor + M_{i-1} \qquad (26)$$

for every $\beta^l \in \mathbb{F}_{q^{m_i}}^* \setminus \mathbb{F}_{q^{m_1}}^*$. Arguing as above, if we take another power of β not in $\mathbb{F}_{q^{m_i}}^*$, say β^h, we obtain maximum subspace distances up to, at least, dimensions m_i and then

$$d_f(\mathcal{F}, \mathcal{F}\beta^h) \geqslant d_f(\mathcal{F}, \mathcal{F}\beta^l).$$

As a consequence, the minimum distance of the code is attained when we consider powers $\beta^l \in \mathbb{F}_{q^{m_i}}^* \setminus \mathbb{F}_{q^{m_1}}^*$ and we have the result. □

Observe that the upper bound for the distance in the first part of Theorem 7 is exactly the maximum possible distance for general flags of the corresponding type. Here below, we go a step further and give a sufficient condition for our construction to provide optimum distance flag codes, i.e., flag codes with the maximum possible distance for their type on $\mathbb{F}_{q^n}$.

Corollary 5. *Consider the generalized Galois flag $\mathcal{F}$ given in (25) and take $\beta \in \mathbb{F}_{q^n}^*$ such that $\langle \beta \rangle \cap \mathbb{F}_{q^{m_1}}^* = \langle \beta \rangle \cap \mathbb{F}_{q^{m_k}}^*$. If $L_{k+1} \leqslant 3$, then $\mathrm{Orb}_\beta(\mathcal{F})$ is an optimum distance flag code.*

Proof. Notice that, under these assumptions, by means of Theorem 7 (part (1)), we have

$$2m_k(L_{k+1} - 1) + M_k \leqslant d_f(\mathrm{Orb}_\beta(\mathcal{F})) \leqslant m_k \left\lfloor \frac{L_{k+1}^2}{2} \right\rfloor + M_k.$$

Moreover, if the degree of the extension $\mathbb{F}_{q^n}/\mathbb{F}_{q^{m_k}}$, that is, the positive integer $L_{k+1} = [\mathbb{F}_{q^n} : \mathbb{F}_{q^{m_k}}] = n/m_{k+1}$, satisfies $1 < L_{k+1} \leqslant 3$, then we have

$$2(L_{k+1} - 1) = \left\lfloor \frac{L_{k+1}^2}{2} \right\rfloor.$$

Hence, both lower and upper bounds for $d_f(\mathrm{Orb}_\beta(\mathcal{F}))$ coincide and the code $\mathrm{Orb}_\beta(\mathcal{F})$ attains the maximum possible distance for its type vector. □

To finish this subsection we address the question (∗) in Section 3.4.2. Recall that the potential distance values of generalized Galois flag code follow the rules stated in Theorem 4 and Definition 10. These conditions arise naturally from the presence of certain subfields among the subspaces of a generalized Galois flag. Concerning question (∗), we wonder if, given a generalized Galois flag $\mathcal{F}$, every potential value of the distance can be truly obtained by a cyclic (or β-cyclic) orbit flag code generated by $\mathcal{F}$. We answer this question by using the β-cyclic construction presented in Section 4.4.

Example 7. *Consider the following parameters choice: $q = 2$, $n = 10$. Moreover, we take nested subfields $\mathbb{F}_2 \subset \mathbb{F}_{2^5}$ of the field $\mathbb{F}_{2^{10}}$, which correspond to the election of divisors $m_1 = 1$ and $m_2 = 5$ of $n = 10$. In this case, we have $L_2 = 5$ and $L_3 = 2$. Let us use the generalized Galois flag $\mathcal{F} = (\mathbb{F}_2, \mathcal{F}_2, \mathcal{F}_3, \mathcal{F}_4, \mathbb{F}_{2^5})$ of type $(1, 2, 3, 4, 5)$ with subspaces:*

$$\mathcal{F}_2 = \mathbb{F}_2 \oplus \mathbb{F}_2 \gamma, \qquad \mathcal{F}_3 = \mathbb{F}_2 \oplus \mathbb{F}_2 \gamma \oplus \mathbb{F}_2 \gamma^2, \quad and \quad \mathcal{F}_4 = \mathbb{F}_2 \oplus \mathbb{F}_2 \gamma \oplus \mathbb{F}_2 \gamma^2 \oplus \mathbb{F}_2 \gamma^3,$$

where γ is a primitive element of $\mathbb{F}_{2^5}$.

The set of potential values of the distance in this case is given by:

$$\{0, 8, 10, 12, 30\}.$$

In this case, we know how to choose $\beta \in \mathbb{F}_{2^{10}}^*$ so that the orbit $\mathrm{Orb}_\beta(\mathcal{F})$ attains some of these distances. More precisely:

- *Distance $d = 0$ is obtained if, and only if, $\beta \in \mathbb{F}_2^* = \{1\} = \mathrm{Stab}(\mathcal{F})$.*
- *For distance $d = 8$, it suffices to take the cyclic orbit code $\mathrm{Orb}(\mathcal{F})$ that, by means of Theorem 5, has distance $d_f(\mathrm{Orb}(\mathcal{F})) = 8$.*
- *Last, since $L_3 = 2 \leqslant 3$, by application of Corollary 5, we know that every $\beta \in \mathbb{F}_{2^{10}}^*$ such that $\langle \beta \rangle \cap \mathbb{F}_{2^5} = \{1\}$ makes $\mathrm{Orb}_\beta(\mathcal{F})$ be an optimum distance flag code. For instance, it suffices to consider subgroups $\langle \beta \rangle$ of $\mathbb{F}_{2^{10}}^*$ of orders $\{3, 11, 33\}$ to attain the maximum distance, i.e., the value $d = 30$.*

Moreover, for this specific example, we have obtained the parameters of the code $\mathrm{Orb}_\beta(\mathcal{F})$, for every subgroup $\langle \beta \rangle$ of $\mathbb{F}_{2^{10}}^*$ by using GAP. First of all, since $\mathrm{Stab}(\mathcal{F}) = \mathbb{F}_2^* = \{1\}$, we have $|\mathrm{Orb}_\beta(\mathcal{F})| = |\beta|$. The next table collects the set of distances for the generating flag $\mathcal{F}$.

Using this example, one can see that not all the potential values of the distance can be obtained by taking a suitable subgroup of $\mathbb{F}_{2^{10}}^*$. It suffices to observe that neither distances $d = 10$ nor $d = 12$ appear in Table 2. Even more, despite the fact that $d_f(\mathrm{Orb}_\beta(\mathcal{F})) \neq 12$ for any $\beta \in \mathbb{F}_{2^{10}}^*$, this value still can be the distance between a couple of flags; for instance, we have

$$d_f(\mathcal{F}, \mathcal{F}\gamma^2) = 2 + 4 + 4 + 2 + 0 = 12.$$

However, this is not even true for distance $d = 10$. In other words, for every $\beta \in \mathbb{F}_{2^{10}}^*$ and any power $1 \leqslant l \leqslant |\beta|$, the distance $d_f(\mathcal{F}, \mathcal{F}\beta^l) \neq 10$.

Table 2. Distance of all the β-cyclic orbit flag codes generated by $\mathcal{F}$.

$|\beta|$	$d_f(\mathrm{Orb}_\beta(\mathcal{F}))$
1	0
3	30
11	30
31	8
33	30
93	8
341	8
1023	8

5. Conclusions and Future Work

In this work, we present new contributions to the study of β-cyclic orbit flag codes started in [16], also following the viewpoint of [9]. The best friend of a flag code still has a crucial role throughout the paper. In particular, we discuss the rich interplay of flag distances, best friend and type vector for this family of codes.

Nevertheless, whereas in [16] the accent was put precisely on the best friend of the flag code, this time we turn our attention to the generating flag of the orbit. We focus specially on those ones having at least one field among their subspaces, by distinguishing the case of having just fields on the generating flag from the case where also at least one subspace not

being a field appears. This dichotomy leads, on one side, to the known β-Galois flag codes and, on the other one, to the generalized β-Galois flag codes, which properties we describe.

Every generalized β-Galois flag code has an underlying β-Galois flag code. Thus, we have addressed the question of determine if the parameters and the behaviour of Galois flag codes drives, in some sense, the parameters of the generalized ones. To do this, we provide a systematic construction of generalized Galois flag codes with a prescribed underlying Galois flag code that presents remarkable properties and helps to us to shed some light on the raised questions.

To future work, we want to deepen the study of β-cyclic orbit codes by determining suitable generating flags that allow us to obtain a prefixed distance value and code sizes as large as possible, even when it is necessary to take unions of orbits.

References

1. Ahlswede, R.; Cai, N.; Li, R.; Yeung, R.W. Network Information Flow. *IEEE Trans. Inf. Theory* **2000**, *46*, 1204–1216. [CrossRef]
2. Koetter, R.; Kschischang, F. Coding for Errors and Erasures in Random Network Coding. *IEEE Trans. Inf. Theory* **2008**, *54*, 3579–3591. [CrossRef]
3. Trautmann, A.-L.; Rosenthal, J. Constructions of Constant Dimension Codes. In *Network Coding and Subspace Designs*; Greferath, M., Pavčević, M., Silberstein, N., Vázquez-Castro, M., Eds.; E-Springer International Publishing AG: Cham, Switzerland, 2018; pp. 25–42.
4. Trautmann, A.-L.; Manganiello, F.; Rosenthal, J. Orbit Codes: A New Concept in the Area of Network Coding. In Proceedings of the IEEE Information Theory Workshop, Dublin, Ireland, 30 August–3 September 2010; pp. 1–4.
5. Zhao, W.; Tang, X. A Characterization of Cyclic Subspace Codes via Subspace Polynomials. *Finite Fields Their Appl.* **2019**, *57*, 1–12. [CrossRef]
6. Ben-Sasson, E.; Etzion, T.; Gabizon, A.; Raviv, N. Subspace Polynomials and Cyclic Subspace Codes. *IEEE Trans. Inf. Theory* **2016**, *62*, 1157–1165. [CrossRef]
7. Chen, B.; Liu, H. Constructions of Cyclic Constant Dimension Codes. *Des. Codes Cryptogr.* **2018**, *86*, 1267–1279. [CrossRef]
8. Etzion, T.; Vardy, A. Error-Correcting Codes in Projective Space. *IEEE Trans. Inf. Theory* **2011**, *57*, 1165–1173. [CrossRef]
9. Gluesing-Luerssen, H.; Morrison, K.; Troha, C. Cyclic Orbit Codes and Stabilizer Subfields. *Adv. Math. Commun.* **2015**, *9*, 177–197. [CrossRef]
10. Otal, K.; Ozbudak, F. Cyclic Subspace Codes via Subspace Polynomials. *Des. Codes Cryptogr.* **2017**, *85*, 191–204. [CrossRef]
11. Roth, R.M.; Raviv, N.; Tamo, I. Construction of Sidon Spaces With Applications to Coding. *IEEE Trans. Inf. Theory* **2018**, *64*, 4412–4422. [CrossRef]
12. Trautmann, A.-L.; Manganiello, F.; Braun, M.; Rosenthal, J. Cyclic Orbit Codes. *IEEE Trans. Inf. Theory* **2013**, *59*, 7386–7404. [CrossRef]
13. Nóbrega, R.W.; Uchôa-Filho, B.F. Multishot Codes for Network Coding: Bounds and a Multilevel Construction. In Proceedings of the 2009 IEEE International Symposium on Information Theory, Proceedings (ISIT), Seoul, Korea, 28 June–3 July 2009; pp. 428–432. [CrossRef]
14. Liebhold, D.; Nebe, G.; Vázquez-Castro, A. Network Coding with Flags. *Des. Codes Cryptogr.* **2018**, *86*, 269–284.
15. Alonso-González, C.; Navarro-Pérez, M.A. Consistent Flag Codes. *Mathematics* **2020**, *8*, 2243. [CrossRef]
16. Alonso-González, C.; Navarro-Pérez, M.A. Cyclic Orbit Flag Codes. *arXiv* **2021**, arXiv:2102.00867. [CrossRef]
17. Alonso-González, C.; Navarro-Pérez, M.A.; Soler-Escrivà, X. An Orbital Construction of Optimum Distance Flag Codes. *Finite Fields Their Appl.* **2021**, *73*, 101861.
18. Alonso-González, C.; Navarro-Pérez, M.A.; Soler-Escrivà, X. Flag Codes: Distance Vectors and Cardinality Bounds. *arXiv* **2021**, arXiv:2111.00910. [CrossRef]

19. Alonso-González, C.; Navarro-Pérez, M.A.; Soler-Escrivà, X. Flag Codes from Planar Spreads in Network Coding. *Finite Fields Their Appl.* **2020**, *68*, 101745.
20. Kurz, S. Bounds for Flag Codes. *Des. Codes Cryptogr.* **2021**, *89*, 2759–2785. [CrossRef]
21. Navarro-Pérez, M.A.; Soler-Escrivà, X. Flag Codes of Maximum Distance and Constructions using Singer Groups. *arXiv* **2021**, arXiv:2109.00270. [CrossRef]
22. Alonso-González, C.; Navarro-Pérez, M.A.; Soler-Escrivà, X. Optimum Distance Flag Codes from Spreads via Perfect Matchings in Graphs. *J. Algebr. Comb.* **2021**, *54*, 1279–1297.
23. Segre, B. Teoria di Galois, Fibrazioni Proiettive e Geometrie non Desarguesiane. *Ann. Mat. Pura Appl.* **1964**, *64*, 1–76. [CrossRef]
24. Gorla, E.; Manganiello, F.; Rosenthal, J. An Algebraic Approach for Decoding Spread Codes. *Adv. Math. Commun.* **2012**, *6*, 443–466. [CrossRef]
25. Manganiello, F.; Gorla, E.; Rosenthal, J. Spread Codes and Spread Decoding in Network Coding. In Proceedings of the 2008 IEEE International Symposium on Information Theory (ISIT), Toronto, ON, Canada, 6–11 July 2008; pp. 851–855. [CrossRef]
26. Manganiello, F.; Trautmann, A.-L. Spread Decoding in Extension Fields. *Finite Fields Their Appl.* **2014**, *25*, 94–105.
27. Rosenthal, J.; Trautmann, A.-L. A Complete Characterization of Irreducible Cyclic Orbit Codes and their Plücker Embedding. *Des. Codes Cryptogr.* **2013**, *66*, 275–289. [CrossRef]
28. Manganiello, F.; Trautmann, A.-L.; Rosenthal, J. 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, Russia, 31 July–5 August 2011; pp. 1916–1920. [CrossRef]