## MULTI-ORBIT CYCLIC SUBSPACE CODES AND LINEAR SETS

FERDINANDO ZULLO

To the beloved memory of my grandmother Elena.

ABSTRACT. Cyclic subspace codes gained a lot of attention especially because they may be used in random network coding for correction of errors and erasures. Roth, Raviv and Tamo in 2018 established a connection between cyclic subspace codes (with certain parameters) and Sidon spaces. These latter objects were introduced by Bachoc, Serra and Zémor in 2017 in relation with the linear analogue of Vosper's Theorem. This connection allowed Roth, Raviv and Tamo to construct large classes of cyclic subspace codes with one or more orbits. In this paper we will investigate cyclic subspace codes associated to a set of Sidon spaces, that is cyclic subspace codes with more than one orbit. Moreover, we will also use the geometry of linear sets to provide some bounds on the parameters of a cyclic subspace code. Conversely, cyclic subspace codes are used to construct families of linear sets which extend a class of linear sets recently introduced by Napolitano, Santonastaso, Polverino and the author. This yields large classes of linear sets with a special pattern of intersection with the hyperplanes, defining rank metric and Hamming metric codes with only three distinct weights.

### 1. INTRODUCTION

Let k be a non-negative integer with  $k \leq n$ , the set of all k-dimensional  $\mathbb{F}_q$ -subspaces of  $\mathbb{F}_{q^n}$ , viewed as an  $\mathbb{F}_q$ -vector space, forms a **Grassmannian space** over  $\mathbb{F}_q$ , which is denoted by  $\mathcal{G}_q(n, k)$ . A **constant dimension subspace code** is a subset C of  $\mathcal{G}_q(n, k)$  endowed with the metric defined as follows

$$d(U,V) = \dim_{\mathbb{F}_q}(U) + \dim_{\mathbb{F}_q}(V) - 2\dim_{\mathbb{F}_q}(U \cap V),$$

where  $U, V \in \mathcal{G}_q(n, k)$ . This metric is also known as **subspace metric**. Subspace codes have been recently used for the error correction in random network coding, see [25]. The first class of subspace codes studied was the one introduced in [16], which is known as **cyclic subspace codes**. A subspace code  $C \subseteq \mathcal{G}_q(n, k)$  is said to be **cyclic** if for every  $\alpha \in \mathbb{F}_{q^n}^*$  and every  $V \in C$  then  $\alpha V \in C$ .

Let  $V \in \mathcal{G}_q(n,k)$ , the **orbit** of V is the set  $C_V = \{\alpha V : \alpha \in \mathbb{F}_{q^n}^*\}$ , and its size is  $(q^n - 1)/(q^t - 1)$ , for some t which divides n. More precisely,

**Theorem 1.1.** [33, Theorem 1] Let U be a k-dimensional  $\mathbb{F}_q$ -subspace of  $\mathbb{F}_{q^n}$ . Then  $\mathbb{F}_{q^d}$  is the largest field such that U is also an  $\mathbb{F}_{q^d}$ -subspace if and only if the orbit size of U is  $\frac{q^n-1}{a^d-1}$ .

In particular, every orbit of a subspace  $V \in \mathcal{G}_q(n,k)$  defines a cyclic subspace code of size  $(q^n - 1)/(q^t - 1)$ , for some  $t \mid n$ . Assume k > 1. Clearly, a cyclic subspace code generated by an orbit of a subspace V with size  $(q^n - 1)/(q - 1)$  has minimum distance at most 2k - 2 and in [41]

FERDINANDO ZULLO, Dipartimento di Matematica e Fisica, Università degli Studi della Campania "Luigi Vanvitelli", Viale Lincoln, 5, I–81100 Caserta, Italy

 $E\text{-}mail\ address: \texttt{ferdinando.zullo@unicampania.it}.$ 

 $<sup>2020\</sup> Mathematics\ Subject\ Classification.\ 11T99;\ 11T06;\ 11T71;\ 94B05.$ 

Key words and phrases. Cyclic subspace code; Sidon space; linear set; projection map; linearized polynomial.

Trautmann, Manganiello, Braun and Rosenthal conjectured the existence of a cyclic code of size  $\frac{q^n-1}{q-1}$  in  $\mathcal{G}_q(n,k)$  and minimum distance 2k-2 for every positive integers n, k such that  $k \leq n/2$ .

<sup>*q*</sup> Ben-Sasson, Etzion, Gabizon and Raviv in [7] used subspace polynomials to generate cyclic subspace codes with size  $\frac{q^n-1}{q-1}$  and minimum distance 2k-2, proving that the conjecture is true for any given k and infinitely many values of n. Such result was then improved in [33] (see also [7,33,38]). Finally, the conjecture was solved in [37] for most of the cases, by making use of *Sidon spaces*. They were originally introduced in [3], as an important tool to prove the linear analogue of Vosper's Theorem, which analyzes the equality in the linear analouge of Kneser's theorem proved in [4,21].

An  $\mathbb{F}_q$ -subspace U of  $\mathbb{F}_{q^n}$  is called a **Sidon space** if the product of any two elements of U has a unique factorization over U, up to multiplying by some elements in  $\mathbb{F}_q$ . More precisely, U is a Sidon space if for all nonzero  $a, b, c, d \in U$ , if ab = cd, then

$$\{a\mathbb{F}_q, b\mathbb{F}_q\} = \{c\mathbb{F}_q, d\mathbb{F}_q\},\$$

where if  $e \in \mathbb{F}_{q^n}$  then  $e\mathbb{F}_q = \{e\lambda \colon \lambda \in \mathbb{F}_q\}$ . Sidon spaces may be seen as the *q*-analogue of **Sidon** set, that is a subset *A* in a commutative group with the property that the sums of two elements of *A* are all distinct except when they coincide because of commutativity. The name comes back to Simon Szidon and was given by Erdős in [15]. Sidon sets have been then intensively studied in several contexts, see e.g. [2, 10, 11]. For a survey the reader is referred to [9].

The connection between Sidon spaces and cyclic subspace codes is the following.

**Theorem 1.2.** [37, Lemma 34] Let U be an  $\mathbb{F}_q$ -subspace of  $\mathbb{F}_{q^n}$  of dimension k. Then  $C_U$  is a cyclic subspace code of size  $\frac{q^n-1}{q-1}$  and minimum distance 2k-2 if and only if U is a Sidon space.

In this paper we deal with cyclic subspace codes containing more than one orbit, which we will refer to as **multi-orbit cyclic subspace codes**. More precisely, our aim is to study the following codes. Let  $U_1, \ldots, U_r$  be  $\mathbb{F}_q$ -subspaces of dimension k in  $\mathbb{F}_{q^n}$  and let

(1) 
$$C = \bigcup_{i \in \{1, \dots, r\}} C_{U_i} \subseteq \mathcal{G}_q(n, k)$$

with minimum distance 2k - 2 and of size  $r\frac{q^n-1}{q-1}$ . These codes have the same minimum distance of the codes associated with Sidon spaces but they are larger, and hence more interesting from a coding theory point of view. See [17, 32, 34] for recent constructions.

The code C is uniquely defined by the subspaces  $U_1, \ldots, U_r$  and therefore we give the following two definitions. The set  $\{U_1, \ldots, U_r\}$  of a cyclic subspace code as in (1) will said to be a set of **representatives** of C, whereas if also its minimum distance is 2k - 2 we will call it a **multi-Sidon space**, in connection with the correspondence between cyclic subspace codes with these parameters with one orbit and Sidon spaces. Equivalently, the set  $\{U_1, \ldots, U_r\}$  is a multi-Sidon space if

$$\dim_{\mathbb{F}_q}(U_i \cap \alpha U_j) \le 1$$

for every  $\alpha \in \mathbb{F}_{q^n}$  and  $i, j \in \{1, \ldots, r\}$  with  $i \neq j$  and for every  $\alpha \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$  if i = j.

Some of the results we will show do not require that all the subspaces have the same dimension k. In this case, the associated code will be still cyclic but not a constant dimension code.

In this paper, we first investigate multi-orbit cyclic subspace codes by analyzing their properties and providing characterizations, involving the Cartesian product of a set of representatives. Then we derive a canonical form for multi-orbit cyclic codes in  $\mathcal{G}_q(n, n/2)$  (and hence of multi-Sidon spaces), when n is even, through some linearized polynomials jointly with direct conditions that can be checked to establish whether or not a set of subspaces is a multi-Sidon space. Then we used these conditions to find a family of multi-orbit cyclic subspace codes defined by linearized monomials, extending the family presented by Roth, Raviv and Tamo in [37], and we can also solve the equivalence issue among the codes belonging to this larger family. We gave a geometric interpretation of the Sidon property in terms of linear sets. This connection yields some new bounds on the parameters involved in a multi-Sidon space and hence on the associated subspace code. With the aid of multi-orbit cyclic subspace codes, we study a special class of linear sets in  $PG(r-1,q^n)$  which may be defined by r points in independent position, which naturally extends those investigated in [29] with Napolitano, Santonastaso and Polverino. In particular, we provide bounds on the rank of such linear sets and we then concentrate our attention on those that have maximum rank. Constructions of such linear sets can be obtained by using multi-orbit cyclic subspace codes and we then analyze the equivalence issue among those. Moreover, when such linear sets have rank n they can be described by projection maps, as shown in the appendix. Some of these properties are natural generalization of the results in [29], but unlike what happens in the projective line, the duals of the above linear sets of maximum rank have a special pattern of intersection with the hyperplanes. This means that such linear sets can be used to define linear rank metric codes and linear Hamming metric codes with only three weights (yielding also to almost MRD codes) and for which one can completely determine their weight distribution. We conclude the paper by showing possible problems that could be of interest for the reader.

### 2. Preliminaries

2.1. Linearized polynomials. Let s be a positive integer such that gcd(s, n) = 1. A  $q^s$ -linearized polynomial (for short  $q^s$ -polynomial) over  $\mathbb{F}_{q^n}$  is a polynomial of the form

$$f(x) = \sum_{i=0}^{\ell} a_i x^{q^{is}},$$

where  $a_i \in \mathbb{F}_{q^n}$  and  $\ell$  is a positive integer. Furthermore, if  $a_\ell \neq 0$  we say that  $\ell$  is the  $q^s$ -degree of f(x). We will denote by  $\mathcal{L}_{n,s}$  the set of all  $q^s$ -polynomials over  $\mathbb{F}_{q^n}$  with  $q^s$ -degree less than n (or  $\mathcal{L}_n$  if s = 1). Together with the classical sum of polynomials, the composition modulo  $x^{q^n} - x$  and the scalar multiplication by an element in  $\mathbb{F}_q$ ,  $\mathcal{L}_{n,s}$  forms an  $\mathbb{F}_q$ -algebra isomorphic to the algebra of  $\mathbb{F}_q$ -linear endomorphisms of  $\mathbb{F}_{q^n}$ . For this reason, we shall identify the elements of  $\mathcal{L}_{n,s}$  with the endomorphisms of  $\mathbb{F}_{q^n}$  they represent and hence we will also speak of kernel and rank of a  $q^s$ -polynomial. Clearly, the kernel of  $f(x) \in \mathcal{L}_{n,s}$  coincides with the set of the roots of f(x) over  $\mathbb{F}_{q^n}$ .

We now recall an important result on linearized polynomials which will play a crucial role in the construction of examples of cyclic subspace codes. This puts together [23, Lemma 3.2] and [20, Theorem 10] (see also [19, Theorem 5]).

## Theorem 2.1. Consider

$$f(x) = a_0 x + a_1 x^{q^s} + \dots + a_{k-1} x^{q^{s(k-1)}} + a_k x^{q^{sk}} \in \mathcal{L}_{n,s},$$

with  $k \leq n-1$  and let  $a_0, a_1, \ldots, a_k$  be elements of  $\mathbb{F}_{q^n}$  not all of them zero. Then

$$\dim_{\mathbb{F}_a}(\ker(f(x))) \le k.$$

Moreover, if  $\dim_{\mathbb{F}_q}(\ker(f(x))) = k$  then  $N_{q^n/q}(a_0) = (-1)^{nk} N_{q^n/q}(a_k)$ .

An important example of a linearized polynomial is given by the trace function, which can be defined as

$$\operatorname{Tr}_{q^n/q}(x) = x + x^q + \ldots + x^{q^{n-1}}.$$

For more details on linearized polynomials we refer to [27, Chapter 3, Section 4].

2.2. Linear sets. A point set L of  $\Lambda = PG(V, \mathbb{F}_{q^n}) = PG(r-1, q^n)$  is said to be an  $\mathbb{F}_q$ -linear set of  $\Lambda$  of rank k if it is defined by the non-zero vectors of a k-dimensional  $\mathbb{F}_q$ -vector subspace U of V, i.e.

$$L = L_U := \{ \langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{\mathbf{0}\} \}.$$

We denote the rank of an  $\mathbb{F}_q$ -linear set  $L_U$  by  $\operatorname{Rank}(L_U)$ . For any subspace  $S = \operatorname{PG}(Z, \mathbb{F}_{q^n})$  of  $\Lambda$ , the **weight** of S in  $L_U$  is defined as  $w_{L_U}(S) = \dim_{\mathbb{F}_q}(U \cap Z)$ . If  $N_i$  denotes the number of points of  $\Lambda$  having weight  $i \in \{0, \ldots, k\}$  in  $L_U$ , the following relations hold:

$$|L_U| \le \frac{q^k - 1}{q - 1},$$

$$|L_U| = N_1 + \ldots + N_k,$$

(4) 
$$N_1 + N_2(q+1) + \ldots + N_k(q^{k-1} + \ldots + q + 1) = q^{k-1} + \ldots + q + 1.$$

We also recall that two linear sets  $L_U$  and  $L_W$  of  $PG(r-1, q^n)$  are said to be  $P\Gamma L$ -equivalent (or simply equivalent) if there is an element  $\varphi$  in  $P\Gamma L(r, q^n)$  such that  $L_U^{\varphi} = L_W$ . In general, it is very hard to determine whether or not two linear sets are projective equivalent, see e.g. [8, 12, 13].

Another notion that we will need is that of the dual of a linear set. Let  $L_U$  be an  $\mathbb{F}_q$ -linear set of rank k in  $\mathrm{PG}(V, \mathbb{F}_{q^n}) = \mathrm{PG}(r-1, q^n)$ . Let  $\sigma: V \times V \to \mathbb{F}_{q^n}$  be a nondegenerate reflexive sesquilinear form on the  $\mathbb{F}_{q^n}$ -vector space V and consider  $\sigma' = \mathrm{Tr}_{q^n/q} \circ \sigma$ , which is a nondegenerate reflexive sesquilinear form on V seen as an  $\mathbb{F}_q$ -vector space of dimension rn. Then we may consider  $\bot$  and  $\bot'$  as the orthogonal complement maps defined by  $\sigma$  and  $\sigma'$ , respectively, and  $\tau$  and  $\tau'$  as the polarities of  $\mathrm{PG}(V, \mathbb{F}_{q^n})$  and  $\mathrm{PG}(V, \mathbb{F}_q)$  defined by  $\bot$  and  $\bot'$ , respectively. Then  $L_U^{\tau} = L_{U^{\perp'}}$  is an  $\mathbb{F}_q$ -linear set in  $\mathrm{PG}(V, \mathbb{F}_{q^n})$  of rank rn - k that is called the **dual linear set of**  $L_U$  with respect to the polarity  $\tau$ . As proved in [35, Proposition 2.5], this linear set does not depend on the polarity  $\tau$ . Indeed, let  $\sigma_1: V \times V \to \mathbb{F}_{q^n}$  be a nondegenerate reflexive sesquilinear form on the  $\mathbb{F}_{q^n}$ -vector space V and let  $\tau_1$  the related polarity, then  $L_U^{\tau}$  and  $L_U^{\tau_1}$  are  $\mathrm{P\GammaL}(2, q^n)$ -equivalent; see also [28].

Moreover, the following result relates the weights of the subspaces with respect to the linear set and its dual.

**Proposition 2.2.** [35, Property 2.6] Let  $L_U$  be an  $\mathbb{F}_q$ -linear set of rank k in  $PG(V, \mathbb{F}_{q^n}) = PG(r - 1, q^n)$ . If  $S = PG(Z, \mathbb{F}_{q^n})$  is an s-dimensional projective subspace then

$$w_{L_{U}^{\tau}}(S^{\tau}) - w_{L_{U}}(S) = rn - k - (s+1)n$$

For further details on linear sets see [26, 35].

#### 3. Structure and properties of multi-orbit cyclic subspace codes

In this section we will analyze properties of multi-orbit cyclic subspace codes, paying special attention to their algebraic description. Interesting results have been proved in this direction for the case of Sidon spaces.

Let U and V be two  $\mathbb{F}_q$ -subspaces of  $\mathbb{F}_{q^n}$ . Denote by  $\langle U^2 \rangle$  the  $\mathbb{F}_q$ -span of  $\{st: s, t \in U\}, U^{-1} = \{u^{-1}: u \in U \setminus \{0\}\}$  and  $U \cdot V = \{uv: u \in U, v \in V\}.$ 

Bachoc, Serra and Zémor proved a lower bound on the dimension of a Sidon space in [3, Theorem 18] and hence the following holds.

**Theorem 3.1.** If U is a Sidon space in  $\mathbb{F}_{q^n}$  of dimension  $k \geq 3$ , then

$$2k \leq \dim_{\mathbb{F}_q}(\langle U^2 \rangle) \leq \binom{k+1}{2}.$$

Clearly, this result implies that if a cyclic subspace code  $C_U$  has minimum distance 2k-2, where  $k = \dim_{\mathbb{F}_q}(U)$ , then  $2k \leq n$ .

We can hence apply the above result to all the subspaces of a multi-Sidon space, obtaining the following bounds.

**Corollary 3.2.** Let  $\{U_1, \ldots, U_r\}$  is a multi-Sidon space of  $\mathbb{F}_{q^n}$ . Let  $k_i = \dim_{\mathbb{F}_q}(U_i) \geq 3$  for any  $i \in \{1, ..., r\}$ . Then

$$2\sum_{i=1}^{r} k_{i} \leq \dim_{\mathbb{F}_{q}}(\langle U_{1}^{2} \rangle \times \ldots \times \langle U_{r}^{2} \rangle) \leq \sum_{i=1}^{r} \binom{k_{i}+1}{2}.$$

In particular,  $k_i \leq n/2$  for each  $i \in \{1, \ldots, r\}$ .

A multi-Sidon space  $\{U_1, \ldots, U_r\}$  of  $\mathbb{F}_{q^n}$ , with  $k_i = \dim_{\mathbb{F}_q}(U_i)$  for any  $i \in \{1, \ldots, r\}$ , is said to be **maximum** if n is even and  $k_i = n/2$  for every  $i \in \{1, \ldots, r\}$ . The interest for maximum multi-Sidon spaces arise from the fact that the associated codes are those with the largest minimum distance, that is n-2.

In [37], it has been described the property of being a Sidon space with an algebraic flavour, using the uniqueness of the factorization of the product of two elements which are in two distinct subspaces.

**Lemma 3.3.** [37, Lemma 36] Let U, V be two distinct  $\mathbb{F}_q$ -subspaces of dimension k of  $\mathbb{F}_{q^n}$ . Then the following conditions are equivalent

- (1)  $\dim_{\mathbb{F}_q}(U \cap \alpha V) \leq 1$ , for any  $\alpha \in \mathbb{F}_{q^n}$ ;
- (2) For any nonzero  $a, c \in U$  and nonzero  $b, d \in V$ , the equality ab = cd implies that  $a\mathbb{F}_q = c\mathbb{F}_q$ and  $b\mathbb{F}_q = d\mathbb{F}_q$ .

Lemma 3.3 can be also applied to a set of subspaces  $\mathcal{U}$ , extending the uniqueness of the factorization of the product of two elements which are in two distinct subspaces in  $\mathcal{U}$ .

**Corollary 3.4.** Let  $\{U_1, \ldots, U_r\}$  be a set of  $\mathbb{F}_q$ -subspaces of  $\mathbb{F}_{q^n}$ . Then the following conditions are equivalent

- (1)  $\dim_{\mathbb{F}_q}(U_i \cap \alpha U_j) \leq 1$ , for any  $\alpha \in \mathbb{F}_{q^n}$  and  $i, j \in \{1, \ldots, r\}$  with  $i \neq j$ ;
- (2) For any nonzero  $a, c \in U_i$  and nonzero  $b, d \in U_j$ , the equality ab = cd implies that  $a\mathbb{F}_q = c\mathbb{F}_q$ and  $b\mathbb{F}_q = d\mathbb{F}_q$ , for any  $i, j \in \{1, \ldots, r\}$  with  $i \neq j$ .

The property of being a multi-Sidon space is inherited by the Cartesian product of such subspaces as follows. To this aim, let  $\mathbf{e}_i \in \mathbb{F}_{q^n}^r$  be the vector whose *i*-th component is 1 and all the others are zero.

**Theorem 3.5.** Let  $\{U_1, \ldots, U_r\}$  be a set of  $\mathbb{F}_q$ -subspaces of  $\mathbb{F}_{q^n}$ . Then the following are equivalent:

- i) the  $\mathbb{F}_q$ -subspace  $U = U_1 \times \ldots \times U_r$  of  $\mathbb{F}_{q^n}^r$  is such that  $\dim_{\mathbb{F}_q}(U \cap \langle \mathbf{v} \rangle_{\mathbb{F}_{q^n}}) \leq 1$  for any  $\mathbf{v} \in \mathbb{F}_{q^n}^r$ such that  $\langle \mathbf{v} \rangle_{\mathbb{F}_{q^n}} \notin \{ \langle \mathbf{e}_i \rangle_{\mathbb{F}_{q^n}} : i \in \{1, \dots, r\} \};$ ii)  $U_i \cdot U_i^{-1} \cap U_j \cdot U_j^{-1} = \mathbb{F}_q$  for every  $i \neq j;$
- iii)  $\dim_{\mathbb{F}_q}(U_i \cap \alpha U_j) \leq 1$ , for every  $\alpha \in \mathbb{F}_{q^n}$  and  $i, j \in \{1, \ldots, r\}$  such that  $i \neq j$ .

*Proof.* Consider a nonzero  $\lambda \in U_i \cdot U_i^{-1} \cap U_j \cdot U_j^{-1}$  for some  $i, j \in \{1, \ldots, r\}$  with  $i \neq j$  and assume that i) holds. Then there exist  $x, x' \in U_i$  and  $y, y' \in U_j$  such that

(5) 
$$\lambda = \frac{x}{x'} = \frac{y}{y'}.$$

If  $\lambda$  were not in  $\mathbb{F}_q$ , then we would have a contradiction. Indeed, consider the vector  $\mathbf{u}$  whose *i*-th entry is x, *j*-th entry is y and all the other entries are zero and the vector  $\mathbf{u}'$  whose *i*-th entry is x', *j*-th entry is y' and all the other entries are zero, whereas x, y, x', y' are nonzero. By (5) we obtain  $\mathbf{u} = \lambda \mathbf{u}'$ , a contradiction to a). Now, suppose that ii) holds. Let  $\mathbf{v} \in U$  such that  $\langle \mathbf{v} \rangle_{\mathbb{F}_{q^n}} \notin \{ \langle \mathbf{e}_i \rangle_{\mathbb{F}_{q^n}} : i \in \{1, \ldots, r\} \}$  and  $\dim_{\mathbb{F}_q}(U \cap \langle \mathbf{v} \rangle_{\mathbb{F}_{q^n}}) \geq 2$ . Then there exist  $i, j \in \{1, \ldots, r\}$  such that  $v_i \neq 0$  and  $v_j \neq 0$  and  $\rho \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$  such that  $\rho \mathbf{v} = \mathbf{u}$  with  $\mathbf{u} \in U$ . In particular  $u_i, u_j$  are non zero and

$$\rho = \frac{u_i}{v_i} = \frac{u_j}{v_j} \in U_i \cdot U_i^{-1} \cap U_j \cdot U_j^{-1},$$

and hence we get a contradiction since  $\rho \notin \mathbb{F}_q$ . Therefore, we have proved that i) and ii) are equivalent. We now conclude the proof by proving the equivalence between ii) and iii). Suppose that  $U_i \cdot U_i^{-1} \cap U_j \cdot U_j^{-1} = \mathbb{F}_q$  for every  $i, j \in \{1, \ldots, r\}$  with  $i \neq j$ . By contradiction, assume the existence of  $\alpha \in \mathbb{F}_{q^n}^*$  such that  $\dim_{\mathbb{F}_q}(U_i \cap \alpha U_j) \geq 2$  for some  $i, j \in \{1, \ldots, r\}$  with  $i \neq j$ . Let  $a_1$ and  $a_2$  be two  $\mathbb{F}_q$ -linearly independent elements in  $U_i \cap \alpha U_j$ . Moreover, since  $a_1, a_2 \in \alpha U_j$ , there exist  $b_1, b_2 \in U_j \setminus \{0\}$  such that  $a_1 = \alpha b_1$  and  $a_2 = \alpha b_2$ , so that

$$a_1 a_2^{-1} = b_1 b_2^{-1} \in U_i \cdot U_i^{-1} \cap U_j \cdot U_j^{-1}$$

and hence, by assumption,  $a_1 a_2^{-1} \in \mathbb{F}_q$ , which is a contradiction. Now, assume that  $\dim_{\mathbb{F}_q}(U_i \cap \alpha U_j) \leq 1$ , for every  $\alpha \in \mathbb{F}_{q^n}$  and  $i, j \in \{1, \ldots, r\}$  such that  $i \neq j$ . Let  $\lambda \in U_i \cdot U_i^{-1} \cap U_j \cdot U_j^{-1} \setminus \{0\}$ . Then there exist  $a, c \in U_i \setminus \{0\}$  and  $b, d \in U_j \setminus \{0\}$  such that  $\lambda = ac^{-1} = db^{-1}$ . Then  $a, c \in U_i \cap \beta U_j$  where  $\beta = a/d = c/b$ . Since  $\dim_{\mathbb{F}_q}(U_i \cap \beta U_j) \leq 1$ , it follows that  $\lambda = ac^{-1} \in \mathbb{F}_q$ .

The above theorem give equivalent conditions to the property of being a multi-Sidon space when we consider a set of Sidon spaces. This result will also be very important in studying the equivalence among linear sets defined by r independent points as we will see later.

We can now describe a canonical form of cyclic subspace codes with minimum distance n-2.

**Theorem 3.6.** Let  $n = 2k \ge 4$ , suppose that  $\mathcal{U} = \{U_1, \ldots, U_r\}$  is a set of  $\mathbb{F}_q$ -subspaces in  $\mathbb{F}_{q^n}$  with dimension k and let  $C = \bigcup_{i=1}^r C_{U_i}$ . Then there exists a set of representatives for C

$$\{W_{f_1,\eta_1},\ldots,W_{f_r,\eta_r}\},\$$

where  $f_1(x), \ldots, f_r(x) \in \mathcal{L}_k, \eta_1, \ldots, \eta_r \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}$  and

$$W_{f_i,\eta_i} = \{ x + \eta_i f_i(x) \colon x \in \mathbb{F}_{q^k} \},\$$

for every  $i \in \{1, \ldots, r\}$ . Let  $\eta_i = A_{i,j}\eta_j + B_{i,j}$  and  $\eta_i^2 = a_i\eta_i + b_i$  with  $A_{i,j}, B_{i,j}, a_i, b_i \in \mathbb{F}_{q^k}$ for any  $i, j \in \{1, \ldots, r\}$ . Moreover, the minimum distance of C is n-2 if and only if for every  $i, j \in \{1, \ldots, r\}$  and  $\alpha_0, \alpha_1 \in \mathbb{F}_{q^k}$  with  $(\alpha_0, \alpha_1) \neq (0, 0)$  the following linearized polynomial in  $\mathcal{L}_k$ 

$$F_{i,j}(x) = f_i(\alpha_0 x) + f_i(\alpha_1 A_{j,i} b_i f_j(x)) + f_i(\alpha_0 B_{j,i} f_j(x)) - \alpha_1 x - \alpha_0 A_{j,i} f_j(x) - \alpha_1 A_{j,i} a_i f_j(x) - \alpha_1 B_{j,i} f_j(x) + f_i(\alpha_0 B_{j,i} f_j(x)) - \alpha_1 x - \alpha_0 A_{j,i} f_j(x) - \alpha_1 A_{j,i} a_i f_j(x) - \alpha_1 B_{j,i} f_j(x) + f_i(\alpha_0 B_{j,i} f_j(x)) - \alpha_1 x - \alpha_0 A_{j,i} f_j(x) - \alpha_1 A_{j,i} a_i f_j(x) - \alpha_1 B_{j,i} f_j(x) + f_i(\alpha_0 B_{j,i} f_j(x)) - \alpha_1 x - \alpha_0 A_{j,i} f_j(x) - \alpha_1 A_{j,i} a_i f_j(x) - \alpha_1 B_{j,i} f_j(x) - \alpha_1 B_{j,$$

$$F_{i,i}(x) = f_i(\alpha_0 x) + f(\alpha_1 b_i f_i(x)) - \alpha_1 x - \alpha_0 f_j(x) - \alpha_1 a_i f_i(x)$$

if i = j, is either the zero polynomial or it has at most q roots over  $\mathbb{F}_{a^k}$ .

*Proof.* Let  $\eta_1, \ldots, \eta_r \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}$ . Clearly,  $\{1, \eta_i\}$  is an  $\mathbb{F}_{q^k}$ -basis of  $\mathbb{F}_{q^n}$  for every *i*. For each  $i \in \{1, \ldots, r\}$ , there exists  $\lambda_i \in \mathbb{F}_{q^n}^*$  such that

$$\lambda_i U_i \cap \eta_i \mathbb{F}_{q^k} = \{0\}.$$

By contradiction assume that  $\lambda U_i \cap \eta_i \mathbb{F}_{q^k} \neq \{0\}$  for each  $\lambda \in \mathbb{F}_{q^n}^*$ . Consider the Desarguesian spread  $\mathcal{D} = \{\langle \mathbf{v} \rangle_{\mathbb{F}_{q^n}} : \mathbf{v} \in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \setminus \{\mathbf{0}\}\} = \{\langle (1,\xi) \rangle_{\mathbb{F}_{q^n}} : \xi \in \mathbb{F}_{q^n}\} \cup \{\langle (0,1) \rangle_{\mathbb{F}_{q^n}}\}$  of  $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ . The  $\mathbb{F}_q$ -subspace  $U_i \times \eta_i \mathbb{F}_{q^k} = \{(a,b) : a \in U_i, b \in \eta_i \mathbb{F}_{q^k}\}$  meets all the elements of  $\mathcal{D}$  in at least one non-zero vector. Indeed, by the hypothesis

$$\{b/a \colon a \in U_i \setminus \{0\}, b \in \eta_i \mathbb{F}_{q^k}\} = \mathbb{F}_{q^n}$$

so that for every  $\xi \in \mathbb{F}_{q^n}$  there exist  $a \in U_i \setminus \{0\}$  and  $b \in \eta_i \mathbb{F}_{q^k}$  such that  $\xi = b/a$  and so

$$\langle (1,\xi) \rangle_{\mathbb{F}_{q^n}} \cap (U_i \times \eta_i \mathbb{F}_{q^k}) \supseteq \langle (a,b) \rangle_{\mathbb{F}_q}.$$

Clearly,  $\langle (0,1) \rangle_{\mathbb{F}_{q^n}} \cap (U_i \times \eta_i \mathbb{F}_{q^k}) = U_i$  and hence  $U_i \times \eta_i \mathbb{F}_{q^k}$  meets all the elements of  $\mathcal{D}$  in at least one non-zero vector. Since  $\dim_{\mathbb{F}_q}(U_i \times \eta_i \mathbb{F}_{q^k}) = n$  this is a contradiction, see e.g. [35, (3) Proposition 2.2]. Therefore, there exists  $\lambda_i \in \mathbb{F}_{q^n}^*$  such that

$$\lambda_i U_i \cap \eta_i \mathbb{F}_{q^k} = \{0\}.$$

This implies that for every  $i \in \{1, ..., r\}$ , since  $\{1, \eta_i\}$  is an  $\mathbb{F}_{q^k}$ -basis of  $\mathbb{F}_{q^n}$ , there exist r linearized polynomials  $f_i(x) \in \mathcal{L}_k$  such that

$$\lambda_i U_i = W_{f_i,\eta_i}.$$

Now, let  $i, j \in \{1, ..., r\}$  with  $i \neq j$  and consider  $w \in W_{f_i, \eta_i} \cap \alpha W_{f_j, \eta_j}$ , for some  $\alpha \in \mathbb{F}_{q^n}^*$ . Then there exist  $u, v \in \mathbb{F}_{q^k}$  such that

(6) 
$$w = u + \eta_i f_i(u) = \alpha(v + \eta_j f_j(v)).$$

Since  $\{1, \eta_i\}$  is an  $\mathbb{F}_{q^k}$ -basis of  $\mathbb{F}_{q^n}$ ,  $\eta_i^2 = a_i \eta_i + b_i$  and  $\eta_j = A_{j,i} \eta_i + B_{j,i}$ , we get that  $\alpha = \alpha_0 + \alpha_1 \eta_i$  for some  $\alpha_0, \alpha_1 \in \mathbb{F}_{q^k}$  and (6) may be rewritten as

$$\begin{cases} u = \alpha_0 v + \alpha_1 A_{j,i} b_i f_j(v) + \alpha_0 B_{j,i} f_j(v), \\ f_i(u) = \alpha_1 v + \alpha_0 A_{j,i} f_j(v) + \alpha_1 A_{j,i} a_i f_j(v) + \alpha_1 B_{j,i} f_j(v), \end{cases}$$

from which we get

$$f_i(\alpha_0 v) + f_i(\alpha_1 A_{j,i} b_i f_j(v)) + f_i(\alpha_0 B_{j,i} f_j(v)) = \alpha_1 v + \alpha_0 A_{j,i} f_j(v) + \alpha_1 A_{j,i} a_i f_j(v) + \alpha_1 B_{j,i} f_j(v).$$

The assertion then follows from the fact that the minimum distance of C is n-2 and noting that the above polynomial is the zero polynomial if and only if  $W_{f_i,\eta_i} = \alpha W_{f_j,\eta_j}$ , a contradiction to the fact that  $i \neq j$ . If i = j, the result can be obtained by repeating the previous argument (see also [29, Corollary 4.7]) noting that the the condition (6) gives rise to the following system

$$\begin{cases} u = \alpha_0 v + \alpha_1 b_i f_i(v), \\ f_i(u) = \alpha_1 v + \alpha_0 f_i(v) + \alpha_1 a_i f_i(v). \end{cases}$$

Remark 3.7. Clearly, since

$$\dim_{\mathbb{F}_q}(W_{f_i,\eta_i} \cap \alpha W_{f_j,\eta_j}) = \dim_{\mathbb{F}_q}(\alpha^{-1}W_{f_i,\eta_i} \cap W_{f_j,\eta_j})$$

for  $\alpha \in \mathbb{F}_{q^n}^*$ , we could just assume that in Theorem 3.6 the condition on the polynomials  $F_{i,j}(x)$  hold for every i, j with  $i \leq j$ .

In particular, the canonical form for a Sidon space in  $\mathbb{F}_{q^n}$  of dimension n/2 is the following.

**Corollary 3.8.** Let  $n = 2k \ge 4$  and let U be an  $\mathbb{F}_q$ -subspace of  $\mathbb{F}_{q^n}$  with dimension k. Then U is equivalent to  $W_{f,\eta} = \{x + \eta f(x) : x \in \mathbb{F}_{q^k}\}$ , where  $f(x) \in \mathcal{L}_k$  and  $\eta \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}$ . Let  $\eta^2 = a\eta + b$  with  $a, b \in \mathbb{F}_{q^k}$ . Then, U is a Sidon space if and only if for every  $\alpha_0, \alpha_1 \in \mathbb{F}_{q^k}$  with  $(\alpha_0, \alpha_1) \neq (0, 0)$  the following linearized polynomial in  $\mathcal{L}_k$ 

$$F(x) = f(\alpha_0 x) + f(\alpha_1 b f(x)) - \alpha_1 x - \alpha_0 f(x) - \alpha_1 a f(x)$$

is either the zero polynomial or it has at most q roots over  $\mathbb{F}_{q^k}$ .

Now we show some examples of multi-orbit cyclic subspace codes with minimum distance n-2, making use of Theorem 3.6.

**Theorem 3.9.** Let s be a positive integer coprime with  $k \ge 2$  and n = 2k, let  $\xi \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}$ and let  $f_i(x) = \mu_i x^{q^s} \in \mathcal{L}_k$  for  $i \in \{1, \ldots, r\}$  such that  $r \le q - 1$ ,  $N_{q^k/q}(\mu_i) \ne N_{q^k/q}(\mu_j)$  and  $N_{q^k/q}(\mu_i \mu_j \xi^{q^k+1}) \ne 1$  for every  $i \ne j$ . Then

$$C = \bigcup_{i=1}^{r} C_{W_{f_i},\xi}$$

is a cyclic subspace code of size  $r\frac{q^n-1}{q-1}$  and minimum distance n-2.

*Proof.* Let  $x^2 - ax - b$  be the minimal polynomial of  $\xi$  over  $\mathbb{F}_{q^k}$ . Clearly,  $b = -\xi^{q^k+1}$ . Let  $i, j \in \{1, \ldots, r\}$ , then the polynomials  $F_{i,j}(x)$  of Theorem 3.6 read as follows

$$F_{i,j}(x) = \mu_i \alpha_0^{q^s} x^{q^s} + \mu_i \alpha_1^{q^s} b^{q^s} \mu_j^{q^s} x^{q^{2s}} - \alpha_1 x - \alpha_0 \mu_j x^{q^s} - \alpha_1 a \mu_j x^{q^s},$$

since the  $\eta_i$ 's in Theorem 3.6 are chosen to be equal to  $\xi$  and hence  $A_{j,i} = 1$  and  $B_{j,i} = 0$ , for every i and j. If  $F_{i,j}(x)$  is not the zero polynomial, then it can be seen as  $q^s$ -polynomial with  $q^s$ -degree at most two. If the coefficient of  $x^{q^{2s}}$  is zero, then by Theorem 2.1 dim<sub> $\mathbb{F}_q$ </sub>(ker $(F_{i,j}(x))$ )  $\leq 1$ . If the coefficient of  $x^{q^{2s}}$  is non-zero and  $F_{i,j}(x)$  admits  $q^2$  roots, Theorem 2.1 implies that

$$\mathcal{N}_{q^k/q}(\mu_i \alpha_1^{q^s} \mu_j^{q^s} b^{q^s}) = \mathcal{N}_{q^k/q}(-\alpha_1),$$

a contradiction to the fact that  $N_{q^k/q}(\mu_i\mu_j\xi^{q^k+1}) \neq 1$  for every *i* and *j*. So, by Theorem 3.6 the assertion follows.

**Remark 3.10.** Note that in the above theorem r cannot reach q - 1 when  $q \ge 4$ . Indeed, suppose that r = q - 1, then

 $\{\mathbf{N}_{q^k/q}(\mu_i)\colon i\in\{1,\ldots,r\}\}=\mathbb{F}_q^*,$ 

and so when  $q \geq 4$ 

$$\{\mathbf{N}_{q^k/q}(\mu_i\mu_j)\colon i,j\in\{1,\ldots,r\}, i\neq j\}=\mathbb{F}_q^*.$$

Therefore,

$$\{ N_{q^k/q}(\mu_i \mu_j) N_{q^k/q}(\xi^{q^k+1}) \colon i, j \in \{1, \dots, r\}, i \neq j \} = \mathbb{F}_q^*,$$

and hence there exist  $i, j \in \{1, ..., r\}$  with  $i \neq j$  such that  $N_{q^k/q}(\mu_i \mu_j) N_{q^k/q}(\xi^{q^k+1}) = 1$ . If q = 3, r = 2 can be reached. Indeed, it is enough to take  $\mu_1, \mu_2 \in \mathbb{F}_{q^k}$  and  $\xi \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}$  such that  $N_{q^k/q}(\mu_1) = 1, N_{q^k/q}(\mu_2) = -1$  and  $N_{q^k/q}(\xi^{q^k+1}) = 1$ .

The first construction of cyclic codes with these parameters was given in [37]. In the above result we have extended it to the case s > 1. As we will see later, this yields to a much larger class of new codes. Choosing the  $\gamma_i$ 's as in the paper [37], we will extend [37, Lemma 38] as follows.

**Corollary 3.11.** For a prime power  $q \ge 3$  and a positive integer  $k \ge 2$ , let w be a primitive element of  $\mathbb{F}_{q^k}$  and let s be a positive integer such that gcd(s,k) = 1. Let  $b \in \mathbb{F}_{q^k}$  be such that the polynomial  $p(x) = x^2 + bx + w$  is irreducible over  $\mathbb{F}_{q^k}$  (such b always exist). For n = 2k, let  $\gamma_0 \in \mathbb{F}_{q^n}$  be a root of p(x). For  $i \in \{0, 1, \ldots, \tau - 1\}$ , where  $\tau = \lfloor (q - 1)/2 \rfloor$ , let  $\gamma_i = w^i \gamma_0$  and let

$$V_i = \{ u + u^{q^\circ} \gamma_i : u \in \mathbb{F}_{q^k} \}$$

The set

$$G_{n,s} = \bigcup_{i \in \{0,1,\dots,\tau-1\}} C_{V_i} \subseteq \mathcal{G}_q(n,k)$$

is a subspace code of size  $\tau \cdot (q^n - 1)/(q - 1)$  and minimum distance n - 2.

Proof. Let  $\mu_i = w^i$  for any i and  $\gamma_0 = \xi$ . Note that  $\gamma_0^{q^k+1} = \xi^{q^k+1} = w$ . Let  $i, j \in \{0, \ldots, \tau - 1\}$ . Note that  $w^i$  and  $w^j$  are such that  $N_{q^k/q}(w^i) \neq N_{q^k/q}(w^j)$ , since w is a primitive element and |i-j| < q-1. Moreover,

$$N_{q^k/q}(\mu_i\mu_j\xi^{q^k+1}) = N_{q^k/q}(w)^{i+j+1},$$

which cannot be one, again since w is primitive and i + j + 1 < q - 1. So, we can apply Theorem 3.9 to get the assertion.

Adding to the list of  $V_i$ 's also the subfield  $\mathbb{F}_{q^k}$  extends the code  $G_{n,s}$  preserving the minimum distance but keeping a large number of codewords.

**Proposition 3.12.** For a prime power  $q \ge 3$  and a positive integer  $k \ge 2$ , let w be a primitive element of  $\mathbb{F}_{q^k}$  and let s be a positive integer such that gcd(s,k) = 1. Let  $b \in \mathbb{F}_{q^k}$  be such that the polynomial  $p(x) = x^2 + bx + w$  is irreducible over  $\mathbb{F}_{q^k}$  (such b always exist). For n = 2k, let  $\gamma_0 \in \mathbb{F}_{q^n}$  be a root of p(x). For  $i \in \{0, 1, \ldots, \tau - 1\}$ , where  $\tau = \lfloor (q - 1)/2 \rfloor$ , let  $\gamma_i = w^i \gamma_0$  and let

$$V_i = \{ u + u^{q^s} \gamma_i : u \in \mathbb{F}_{q^k} \}.$$

Then

$$\lim_{\mathbb{F}_q} (\mathbb{F}_{q^k} \cap \alpha V_i) \le 1$$

for every  $i \in \{0, \ldots, \tau - 1\}$ . In particular, the set

$$\overline{G}_{n,s} = \bigcup_{i \in \{0,1,\dots,\tau-1\}} C_{V_i} \cup C_{\mathbb{F}_{q^k}} \subseteq \mathcal{G}_q(n,k)$$

is a subspace code of size  $\tau \cdot (q^n - 1)/(q - 1) + q^k + 1$  with minimum distance n - 2.

*Proof.* Clearly, C is a cyclic code and its size is  $\tau \cdot (q^n - 1)/(q - 1) + q^k + 1$  because of Theorem 1.1 and Corollary 3.11. Let  $\alpha \in \mathbb{F}_{q^n}^*$ . We now first show that

$$\dim_{\mathbb{F}_q}(\mathbb{F}_{q^k} \cap \alpha V_i) \le 1.$$

Then there exist  $\alpha_0, \alpha_1 \in \mathbb{F}_{q^k}$  such that  $\alpha = \alpha_0 + \alpha_1 \gamma_0$ . Let  $v \in \mathbb{F}_{q^k}$ , we look for solutions in  $u \in \mathbb{F}_{q^k}$  such that

$$v = \alpha(u + u^{q^s} \gamma_i).$$

Using that  $\gamma_0^2 = a\gamma_0 + b$ , for some  $a, b \in \mathbb{F}_{q^k}$ , and that  $\alpha = \alpha_0 + \alpha_1\gamma_0$ , the above relation reads as follows

$$\begin{cases} \alpha_0 u + b\alpha_1 u^{q^s} w^i = v, \\ \alpha_1 u + \alpha_0 w^i u^{q^s} + w^i \alpha_1 a u^{q^s} = 0. \end{cases}$$

Since gcd(s,k) = 1,  $\alpha_1 u + \alpha_0 w^i u^{q^s} + w^i \alpha_1 a u^{q^s}$  can be seen as a non-zero  $q^s$ -polynomial in u over  $\mathbb{F}_{q^k}$  of  $q^s$ -degree at most one. Therefore, by Theorem 2.1 it follows that the number of  $u \in \mathbb{F}_{q^k}$  which are solutions of the above system is at most q and hence

$$\dim_{\mathbb{F}_a}(\mathbb{F}_{a^k} \cap \alpha V_i) \le 1$$

Now, note that for any  $\alpha \notin \mathbb{F}_{q^k}$  we have

$$\dim_{\mathbb{F}_q}(\mathbb{F}_{q^k} \cap \alpha \mathbb{F}_{q^k}) = 0.$$

By Corollary 3.11, we have that

$$\dim_{\mathbb{F}_q}(V_i \cap \alpha V_j) \le 1$$

for each  $i, j \in \{0, \ldots, \tau - 1\}$ . So, the minimum distance of C is n - 2.

## 4. Equivalences of multi-orbit cyclic subspace codes

In [40] Horlemann-Trautmann initiated the study of the equivalence for subspace codes in a very general setting. More recently in [18] Gluesing-Luerssen and Lehmann investigate the case of cyclic orbit codes, that is *G*-orbits of a subspace *U* of  $\mathbb{F}_{q^n}$  with *G* a Singer cycle of  $\mathrm{GL}(n,q)$ . Therefore, motivated by [18, Theorem 2.4] and according to [18, Definition 3.5], we say that two cyclic subspace codes  $C_U$  and  $C_V$  are **linearly equivalent** if there exists  $i \in \{0, \ldots, n-1\}$  such that

$$C_U = C_{V^{q^i}}$$

where  $V^{q^i} = \{v^{q^i} : v \in V\}$ . This happens if and only if  $U = \alpha V^{q^i}$ , for some  $\alpha \in \mathbb{F}_{q^n}^*$ .

We can hence extend this definition to the case of cyclic subspace codes with r orbits.

**Definition 4.1.** Let  $C = \bigcup_{i \in \{1,...,r\}} C_{U_i}$  and  $C' = \bigcup_{i \in \{1,...,r\}} C_{V_i}$ , with  $U_1, \ldots, U_r$  and  $V_1, \ldots, V_r$  $\mathbb{F}_q$ -subspaces in  $\mathcal{G}_q(n,k)$ . We say that C and C' are **linearly equivalent** if there exists  $j \in \{0,\ldots,n-1\}$  such that

$$C = \bigcup_{i \in \{1, \dots, r\}} C_{V_i^{q^j}}$$

Equivalently,  $C = \bigcup_{i \in \{1,...,r\}} C_{U_i}$  and  $C' = \bigcup_{i \in \{1,...,r\}} C_{V_i}$  are linearly equivalent if there exist  $\alpha_1, \ldots, \alpha_r \in \mathbb{F}_{q^n}^*, \sigma \in S_r$  and  $j \in \{0, \ldots, n-1\}$  such that

$$U_i = \alpha_i V_{\sigma(i)}^{q^j}$$

for any  $i \in \{1, ..., r\}$ .

Clearly, if C and C' are two linearly equivalent cyclic subspace codes, then |C| = |C'| and their minimum distances coincide. Such properties are also satisfied if we weaken the definition as follows.

**Definition 4.2.** Let  $C = \bigcup_{i \in \{1,...,r\}} C_{U_i}$  and  $C' = \bigcup_{i \in \{1,...,r\}} C_{V_i}$ , with  $U_1, \ldots, U_r$  and  $V_1, \ldots, V_r$  $\mathbb{F}_q$ -subspaces in  $\mathcal{G}_q(n,k)$ . We say that C and C' are **semilinearly equivalent** if there exists  $\rho \in \operatorname{Aut}(\mathbb{F}_{q^n})$  such that

$$C = \bigcup_{i \in \{1, \dots, r\}} C_{V_i^{\rho}}.$$

Equivalently,  $C = \bigcup_{i \in \{1,...,r\}} C_{U_i}$  and  $C' = \bigcup_{i \in \{1,...,r\}} C_{V_i}$  are semilinearly equivalent if there exist  $\alpha_1, \ldots, \alpha_r \in \mathbb{F}_{q^n}^*$ ,  $\sigma \in S_r$  such that

$$U_i = \alpha_i V^{\rho}_{\sigma(i)},$$

for any  $i \in \{1, ..., r\}$ .

Now, we will study the equivalence issue among the family of codes  $G_{n,s}$ , showing that such a family contains a large number of inequivalent codes. To this aim, we start by recalling the following technical lemma proved in [29].

**Lemma 4.3.** [29, Lemma 4.13] Let n = 2k be an even positive integer and  $k \ge 3$ . Let  $\xi, \eta \in$  $\mathbb{F}_{q^{2k}} \setminus \mathbb{F}_{q^k}$ . Let s, s' be positive integers such that gcd(s,k) = gcd(s',k) = 1. Let  $\mu, \overline{\mu} \in \mathbb{F}_{q^k}^*$  and consider the  $\mathbb{F}_q$ -subspaces of  $\mathbb{F}_{q^{2k}}$ 

$$W_{\mu x^{q^s},\xi} = \{ u + \xi \mu u^{q^s} \colon u \in \mathbb{F}_{q^k} \}$$

and

$$W_{\overline{\mu}x^{q^{s'}},\eta} = \{ v + \eta \overline{\mu}v^{q^{s'}} \colon v \in \mathbb{F}_{q^k} \}.$$

There exists  $\lambda \in \mathbb{F}_{q^n}^*$  such that

(7) 
$$W_{\mu x^{q^s},\xi} = \lambda (W_{\overline{\mu} x^{q^{s'}},\eta})^{\rho}$$

if and only if one of the following condition holds

- $s \equiv s' \pmod{k}$ , B = 0,  $\xi = \frac{\eta^{\rho}}{A}$  and  $\overline{\mu} = \frac{\mu^{\rho^{-1}c}}{A^{\rho^{-1}}}$ , where  $c \in \mathbb{F}_{q^k}$  is such that  $N_{q^k/q}(c) = 1$ ;  $s \equiv -s' \pmod{k}$ ,  $\xi = \frac{\eta^{\rho} + Aa}{A}$ ,  $\overline{\mu} = \frac{1}{c\mu^{q^{-s}\rho^{-1}}A^{\rho^{-1}}b^{\rho^{-1}}}$  and B = -Aa, where  $c \in \mathbb{F}_{q^k}$  is such
- that  $N_{a^k/a}(c) = 1$ ,

where  $\xi^2 = a\xi + b$ ,  $\eta^{\rho} = A\xi + B$  with  $a, b, A, B \in \mathbb{F}_{q^k}$  and  $\rho \in \operatorname{Aut}(\mathbb{F}_{q^n})$ .

Using the above result, similarly to what has been done in [29, Theorem 4.14], we obtain the following result.

**Corollary 4.4.** Let s, s' be two positive integers coprime with  $k \geq 3$  and let n = 2k, let  $\xi, \eta \in$  $\mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k} \text{ and let } f_i(x) = \mu_i x^{q^s} \in \mathcal{L}_k \text{ and } g_i(x) = \overline{\mu}_i x^{q^{s'}} \in \mathcal{L}_k \text{ for } i \in \{1, \dots, r\} \text{ such that } r \leq q-1,$  $N_{q^k/q}(\mu_i) \neq N_{q^k/q}(\mu_j), N_{q^k/q}(\overline{\mu}_i) \neq N_{q^k/q}(\overline{\mu}_j), N_{q^k/q}(\mu_i\mu_j\xi^{q^k+1}) \neq 1 \text{ and } N_{q^k/q}(\overline{\mu}_i\overline{\mu}_j\eta^{q^k+1}) \neq 1 \text{ for } n \in \mathbb{N}$ every  $i \neq j$ . Then  $C = \bigcup_{i=1}^{n} C_{W_{f_i,\xi_i}}$  and  $\overline{C} = \bigcup_{i=1}^{n} C_{W_{g_i,\eta_i}}$  are semilinearly equivalent if and only if there exist a permutation  $\sigma \in S_r$  and  $\rho \in \operatorname{Aut}(\mathbb{F}_{q^n})$  such that, for every  $i \in \{1, \ldots, r\}$ , one of the following occur

• 
$$s \equiv s' \pmod{k}$$
,  $B = 0$ ,  $\xi = \frac{\eta^{\rho}}{A}$  and  $\overline{\mu}_{\sigma(i)} = \frac{\mu_i^{\rho-c}}{A^{\rho-1}}$ , where  $c \in \mathbb{F}_{q^k}$  is such that  $N_{q^k/q}(c) = 1$ ;  
•  $s \equiv -s' \pmod{k}$ ,  $\xi = \frac{\eta^{\rho} + Aa}{A}$ ,  $\overline{\mu}_{\sigma(i)} = \frac{1}{c\mu_i^{q^{-s}\rho^{-1}}A^{\rho^{-1}}b^{\rho^{-1}}}$  and  $B = -Aa$ , where  $c \in \mathbb{F}_{q^k}$  is such that  $N_{q^k/q}(c) = 1$ ,

where  $\xi^2 = a\xi + b$  and  $\eta^{\rho} = A\xi + B$  with  $a, b, A, B \in \mathbb{F}_{a^k}$ .

*Proof.* Suppose that C and  $\overline{C}$  are semilinearly equivalent, that is there exist a permutation  $\sigma \in S_r$ ,  $\lambda_1, \ldots, \lambda_r \in \mathbb{F}_{q^n}^*$  and  $\rho \in \operatorname{Aut}(\mathbb{F}_{q^n})$  such that

$$W_{f_i,\xi} = \lambda_i (W_{g_{\sigma(i)},\eta})^{\rho}$$

for every  $i \in \{1, \ldots, r\}$ . By Lemma 4.3 then  $s \equiv \pm s' \pmod{k}$ . Moreover, if  $s \equiv s' \pmod{k}$  then  $B = 0, \ \xi = \frac{\eta^{\rho}}{A} \text{ and } \overline{\mu}_{\sigma(i)} = \frac{\mu_i^{\rho^{-1}}c}{A^{\rho^{-1}}}, \text{ where } c \in \mathbb{F}_{q^k} \text{ such that } \mathcal{N}_{q^k/q}(c) = 1; \text{ whereas if } s \equiv -s' \pmod{k}$ then  $\xi = \frac{\eta^{\rho} + Aa}{A}, \ \overline{\mu}_{\sigma(i)} = \frac{1}{c\mu_i^{q^{-s}\rho^{-1}}A^{\rho^{-1}}b^{\rho^{-1}}} \text{ and } B = -Aa, \text{ where } c \in \mathbb{F}_{q^k} \text{ such that } \mathcal{N}_{q^k/q}(c) = 1, \text{ for } t$ every  $i \in \{1, \ldots, r\}$ . The converse follows by Lemma 4.3. 

In particular, we can give the following bound on the number of inequivalent codes of type  $G_{n,s}$ .

**Corollary 4.5.** The number of semilinearly inequivalent codes of Corollary 3.11 is at least  $\varphi(k)/2$ , where  $\varphi$  is the Euler totient function.

To prove the above corollary, we did not use the complete characterization of the equivalence given by Corollary 4.4. This means that the family of the codes of form  $G_{n,s}$  could be even larger.

### 5. A Geometric interpretation of cyclic subspace codes

In this section we present a geometric interpretation of the Sidon property via linear sets that will give a bound on the number of orbits of a multi-orbit cyclic subspace code.

The Sidon property in terms of linear sets reads as follows.

**Theorem 5.1.** Let U be a k-dimensional  $\mathbb{F}_q$ -subspace of  $\mathbb{F}_{q^n}$ . Then U is a Sidon space if and only if the only points of  $L_{U\times U} \subseteq \mathrm{PG}(1,q^n) = \mathrm{PG}(\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}, \mathbb{F}_{q^n})$  of weight greater than one are those in  $\mathrm{PG}(\mathbb{F}_q \times \mathbb{F}_q, \mathbb{F}_q)$ . Furthermore, the weight of such points is k.

In particular, if U is a Sidon space then the size of  $L_{U \times U}$  is

$$\frac{q^k - 1}{q - 1}(q^k - q) + q + 1.$$

*Proof.* Let  $\alpha \in \mathbb{F}_{q^n}^*$ . Let  $\langle (1, \alpha) \rangle_{\mathbb{F}_{q^n}} \in L_{U \times U}$ . Then there exists some  $\rho \in \mathbb{F}_{q^n}^*$  such that

$$\rho(1,\alpha) \in U \times U,$$

that is  $\rho \in U \cap \alpha^{-1}U$ . Therefore, if U is a Sidon space by Theorem 1.2 it follows that  $\dim_{\mathbb{F}_q}(U \cap \alpha^{-1}U) \leq 1$  if  $\alpha \notin \mathbb{F}_q$  and  $\dim_{\mathbb{F}_q}(U \cap \alpha^{-1}U) = k$  if  $\alpha \in \mathbb{F}_q$ . So  $w_{L_U \times U}(\langle (1, \alpha) \rangle_{\mathbb{F}_{q^n}}) = 1$  if and only if  $\alpha \notin \mathbb{F}_q$  and if  $w_{L_U \times U}(\langle (1, \alpha) \rangle_{\mathbb{F}_{q^n}}) \geq 2$  then  $\alpha \in \mathbb{F}_q$  and  $w_{L_U \times U}(\langle (1, \alpha) \rangle_{\mathbb{F}_{q^n}}) = k$ . Suppose now that the only points of  $L_{U \times U} \subseteq \mathrm{PG}(1, q^n)$  of weight greater than one are those in  $L_{U \times U} \cap \mathrm{PG}(\mathbb{F}_q \times \mathbb{F}_q, \mathbb{F}_q)$ . Then if  $\alpha \notin \mathbb{F}_q$  we have  $\dim_{\mathbb{F}_q}(U \cap \alpha^{-1}U) \leq 1$  and so by Theorem 1.2 the subspace U turns out to be a Sidon space. The last part follows by (3) and (4).  $\Box$ 

The above result can be extended to the case of multi-Sidon spaces and, when they all have dimension n/2, to those cyclic subspace codes with minimum distance n-2.

**Theorem 5.2.** Let  $\{U_1, \ldots, U_r\}$  be a set of  $\mathbb{F}_q$ -subspaces in  $\mathbb{F}_{q^n}$  and let  $k_i = \dim_{\mathbb{F}_q}(U_i) \ge 2$  for every  $i \in \{1, \ldots, r\}$ . Then  $\{U_1, \ldots, U_r\}$  is a multi-Sidon space if and only if

- the only points of  $L_{U_i \times U_i} \subseteq PG(1, q^n) = PG(\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}, \mathbb{F}_{q^n})$  of weight greater than one are those in  $PG(\mathbb{F}_q \times \mathbb{F}_q, \mathbb{F}_q)$ , for every  $i \in \{1, \ldots, r\}$ ;
- $L_{U_i \times U_i} \cap L_{U_j \times U_j} = \operatorname{PG}(\mathbb{F}_q \times \mathbb{F}_q, \mathbb{F}_q)$ , for every  $i, j \in \{1, \ldots, r\}$  with  $i \neq j$ .

*Proof.* Let  $\alpha \in \mathbb{F}_{q^n}^*$ . Let  $\langle (1, \alpha) \rangle_{\mathbb{F}_{q^n}} \in L_{U_i \times U_i} \cap L_{U_j \times U_j}$ , with  $i \neq j$ . In particular, there exists  $\rho \in \mathbb{F}_{q^n}^*$  such that

$$\rho(1,\alpha) = (u,\overline{u}),$$

for some  $u, \overline{u} \in U_i$ . Hence,  $\alpha = \rho^{-1}\overline{u} = \overline{u}/u$ . Similarly,  $\alpha = \overline{v}/v$ , for some  $v, \overline{v} \in U_j$ . So that  $\alpha \in U_i \cdot U_i^{-1} \cap U_j \cdot U_j^{-1}$ . The assertion now follows by Theorem 3.5 and by Theorem 5.1.

We can hence derive some bounds that involve the number and the dimensions of the subspaces of a multi-Sidon space, the degree of the field extension and q.

**Theorem 5.3.** Let  $\{U_1, \ldots, U_r\}$  be a multi-Sidon space and let  $k_i = \dim_{\mathbb{F}_q}(U_i) \ge 2$  for every  $i \in \{1, \ldots, r\}$ . Then

$$\sum_{i=1}^{r} \frac{q^{k_i} - 1}{q - 1} (q^{k_i} - q) \le q^n - q.$$

If  $\{U_1, \ldots, U_r\}$  is a maximum multi-Sidon space then

$$r \le \frac{(q^n - q)(q - 1)}{(q^{n/2} - q)(q^{n/2} - 1)}$$

In particular,

$$r \le \begin{cases} q-1 & \text{if } n > 4, \\ q & \text{if } n = 4. \end{cases}$$

*Proof.* By Theorem 5.2, the  $L_{U_i \times U_i}$ 's pairwise intersect each other only in  $PG(\mathbb{F}_q \times \mathbb{F}_q, \mathbb{F}_q)$ , so that

$$\left| \left( \bigcup_{i=1}^{r} L_{U_i \times U_i} \right) \setminus \mathrm{PG}(\mathbb{F}_q \times \mathbb{F}_q, \mathbb{F}_q) \right| = \sum_{i=1}^{r} \frac{q^{k_i} - 1}{q - 1} (q^{k_i} - q).$$

Since  $(\bigcup_{i=1}^{r} L_{U_i \times U_i}) \setminus \mathrm{PG}(\mathbb{F}_q \times \mathbb{F}_q, \mathbb{F}_q) \subseteq \mathrm{PG}(1, q^n) \setminus \mathrm{PG}(\mathbb{F}_q \times \mathbb{F}_q, \mathbb{F}_q)$ , the assertion follows.  $\Box$ 

Combining Theorem 5.3 with the definition of multi-Sidon space we obtain the following bound on the number of orbits of a cyclic subspace code (whose subspaces have dimension n/2).

**Corollary 5.4.** Let  $n = 2k \ge 4$  and let  $U_1, \ldots, U_r$  be  $\mathbb{F}_q$ -subspaces of dimension k in  $\mathbb{F}_{q^n}$  and let

$$C = \bigcup_{i \in \{1, \dots, r\}} C_{U_i} \subseteq \mathcal{G}_q(n, k)$$

be a subspace code. If the minimum distance of C is n-2, then

$$r \le \begin{cases} q-1 & \text{if } n > 4 \\ q & \text{if } n = 4 \end{cases}$$

**Remark 5.5.** Corollary 5.4 implies that when n = 2k > 4 and  $U_1, \ldots, U_r$  are  $\mathbb{F}_q$ -subspaces of dimension k in  $\mathbb{F}_{q^n}$  and

$$C = \bigcup_{i \in \{1, \dots, r\}} C_{U_i} \subseteq \mathcal{G}_q(n, k),$$

with C of minimum distance n-2, then  $|C| \leq q^n - 1$ . This bound cannot be derived directly from the sphere-packaging bound for subspace codes, but we note that they coincide asymptotically.

6. Linear sets with only r points of weight greater than one

In this section we will make use of cyclic subspace codes to construct a special type of linear sets in  $PG(r-1, q^n)$  with exactly r points of weight greater than one. More precisely, our purpose is to investigate linear sets  $L_U$  in  $PG(r-1, q^n)$  of rank  $k \leq (r-1)n$  containing r independent points  $P_1, \ldots, P_r$  such that

$$w_{L_U}(P_1) + \ldots + w_{L_U}(P_r) = k.$$

We will characterize these linear sets, we will provide bounds on their rank and constructions, using multi-orbit cyclic subspace codes via their representatives. Then we will give a polynomial representation of those linear sets having rank n. Then we will study the dual of these linear sets, which have few intersection numbers with hyperplanes, yielding linear rank metric codes with few weights.

Linear sets of this form in  $PG(1, q^n)$  have been already studied in [29] (see also [24, 30]), where the authors study linear sets on the projective line containing two points whose sum of their weights equals the rank of the linear set.

We start our investigation by proving that, up to equivalence, one can write the linear sets as the one defined by the Cartesian product of  $r \mathbb{F}_q$ -subspaces of  $\mathbb{F}_{q^n}$ , as shown in the next result.

**Proposition 6.1.** Let  $L_W$  be an  $\mathbb{F}_q$ -linear set in  $PG(r-1, q^n)$  of rank k containing r independent points  $P_1 = \langle \mathbf{v}_1 \rangle_{\mathbb{F}_{q^n}}, \ldots, P_r = \langle \mathbf{v}_r \rangle_{\mathbb{F}_{q^n}}$  such that

$$w_{L_W}(P_1) + \ldots + w_{L_W}(P_r) = k \le (r-1)n$$

Then  $L_W$  is  $\operatorname{PGL}(r, q^n)$ -equivalent to  $L_U$  where  $U = U_1 \times \ldots \times U_r$ , for some  $\mathbb{F}_q$ -subspaces  $U_1, \ldots, U_r$ of  $\mathbb{F}_{q^n}$  such that  $\dim_{\mathbb{F}_q}(U_i) = w_{L_W}(P_i)$  for every  $i \in \{1, \ldots, r\}$ . Moreover, if  $k \leq n$  then  $U_1, \ldots, U_r$ can be chosen in such a way that  $U_1 + \ldots + U_r$  is a direct sum.

*Proof.* Consider a collineation  $\varphi \in PGL(r, q^n)$  such that

$$\varphi(P_i) = \langle \mathbf{e}_i \rangle_{\mathbb{F}_{a^n}},$$

 $\mathbf{e}_i \in \mathbb{F}_{q^n}^r$  is the vector whose *i*-th component is 1 and all the others are zero. Denote by f the associated linear isomorphism of  $\mathbb{F}_{q^n}^r$  and let U = f(W). Since

$$W = (W \cap \langle \mathbf{v}_1 \rangle_{\mathbb{F}_{q^n}}) \oplus \ldots \oplus (W \cap \langle \mathbf{v}_r \rangle_{\mathbb{F}_{q^n}}),$$

then

$$U = (U \cap \langle \mathbf{e}_1 \rangle_{\mathbb{F}_{q^n}}) \oplus \ldots \oplus (U \cap \langle \mathbf{e}_r \rangle_{\mathbb{F}_{q^n}}).$$

Therefore,  $U \cap \langle \mathbf{e}_i \rangle_{\mathbb{F}_{q^n}}$  is equal to  $\{(0, \ldots, 0, u, 0, \ldots, 0) \colon u \in U_i\}$  for any  $i \in \{1, \ldots, r\}$  and for a subspace  $U_i$  of  $\mathbb{F}_{q^n}$ . So we obtain the first part of the assertion. Now suppose that  $k \leq n$ . Our aim is to prove that there exists  $(\lambda_1, \ldots, \lambda_r) \in (\mathbb{F}_{q^n}^*)^r$  such that  $\lambda_i U_i \cap \langle \lambda_j U_j \colon j \in \{1, \ldots, r\} \setminus \{i\} \rangle_{\mathbb{F}_q} = \{\mathbf{0}\}$  for any  $i \in \{1, \ldots, r\}$ . We proceed by finite induction proving that there exist  $\lambda_i \in \mathbb{F}_{q^n}^*$  such that

(8) 
$$\lambda_i U_i \cap \langle \lambda_j U_j \colon j \in \{1, \dots, i-1\} \rangle_{\mathbb{F}_q} = \{\mathbf{0}\},$$

for every  $i \in \{2, ..., r\}$ . This is enough to show the last part of the assertion. The case i = 2 has been proved in [29, Proposition 3.2]. Now, let  $i \in \{1, ..., r\}$  and suppose that (8) holds for every  $j \leq i$ . Then, using (8) recursively we get

$$\dim_{\mathbb{F}_q}(\langle \lambda_j U_j \colon j \in \{1, \dots, i\} \rangle_{\mathbb{F}_q}) = \dim_{\mathbb{F}_q}(\lambda_i U_i) + \dim_{\mathbb{F}_q}(\langle \lambda_j U_j \colon j \in \{1, \dots, i-1\} \rangle_{\mathbb{F}_q})$$
$$- \dim_{\mathbb{F}_q}(\lambda_i U_i \cap \langle \lambda_j U_j \colon j \in \{1, \dots, i-1\} \rangle_{\mathbb{F}_q}) = \dim_{\mathbb{F}_q}(U_1) + \dots + \dim_{\mathbb{F}_q}(U_i).$$

Let  $h \in \{1, \ldots, i\}$ , then

$$\dim_{\mathbb{F}_q}(\lambda_h U_h \cap \langle \lambda_j U_j \colon j \in \{1, \dots, i\} \setminus \{h\}\rangle_{\mathbb{F}_q}) = \dim_{\mathbb{F}_q}(U_h)$$

 $+\dim_{\mathbb{F}_q}(\langle \lambda_j U_j \colon j \in \{1, \dots, i\} \setminus \{h\}\rangle_{\mathbb{F}_q}) - \dim_{\mathbb{F}_q}(\langle \lambda_j U_j \colon j \in \{1, \dots, i\}\rangle_{\mathbb{F}_q}).$ 

The last two equations imply  $\dim_{\mathbb{F}_q}(\lambda_h U_h \cap \langle \lambda_j U_j : j \in \{1, \ldots, i\} \setminus \{h\}\rangle_{\mathbb{F}_q}) = 0.$ 

We now prove (8). Suppose now that

$$\lambda_i U_i \cap \langle \lambda_j U_j \colon j \in \{1, \dots, i-1\} \rangle_{\mathbb{F}_q} = \{\mathbf{0}\}$$

Suppose that for each  $\lambda \in \mathbb{F}_{q^n}^*$ 

(9) 
$$\lambda U_{i+1} \cap \langle \lambda_j U_j \colon j \in \{1, \dots, i\} \rangle_{\mathbb{F}_q} \neq \{\mathbf{0}\}$$

Denote by  $\overline{U} = \langle \lambda_j U_j : j \in \{1, \dots, i\} \rangle_{\mathbb{F}_q}$ . By (9) it follows that the  $\mathbb{F}_q$ -linear set  $L_{U_{i+1} \times \overline{U}}$  of rank less than or equal to *n* contains at least  $q^n + 1$  points, a contradiction to (2). So, there exists  $\lambda_{i+1} \in \mathbb{F}_{q^n}^*$  such that  $\lambda_{i+1} U_{i+1} \cap \overline{U} = \{\mathbf{0}\}$ .

In terms of linear sets, Theorem 3.5 reads as a characterization of linear sets with only r points of weight greater than one (in independent position).

**Theorem 6.2.** Let  $U_1, \ldots, U_r$  be  $r \mathbb{F}_q$ -subspaces of  $\mathbb{F}_{q^n}$  such that  $\sum_{i=1}^r \dim_{\mathbb{F}_q}(U_i) = k \leq (r-1)n$ . Let  $k_i = \dim_{\mathbb{F}_q}(U_i) \ge 2$ , for any  $i \in \{1, \ldots, r\}$  and  $U = U_1 \times \ldots \times U_r$ . Then, the following are equivalent

- i) all the points of  $L_U$  different from  $P_i = \langle \mathbf{e}_i \rangle_{\mathbb{F}_{q^n}}$  with  $i \in \{1, \ldots, r\}$  have weight one in  $L_U$ ;
- ii)  $U_i \cdot U_i^{-1} \cap U_j \cdot U_j^{-1} = \mathbb{F}_q$  for any  $i, j \in \{1, \dots, r\}$  with  $i \neq j$ ;
- iii)  $\dim_{\mathbb{F}_a}(U_i \cap \alpha U_j) \leq 1$ , for every  $\alpha \in \mathbb{F}_{a^n}^*$  and  $i, j \in \{1, \ldots, r\}$  with  $i \neq j$ .

Now, we will prove a bound on the rank of these linear sets. This bound relies on the following result from [29].

**Theorem 6.3.** [29, Theorem 4.4] Let L be an  $\mathbb{F}_q$ -linear set of  $PG(1, q^n)$  with exactly two points P and Q of weight greater than one, then

$$w_L(P) \leq \frac{n}{2} \text{ and } w_L(Q) \leq \frac{n}{2}$$

The next result extends [29, Theorem 4.4] to linear sets in  $PG(r-1, q^n)$ .

**Theorem 6.4.** Let  $L_W$  be an  $\mathbb{F}_q$ -linear set in  $PG(r-1,q^n)$  of rank k containing r independent points  $P_1 = \langle \mathbf{v}_1 \rangle_{\mathbb{F}_{q^n}}, \dots, P_r = \langle \mathbf{v}_r \rangle_{\mathbb{F}_{q^n}}$  such that

$$w_{L_W}(P_1) + \ldots + w_{L_W}(P_r) = k \le (r-1)n.$$

Suppose that  $w_{L_W}(Q) \leq 1$  for every  $Q \in PG(r-1,q^n) \setminus \{P_1,\ldots,P_r\}$ . Then

(10) 
$$w_{L_W}(P_i) \le$$

for every  $i \in \{1, \ldots, r\}$ . Moreover,

- Rank $(L_W) \leq \frac{rn}{2}$ ; *if* Rank $(L_W) = \frac{rn}{2}$ , then  $w_{L_W}(P_i) = \frac{n}{2}$  for every  $i \in \{1, \dots, r\}$ .

*Proof.* By Proposition 6.1  $L_W$  is  $PGL(r, q^n)$ -equivalent to  $L_U$  where  $U = U_1 \times \ldots \times U_r$ , for some  $\mathbb{F}_q$ -subspaces  $U_1, \ldots, U_r$  of  $\mathbb{F}_{q^n}$  such that  $\dim_{\mathbb{F}_q}(U_i) = w_{L_W}(P_i)$  for every  $i \in \{1, \ldots, r\}$ . So, the only points with weight greater than one in  $L_U$  are  $Q_i = \langle \mathbf{e}_i \rangle_{\mathbb{F}_{q^n}}$  for every  $i \in \{1, \ldots, r\}$  and  $w_{L_W}(P_i) = w_{L_U}(Q_i)$  for every  $i \in \{1, \ldots, r\}$ . Let  $i, j \in \{1, \ldots, r\}$  with  $i \neq j$  and consider the line  $\ell = \mathrm{PG}(\langle \mathbf{e}_i, \mathbf{e}_j \rangle_{\mathbb{F}_{q^n}}, \mathbb{F}_{q^n}) = \langle Q_i, Q_j \rangle$ . We first observe that for each  $Q \in \ell$  then  $w_{L_U}(Q) = w_{L_U \cap \ell}(Q)$ and hence the only points of weight greater than one in  $L_U \cap \ell$  are  $Q_i$  and  $Q_j$ . By Theorem 6.3 we have that

$$w_{L_U \cap \ell}(Q_i) = w_{L_U}(Q_i) \le \frac{n}{2}$$
 and  $w_{L_U \cap \ell}(Q_j) = w_{L_U}(Q_j) \le \frac{n}{2}$ 

and the first part of the assertion then follows. The second part is a consequence of (10). 

**Remark 6.5.** Let  $L_W$  be an  $\mathbb{F}_q$ -linear set in  $PG(r-1,q^n)$  of rank  $\frac{rn}{2}$  containing r independent points  $P_1 = \langle \mathbf{v}_1 \rangle_{\mathbb{F}_{q^n}}, \ldots, P_r = \langle \mathbf{v}_r \rangle_{\mathbb{F}_{q^n}}$  such that  $w_{L_W}(P_i) = \frac{n}{2}$  for every  $i \in \{1, \ldots, r\}$ . By (3) and (4), recalling that  $N_i$  is the number of points in  $L_W$  having weight i, we obtain that

$$N_1 = q^{\frac{rn}{2}-1} + \ldots + q^{\frac{n}{2}} - (r-1)(q^{\frac{n}{2}-1} + \ldots + 1), \quad N_{\frac{n}{2}} = r \text{ and } N_0 = \frac{q^{rn}-1}{q^n-1} - N_1 - N_{\frac{n}{2}}.$$

In particular

$$|L_W| = q^{\frac{rn}{2}-1} + \ldots + q^{\frac{n}{2}} - (r-1)(q^{\frac{n}{2}-1} + \ldots + q) + 1.$$

We can now construct linear sets in  $PG(r-1, q^n)$  with exactly r points of weight greater than one and in particular we will see constructions when then rank is maximum, that is  $\frac{rn}{2}$ . Multi-Sidon spaces can be used to this aim.

**Proposition 6.6.** Let  $U_1, \ldots, U_r$  be  $r \mathbb{F}_q$ -subspaces of  $\mathbb{F}_{q^n}$  of dimensions  $k_1, \ldots, k_r$ , respectively. Let  $U = U_1 \times \ldots \times U_r$ . If  $\{U_1, \ldots, U_r\}$  is a multi-Sidon space, then  $L_U$  is an  $\mathbb{F}_q$ -linear set of rank  $k_1 + \ldots + k_r$  in  $\mathrm{PG}(r-1, q^n)$  such that the only points of weight greater than one are the  $P_i = \langle \mathbf{e}_i \rangle_{\mathbb{F}_{q^n}}$ 's with  $i \in \{1, \ldots, r\}$ .

*Proof.* Since  $\{U_1, \ldots, U_r\}$  is a multi-Sidon space, we have that

$$\dim_{\mathbb{F}_q}(U_i \cap \alpha U_j) \le 1,$$

for every  $\alpha \in \mathbb{F}_{q^n}$  and  $i, j \in \{1, \ldots, r\}$  with  $i \neq j$ . The assertion then follows directly by Theorem 6.2.

In particular, when considering maximum multi-Sidon spaces, we can get examples of linear sets whose rank satisfy the equality in Theorem 6.4.

**Corollary 6.7.** Let n = 2k and  $U_1, \ldots, U_r$  be  $r \mathbb{F}_q$ -subspaces of  $\mathbb{F}_{q^n}$  of dimension k. Let  $U = U_1 \times \ldots \times U_r$ . If  $\{U_1, \ldots, U_r\}$  is a multi-Sidon space, then  $L_U$  is an  $\mathbb{F}_q$ -linear set of rank rk in  $PG(r-1,q^n)$  such that the only points of weight greater than one are the  $P_i = \langle \mathbf{e}_i \rangle_{\mathbb{F}_{q^n}}$  is with  $i \in \{1, \ldots, r\}$ .

The multi-cyclic subspace codes found in Proposition 3.9 can be used to get constructions of such linear sets via Corollary 6.7.

**Corollary 6.8.** Let s be a positive integer coprime with  $k \geq 2$  and n = 2k, let  $\xi \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}$ and let  $f_i(x) = \mu_i x^{q^s} \in \mathcal{L}_k$  for  $i \in \{1, \ldots, r\}$  such that  $r \leq q - 1$ ,  $N_{q^k/q}(\mu_i) \neq N_{q^k/q}(\mu_j)$  and  $N_{q^k/q}(\mu_i \mu_j \xi^{q^{k+1}}) \neq 1$  for every  $i \neq j$ . Denote by  $U_i = W_{f_i,\xi}$  for every  $i \in \{1, \ldots, r\}$ . Let  $U = U_1 \times \ldots \times U_r$ , then  $L_U$  is an  $\mathbb{F}_q$ -linear sets of rank rk in  $\mathrm{PG}(r-1, q^n)$  such that the only points of weight greater than one are the  $P_i = \langle \mathbf{e}_i \rangle_{\mathbb{F}_{q^n}}$ 's with  $i \in \{1, \ldots, r\}$ .

Another construction may be obtained by extending a multi-Sidon space with subfield  $\mathbb{F}_{q^k}$  of  $\mathbb{F}_{q^n}$ .

**Corollary 6.9.** Let s be a positive integer coprime with  $k \ge 2$  and n = 2k, let  $\xi \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}$ and let  $f_i(x) = \mu_i x^{q^s} \in \mathcal{L}_k$  for  $i \in \{1, \ldots, r-1\}$  such that  $r \le q-1$ ,  $N_{q^k/q}(\mu_i) \ne N_{q^k/q}(\mu_j)$  and  $N_{q^k/q}(\mu_i \mu_j \xi^{q^k+1}) \ne 1$  for every  $i \ne j$ . Denote by  $U_i = W_{f_i,\xi}$  for every  $i \in \{1, \ldots, r-1\}$  and by  $U_r = \mathbb{F}_{q^k}$ . Let  $U = U_1 \times \ldots \times U_r$ , then  $L_U$  is an  $\mathbb{F}_q$ -linear set of rank rk in  $PG(r-1, q^n)$  such that the only points of weight greater than one are the  $P_i = \langle \mathbf{e}_i \rangle_{\mathbb{F}_{q^n}}$  's with  $i \in \{1, \ldots, r\}$ .

*Proof.* By Theorem 6.2 and by Proposition 3.9, it is enough to show that

$$\dim_{\mathbb{F}_q}(\mathbb{F}_{q^k} \cap \alpha U_i) \le 1,$$

for every  $i \in \{1, \ldots, r-1\}$  for any  $\alpha \in \mathbb{F}_{q^n}^*$ . Let  $\alpha \in \mathbb{F}_{q^n}^*$ . Then there exist  $\alpha_0, \alpha_1 \in \mathbb{F}_{q^k}$  such that  $\alpha = \alpha_0 + \alpha_1 \xi$ . Let  $v \in \mathbb{F}_{q^k}$ , we look for solutions in  $u \in \mathbb{F}_{q^k}$  such that

$$v = \alpha(u + u^{q^s} \mu_i \xi).$$

Using that  $\xi^2 = a\xi + b$ , for some  $a, b \in \mathbb{F}_{q^k}$ , and that  $\alpha = \alpha_0 + \alpha_1 \xi$ , the above relation reads as follows

$$\begin{cases} \alpha_0 u + b\alpha_1 u^{q^s} \mu_i = v, \\ \alpha_1 u + \alpha_0 \mu_i u^{q^s} + \mu_i \alpha_1 a u^{q^s} = 0. \end{cases}$$

Since gcd(s,k) = 1,  $\alpha_1 u + \alpha_0 \mu_i u^{q^s} + \mu_i \alpha_1 a u^{q^s}$  can be seen as a non-zero  $q^s$ -polynomial over  $\mathbb{F}_{q^k}$  of  $q^s$ -degree at most one. Therefore, by Theorem 2.1 it follows that the number of  $u \in \mathbb{F}_{q^k}$  which are solutions of the above system is at most q and hence

$$\dim_{\mathbb{F}_a}(\mathbb{F}_{a^k} \cap \alpha U_i) \le 1.$$

In the next subsection we will prove that the two  $\mathbb{F}_q$ -subspaces defined in the above corollaries are  $\Gamma L(r, q^n)$ -inequivalent.

6.1.  $\Gamma L(r, q^n)$ -equivalence. We now provide a useful tool that can be used to study the  $\Gamma L(r, q^n)$ -equivalence of the subspaces representing linear sets with only r points of weight greater than one, which extends [29, Lemma 3.3].

**Theorem 6.10.** Let  $U_1, \ldots, U_r$  and  $W_1, \ldots, W_r$  be  $\mathbb{F}_q$ -subspaces of  $\mathbb{F}_{q^n}$  such that

$$\dim_{\mathbb{F}_q}(U_1) + \ldots + \dim_{\mathbb{F}_q}(U_r) = k \le (r-1)n$$

and

$$\dim_{\mathbb{F}_q}(W_1) + \ldots + \dim_{\mathbb{F}_q}(W_r) = k \le (r-1)n.$$

Let  $U = U_1 \times \ldots \times U_r$  and  $W = W_1 \times \ldots \times W_r$  and suppose that  $P_i = \langle \mathbf{e}_i \rangle_{\mathbb{F}_{q^n}}$  are the only points of weight greater than one in  $L_U$  and in  $L_W$ . Then U and W are  $\Gamma L(r, q^n)$ -equivalent if and only if there exist a permutation  $\sigma \in S_r$ ,  $\lambda_1, \ldots, \lambda_r \in \mathbb{F}_{q^n}^*$  and  $\rho \in \operatorname{Aut}(\mathbb{F}_{q^n})$  such that

$$W_i = \lambda_i U^{\rho}_{\sigma(i)},$$

for every  $i \in \{1, \ldots, r\}$ . In particular,  $\dim_{\mathbb{F}_q}(W_i) = \dim_{\mathbb{F}_q}(U_{\sigma(i)})$ , for every  $i \in \{1, \ldots, r\}$ .

*Proof.* The "if" part is trivial. So, suppose that U and W are  $\Gamma L(r, q^n)$ -equivalent via  $\varphi \in \Gamma L(r, q^n)$  defined by the matrix  $A \in \operatorname{GL}(r, q^n)$  and the automorphism  $\rho \in \operatorname{Aut}(\mathbb{F}_{q^n})$ . Let  $\dim_{\mathbb{F}_q}(U_i) = k_i$  and  $\dim_{\mathbb{F}_q}(W_i) = k'_i$ , for any  $i \in \{1, \ldots, r\}$ .

By Theorem 3.5, we have that

- a)  $\dim_{\mathbb{F}_q}(U \cap \langle \mathbf{v} \rangle_{\mathbb{F}_{q^n}}) \leq 1$  for any  $\mathbf{v} \in \mathbb{F}_{q^n}^r$  such that  $\langle \mathbf{v} \rangle_{\mathbb{F}_{q^n}} \notin \{ \langle \mathbf{e}_i \rangle_{\mathbb{F}_{q^n}} : i \in \{1, \dots, r\} \};$
- b)  $\dim_{\mathbb{F}_q}(U \cap \langle \mathbf{e}_i \rangle_{\mathbb{F}_q^n}) = k_i \text{ for any } i \in \{1, \dots, r\},$

and the same properties hold for W. As a consequence, there exists  $\sigma \in S_r$  such that  $\varphi(\langle \mathbf{e}_i \rangle_{\mathbb{F}_{q^n}}) = \langle \mathbf{e}_{\sigma(i)} \rangle_{\mathbb{F}_{q^n}}$ . In particular, this means that A is the product of a permutation matrix (the one induced by  $\sigma$ ) and a diagonal matrix (whose diagonal elements are  $\lambda_1, \ldots, \lambda_r \in \mathbb{F}_{q^n}^*$ ). So,

$$W_i = \lambda_i U^{p}_{\sigma(i)},$$
  
for every  $i \in \{1, ..., r\}$  and  $\{k_1, ..., k_r\} = \{k'_1, ..., k'_r\}.$ 

As an easy consequence we obtain that the dimensions of the subspaces are not in one-to-one correspondence, then the two subspaces are inequivalent.

**Corollary 6.11.** Let  $U_1, \ldots, U_r$  and  $W_1, \ldots, W_r$  be  $\mathbb{F}_q$ -subspaces of  $\mathbb{F}_{q^n}$  of dimension  $k_1, \ldots, k_r$ and  $k'_1, \ldots, k'_r$ , respectively. Let  $U = U_1 \times \ldots \times U_r$  and  $W = W_1 \times \ldots \times W_r$  and suppose that  $P_i = \langle \mathbf{e}_i \rangle_{\mathbb{F}_{q^n}}$  are the only points of weight greater than one in  $L_U$  and in  $L_W$ . If  $(k_1, \ldots, k_r)$  cannot be obtained from  $(k'_1, \ldots, k'_r)$  by permuting their entries, then  $U_1 \times \ldots \times U_r$  and  $W_1 \times \ldots \times W_r$  are  $\Gamma L(r, q^n)$ -inequivalent.

The  $\Gamma L(r, q^n)$ -equivalence of the examples in Proposition 3.9 has been already studied in Corollary 4.4. Whereas, as shown in the next result, the examples of Corollaries 6.8 and 6.9 cannot be  $\Gamma L(r, q^n)$ -equivalent.

**Proposition 6.12.** Let s, s' be two positive integers coprime with  $k \ge 2$  and let n = 2k, let  $\xi, \eta \in$  $\mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}$  and let  $f_i(x) = \mu_i x^{q^s} \in \mathcal{L}_k$  and  $g_\ell(x) = \overline{\mu}_\ell x^{q^{s'}} \in \mathcal{L}_k$  for  $i \in \{1, \ldots, r\}$  and  $\ell \in \{1, \ldots, r-1\}$ such that  $r \leq q-1$ ,  $N_{q^k/q}(\mu_i) \neq N_{q^k/q}(\mu_j)$ ,  $N_{q^k/q}(\overline{\mu}_i) \neq N_{q^k/q}(\overline{\mu}_j)$ ,  $N_{q^k/q}(\mu_i\mu_j\xi^{q^k+1}) \neq 1$  and  $N_{q^k/q}(\overline{\mu}_i\overline{\mu}_j\eta^{q^k+1}) \neq 1$  for every  $i \neq j$ . Then  $U = W_{f_1,\xi} \times \ldots \times W_{f_r,\xi}$  and  $W = W_{g_1,\eta} \times \ldots \times W_{f_r,\xi}$  $W_{g_{r-1},\eta} \times \mathbb{F}_{q^k}$  are  $\Gamma L(r,q^n)$ -inequivalent.

*Proof.* By Proposition 6.10, if U and W are  $\Gamma L(r, q^n)$ -equivalent then there exist  $i \in \{1, \ldots, r\}$ ,  $\lambda \in \mathbb{F}_{q^n}^*$  and  $\rho \in \operatorname{Aut}(\mathbb{F}_{q^n})$  such that

$$\mathbb{F}_{q^k} = \lambda(W_{f_i,\xi})^{\rho}$$

This cannot happen since the  $\mathbb{F}_q$ -subspace  $W_{f_i,\xi}$  has the property that

$$\dim_{\mathbb{F}_q}(W_{f_i,\xi} \cap \alpha W_{f_i,\xi}) \le 1,$$

for every  $\alpha \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$ . This property is preserved also by  $\lambda(W_{f_i,\xi})^{\rho}$ , but clearly  $\dim_{\mathbb{F}_q}(\mathbb{F}_{q^k} \cap \alpha \mathbb{F}_{q^k}) = k$  $\square$ if  $\alpha \in \mathbb{F}_{q^k} \setminus \mathbb{F}_q$ .

Moreover, arguing as before, the  $\Gamma L(r, q^n)$ -equivalence between two examples in Corollary 6.9 is determined in the next result.

**Proposition 6.13.** Let s, s' be two positive integers coprime with k and let n = 2k, let  $\xi, \eta \in$  $\mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}$  and let  $f_i(x) = \mu_i x^{q^s} \in \mathcal{L}_k$  and  $g_i(x) = \overline{\mu}_i x^{q^{s'}} \in \mathcal{L}_k$  for  $i \in \{1, \ldots, r-1\}$  such that  $r \leq q-1$ ,  $N_{q^k/q}(\mu_i) \neq N_{q^k/q}(\mu_j), N_{q^k/q}(\overline{\mu}_i) \neq N_{q^k/q}(\overline{\mu}_j), N_{q^k/q}(\mu_i\mu_j\xi^{q^k+1}) \neq 1 \text{ and } N_{q^k/q}(\overline{\mu}_i\overline{\mu}_j\eta^{q^k+1}) \neq 1 \text{ for } n \in \mathbb{N}$ every  $i \neq j$ . Then  $U = W_{f_1,\xi} \times \ldots \times W_{f_{r-1},\xi} \times \mathbb{F}_{q^k}$  and  $W = W_{g_1,\eta} \times \ldots \times W_{g_{r-1},\eta} \times \mathbb{F}_{q^k}$  are  $\Gamma L(r,q^n)$ equivalent if and only if there exist a permutation  $\sigma \in S_{r-1}$ ,  $\lambda_1, \ldots, \lambda_{r-1} \in \mathbb{F}_{q^n}^*$  and  $\rho \in \operatorname{Aut}(\mathbb{F}_{q^n})$ such that, for every  $i \in \{1, \ldots, r-1\}$ , one of the following occurs

• 
$$s \equiv s' \pmod{k}$$
,  $B = 0$ ,  $\xi = \frac{\eta^{\rho}}{A}$  and  $\overline{\mu}_{\sigma(i)} = \frac{\mu_{i}^{\nu} c}{A^{\rho-1}}$ , where  $c \in \mathbb{F}_{q^{k}}$  is such that  $N_{q^{k}/q}(c) = 1$ ;

• 
$$s \equiv -s' \pmod{k}, \ \xi = \frac{\eta^{\nu} + Aa}{A}, \ \overline{\mu}_{\sigma(i)} = \frac{1}{c\mu_i^{q^{-s_{\rho}-1}}A^{\rho^{-1}}b^{\rho^{-1}}} and B = -Aa, where \ c \in \mathbb{F}_{q^k} is such that N_{q^k/q}(c) = 1,$$

where  $\xi^2 = a\xi + b$  and  $\eta^{\rho} = A\xi + B$  with  $a, b, A, B \in \mathbb{F}_{a^k}$ .

6.2. Dual linear sets. Interestingly, the linear sets  $L_U$  of this section by duality give examples of sets with only three weights with respect to the hyperplanes and for each of these values there exists at least one hyperplane having this weight with respect to  $L_U$ .

**Theorem 6.14.** Let  $L_U$  be an  $\mathbb{F}_q$ -linear set in  $PG(r-1,q^n)$  of rank  $\frac{rn}{2}$  containing r independent points  $P_1 = \langle \mathbf{v}_1 \rangle_{\mathbb{F}_{q^n}}, \dots, P_r = \langle \mathbf{v}_r \rangle_{\mathbb{F}_{q^n}}$  such that

$$w_{L_U}(P_1) + \ldots + w_{L_U}(P_r) = \frac{rn}{2}.$$

Then for every hyperplane H in  $PG(r-1, q^n)$ 

$$w_{L_U^{\tau}}(H) \in \left\{ \frac{rn}{2} - n, \frac{rn}{2} - n + 1, \frac{rn}{2} - n + r \right\}.$$

More precisely,

- $w_{L_{U}^{\tau}}(H) = \frac{rn}{2} n + r$  if and only if  $H = P_i^{\tau}$  for some  $i \in \{1, \ldots, r\}$ ;

•  $w_{L_U^{\tau}}(H) = \frac{rn}{2} - n + 1$  if and only if  $H = P^{\tau}$  for some  $P \in L_U \setminus \{P_1, \dots, P_r\};$ •  $w_{L_U^{\tau}}(H) = \frac{rn}{2} - n$  if and only if  $H = P^{\tau}$  for some  $P \in PG(r-1, q^n) \setminus L_U.$ Moreover,

- the number of hyperplanes H such that  $w_{L_{U}^{\tau}}(H) = \frac{rn}{2} n + r$  is r;
- the number of hyperplanes H such that  $w_{L_U^{\tau}}(H) = \frac{rn}{2} n + 1$  is  $q^{\frac{rn}{2}-1} + \ldots + q^{\frac{n}{2}} (r 1)(q^{\frac{n}{2}-1} + \ldots + 1);$
- the number of hyperplanes H such that  $w_{L_U^{\tau}}(H) = \frac{rn}{2} n$  is  $\frac{q^{rn}-1}{q^n-1} q^{\frac{rn}{2}-1} \dots q^{\frac{n}{2}} + (r-1)(q^{\frac{n}{2}-1} + \dots + q) 1.$

*Proof.* By Theorem 6.4, it follows that all the point  $P_i$  have the same weight, that is,  $w_{L_U}(P_i) = \frac{n}{2}$  for every *i*. By applying Proposition 2.2 choosing *H* to be a hyperplane, we obtain

$$w_{L_U^{\tau}}(H) = w_{L_U}(H^{\tau}) + \frac{rn}{2} - (s+1)n$$

The assertion then follows by Remark 6.5.

The interest for these linear sets with few possible values for the weight of the hyperplanes is especially due to their coding theoretical counterparts that now we will briefly describe.

Let U be an  $\mathbb{F}_q$ -subspace of  $\mathbb{F}_{q^m}^r$  such that  $\langle U \rangle_{\mathbb{F}_{q^m}} = \mathbb{F}_{q^m}^r$ . Let G be a matrix in  $\mathbb{F}_{q^m}^{r \times \frac{rn}{2}}$  whose columns form an  $\mathbb{F}_q$ -basis of U. Let denote by  $\mathcal{C}$  be the  $\mathbb{F}_{q^m}$ -span of the rows of G and equip it with the *rank metric*, which is defined as follows

$$d(\mathbf{u},\mathbf{v}) = w(\mathbf{u}-\mathbf{v}) = \dim_{\mathbb{F}_q}(\langle u_1 - v_1, \dots, u_r - v_r \rangle_{\mathbb{F}_q}),$$

for any  $\mathbf{u} = (u_1, \ldots, u_r), \mathbf{v} = (v_1, \ldots, v_r) \in \mathbb{F}_{q^m}^r$ . So,  $\mathcal{C}$  is a **rank metric code** in  $\mathbb{F}_{q^m}^r$  and  $w(\mathbf{u})$  is said the **rank weight** of  $\mathbf{u}$ ; see [22, 39] for more details on rank metric codes. Noting that any element of  $\mathcal{C}$  may be seen as  $\mathbf{x}G$  for some  $\mathbf{x} \in \mathbb{F}_{q^m}^r$ , then in [36] (see also [1]) it was shown that

$$w(\mathbf{x}G) = \frac{rn}{2} - \dim_{\mathbb{F}_q}(U \cap \mathbf{x}^{\perp}),$$

where  $\mathbf{x}^{\perp}$  is the hyperplane whose equation is defined by the entries of  $\mathbf{x}$ .

As a consequence of Theorem 6.14 and the above described connection, the rank metric codes C have exactly three nonzero weights, which are n - r, n - 1, n. In particular, they are examples of (r - 1)-almost MRD codes, see [14], which means that the rank defect in the Singleton bound for rank metric codes is r - 1. Furthermore, we can also derive their weight distribution, indeed except for the zero vector we have

- $(q^n 1)r$  elements in  $\mathcal{C}$  having rank weight n r;
- $(q^n-1)\left(q^{\frac{rn}{2}-1}+\ldots+q^{\frac{n}{2}}-(r-1)(q^{\frac{n}{2}-1}+\ldots+1)\right)$  elements in  $\mathcal{C}$  having rank weight n-1;  $(q^n-1)\left(\frac{q^{rn}-1}{q^n-1}-q^{\frac{rn}{2}-1}-\ldots-q^{\frac{n}{2}}+(r-1)(q^{\frac{n}{2}-1}+\ldots+q)-1\right)$  elements in  $\mathcal{C}$  having rank weight n;

Moreover, using [1, Theorem 4.8], from  $L_U$  we can also construct linear Hamming metric codes with only three weights and for which we can completely establish their weight distribution, as already done for some classes of linear sets (see also [31,42]).

## 7. Conclusions

We conclude the paper with some problems that we think could be of interest for the reader.

**Problem 7.1.** In Theorem 3.6, we find a canonical form and explicit conditions for multi-orbit subspace codes with large minimum distance. Can this be used to provide new constructions and/or classification results?

**Problem 7.2.** In Corollary 4.5, we provide a lower bound on the number of semilinearly inequivalent codes of the form  $G_{n,s}$ . Determine the precise number of inequivalent codes of the form  $G_{n,s}$ .

Moreover, a multi-Sidon space U still preserves the uniqueness (up to some scalars in  $\mathbb{F}_q$ ) of the factorization of the product of any two elements contained in U.

**Proposition 7.3.** Let  $\{U_1, \ldots, U_r\}$  be a multi-Sidon space. Let  $k_i = \dim_{\mathbb{F}_q}(U_i) \ge 2$  for any  $i \in \{1, \ldots, r\}$ . Then for any  $i, j \in \{1, \ldots, r\}$  if  $a, c \in U_i$  and  $b, d \in U_j$  are such that ab = cd then  $\{a\mathbb{F}_q, b\mathbb{F}_q\} = \{c\mathbb{F}_q, d\mathbb{F}_q\}.$ 

*Proof.* By Corollary 3.4, when  $i \neq j$  the  $\mathbb{F}_q$ -subspaces  $U_i$  and  $U_j$  satisfy the property that for any nonzero  $a, c \in U_i$  and nonzero  $b, d \in U_j$  the equality ab = cd implies that  $a\mathbb{F}_q = c\mathbb{F}_q$  and  $b\mathbb{F}_q = d\mathbb{F}_q$ . The condition  $\dim_{\mathbb{F}_q}(U_i \cap \alpha U_i) \leq 1$  for every  $\alpha \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$  and  $i \in \{1, \ldots, r\}$  is equivalent to the fact that  $U_i$  is a Sidon space for every i because of Theorem 1.2. Therefore the assertion follows.  $\Box$ 

So, a possible generalization of Sidon spaces could be the following one.

Consider  $U_1, \ldots, U_r$  be r distinct  $\mathbb{F}_q$ -subspaces of  $\mathbb{F}_{q^n}$ . We say that  $\{U_1, \ldots, U_r\}$  is a **weak multi-Sidon space** of  $\mathbb{F}_{q^n}$  if the product of any two nonzero elements from  $U_i$ 's may be uniquely factorized, up to a scalar factor from  $\mathbb{F}_q$ . More precisely, for any  $i, j \in \{1, \ldots, r\}$  if  $a, c \in U_i$  and  $b, d \in U_j$  are such that ab = cd then

$$\{a\mathbb{F}_q, b\mathbb{F}_q\} = \{c\mathbb{F}_q, d\mathbb{F}_q\}.$$

This latter definition generalizes the property of being multi-Sidon space, as proved in Proposition 7.3. However, we still do not know whether or not there exists examples of weakly multi-Sidon spaces which are not multi-Sidon spaces. So, we propose the following problem.

**Problem 7.4.** Are the properties of being multi-Sidon space and weaker multi-Sidon space equivalent? If not, construct counterexamples.

### Acknowledgements

I would like to thank Oriol Serra, who suggested me to study Sidon spaces during the conference *Discretaly* (2018). I would also like to thank the anonymous referee for their suggestions. The research was supported by the project "VALERE: VanviteLli pEr la RicErca" of the University of Campania "Luigi Vanvitelli" and was partially supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM).

### References

- G.N. ALFARANO, M. BORELLO, A. NERI AND A. RAVAGNANI: Linear cutting blocking sets and minimal codes in the rank metric, J. Combin. Theory Ser. A 192 (203): 105658.
- [2] L. BABAI AND V.T. Sós: Sidon sets in groups and induced subgraphs of Cayley graphs, European J. Combin. 6(2) (1985), 101–114.
- [3] C. BACHOC, O. SERRA AND G. ZÉMOR: An analogue of Vosper's theorem for extension fields, Math. Proc. Cambridge Philos. Soc. 163(3) (2017), 423–452.
- [4] C. BACHOC, O. SERRA AND G. ZÉMOR: Revisiting Kneser's theorem for field extensions, Combinatorica 38(4) (2018), 759–777.
- [5] S. BALL: The number of directions determined by a function over finite field, J. Combin. Theory Ser. A 104 (2003), 341–350.
- [6] S. BALL, A. BLOKHUIS, A. E. BROUWER, L. STORME AND T. SZŐNYI: On the number of slopes of the graph of a function defined on a finite field, J. Combin. Theory Ser. A 86(1) (1999), 187–196.
- [7] E. BEN-SASSON, T. ETZION, A. GABIZON AND N. RAVIV: Subspace polynomials and cyclic subspace codes, IEEE Trans. Inform. Theory 62(3) (2016), 1157–1165.
- [8] G. BONOLI AND O. POLVERINO:  $\mathbb{F}_q$ -linear blocking sets in PG(2,  $q^4$ ), Innov. Incidence Geom. 2 (2005), 35–56.

- [9] K. O'BRYANT: A complete annotated bibliography of work related to Sidon sequences, *Electron. J. Combin.* 575(1) (2004), 1–39.
- [10] J. CILLERUELO: Combinatorial problems in finite fields and Sidon sets, Combinatorica 32(5) (2012), 497–511.
- [11] J. CILLERUELO, I. RUZSA AND C. VINUESA: Generalized Sidon sets, Adv. Math. 225(5) (2010), 2786–2807.
- [12] B. CSAJBÓK, G. MARINO AND O. POLVERINO: Classes and equivalence of linear sets in  $PG(1, q^n)$ , J. Combin. Theory Ser. A 157 (2018), 402–426.
- [13] B. CSAJBÓK AND C. ZANELLA: On the equivalence of linear sets, Des. Codes Cryptogr. 81 (2016), 269–281.
- [14] J. DE LA CRUZ: On dually almost MRD codes, *Finite Fields Appl.* 53 (2018), 1–20.
- [15] P. ERDŐS: Solved and unsolved problems in combinatorics and combinatorial number theory, Congr. Numer. 32 (1981), 49–62.
- [16] T. ETZION AND A. VARDY: Error-correcting codes in projective space, IEEE Trans. Inform. Theory 57(2) (2011), 1165—1173.
- [17] T. FENG AND Y. WANG: New constructions of large cyclic subspace codes and Sidon spaces, Discrete Math. 344(4) (2021), 112273.
- [18] H. GLUESING-LUERSSEN AND H. LEHMANN: Automorphism groups and isometries for cyclic orbit codes, to appear in Advances in Mathematics of Communications (2021), https://doi.org/10.3934/amc.2021040.
- [19] R. GOW AND R. QUINLAN: Galois extensions and subspaces of alterning bilinear forms with special rank properties, *Linear Algebra Appl.* 430 (2009), 2212–2224.
- [20] R. GOW AND R. QUINLAN: Galois theory and linear algebra, Linear Algebra Appl. 430 (2009), 1778–1789.
- [21] X. HOU, K.H. LEUNG AND Q. XIANG: A generalization of an addition theorem of Kneser, J. Number Theory 97 (2002), 1–9.
- [22] E. GORLA: Rank-metric codes, A Concise Encyclopedia of Coding Theory, W.C. Huffman, J.-L. Kim, and P. Solé Eds., CRC Press.
- [23] R.M. GURALNICK: Invertible preservers and algebraic groups, Linear Algebra Appl. 212 (1994), 249–257.
- [24] D. JENA AND G. VAN DE VOORDE: The geometric field of linearity of linear sets, Des. Codes Cryptogr. (2022), 1-21, https://doi.org/10.1007/s10623-022-01011-9.
- [25] R. KOETTER AND F. R. KSCHISCHANG: Coding for errors and erasures in random network coding, *IEEE Trans. Inform. Theory* 54 (2008), 3579—3591.
- [26] M. LAVRAUW AND G. VAN DE VOORDE: Field reduction and linear sets in finite geometry, In: Topics in Finite Fields, AMS Contemporary Math, vol. 623, pp. 271-293. American Mathematical Society, Providence (2015).
- [27] R. LIDL AND H. NIEDERREITER: Finite fields, volume 20 of *Encyclopedia of Mathematics and its Applications*, Cambridge University Press, Cambridge, second edition, 1997.
- [28] G. LUNARDON, G. MARINO, O. POLVERINO AND R. TROMBETTI: Translation dual of a semifield, J. Combin. Theory Ser. A Ser. A 115(8) (2008), 1321–1332.
- [29] V. NAPOLITANO, P. SANTONASTASO, O. POLVERINO AND F. ZULLO: Linear sets on the projective line with complementary weights, *Discrete Math.* **345(7)** (2022), 112890.
- [30] V. NAPOLITANO, P. SANTONASTASO, O. POLVERINO AND F. ZULLO: Classifications and constructions of minimum size linear sets, arXiv:2201.02003.
- [31] V. NAPOLITANO AND F. ZULLO: Codes with few weights arising from linear sets. to appear in Advances in Mathematics of Communications (2020), https://doi.org/10.3934/amc.2020129.
- [32] Y. NIU, Y. QIN AND Y. WU: Several kinds of large cyclic subspace codes via Sidon spaces, *Discrete Math.* 343(5) (2020), 111788.
- [33] K. OTAL AND F. OZBUDAK: Cyclic subspace codes via subspace polynomials, Des. Codes Cryptogr. 85(2) (2017), 191–204.
- [34] K. OTAL AND F. OZBUDAK: Constructions of cyclic subspace codes and maximum rank distance codes, Network Coding and Subspace Designs, Springer, Cham (2018), 43–66.
- [35] O. POLVERINO: Linear sets in finite projective spaces, Discrete Math. 310(22) (2010), 3096–3107.
- [36] T.H. RANDRIANARISOA: A geometric approach to rank metric codes and a classification of constant weight codes, *Des. Codes Cryptogr.* 80(1) (2020).
- [37] R. M. ROTH, N. RAVIV AND I. TAMO: Construction of Sidon spaces with applications to coding, *IEEE Trans. Inform. Theory* 64(6) (2018), 4412–4422.
- [38] P. SANTONASTASO AND F. ZULLO: Linearized trinomials with maximum kernel, J. Pure Appl. Algebra **226(3)** (2022), 106842.
- [39] J. SHEEKEY: 13. MRD codes: Constructions and connections, Combinatorics and finite fields: Difference sets, polynomials, pseudorandomness and applications, Vol. 23. de Gruyter (2019), 255–286.

- [40] A.-L. TRAUTMANN: Isometry and automorphisms of constant dimension codes, Adv. Math. Commun. 7 (2013), 147–160.
- [41] A. L. TRAUTMANN, F. MANGANIELLO, M. BRAUN AND J. ROSENTHAL: Cyclic orbit codes, IEEE Trans. Inform. Theory 59(11) (2013), 7386–7404.
- [42] G. ZINI AND F. ZULLO: Scattered subspaces and related codes, Des. Codes Cryptogr. 89 (2021), 1853–1873.

# Appendix A. Polynomial representation of linear sets in $PG(r-1, q^n)$ determined by r points

One of the most studied research topic on polynomials over finite fields regards the construction of polynomials or functions for which their value sets over a fixed finite field has some interesting properties, such as being small, large or with other preassigned conditions. Clearly, the problem becomes more and more difficult when considering t-tuple of polynomials. In this appendix, we will show examples of t-tuples of linearized polynomials such that the size of the value set

$$\operatorname{Im}\left(\frac{f_1(x)}{x},\ldots,\frac{f_t(x)}{x}\right) = \left\{\left(\frac{f_1(x)}{x},\ldots,\frac{f_t(x)}{x}\right) : x \in \mathbb{F}_{q^n}^*\right\}$$

is determined, see [5,6]. The key idea is to use the linear sets investigated in Section 6.

Let  $U_1, \ldots, U_t$  be  $\mathbb{F}_q$ -subspaces of  $\mathbb{F}_{q^n}$  seen as an *n*-dimensional  $\mathbb{F}_q$ -vector space such that

$$U_1 \oplus \ldots \oplus U_t = \mathbb{F}_{q^n}.$$

Every vector  $\mathbf{v} \in \mathbb{F}_{q^n}$  can be written uniquely as

$$\mathbf{v} = \mathbf{v}_1 + \ldots + \mathbf{v}_t,$$

where  $\mathbf{v}_i \in U_i$  for every  $i \in \{1, \ldots, t\}$ . The vector  $\mathbf{v}_i$  will be called the *i*-th **component** of  $\mathbf{v}$  (with respect to  $U_1, \ldots, U_t$ ) and the map  $p_i \colon \mathbb{F}_{q^n} \to U_i$  such that  $p_i(\mathbf{v}) = \mathbf{v}_i$  is called the *i*-th **projection** map.

We also recall the definition of dual bases. Two ordered  $\mathbb{F}_q$ -bases  $\mathcal{B} = (\xi_0, \ldots, \xi_{n-1})$  and  $\mathcal{B}^* = (\xi_0^*, \ldots, \xi_{n-1}^*)$  of  $\mathbb{F}_{q^n}$  are said to be **dual bases** if  $\operatorname{Tr}_{q^n/q}(\xi_i\xi_j^*) = \delta_{ij}$ , for  $i, j \in \{0, \ldots, n-1\}$ , where  $\delta_{ij}$  is the Kronecker symbol. It is well known that for any  $\mathbb{F}_q$ -basis  $\mathcal{B} = (\xi_0, \ldots, \xi_{n-1})$  there exists a unique dual basis  $\mathcal{B}^* = (\xi_0^*, \ldots, \xi_{n-1}^*)$  of  $\mathcal{B}$ , see e.g. [27, Definition 2.30].

**Lemma A.1.** Let  $U_1, \ldots, U_t$  be  $\mathbb{F}_q$ -subspaces of  $\mathbb{F}_{q^n}$  seen as an n-dimensional  $\mathbb{F}_q$ -vector space such that

$$U_1 \oplus \ldots \oplus U_t = \mathbb{F}_{q^n}.$$

Denote by  $k_i$  the dimension of  $U_i$  and let  $\mathcal{B}_i = (\xi_{i,0}, \ldots, \xi_{i,k_i-1})$  an ordered  $\mathbb{F}_q$ -basis of  $U_i$  for every  $i \in \{1, \ldots, t\}$ . Let  $\mathcal{B}^* = (\xi_{1,0}^*, \ldots, \xi_{1,k_1-1}^*, \ldots, \xi_{t,0}^*, \ldots, \xi_{t,k_t-1}^*)$  be the dual basis of  $\mathcal{B} = (\xi_{1,0}, \ldots, \xi_{1,k_1-1}, \ldots, \xi_{t,0}, \ldots, \xi_{t,k_t-1})$ . Then

$$p_i(x) = \sum_{j=0}^{k_i - 1} \xi_{i,j} \operatorname{Tr}_{q^n/q}(\xi_{i,j}^* x) = \sum_{\ell=0}^{n-1} \left( \sum_{j=0}^{k_i - 1} \xi_{i,j} \xi_{i,j}^{*q^{\ell}} \right) x^{q^{\ell}}.$$

*Proof.* Since  $U_1 \oplus \ldots \oplus U_t = \mathbb{F}_{q^n}$ , every  $x \in \mathbb{F}_{q^n}$  can be uniquely written as

$$x = x_1 + \ldots + x_t,$$

with  $x_i \in U_i$  for every  $i \in \{1, \ldots, t\}$ . Let  $i \in \{1, \ldots, t\}$  and let

$$\overline{p}(x) = \sum_{j=0}^{k_i-1} \xi_{i,j} \operatorname{Tr}_{q^n/q}(\xi_{i,j}^* x).$$

Then it is easy to see that

$$\overline{p}(\xi_{\ell,m}) = \sum_{j=0}^{k_i-1} \xi_{i,j} \operatorname{Tr}_{q^n/q}(\xi_{i,j}^* \xi_{\ell,m}) = \begin{cases} \xi_{\ell,m} & \text{if } \ell = i, \\ 0 & \text{otherwise,} \end{cases}$$

for any  $(\ell, m)$  such that  $\ell \in \{1, \ldots, t\}$  and  $m \in \{0, \ldots, k_{\ell} - 1\}$ . This means that  $\overline{p}(x)$  coincides with the *i*-th projection map.

For linear sets  $L_U$  in  $PG(r-1, q^n)$  of rank *n* containing *r* independent points  $P_1, \ldots, P_r$  such that

$$w_{L_U}(P_1) + \ldots + w_{L_U}(P_r) = n$$

we can determine r linearized polynomials representing it.

**Theorem A.2.** Let  $L_W$  be an  $\mathbb{F}_q$ -linear set in  $PG(r-1, q^n)$  of rank n containing r independent points  $P_1 = \langle \mathbf{v}_1 \rangle_{\mathbb{F}_{q^n}}, \ldots, P_r = \langle \mathbf{v}_r \rangle_{\mathbb{F}_{q^n}}$  such that

$$w_{L_W}(P_1) + \ldots + w_{L_W}(P_r) = n.$$

Then  $L_W$  is  $PGL(r, q^n)$ -equivalent to

$$L_p = \{ \langle (x, p_2(x), \dots, p_r(x)) \rangle_{\mathbb{F}_{q^n}} \colon x \in \mathbb{F}_{q^n}^* \}$$

where  $p_i(x)$  is the *i*-th projection map with respect to  $r \mathbb{F}_q$ -subspaces  $U_1, \ldots, U_r$  of  $\mathbb{F}_{q^n}$  such that

$$U_1 \oplus \ldots \oplus U_r = \mathbb{F}_{q^r}$$

Moreover, if  $k_i$  is the dimension of  $U_i$  and  $\mathcal{B}_i = (\xi_{i,0}, \ldots, \xi_{i,k_i-1})$  is an ordered  $\mathbb{F}_q$ -basis of  $U_i$  for every  $i \in \{1, \ldots, t\}$ , then

$$p_i(x) = \sum_{j=0}^{k_i-1} \xi_{i,j} \operatorname{Tr}_{q^n/q}(\xi_{i,j}^* x) = \sum_{\ell=0}^{n-1} \left( \sum_{j=0}^{k_i-1} \xi_{i,j} \xi_{i,j}^{*q^{\ell}} \right) x^{q^{\ell}}$$

for every  $i \in \{2, \ldots, r\}$ , where  $\mathcal{B}^* = (\xi_{1,0}^*, \ldots, \xi_{1,k_1-1}^*, \ldots, \xi_{t,0}^*, \ldots, \xi_{t,k_t-1}^*)$  is the dual basis of  $\mathcal{B} = (\xi_{1,0}, \ldots, \xi_{1,k_1-1}, \ldots, \xi_{t,0}, \ldots, \xi_{t,k_t-1})$ .

Proof. By Proposition 6.1,  $L_W$  is  $\operatorname{PGL}(r, q^n)$ -equivalent to  $L_U$  where  $U = U_1 \times \ldots \times U_r$ , for some  $\mathbb{F}_q$ -subspaces  $U_1, \ldots, U_r$  of  $\mathbb{F}_{q^n}$  such that  $U_i \cap \langle U_j : j \in \{1, \ldots, r\} \setminus \{i\} \rangle_{\mathbb{F}_q} = \{\mathbf{0}\}$  for any  $i \in \{1, \ldots, r\}$ . Let f be the  $\mathbb{F}_{q^n}$ -linear isomorphism of  $\mathbb{F}_{q^n}^r$  determined by the matrix

then

$$f(U) = \{(x, p_2(x), \dots, p_r(x)) \colon x \in \mathbb{F}_{q^n}\}$$

and the assertion then follows by Lemma A.1.