2021

Weight Distributions, Automorphisms, and Isometries of Cyclic Orbit Codes

Hunter Lehmann
University of Kentucky, hlehmann277@gmail.com
Author ORCID Identifier:
https://orcid.org/0000-0002-2913-0883
Digital Object Identifier: https://doi.org/10.13023/etd.2021.246

STUDENT AGREEMENT:

I represent that my thesis or dissertation and abstract are my original work. Proper attribution has been given to all outside sources. I understand that I am solely responsible for obtaining any needed copyright permissions. I have obtained needed written permission statement(s) from the owner(s) of each third-party copyrighted matter to be included in my work, allowing electronic distribution (if such use is not permitted by the fair use doctrine) which will be submitted to UKnowledge as Additional File.

I hereby grant to The University of Kentucky and its agents the irrevocable, non-exclusive, and royalty-free license to archive and make accessible my work in whole or in part in all forms of media, now or hereafter known. I agree that the document mentioned above may be made available immediately for worldwide access unless an embargo applies.

I retain all other ownership rights to the copyright of my work. I also retain the right to use in future works (such as articles or books) all or part of my work. I understand that I am free to register the copyright to my work.

REVIEW, APPROVAL AND ACCEPTANCE

The document mentioned above has been reviewed and accepted by the student's advisor, on behalf of the advisory committee, and by the Director of Graduate Studies (DGS), on behalf of the program; we verify that this is the final, approved version of the student's thesis including all changes required by the advisory committee. The undersigned agree to abide by the statements above.

Hunter Lehmann, Student

Dr. Heide Gluesing-Luerssen, Major Professor

Dr. Benjamin Braun, Director of Graduate Studies

Weight Distributions, Automorphisms, and Isometries of Cyclic Orbit Codes

DISSERTATION

A dissertation submitted in partial
fulfillment of the requirements for
the degree of Doctor of Philosophy
in the College of Arts and Sciences
at the University of Kentucky

By
Hunter Ryan Lehmann
Lexington, Kentucky

Director: Dr. Heide Gluesing-Luerssen, Professor of Mathematics
Lexington, Kentucky
2021

https://orcid.org/0000-0002-2913-0883

ABSTRACT OF DISSERTATION

Weight Distributions, Automorphisms, and Isometries of Cyclic Orbit Codes

Cyclic orbit codes are subspace codes generated by the action of the Singer subgroup $\mathbb{F}_{q^n}^*$ on an $\mathbb{F}_q$-subspace U of $\mathbb{F}_{q^n}$. The weight distribution of a code is the vector whose i^{th} entry is the number of codewords with distance i to a fixed reference space in the code. My dissertation investigates the structure of the weight distribution for cyclic orbit codes. We show that for full-length orbit codes with maximal possible distance the weight distribution depends only on q, n, and the dimension of U. For full-length orbit codes with lower minimum distance, we provide partial results towards a characterization of the weight distribution, especially in the case that any two codewords intersect in a space of dimension at most 2. We also briefly address the weight distribution of a union of full-length orbit codes with maximum distance.

A related problem is to find the automorphism group of a cyclic orbit code, which plays a role in determining the isometry classes of the set of all cyclic orbit codes. First we show that the automorphism group of a cyclic orbit code is contained in the normalizer of the Singer subgroup if the orbit is generated by a subspace that is not contained in a proper subfield of $\mathbb{F}_{q^n}$. We then generalize to orbits under the normalizer of the Singer subgroup, although in this setup there is a remaining exceptional case. Finally, we can characterize linear isometries between such codes.

KEYWORDS: coding theory, subspace codes, cyclic orbit codes, linear isometries, automorphism groups, weight distribution

Hunter Ryan Lehmann

July 8, 2021

Weight Distributions, Automorphisms, and Isometries of Cyclic Orbit Codes

By
Hunter Ryan Lehmann

Dr. Heide Gluesing-Luerssen
Director of Dissertation

Dr. Benjamin Braun
Director of Graduate Studies

July 8, 2021
Date

Dedicated to Mom and Dad.

ACKNOWLEDGMENTS

There are so many people I have to thank for helping me get to this point, but foremost among them is my amazing advisor Dr. Heide Gluesing-Luerssen. You have helped me develop so much as a researcher over the last four years. Thank you for all of your help and patience, most notably when I'm rambling during our meetings and when I struggle to stay focused.

I also want to thank the rest of the amazing people in the math department, especially Sheri, Christine, and Rejeana, who have made sure that all the gears keep spinning. Dr. Braun, Dr. Whitaker, thank you for all of your help and mentorship with all things teaching - your advice throughout the years has been immeasurably helpful.

I wouldn't be in grad school at all, let alone finishing my PhD, without the help and inspiring examples of many of my professors from undergrad, especially Jason Heinze and Dr. Howell at Olympic College and Dr. Bahuaud, Dr. Henrich, Dr. Klee, Dr. Oliveras, and Dr. Robertson at Seattle University. If I can be half the teacher and mentor to my future students that you were to me I will be happy.

Next, all of my friends I've made here who keep me (mostly) sane. In particular, thanks Kalila for making the world a brighter place all the time. Kaelin, Margaret, Camille - I'll miss you all and our various hikes and game nights. Joe, Carissa, thanks for helping make the eighth floor the best floor and dragging me to Country Boy. Finally, thanks to Jessica, Matias, Susanna, Jake, and the rest of the cohort for being friends during the crucible that is graduate school.

Last but not least, my parents. Dad, you've been my role model for years - thank you for showing me a great example and telling me that it's ok to make big changes during the tough times in my life. Mom, I doubt I would be here now if you hadn't

seen that I could do more back in first grade and spent the next twelve years of your life homeschooling me. Thank you for always believing in me and supporting me throughout everything.

TABLE OF CONTENTS

LIST OF TABLES

Chapter 1 Introduction & Preliminaries

1.1 Introduction

This dissertation is comprised of three major sections: first, we discuss some preliminary facts regarding subspace codes and cyclic orbit codes in particular; second, we introduce the concept of the weight distribution of a cyclic orbit code and prove a variety of results about it; third, we discuss the linear isometry classes of cyclic orbit codes.

Subspace codes came into focus in 2008 when Kötter and Kschischang [22] proposed them as a solution to the problem of random network coding. Since then, many authors have investigated subspace codes, especially focusing on the problems of maximizing their size given a fixed ambient space and minimum distance and of finding algebraic constructions; see the papers [4, 13, 19, 17, 16, 27] and themonograph [15] for some of the more recent efforts. A cyclic orbit code is a subspace code of the form $\mathrm{Orb}(U) := \{\alpha U \mid \alpha \in \mathbb{F}_{q^n}^*\}$, where U is an $\mathbb{F}_q$-subspace of the field extension $\mathbb{F}_{q^n}$. These codes have been researched heavily in the last ten years; see [1, 3, 8, 12, 25, 30, 31]. In particular it is a constant-dimension code, that is, all subspaces in the code have the same dimension, namely $k := \dim(U)$.

The weight distribution of a cyclic orbit code encodes, for any possible subspace distance, the number of codewords with that distance to a specified generator, and can thus detect subspace codes with the fewest number of codeword pairs attaining the minimum distance. Such codes may be regarded as superior to those with the same minimum distance but with more codewords attaining that distance. In this sense, the weight distribution is a tool for a finer classification of cyclic orbit codes than the distance.

It is well known that if $\mathrm{Orb}(U)$ has maximum possible distance, i.e. $2k$, then k is a divisor of n and U is a shift of the subfield $\mathbb{F}_{q^k}$. These codes are known as spread codes and their weight distribution is trivial because all subspaces intersect pairwise trivially. Their downside is their small size: they contain only $(q^n-1)/(q^k-1)$ codewords, which is the smallest size of any cyclic orbit code generated by a k-dimensional subspace. On the other hand, the largest size of such a code is $(q^n-1)/(q-1)$, and codes attaining this size will be called full-length orbit codes. Full-length orbit codes with distance $2k-2$, which is the best possible, will be called optimal full-length orbit codes. Hence optimal full-length orbit codes maximize the size of the code as well as the distance (as long as the latter is less than $2k$).

Over the last few years, several different constructions of optimal full-length orbit codes have been found [1, 3, 25]. In 2018, Roth, Raviv, and Tamo [26] showed that all of these codes are generated by subspaces known as Sidon spaces. Our first major result, Theorem 21, shows that the weight distribution of optimal full-length orbit codes is fully determined by the parameters q, n, and k, regardless of the choice of Sidon space. In deriving this result, another interesting parameter arises, namely the number, $f(U)$, of fractions inside the field $\mathbb{F}_{q^n}$ that can be obtained from elements

of the given subspace U (up to factors from $\mathbb{F}_q$). For Sidon spaces this number is fully determined by q, n, k. Furthermore, we provide the minimum and maximum possible value of $f(U)$ over all k-dimensional subspaces and show that $f(U)$ is minimal iff $\mathrm{Orb}(U)$ is a spread code and maximal iff $\mathrm{Orb}(U)$ is an optimal full-length orbit code.

In Section 2.3, we investigate the weight distribution of full-length orbit codes with distance less than $2k-2$. In this case, the weight distribution is – unsurprisingly – not fully determined by q, n, k and the distance. In Theorem 23 we describe the weight distribution as closely as possible for the case where the distance is $2k-4$. It involves, in addition to q, n, and k, a further parameter r, whose meaning will become clear in Section 2.3. Various examples illustrate possible values of this parameter, but more work is needed to find its exact range or at least bounds. Alternatively, the weight distribution is fully determined by q, n, k and the above mentioned parameter $f(U)$. However, we do not yet understand what values $f(U)$ may take or how to design subspaces with a particular value.

Finally, in Section 2.4 we consider codes that are the union of optimal full-length orbit codes. Constructions of such codes can be found in [26]. We show that Theorem 21 generalizes straightforwardly to this scenario, that is, the weight distribution is fully determined by q, n, k, and the number of orbits in the union.

Throughout the dissertation, we will in fact study the intersection distribution rather than the weight distribution. That is, we count the number of codeword pairs whose intersection attains a given dimension. Thanks to the definition of the subspace distance in (1.2.1) this is clearly equivalent to studying the weight distribution.

Given the result of Theorem 21, it is natural to ask whether all optimal cyclic orbit codes are in fact 'the same'. In this context, the proper notion of 'same' is that of linear isometry. In Chapter 3, we will study the automorphism groups of cyclic orbit codes and orbit codes under the Singer normalizer in order to determine these possible isometries. As usual, the automorphism group of a subspace code is defined as the subgroup of $\mathrm{GL}_n(q)$ that leaves the code invariant. We will prove the following result. Let $\mathcal{U}$ be a subspace of $\mathbb{F}_{q^n}$ containing 1 (which is no restriction) and let $\mathbb{F}_{q^s}$ be the smallest subfield of $\mathbb{F}_{q^n}$ containing $\mathcal{U}$. Then the automorphism group is contained in the normalizer of the extension-field subgroup $\mathrm{GL}_{n/s}(q^s)$, where the latter is defined as the subgroup of all $\mathbb{F}_{q^s}$-linear automorphisms of $\mathbb{F}_{q^n}$. In particular, if $\mathcal{U}$ is generic, i.e., not contained in a proper subfield of $\mathbb{F}_{q^n}$, the automorphism group of the cyclic orbit code generated by $\mathcal{U}$ is contained in the normalizer of the Singer subgroup $\mathbb{F}_{q^n}^*$. In order to prove these results we will derive a lower bound on the length of the $\mathrm{GL}_{n/s}(q^s)$-orbit of $\mathcal{U}$ for any given divisor s of n. A crucial role will be played by the parameter $\delta_s(\mathcal{U})$, which is the $\mathbb{F}_{q^s}$-dimension of the $\mathbb{F}_{q^s}$-subspace generated by $\mathcal{U}$. Note that $\delta_s(\mathcal{U}) = 1$ iff $\mathcal{U} \subseteq \mathbb{F}_{q^s}$.

We then turn to orbit codes under the normalizer of the Singer subgroup and derive the same results for the automorphism groups as long as the orbit code is generated by a subspace $\mathcal{U}$ satisfying $\delta_s(\mathcal{U}) \neq 2$. The case $\delta_s(\mathcal{U}) = 2$ is of particular interest: the above results hold for many parameter cases, while there exist counterexamples for others. We strongly believe that these examples are the only exceptions to our main result on the automorphism group.

We finally discuss linear isometries, i.e., maps from $\mathrm{GL}_n(q)$, between cyclic orbit codes and orbit codes under the Singer normalizer. Our results on the automorphism groups immediately imply the following facts for orbits generated by generic subspaces: (i) a linear isometry between cyclic orbit codes is in the normalizer of $\mathbb{F}_{q^n}^*$; (ii) linearly isometric orbit codes under the Singer normalizer are in fact equal – with the possible exception of orbits generated by subspaces $\mathcal{U}$ with $\delta_s(\mathcal{U}) = 2$ for some s. This drastically reduces the work load for testing isometry between such codes. The nature of our counterexamples leads us to believe that the last statement does not need the assumption on $\delta_s(\mathcal{U})$. We close the chapter with some examples listing the number of distinct isometry classes of cyclic orbit codes and, making use of the results of Chapter 2, also provide the weight distribution for each class.

1.2 Preliminaries

In this section, we'll collect the basic results that we will make use of throughout the rest of the dissertation.

Subspace Codes and Cyclic Orbit Codes

We begin by recalling some basic facts about subspace codes and cyclic orbit codes. Throughout we fix a finite field $\mathbb{F}_q$ with q a prime power. A *subspace code (of block length n)* is simply a collection of subspaces in $\mathbb{F}_q^n$ with at least two elements. The code is called a *constant-dimension code* if all subspaces have the same dimension. The *distance between two subspaces* $V, W \subseteq \mathbb{F}_q^n$ is defined as

$$\mathrm{d}(V, W) := \dim V + \dim W - 2\dim(V \cap W) \tag{1.2.1}$$

and the *subspace distance* of a subspace code $\mathcal{C}$ is

$$\mathrm{d}(\mathcal{C}) := \min\{\mathrm{d}(V, W) \mid V, W \in \mathcal{C}, V \neq W\}. \tag{1.2.2}$$

We can see immediately that any two subspaces V and W of the same dimension k have distance $2k - 2\dim(V \cap W)$ which must be even and is at most $2k$. In a constant-dimension code, therefore, the subspace distance of the code is also even and at most $2k$.

Cyclic orbit codes are most conveniently defined in the field extension $\mathbb{F}_{q^n}$, considered as an n-dimensional $\mathbb{F}_q$-vector space. Let $\mathcal{G}_q(k, n)$ be the Grassmannian of k-dimensional $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^n}$. Then $\mathbb{F}_{q^n}^*$ induces a group action on $\mathcal{G}_q(k, n)$ via $(\alpha, U) \longmapsto \alpha U$, where $\alpha U = \{\alpha u \mid u \in U\}$, which of course is a subspace in $\mathcal{G}_q(k, n)$. A constant-dimension code in $\mathcal{G}_q(k, n)$ is called a *cyclic subspace code* if it is invariant under this group action. Hence cyclic subspace codes are unions of orbits under this action. Throughout most of Chapter 2 we will study codes that form a single orbit and only in Section 2.4 turn to more general cyclic subspace codes. We fix the terminology of cyclic orbit codes and list some properties in the next definition. Further details can be found in [12].

Definition 1. Let $U \in \mathcal{G}_q(k,n)$. The orbit of U under the group action given by $\mathbb{F}_{q^n}^*$, that is $\mathrm{Orb}(U) := \{\alpha U \mid \alpha \in \mathbb{F}_{q^n}^*\}$, is called the *cyclic orbit code generated by* U. It is a constant-dimension code of dimension k. The *stabilizer* of U is denoted by $\mathrm{Stab}(U) := \{\alpha \in \mathbb{F}_{q^n}^* \mid \alpha U = U\}$. It is easy to see that $\mathrm{Stab}(U) = \mathbb{F}_{q^t}^*$ for some $t \in \mathbb{N}$ (which is a divisor of $\gcd(k,n)$). In fact, the field $\mathbb{F}_{q^t}$ is the largest subfield of $\mathbb{F}_{q^n}$ over which U is a vector space, i.e., U is closed under multiplication by scalars in $\mathbb{F}_{q^t}$. The orbit-stabilizer theorem tells us that if $\mathrm{Stab}(U) = \mathbb{F}_{q^t}^*$ then $|\mathrm{Orb}(U)| = (q^n-1)/(q^t-1)$. If $t = 1$, we call $\mathrm{Orb}(U)$ a *full-length orbit code*.

From this we can see that the longest possible length of a cyclic orbit code is $(q^n-1)/(q-1)$ and the smallest possible length is 1, achieved by picking $U = \mathbb{F}_{q^n}$.

In [6, Thm. 2.1] it has been shown that for any divisor t of $\gcd(k,n)$ the number of orbits in $\mathcal{G}_q(k,n)$ of length $(q^n-1)/(q^t-1)$ is given by

$$\frac{q^t-1}{q^n-1}\sum_{s\in\mathcal{S}}\mu(s/t)\begin{bmatrix} n/s \\ k/s \end{bmatrix}_{q^s},$$

where $\mathcal{S} = \{s \in \mathbb{N} : t \mid s \text{ and } s \mid \gcd(k,n)\}$ and μ is the Möbius function.

Taking the stabilizer into account, we can give a more concise description of the orbit. In order to do so, we make the following definition. It appeared first in [1, Def. 4].

Definition 2. Let $t \in \mathbb{N}$ be a divisor of n. On $\mathbb{F}_{q^n}^*$ we define the equivalence relation

$$\alpha \sim_t \beta \iff \frac{\alpha}{\beta} \in \mathbb{F}_{q^t}.$$

Note that the right hand side is equivalent to $\alpha\mathbb{F}_{q^t}^* = \beta\mathbb{F}_{q^t}^*$. We set $\mathbb{F}_{q^n}^*/_{\sim_t} = \mathbb{P}_t(\mathbb{F}_{q^n})$, the *projective space* over the $\mathbb{F}_{q^t}$-vector space $\mathbb{F}_{q^n}$. Clearly $|\mathbb{P}_t(\mathbb{F}_{q^n})| = \frac{q^n-1}{q^t-1}$. The equivalence class of $\alpha \in \mathbb{F}_{q^n}^*$ is denoted by $\overline{\alpha}^{(t)}$. For $t = 1$ we omit the subscript/superscript; thus $\alpha \sim \beta \iff \alpha\beta^{-1} \in \mathbb{F}_q$ and $\mathbb{P}(\mathbb{F}_{q^n}) = \mathbb{P}_1(\mathbb{F}_{q^n}) = \{\overline{\alpha} \mid \alpha \in \mathbb{F}_{q^n}\}$.

Note that $\overline{\alpha}^{(t)} = \alpha\mathbb{F}_{q^t}^*$ and the projective space $\mathbb{P}_t(\mathbb{F}_{q^n})$ is actually the cyclic orbit code generated by $\mathbb{F}_{q^t}$ if we add the zero vector to every equivalence class $\alpha\mathbb{F}_{q^t}^*$. With this notation the orbit-stabilizer theorem can be phrased as follows.

Remark 3. Let $U \in \mathcal{G}_q(k,n)$ and $\mathrm{Stab}(U) = \mathbb{F}_{q^t}^*$. Then the map

$$\mathbb{P}_t(\mathbb{F}_{q^n}) \longrightarrow \mathrm{Orb}(U),\ \overline{\alpha}^{(t)} \longmapsto \alpha U$$

is a well-defined bijection.

The most interesting possibilities for the stabilizer are when $\mathrm{Stab}(U) = \mathbb{F}_{q^k}^*$ and when $\mathrm{Stab}(U) = \mathbb{F}_q^*$ - i.e. when the stabilizer is as large or as small as possible. The former possibility leads to a *spread code*. In this case, $\mathrm{Orb}(U)$ has the best possibile minimum distance of $2k$ - every pair of subspaces in the orbit intersect trivially. However, the orbit length is only $(q^n-1)/(q^k-1)$.

The latter possibility gives the best possible orbit length, $(q^n-1)/(q^k-1)$. A simple counting argument shows that for an orbit of this length the minimum distance must be at most $2k-2$ - there has to be at least one pair of subspaces that have a nontrivial intersection. This motivates the following definition.

Definition 4. A full-length orbit code with distance $2k-2$ is called an *optimal full-length orbit*.

The existence of such codes has been studied in detail in [23, 24, 26] and for the case $q=2$ also earlier in [7].

Definition 5 ([26, Def. 1]; see also [7, Def. 2.5])**.** A subspace $U \in \mathcal{G}_q(k,n)$ is called a *Sidon space* if it has the property that whenever $a,b,c,d \in U \setminus 0$ are such that $ab=cd$, then $\{\overline{a},\overline{b}\}=\{\overline{c},\overline{d}\}$.

Theorem 6 ([26, Lemma 34]; see also [7, Rem. 2.6])**.** Let $U \in \mathcal{G}_q(k,n)$. Then $\mathrm{Orb}(U)$ is a full-length orbit with minimum distance $2k-2$ if and only if U is a Sidon space.

In [26, Thm. 12 and Thm. 16] Sidon spaces in $\mathcal{G}_q(k,n)$ are constructed for the case where $k<n/2$ is a divisor of n or $k=n/2$ and $q \geq 3$, and thus the existence of full-length orbits with maximum possible distance is guaranteed for these cases. In [23] the authors extend these constructions to allow constructions of full-length orbits where k is the sum of up to three relatively prime divisors of n. Furthermore, in [7, Prop. 2.13] it has been shown by a counting argument that Sidon spaces in $\mathcal{G}_2(k,n)$ exist whenever $n \geq 4k-6$.

The Weight Distribution

Let us now turn to the minimum distance and the weight distribution of a cyclic orbit code. Fix a subspace $U \in \mathcal{G}_q(k,n)$ and let $\mathrm{Stab}(U)=\mathbb{F}_{q^t}^*$. By the definition of the subspace distance in (1.2.1) we have $\mathrm{d}(\beta U,\alpha U)=\mathrm{d}(U,\alpha\beta^{-1}U)$ for all $\alpha,\beta \in \mathbb{F}_{q^n}^*$. Furthermore, $\mathrm{d}(U,\alpha U)=2k-2\dim(U\cap\alpha U)$ for any $\alpha \in \mathbb{F}_{q^n}^*$. This implies

$$\begin{aligned}\mathrm{d}(\mathrm{Orb}(U)) &= \min\{\mathrm{d}(U,\alpha U) \mid \alpha \in \mathbb{F}_{q^n}^*,\, \alpha U \neq U\} \\ &= 2k-2\max\{\dim(U\cap\alpha U) \mid \alpha \in \mathbb{F}_{q^n}^*,\, \alpha U \neq U\}.\end{aligned}$$

In this dissertation we will primarily study the weight distribution of cyclic orbit codes. Without loss of generality we may restrict ourselves to the case where $2k \leq n$. Indeed, because $\mathrm{d}(V^\perp,W^\perp)=\mathrm{d}(V,W)$, where $V^\perp$ denotes the orthogonal complement of V with respect to the standard dot product, a subspace code and its dual will have the same weight distribution.

Definition 7. Let $k \leq n/2$ and $U \in \mathcal{G}_q(k,n)$. For $i=0,\ldots,2k$ define $\delta_i=|\{\alpha U \in \mathrm{Orb}(U) \mid \alpha \in \mathbb{F}_{q^n}^*, \mathrm{d}(U,\alpha U)=i\}|$. We call $(\delta_0,\ldots,\delta_{2k})$ the *weight distribution* of $\mathrm{Orb}(U)$.

A few comments are in order. Note first that in the weight distribution we only count the distances to the "reference space" U. This may be regarded as the analogue of the weight distribution of a linear block code where only the distances to the zero vector are counted as opposed to all pairwise distances. If $\mathrm{Stab}(U) = \mathbb{F}_{q^t}^*$, the number of all pairs $(\beta U, \alpha U)$ such that $\mathrm{d}(\beta U, \alpha U) = 2i$ is given by $(q^n-1)(q^t-1)^{-1}\delta_{2i}$. Next, since $\mathrm{d}(U, \alpha U) = 2k - 2\dim(U \cap \alpha U)$, we obtain $\delta_j = 0$ for odd j. Moreover, $\delta_0 = 1$ and $\delta_{2i} = 0$ for $i = 1, \ldots, d-1$ if $\mathrm{d}(\mathrm{Orb}(U)) = 2d$. Hence the only nontrivial part of the weight distribution is $(\delta_{2d}, \delta_{2d+2}, \ldots, \delta_{2k})$.

Singer Subgroups and Extension-Field Subgroups

Our final preliminary topic, needed for Chapter 3 is the idea of an extension-field subgroup. Again, we take the field extension $\mathbb{F}_{q^n}$ as our model for the n-dimensional vector space over $\mathbb{F}_q$. We denote by $\mathrm{PG}(n-1, q)$ the *n-dimensional projective geometry over $\mathbb{F}_q$*, that is, the set of all subspaces of $\mathbb{F}_{q^n}$. Accordingly, $\mathrm{GL}_n(q)$ denotes the group of all $\mathbb{F}_q$-automorphisms of $\mathbb{F}_{q^n}$. Specific subgroups will play a crucial role later in Chapter 3.

Definition 8. Let $\mathbb{F}_{q^s}$ be a subfield of $\mathbb{F}_{q^n}$, thus $\mathbb{F}_{q^n}$ is an $\mathbb{F}_{q^s}$-vector space of dimension n/s. The *extension-field subgroup of degree s* is defined as

$$\mathrm{GL}_{n/s}(q^s) = \{\phi \in \mathrm{GL}_n(q) \mid \phi \text{ is } \mathbb{F}_{q^s}\text{-linear}\}.$$

The subgroup $\mathrm{GL}_1(q^n)$ will be identified with the multiplicative group $\mathbb{F}_{q^n}^*$ via the map $a \mapsto m_a$, where m_a is the multiplication by a, that is,

$$m_a : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n},\ x \longmapsto ax. \tag{1.2.3}$$

Clearly, $\mathrm{GL}_1(q^n)$ is a cyclic subgroup of order $q^n - 1$. Subgroups of $\mathrm{GL}_n(q)$ of this form are well known.

Definition 9. A cyclic subgroup of $\mathrm{GL}_n(q)$ of order $q^n - 1$ is called a *Singer subgroup*.

Lemma 10 ([9, Lem. 3])**.** Every Singer subgroup of $\mathrm{GL}_n(q)$ is conjugate to $\mathbb{F}_{q^n}^*$.

This shows us that the cyclic orbit codes we introduced previously are the orbits of Singer subgroups. Let us briefly comment on this result. Consider the extension-field subgroups $\mathrm{GL}_{n/s}(q^s)$ from Definition 8, and let $\rho \in \mathrm{GL}_n(q)$. Then the $\mathbb{F}_q$-linear isomorphism ρ leads to new field structures $\rho(\mathbb{F}_{q^n})$ and $\rho(\mathbb{F}_q)$ with identity $\rho(1)$ (they turn ρ into a ring homomorphism). The conjugate group $\rho\mathrm{GL}_{n/s}(q^s)\rho^{-1}$ is now the group of all $\rho(\mathbb{F}_{q^s})$-linear automorphisms of the field $\rho(\mathbb{F}_{q^n})$, and in particular the conjugate Singer subgroup $\rho\mathbb{F}_{q^n}^*\rho^{-1}$ is the group of all $\rho(\mathbb{F}_{q^n})$-linear automorphisms of the field $\rho(\mathbb{F}_{q^n})$. Thus, conjugation of any of these subgroups corresponds to an isomorphic field structure. For this reason we may and will restrict ourselves to the Singer subgroup $\mathbb{F}_{q^n}^*$.

The following results will be needed later on and are well known. The normalizer of a subgroup H in a group G is denoted by $N_G(H)$.

Theorem 11. Let $S = \langle \tau \rangle \leq \mathrm{GL}_n(q)$ be a Singer subgroup.

(a) The normalizer of S is $N_{\mathrm{GL}_n(q)}(S) = \langle \tau, \sigma \rangle \cong \mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q) \rtimes S$, where $\sigma \in \mathrm{GL}_n(q)$ is the Frobenius homomorphism of order n. Moreover, $N_{\mathrm{GL}_n(q)}(S)$ is self-normalizing in $\mathrm{GL}_n(q)$.

(b) The only Singer subgroup contained in $N_{\mathrm{GL}_n(q)}(S)$ is S.

(c) Let $H \leq \mathrm{GL}_n(q)$ such that $S \leq H$. Then there is a divisor s of n such that $\mathrm{GL}_{n/s}(q^s) \trianglelefteq H$.

(d) $N_{\mathrm{GL}_n(q)}(\mathrm{GL}_{n/s}(q^s)) \cong \mathrm{Gal}(\mathbb{F}_{q^s} \,|\, \mathbb{F}_q) \rtimes \mathrm{GL}_{n/s}(q^s)$.

Proof. (a) is in [20, Ch. II, Satz 7.3(a) and its proof], (b) in [5, Prop. 2.5], (c) is in [21, p. 232] and [9, Thm. 7], and (d) is in [9, Sec. 2]. □

The following is immediate.

Corollary 12. Let $S \leq \mathrm{GL}_n(q)$ be a Singer subgroup. If n is an odd prime or $n = 2$ and $q \geq 3$, then $N_{\mathrm{GL}_n(q)}(S)$ is a maximal subgroup of $\mathrm{GL}_n(q)$.

All of the above can, of course, be translated into matrix groups. In order to do so, we consider the following isomorphism. Fix a primitive element ω of $\mathbb{F}_{q^n}$, and let $f = x^n - \sum_{i=0}^{n-1} f_i x^i \in \mathbb{F}_q[x]$ be its minimal polynomial over $\mathbb{F}_q$. Let

$$M_f = \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ f_0 & f_1 & \cdots & f_{n-1} \end{pmatrix} \in \mathbb{F}_q^{n \times n} \tag{1.2.4}$$

be the companion matrix of f. Then $1, \omega, \ldots, \omega^{n-1}$ form a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and we have the isomorphism

$$\Phi : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_q^n, \quad \sum_{i=0}^{n-1} a_i \omega^i \longmapsto (a_0, \ldots, a_{n-1}). \tag{1.2.5}$$

It satisfies

$$\Phi(c\,\omega^i) = \Phi(c) M_f^i \ \text{ for all } c \in \mathbb{F}_{q^n} \text{ and all } i \in \mathbb{N}_0. \tag{1.2.6}$$

In other words, M_f^i is the matrix representation of the linear map m_{ω^i} with respect to the basis $1, \omega, \ldots, \omega^{n-1}$.

Remark 13. Denote by $\mathrm{GL}_n(\mathbb{F}_q)$ the general linear group of invertible $n \times n$-matrices over $\mathbb{F}_q$ and identify a matrix $A \in \mathrm{GL}_n(\mathbb{F}_q)$ in the usual way with the isomorphism $\mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n,\ v \longmapsto vA$. Then we have the group isomorphism

$$\mathrm{GL}_n(\mathbb{F}_q) \longrightarrow \mathrm{GL}_n(q),\ A \longmapsto \phi_A = \Phi^{-1} \circ A \circ \Phi,$$

which satisfies

$$\phi_A(a) = \Phi^{-1}\big(\Phi(a)A\big) \text{ for all } a \in \mathbb{F}_{q^n}. \tag{1.2.7}$$

Let now s be a divisor of n and set $N = (q^n - 1)/(q^s - 1)$. Thus ω^N is a primitive element of $\mathbb{F}_{q^s}$. Then for any $A \in \mathrm{GL}_n(\mathbb{F}_q)$

$$\phi_A \text{ is } \mathbb{F}_{q^s}\text{-linear} \iff AM_f^N = M_f^N A.$$

As a consequence, the subgroup $\{A \in \mathrm{GL}_n(\mathbb{F}_q) \mid AM_f^N = M_f^N A\}$ may be identified with the extension-field subgroup $\mathrm{GL}_{n/s}(q^s)$. Consider the special case $s = 1$. From [18, Thm. 2.9] it is known that $\langle M_f \rangle$ is self-centralizing, i.e., $\{A \in \mathrm{GL}_n(\mathbb{F}_q) \mid AM_f = M_f A\} = \langle M_f \rangle$ (see also [14, Cor. 2 and Cor. 3]). Since $\mathrm{GL}_1(q^n) \cong \mathbb{F}_{q^n}^*$, this simply reflects the well-known isomorphism $\mathbb{F}_{q^n}^* \cong \langle M_f \rangle$ (and $\mathbb{F}_{q^n} \cong \mathbb{F}_q[M_f]$).

Chapter 2 Weight Distributions of Cyclic Orbit Codes

The material of this chapter can be found also in [11]. In that paper, we refer to the weight distribution as the distance distribution.

2.1 The Intersection Distribution

Our goal is to determine the possible weight distributions of cyclic orbit codes. It is clear that the weight distribution is fully determined by counting the subspaces αU that intersect with U in a given dimension. For later convenience we introduce this intersection distribution in the following projectified form.

Definition 14. Let $k \leq n/2$ and $U \in \mathcal{G}_q(k,n)$. Suppose $\mathrm{d}(\mathrm{Orb}(U)) = 2(k-\ell)$. Then $\ell = \max\{\dim(U \cap \alpha U) \mid a \in \mathbb{F}_{q^n}^*, U \neq \alpha U\}$. We call ℓ the *maximum intersection dimension of* $\mathrm{Orb}(U)$. For $i = 0, \ldots, \ell$ we define $\lambda_i = |\mathcal{L}_i|$, where

$$\mathcal{L}_i = \mathcal{L}_i(U) = \{\overline{\alpha} \in \mathbb{P}(\mathbb{F}_{q^n}) \mid \dim(U \cap \alpha U) = i\},$$

and call $(\lambda_0, \ldots, \lambda_\ell)$ the *intersection distribution* of $\mathrm{Orb}(U)$.

We briefly describe the relation between the intersection and weight distributions.

Remark 15. Let U be as Definition 14. Set $d = k - \ell$, hence $\mathrm{d}(\mathrm{Orb}(U)) = 2d$. Suppose $\mathrm{Stab}(U) = \mathbb{F}_{q^t}^*$ and set $s = (q^t - 1)/(q - 1)$. Since for the intersection distribution we count each single subspace αU with a multiplicity $s = |\mathbb{P}(\mathbb{F}_{q^t})|$, we have

$$(\lambda_0, \lambda_1, \ldots, \lambda_\ell) = s(\delta_{2k}, \delta_{2k-2}, \ldots, \delta_{2d}).$$

As a consequence, $\sum_{i=0}^{\ell} s^{-1}\lambda_i = \sum_{i=d}^{k} \delta_{2i} = |\mathrm{Orb}(U) \setminus \{U\}| = (q^n - 1)/(q^t - 1) - 1$.

From now on we will study the intersection distribution. Accordingly, instead of the subspace distance $\mathrm{d}(\mathrm{Orb}(U)) = 2d$ we will specify the maximum intersection dimension ℓ.

We collect a few well-known properties and special cases in the following remark.

Remark 16. Consider the situation of Definition 14 where $\mathrm{Stab}(U) = \mathbb{F}_{q^t}^*$. Then U and all its cyclic shifts are vector spaces over $\mathbb{F}_{q^t}$, and hence $t \mid k$. As a consequence, $\mathrm{d}(U, \alpha U) = 2k - 2\dim(U \cap \alpha U)$ is a multiple of t for all $\alpha \in \mathbb{F}_{q^n}$ and $\delta_j = 0$ if $j \notin r\mathbb{Z}$, where $r = \mathrm{lcm}(2, t)$. For the same reason $\mathcal{L}_i = \emptyset$ if $t \nmid i$. This also implies that $t \mid \ell$, thus either $\ell \geq t$ or $\ell = 0$. If $\ell = 0$, then all subspaces of the orbit code intersect trivially, and thus their union consists of $(q^n - 1)(q^t - 1)^{-1}(q^k - 1) + 1$ elements. Since this number can be at most q^n, we conclude that $t = k$. Thus we have the following scenarios:

(a) If $\mathrm{d}(\mathrm{Orb}(U)) = 2k$, then $\mathrm{Stab}(U) = \mathbb{F}_{q^k}^*$ and thus $U = a\mathbb{F}_{q^k}$ for some $a \in \mathbb{F}_{q^n}$. This is the best distance a cyclic orbit code can have, but comes at the cost of the length, which is just $(q^n-1)/(q^k-1)$, the shortest possible among all cyclic orbit codes of dimension k. The code is a spread code, i.e., all subspaces intersect pairwise trivially and their union is the entire space. The intersection distribution is simply given by $\lambda_0 = (q^n - q^k)/(q-1)$.

(b) If $\mathrm{d}(\mathrm{Orb}(U)) < 2k$, then we even have the upper bound $\mathrm{d}(\mathrm{Orb}(U)) \leq 2(k-t)$. In particular, if $t = 1$, the code is a full-length orbit, i.e., has maximal possible length $(q^n-1)/(q-1)$, and its distance is at most $2k-2$. Later in Theorem 21 we will see that all full-length orbits with distance $2k-2$ have the same intersection distribution (λ_0, λ_1).

Part (a) tells us in particular that the intersection distribution of $\mathrm{Orb}(U)$ is fully determined for any 1-dimensional subspace U. Therefore, we may restrict ourselves to $k \geq 2$. The intersection distribution of optimal cyclic orbit codes will be presented in the next section.

2.2 Fundamental Properties of the Intersection Distribution

We fix $k, n \in \mathbb{N}$ such that $2 \leq k \leq n/2$ and introduce some crucial parameters associated with a given subspace. They will be needed later to study the intersection distribution of cyclic orbit codes. For $q = 2$ the non-projective version of the set $\mathcal{F}$ below appears already in the (unpublished) preprint [7, Def. 2.5].

Definition 17. Let $U \in \mathcal{G}_q(k,n)$ and $\mathrm{d}(\mathrm{Orb}(U)) = 2k - 2\ell$, thus ℓ is the maximum intersection dimension of $\mathrm{Orb}(U)$. We define
(1) $\mathcal{L} = \mathcal{L}(U) = \bigcup_{i=1}^{\ell} \mathcal{L}_i$, where $\mathcal{L}_i$ is as in Definition 14.
(2) $\mathcal{S} = \mathcal{S}(U) = \{\overline{\alpha} \in \mathbb{P}(\mathbb{F}_{q^n}) \mid \alpha \in \mathrm{Stab}(U)\}$.
(3) $\mathcal{M} = \mathcal{M}(U) = \{(\overline{u}, \overline{v}) \mid u, v \in U \setminus 0,\ \overline{u} \neq \overline{v}\}$.
(4) $\mathcal{F} = \mathcal{F}(U) = \{\overline{uv^{-1}} \mid u, v \in U \setminus 0\}$ and $f := |\mathcal{F}|$. We call $\mathcal{F}$ the *set of fractions* of U.
If $\mathrm{Stab}(U) = \mathbb{F}_{q^t}^*$, we have $s := |\mathcal{S}| = (q^t-1)/(q-1)$.

Note that $\mathcal{L} = \{\overline{\alpha} \mid 0 \neq U \cap \alpha U \neq U\}$. In particular $\mathcal{L} \cap \mathcal{S} = \emptyset$. Recall the intersection distribution $(\lambda_0, \ldots, \lambda_\ell)$, where $\lambda_i = |\mathcal{L}_i|$. Since λ_0 is fully determined by $(\lambda_1, \ldots, \lambda_\ell)$, it suffices to study the sets $\mathcal{L}_1, \ldots, \mathcal{L}_\ell$. Hence we omit $\mathcal{L}_0$ in the union $\mathcal{L}$. As for part (3) above, note that for nonzero vectors $u, v \in U$ the property $\overline{u} \neq \overline{v}$ is equivalent to the linear independence of u, v in the $\mathbb{F}_q$-vector space U. Therefore,

$$Q := |\mathcal{M}| = \frac{q^k - 1}{q-1} \frac{q^k - q}{q-1}. \tag{2.2.1}$$

Finally, the set $\mathcal{F}$ consists of all equivalence classes of fractions (within the field $\mathbb{F}_{q^n}$) of nonzero elements in U. Its size f will play a crucial role later on in the study of the intersection distribution of $\mathrm{Orb}(U)$. The next result shows the relation of $\mathcal{F}$ to $\mathrm{Orb}(U)$: the elements in the equivalence classes of $\mathcal{F}$ correspond to the shifts αU

such that $\alpha U \cap U \neq 0$. In particular, for determining the intersection distribution we only need to consider shifts αU where $\overline{\alpha} \in \mathcal{F}$, which reduces considerably the computational effort.

Proposition 18. Let $U \in \mathcal{G}_q(k,n)$ such that $\mathrm{Stab}(U) = \mathbb{F}_{q^t}^*$. Let $\mathrm{d}(\mathrm{Orb}(U)) = 2k - 2\ell$. Then the map $\psi : \mathcal{M} \longrightarrow \mathcal{F}, \quad (\overline{u}, \overline{v}) \longmapsto \overline{uv^{-1}}$ is well-defined and satisfies $\mathcal{F} = \psi(\mathcal{M}) \cup \{\overline{1}\} = \mathcal{L} \cup \mathcal{S}$. Furthermore, for any $\overline{\alpha} \in \mathcal{F}$ we have
(a) $\overline{\alpha} \in \mathcal{S} \iff |\psi^{-1}(\overline{\alpha})| = (q^k - 1)/(q-1)$,
(b) $\overline{\alpha} \in \mathcal{L}_i \iff |\psi^{-1}(\overline{\alpha})| = (q^i - 1)/(q-1)$.
Since $\mathcal{L}_i = \emptyset$ if $t \nmid i$, this implies that the pre-images never have size $(q^i - 1)/(q-1)$, where $t \nmid i$.

Proof. The well-definedness of ψ is clear and so is $\psi(\mathcal{M}) \cup \{\overline{1}\} = \mathcal{F}$. To show that $\psi(\mathcal{M}) \cup \{\overline{1}\} = \mathcal{L} \cup \mathcal{S}$, let $\overline{\alpha} = \overline{uv^{-1}} \in \psi(\mathcal{M})$ for some $u, v \in U \setminus 0$. Then there exists $\lambda \in \mathbb{F}_q^*$ such that $u = \lambda \alpha v$. Since $\lambda U = U$ this implies $U \cap \alpha U \neq 0$. Hence either $U = \alpha U$ or $\dim(U \cap \alpha U) \in \{1, \ldots, \ell\}$. In the first case $\alpha \in \mathbb{F}_{q^t}$, thus $\overline{\alpha} \in \mathcal{S}$ and in the second case $\overline{\alpha} \in \mathcal{L}$. Since obviously $\overline{1} \in \mathcal{S}$, this shows $\psi(\mathcal{M}) \cup \{\overline{1}\} \subseteq \mathcal{L} \cup \mathcal{S}$. The proof of the reverse inclusion proceeds similarly. If $\overline{\alpha} \in \mathcal{L} \cup \mathcal{S}$, then $1 \leq \dim(U \cap \alpha U) \leq k$. Hence there exist $u, v \in U$ with $u = \alpha v$. So $\overline{\alpha} = \overline{uv^{-1}}$ is either $\overline{1}$ or in $\psi(\mathcal{M})$.

It remains to show (a) and (b). Note first that for $(\overline{v}, \overline{w}) \in \psi^{-1}(\overline{\alpha})$, the second component $\overline{w}$ is uniquely determined by the first one. Thus it suffices to count the number of possible first components.

Let $\overline{\alpha} \in \mathcal{S}$. Then $U = \alpha U$. As a consequence, for every $v \in U$ there exists a unique $w \in U$ such that $v = \alpha w$. Hence $\overline{\alpha} = \overline{vw^{-1}} = \psi(\overline{v}, \overline{w})$. Because there exist $(q^k - 1)/(q-1)$ elements $\overline{v}$ such that $v \in U$, the result follows.

Let $\overline{\alpha} \in \mathcal{L}_i$. Hence $\dim(U \cap \alpha U) = i$. Then for every $v \in U \cap \alpha U$ there exists $w \in U$ such that $v = \alpha w$. Using that there exist $(q^i - 1)/(q-1)$ elements $\overline{v}$ such that $v \in U \cap \alpha U$, we may argue as above to conclude that $|\psi^{-1}(\overline{\alpha})| \geq (q^i - 1)/(q-1)$. Conversely, suppose that $(\overline{x}, \overline{y}) \in \psi^{-1}(\overline{\alpha})$. Then $\overline{x} = \overline{\alpha y}$ and $x = \lambda \alpha y$ for some $\lambda \in \mathbb{F}_q$. Thus $x \in U \cap \alpha U$. This leaves $(q^i - 1)/(q-1)$ choices for $\overline{x}$, and thus $|\psi^{-1}(\overline{\alpha})| \leq (q^i - 1)/(q-1)$. Hence $|\psi^{-1}(\overline{\alpha})| = (q^i - 1)/(q-1)$. □

Now we can formulate the following linear relations for the intersection distribution.

Corollary 19. Let $U \in \mathcal{G}_q(k,n)$ such that $\mathrm{Stab}(U) = \mathbb{F}_{q^t}^*$. Let $\mathrm{d}(\mathrm{Orb}(U)) = 2k - 2\ell$. Recall the cardinalities $f = |\mathcal{F}|$, $s = |\mathcal{S}|$, $Q = |\mathcal{M}|$, and $\lambda_i = |\mathcal{L}_i|$ for $i = 1, \ldots, \ell$. Then

$$f = s + \sum_{i=1}^{\ell} \lambda_i. \tag{2.2.2}$$

and

$$Q = \sum_{i=1}^{\ell} \frac{q^i - 1}{q-1} \lambda_i + \frac{q^k - 1}{q-1}(s-1). \tag{2.2.3}$$

In the special case where $t = 1$, i.e. $\mathrm{Orb}(U)$ is a full-length orbit, we have $s = 1$, and thus

$$f = 1 + \sum_{i=1}^{\ell} \lambda_i \quad \text{and} \quad Q = \sum_{i=1}^{\ell} \frac{q^i - 1}{q - 1} \lambda_i. \tag{2.2.4}$$

Proof. The identity in (2.2.2) is a consequence of $\mathcal{L} \cup \mathcal{S} = \mathcal{F}$ from Proposition 18 along with $\mathcal{L} \cap \mathcal{S} = \emptyset$. From the same proposition we have $\psi(\mathcal{M}) = \mathcal{L} \cup \mathcal{S} \setminus \{\overline{1}\}$, thus $\mathcal{M} = \bigcup_{i=1}^{\ell} \psi^{-1}(\mathcal{L}_i) \cup \psi^{-1}(\mathcal{S} \setminus \{\overline{1}\})$. Now (2.2.3) follows from Proposition 18(a) and (b) and the cardinality of $\mathcal{M}$ in (2.2.1). The rest follows from $s = (q^t - 1)/(q - 1)$. □

Recalling Q from (2.2.1), the above identities (2.2.2) and (2.2.3) allow us to give a lower and upper bound on the number of fractions of U in terms of q and k.

Proposition 20. With the data as in Corollary 19 we have

$$\frac{q^k - 1}{q - 1} \leq f \leq Q + 1.$$

Furthermore,

(a) $f = (q^k - 1)/(q - 1) \iff \ell = 0 \iff t = k$. This is the spread-code case, thus $U = a\mathbb{F}_{q^k}$ for some $a \in \mathbb{F}_{q^n}$.

(b) $f = Q + 1 \iff \ell = 1 \iff \mathrm{d}(\mathrm{Orb}(U)) = 2k - 2$. This is the case of optimal full-length orbits (see Definition 4).

Proof. The lower bound for f is obvious from $\dim(U) = k$. As for the upper bound, note that $\frac{q^i - 1}{q - 1} \geq 1$ for $i = 1, \ldots, \ell$ and $i = k$. So by (2.2.2) and (2.2.3)

$$f - 1 = \sum_{i=1}^{\ell} \lambda_i + (s - 1) \leq \sum_{i=1}^{\ell} \left(\frac{q^i - 1}{q - 1} \right) \lambda_i + \frac{q^k - 1}{q - 1}(s - 1) = Q. \tag{2.2.5}$$

It remains to prove (a) and (b). (a) If $\ell = 0$, then $t = k$ by Remark 16 and $f = s = (q^k - 1)/(q - 1)$ thanks to (2.2.2) and Definition 17. Conversely, let $f = (q^k - 1)/(q - 1)$. Then $f = |\{\overline{u} \mid u \in U \setminus 0\}|$. Replacing U by a suitable shift we may assume without loss of generality that $1 \in U$. Then the above along with the definition $f = |\mathcal{F}| = |\{\overline{uv^{-1}} \mid u, v \in U \setminus 0\}|$ tells us that for every $u, v \in U \setminus 0$ there exists $w \in U$ and $\lambda \in \mathbb{F}_q$ such that $uv^{-1} = \lambda w$. Hence U is closed under division and inverses and is therefore the subfield $\mathbb{F}_{q^k}$. The rest follows again from Remark 16.

(b) Suppose $\ell = 1$, i.e., $\mathrm{d}(\mathrm{Orb}(U)) = 2k - 2$. Then Remark 16(b) implies $t = 1$. Thus $s = 1$ and subsequently $f = Q + 1$ by (2.2.4). On the other hand, if $f = Q + 1$ then we have equality in (2.2.5), which in turn implies $\ell = s = 1$ since $\frac{q^i - 1}{q - 1} > 1$ for $i > 1$. □

We now turn to optimal full-length orbits; recall that these are cyclic orbit codes of length $(q^n - 1)/(q - 1)$ and distance $2k - 2$ and equivalently are generated by a Sidon space. It follows easily from the above results that all optimal full-length orbits have the same intersection distribution.

Theorem 21. Let $U \in \mathcal{G}_q(k,n)$ be a Sidon space. Then the optimal full-length orbit $\mathrm{Orb}(U)$ has intersection distribution (λ_0, λ_1), where

$$\lambda_1 = Q = \frac{q^k-1}{q-1}\frac{q^k-q}{q-1} = f-1, \quad \lambda_0 = \frac{q^n-1}{q-1} - \lambda_1 - 1.$$

In particular, the intersection distribution of an optimal full-length orbit depends only on the parameters q, n, and k. Furthermore, all k-dimensional Sidon spaces in $\mathbb{F}_{q^n}$ have the same number of fractions.

Proof. Under the given assumptions we have $t = 1$, and thus $s = 1$, as well as $\ell = 1$. Now the result for λ_1 follows from (2.2.4), while λ_0 can be computed using Remark 15. □

Since for $k = 2$ every $U \in \mathcal{G}_q(k,n)$ leads to an orbit code with distance $\mathrm{d} = 2k$ or $\mathrm{d} = 2(k-1)$, we have fully described the intersection distribution of all such orbit codes. Hence from now on we may assume $k \geq 3$.

Examples show that for full-length orbit codes with minimum distance at most $2(k-2)$ the intersection distribution does not only depend on q, n, k and the minimum distance. We will study that case in further detail in the next section.

We close this section with a generalization of the previous results by taking the stabilizer into account. This improves on the upper bound for f given in Proposition 20.

Proposition 22. Let $U \in \mathcal{G}_q(k,n)$ and $\mathrm{Stab}(U) = \mathbb{F}_{q^t}^*$. Then

$$\frac{q^k-1}{q-1} \leq f \leq \frac{q^k-1}{q^t-1}\frac{q^k-q^t}{q-1} + \frac{q^t-1}{q-1}.$$

(a) $f = \frac{q^k-1}{q^t-1}\frac{q^k-q^t}{q-1} + \frac{q^t-1}{q-1} \iff \mathrm{d}(\mathrm{Orb}(U)) = 2(k-t)$ (which is the maximum possible distance for a cyclic orbit code with stabilizer $\mathbb{F}_{q^t}^*$). This is the case if and only if U is a Sidon space over $\mathbb{F}_{q^t}$, i.e., if $a, b, c, d \in U \setminus 0$ and $ab = cd$, then $\{\overline{a}^{(t)}, \overline{b}^{(t)}\} = \{\overline{c}^{(t)}, \overline{d}^{(t)}\}$.

(b) If $\mathrm{d}(\mathrm{Orb}(U)) = 2(k-t)$, then the intersection distribution is given by (λ_0, λ_t), where

$$\lambda_t = \frac{q^k-1}{q^t-1}\frac{q^k-q^t}{q-1} = f - \frac{q^t-1}{q-1}, \quad \lambda_0 = \frac{q^n-q^t}{q-1} - \lambda_t.$$

In particular, if $\mathrm{Stab}(U) = \mathbb{F}_{q^{k/2}}^*$ then $f = (q^{3k/2}-1)/(q-1)$.

Proof. By assumption $t \mid \gcd(n,k)$. Set $\hat{q} = q^t$, $\hat{k} = k/t$, and $\hat{n} = n/t$. Then $|\mathrm{Orb}(U)| = (\hat{q}^{\hat{n}}-1)/(\hat{q}-1)$, and thus it is a full-length orbit if considered as a collection of $\mathbb{F}_{\hat{q}}$-subspaces in the ambient space $\mathbb{F}_{\hat{q}^{\hat{n}}}$. Hence we may apply (2.2.4) if we replace $\mathbb{F}_q$ by $\mathbb{F}_{\hat{q}}$. In order to do so, we need to generalize Definition 17 and the sets $\mathcal{L}_i$ by projectifying with respect to the scalar field $\mathbb{F}_{\hat{q}}$. We denote the resulting

sets and cardinalities with a superscript (t), thus $\mathcal{L}_i^{(t)} = \{\overline{\alpha}^{(t)} \mid \dim_{\mathbb{F}_{\hat{q}}}(U \cap \alpha U) = i\}$ etc. Then $\mathcal{S}^{(t)} = \{\overline{1}^{(t)}\}$ and

$$\lambda_{it} = \frac{q^t-1}{q-1}\lambda_i^{(t)}, \quad f = \frac{q^t-1}{q-1}f^{(t)}, \quad s = \frac{q^t-1}{q-1}s^{(t)}, \quad Q^{(t)} = |\mathcal{M}^{(t)}| = \frac{\hat{q}^{\hat{k}}-1}{\hat{q}-1}\,\frac{\hat{q}^{\hat{k}}-\hat{q}}{\hat{q}-1}. \tag{2.2.6}$$

Now we can prove the above statement. From Proposition 20 we have $(\hat{q}^{\hat{k}}-1)/(\hat{q}-1) \le f^{(t)} \le Q^{(t)}+1$, and (2.2.6) leads to the stated inequalities.
(a) Proposition 20(b) tells us that $f^{(t)} = Q^{(t)}+1$ iff the subspace distance is $2(\hat{k}-1)$, and where the distance is computed via dimensions over $\mathbb{F}_{q^t}$. Hence the latter becomes $\mathrm{d}(\mathrm{Orb}(U)) = 2t(\hat{k}-1) = 2(k-t)$ as dimensions over $\mathbb{F}_q$.
(b) From Theorem 21 we have $\lambda_1^{(t)} = Q^{(t)} = f^{(t)}-1$ and $\lambda_0^{(t)} = (\hat{q}^{\hat{n}}-1)/(\hat{q}-1)-\lambda_1^{(t)}-1$. Using (2.2.6), we obtain the stated expression for λ_t and λ_0.

Finally, if $t = k/2$, then U is not a cyclic shift of a field and thus must be Sidon over $\mathbb{F}_{q^t}$. Hence we may apply (a) and simplify. □

2.3 Intersection Distributions of General Full-Length Orbit Codes

In this section we will generalize some of the results of the previous section to the intersection distribution of a cyclic orbit code with smaller minimum distance. After the spread codes and optimal full-length orbits, the cyclic orbit codes with the best combination of orbit size and minimum distance are full-length orbit codes with minimum distance $2k-4$. Our goal in this section is to describe the intersection distribution of such codes in terms of the parameters q, n, k and a new parameter r. This new parameter counts the number of cyclic orbits generated by the 2-dimensional intersections $U \cap \alpha U$. These parameters together with (2.2.3) are enough to completely determine the intersection distribution, which we give in the following theorem. In this section we may and will assume $3 \le k \le n/2$. Recall $Q = |\mathcal{M}|$ from (2.2.1).

Theorem 23. Let $U \in \mathcal{G}_q(k,n)$ generate a full-length orbit with $\mathrm{d}(\mathrm{Orb}(U)) = 2k-4$. Then one of the following cases occurs.
(a) U contains a cyclic shift of $\mathbb{F}_{q^2}$ (hence n is even). In this case $\mathrm{Orb}(U)$ has intersection distribution $(\lambda_0, \lambda_1, \lambda_2)$, where

$$\begin{aligned}
\lambda_2 &= q + rq(q+1),\\
\lambda_1 &= Q - (q+1)\lambda_2 = \frac{q^k-1}{q-1}\frac{q^k-q}{q-1} - (q+1)(q+rq(q+1)),\\
\lambda_0 &= |\mathbb{P}(\mathbb{F}_{q^n})| - \lambda_1 - \lambda_2 - 1 = \frac{q^n-1}{q-1} + q^2(1+r(q+1)) - Q - 1
\end{aligned}$$

for some $r \ge 0$.

(b) U does not contain a cyclic shift of $\mathbb{F}_{q^2}$. In this case, $\mathrm{Orb}(U)$ has intersection distribution $(\lambda_0, \lambda_1, \lambda_2)$, where

$$\begin{aligned}
\lambda_2 &= rq(q+1), \\
\lambda_1 &= Q - (q+1)\lambda_2 = \frac{q^k-1}{q-1}\frac{q^k-q}{q-1} - rq(q+1)^2, \\
\lambda_0 &= |\mathbb{P}(\mathbb{F}_{q^n})| - \lambda_1 - \lambda_2 - 1 = \frac{q^n-1}{q-1} + rq^2(q+1) - Q - 1
\end{aligned}$$

for some $r \geq 1$.

The proof is deferred to the end of this section. Before setting up the necessary preparation, we draw some further conclusions about the possible values of λ_1 and λ_2.

Corollary 24. Let $U \in \mathcal{G}_q(k,n)$ generate a full-length orbit with $\mathrm{d}(\mathrm{Orb}(U)) = 2k-4$. Then the intersection distribution $(\lambda_0, \lambda_1, \lambda_2)$ of $\mathrm{Orb}(U)$ depends only on q, n, k, and f. Further, the following inequalities hold.

$$q \leq \lambda_2 \leq \frac{Q}{q+1}, \qquad 0 \leq \lambda_1 \leq Q - q(q+1), \qquad \frac{Q}{q+1} \leq f - 1 \leq Q - q^2. \quad (2.3.1)$$

Proof. By assumption $\mathrm{Stab}(U) = \mathbb{F}_q^*$, and thus $t = s = 1$ in Corollary 19. Hence Eq. (2.2.4) reduces to

$$f - 1 = \lambda_1 + \lambda_2 \qquad Q = \lambda_1 + (q+1)\lambda_2. \quad (2.3.2)$$

Because either $\frac{q^k-1}{q-1}$ or $\frac{q^{k-1}-1}{q-1}$ is divisible by $q+1$, we have $Q \in q(q+1)\mathbb{Z}$; see (2.2.1). Since Theorem 23 says that $\lambda_2 \in q\mathbb{Z}$, we also have $\lambda_1 \in q(q+1)\mathbb{Z}$ and $(f-1) \in q\mathbb{Z}$. In fact Theorem 23 implies the stronger statement that $f - 1 \in q(q+1)\mathbb{Z}$ if and only if U does not contain any cyclic shift of $\mathbb{F}_{q^2}$. Now we can solve this system of equations for λ_1 and λ_2 in terms of q, Q, and f to get

$$\lambda_1 = \frac{1}{q}((q+1)(f-1) - Q) \qquad \lambda_2 = \frac{1}{q}(Q - (f-1)). \quad (2.3.3)$$

Both of these values are guaranteed to be in $\mathbb{Z}$ by the above discussion. Therefore the intersection distribution of $\mathrm{Orb}(U)$ is completely determined by q, n, k and the value $f = |\mathcal{F}(U)|$. The inequalities of (2.3.1) follow from $\lambda_1 \geq 0$ and $\lambda_2 \geq q$ together with (2.3.2). □

The next example shows that equality can be achieved on both sides of (2.3.1), with the maximum of λ_2 corresponding to the minimum of λ_1 and vice versa. In other words, there exist subspaces U where $\ell = 2$, $t = 1$, and $\dim(U \cap \alpha U) \in \{0, 2, k\}$ for all $\alpha \in \mathbb{F}_{q^n}^*$, and hence $\lambda_1 = 0$. Similarly, there exist subspaces U with $\ell = 2, t = 1$, and $\lambda_2 = q$. However, in general the restriction that $\lambda_2 \pmod{q(q+1)} \in \{0, q\}$ means that the upper bound of $Q/(q+1)$ may not be attainable.

Example 25. Let $q = 3, k = 3, n = 8$ and let γ be primitive in $\mathbb{F}_{3^8}$. Then $\alpha = \gamma^{\frac{3^8-1}{3^2-1}}$ is a primitive element of $\mathbb{F}_9 \subseteq \mathbb{F}_{3^8}$ and $\beta = \gamma^{\frac{3^8-1}{3^4-1}}$ is a primitive element of $\mathbb{F}_{81} \subseteq \mathbb{F}_{3^8}$. Define $U = \langle 1, \alpha, \rho \rangle$ for some $\rho \in \mathbb{F}_{3^8}^* \setminus \langle 1, \alpha \rangle$. Hence $\mathbb{F}_9 \subseteq U$. Since $\gcd(k, n) = 1$, the subspace U generates a full-length orbit for any linearly independent choice of ρ. There are two possibilities:
(a) $\rho \in \mathbb{F}_{81} \setminus \mathbb{F}_9$
(b) $\rho \in \mathbb{F}_{3^8} \setminus \mathbb{F}_{81}$.
In (a), we have $U \subseteq \mathbb{F}_{81}$, and thus $\frac{v}{w} \in \mathbb{F}_{81}$ for any $v, w \in U \setminus 0$. As a consequence, the only nonzero intersections are of the form $U \cap \beta^s U$. Since U and $\beta^s U$ are both 3-dimensional $\mathbb{F}_3$-subspaces of the 4-dimensional $\mathbb{F}_3$-subspace $\mathbb{F}_{81}$, we conclude $\dim(U \cap \beta^s U) \in \{2, 3\}$. This leads to

$$\lambda_1 = 0, \qquad \lambda_2 = \frac{Q}{q+1} = 39$$

for any such choice of ρ. The 39 elements resulting in a 2-dimensional intersection are exactly the elements of $\mathbb{P}(\mathbb{F}_{81}) \setminus \{\overline{1}\}$.
In (b), a computation using SageMath shows that

$$\lambda_1 = Q - q(q+1) = 144, \qquad \lambda_2 = q = 3$$

for any such choice of ρ. Noting that $\alpha^s \mathbb{F}_9 = \mathbb{F}_9$ for any s and $\mathrm{Stab}(U) = \mathbb{F}_3$, we conclude that $\mathbb{F}_9 \subseteq U \cap \alpha^s U \subsetneq U$ for any s such that $\alpha^s \notin \mathbb{F}_3$. It follows that $U \cap \alpha^s U = \mathbb{F}_9$ and therefore the three elements that result in a 2-dimensional intersection are exactly the elements of $\mathbb{P}(\mathbb{F}_9) \setminus \{\overline{1}\}$. We will see later in Proposition 30 that this can be generalized.

The construction in part (a) of this example generalizes to provide examples of full-length orbit codes where the subspace distance is $2k - 2\ell$ for arbitrarily large ℓ and $\lambda_i = 0$ for small i. Since computation with SageMath shows that many, if not most, subspaces have $\lambda_1 > \lambda_i$ for $i > 1$, these are unusual subspaces. The following example generalizes Example 25(a).

Example 26. Let q be a prime power and consider a tower of fields $\mathbb{F}_q \subset \mathbb{F}_{q^s} \subset \mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$. Our goal is to find U so that U has full length orbit but $\lambda_i = 0$ for small values of i, generalizing Example 25 (a). To this end, let U be a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ containing $\mathbb{F}_{q^s}$ and that is not an $\mathbb{F}_{q^s}$-vector space. As in the previous example, all fractions of elements of U are in $\mathbb{F}_{q^m}$, and thus any nontrivial intersection $U \cap \alpha U$ arises from some $\alpha \in \mathbb{F}_{q^m}$. For any such α we have $\dim(U + \alpha U) + \dim(U \cap \alpha U) = \dim U + \dim \alpha U$ and thus $\dim(U \cap \alpha U) = 2k - \dim(U + \alpha U)$. From $k \leq \dim(U + \alpha U) \leq m$ we obtain

$$2k - m \leq \dim_{\mathbb{F}_q}(U \cap \alpha U) \leq k.$$

Since $\mathbb{F}_{q^s} \subset U$ is fixed by any shift by an element of $\mathbb{F}_{q^s}$ we see that there exist intersections with $\dim(U \cap \alpha U) \geq s$. Because U is not an $\mathbb{F}_{q^s}$-vector space it follows

that these intersections are not all of U, hence $\mathrm{d}(\mathrm{Orb}(U)) \leq 2(k-s)$. Choose now k such that $k \geq \frac{s+m}{2}$. Then the above shows that $\lambda_i = 0$ for $i = 1, \ldots, s-1$ as desired. Example 25(a) is an example of such a choice of U with $q = 3, s = 2, m = 4, n = 8$, and $k = 3$.

In order to prove Theorem 23 we need to develop a few tools. The next definitions make sense even when $\mathrm{d}(\mathrm{Orb}(U)) < 2k-4$, so we give the general versions before specializing to the scenario of Theorem 23.

Definition 27. Let $U \in \mathcal{G}_q(k,n)$ such that $\mathrm{d}(\mathrm{Orb}(U)) = 2k - 2\ell$. For any subspace $V \subseteq U$ with $\dim(V) = \ell$, we define $A_V = \{\overline{\alpha} \in \mathbb{P}(\mathbb{F}_{q^n}) \mid V \subseteq U \cap \alpha U\}$.

Note that $A_V = \mathcal{S}(U) \cup \{\overline{\alpha} \in \mathbb{P}(\mathbb{F}_{q^n}) \mid V = U \cap \alpha U\}$, where $\mathcal{S}(U)$ is as in Definition 17. Then

$$\mathcal{S}(U) \subsetneq A_V \iff V = U \cap \alpha U \text{ for some } \alpha \in \mathbb{F}_{q^n}. \tag{2.3.4}$$

We are, of course, interested in the case that V arises as a maximal dimension intersection $U \cap \alpha U$ for some α. To this end, we introduce a group action of $(\mathbb{F}_q, +)$ on $\mathbb{F}_{q^n}$.

Proposition 28. The map

$$\varphi : (\mathbb{F}_{q^n} \setminus \mathbb{F}_q) \times \mathbb{F}_q \longrightarrow (\mathbb{F}_{q^n} \setminus \mathbb{F}_q), \quad (\alpha, \lambda) \longmapsto \frac{\alpha}{1+\lambda\alpha},$$

is well-defined and satisfies the following properties.

(a) The map φ is a group action of $(\mathbb{F}_q, +)$ on $\mathbb{F}_{q^n} \setminus \mathbb{F}_q$.

(b) Let $\mathbb{F}_{q^t}$ be a subfield of $\mathbb{F}_{q^n}$ and $\lambda \in \mathbb{F}_q$. Then $\varphi(\alpha, \lambda) \in \mathbb{F}_{q^t} \setminus \mathbb{F}_q \iff \alpha \in \mathbb{F}_{q^t} \setminus \mathbb{F}_q$.

(c) $|\mathrm{Orb}_\varphi(\alpha)| = q$ for all $\alpha \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$, and thus $\mathbb{F}_{q^t} \setminus \mathbb{F}_q$ is the disjoint union of $q^{t-1} - 1$ orbits for any divisor t of n.

(d) For any $\alpha \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$ the set $\overline{\mathrm{Orb}_\varphi(\alpha)} = \{\overline{\frac{\alpha}{1+\lambda\alpha}} \mid \lambda \in \mathbb{F}_q\}$ has cardinality q.

(e) Let $\alpha \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$ and $\beta = \rho\alpha$ for some $\rho \in \mathbb{F}_q^*$. Then $\varphi(\beta, \lambda) = \rho\varphi(\alpha, \rho\lambda)$. As a consequence, the set $\overline{\mathrm{Orb}_\varphi(\alpha)}$ depends only on the projective equivalence class $\overline{\alpha}$.

(f) $\mathbb{P}(\mathbb{F}_{q^n}) \setminus \{\overline{1}\}$ is the disjoint union of $(q^{n-1}-1)/(q-1)$ sets of the form $\overline{\mathrm{Orb}_\varphi(\alpha)}$.

It should be noted that the map φ is not a well-defined map on equivalence classes in projective space, yet it leads to a disjoint union of projectivized orbits.

Proof. Since $\alpha \notin \mathbb{F}_q$, we have $1 + \lambda\alpha \neq 0$ for any $\lambda \in \mathbb{F}_q$. Further, suppose $\varphi(\alpha, \lambda) \in \mathbb{F}_q$, say $\frac{\alpha}{1+\lambda\alpha} = \mu \in \mathbb{F}_q$. Then $\alpha(1 - \lambda\mu) = \mu$ and either $\alpha = \frac{\mu}{1-\mu\lambda} \in \mathbb{F}_q$ or $1 - \lambda\mu = 0$ and $\mu = 0$. Since both are a contradiction, φ is well-defined. It remains to prove (a)–(f).

(a) One straightforwardly verifies that $\varphi(\varphi(\alpha, \lambda), \mu) = \varphi(\alpha, \lambda + \mu)$.

(b) Suppose $\varphi(\alpha, \lambda) \in \mathbb{F}_{q^t} \setminus \mathbb{F}_q$, say $\frac{\alpha}{1+\lambda\alpha} = \mu \in \mathbb{F}_{q^t} \setminus \mathbb{F}_q$. Then with the same reasoning as above we conclude $\alpha \in \mathbb{F}_{q^t} \setminus \mathbb{F}_q$. The converse is trivial.

(c) $\varphi(\alpha,\lambda)=\varphi(\alpha,\mu)$ implies $\lambda=\mu$ (since $\alpha\neq 0$). Hence $|\operatorname{Orb}_\varphi(\alpha)|=q$, and the rest is clear.
(d) We want to show that the cardinality of an orbit under φ is preserved by passing to projective space. So suppose that $\overline{\varphi(\alpha,\lambda)}=\overline{\varphi(\alpha,\mu)}$. Then we have $1+\lambda\alpha=\rho(1+\mu\alpha)$ for some $\rho\in\mathbb{F}_q^*$. Since $\alpha\notin\mathbb{F}_q$, $\{1,\alpha\}$ is $\mathbb{F}_q$-linearly independent and so we have $\rho=1$ and $\lambda=\mu$.
(e) Suppose $\beta=\rho\alpha$ for some $\rho\in\mathbb{F}_q^*$. Then $\varphi(\beta,\lambda)=\frac{\beta}{1+\rho\lambda\alpha}=\rho\frac{\alpha}{1+\rho\lambda\alpha}=\rho\varphi(\alpha,\rho\lambda)$.
(f) By (d) $\operatorname{Orb}_\varphi(\alpha)\cap\operatorname{Orb}_\varphi(\rho\alpha)=\emptyset$ for all $\rho\in\mathbb{F}_q^*\setminus\{1\}$ and $\alpha\in\mathbb{F}_{q^n}\setminus\mathbb{F}_q$. On the other hand, thanks to (e), $\overline{\operatorname{Orb}_\varphi(\alpha)}=\overline{\operatorname{Orb}_\varphi(\rho\alpha)}$ for all $\rho\in\mathbb{F}_q^*$. Since $|\mathbb{P}(\mathbb{F}_{q^n})\setminus\{\overline{1}\}|=(q^n-q)/(q-1)$, all of this together with (d) shows that the $q^{n-1}-1$ disjoint orbits covering $\mathbb{F}_{q^n}\setminus\mathbb{F}_q$ collapse to $(q^{n-1}-1)/(q-1)$ projectivized orbits covering $\mathbb{P}(\mathbb{F}_{q^n})\setminus\{\overline{1}\}$. □

We next show that the sets A_V decompose into the projectivized versions of the orbits of φ.

Proposition 29. Let $U\in\mathcal{G}_q(k,n)$ such that $\mathrm{d}(\operatorname{Orb}(U))=2k-2\ell$ and let $\operatorname{Stab}(U)=\mathbb{F}_{q^t}^*$. Furthermore, let $V\subseteq U$ with $\dim(V)=\ell$. Then we have the following.
(a) If $\overline{\alpha}\in A_V$, then $\overline{\varphi(\alpha,\lambda)}\in A_V$ for each $\lambda\in\mathbb{F}_q$.
(b) Suppose $V=U\cap\alpha U$ for some $\alpha\in\mathbb{F}_{q^n}$. Write $A_V=\mathcal{S}(U)\cup\mathcal{A}$, where $\mathcal{S}(U)$ is as in Definition 17 and $\mathcal{A}:=\{\overline{\beta}\mid V=U\cap\beta U\}$. Then $\mathcal{A}$ is a disjoint union of projectivized orbits $\overline{\operatorname{Orb}_\varphi(\beta)}$. Thus $|A_V|=aq+\frac{q^t-1}{q-1}$ for some $a\in\mathbb{N}$ and in particular $|A_V|\geq q+1$.
(c) If $\overline{\beta}=\overline{\varphi(\alpha,\lambda)}\in A_V$ for $\lambda\neq 0$, then $\overline{\beta\alpha^{-1}}=\overline{\varphi(\alpha^{-1},\lambda^{-1})}\in A_{\alpha^{-1}V}$.

Proof. (a) Suppose $V\subseteq U\cap\alpha U$ and $\lambda\in\mathbb{F}_q$. We have to show that $V\subseteq U\cap\varphi(\alpha,\lambda)U$. Let $\{v_1,\ldots,v_m\}$ be a basis of V. Since $V\subset U\cap\alpha U$ there exist $\{u_1,\ldots,u_m\}\subset U$ such that $v_i=\alpha u_i$ for $i=1,\ldots,\ell$. Then $u_i+\lambda v_i\in U$ and

$$\varphi(\alpha,\lambda)(u_i+\lambda v_i)=\frac{\alpha u_i(1+\lambda\alpha)}{1+\lambda\alpha}=v_i.$$

Therefore $V\subseteq U\cap\varphi(\alpha,\lambda)U$.
(b) Let $V=U\cap\alpha U$ and $\lambda\in\mathbb{F}_q$. Then (a) implies $V\subseteq U\cap\varphi(\alpha,\lambda)U$. Since $\dim(V)=\ell$ is the maximum possible intersection dimension, we conclude that either $V=U\cap\varphi(\alpha,\lambda)U$ or $U\cap\varphi(\alpha,\lambda)U=U$. In the latter case $\varphi(\alpha,\lambda)\in\operatorname{Stab}(U)=\mathbb{F}_{q^t}^*$, and thus by Proposition 28(b) also $\alpha\in\mathbb{F}_{q^t}^*$, which is a contradiction. Thus $V=U\cap\varphi(\alpha,\lambda)U$. All of this shows that if $\overline{\alpha}\in\mathcal{A}$, then $\overline{\varphi(\alpha,\lambda)}\in\mathcal{A}$. With the aid of Proposition 28(f) we obtain that $\mathcal{A}$ is a disjoint union of projectivized orbits. The rest is clear.
(c) Without loss of generality $\beta=\varphi(\alpha,\lambda)$. By assumption $V\subseteq U\cap\beta U$. Because $\alpha\in\operatorname{Orb}_\varphi(\beta)$, Part (a) shows that $V\subseteq U\cap\alpha U$. Therefore $\alpha^{-1}V\subseteq U\cap\alpha^{-1}U$ and so $\overline{\alpha^{-1}}\in A_{\alpha^{-1}V}$. By (a) again $\overline{\varphi(\alpha^{-1},\lambda^{-1})}\in A_{\alpha^{-1}V}$. Now

$$\beta\alpha^{-1}=\alpha^{-1}\varphi(\alpha,\lambda)=\frac{1}{1+\lambda\alpha}=\lambda^{-1}\frac{\alpha^{-1}}{1+\lambda^{-1}\alpha^{-1}}=\lambda^{-1}\varphi(\alpha^{-1},\lambda^{-1}).$$

Since $\lambda^{-1}\in\mathbb{F}_q$, we conclude $\overline{\beta\alpha^{-1}}=\overline{\varphi(\alpha^{-1},\lambda^{-1})}$ and the claim follows. □

We now focus on subspaces U that generate a full-length orbit code (i.e., $\mathrm{Stab}(U) = \mathbb{F}_q^*$) and satisfy $\mathrm{d}(\mathrm{Orb}(U)) = 2k-4$. We will show next that in this case $|A_V| = q+1$ for any 2-dimensional intersection $V = U \cap \alpha U$; that is, A_V is the union of $\{\overline{1}\}$ and a single projectivized orbit. There are two possibilities for a 2-dimensional subspace V over $\mathbb{F}_q$: either $V = \gamma\mathbb{F}_{q^2}$ for some $\gamma \in \mathbb{F}_{q^n}$ (hence n is even) or V itself has full-length orbit. In the first case, we can explicitly describe A_V.

Proposition 30. Let n be even and $U \in \mathcal{G}_q(k,n)$ generate a full-length orbit with $\mathrm{d}(\mathrm{Orb}(U)) = 2k-4$. Suppose there exist $\alpha, \gamma \in \mathbb{F}_{q^n}^*$ such that $V := \gamma\mathbb{F}_{q^2} = U \cap \alpha U$. Then $A_V = \mathbb{P}(\mathbb{F}_{q^2})$ and thus $|A_V| = q+1$.

Proof. We can reduce to the case $\gamma = 1$ since any $\beta \in \mathbb{F}_{q^n}^*$ satisfies

$$\gamma\mathbb{F}_{q^2} = U \cap \beta U \iff \mathbb{F}_{q^2} = \gamma^{-1}U \cap \beta\gamma^{-1}U = U' \cap \beta U', \tag{2.3.5}$$

where $U' = \gamma^{-1}U$. Notice that $\mathrm{Orb}(U') = \mathrm{Orb}(U)$. If we can show that

$$\{\overline{\beta} \mid \mathbb{F}_{q^2} \subseteq U' \cap \beta U'\} = \mathbb{P}(\mathbb{F}_{q^2}),$$

the claim follows from (2.3.5). Thus we assume that $V = \mathbb{F}_{q^2} = U \cap \alpha U$.

In order to show $A_V \subseteq \mathbb{P}(\mathbb{F}_{q^2})$ suppose to the contrary that there exists $\beta \in A_V \setminus \mathbb{P}(\mathbb{F}_{q^2})$. Then $\mathbb{F}_{q^2} = U \cap \beta U$ and $\beta^{-1}\mathbb{F}_{q^2} \cap \mathbb{F}_{q^2} = \{0\}$. Furthermore,

$$\mathbb{F}_{q^2} \subset U \quad \text{and} \quad \beta^{-1}\mathbb{F}_{q^2} \subset U.$$

Therefore $k \geq 4$ and we can decompose U as $U = \mathbb{F}_{q^2} \oplus \beta^{-1}\mathbb{F}_{q^2} \oplus U'$ for some $U' \in \mathcal{G}_q(k-4,n)$. Now we have for any $\rho \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$

$$\rho^{-1}(\mathbb{F}_{q^2} \oplus \beta^{-1}\mathbb{F}_{q^2}) = \mathbb{F}_{q^2} \oplus \beta^{-1}\mathbb{F}_{q^2} \subseteq U,$$

so $\mathbb{F}_{q^2} \oplus \beta^{-1}\mathbb{F}_{q^2} \subseteq U \cap \rho U$ and thus $\dim(U \cap \rho U) \geq 4$. Since $\rho \notin \mathrm{Stab}(U) = \mathbb{F}_q^*$, this contradicts $\mathrm{d}(\mathrm{Orb}(U)) = 2k-4$. All of this shows that $A_V \subseteq \mathbb{P}(\mathbb{F}_{q^2})$.

In the same way, since $\mathbb{F}_{q^2} \subseteq U$, every $\overline{\rho} \in \mathbb{P}(\mathbb{F}_{q^2})$ leads to $\mathbb{F}_{q^2} \subseteq U \cap \rho U$, and thus $\overline{\rho} \in A_V$. Hence $\mathbb{P}(\mathbb{F}_{q^2}) \subseteq A_V$, and this concludes the proof. □

Remark 31. The above result generalizes straightforwardly to full-length orbits with distance $2k-2\ell$ and intersections of the form $V = \gamma\mathbb{F}_{q^\ell} = U \cap \alpha U$. In that case one arrives at $A_V = \mathbb{P}(\mathbb{F}_{q^\ell})$.

The line of argument in the first part of the above proof can be extended to show that there is at most one such V arising as an intersection $U \cap \alpha U$.

Proposition 32. Let $U \in \mathcal{G}_q(k,n)$ generate a full-length orbit with $\mathrm{d}(\mathrm{Orb}(U)) = 2k-4$. Then there exists at most one subspace $V \in \mathcal{G}_q(2,n)$ such that $V = U \cap \alpha U$ for some $\alpha \in \mathbb{F}_{q^n}^*$ and $V = \gamma\mathbb{F}_{q^2}$ for some $\gamma \in \mathbb{F}_{q^n}^*$.

Proof. If n is odd, no such subspace exists, so let n be even. Suppose to the contrary that there exist distinct subspaces V_1, V_2 such that $V_1 = U \cap \alpha_1 U = \gamma_1 \mathbb{F}_{q^2}$ and $V_2 = U \cap \alpha_2 U = \gamma_2 \mathbb{F}_{q^2}$. We will show that $\mathrm{d}(\mathrm{Orb}(U)) < 2k-4$.

Since $V_1 \neq V_2$, we must have $\frac{\gamma_1}{\gamma_2} \notin \mathbb{F}_{q^2}$ and even $\gamma_1 \mathbb{F}_{q^2} \cap \gamma_2 \mathbb{F}_{q^2} = \{0\}$. Now $\gamma_1 \mathbb{F}_{q^2} \subseteq U$ and $\gamma_2 \mathbb{F}_{q^2} \subseteq U$ implies $U = \gamma_1 \mathbb{F}_{q^2} \oplus \gamma_2 \mathbb{F}_{q^2} \oplus U'$ for some $U' \in \mathcal{G}_q(k-4, n)$. This in turn leads to $\gamma_1 \mathbb{F}_{q^2} \oplus \gamma_2 \mathbb{F}_{q^2} \subseteq U \cap \rho U$ for any $\rho \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Since $\rho \notin \mathrm{Stab}(U)$, we arrive at the contradiction $\mathrm{d}(\mathrm{Orb}(U)) \leq 2k-8 < 2k-4$. □

It remains to describe the behavior when a maximal intersection $V = U \cap \alpha U$ has full-length orbit. In this case it turns out that there is a collection of related subspaces $\{V_i\}$ that all have associated sets A_{V_i} of the same cardinality. Further, each V_i is given by the cyclic shift $\alpha_i^{-1} V$ for some $\alpha_i \in A_V$ and we can explicitly describe the elements of A_{V_i} in terms of those of A_V. This holds even in the more general setting where $\mathrm{d}(\mathrm{Orb}(U)) = 2k - 2\ell$. Although we will give the proof for the case $\ell = 2$, the general case does not differ significantly. Therefore Proposition 33 can be easily extended to the general case where U has full-length orbit with $\mathrm{d}(\mathrm{Orb}(U)) = 2k-2\ell$ and $V = U \cap \alpha U \in \mathcal{G}_q(\ell, n)$ such that $\mathrm{Stab}(V) = \mathbb{F}_q^*$. In particular, if $\gcd(\ell, n) = 1$ then $\mathrm{Stab}(V) = \mathbb{F}_q^*$ for *every* maximal intersection $V = U \cap \alpha U$ and the proposition applies.

For the following result recall from Definition 27 that if U generates a full-length orbit then $A_V = \{\overline{1}\} \cup \{\overline{\beta} \mid V = U \cap \beta U\}$.

Proposition 33. Let $U \in \mathcal{G}_q(k, n)$ generate a full-length orbit with $\mathrm{d}(\mathrm{Orb}(U)) = 2k-4$. Furthermore, suppose there exists $V \in \mathcal{G}_q(2, n)$ such that $V = U \cap \alpha_1 U$ for some $\alpha_1 \in \mathbb{F}_{q^n}^*$ and V generates a full-length orbit. Let $|A_V| = s+1$ and write $A_V = \{\overline{\alpha_1}, \ldots, \overline{\alpha_s}, \overline{1}\}$.

(a) The distinct cyclic shifts of V that arise as intersections $U \cap \beta U$ are precisely the shifts by elements $\{\overline{\alpha_i^{-1}} \mid i = 1, \ldots, s\} \cup \{\overline{1}\}$. In particular, there are $|A_V| = s+1$ such shifts.

(b) For each $i = 1, \ldots, s$ we have $A_{\alpha_i^{-1} V} = \{\overline{\alpha_j \alpha_i^{-1}} \mid j = 1, \ldots, s\} \cup \{\overline{\alpha_i^{-1}}\}$ and $|A_{\alpha_i^{-1} V}| = s+1$.

Proof. (a) First we show that each $\alpha_i^{-1} V$ arises as an intersection $U \cap \beta U$. By assumption, $V = U \cap \alpha U = \langle v_0, w_0 \rangle$ for some $v_0, w_0 \in V$. Then for each $i \in \{1, \ldots, s\}$ there exist $v_i, w_i \in U$ such that

$$v_0 = \alpha_i v_i \quad \text{and} \quad w_0 = \alpha_i w_i.$$

Define $V_i = \alpha_i^{-1} V = \langle v_i, w_i \rangle$. Then

$$U \cap \alpha_i^{-1} U = \alpha_i^{-1}(U \cap \alpha_i U) = \alpha_i^{-1} V = V_i, \tag{2.3.6}$$

so each of the shifts V_i arises as an intersection.

Next we show that $V, V_1, \ldots, V_s$ are distinct. It follows immediately that $V \neq V_i$ for any i because $\mathrm{Stab}(V) = \mathbb{F}_q^*$ and $\overline{\alpha_i} \neq \overline{1}$. Suppose now $V_i = V_j$, thus $\langle v_i, w_i \rangle = \langle v_j, w_j \rangle$. From

$$v_i = \frac{\alpha_j}{\alpha_i} v_j \quad \text{and} \quad w_i = \frac{\alpha_j}{\alpha_i} w_j \tag{2.3.7}$$

we conclude that $\frac{\alpha_j}{\alpha_i} \in \mathrm{Stab}(V_i) = \mathrm{Stab}(V) = \mathbb{F}_q^*$, and since $\overline{\alpha_i} \neq \overline{\alpha_j}$ if $i \neq j$, we arrive at $i = j$.

It remains to show that the shifts V_i are the only cyclic shifts of V that arise as intersections. Suppose $W = \gamma V = U \cap \beta U$ for some $\gamma, \beta \in \mathbb{F}_{q^n}^*$. Then $V = \gamma^{-1}W \subseteq \gamma^{-1}U$ and thus $V \subseteq U \cap \gamma^{-1}U$ by choice of V. Thus $\overline{\gamma^{-1}} \in A_V$, as desired.
(b) Recall that $A_{V_i} = \{\overline{\beta} \in \mathbb{P}(\mathbb{F}_{q^n}) \mid U \cap \beta U = V_i\} \cup \{\overline{1}\}$. We want to show that

$$A_{V_i} = \left\{ \overline{\frac{1}{\alpha_i}}, \overline{\frac{\alpha_1}{\alpha_i}}, \ldots, \overline{\frac{\alpha_s}{\alpha_i}} \right\}. \tag{2.3.8}$$

For "$\supseteq$" note that trivially $\overline{1} \in A_{V_i}$ and $\overline{\alpha_i^{-1}} \in A_{V_i}$ thanks to (2.3.6). Consider now $\overline{\alpha_j \alpha_i^{-1}}$ for $j \neq i$. Then $\overline{\alpha_j} \neq \overline{\alpha_i}$ and thus $\frac{\alpha_j}{\alpha_i} \notin \mathbb{F}_q^* = \mathrm{Stab}(U)$. Moreover, (2.3.7) yields $V_i \subseteq U \cap \frac{\alpha_j}{\alpha_i}U$. Since by assumption the dimension of the intersection cannot be bigger than 2, we conclude $V_i = U \cap \frac{\alpha_j}{\alpha_i}U$.
For "$\subseteq$" suppose $\overline{\beta} \in A_{V_i} \setminus \{\overline{\alpha_i^{-1}}, \overline{1}\}$. Then there exist $u_1, u_2 \in U$ such that $v_i = \beta u_1$ and $w_i = \beta u_2$. Thus $\alpha_i \beta u_1 = v_0$, $\alpha_i \beta u_2 = w_0$ and $\overline{\alpha_i \beta} \neq \overline{1}$. All of this shows that $U \cap \alpha_i \beta U = V$. Hence $\overline{\alpha_i \beta} \in A_V$ and so $\overline{\alpha_i \beta} = \overline{\alpha_j}$ for some $j \in \{1, \ldots, s\}$. Thus $\overline{\beta} = \overline{\alpha_j \alpha_i^{-1}}$. This establishes (2.3.8). Finally, it is easy to see that the listed elements in (2.3.8) are distinct and thus $|A_{V_i}| = s + 1$. □

Our next result says that $|A_V| = q + 1$ in the situation of Proposition 33.

Proposition 34. Let $U \in \mathcal{G}_q(k, n)$ generate a full-length orbit with $\mathrm{d}(\mathrm{Orb}(U)) = 2k - 4$. Suppose there exists $V \in \mathcal{G}_q(2, n)$ such that $V = U \cap \alpha U$ for some $\alpha \in \mathbb{F}_{q^n}^*$. Let $\overline{\beta} \in A_V \setminus \{\overline{1}\}$. Then
(a) $\overline{\alpha} = \overline{\beta}$ or $1 = \lambda\alpha^{-1} + \mu\beta^{-1}$ for some $\lambda, \mu \in \mathbb{F}_q^*$,
(b) $|A_V| = q + 1$.

Proof. (a) Let $V = \langle v_1, v_2 \rangle = U \cap \alpha U$ and let $\overline{\beta} \in A_V \setminus \{\overline{1}\}$. Then there exist $u_1, u_2, w_1, w_2 \in U$ such that

$$v_i = \alpha u_i = \beta w_i \text{ for } i = 1, 2.$$

Note that $v_1, v_2 \in U$ as well. Define $\tilde{U} = \langle v_1, u_1, w_1 \rangle$. Then $\tilde{U} \subseteq U$ and

$$\frac{v_2}{v_1}\tilde{U} = \langle v_2, u_2, w_2 \rangle \subseteq U \cap \frac{v_2}{v_1}U.$$

Since v_1, v_2 are $\mathbb{F}_q$-linearly independent, the element $\frac{v_2}{v_1}$ is not in $\mathbb{F}_q^* = \mathrm{Stab}(U)$, and thus $U \cap \frac{v_2}{v_1}U \neq U$. Therefore $\dim(U \cap \frac{v_2}{v_1}U) \leq 2$ and so $\{v_1, u_1, w_1\}$ must be $\mathbb{F}_q$-linearly dependent.

Now we may argue as follows. First of all, the sets $\{v_1, u_1\}$ and $\{v_1, w_1\}$ are both $\mathbb{F}_q$-linearly independent because $\alpha, \beta \notin \mathbb{F}_q$. Next, if $u_1 = \lambda w_1$ for some $\lambda \in \mathbb{F}_q$ then $\beta w_1 = \alpha u_1 = \alpha\lambda w_1$, and hence $\overline{\beta} = \overline{\alpha}$. It remains to consider the case $v_1 = \lambda u_1 + \mu w_1$ for some $\lambda, \mu \in \mathbb{F}_q^*$. But this implies immediately $1 = \lambda\alpha^{-1} + \mu\beta^{-1}$, as desired.

(b) Let $\overline{\beta} \in A_V \setminus \{\overline{1}, \overline{\alpha}\}$. Part (a) tells us that $\mu\beta^{-1} = 1 - \lambda\alpha^{-1}$ for some $\lambda, \mu \in \mathbb{F}_q^*$. The $q - 1$ choices for λ imply that there are at most $q - 1$ options for such $\overline{\beta}$. Thus $|A_V| \leq q + 1$. The reverse inequality has been established in Proposition 29(b). □

We now have all of the pieces in place to prove Theorem 23.

Proof of Theorem 23. By applying (2.2.4) and Remark 15 with $t = 1$ and $\ell = 2$ we notice that it suffices to compute λ_2 for such a subspace U. Hence we need to determine $|\{\overline{\beta} \mid \dim(U \cap \beta U) = 2\}|$. We distinguish two cases.
Case 1: Suppose U contains a cyclic shift of $\mathbb{F}_{q^2}$. Then $U = \gamma\mathbb{F}_{q^2} \oplus U'$ for some $U' \in \mathcal{G}_q(k-2, n)$ and $\gamma \in \mathbb{F}_{q^n}$. Then $|A_{\gamma\mathbb{F}_{q^2}} \setminus \{\overline{1}\}| = q$ by Proposition 30, and this is the number of $\overline{\beta} \in \mathbb{P}(\mathbb{F}_{q^n})$ such that $U \cap \beta U = \gamma\mathbb{F}_{q^2}$. Moreover, thanks to Proposition 32 there does not exist any $V \in \mathcal{G}_q(2, n)$ such that $V = \gamma'\mathbb{F}_{q^2} = U \cap \alpha U$ for some $\alpha, \gamma' \in \mathbb{F}_{q^n}$ except for $V = \gamma\mathbb{F}_{q^2}$. In other words, any other 2-dimensional intersection $V = U \cap \alpha U$ has full-length orbit. Proposition 34 shows that for each such V we have $|A_V \setminus \{\overline{1}\}| = q$, which is the number of $\overline{\beta} \in \mathbb{P}(\mathbb{F}_{q^n})$ leading to the 2-dimensional intersection V. Furthermore, Proposition 33 says that the collection of all 2-dimensional intersections with full-length orbit can be partitioned into sets of the form $\{V, \alpha_1^{-1}V, \ldots, \alpha_q^{-1}V\}$, each one with cardinality $q+1$. Suppose we have r such sets. Note that $r = 0$ is possible. Then

$$\sum_{\substack{V=U\cap\alpha U \\ \dim(V)=2 \\ V\neq\gamma\mathbb{F}_{q^2}}} |A_V \setminus \{\overline{1}\}| = rq(q+1).$$

Combining all of this, we arrive at $\lambda_2 = q + rq(q+1)$, as desired.
Case 2: Suppose U does not contain a cyclic shift of $\mathbb{F}_{q^2}$. Then any $V \in \mathcal{G}_q(2, n)$ with $V = U \cap \alpha U$ for some α has full-length orbit and since $\mathrm{d}(\mathrm{Orb}(U)) = 2k-4$ there exists at least one such subspace. So the previous argument shows that

$$\sum_{\substack{V=U\cap\alpha U \\ \dim(V)=2}} |A_V \setminus \{\overline{1}\}| = rq(q+1) \text{ for some } r \geq 1$$

and $\lambda_2 = rq(q+1)$, as stated. □

We conclude this section with some examples illustrating various intersection distributions for full-length orbits with distance $2k-4$. We used SageMath to compute the values of λ_2 and r that occurred for some different values of the parameters q, n, and k. Recall from Theorem 23 that λ_2 fully determines the intersection distribution. For each triple (q, n, k), we generated random subspaces in $\mathcal{G}_q(k, n)$ containing the element 1 and analyzed those that generated a full-length orbit with distance $2k-4$. In Table 2.1 we list all occurring values for λ_2 along with their frequency N, ordered accordingly. For example, when $(q, n, k) = (2, 10, 4)$ we found 248 subspaces with $\lambda_2 = 2$ and 2598 subspaces with $\lambda_2 = 6$ etc. In the same way we list the corresponding value of r. Recall from Corollary 24 that the maximum possible value for λ_2 is $Q/(q+1)$.

Besides these random searches we also performed, for various choices of parameters, exhaustive searches among all subspaces in $\mathcal{G}_q(k, n)$ that contain 1. We mostly restricted ourselves to $k = 3$ because of computational feasibility. The results of these exhaustive searches are presented in Table 2.2 on the following pages. Recall that

Table 2.1: Example values of λ_2, r for random search of full-length orbits with distance $2k-4$

q	n	k	λ_2	r	N	$\frac{Q}{q+1}$
2	10	4	$2,6,8,12,14,$ $18,20,24,30$	$0,1,1,2,2,$ $3,3,4,5$	$248,2598,34,2059,90,$ $298,94,195,49$	70
2	11	4	$6,12,18,24,30,42$	$1,2,3,4,5,7$	$1760,1251,63,57,12,24$	70
2	11	5	$6,12,18,24,30,36,42,$ $48,54,60,66,$ $72,78,84,90,$ $96,102,108,114,120,126$	$1,2,3,4,5,6,7,$ $8,9,10,11,$ $12,13,14,15,$ $16,17,18,19,20,21$	$3,7,22,67,243,494,982,$ $1228,1483,1285,1143,$ $783,519,258,153,$ $90,39,29,11,2,1$	310
2	12	4	$2,6,8,12,14,18,$ $20,24,30,42$	$0,1,1,2,2,3,$ $3,4,5,6$	$150,953,4,664,6,13,$ $9,13,2,4$	70
2	13	4	$6,12,18,24,30,42$	$1,2,3,4,5,7$	$1486,967,7,8,3,18$	70
2	13	5	$6,12,18,24,36,42,$ $48,54,60,66,72$	$1,2,3,4,5,6,7,$ $8,9,10,11,12$	$1136,2933,1535,1485,528,$ $437,148,97,36,26,6,6$	310
3	9	4	$12,24,36,$ $48,60,72,84$	$1,2,3,$ $4,5,6,7$	$2900,3537,283,$ $354,290,160,55$	390 390
3	11	4	$12,24,36,48,60,72,84$	$1,2,3,4,5,6,7$	$1048,1091,4,8,12,6,2$	390
3	12	4	$3,12,24,27,36,48$	$0,1,2,2,3,4$	$21,288,397,1,2,4$	390

only subspaces containing 1 and generating a full-length orbit of distance $2k-4$ are being considered. Again, the values of N in the table are the frequencies of the values of λ_2 (and r). Notice in particular that the values of λ_2 we found by random search in Table 2.1 for $q=2, n=10, k=4$ do indeed exhaust all possible values of λ_2 for these parameters.

Each value of N appearing in Table 2.2 is a multiple of $(q^k-1)/(q-1)$; this is due to the fact that for any subspace U containing 1, the shifts $\alpha^{-1}U$ for $\alpha \in U \setminus 0$ also contain 1 and generate the same orbit as U. Furthermore, these are all of the elements of $\mathrm{Orb}(U)$ that contain 1. This means that our exhaustive search counts every cyclic orbit code $(q^k-1)/(q-1)$ times. Note that Table 2.2 shows that the upper bound for λ_2 in Corollary 24 is quite poor in general.

Finally we present an example concerning the value $f(U)$. From Theorem 21 and Corollary 24 we know that for full-length orbits $\mathrm{Orb}(U)$ with distance $2k-2$ or $2k-4$ the intersection distribution is completely determined by q, n, k, and $f(U)$; see also (2.3.3). In fact, this also holds when the distance is $2k$ because in that case the intersection distribution is trivial. It is thus natural to ask whether $q, n, k, f(U)$ along with the distance also determine the intersection distribution of full-length orbits if the distance is at most $2k-6$.

However, this does not hold. Furthermore, q, n, k, and $f(U)$ do not determine the distance of the orbit code.

Table 2.2: Values of λ_2, r for exhaustive search of full-length orbits with distance $2k-4$

q	n	k	λ_2	r	N	$\frac{Q}{q+1}$
2	6	3	$2,6$	$0,1$	$35,63$	14
2	7	3	6	1	147	14
2	8	3	$2,6,14$	$0,1,2$	$140,280,7$	14
2	8	4	$12,14,18,20$ $24,30,38$	$2,2,3,4,$ $4,5,6$	$1080,1200,3000,1200,$ $2760,1200,750$	70
2	9	3	6	1	588	14
2	9	4	$6,12,18,24,30$	$1,2,3,4,5$	$31995,33120,11340,7560,2025$	70
2	10	3	$2,6$	$0,1$	$595,1190$	14
2	10	4	$2,6,8,12,14,$ $18,20,24,30$	$0,1,1,2,2,$ $3,3,4,5$	$35700,213375,2550,164235,7650,$ $22725,7650,14325,3750$	70
3	6	3	$3,12$	$0,1$	$130,377$	39
3	7	3	12	1	1183	39
3	8	3	$3,12,39$	$0,1,3$	$1170,3510,13$	39
3	9	3	12	1	10647	39
5	6	3	$5,30$	$0,1$	$806,3999$	155

Example 35. Let $q=2, n=11, k=5$ and suppose ω is a primitive element of $\mathbb{F}_{2^{11}}$ over $\mathbb{F}_2$ satisfying $\omega^{11}=\omega^2+1$. Define

$$\begin{aligned} U &= \langle 1, \omega^{417}, \omega^{1823}, \omega^{1983}, \omega^{64} \rangle, \\ V &= \langle 1, \omega^{1332}, \omega^{468}, \omega^{749}, \omega^{1627} \rangle, \\ W &= \langle 1, \omega^{1618}, \omega^{942}, \omega^{1041}, \omega^{1315} \rangle. \end{aligned}$$

Then all three subspaces generate full-length orbits. A computation using SageMath shows that $\mathrm{d}(\mathrm{Orb}(U)) = \mathrm{d}(\mathrm{Orb}(V)) = 4 = 2k-6$, whereas $\mathrm{d}(\mathrm{Orb}(W)) = 6 = 2k-4$. Furthermore, $f(U) = f(V) = f(W) = 703$, and hence f does not determine the distance. Finally $\mathrm{Orb}(U)$ has intersection distribution $(\lambda_0, \lambda_1, \lambda_2, \lambda_3) = (1343, 624, 60, 18)$ while $\mathrm{Orb}(V)$ has $(\lambda_0, \lambda_1, \lambda_2, \lambda_3) = (1343, 600, 96, 6)$. Thus, the intersection distribution is not determined by q, n, k, f and the distance.

2.4 Intersection Distributions of Unions of Full-Length Orbits

In this section we generalize the ideas of Sections 1.2 and 2.2 to codes that arise as union of orbits generated by subspaces of the same dimension. We need to start by adapting the definitions from the single orbit case to multiple orbits. Analogously to Definitions 7 and 14 we define the distance and intersection distributions with respect to fixed reference spaces for each orbit. In order to relate these two distributions we need to restrict ourselves to subspaces with the same stabilizer.

Definition 36. Let $k \leq n/2$ and $U_j \in \mathcal{G}_q(k,n)$ with $\mathrm{Stab}(U_j) = \mathbb{F}_{q^t}$ for $j = 1, \ldots, m$ such that the U_j generate distinct orbits and define $\mathcal{C} = \bigcup_{j=1}^{m} \mathrm{Orb}(U_j)$. Suppose $\mathrm{d}(\mathcal{C}) = 2d$. For $i = 0, \ldots, k$ define

$$\delta_{2i} = |\{(U_j, \alpha U_{j'}) \mid 1 \leq j \leq j' \leq m,\ \alpha \in \mathbb{F}_{q^n}^*,\ \mathrm{d}(U_j, \alpha U_{j'}) = 2i\}|.$$

We call $(\delta_0, \ldots, \delta_{2k})$ the *weight distribution* of $\mathcal{C}$. Then $\delta_0 = m$ and as in Definition 7 the only other possibly nonzero entries are $(\delta_{2d}, \ldots, \delta_{2k})$ Furthermore, we set $\ell = k-d$, thus ℓ is the maximum dimension of the intersection spaces $U_j \cap \alpha U_{j'}$. For $i = 0, \ldots, \ell$ and $1 \leq j \leq j' \leq m$ we define $\mathcal{L}_i(U_j, U_{j'}) = \{\overline{\alpha} \in \mathbb{P}(\mathbb{F}_{q^n}) \mid \dim(U_j \cap \alpha U_{j'}) = i\}$ and set λ_i as

$$\lambda_i(\mathcal{C}) = \sum_{j \leq j'} |\mathcal{L}_i(U_j, U_{j'})|.$$

We call $(\lambda_0, \ldots, \lambda_\ell)$ the *intersection distribution* of $\mathcal{C}$. As in Remark 15 we have $\lambda_i = (q^t - 1)/(q-1)\delta_{2(k-i)}$ for $i = 0, \ldots, \ell$.

We now extend Definition 17 to the case of multiple generating subspaces. It will suffice to extend the definitions to pairs (U, V) of subspaces and we will do so for $\mathcal{L}$, $\mathcal{M}$, and $\mathcal{F}$. There is no meaningful generalization of $\mathcal{S}(U)$ to two spaces, and in fact no such space will be needed.

Definition 37. Let $k \leq n/2$ and $U, V \in \mathcal{G}_q(k, n)$. Define $\ell = \max\{\dim(U \cap \alpha V) \mid \alpha \in \mathbb{F}_{q^n}^*\}$. Note that the cyclic code $\mathrm{Orb}(U) \cup \mathrm{Orb}(V)$ has minimum distance at most $2k - 2\ell$. We define
(1) $\mathcal{L}(U, V) = \bigcup_{i=1}^{\ell} \mathcal{L}_i(U, V)$, where $\mathcal{L}_i(U, V)$ is as in Definition 36.
(2) $\mathcal{M}(U, V) = \{(\overline{u}, \overline{v}) \mid u \in U \setminus 0, v \in V \setminus 0\}$.
(3) $\mathcal{F}(U, V) = \{\overline{uv^{-1}} \mid u \in U \setminus 0, v \in V \setminus 0\}$ and $f_{U,V} := |\mathcal{F}(U, V)|$.

Notice that when $U = V$, each of these definitions reduces to the corresponding part in Definition 17. As in the single subspace case, we omit $i = 0$ from the definition of $\mathcal{L}(U, V)$ since λ_0 can be calculated from λ_i, $i = 1, \ldots, \ell$. We will carry this out in the proof of Theorem 42.

Again, the cardinality of $\mathcal{M}(U, V)$ depends only on q, n, and k and we denote this by

$$\widehat{Q} := |\mathcal{M}(U, V)| = \left(\frac{q^k - 1}{q - 1}\right)^2. \tag{2.4.1}$$

For any two subspaces $U, V \in \mathcal{G}_q(k, n)$ generating different orbit codes we have again a map $\psi : \mathcal{M}(U, V) \to \mathbb{P}(\mathbb{F}_{q^n})$ given by $\psi(\overline{u}, \overline{v}) = \overline{uv^{-1}}$. As in Section 2.2, ψ surjects onto $\mathcal{L}(U, V)$.

Proposition 38. Let $U, V \in \mathcal{G}_q(k, n)$ such that $\mathrm{Orb}(U) \neq \mathrm{Orb}(V)$ and set $\ell = \max\{\dim(U \cap \alpha V) \mid \alpha \in \mathbb{F}_{q^n}^*\}$. The map $\psi : \mathcal{M}(U, V) \to \mathcal{F}(U, V), \quad (\overline{u}, \overline{v}) \longmapsto \overline{uv^{-1}}$ is well-defined. It satisfies $\mathcal{F}(U, V) = \psi(\mathcal{M}(U, V)) = \mathcal{L}(U, V)$. Furthermore, for any $\overline{\alpha} \in \mathcal{F}(U, V)$ we have

$$\overline{\alpha} \in \mathcal{L}_i(U, V) \iff |\psi^{-1}(\overline{\alpha})| = (q^i - 1)/(q - 1).$$

Proof. The well-definedness of ψ is clear and so is $\psi(\mathcal{M}(U, V)) = \mathcal{F}(U, V)$. We show next that $\psi(\mathcal{M}(U, V)) = \mathcal{L}(U, V)$. First, let $\overline{\alpha} = \overline{uv^{-1}} \in \psi(\mathcal{M}(U, V))$ for some $u \in U \setminus 0, v \in V \setminus 0$. Then there exists $\lambda \in \mathbb{F}_q^*$ such that $u = \lambda \alpha v$. Since $\lambda V = V$ this implies $U \cap \alpha V \neq 0$. Hence $\dim(U \cap \alpha V) \in \{1, \ldots, \ell\}$ and thus $\overline{\alpha} \in \mathcal{L}(U, V)$. This shows $\psi(\mathcal{M}(U, V)) \subseteq \mathcal{L}(U, V)$. The proof of the reverse inclusion proceeds similarly.

If $\overline{\alpha} \in \mathcal{L}(U,V)$, then $1 \leq \dim(U \cap \alpha V) \leq \ell$. Hence there exist $u \in U \setminus 0, v \in V \setminus 0$ with $u = \alpha v$. So $\overline{\alpha} = \overline{uv^{-1}}$ is in $\psi(\mathcal{M}(U,V))$.

It remains to show $\overline{\alpha} \in \mathcal{L}_i(U,V) \iff |\psi^{-1}(\overline{\alpha})| = (q^i-1)/(q-1)$. Fix $\overline{\alpha} \in \mathcal{F}(U,V)$. Note first that for $(\overline{v},\overline{w}) \in \psi^{-1}(\overline{\alpha})$, the second component $\overline{w}$ is uniquely determined by the first one. Thus it suffices to count the number of possible first components.

Let $\overline{\alpha} \in \mathcal{L}_i(U,V)$. Hence $\dim(U \cap \alpha V) = i$. Then for every $v \in U \cap \alpha V$ there exists $w \in V$ such that $v = \alpha w$. Using that there exist $(q^i-1)/(q-1)$ elements $\overline{v}$ such that $v \in U \cap \alpha V$, it follows that $|\psi^{-1}(\overline{\alpha})| \geq (q^i-1)/(q-1)$. Conversely, suppose that $(\overline{x},\overline{y}) \in \psi^{-1}(\overline{\alpha})$. Then $\overline{x} = \overline{\alpha y}$ and $x = \lambda \alpha y$ for some $\lambda \in \mathbb{F}_q$. Thus $x \in U \cap \alpha V$. This leaves $(q^i-1)/(q-1)$ choices for $\overline{x}$, and thus $|\psi^{-1}(\overline{\alpha})| \leq \frac{q^i-1}{q-1}$. Hence $|\psi^{-1}(\overline{\alpha})| = \frac{q^i-1}{q-1}$. □

The restriction that $\mathrm{Orb}(U) \neq \mathrm{Orb}(V)$ implies that $U \neq \alpha V$ for any α, hence the differences between the statements of Proposition 18 and Proposition 38. As in Section 2.2, we can use this result to derive identities relating the sizes $|\mathcal{L}_i(U,V)|$ for $i = 1, \ldots, \ell$.

Corollary 39. Let $U, V \in \mathcal{G}_q(k,n)$ such that $\mathrm{Orb}(U) \neq \mathrm{Orb}(V)$.
Let $\ell = \max\{\dim(U \cap \alpha V) \mid \alpha \in \mathbb{F}_{q^n}^*\}$. Recall the cardinalities $f_{U,V} = |\mathcal{F}(U,V)|$, $\widehat{Q} = |\mathcal{M}(U,V)|$, and set $\lambda_i = |\mathcal{L}_i(U,V)|$ for $i = 1, \ldots, \ell$. Then

$$f_{U,V} = \sum_{i=1}^{\ell} \lambda_i. \tag{2.4.2}$$

and

$$\widehat{Q} = \sum_{i=1}^{\ell} \frac{q^i-1}{q-1} \lambda_i. \tag{2.4.3}$$

Proof. The identity in (2.4.2) follows immediately from $\mathcal{L}(U,V) = \mathcal{F}(U,V)$ from Proposition 38. From the same proposition we have $\psi(\mathcal{M}(U,V)) = \mathcal{L}(U,V)$, thus $\mathcal{M}(U,V) = \bigcup_{i=1}^{\ell} \psi^{-1}(\mathcal{L}_i(U,V))$. Now (2.4.3) follows from Proposition 38 and the cardinality of $\mathcal{M}(U,V)$ in (2.4.1). □

In the single orbit case, we saw that orbit codes generated by a Sidon space have full length and maximal possible dimension. The Sidon property can be extended to various spaces in such a way that the orbits stay sufficiently far away from each other in the subspace distance. This reads as follows.

Definition 40. Let U and V be distinct k-dimensional subspaces of $\mathbb{F}_{q^n}$. We say that U and V are *combinable* if any $a, c \in U \setminus 0$ and $b, d \in V \setminus 0$ with $ab = cd$ satisfy $\overline{a} = \overline{c}$ and $\overline{b} = \overline{d}$.

Lemma 41 ([26, Lemma 36])**.** Let U and V be distinct subspaces in $\mathcal{G}_q(k,n)$. The following conditions are equivalent.
(a) $\dim(U \cap \alpha V) \leq 1$ for all $\alpha \in \mathbb{F}_{q^n}^*$.
(b) U and V are combinable.

As a consequence, if $U, V \in \mathcal{G}_q(k,n)$ are Sidon spaces and are combinable then the cyclic subspace code $\mathrm{Orb}(U) \cup \mathrm{Orb}(V)$ has cardinality $2(q^n-1)/(q-1)$ and distance $2k-2$.

For $q=2$, Elsenhans and Kohnert [7, 2.5 iv)] defined combinable to mean that U and V have property (a) of Lemma 41. We use combinable for the equivalent generalized property of Definition 40. Comparing the above definition with Definition 5 one may wonder whether the assumption $ab = cd$ should also allow for the conclusion $\overline{a} = \overline{d}$ and $\overline{c} = \overline{b}$, which is an option in the case where $a, b, v, d \in U \cap V$. However, this is not necessary. The difference between the above lemma and the situation in Theorem 6 lies in the obvious fact that the property $\dim(U \cap \alpha V) \leq 1$ for all $\alpha \in \mathbb{F}_{q^n}^*$ can never be true if $V = U$. For further details we refer to the proofs of Theorem 6 and Lemma 41 in [26].

We can use the above lemma to extend our earlier results to cyclic codes that are unions of cyclic orbits generated by Sidon spaces that are pairwise combinable. Such codes have maximal possible length and distance $2k-2$. Their existence has been established in [26, Construction 37], where the authors give a construction as a generalization of their own [26, Construction 15]. Another construction from the same paper, [26, Construction 11], can be generalized in the same way to give another class of cyclic codes of this type.

We have now all of the necessary pieces to describe the intersection distribution of such codes.

Theorem 42. Let $U_1, \ldots, U_m \in \mathcal{G}_q(k,n)$ be distinct subspaces such that each U_i is a Sidon space and each pair U_i, U_j with $i \neq j$ is combinable. Let $\mathcal{C} = \bigcup_{i=1}^{m} \mathrm{Orb}(U_i)$. Then $\mathcal{C}$ is a cyclic subspace code with $|\mathcal{C}| = m(q^n-1)(q-1)^{-1}$ and $\mathrm{d}(\mathcal{C}) = 2k-2$. Further $\mathcal{C}$ has intersection distribution (λ_0, λ_1) where

$$\lambda_1 = mQ + \binom{m}{2}\widehat{Q},$$
$$\lambda_0 = m\left(\frac{q^n-1}{q-1} - Q - 1\right) + \binom{m}{2}\left(\frac{q^n-1}{q-1} - \widehat{Q}\right).$$

Proof. Clearly $\mathcal{C}$ is a cyclic subspace code (in the sense of the paragraph before Definition 1). Each orbit has size $(q^n-1)(q-1)^{-1}$ since it is generated by a Sidon space, and because each pair is combinable, Lemma 41 implies that the orbits are disjoint. Hence $|\mathcal{C}| = m(q^n-1)(q-1)^{-1}$. As for the minimum distance note that on the one hand $\min\{\mathrm{d}(U_j, \alpha U_{j'}) \mid j < j',\, \alpha \in \mathbb{F}_{q^n}^*\} \geq 2k-2$ thanks to Lemma 41 while on the other hand each orbit itself has distance $2k-2$ by Theorem 6.

For the intersection distribution define $\lambda_{i,j,j'} = |\mathcal{L}_i(U_j, U_{j'})|$ for $i = 0, 1$ and $1 \leq j \leq j' \leq m$. Recall that $\lambda_i = \sum_{j \leq j'} \lambda_{i,j,j'}$. Since each U_j is a Sidon space, Theorem 21 gives us

$$\lambda_{1,j,j} = Q = \left(\frac{q^k-1}{q-1}\right)\left(\frac{q^k-q}{q-1}\right).$$

For $j < j'$, Eq. (2.4.3) gives

$$\lambda_{1,j,j'} = \widehat{Q} = \left(\frac{q^k - 1}{q - 1}\right)^2.$$

Now the statement for λ_1 follows from the fact that there are m distinct orbits and $\binom{m}{2}$ pairs thereof.

It remains to compute λ_0. For each of the m orbits we have $\lambda_{0,j,j} = (q^n - 1)/(q - 1) - 1 - \lambda_{1,j,j}$; see also Theorem 21. On the other hand, the intersection distribution in Definition 36 takes $(q^n - 1)/(q - 1)$ intersections between distinct orbits into account. Hence for each of the $\binom{m}{2}$ pairs of distinct orbits we have $\lambda_{0,j,j'} = (q^n - 1)/(q - 1) - \lambda_{1,j,j'}$. Now the result for λ_0 follows. □

A few remarks about the number of such combinable subspaces m are in order. When each U_i is a Sidon space, every two dimensional subspace in $\mathcal{G}_q(2, n)$ is contained in at most one subspace in the combined code. It follows that the maximal number of combinable orbits is attained when every two dimensional subspace is contained in exactly one subspace in the combined code. Such a collection of subspaces is known as a q-Steiner system and denoted $\mathcal{S}_q[2, k, n]$. In this case, we have

$$m_{max} = \frac{\begin{bmatrix} n \\ 2 \end{bmatrix}}{\begin{bmatrix} k \\ 2 \end{bmatrix}} \cdot \frac{q - 1}{q^n - 1} = \frac{(q^{n-1} - 1)(q - 1)}{(q^k - 1)(q^{k-1} - 1)}.$$

Very little is known about the existence of such systems. When $q = 2, k = 3, n = 13$, a variety of non-isomorphic $\mathcal{S}_2[2, 3, 13]$ Steiner systems of the form of a code as in Theorem 42 are known to exist [2]. On the other hand, an exhaustive search for the smaller parameter set $q = 2, k = 3, n = 7$ shows that no $\mathcal{S}_2[2, 3, 7]$ Steiner system which is the union of cyclic orbits exist [28]. In this case every 3-dimensional subspace is a Sidon space and there are 93 orbits of these subspaces, but while there are some pairs of combinable subspaces, no triple of subspaces are combinable.

In general the maximum attainable value of m for other parameter sets is unknown. As we mentioned earlier, the existence of the constructions given in [26] show that the maximum attainable m is greater than one when either $q > 2$ and $k \mid n$ or $q = 2$ and $k \mid n$ and $n \geq 3k$.

2.5 Conclusion and Open Problems

In this chapter we investigated the intersection distribution, and thus the weight distribution, for cyclic orbit codes that have maximum possible length and distance at least $2k-4$. For distance $2k-2$ the intersection distribution can be fully described and in fact depends only on q, n, k, while for distance $2k-4$ the additional parameter $f = f(U)$ plays a role. Many cases remain to be investigated. We conclude with some specific open problems and directions for future work.

(1) Throughout our work, the parameter $f = |\mathcal{F}(U)|$ plays a prominent role. Can we provide more information about f for more general subspaces? For instance, can we find a lower bound on f that guarantees distance $2k-4$? The question of how many fractions a subspace has may also be related to questions raised in [26] about the size of the "product" space $U^2 = \langle \sum_{i=1}^{n} u_i v_i \mid u_i, v_i \in U \rangle$.
(2) Can we determine for given parameters (q, n, k) the range for r (or λ_2) in Theorem 23? Tables 2.1 and 2.2 in Section 2.3 show that the upper bound for λ_2 given in Corollary 24 is in most cases very poor.
(3) Our main tool for proving Theorem 23 was a detailed study of intersections $U \cap \alpha U$ of maximal dimension $\ell = 2$. However, to find the intersection distribution for $\ell \geq 3$, studying intersections of maximal dimension is insufficient. What can we say about intersections that are not of maximal dimension?
(4) Can Theorem 23 be generalized to cyclic subspace codes with multiple orbits and distance $2k-4$?

Chapter 3 Automorphisms of Cyclic Orbit Codes

The material of this chapter can be found also in [10].

3.1 Orbit Codes and Linear Isometries

In this section we turn to more general orbit subspace codes. The orbit subspace codes defined next are again *constant-dimension codes*, that is, they are contained in some $\mathcal{G}_q(k,n)$.

Definition 43. Let $G \leq \mathrm{GL}_n(q)$ be a subgroup and let $\mathcal{U} \in \mathcal{G}_q(k,n)$. Then the G-orbit of $\mathcal{U}$, defined as $\mathrm{Orb}_G(\mathcal{U}) = \{\phi(\mathcal{U}) \mid \phi \in G\}$, is called an *orbit code*. For a Singer subgroup S, the orbit $\mathrm{Orb}_S(\mathcal{U})$ is called a *cyclic orbit code*.

Two classes of orbit codes will be in the focus of this chapter: orbits under the Singer subgroup $\mathbb{F}_{q^n}^*$ and orbits under the normalizer of $\mathbb{F}_{q^n}^*$. They take the following explicit form. Let ω be a primitive element of $\mathbb{F}_{q^n}$. Furthermore, for $\mathcal{U} \in \mathcal{G}_q(k,n)$ define $\mathcal{U}^{[i]} := \{u^{[i]} \mid u \in \mathcal{U}\}$, where we use the standard notation $[i] := q^i$. Consider the Singer subgroup $\mathbb{F}_{q^n}^*$ and its normalizer $N := N_{\mathrm{GL}_n(q)}(\mathbb{F}_{q^n}^*) \cong \mathrm{Gal}(\mathbb{F}_{q^n} | \mathbb{F}_q) \rtimes \mathbb{F}_{q^n}^*$. Then

$$\mathrm{Orb}_{\mathbb{F}_{q^n}^*}(\mathcal{U}) = \{\omega^i \mathcal{U} \mid i = 0, \ldots, q^n - 2\} \text{ and } \mathrm{Orb}_N(\mathcal{U}) = \bigcup_{i=0}^{n-1} \mathrm{Orb}_{\mathbb{F}_{q^n}^*}(\mathcal{U}^{[i]}). \quad (3.1.1)$$

For later reference we recall the following simple fact about the sizes of these orbits.

Remark 44 ([12, Cor. 3.13])**.** Let $\mathcal{U} \in \mathcal{G}_q(k,n)$. Suppose $\mathbb{F}_{q^t}$ is the largest subfield of $\mathbb{F}_{q^n}$ such that $\mathcal{U}$ is closed under multiplication by scalars from $\mathbb{F}_{q^t}$ (i.e., $\mathcal{U}$ is an $\mathbb{F}_{q^t}$-vector space with respect to the ordinary multiplication in $\mathbb{F}_{q^n}$). Then

$$|\mathrm{Orb}_{\mathbb{F}_{q^n}^*}(\mathcal{U})| = \frac{q^n - 1}{q^t - 1}.$$

As a consequence, $|\mathrm{Orb}_N(\mathcal{U})| \leq n(q^n-1)/(q^t-1)$ for the normalizer $N := N_{\mathrm{GL}_n(q)}(\mathbb{F}_{q^n}^*)$.

Let us return to general G-orbits. In matrix notation, they take the following form. This is the setting in which they have been studied in [30].

Remark 45. Let $\mathcal{U} \in \mathcal{G}_q(k,n)$ and $G \leq \mathrm{GL}_n(q)$. Define $\tilde{G} := \{\Phi \circ \phi \circ \Phi^{-1} \mid \phi \in G\}$ and $\tilde{\mathcal{U}} = \Phi(\mathcal{U})$, where Φ is the isomorphism from (1.2.5). Then $\tilde{G} \leq \mathrm{GL}_n(\mathbb{F}_q)$ and $\mathcal{U} \subseteq \mathbb{F}_q^n$, and (1.2.7) shows that

$$\Phi(\mathrm{Orb}_G(\mathcal{U})) = \mathrm{Orb}_{\tilde{G}}(\tilde{\mathcal{U}}) := \{\tilde{\mathcal{U}} A \mid A \in \tilde{G}\}.$$

In this chapter we want to study linear isometries between orbit codes.

Definition 46. An *isometry* on $\mathrm{PG}(n-1,q)$ is a distance-preserving map $\varphi : \mathrm{PG}(n-1,q) \to \mathrm{PG}(n-1,q)$, thus, $\mathrm{d}(\mathcal{U},\mathcal{V}) = \mathrm{d}(\varphi(\mathcal{U}),\varphi(\mathcal{V}))$ for all $\mathcal{U},\mathcal{V} \in \mathrm{PG}(n-1,q)$.

It is clear that an isometry is bijective. In [29, 2.3–2.8] it has been shown that the dimension-preserving isometries are precisely the elements of the projective general semi-linear group $\mathrm{GL}_n(q)/Z \rtimes \mathrm{Aut}(\mathbb{F}_q)$, where Z is the center of $\mathrm{GL}_n(q)$, that is, $Z = \{m_a \mid a \in \mathbb{F}_q^*\}$ with m_a as in (1.2.3). Thanks to the Fundamental Theorem of Projective Geometry, these are exactly the automorphisms (i.e., incidence-preserving bijections) of $\mathrm{PG}(n-1,q)$. We will only consider linear isometries, that is, maps in the projective linear group $\mathrm{PGL}_n(q) = \mathrm{GL}_n(q)/Z$. Note that a map $\phi \in \mathrm{GL}_n(q)$ is in Z if and only if it fixes every $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$, which is why we may factor out Z. For ease of notation, we will simply consider linear isometries in $\mathrm{GL}_n(q)$. This will have no impact on our considerations (one can just factor out Z in all groups occurring below).

Definition 47. Let $G \leq \mathrm{GL}_n(q)$ and $\mathcal{U}_1, \mathcal{U}_2 \in \mathcal{G}_q(k,n)$. Consider the G-orbits $\mathcal{C}_i = \mathrm{Orb}_G(\mathcal{U}_i)$ for $i = 1,2$. Then $\mathcal{C}_1$ and $\mathcal{C}_2$ are called *(linearly) isometric* if there exists an isomorphism $\psi \in \mathrm{GL}_n(q)$ such that $\psi(\mathcal{C}_1) = \mathcal{C}_2$, where $\psi(\mathcal{C}_1) := \{\psi(\mathcal{V}) \mid \mathcal{V} \in \mathcal{C}_1\}$. In this case ψ is called a *(linear) isometry* between $\mathcal{C}_1$ and $\mathcal{C}_2$. In the special case, where $G = S$ is a Singer subgroup and $\psi(\mathcal{C}_1) = \mathcal{C}_2$ for some $\psi \in N_{\mathrm{GL}_n(q)}(S)$, we call the cyclic orbit codes $\mathrm{Orb}_S(\mathcal{U}_1)$ and $\mathrm{Orb}_S(\mathcal{U}_2)$ *Frobenius-isometric* and ψ a *Frobenius-isometry*.

The terminology Frobenius-isometry is motivated by the fact that, thanks to Theorem 11(a), $N_{\mathrm{GL}_n(q)}(S) \cong \mathrm{Gal}(\mathbb{F}_{q^n} \,|\, \mathbb{F}_q) \rtimes S$.

Later in Section 3.4 we will see that – just like for block codes with the Hamming metric – not every weight-preserving bijection between cyclic orbit codes is an isometry. Hence not every such map extends to an isometry on $\mathrm{PG}(n-1,q)$.

The following is easy to see.

Theorem 48 (see also [30, Thm. 10])**.** Let $G \leq \mathrm{GL}_n(q)$, $\psi \in \mathrm{GL}_n(q)$, and $\mathcal{U} \in \mathcal{G}_q(k,n)$.

(a) Set $G' = \psi G \psi^{-1}$ and $\mathcal{U}' = \psi(\mathcal{U})$. Then the orbit codes $\mathcal{C} = \mathrm{Orb}_G(\mathcal{U})$ and $\mathcal{C}' = \mathrm{Orb}_{G'}(\mathcal{U}')$ are linearly isometric with $\mathcal{C}' = \psi(\mathcal{C})$.

(b) Let $\mathcal{C} = \mathrm{Orb}_G(\mathcal{U})$ and $\mathcal{C}' = \psi(\mathcal{C})$. Then $\mathcal{C}' = \mathrm{Orb}_{\psi G \psi^{-1}}(\mathcal{U}')$ with $\mathcal{U}' = \psi(\mathcal{U})$. As a consequence, if $\psi \in N_{\mathrm{GL}_n}(G)$, then $\mathcal{C}$ and $\mathcal{C}'$ are isometric G-orbit codes.

In order to study isometries between cyclic orbit codes, we need to understand their automorphism groups. This is the subject of the next section. For these considerations it will suffice to restrict to orbit codes generated by subspaces $\mathcal{U} \in \mathcal{G}_q(k,n)$, where $k \leq n/2$. In order to see this, we need to briefly introduce the dual code. Let ω be a primitive element of $\mathbb{F}_{q^n}$ and choose the symmetric, non-degenerate, $\mathbb{F}_q$-bilinear form $\langle \cdot \,|\, \cdot \rangle$ on $\mathbb{F}_{q^n}$ defined via $\langle \omega^i \,|\, \omega^j \rangle = \delta_{i,j}$ for all $i,j = 0,\ldots,n-1$ (this is simply the standard dot product on $\mathbb{F}_q^n$ under the isomorphism in (1.2.5)). Define the dual of a subspace $\mathcal{W} \leq \mathbb{F}_{q^n}$ in the usual way as $\mathcal{W}^\perp = \{v \in \mathbb{F}_{q^n} \mid \langle v \,|\, w \rangle = 0 \text{ for all } w \in \mathcal{W}\}$. Clearly, $\dim \mathcal{W}^\perp = n - \dim \mathcal{W}$. The *dual* of a subspace code $\mathcal{C} \subseteq \mathbb{F}_{q^n}$ is simply defined as $\mathcal{C}^\perp := \{\mathcal{W}^\perp \mid \mathcal{W} \in \mathcal{C}\}$. We can now describe the dual of an orbit code. For an

$\mathbb{F}_q$-linear map $\phi : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$ denote by $\phi^\dagger$ its adjoint map, that is, the unique linear map satisfying $\langle \phi(x) \,|\, y \rangle = \langle x \,|\, \phi^\dagger(y) \rangle$ for all $x, y \in \mathbb{F}_{q^n}$. Clearly $\phi^\dagger \in \mathrm{GL}_n(q)$ for any $\phi \in \mathrm{GL}_n(q)$.

Remark 49. Suppose $\mathcal{C} = \mathrm{Orb}_G(\mathcal{U})$ for some subgroup $G \leq \mathrm{GL}_n(q)$. Then $\mathcal{C}^\perp = \mathrm{Orb}_{G^\dagger}(\mathcal{U}^\perp)$, where $G^\dagger = \{\phi^\dagger \mid \phi \in G\}$, which is clearly a subgroup of $\mathrm{GL}_n(q)$. This follows immediately from $\phi(\mathcal{U})^\perp = (\phi^\dagger)^{-1}(\mathcal{U}^\perp)$. We call $G^\dagger$ the *adjoint group of* G.

In the setting of Remark 45, where subgroups of the matrix group $\mathrm{GL}_n(\mathbb{F}_q)$ act on subspaces in $\mathbb{F}_q^n$, this fact also appears in [30, Thm. 18].

The following surprising result tells us that the adjoint groups of all groups of interest in this dissertation are conjugate to the group itself, and even more, we may choose the same conjugation matrix for all these groups.

Theorem 50. There exists a map $\rho \in \mathrm{GL}_n(q)$ such that

$$\rho^{-1} G^\dagger \rho = G \quad \text{for all } G \in \{\mathbb{F}_{q^n}^*, \mathrm{Gal}(\mathbb{F}_{q^n} \,|\, \mathbb{F}_q)\} \cup \{\mathrm{GL}_{n/s}(q^s) \mid s \text{ divisor of } n\}.$$

The proof, which is not needed for the rest of this dissertation, can be found in our paper [10]. Returning to our orbit codes, Theorem 50 along with Remark 49 tells us that the dual of a G-orbit, where G is any of the groups above, is again an orbit of the same type, but with respect to an isomorphic field structure; see the paragraph following Lemma 10. The isomorphic field structure does not depend on the group.

All of this tells us that it suffices to study isometries (and automorphisms) for orbit codes generated by subspaces of dimension at most $n/2$. Hence from now on we only consider subspaces $\mathcal{U} \in \mathcal{G}_q(k, n)$, where $k \leq n/2$.

3.2 Automorphism Groups of Singer Orbits

In this section we will derive information about the automorphism groups of cyclic orbit codes. This will be sufficient to discuss isometries between cyclic orbit codes later in the chapter. In accordance with earlier notation we will consider automorphisms in $\mathrm{GL}_n(q)$ rather than $\mathrm{PGL}_n(q) = \mathrm{GL}_n(q)/Z$.

Definition 51. Let $\mathcal{C} \subseteq \mathrm{PG}(n-1, q)$ be a subspace code. The *automorphism group* of $\mathcal{C}$ is defined as the group of linear isometries that fix $\mathcal{C}$, that is, $\mathrm{Aut}(\mathcal{C}) := \{\psi \in \mathrm{GL}_n(q) \mid \psi(\mathcal{C}) = \mathcal{C}\}$. Any subgroup of $\mathrm{Aut}(\mathcal{C})$ is called *a group of automorphisms* of $\mathcal{C}$.

Clearly, for any $G \leq \mathrm{GL}_n(q)$ and any orbit code $\mathcal{C} = \mathrm{Orb}_G(\mathcal{U})$, the group G is a group of automorphisms of $\mathcal{C}$. Furthermore, if $H \leq \mathrm{GL}_n(q)$ then

$$H \leq \mathrm{Aut}(\mathrm{Orb}_G(\mathcal{U})) \iff \mathrm{Orb}_H(\mathcal{U}) \subseteq \mathrm{Orb}_G(\mathcal{U}). \tag{3.2.1}$$

We will now focus on the case where $\mathcal{C}$ is a cyclic orbit code, that is, $\mathcal{C} = \mathrm{Orb}_S(\mathcal{U})$ for some subspace $\mathcal{U} \leq \mathbb{F}_{q^n}$ and a Singer subgroup $S \leq \mathrm{GL}_n(q)$. Thanks to Lemma 10 and Theorem 48(a) it suffices to study the case where $S = \mathbb{F}_{q^n}^*$. The following result is immediate with Theorem 11(c).

Proposition 52. Let $\mathcal{C} = \mathrm{Orb}_{\mathbb{F}_{q^n}^*}(\mathcal{U})$ be a cyclic orbit code. Then there exists a divisor s of n such that $\mathrm{GL}_{n/s}(q^s) \trianglelefteq \mathrm{Aut}(\mathcal{C}) \leq N_{\mathrm{GL}_n(q)}(\mathrm{GL}_{n/s}(q^s))$.

The following notion will be convenient throughout.

Definition 53. A subspace $\mathcal{U} \subseteq \mathbb{F}_{q^n}$ is called *generic* if $\mathcal{U}$ is not contained in a proper subfield of $\mathbb{F}_{q^n}$.

The next theorem is the main result of this section. It shows that for any subspace $\mathcal{U}$, the parameter s from Proposition 52 is the smallest divisor of n such that $\mathcal{U} \subseteq \mathbb{F}_{q^s}$. As a consequence, the automorphism group of $\mathcal{C}$ contains linear isometries that are outside the normalizer of $\mathbb{F}_{q^n}^*$ if and only if $\mathcal{U}$ is not generic.

Since any cyclic orbit code contains a subspace $\mathcal{U}$ such that $1 \in \mathcal{U}$, we may assume without loss of generality that 1 is contained in the generating subspace. If, in addition, $\dim(\mathcal{U}) = 1$, then $\mathcal{U} = \mathbb{F}_q$ and $\mathrm{Orb}_{\mathbb{F}_{q^n}^*}(\mathcal{U}) = \mathrm{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U}) = \mathcal{G}_q(1,n)$ for all divisors s of n. Hence from now on we assume $k \geq 2$ and thus $n \geq 4$.

Theorem 54. Let $S = \mathbb{F}_{q^n}^*$ and let $\mathcal{U} \in \mathcal{G}_q(k,n)$ be such that $1 \in \mathcal{U}$. Let s be a divisor of n. Then

$$\mathcal{U} \subseteq \mathbb{F}_{q^s} \iff \mathrm{GL}_{n/s}(q^s) \leq \mathrm{Aut}(\mathrm{Orb}_S(\mathcal{U})). \tag{3.2.2}$$

Moreover, if $\mathbb{F}_{q^s}$ is the smallest subfield containing $\mathcal{U}$, then $\mathrm{GL}_{n/s}(q^s)$ is normal in $\mathrm{Aut}(\mathrm{Orb}_S(\mathcal{U}))$ and thus $\mathrm{Aut}(\mathrm{Orb}_S(\mathcal{U})) \leq N_{\mathrm{GL}_n(q)}(\mathrm{GL}_{n/s}(q^s))$. As a consequence,

$$\mathcal{U} \text{ is generic } \iff \mathrm{Aut}(\mathrm{Orb}_S(\mathcal{U})) \leq N_{\mathrm{GL}_n(q)}(S).$$

The proof is postponed to the end of this section. We first need some technical results. We start with a lower bound on the size of the orbits $\mathrm{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U})$ for a given divisor s of n. As we will see, this size depends on the dimension of the $\mathbb{F}_{q^s}$-subspace of $\mathbb{F}_{q^n}$ generated by $\mathcal{U}$.

Definition 55. For any $\mathbb{F}_q$-subspace $\mathcal{V}$ of $\mathbb{F}_{q^n}$ we set $\widehat{\mathcal{V}} := \mathrm{span}_{\mathbb{F}_{q^s}}(\mathcal{V})$ and $\delta_s(\mathcal{V}) := \dim_{\mathbb{F}_{q^s}}(\widehat{\mathcal{V}})$. Note that $\delta_s(\mathcal{V})s = \dim_{\mathbb{F}_q}(\widehat{\mathcal{V}}) \leq n$.

Clearly $\delta_s(\,\cdot\,)$ is invariant under the actions of the groups $\mathbb{F}_{q^n}^*$, $\mathrm{Gal}(\mathbb{F}_{q^n} \,|\, \mathbb{F}_q)$, and $\mathrm{GL}_{n/s}(q^s)$.

Proposition 56. Let $\mathcal{U} \in \mathcal{G}_q(k,n)$ be such that $1 \in \mathcal{U}$, and let s be a divisor of n. Set $\delta_s(\mathcal{U}) = r$. Then $1 \leq r \leq k$ and

$$|\,\mathrm{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U})| \geq \frac{q^{\binom{r}{2}(s-1)}}{\begin{bmatrix} k \\ r \end{bmatrix}_q} \prod_{i=0}^{r-1} \frac{q^{n-is}-1}{q^{r-i}-1}$$

with equality if $r = k$.

Note that $(r-1)s < rs = \dim_{\mathbb{F}_q}(\widehat{\mathcal{U}}) \leq n$. This shows that the right hand side is not 0.

Proof. First let $s = 1$. Then $\mathbb{F}_{q^s} = \mathbb{F}_q$ and $\widehat{\mathcal{U}} = \mathcal{U}$, and thus $r = k$. In this case, $\mathrm{Orb}_{\mathrm{GL}_n(q)}(\mathcal{U})$ consists of all k-dimensional subspaces of $\mathbb{F}_{q^n}$, and hence its size is $\begin{bmatrix} n \\ k \end{bmatrix}_q$, which is the right hand side above. From now on let $s > 1$.
Case 1) Let $r = k$. Let $B = (u_1, \ldots, u_k)$ be an ordered $\mathbb{F}_q$-basis of $\mathcal{U}$. Thanks to $\delta_s(\mathcal{U}) = k$, the vectors $u_1, \ldots, u_k$ are also $\mathbb{F}_{q^s}$-linearly independent. Under the action of $\mathrm{GL}_{n/s}(q^s)$ the orbit of the basis B consists of all k-tuples of $\mathbb{F}_{q^s}$-linearly independent vectors in $\mathbb{F}_{q^n}$. This implies that $|\operatorname{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U})|$ is given by the number of k-tuples of $\mathbb{F}_{q^s}$-linearly independent vectors in $\mathbb{F}_{q^n}$ divided by the number of ordered $\mathbb{F}_q$-bases for a k-dimensional $\mathbb{F}_q$-subspace. We conclude

$$|\operatorname{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U})| = \frac{\prod_{i=0}^{k-1}(q^n - q^{is})}{\prod_{i=0}^{k-1}(q^k - q^i)} = q^{\binom{k}{2}(s-1)} \prod_{i=0}^{k-1} \frac{q^{n-is}-1}{q^{k-i}-1}.$$

Case 2) Let now $1 \leq r < k$. There exists a subspace $\mathcal{V}$ of $\mathcal{U}$ such that $\dim_{\mathbb{F}_q}(\mathcal{V}) = r$ and $\widehat{\mathcal{V}} = \widehat{\mathcal{U}}$. Clearly, each subspace $\psi(\mathcal{U}) \in \mathrm{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U})$ contains exactly $K := \begin{bmatrix} k \\ r \end{bmatrix}_q$ subspaces of $\mathbb{F}_q$-dimension r, and thus in particular at most K subspaces of the form $\psi'(\mathcal{V})$ for some $\psi' \in \mathrm{GL}_{n/s}(q^s)$. Since each $\psi'(\mathcal{V}) \in \mathrm{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{V})$ is contained in at least one $\psi(\mathcal{U}) \in \mathrm{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U})$, we obtain

$$|\operatorname{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U})| \geq \frac{1}{K} |\operatorname{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{V})|.$$

Since $\mathcal{V}$ satisfies $\delta_1(\mathcal{V}) = \delta_s(\mathcal{V})$,we may apply Case 1) to $\mathcal{V}$ to obtain the desired result. □

In order to compare the sizes of the $\mathrm{GL}_{n/s}(q^s)$-orbits and the Singer orbits, we need some technical lemmas.

Lemma 57. Let $2 \leq r \leq n/2$ and $1 \leq s < n$ be such that $sr \leq n$. Then

$$\prod_{i=0}^{r-1} \frac{q^{n-is}-1}{q^{r-i}-1} > q^{r(n-r)-(s-1)\binom{r}{2}}.$$

Proof. Note first that by the assumptions

$$n - is - r + i \geq 1 \text{ for all } i = 0, \ldots, r-1. \tag{3.2.3}$$

Indeed, $n-is-r+i = n-r-i(s-1) \geq n-r-(r-1)(s-1) = n-rs+s-1$. If $s \geq 2$ the latter is clearly at least 1, while for $s = 1$ we have $n-rs+s-1 = n-r \geq n/2 \geq 1$, too. Using the inequality

$$\frac{q^a - 1}{q^b - 1} > q^{a-b} \quad \text{whenever } a > b, \tag{3.2.4}$$

we obtain from (3.2.3) the inequality $\prod_{i=0}^{r-1} \frac{q^{n-is}-1}{q^{r-i}-1} > q^M$, where $M = \sum_{i=0}^{r-1}(n - is - r + i) = r(n-r) - (s-1)\binom{r}{2}$, as desired. □

The next lemma gives two lower bounds for the right-hand side of Proposition 56, one with a factor n on the right hand side and one without such a factor. The version with factor n will be needed in Section 3.3 when we study orbits under the normalizer of the Singer subgroup.

Lemma 58. Let $2 \leq r \leq k \leq n/2$ and $1 \leq s < n$ such that $rs \leq n$.
(a) Let $r \geq 3$. Then

$$q^{\binom{r}{2}(s-1)} \prod_{i=0}^{r-1} \frac{q^{n-is}-1}{q^{r-i}-1} > n \begin{bmatrix} k \\ r \end{bmatrix}_q \frac{q^n-1}{q-1}. \tag{3.2.5}$$

(b) If $r = 2$, then $q^{\binom{r}{2}(s-1)} \prod_{i=0}^{r-1} \frac{q^{n-is}-1}{q^{r-i}-1} > \begin{bmatrix} k \\ r \end{bmatrix}_q \frac{q^n-1}{q-1}$.

Proof. (a) Let $r \geq 3$, thus $n \geq 6$. Setting $c = q/(q-1)$ we have $(q^n-1)/(q-1) < cq^{n-1}$. Furthermore, $r \geq 3$ implies

$$r(k-r) + n - 1 \leq r(n-r) - (n/2+1),$$

because $r(k-r) + n - 1 \leq r(n/2-r) + n - 1 = r(n-r) - rn/2 + n - 1 \leq r(n-r) - 3n/2 + n - 1$. Using the above inequalities along with $\begin{bmatrix} k \\ r \end{bmatrix}_q < 4q^{r(k-r)}$ (see [22, Lem. 4]) and Lemma 57 we compute

$$n \begin{bmatrix} k \\ r \end{bmatrix}_q \frac{q^n-1}{q-1} < 4ncq^{r(k-r)+n-1} < \frac{4nc}{q^{n/2+1}} q^{\binom{r}{2}(s-1)} \prod_{i=0}^{r-1} \frac{q^{n-is}-1}{q^{r-i}-1}.$$

Finally, one easily checks that $\frac{4nc}{q^{n/2+1}} = \frac{4n}{q^{n/2}(q-1)} \leq 1$ for $q \geq 3$ and $n \geq 4$ as well as $q = 2$ and $n \geq 11$. For the remaining cases ($q = 2$ and $n = 6, \ldots, 10$) inequality (3.2.5) can be verified directly.
(b) Let $r = 2$. In this case the desired inequality is equivalent to

$$Q := (q-1)(q^n - q^s) - (q^k - 1)(q^k - q) > 0.$$

Since Q decreases with increasing s or k, we may lower bound Q by using $s = k = n/2$ (ignoring that this may not be an integer). This leads to

$$\begin{aligned} Q &\geq (q-1)(q^n - q^{n/2}) - (q^{n/2}-1)(q^{n/2}-q) = \big((q-1)q^{n/2} - (q^{n/2}-q)\big)(q^{n/2}-1) \\ &= \big((q-2)q^{n/2} + q\big)(q^{n/2}-1) > 0, \end{aligned}$$

as desired. □

Lemma 59. Let s, $t \in \mathbb{N}$ such that $s \,|\, t \,|\, n$ and $s \neq t$. Then

$$\left|\mathrm{GL}_{n/s}(q^s)\right| > \left|N_{\mathrm{GL}_n(q)}(\mathrm{GL}_{n/t}(q^t))\right|.$$

Proof. Set $\hat{q} = q^s$, $\hat{n} = n/s$ and let $sa = t$. Then $\left|\mathrm{GL}_{n/s}(q^s)\right| = \prod_{i=0}^{\hat{n}-1}(\hat{q}^{\hat{n}} - \hat{q}^i)$ and from Theorem 11(d) we know that

$$\left|N_{\mathrm{GL}_n(q)}(\mathrm{GL}_{n/t}(q^t))\right| = t \prod_{i=0}^{\hat{n}/a-1} ((\hat{q}^a)^{\hat{n}/a} - (\hat{q}^a)^i) \leq n \prod_{i=0}^{\hat{n}/a-1} (\hat{q}^{\hat{n}} - \hat{q}^{ai}).$$

Clearly, all factors in the product on the right hand side appear in $|\mathrm{GL}_{n/s}(q^s)|$. Furthermore, since $a > 1$, the factor $\hat{q}^{\hat{n}} - \hat{q} = q^n - q^s$ of $|\mathrm{GL}_{n/s}(q^s)|$ does not appear in $|N_{\mathrm{GL}_n(q)}(\mathrm{GL}_{n/t}(q^t))|$. Hence the desired inequality follows if we can show that $q^n - q^s > n$. Since $s \neq n$ and s is a divisor of n, we have $q^n - q^s - n \geq q^n - q^{n/2} - n$. One easily verifies that the function $f(x) = q^x - q^{x/2} - x$ is indeed positive on $[4, \infty)$. This concludes the proof. □

Now we are ready to prove our main result.

Proof of Theorem 54. Let S, s, $\mathcal{U}$ be as in the theorem. Set $\widehat{\mathcal{U}} = \mathrm{span}_{\mathbb{F}_{q^s}}(\mathcal{U})$ as in Definition 55. Then $1 \leq \delta_s(\mathcal{U}) \leq \dim_{\mathbb{F}_q}(\mathcal{U})$ and

$$\mathcal{U} \subseteq \mathbb{F}_{q^s} \iff 1 = \delta_s(\mathcal{U}) \iff \widehat{\mathcal{U}} = \mathbb{F}_{q^s}, \tag{3.2.6}$$

where the last equivalence follows from the fact that $1 \in \mathcal{U}$. Since $|S| = q^n - 1$ and $\mathbb{F}_q^*$ stabilizes $\mathcal{U}$, we have $|\operatorname{Orb}_S(\mathcal{U})| \leq (q^n - 1)/(q - 1)$ by the orbit-stabilizer theorem (see also Remark 44). Moreover, since $S \leq \mathrm{GL}_{n/s}(q^s)$, we have

$$\operatorname{Orb}_S(\mathcal{U}) \subseteq \operatorname{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U}) \text{ with equality iff } \mathrm{GL}_{n/s}(q^s) \leq \mathrm{Aut}(\operatorname{Orb}_S(\mathcal{U})). \tag{3.2.7}$$

We now prove the equivalence (3.2.2).

"$\Longrightarrow$" Let $\mathcal{U} \subseteq \mathbb{F}_{q^s}$, thus $\widehat{\mathcal{U}} = \mathbb{F}_{q^s}$. Since $1 \in \mathcal{U}$ we obtain $\psi(\mathcal{U}) = \{u \cdot \psi(1) \mid u \in \mathcal{U}\}$ for every $\psi \in \mathrm{GL}_{n/s}(q^s)$. Hence $\psi(\mathcal{U})$ is the cyclic shift $\psi(1)\mathcal{U}$ and thus contained in $\operatorname{Orb}_S(U)$. This shows $\operatorname{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U}) \subseteq \operatorname{Orb}_S(\mathcal{U})$ and (3.2.7) implies the desired result.

"$\Longleftarrow$" Suppose $\mathcal{U} \not\subseteq \mathbb{F}_{q^s}$. Then $r := \delta_s(\mathcal{U}) \geq 2$ by (3.2.6). Proposition 56 and Lemma 58 imply

$$\left|\operatorname{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U})\right| \geq \frac{q^{\binom{r}{2}(s-1)}}{\begin{bmatrix} k \\ r \end{bmatrix}_q} \prod_{i=0}^{r-1} \frac{q^{n-is} - 1}{q^{r-i} - 1} > \frac{q^n - 1}{q - 1} \geq |\operatorname{Orb}_S(\mathcal{U})|.$$

(3.2.7) implies $\mathrm{GL}_{n/s}(q^s) \not\leq \mathrm{Aut}(\operatorname{Orb}_S(\mathcal{U}))$.

We now turn to the remaining statements of Theorem 54. Let $\mathbb{F}_{q^s}$ be the smallest subfield containing $\mathcal{U}$. We want to show that $\mathrm{GL}_{n/s}(q^s)$ is normal in $\mathrm{Aut}(\operatorname{Orb}_S(\mathcal{U}))$. To this end set $\mathcal{T} = \left\{t \in \mathbb{N} \,\middle|\, s \,|\, t \,|\, n\right\}$. Clearly $\mathrm{GL}_{n/t}(q^t) \leq \mathrm{GL}_{n/s}(q^s)$ for all $t \in \mathcal{T}$. From (3.2.2) we conclude that for any $t \in \mathbb{N}$

$$\mathrm{GL}_{n/t}(q^t) \leq \mathrm{Aut}(\operatorname{Orb}_S(\mathcal{U})) \iff t \in \mathcal{T}.$$

Furthermore, thanks to Theorem 11(c) one of the subgroups $\mathrm{GL}_{n/t}(q^t)$, $t \in \mathcal{T}$, is normal in $\mathrm{Aut}(\mathrm{Orb}_S(\mathcal{U}))$. Suppose $\mathrm{GL}_{n/t}(q^t)$ is normal in $\mathrm{Aut}(\mathrm{Orb}_S(\mathcal{U}))$ for some $t \in \mathcal{T} \setminus \{s\}$. Then $\mathrm{Aut}(\mathrm{Orb}_S(\mathcal{U})) \leq N_{\mathrm{GL}_n(q)}(\mathrm{GL}_{n/t}(q^t))$. Now, Lemma 59 along with $\mathrm{GL}_{n/s}(q^s) \leq \mathrm{Aut}(\mathrm{Orb}_S(\mathcal{U}))$ leads to a contradiction. Thus $\mathrm{GL}_{n/s}(q^s)$ is the only extension-field subgroup that is normal in $\mathrm{Aut}(\mathrm{Orb}_S(\mathcal{U}))$. The rest of the theorem follows. □

3.3 Automorphism Groups of Orbits under the Singer Normalizer

The considerations of the previous sections allow us to also describe the automorphism group of orbits under the normalizer of the Singer subgroup in most cases. Recall the notation in (3.1.1). The following theorem is analogous to Theorem 54, but needs the assumption $\delta_s(\mathcal{U}) \neq 2$. We will deal with the case $\delta_s(\mathcal{U}) = 2$ afterwards.

Throughout this section, let $N := N_{\mathrm{GL}_n(q)}(\mathbb{F}_{q^n}^*)$, i. e., N is the normalizer of $\mathbb{F}_{q^n}^*$. Recall also that we assume $2 \leq k \leq n/2$.

Theorem 60. Let s be a divisor of n and $\mathcal{U} \in \mathcal{G}_q(k,n)$ be such that $1 \in \mathcal{U}$ and such that $\delta_s(\mathcal{U}) \neq 2$. Then

$$\mathcal{U} \subseteq \mathbb{F}_{q^s} \iff \mathrm{GL}_{n/s}(q^s) \leq \mathrm{Aut}(\mathrm{Orb}_N(\mathcal{U})). \tag{3.3.1}$$

Moreover, if $\mathbb{F}_{q^s}$ is the smallest subfield containing $\mathcal{U}$ and $\delta_t(\mathcal{U}) \neq 2$ for all divisors t of n, then $\mathrm{GL}_{n/s}(q^s)$ is normal in $\mathrm{Aut}(\mathrm{Orb}_N(\mathcal{U}))$ and thus $\mathrm{Aut}(\mathrm{Orb}_N(\mathcal{U})) \leq N_{\mathrm{GL}_n(q)}(\mathrm{GL}_{n/s}(q^s))$. As a consequence:
(a) If $\mathcal{U}$ is generic and $\delta_t(\mathcal{U}) \neq 2$ for all divisors t of n, then $\mathrm{Aut}(\mathrm{Orb}_N(\mathcal{U})) = N$;
(b) If $\mathrm{Aut}(\mathrm{Orb}_N(\mathcal{U})) = N$, then $\mathcal{U}$ is generic.

Note that the left hand side of (3.3.1) means that $\delta_s(\mathcal{U}) = 1$. Hence the excluded case $\delta_s(\mathcal{U}) = 2$ may be regarded as a transitional case, and we will see below that in that case either is possible: $\mathrm{GL}_{n/s}(q^s) \leq \mathrm{Aut}(\mathrm{Orb}_N(\mathcal{U}))$ or $\mathrm{GL}_{n/s}(q^s) \not\leq \mathrm{Aut}(\mathrm{Orb}_N(\mathcal{U}))$.

Proof. For "$\Longrightarrow$" of (3.3.1) recall that $\mathrm{Orb}_N(\mathcal{U}) = \bigcup_{i=0}^{n-1} \mathrm{Orb}_{\mathbb{F}_{q^n}^*}(\mathcal{U}^{[i]})$, see (3.1.1). Since $1 \in \mathcal{U}^{[i]}$ and $\mathcal{U}^{[i]} \subseteq \mathbb{F}_{q^s}$ for all i, the desired statement follows from Theorem 54. "$\Longleftarrow$" The proof is similar to the one of Theorem 54. Suppose $\mathcal{U} \not\subseteq \mathbb{F}_{q^s}$. Thanks to our assumption this implies $\delta_s(\mathcal{U}) =: r \geq 3$. Thus Proposition 56, Lemma 58(a), and Remark 44 lead to

$$\left|\mathrm{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U})\right| \geq \frac{q^{\binom{r}{2}(s-1)}}{\begin{bmatrix} k \\ r \end{bmatrix}_q} \prod_{i=0}^{r-1} \frac{q^{n-is}-1}{q^{r-i}-1} > n\frac{q^n-1}{q-1} \geq |\mathrm{Orb}_N(\mathcal{U})|,$$

and therefore $\mathrm{GL}_{n/s}(q^s) \not\leq \mathrm{Aut}(\mathrm{Orb}_N(\mathcal{U}))$. The rest of the proof is identical to the one for Theorem 54. For Part (b) notice that "$\Rightarrow$" of (3.3.1) holds true for general $\delta_s(\mathcal{U})$. □

We now turn to the remaining case $r = \delta_s(\mathcal{U}) = 2$. In this case there are indeed instances where $\mathrm{GL}_{n/s}(q^s) \leq \mathrm{Aut}(\mathrm{Orb}_N(\mathcal{U}))$ even though $\mathcal{U} \not\subseteq \mathbb{F}_{q^s}$. Clearly, this containment is equivalent to $\mathrm{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U}) \subseteq \mathrm{Orb}_N(\mathcal{U})$. In all known examples we even have $\mathrm{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U}) = \mathrm{Orb}_N(\mathcal{U})$. In fact, we believe that we have $\mathrm{Orb}_N(\mathcal{U}) \subseteq \mathrm{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U})$ for all subspaces $\mathcal{U}$ (i.e., $\mathcal{U}^q = \phi(\mathcal{U})$ for some $\phi \in \mathrm{GL}_{n/s}(q^s)$), but unfortunately we are not able at this point to prove this statement.

Example 61. Let $(q, n, k, s) = (2, 4, 2, 2)$. A 2-dimensional subspace $\mathcal{U} \leq \mathbb{F}_{2^4}$ with $\delta_2(\mathcal{U}) = 2$ is of the form $\mathcal{U} = \mathrm{span}_{\mathbb{F}_2}\{1, \alpha\}$ for some $\alpha \in \mathbb{F}_{2^4} \setminus \mathbb{F}_{2^2}$. One can directly verify (using, e.g., SageMath) that all these subspaces generate the same N-orbit, and this orbit agrees with the $\mathrm{GL}_2(4)$-orbit. The orbit size is $n/2(2^n - 1)/(2 - 1) = 30$ (see also Proposition 63 below).

Example 62. Let $(q, n, k, s) = (2, 8, 4, 4)$. Let $\alpha \in \mathbb{F}_{2^8} \setminus \mathbb{F}_{2^4}$ and consider the subspace $\mathcal{U} = \mathrm{span}_{\mathbb{F}_{2^2}}\{1, \alpha\}$. Then $\mathcal{U} \not\subseteq \mathbb{F}_{2^4}$, hence $\delta_4(\mathcal{U}) = 2$, and one straightforwardly verifies that $\mathrm{Orb}_{\mathrm{GL}_2(2^4)}(\mathcal{U}) = \mathrm{Orb}_N(\mathcal{U})$, and the orbit has size 340 (for comparison, the lower bound from Proposition 56 is 292). These observations can also be seen as follows. Let $S = \mathbb{F}_{2^8}^*$.

(i) By Remark 44 the Singer orbit has size $|\mathrm{Orb}_S(\mathcal{U})| = (2^n - 1)/(2^2 - 1) = 85$.

(ii) As Proposition 63 below shows, $\mathcal{U}^{[4]} \in \mathrm{Orb}_S(\mathcal{U})$; thus σ^4 stabilizes $\mathrm{Orb}_S(\mathcal{U})$, where σ is the Frobenius automorphism. Furthermore, no other non-trivial element of the Galois group $\mathrm{Gal}(\mathbb{F}_{2^8} | \mathbb{F}_2)$ stabilizes $\mathrm{Orb}_S(\mathcal{U})$ (this is true for these specific parameters, but not in the general situation of Proposition 63). Together with (i) this shows that $|\mathrm{Orb}_N(\mathcal{U})| = 4 \cdot 85 = 340$.

(iii) Since $\mathcal{U} = \mathrm{span}_{\mathbb{F}_{2^2}}\{1, \alpha\}$ and $\mathbb{F}_{2^2} \subseteq \mathbb{F}_{2^4}$, an $\mathbb{F}_{2^4}$-linear isomorphism ϕ maps $\mathcal{U}$ to the space $\mathrm{span}_{\mathbb{F}_{2^2}}\{\phi(1), \phi(\alpha)\}$. As a consequence, $\mathrm{Orb}_{\mathrm{GL}_2(2^4)}(\mathcal{U})$ consists of all subspaces in $\mathbb{F}_{2^8}$ that are 2-dimensional over $\mathbb{F}_{2^2}$ and not 1-dimensional over $\mathbb{F}_{2^4}$, i.e., not a cyclic shift of $\mathbb{F}_{2^4}$. Thus $|\mathrm{Orb}_{\mathrm{GL}_2(2^4)}(\mathcal{U})| = \begin{bmatrix} 4 \\ 2 \end{bmatrix}_4 - |\mathrm{Orb}_S(\mathbb{F}_{2^4})| = \begin{bmatrix} 4 \\ 2 \end{bmatrix}_4 - (2^8 - 1)/(2^4 - 1) = 340$.

(iv) Finally, $\mathrm{Orb}_N(\mathcal{U}) \subseteq \mathrm{Orb}_{\mathrm{GL}_2(2^4)}(\mathcal{U})$. To see this, it suffices to show that $\mathcal{U}^{[i]} \in \mathrm{Orb}_{\mathrm{GL}_2(2^4)}(\mathcal{U})$ for all $i \in \{0, \ldots, n-1\}$. Note that $\mathcal{U}^{[i]} = \mathrm{span}_{\mathbb{F}_{2^2}}\{1, \alpha^{[i]}\}$. Since 1 and $\alpha^{[i]}$ are $\mathbb{F}_{2^4}$-linearly independent, there exists $\phi \in \mathrm{GL}_2(2^4)$ such that $\phi(1) = 1$ and $\phi(\alpha) = \alpha^{[i]}$. Hence $\mathcal{U}^{[i]} = \phi(\mathcal{U}) \in \mathrm{Orb}_{\mathrm{GL}_2(2^4)}(\mathcal{U})$.

We wish to add that all subspaces of the form $\mathrm{span}_{\mathbb{F}_{2^2}}\{1, \alpha\}$ with $\alpha \in \mathbb{F}_{2^8} \setminus \mathbb{F}_{2^4}$ generate the same orbit, and this is the only N-orbit of a 4-dimensional subspace that coincides with the $\mathrm{GL}_{n/s}(q^s)$-orbit. Finally, since $\mathcal{U}$ is actually an $\mathbb{F}_4$-vector space and $\mathbb{F}_{2^8} = \mathbb{F}_{4^4}$, we may regard all of this also as an example for the parameters $(q, n, k, s) = (4, 4, 2, 2)$. Thus $\mathrm{Orb}_{\mathrm{GL}_2(4^2)}(\mathcal{U}) = \mathrm{Orb}_{N'}(\mathcal{U})$, where $N' = N_{\mathrm{GL}_4(4)}(\mathbb{F}_{4^4}^*)$.

The subspaces $\mathcal{U}$ in the above examples are both of the form $\mathcal{U} = \mathrm{span}_{\mathbb{F}_{q^a}}\{1, \alpha\} \subseteq \mathbb{F}_{q^n}$, where $a = n/4$ and $s = k = n/2$ and $\mathcal{U} \not\subseteq \mathbb{F}_{q^s}$. In Corollary 65 below we will show that for no other subspaces of this type the $\mathrm{GL}_{n/s}(q^s)$-orbit coincides with the N-orbit. We start with showing that all such subspaces $\mathcal{U}$ satisfy $\mathcal{U}^{[s]} \in \mathrm{Orb}_{\mathbb{F}_{q^n}^*}(\mathcal{U})$.

Proposition 63. Let $a \in \mathbb{N}$, $n = 4a$, and $s = k = 2a$. Choose $\alpha \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^s}$ and set $\mathcal{U} = \mathrm{span}_{\mathbb{F}_{q^a}}\{1, \alpha\} \subseteq \mathbb{F}_{q^n}$. Then $\mathcal{U}^{[s]} \in \mathrm{Orb}_{\mathbb{F}_{q^n}^*}(\mathcal{U})$. Thus

$$|\mathrm{Orb}_N(\mathcal{U})| \leq \frac{n}{2}\frac{q^n-1}{q^a-1}.$$

Proof. By Remark 44 we have $|\mathrm{Orb}_{\mathbb{F}_{q^n}^*}(\mathcal{U})| = (q^n-1)/(q^a-1)$. Thus the second statement follows once we establish $\mathcal{U}^{[s]} \in \mathrm{Orb}_{\mathbb{F}_{q^n}^*}(\mathcal{U})$. To do so we proceed as follows.
1) We show first that

$$\alpha^{[s]}\mathcal{U} \cap \mathcal{U} \neq \{0\}. \tag{3.3.2}$$

Since both $\mathcal{U}$ and $\alpha^{[s]}\mathcal{U} = \mathrm{span}_{\mathbb{F}_{q^a}}\{\alpha^{[s]}, \alpha\alpha^{[s]}\}$ have dimension $2a = n/2$, (3.3.2) is equivalent to $\alpha^{[s]}\mathcal{U} + \mathcal{U} \neq \mathbb{F}_{q^n}$. Hence we have to show that 1, α, $\alpha^{[s]}$, $\alpha\alpha^{[s]}$ are linearly dependent over $\mathbb{F}_{q^a}$. We show that there exist $\lambda, \mu, \nu \in \mathbb{F}_{q^a}$ such that

$$\lambda + \mu\alpha + \mu\alpha^{[s]} + \nu\alpha\alpha^{[s]} = 0. \tag{3.3.3}$$

Raising (3.3.3) to the power $[a]$ and using $s = 2a$ we obtain a second equation, which together with (3.3.3) can be written as

$$\begin{pmatrix} 1 & \alpha + \alpha^{[2a]} & \alpha\alpha^{[2a]} \\ 1 & \alpha^{[a]} + \alpha^{[3a]} & \alpha^{[a]}\alpha^{[3a]} \end{pmatrix} \begin{pmatrix} \lambda \\ \mu \\ \nu \end{pmatrix} = 0. \tag{3.3.4}$$

The matrix is row equivalent to

$$\begin{pmatrix} 1 & \alpha + \alpha^{[2a]} & \alpha\alpha^{[2a]} \\ 0 & \alpha^{[a]} + \alpha^{[3a]} - \alpha - \alpha^{[2a]} & \alpha^{[a]}\alpha^{[3a]} - \alpha\alpha^{[2a]} \end{pmatrix}.$$

Now we can find a solution of the desired form. Suppose first that $\alpha - \alpha^{[a]} + \alpha^{[2a]} - \alpha^{[3a]} \neq 0$. Set $\nu = 1$. Then (3.3.4) has the unique (normalized) solution

$$\nu = 1, \quad \mu = \frac{\alpha^{[a]}\alpha^{[3a]} - \alpha\alpha^{[2a]}}{\alpha - \alpha^{[a]} + \alpha^{[2a]} - \alpha^{[3a]}}, \quad \lambda = -\mu(\alpha + \alpha^{[2a]}) - \alpha\alpha^{[2a]}.$$

Using that $4a = n$, one easily verifies that $\mu^{[a]} = \mu$ and $\lambda = \lambda^{[a]}$, and thus $(\lambda, \mu, \nu) \in \mathbb{F}_{q^a}^3$. If $\alpha - \alpha^{[a]} + \alpha^{[2a]} - \alpha^{[3a]} = 0$, (3.3.3) has the solution $(\lambda, \mu, \nu) = (-(\alpha + \alpha^{[2a]}), 1, 0)$, which again is in $\mathbb{F}_{q^a}^3$. All of this establishes (3.3.2).
2) (3.3.2) implies that also $\alpha^{-[s]}\mathcal{U} \cap \mathcal{U} \neq \{0\}$. Choose $\delta \in \alpha^{-[s]}\mathcal{U} \cap \mathcal{U} \setminus \{0\}$ and let $\gamma \in \mathbb{F}_{q^n}^*$ be such that $\gamma^{[s]} = \delta$. Then $\gamma = \gamma^{[2s]} = \delta^{[s]} \in \mathcal{U}^{[s]}$. Moreover, $\gamma^{[s]}\alpha^{[s]} \in \mathcal{U}$ and thus $\gamma\alpha \in \mathcal{U}^{[s]}$. All of this shows that $\gamma\mathcal{U} = \mathrm{span}_{\mathbb{F}_{q^a}}\{\gamma, \gamma\alpha\} = \mathcal{U}^{[s]}$. Thus, $\mathcal{U}^{[s]} \in \mathrm{Orb}_{\mathbb{F}_{q^n}^*}(\mathcal{U})$, as desired. □

Remark 64. Proposition 63 only provides an upper bound for $|\mathrm{Orb}_N(\mathcal{U})|$. In fact, there even exist subspaces $\mathcal{U}$ of the specified form for which $\mathcal{U}^{[i]} \in \mathrm{Orb}_S(\mathcal{U})$ for all i and thus $\mathrm{Orb}_N(\mathcal{U}) = \mathrm{Orb}_S(\mathcal{U})$; for instance for $q = 3$ and $a = 2$. On the other hand, for $q = 2$ and $a = 2$ we have equality in Proposition 63 for all subspaces of the given form.

Corollary 65. Let the data be as in Proposition 63. Then

$$\mathrm{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U}) = \mathrm{Orb}_N(\mathcal{U}) \iff (q,a) \in \{(2,1),\,(2,2)\}.$$

Proof. "$\Longleftarrow$" Examples 61 and 62.
"$\Longrightarrow$" Let $(q,a) \notin \{(2,1),\,(2,2)\}$. We show that $|\,\mathrm{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U})| > |\,\mathrm{Orb}_N(\mathcal{U})|$. Thanks to Proposition 63 it suffices to show $|\,\mathrm{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U})| - n/2(q^n-1)/(q^a-1) > 0$. Using $r = \delta_s(\mathcal{U}) = 2$ and $k = 2a = s = n/2$ along with the lower bound in Proposition 56 the inequality follows if we prove $Q := q^{2a-1}(q^a-1) - 2a(q^{2a-1}-1) > 0$. We have

$$Q > (q^{2a-1}-1)(q^a - 1 - 2a).$$

The first factor is clearly positive. As for the second factor, note that the function $f(x) = q^x - (2x+1)$ is non-negative on $[1,\infty)$ if $q \geq 3$, while for $q = 2$ this is the case for the interval $[3,\infty)$. This shows that $Q > 0$ whenever $(q,a) \notin \{(2,1),\,(2,2)\}$ and concludes the proof. □

There is one more known example where the $\mathrm{GL}_{n/s}(q^s)$-orbit coincides with the N-orbit even though the subspace is not contained in $\mathbb{F}_{q^s}$. In fact, it is the only such example for $s = 1$. Indeed, note that $s = 1$ together with $\delta_s(\mathcal{U}) = 2$ forces $\dim(\mathcal{U}) = 2$. In Proposition 68 below we will list all 2-dimensional subspaces for which the orbits coincide.

Example 66. Let $(q,n,s) = (2,5,1)$ and choose any subspace $\mathcal{U} \in \mathcal{G}_2(2,5)$. Then $\mathrm{Orb}_{\mathrm{GL}_5(2)}(\mathcal{U})$ is the entire Grassmannian $\mathcal{G}_2(2,5)$. It has cardinality $\begin{bmatrix}5\\2\end{bmatrix}_2 = 155 = 5(2^5-1)/(2-1)$ and satisfies $\mathrm{Orb}_{\mathrm{GL}_5(2)}(\mathcal{U}) = \mathrm{Orb}_N(\mathcal{U})$.

We now turn to cases where Inequality (3.2.5) of Lemma 58(a) holds true even with $r = 2$. Recall that $\delta_s(\mathcal{U}) = 2$ implies $s \leq n/2$ because $\delta_s(\mathcal{U})s \leq n$.

Proposition 67. Let $k \leq 3n/8$ and $s \leq n/2$ be a divisor of n. Let $\mathcal{U} \in \mathcal{G}_q(k,n)$ be such that $1 \in \mathcal{U}$. Then either $\mathcal{U} \subseteq \mathbb{F}_{q^s}$ or

$$\left|\,\mathrm{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U})\right| > |\,\mathrm{Orb}_N(\mathcal{U})|,$$

and thus $\mathrm{GL}_{n/s}(q^s) \not\leq \mathrm{Aut}(\mathrm{Orb}_N(\mathcal{U}))$.

Moreover, if $\mathbb{F}_{q^s}$ is the smallest subfield containing $\mathcal{U}$, then $\mathrm{GL}_{n/s}(q^s)$ is normal in $\mathrm{Aut}(\mathrm{Orb}_N(\mathcal{U}))$ and thus $\mathrm{Aut}(\mathrm{Orb}_N(\mathcal{U})) \leq N_{\mathrm{GL}_n(q)}(\mathrm{GL}_{n/s}(q^s))$. As a consequence, $\mathcal{U}$ is generic iff $\mathrm{Aut}(\mathrm{Orb}_N(\mathcal{U})) = N$.

Proof. All statements follow as in Theorem 60 if we can show that (3.2.5) holds true in the case that $\delta_s(\mathcal{U}) = 2$. As we will see, this is indeed the case for most parameters. The remaining values will be discussed subsequently. For $r := \delta_s(\mathcal{U}) = 2$ Inequality (3.2.5) is equivalent to

$$Q := (q-1)(q^n - q^s) - n(q^k-1)(q^k-q) > 0. \tag{3.3.5}$$

The left hand side decreases for increasing s, and thus we may assume $s = n/2$. With the aid of (3.2.4) we compute

$$\begin{aligned} Q &\geq (q-1)q^{n/2}(q^{n/2}-1) - nq(q^k-1)(q^{k-1}-1) \\ &> \big((q-1)q^{n/2}q^{n/2-k+1} - nq(q^k-1)\big)(q^{k-1}-1) \\ &= \Big(\frac{(q-1)q^{n-k}}{q^k-1} - n\Big)q(q^k-1)(q^{k-1}-1) \\ &> \big((q-1)q^{n-2k} - n\big)q(q^k-1)(q^{k-1}-1) \qquad (3.3.6) \\ &> \big((q-1)q^{n/4} - n\big)q(q^k-1)(q^{k-1}-1), \end{aligned}$$

where in the last step we used that $k \leq 3n/8$. Clearly the last three factors are positive. As for the first factor, consider the function $f(x) = (x-1)x^{n/4} - n$. For fixed n the function is increasing on $[2, \infty)$. Furthermore,

$$f(2) \geq 0 \text{ for } n \geq 16, \quad f(3) \geq 0 \text{ for } n \geq 8, \ f(4) \geq 0 \text{ for } n \geq 4.$$

Thus $Q > 0$ if (i) $q \geq 4$ and $n \geq 4$, (ii) $q = 3$ and $n \geq 8$, or (iii) $q = 2$ and $n \geq 16$. For the cases $q = 2$ with $4 \leq n \leq 15$ and $q = 3$ with $4 \leq n \leq 7$, direct verification shows that (3.3.5) holds true unless $(q, n, k) \in \{(2, 8, 3), (2, 11, 4)\}$. We consider these cases separately.
a) Let $(q, n, k) = (2, 11, 4)$. Then $s = 1$ (since s is a divisor of n). But then every 4-dimensional subspace $\mathcal{U}$ satisfies $\delta_s(\mathcal{U}) = 4$, and thus there is nothing to show.
b) Let $(q, n, k) = (2, 8, 3)$. In this case $s \in \{2, 4\}$. Exhaustive consideration of all 3-dimensional subspaces $\mathcal{U}$ in $\mathbb{F}_{2^8}$ with $\delta_s(\mathcal{U}) = 2$ shows that in each case the orbit $\mathrm{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U})$ is strictly larger than $n(2^n - 1) = 2040$, which is an upper bound for $|\mathrm{Orb}_N(\mathcal{U})|$. To be precise, for $s = 2$, there is exactly one $\mathrm{GL}_{n/s}(q^s)$-orbit and it has size 5355, while for $s = 4$ there exists one orbit of size 61200, two orbits of size 15300, and one orbit of size 5100. For comparison, the lower bound in Proposition 56 only provides $|\mathrm{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U})| \geq 1530$ if $s = 2$ and $|\mathrm{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U})| \geq 1458$ if $s = 4$. □

Now we can fully cover the case where $k = r = 2$. Let $N := N_{\mathrm{GL}_n(q)}(\mathbb{F}_{q^n}^*)$.

Proposition 68. Let $n \geq 4$ and $1 \leq s \leq n/2$ be a divisor of n. The following are equivalent.
(i) There exists $\mathcal{U} \in \mathcal{G}_q(2, n)$ such that $\delta_s(\mathcal{U}) = 2$ and $\mathrm{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U}) = \mathrm{Orb}_N(\mathcal{U})$.
(ii) $(q, n, s) \in \{(2, 4, 2), (2, 5, 1), (4, 4, 2)\}$.

Proof. "(ii) ⇒ (i)" Examples 61, 66, and 62.
"(i) ⇒ (ii)" By Proposition 67 we must have $k = 2 > 3n/8$, hence $n \leq 5$. Since s is a divisor of n and $s \leq n/2$, this leaves the cases $(n, s) \in \{(4, 1), (4, 2), (5, 1)\}$ with arbitrary q. Using Proposition 56 for the case $r = k = 2$ and $|\mathrm{Orb}_N(\mathcal{U})| \leq n(q^n - 1)/(q - 1)$, we conclude that $|\mathrm{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U})| > |\mathrm{Orb}_N(\mathcal{U})|$ if

$$Q := q^{s-1}(q^{n-s} - 1) - n(q^2 - 1) > 0.$$

Case 1: $(n, s) = (4, 1)$.
In this case $Q > 0$ iff $q \geq 4$. Thus it remains to consider $q \in \{2, 3\}$. Since $s = 1$, every 2-dimensional subspace $\mathcal{U}$ satisfies $\delta_s(\mathcal{U}) = 2$ and $|\operatorname{Orb}_{\mathrm{GL}_4(q)}(\mathcal{U})| = \begin{bmatrix} 4 \\ 2 \end{bmatrix}_q$. Furthermore, exhaustive verification shows that $|\operatorname{Orb}_N(\mathcal{U})| \leq n/2(q^n - 1)/(q - 1)$. Thus $|\operatorname{Orb}_{\mathrm{GL}_4(q)}(\mathcal{U})| > |\operatorname{Orb}_N(\mathcal{U})|$.

Case 2: $(n, s) = (4, 2)$.
In this case $Q > 0$ for all $q \geq 5$, and exhaustive verification shows that for $q = 3$ every 2-dimensional subspace $\mathcal{U}$ in $\mathbb{F}_{3^4}$ with $\delta_2(\mathcal{U}) = 2$ satisfies $|\operatorname{Orb}_N(\mathcal{U})| \leq n/2(q^n - 1)/(q - 1) < |\operatorname{Orb}_{\mathrm{GL}_4(3)}(\mathcal{U})|$ (where the first inequality also follows from Proposition 63). This leaves the cases $(q, n, s) \in \{(2, 4, 2), (4, 4, 2)\}$.

Case 3: $(n, s) = (5, 1)$. In this case $Q > 0$ iff $q \geq 3$, and thus only $(q, n, s) = (2, 5, 1)$ remains. □

Similarly we can cover all cases where $k = 3$ (hence $n \geq 6$). In this case, $\operatorname{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U})$ is always strictly bigger than $\operatorname{Orb}_N(\mathcal{U})$.

Proposition 69. Let $n \geq 6$ and $s \leq n/2$ be a divisor of n. Then for every subspace $\mathcal{U} \in \mathcal{G}_q(3, n)$ such that $\delta_s(\mathcal{U}) = 2$ we have $|\operatorname{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U})| > |\operatorname{Orb}_N(\mathcal{U})|$.

Proof. By Lemma 67 we only need to verify the cases where $k = 3 > 3n/8$, thus $n < 8$. Since $\delta_s(\mathcal{U}) = 2 \neq \dim(\mathcal{U}) = 3$, we must have $s \neq 1$. This leaves $(n, s) \in \{(6, 2), (6, 3)\}$. Using $n = 6$, $k = 3$ and $s \in \{2, 3\}$ one verifies that (3.3.5) is true whenever $q \geq 7$. Exhaustive verification for $q \in \{2, 3, 4, 5\}$ establishes the desired result. □

As the proofs in this section have shown, for given parameters (n, k, s) and $r = 2$ the inequality in (3.2.5) is true for sufficiently large q (for instance, if $k < n/2$, then this is the case for $q \geq n + 1$ as (3.3.6) shows). Thus, any further examples where the N-orbit agrees with the $\mathrm{GL}_{n/s}(q^s)$-orbit requires a relatively small field size. We strongly believe that no further example exists and thus close this section with

Conjecture 70. Let $s \leq n/2$ be a divisor of n and $\mathcal{U} \in \mathbb{F}_{q^n}$ be such that $\delta_s(\mathcal{U}) = 2$ and $\operatorname{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U}) \subseteq \operatorname{Orb}_N(\mathcal{U})$. Then the orbits coincide and $\mathcal{U}$ is one of the subspaces from Examples 61, 62, and 66.

3.4 Isometries of Orbit Codes

In this section we turn to the question when two orbit codes (under the Singer subgroup or its normalizer) are linearly isometric. Our first result provides a criterion for when two cyclic orbit codes are not linearly isometric.

Theorem 71. Let $\mathcal{C}, \mathcal{C}'$ be distinct Singer orbits. If $\operatorname{Aut}(\mathcal{C}') = N_{\mathrm{GL}_n(q)}(\mathbb{F}_{q^n}^*) \subseteq \operatorname{Aut}(\mathcal{C})$, then $\mathcal{C}$ and $\mathcal{C}'$ are not linearly isometric.

Our proof is an adaptation of [2, Thm. 5], where the authors prove an analogous result for q-Steiner systems.

Proof. We prove the contrapositive. Suppose that $\mathcal{C}$ and $\mathcal{C}'$ are linearly isometric, so that there exists $\psi \in \mathrm{GL}_n(q)$ such that $\psi(\mathcal{C}) = \mathcal{C}'$. Let $\tau \in N := N_{\mathrm{GL}_n}(\mathbb{F}_{q^n}^*)$. Then our assumptions on $\mathrm{Aut}(\mathcal{C}')$ and $\mathrm{Aut}(\mathcal{C})$ imply $\psi \circ \tau \circ \psi^{-1}(\mathcal{C}') = \psi \circ \tau(\mathcal{C}) = \psi(\mathcal{C}) = \mathcal{C}'$, and thus $\psi \circ \tau \circ \psi^{-1} \in \mathrm{Aut}(\mathcal{C}') = N$. This shows that ψ is in the normalizer of N. But the latter is N itself thanks to Theorem 11(a), and hence $\psi \in \mathrm{Aut}(\mathcal{C}')$ and $\mathcal{C} = \mathcal{C}'$. □

The main result of this section shows that Singer orbits of generic subspaces are linearly isometric iff they are Frobenius-isometric. This drastically reduces the workload when finding isometry classes of such codes.

Theorem 72. Let $\mathcal{U}, \mathcal{U}' \in \mathcal{G}_q(k, n)$ such that $1 \in \mathcal{U}'$ and $\mathcal{U}'$ is generic.
(a) Let $S = \mathbb{F}_{q^n}^*$. Then $\mathrm{Orb}_S(\mathcal{U})$ and $\mathrm{Orb}_S(\mathcal{U}')$ are linearly isometric iff they are Frobenius-isometric.
(b) Let $k \leq 3n/8$ or $\delta_s(\mathcal{U}) \geq 3$ for all divisors s of n. Let $N = N_{\mathrm{GL}_n(q)}(\mathbb{F}_{q^n}^*)$. Then $\mathrm{Orb}_N(\mathcal{U})$ and $\mathrm{Orb}_N(\mathcal{U}')$ are linearly isometric iff they are equal.

Proof. (a) Only "$\Longrightarrow$" needs proof. Set $\mathcal{C} = \mathrm{Orb}_S(\mathcal{U})$ and $\mathcal{C}' = \mathrm{Orb}_S(\mathcal{U}')$. Let $\psi \in \mathrm{GL}_n(q)$ be such that $\psi(\mathcal{C}) = \mathcal{C}'$. Theorem 48(b) tells us that $\mathcal{C}' = \mathrm{Orb}_{\psi S \psi^{-1}}(\mathcal{U}'')$, where $\mathcal{U}'' = \psi(\mathcal{U})$. Hence $\mathrm{Aut}(\mathcal{C}')$ contains the Singer subgroups S and $\psi S \psi^{-1}$. By Theorem 54 the automorphism group $\mathrm{Aut}(\mathcal{C}')$ is contained in $N_{\mathrm{GL}_n(q)}(S)$. However, by Theorem 11(b) $N_{\mathrm{GL}_n(q)}(S)$ contains only one Singer subgroup. This implies $\psi S \psi^{-1} = S$, and thus $\psi \in N_{\mathrm{GL}_n(q)}(S)$.
(b) Let $\mathcal{C} := \mathrm{Orb}_N(\mathcal{U})$ and $\psi(\mathcal{C}) = \mathcal{C}' := \mathrm{Orb}_N(\mathcal{U}')$. Then $\mathcal{C}' = \mathrm{Orb}_{\psi N \psi^{-1}}(\mathcal{U}'')$, where $\mathcal{U}'' = \psi(\mathcal{U})$, and thus $\psi N \psi^{-1} \leq \mathrm{Aut}(\mathcal{C}') = N$, where the last identity follows from Theorem 60 and Proposition 67. Hence $\psi \in N$ thanks to Theorem 11(a), and thus $\mathcal{C}' = \psi(\mathcal{C}) = \mathcal{C}$. □

As the proof shows, Part (b) above is true for all subspaces that satisfy $\mathrm{Aut}(\mathrm{Orb}_N(\mathcal{U})) = N$. Since the three outliers from Examples 61, 62, and 66 are the only orbit of their size in the respective ambient space, they trivially satisfy the equivalence in (b) above even though their automorphism group is much larger.

We close this section with some examples and a comparison of isometries and weight-preserving bijections between cyclic orbit codes, where we define the weight of a codeword in $\mathrm{Orb}_{\mathbb{F}_{q^n}^*}(\mathcal{U})$ as the distance to the 'reference space' $\mathcal{U}$. Since we will exclusively consider cyclic orbit codes, we write from now on $\mathrm{Orb}(\mathcal{U})$ instead of $\mathrm{Orb}_{\mathbb{F}_{q^n}^*}(\mathcal{U})$.

In Chapter 2 we studied the distance (weight) distribution of cyclic orbit codes $\mathrm{Orb}(\mathcal{U})$. We will see later that codes with the same weight distribution may not be isometric. Before providing details we first summarize the results from the previous chapter. Recall the notation from (1.2.1) and (1.2.2). As before we assume $k \leq n/2$. First, let's recall the defintion of the weight distribution.

Definition 73. Let $\mathcal{U} \in \mathcal{G}_q(k,n)$. Define $\omega_i = |\{\alpha\mathcal{U} \in \mathrm{Orb}(\mathcal{U}) \mid \alpha \in \mathbb{F}_{q^n}^*, \mathrm{d}(\mathcal{U}, \alpha\mathcal{U}) = i\}|$ for $i = 0, \ldots, 2k$. We call $(\omega_0, \ldots, \omega_{2k})$ the *weight distribution* of $\mathrm{Orb}(\mathcal{U})$.

Clearly $\omega_0 = 1$ and $\omega_i = 0$ for $i = 1, \ldots, d-1$, where $d = \mathrm{d_s}(\mathrm{Orb}(\mathcal{U}))$. Obviously, the weight distribution is trivial for spread codes (i.e., if $\mathrm{d_s}(\mathrm{Orb}(\mathcal{U})) = 2k$). From (1.2.1) it follows that $\mathrm{d_s}(\mathrm{Orb}(\mathcal{U}) = 2(k-\ell)$, where $\ell = \max\{\dim(\mathcal{U} \cap \alpha\mathcal{U}) \mid \alpha \in \mathbb{F}_{q^n}^*\}$.

In Theorem 74 below we collect again some facts about the weight distribution. Part (a) shows that all cyclic orbit codes with distance $2(k-1)$ have the same weight distribution. Hence there exists a weight-preserving bijection between any such codes. However, as we will see below, the codes are not necessarily isometric. Subspaces $\mathcal{U}$ that generate cyclic orbit codes with distance $2(k-1)$ are known as Sidon spaces; see [26, 23, 24] where also constructions of such spaces can be found.

We also saw in the previous chapter that codes with distance up to $2k-4$ do not share the same weight distribution in general. For distance equal to $2k-4$, Part (b) below provides information about the weight distribution. Further details about the parameter r in Part (b) can be found in Section 2.3. However, we do not yet fully understood which values this parameter can assume in general.

Theorem 74 ([11, Thms. 3.7 and 4.1])**.** Let $\mathcal{U} \in \mathcal{G}_q(k,n)$ be such that $1 \in \mathcal{U}$. Let $\mathrm{d_s}(\mathrm{Orb}(\mathcal{U}) = 2(k-\ell)$, where $\ell > 0$. Set $Q = (q^k-1)(q^k-q)/(q-1)^2$ and $N = (q^n-1)/(q-1)$.

(a) Suppose $\ell = 1$. Then $|\mathrm{Orb}(\mathcal{U})| = N$ and

$$\big(\omega_{2k-2},\, \omega_{2k}\big) = \big(Q,\ N-Q-1\big).$$

(b) Suppose $\ell = 2$ and $|\mathrm{Orb}(\mathcal{U})| = N$. Then there exits $r \in \mathbb{N}_0$ and $\epsilon \in \{0,1\}$ such that

$$\big(\omega_{2k-4},\, \omega_{2k-2},\, \omega_{2k}\big) = \big(\epsilon q + rq(q+1),\ Q-(q+1)\omega_{2k-4},\ N-\omega_{2k-2}-\omega_{2k-4}-1\big).$$

The case $\epsilon = 1$ occurs iff $\mathcal{U}$ contains the subfield $\mathbb{F}_{q^2}$ (which implies that n is even).

In the following examples we list all isometry classes of the subspaces in question along with their automorphism group. In most cases the size of the isometry class is determined by the automorphism group as follows.

Remark 75. Let $\mathcal{C} = \mathrm{Orb}_{\mathbb{F}_{q^n}^*}(\mathcal{U})$ be a cyclic orbit code with automorphism group A contained in $N_{\mathrm{GL}_n(q)}(\mathbb{F}_{q^n}^*)$. Then the isometry class of $\mathcal{C}$ consists of ν cyclic orbit codes, where $\nu = n(q^n-1)/|A|$. This is due to Theorem 72, which tells us that two cyclic orbit codes are isometric iff they belong to the same orbit under the normalizer of the Singer subgroup $\mathbb{F}_{q^n}^*$.

In the following examples, the total number of orbits also follows from the formula for the number of Singer orbits of a given length that is provided in [6, Thm. 2.1] for general (q,n,k).

Example 76. Let $(q, n, k) = (2, 6, 3)$. There exist 23 cyclic orbit codes generated by 3-dimensional subspaces. One of them is $\mathrm{Orb}(\mathbb{F}_{2^3})$, which is a spread code (i.e., it consists of 9 subspaces and its subspace distance is 6; hence the union of its subspaces is $\mathbb{F}_{2^6}$). Its automorphism group is $\mathrm{Aut}(\mathrm{Orb}(\mathbb{F}_{2^3})) = N_{\mathrm{GL}_6(2)}(\mathrm{GL}_2(2^3))$. This follows directly from Theorem 54 along with the fact that $\mathrm{Gal}(\mathbb{F}_{2^3} \mid \mathbb{F}_2)$ acts trivially on $\mathrm{Orb}(\mathbb{F}_{2^3})$. Clearly, this is the only orbit generated by a non-generic subspace of $\mathbb{F}_{2^6}$. Even more, it is the only orbit with a generating subspace $\mathcal{U}$ such that $\delta_3(\mathcal{U}) \neq 2$ (see Definition 55). The other 22 orbits have length $2^6 - 1$, and their automorphism group is contained in $N_{\mathrm{GL}_6(2)}(\mathbb{F}_{2^6}^*)$ thanks to Theorem 54. They classify as follows. Note that distance 4 corresponds to Case (a) of the above theorem and distance 2 to Case (b). In the latter case we also present the value of $\omega_{2k-4} = \omega_2$ (which fully determines the weight distribution). It is, of course, invariant under isometry and thus identical for all orbits in the isometry class. Finally, we also present $\delta_2(\mathcal{U})$ for any subspace $\mathcal{U}$ in any of the orbits.

(a) Orbits with automorphism group $\mathbb{F}_{2^6}^*$:
  – 1 isometry class, consisting of orbits with distance 4 ($\delta_2(\mathcal{U}) = 3$).
  – 1 isometry class, consisting of orbits with distance 2 and $\omega_2 = 6$ ($\delta_2(\mathcal{U}) = 3$).

(b) Orbits with automorphism group $\mathrm{Gal}(\mathbb{F}_{2^6} \,|\, \mathbb{F}_{2^3}) \rtimes \mathbb{F}_{2^6}^*$:
  – 1 isometry class, consisting of orbits with distance 2 and $\omega_2 = 2$ ($\delta_2(\mathcal{U}) = 2$).
  – 1 isometry class, consisting of orbits with distance 2 and $\omega_2 = 6$ ($\delta_2(\mathcal{U}) = 3$).

(c) Orbits with automorphism group $\mathrm{Gal}(\mathbb{F}_{2^6} \,|\, \mathbb{F}_{2^2}) \rtimes \mathbb{F}_{2^6}^*$:
  – 1 isometry class, consisting of orbits with distance 4 ($\delta_2(\mathcal{U}) = 3$).
  – 1 isometry class, consisting of orbits with distance 2 and $\omega_2 = 2$ ($\delta_2(\mathcal{U}) = 2$).

Example 77. Let $(q, n, k) = (2, 7, 3)$. In this case, there are no proper subfields of $\mathbb{F}_{2^7}$ to be taken into account, and in particular $\epsilon = 0$ in Case (b) of Theorem 74. There exist 93 cyclic orbit codes generated by 3-dimensional subspaces. All of them have length $2^7 - 1$. They classify as follows.

(a) Orbits with automorphism group $\mathbb{F}_{2^7}^*$:
  – 10 isometry classes, consisting of orbits with distance 4.
  – 3 isometry classes, consisting of orbits with distance 2 and $\omega_2 = 6$.

(b) Orbits with automorphism group $\mathrm{Gal}(\mathbb{F}_{2^7} \,|\, \mathbb{F}_2) \rtimes \mathbb{F}_{2^7}^*$:
  – 2 isometry classes, each consisting of a single orbit with distance 4.

Example 78. Let $(q, n, k) = (2, 8, 3)$. There exist 381 cyclic orbit codes generated by a 3-dimensional subspace. All orbits have length $2^8 - 1$. Exactly one orbit is generated by a subspace contained in $\mathbb{F}_{2^4}$. Clearly, all other orbits are generated by subspaces $\mathcal{U}$ with $\delta_4(\mathcal{U}) = 2$. The orbits classify as follows. We present the data as in Example 76.

(a) Orbits with automorphism group $\mathbb{F}_{2^8}^*$:
  – 38 isometry classes, consisting of orbits with distance 4 ($\delta_2(\mathcal{U}) = 3$).
  – 4 isometry classes, consisting of orbits with distance 2 and $\omega_2 = 6$ ($\delta_2(\mathcal{U}) = 3$).
  – 2 isometry classes, consisting of orbits with distance 2 and $\omega_2 = 2$ ($\delta_2(\mathcal{U}) = 2$).

(b) Orbits with automorphism group $\mathrm{Gal}(\mathbb{F}_{2^8} \,|\, \mathbb{F}_{2^4}) \rtimes \mathbb{F}_{2^8}^*$:
  – 3 isometry classes, consisting of orbits with distance 4 ($\delta_2(\mathcal{U}) = 3$).

– 2 isometry classes, consisting of orbits with distance 2 and $\omega_2 = 6$ ($\delta_2(\mathcal{U}) = 3$).
– 1 isometry class, consisting of orbits with distance 2 and $\omega_2 = 2$ ($\delta_2(\mathcal{U}) = 2$).

(c) Orbits with automorphism group $\mathrm{Gal}(\mathbb{F}_{2^8} \,|\, \mathbb{F}_{2^2}) \rtimes \mathbb{F}_{2^8}^*$:
– 2 isometry classes, consisting of orbits with distance 4 ($\delta_2(\mathcal{U}) = 3$).

(d) Orbits with automorphism group $\mathrm{Gal}(\mathbb{F}_{2^4} \,|\, \mathbb{F}_2) \rtimes \mathrm{GL}_2(2^4)$:
– 1 isometry class, consisting of a single orbit with distance 2 and $\omega_2 = 14$ ($\delta_2(\mathcal{U}) = 2$). This cyclic orbit code is the only orbit generated by a subspace contained in $\mathbb{F}_{2^4}$ (and it contains $\mathbb{F}_{2^2}$).

3.5 Conclusion and Open Problems

We studied orbits of $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^n}$ under the Singer subgroup and under the normalizer of the Singer group. For cyclic orbit codes generated by generic subspaces we proved that a linear isometry between such orbits is contained in the normalizer of the Singer group. The result implies that, for most parameter cases, distinct orbits under the normalizer of the Singer subgroup are not linearly isometric. The following questions remain.

(a) We strongly believe that the isometry result for orbits under the normalizer is true for all parameter cases. This would follow if Conjecture 70 can be established, that is: the automorphism group of a normalizer orbit generated by a subspace $\mathcal{U}$ does not contain the field-extension subgroup $\mathrm{GL}_{n/s}(q^s)$ if $\mathcal{U}$ is not contained in $\mathbb{F}_{q^s}$ – unless $\mathcal{U}$ is one of the exceptional cases from Examples 61, 62, and 66.

(b) Furthermore, our isometry result in Theorem 72 is true only for orbits generated by generic subspaces. It is an open question whether the same result is true for arbitrary orbits.

(c) Finally, as we briefly address in Section 3.3 we believe that any subspace $\mathcal{U} \subseteq \mathbb{F}_{q^n}$ satisfies $\mathrm{Orb}_N(\mathcal{U}) \subseteq \mathrm{Orb}_{\mathrm{GL}_{n/s}(q^s)}(\mathcal{U})$, where $N = N_{\mathrm{GL}_n(q)}(\mathbb{F}_{q^n}^*)$ and $s \leq n/2$ is any divisor of n. We have to leave this to future research.

Bibliography

[1] E. Ben-Sasson, T. Etzion, A. Gabizon, and N. Raviv. Subspace polynomials and cyclic subspace codes. *IEEE Transactions on Information Theory*, 62(3):1157–1165, March 2016.

[2] M. Braun, T. Etzion, P. R. J. Östergård, A. Vardy, and A. Wasserman. Existence of q-analogs of Steiner systems. *Forum of Mathematics, Pi*, 4:e7, 2016.

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

[4] A. Cossidente, S. Kurz, G. Marino, and F. Pavese. Combining subspace codes. *Advances in Mathematics of Communications*, 0:–, 2021.

[5] A. Cossidente and M. Resmini. Remarks on Singer cylic groups and their normalizers. *Designs, Codes and Cryptography*, 32:97–102, 05 2004.

[6] K. Drudge. On the orbits of Singer groups and their subgroups. *Electr. J. Comb.*, 9, 01 2002.

[7] A.-S. Elsenhans and A. Kohnert. Constructing network codes using Möbius transformations. preprint, 2010. `https://math.uni-paderborn.de/fileadmin/mathematik/AG-Computeralgebra/Preprints-elsenhans/net{_}moebius{_}homepage.pdf`.

[8] T. Etzion and A. Vardy. Error-correcting codes in projective space. *IEEE Transactions on Information Theory*, 57(2):1165–1173, 2011.

[9] N. Gill. On a conjecture of Degos. *Cah. Topol. Géom. Différ. Catég.*, 57:229–237, 2016.

[10] H. Gluesing-Luerssen and H. Lehmann. Automorphism groups and isometries for cyclic orbit codes. `https://arxiv.org/abs/2101.09548`, 2021.

[11] H. Gluesing-Luerssen and H. Lehmann. Distance distributions of cyclic orbit codes. *Designs, Codes and Cryptography*, 89:447–470, 2021.

[12] H. Gluesing-Luerssen, K. Morrison, and C. Troha. Cyclic orbit codes and stabilizer subfields. *Advances in Mathematics of Communications*, 9(2):177–197, 2015.

[13] H. Gluesing-Luerssen and C. Troha. Construction of subspace codes through linkage. *Adv. Math. Commun.*, 10(3):525–540, 2016.

[14] J. Gomez-Calderon. On the stabilizer of companion matrices. *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 69(5):140 – 143, 1993.

[15] M. Greferath, M. Pavčević, N. Silberstein, and M. Vázques-Castro, editors. *Network Coding and Subspace Designs*. Signals and Communication Technology. Springer, 2018.

[16] D. Heinlein, M. Kiermaier, S. Kurz, and A. Wassermann. Tables of subspace codes, 2019.

[17] D. Heinlein and S. Kurz. Coset construction for subspace codes. *IEEE Transactions on Information Theory*, 63(12):7651–7660, 2017.

[18] M. D. Hestenes. Singer groups. *Canadian Journal of Mathematics*, 22(3):492–513, 1970.

[19] T. Honold, M. Kiermaier, and S. Kurz. Optimal binary subspace codes of length 6, constant dimension 3 and minimum distance 4. *Contemp. Math.*, 632:157–176, 2015.

[20] B. Huppert, B. *Endliche Gruppen.* Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Berucksichtigung der Anwendungsgebiete ; Bd. 134, v. 1. Springer, Berlin, Heidelberg, New York, 1967.

[21] W. M. Kantor. Linear groups containing a Singer cycle. *Journal of Algebra*, 62(1):232 – 234, 1980.

[22] R. Koetter and F. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory*, 54:3579 – 3591, 09 2008.

[23] Y. Li and H. Liu. Cyclic subspace codes via the sum of Sidon spaces, 2021.

[24] Y. Niu, Q. Yue, and Y. Wu. Several kinds of large cyclic subspace codes via Sidon spaces. *Discrete Mathematics*, 343(5):111788, 2020.

[25] K. Otal and F. Özbudak. Cyclic subspace codes via subspace polynomials. *Des. Codes Cryptography*, 85(2):191–204, Nov. 2017.

[26] R. M. Roth, N. Raviv, and I. Tamo. Construction of Sidon spaces with applications to coding. *IEEE Transactions on Information Theory*, 64(6):4412–4422, June 2018.

[27] N. Silberstein and A.-L. Horlemann-Trautmann. Subspace codes based on graph matchings, ferrers diagrams, and pending blocks. *IEEE Transactions on Information Theory*, 61, 04 2014.

[28] S. Thomas. Designs over finite fields. *Geometriae Dedicata*, 24:237–242, 1987.

[29] A.-L. Trautmann. Isometry and automorphisms of constant dimension codes. *Advances in Mathematics of Communications*, 7:147, 2013.

[30] A. L. Trautmann, F. Manganiello, M. Braun, and J. Rosenthal. Cyclic orbit codes. *IEEE Transactions on Information Theory*, 59(11):7386–7404, Nov 2013.

[31] W. Zhao and X. Tang. A characterization of cyclic subspace codes via subspace polynomials. *Finite Fields and Their Applications*, 57:1–12, 2019.

Vita

Hunter Ryan Lehmann

Place of Birth:

- Clarksville, TN

Education:

- University of Kentucky, Lexington, KY
  M.A. in Mathematics, May 2018
- Seattle University, Seattle, WA
  B.S. in Mathematics, June 2016
  Summa cum laude

Professional Positions:

- Graduate Teaching Assistant, University of Kentucky Fall 2016–Summer 2021

Honors

- Certificate for Outstanding Teaching, College of Arts and Sciences, University of Kentucky
- Enochs Scholarship in Algebra, Department of Mathematics, University of Kentucky
- John Ju Award, College of Science and Engineering, Seattle University
- Janet E. Mills Award for Undergraduate Research, Department of Mathematics, Seattle University

Publications & Preprints:

- H. Gluesing-Luerssen, H. Lehmann, *Automorphism groups and isometries for cyclic orbit codes*, submitted, 2021, arXiv:2101.09548.
- H. Gluesing-Luerssen, H. Lehmann, *Distance distributions of cyclic orbit codes*, Designs, Codes, and Cryptography, 89(3), 447-470 (2021)
- B. Larsen, H. Lehmann, A. Park, L. Robertson, *Coprime mappings on n-sets,* Integers, **17** (2017), Paper No. A51, 11 pp.
- S. Klee, H. Lehmann, A. Park, *Prime labeling of families of trees with the Gaussian integers,* AKCE International Journal of Graphs and Combinatorics, **13**, (2016), no. 2, 165–176.
- H. Lehmann, A. Park, *Prime labeling of small trees with the Gaussian integers,* Rose-Hulman Undergraduate Math Journal, **17** (2016), no. 1, 27pp.