2015

Analysis and Constructions of Subspace Codes

Carolyn E. Troha
University of Kentucky, cetroha@gmail.com

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.

Carolyn E. Troha, Student

Dr. Heide Gluesing-Luerssen, Major Professor

Dr. Peter Perry, Director of Graduate Studies

Analysis and Constructions of Subspace 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
Carolyn E. Troha
Lexington, Kentucky

Director: Dr. Heide Gluesing-Luerssen, Professor of Mathematics
Lexington, Kentucky 2015

ABSTRACT OF DISSERTATION

Analysis and Constructions of Subspace Codes

Random network coding is the most efficient way to send data across a network, but it is very susceptible to errors and erasures. In 2008, Kotter and Kschischang introduced subspace codes as an algebraic approach to error correcting in random network coding. Since this paper, there has been much work in constructing large subspace codes, as well as exploring the properties of such codes. This dissertation explores properties of one particular construction and introduces a new construction for subspace codes. We begin by exploring properties of irreducible cyclic orbit codes, which were introduced in 2011 by Rosenthal et al. As the name implies, irreducible cyclic orbit codes are the orbits of a group action of the general linear group on subspaces. By studying the stabilizers of this action, we formalize the notion of the stabilizer subfield of a subspace and utilize it to gain information about cardinality and distance of the code. Additionally, I define the linkage construction, which is recursive, and compare it to other subspace code constructions. In particular, we use the linkage construction to generalize some constructions of partial spreads. Finally, we address situations for which the linkage construction is efficiently decodable.

KEYWORDS: algebraic coding theory, random network coding, subspace codes, orbit codes, recursive construction

Author's signature: Carolyn E. Troha

Date: May 1, 2015

Analysis and Constructions of Subspace Codes

By
Carolyn E. Troha

Director of Dissertation: Heide Gluesing-Luerssen

Director of Graduate Studies: Peter Perry

Date: May 1, 2015

Dedicated to Sheri Rhine.

ACKNOWLEDGMENTS

First, I would like to thank my advisor, Dr. Heide Gluesing-Luerssen for all her help throughout all of my studies. I am thankful for her patience and for constantly pushing me to better than I ever thought I could be. I would not have complete this entire process if her excellent teaching had not captivated me, during my first year of study. I am also grateful to all the other members of my committee, Drs. Nagel, Enochs, Yoshida and Thompson, for their help throughout this process as well.

I would also like to thank all the professors who have given me great guidance throughout my studies, particularly Drs. Braun, Jensen, and Ponto, who have allowed me to complain and ask many silly questions. I could not have managed all the stress of graduate school without such great faculty support.

Now, I would like to thank many of my friends. First, I must thank Jay who kept me from dropping out of graduate school my first semester; I am not sure how I will ever repay him. Also, I thank Brad and Devin for making my office a place in which I enjoy being. Next, I thank Cliff, Rob and Robert for being my source of sanity and Sav's in a very crazy part of my life. Finally, I thank Sarah for everything you do but mostly for your love, kindness, warmth and hugs. I would not be at this point without the strength and support all my friends have provided. I will not soon forget the wonderful times shared playing Super Smash Brothers, attending Bible study or hiking and climbing.

Lastly, I must thank my parents for their undying love and support. Thank you to my father who has always been proud of me just for being myself. Your laugh, smile and proud thoughts have helped me stay strong through this whole process. Thank you for showing me the practical parts of life and keeping me grounded, without you I might just get lost in my mind. To my mother, thank you for always being

just a phone call away. You have dried my tears, laughed at my ridiculousness and understood me even when I don't understand myself. I am so very grateful that I am your spitting image because I cannot think of a better person to be. I really have no words to express how much both of you have made this dissertation possible.

TABLE OF CONTENTS

LIST OF FIGURES

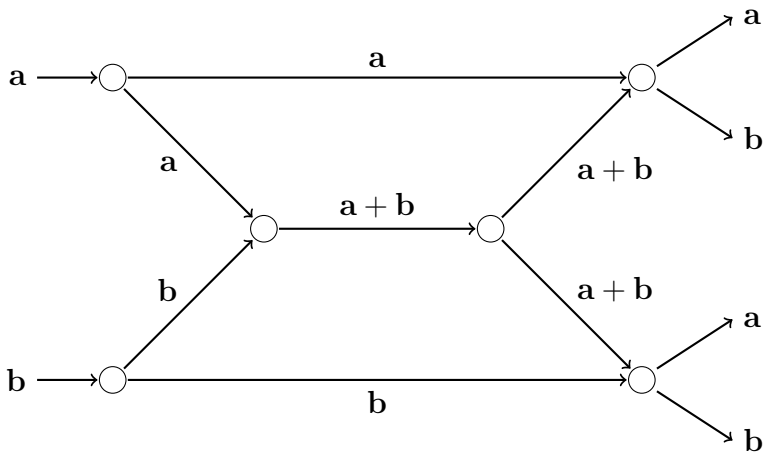
Chapter 1 Introduction

1.1 Random Network Coding

The purpose of algebraic coding theory is to use algebraic techniques to add mathematical redundancy to data, in order to account for errors and erasures that occur during the transmission of said data. Traditionally, coding theory was used for situations where there was one channel with only one input and output. In this situation, the appropriate mathematical redundancy to add is to encode a shorter data vector as a longer data vector. Thus codes are vector spaces and codewords are vectors.

However, in many modern uses, we have data that needs to travel from multiple sources to multiple sinks. Thus, we need to transmit data across a network rather than a single channel. Originally, data was transmitted through the process of routing, where a node would just send on one packet of data at a time. This is an inefficient way to send data, since only one route can be used at one time. In 2000, Ahlswede et. al. introduced the idea of network coding, which maximizes information flow across the network [1]. In this method, rather than having each node passing on the same packet, each node combines packets of data and sends on the combination of the data toward the sinks. Figure 1.1 gives an example of the butterfly network, a network for which network coding is more efficient, as well as, the packets and how each node combines the packets.

Figure 1.1: Information flow on the butterfly network, using network coding.



As we see in the butterfly network example, we take each packet **a** and **b** and send along the sum of the two packets when they come together. As we see, each

sink receives both $a + b$ and either a or b, so the sink can retrieve the original data, a and b. The idea of sending along information as a linear combination was introduced as linear network coding by Li, Yeung and Cai [24]. In this encoding scheme, which is now called random network coding, each node creates random linear combinations of the packets, with coefficients in a finite field. This scheme allows close to optimal throughput, i.e., the rate of successful message delivery over a communication channel. With a large field size the linear combinations have a high probability of being linearly independent, and thus containing unique data. All of these factors make random network coding a good encoding scheme for network coding.

1.2 History of Subspace Codes

While random network coding is a good choice of scheme for network coding, it is more susceptible to error propagation. Since one error will be combined into other linear combinations, errors are disseminated to many final sinks. Additionally, erasures are common when packets of data do not get correctly combined in the linear combinations. Thus, an algebraic approach to error correction for random network coding is required. In 2008, Kötter and Kschischang designed such an approach for error correcting in random network coding [23], which uses subspaces as the codewords. This approach makes sense, since the data needed at the sinks is the linear combinations of packets rather than the packets themselves. Since Kötter and Kschischang's paper there has been a great deal of activity studying collections of subspaces, known as subspace codes. Additionally, constant dimension codes can also be considered q-analogs of packing designs, and have been investigated in that context as well, see [5, 4]. The following will try to summarize many of the constructions and much of the literature on subspace codes.

In order to use collections of subspaces as codes, Kötter and Kschischang introduced the subspace distance as a metric on the projective geometry, that is, the set of all subspaces. Other metrics for the projective geometry were studied in [28] and bounds for these codes were studied in [21]. Improvements on some of these bounds were found in [12], as well as, providing additional constructions. Many constructions have been considered in attempts to find codes which attain these bounds. However, in most cases, such codes are not known and there continues to be activity in the area to try and make improvements on lower bounds for subspace codes.

In [29], Silva et al. introduced a type of subspace code, which is based on lifting rank metric codes, a type of matrix code, to subspace codes. Their construction re-

lied on a type of matrix code that had been introduced and studied by Gabidulin in [13]. For more information on these codes see Section 2.3 of this thesis. This lifting construction generalized the original construction given by Kötter and Kschischang [23] and provided an efficient decoding algorithm. While these lifted codes do not attain any of the known bounds, they are asymptotic to the bounds, which lead to further consideration of this construction. Eztion and Silberstein in [10], introduced the multilevel construction, which unions a lifted rank metric code with other modified lifted rank metric codes. This construction, called the multilevel construction or the lifted Ferrer's diagram rank metric code construction, improves on the cardinality of lifted MRD codes and is efficient to decode and so continues to be studied. The first improvement on Ferrer's diagram codes were given by Trautmann and Rosenthal in [34] and Etzion and Silberstein published other improvements in [11]. Recently, Silberstein and Trautmann have discovered some refinements to the multilevel construction which allow for even larger codes [27]. Additionally, Gorla and Ravagnani [17] and Wachter-Zeh and Etzion [36] have recently explored the underlying Ferrer's diagram rank metric codes and have found additional classes of maximal codes. This progress on the underlying rank metric codes may lead to better Ferrer's diagram subspace codes.

Skachek took a different approach to extending lifted rank metric codes, instead of trying to layer multiple lifted codes as Eztion and Silberstein did, he used a recursive process in [30]. While being decodable, these extended MRD codes are not as large the multilevel Ferrer's diagram codes constructed by Silberstein and Etzion and have not been studied further. Gorla et. al. completely left behind lifting matrix codes, and instead explored combinatorial spreads as subspace codes [16]. For more information on spread codes, see Section 2.4.

Trautmann et al. introduced a different construction of constant dimension codes, which generalized the idea of spread codes [33]. Their construction uses the orbits of a natural group action of $\mathrm{GL}_n(\mathbb{F}_q)$ on the projective geometry as a subspace codes. These codes are aptly named orbits codes. Rosenthal and Trautmann studied and classified the case where the matrix group is a(n) (irreducible) cyclic group in [26]. In Chapter 3, we will explore properties of such codes using a new technique. While cyclic orbit codes are small, there is some promise for encoding and decoding these codes, which can be found in [31], and they are the building blocks for cyclic codes, which have much better cardinality.

The idea of a cyclic subspace code was introduced in [12, Exa. 1-3]. Cyclic codes are subspace codes which are closed under the appropriate cyclic shift. For a more

precise definition see section 3.1, where we show that these codes are comprised of unions of cyclic orbit codes. The largest cyclic subspace codes beat many known lower bounds given by the multilevel construction, but are found mostly by computer search. In [2], Ben-Sasson et. al. explore a more algebraic approach to creating cyclic subspace codes. They use specific linearized polynomials to help create such codes, by exploiting the fact that the roots of a linearized polynomial are a subspace.

Kohnert and Kurz also created cyclic subspace codes by computer search, see [22]. However, they did not use the notion of cyclic codes, instead they found these codes by reducing and solving a linear programming problem. The major advance that Kohnert and Kurz made was to reduce the problem by prescribing the automorphism group of the entire code. In most cases, the group that they use is that of a singer cycle, i.e. an element of $\mathrm{GL}_n(\mathbb{F}_q)$ whose order is $q^n - 1$. In the cases when the automorphism group is generated by singer cycle, the authors get a cyclic code. In all cases, the codes are unions of orbit codes, but not always cyclic. Braun and Reichelt, in [5], used the same method, but they reduced the problem slightly less. Instead of prescribing the automorphism for the entire code, they only require part of the code to have the whole automorphism group; the rest of the code may only admit a subgroup as its automorphism group. By lessening the restriction, they are able to create codes very close to the known bounds, but their codes are not cyclic. Additionally, because there is not much structure to these codes, there are no known decoding algorithms for any computer search codes. Thus, most current research is moving away from strict computer search and looking for constructions with more algebraic structure.

So, we see that there are many different types of constructions for subspace codes. We will rely on many of these know constructions in later chapters, particularly Chapter 4. In this thesis, we will both analyze cyclic orbit codes, as well as, introduce a new construction. As we have seen, there are reasons to study cyclic orbit codes, as the building blocks of cyclic subspace codes and our new construction will be both recursive and decodable (in certain situations).

1.3 Thesis Outline

This thesis is organized as follows. Chapter 2 will introduce preliminary ideas we will use through the thesis. Specifically, we will formally define subspace codes and the tools to work with them. Then, we will discuss rank metric codes, a type of matrix code heavily used in subspace coding and two basic constructions of subspace codes,

lifted rank metric codes and spread codes.

In chapter 3, we will carefully analyze the construction of cyclic orbit codes. We will begin by defining the notion of β-cyclic orbit codes and showing the relationship between these codes and the codes introduced by Trautmann et. al. in [33]. Next, we will look at and define the notions of the stabilizer subfield, friends and best friends, as well as their relationship to the cardinality of a cyclic orbit code. We will conclude the chapter by looking at how the best friend can be used to consider the distance of a cyclic orbit code.

In chapter 4, we will introduce a recursive construction for subspace codes, called the linkage construction. We will give examples of this construction and compare it to some of the other methods mentioned above in terms of cardinality and other properties. We will show how the linkage construction nicely generalizes two constructions of partial spread codes and can be used to create both maximum and maximal partial spreads. Finally, we look into the decoding of linkage codes. While there are challenges to decoding in the general case, we show two cases that can be decoded.

Chapter 2 Preliminaries

In this chapter, we will go through some of the mathematical preliminaries we will need throughout this thesis. We start by fixing a finite field $\mathbb{F}_q$, where q is a power of a prime. We consider all vectors as row vectors. Thus $\mathbb{F}_q^n = \{(a_0, \ldots, a_{n-1}) \mid a_i \in \mathbb{F}_q\}$. Because of this, we always work with row spaces of matrices and we will denote the row space of a matrix $M \in \mathbb{F}_q^{k\times n}$ by

$$\operatorname{im}(M) := \{vM \mid v \in \mathbb{F}_q^k\}.$$

Lastly, we use $\mathbb{F}_q^{k\times n}$ to denote the set of k by n matrices with entries in $\mathbb{F}_q$ and $\mathrm{GL}_n(\mathbb{F}_q) \subset \mathbb{F}_q^{n\times n}$ to denote the general linear group, that is, the group invertible matrices.

2.1 Subspace Codes

For a $\mathbb{F}_q$-vector space $\mathcal{W}$ of dimension n, we define the *projective geometry*, denoted $\mathbb{PG}(\mathcal{W})$, as the set of subspaces of $\mathcal{W}$. Most often people work with $\mathcal{W} = \mathbb{F}_q^n$, in which case we denote $\mathbb{PG}(\mathcal{W}) = \mathbb{PG}(q, n)$. However, in Chapter 3, we will let $\mathcal{W} = \mathbb{F}_{q^n}$. We define the *Grassmannian*, denoted $\mathcal{G}_q(n, k)$, as the set of k-dimensional subspaces of $\mathcal{W}$. Thus

$$\mathbb{PG}(\mathcal{W}) = \bigcup_{k=0}^{n} \mathcal{G}_q(n, k).$$

While not necessary to our discussion, we should note that the cardinality of the Grassmannian is given by the Gaussian binomial coefficient, i.e., $|\mathcal{G}_q(n, k)| = \begin{bmatrix} n \\ k \end{bmatrix}_q$. Because of this fact, there are many connections between network coding and q-analogs in combinatorics, some of which we will explore later.

For any two subspace $\mathcal{U}, \mathcal{V} \in \mathbb{PG}(\mathcal{W})$, we define the *subspace distance* between them as

$$\mathrm{d}_S(\mathcal{U}, \mathcal{V}) := \dim \mathcal{U} + \dim \mathcal{V} - 2\dim(\mathcal{U} \cap \mathcal{V}). \tag{2.1}$$

Equivalently, $\mathrm{d}_S(\mathcal{U}, \mathcal{V}) = \dim(\mathcal{U} + \mathcal{V}) - \dim(\mathcal{U} \cap \mathcal{V})$. From our discussion in the introduction, we can think of the subspace distance as the number of insertions and deletions needed to transform a basis of $\mathcal{U}$ into a basis of $\mathcal{V}$. We see that two spaces are close together if they intersect greatly, which is to say that both have bases that differs by very few vectors. Notice that we must subtract twice the dimension of the

intersection so that $\mathrm{d}_S(\mathcal{U},\mathcal{U}) = 0$. It can be shown that the subspace distance is a metric, see [23, Lemma 1], which makes it useful in decoding. However, the subspace distance is not the only distance in use.

The other major distance is the injection distance, which is defined as

$$\mathrm{d}_\mathrm{I}(\mathcal{U},\mathcal{V}) := \max\{\dim(\mathcal{U}),\dim(\mathcal{V})\} - \dim(\mathcal{U}\cap\mathcal{V}),$$

for $\mathcal{U},\mathcal{V} \in \mathbb{PG}(\mathcal{W})$. It is easy to see that $\mathrm{d}_S(\mathcal{U},\mathcal{V}) \leq 2\mathrm{d}_\mathrm{I}(\mathcal{U},\mathcal{V})$ and if $\dim(\mathcal{U}) = \dim(\mathcal{V})$ then $\mathrm{d}_S(\mathcal{U},\mathcal{V}) = 2\mathrm{d}_\mathrm{I}(\mathcal{U},\mathcal{V})$. Because of this relationship, we will choose to work with the subspace distance throughout this thesis.

Now we move on to formally defining a subspace code.

Definition 1. A *subspace code of length* n is a nonempty subset of $\mathbb{PG}(\mathcal{W})$. A code is called *constant dimension* if all subspaces have the same dimension, i.e., it is contained in a single Grassmannian. The *subspace distance* of a subspace code $\mathcal{C}$ is defined as

$$\mathrm{d}_S(\mathcal{C}) := \min\{\mathrm{d}_S(\mathcal{U},\mathcal{V}) \mid \mathcal{U},\,\mathcal{V}\in\mathcal{C}, \mathcal{U}\neq\mathcal{V}\}.$$

We call a subspace code of length n, with cardinality N and distance d a $(n,N,d)_q$-subspace code. If it is of a constant dimension k, we call it a $(n,N,d,k)_q$-subspace code.

Throughout this thesis we will work most commonly with constant dimension subspace codes. Thus, we make the following observations about the subspace distance for these codes. If $\dim\mathcal{U} = \dim\mathcal{V} = k$, then

$$\mathrm{d}_S(\mathcal{U},\mathcal{V}) = 2(k - \dim(\mathcal{U}\cap\mathcal{V})) = 2\big(\dim(\mathcal{U}+\mathcal{V}) - k\big).$$

Hence, if $\mathcal{C}$ is a constant dimension code of dimension k then

$$\mathrm{d}_S(\mathcal{C}) \leq \min\{2k,\, 2(n-k)\}. \tag{2.2}$$

As with traditional error correcting codes, there is a notion of a dual code. The *dual* of a subspace code $\mathcal{C}$ is defined as

$$\mathcal{C}^\perp := \{\mathcal{U}^\perp \mid \mathcal{U}\in\mathcal{C}\}. \tag{2.3}$$

It is easy to see that $\mathrm{d}_S(\mathcal{U}^\perp,\mathcal{V}^\perp) = \mathrm{d}_S(\mathcal{U},\mathcal{V})$, and therefore $\mathrm{d}_S(\mathcal{C}) = \mathrm{d}_S(\mathcal{C}^\perp)$. Additionally, the length of the code remains unchanged. However, the dimension of each subspace is changed to be $n-k$. Thus, we can easily assume, without loss of generality, that our $(n,N,d,k)_q$-codes satisfy, $k \leq \frac{n}{2}$. Otherwise, we can take the dual code which will have the same distance.

When we let $\mathcal{W} = \mathbb{F}_q^n$, we say two subspace codes $\mathcal{C}, \mathcal{C}'$ of length n are *linearly isometric* if there exists an $\mathbb{F}_q$-linear isomorphism $\psi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ such that $\mathcal{C}' = \{\psi(\mathcal{U}) \mid \mathcal{U} \in \mathcal{C}\}$ (see also [32, Def. 2.9]). We know that this linear isomorphism preserves dimensions of subspaces and thus preserves the distance between any two subspaces. Hence, linearly isometric codes have the same subspace distance and even the same distance distribution, i.e., the list of all distances between any two distinct subspaces in $\mathcal{C}$ coincides up to order with the corresponding list of $\mathcal{C}'$. Thus we consider linearly isometric codes to be the same. Multiplying by an invertible matrix is a type of linear isometry, so often we look for this type of transformation to show codes are linearly isometric.

2.2 Finite Fields

Since we will be working with $\mathbb{F}_{q^n}$ in Chapter 3, we will go over some basic facts about $\mathbb{F}_{q^n}$ that we will rely on later. First, we note that $\mathbb{F}_{q^n}$ is a n-dimensional vector space over $\mathbb{F}_q$, since it is a degree n field extension. We denote the multiplicative identity of $\mathbb{F}_q$ as 1 and the multiplicative group of $\mathbb{F}_{q^n}$ as $\mathbb{F}_{q^n}^* = \mathbb{F}_{q^n} \backslash \{0\}$.

Recall that $\mathbb{F}_{q^n}^*$ is a cyclic group and we call any α which generates $\mathbb{F}_{q^n}^*$ a *primitive element*. For an element $\beta \in \mathbb{F}_{q^n}^*$, we denote its order by $|\beta|$ and the cyclic group generated by β as $\langle\beta\rangle := \{\beta^i \mid i = 0, \ldots, |\beta| - 1\}$. Thus if α is primitive then $\langle\alpha\rangle = \mathbb{F}_{q^n}^*$. Also it should be noted that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for $\mathbb{F}_{q^n}$ as $\mathbb{F}_q$-vector space.

We will use the following $\mathbb{F}_q$-isomorphism:

$$\varphi : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_q^n, \quad \sum_{i=0}^{n-1} a_i \alpha^i \longmapsto (a_0, \ldots, a_{n-1}). \tag{2.4}$$

Since α is primitive we know that its minimal polynomial has degree n. Let $f = f_0 + f_1 x + \cdots + f_{n-1} x^{n-1} + x^n$ be the minimal polynomial of α, which we will refer to as a primitive polynomial, since it has a primitive root. Let $M_f \in \mathrm{GL}_n(\mathbb{F}_q)$ be the companion matrix of f, thus

$$M_f = \begin{pmatrix} 0 & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ -f_0 & -f_1 & -f_2 & \ldots & -f_{n-1} \end{pmatrix}. \tag{2.5}$$

Note that this companion matrix is the transpose of the classical companion matrix, since we use row vectors instead of column vectors. Additionally, we can define M_f for any irreducible polynomial of degree n, not just for primitive polynomials.

Finally, recall that if $r|n$ then there is exactly one subfield of $\mathbb{F}_{q^n}$ with cardinality q^r and any subfield of $\mathbb{F}_{q^n}$ is of the form $\mathbb{F}_{q^r}$ where $r|n$. This fact about subfields will play a large role in Chapter 3.

2.3 Rank Metric Codes and Lifted Rank Metric Codes

In this section, we define a type of matrix code which is greatly used in network coding. We will use $\mathbb{F}_q^{k\times n}$ to denote the space of k by n matrices with entries in $\mathbb{F}_q$. We begin be defining the rank distance for two matrices $X, Y \in \mathbb{F}_q^{k\times n}$ as

$$\mathrm{d}_R(X,Y) := \mathrm{rank}\,(X-Y).$$

It is shown in [13] that this is indeed a metric on this matrix space.

Definition 2. A *rank metric code*, $\mathcal{C}$, is a non-empty subset of $\mathbb{F}_q^{k\times n}$ endowed with the rank metric. We define the distance of $\mathcal{C}$ as

$$\mathrm{d}_R(\mathcal{C}) := \min\{\mathrm{d}_R(X,Y) \mid X,Y \in \mathcal{C},\, X \neq Y\}.$$

Notice that $k \leq n$ or vice versa, but for the purposes of this thesis we will be concerned only with the former case. It is well known that rank metric codes satisfy a version of the Singleton bound (see [13, 7]). This bound states that for a code $\mathcal{C} \subset \mathbb{F}_q^{k\times n}$ with distance d and $k \leq n$ we have

$$|\mathcal{C}| \leq q^{n(k-d+1)}.$$

Codes which meet this bound are called *maximum rank distance codes*, which we abbreviate as MRD codes. A well studied class of MRD codes are the Gabidulin codes presented in [13]. While these codes are originally given as vector codes, we can easily convert them to matrix codes. One reason this class of codes is well studied is that Gabidulin presents an efficient decoding algorithm for them in [13]. Other types of MRD codes have been found by de la Cruz et al. [6] and Hernandez/Sison [19] but as of yet do not have decoding algorithms. We will use MRD codes in Chapter 4, but they are also used to construct subspace codes.

To construct a subspace code from a rank metric code, we use the process of lifting which Kötter and Kschischang utilized in their seminal paper [23]. For $X \in \mathbb{F}_q^{k\times n}$ we

define its lifting as the subspace

$$\Lambda(X) := \mathrm{im}\,(I_k \mid X),$$

where $\mathrm{im}\,(Y)$ is used to denote the row space of Y. We extend this lifting process to an entire rank metric code $\mathcal{C}$ by

$$\Lambda(\mathcal{C}) := \{\Lambda(X) \mid X \in \mathcal{C}\}.$$

We call $\Lambda(\mathcal{C})$ a lifted rank metric code and observe that it is always a constant dimension code. In [29], Silva, Kschischang, and Kötter show that for $X, Y \in \mathbb{F}_q^{k\times n}$,

$$\mathrm{d}_S(\Lambda(X), \Lambda(Y)) = 2\mathrm{d}_R(X, Y),$$

so we know that $\mathrm{d}_S(\Lambda(\mathcal{C})) = 2\mathrm{d}_R(\mathcal{C})$, for any rank metric code $\mathcal{C} \subset \mathbb{F}_q^{k\times n}$. Additionally, they provide an efficient decoding algorithm for lifted rank metric codes, where $\mathcal{C}$ is a Gabidulin code. Many other constructions of subspace codes, such as the multilevel construction [11], are based on the idea of lifting rank metric codes.

2.4 Spread and Partial Spread Codes

A $P_q(t, k, n)$ q-packing design is a selection of k-subspaces of $\mathbb{F}_q^n$ such that each t-subspace is contained in at most one element of the collection. These packing designs are the q-analogs of traditional packing designs, which have been studied in combinatorics. It is easy to see that a $P_q(t, k, n)$ q-packing design with cardinality N is a $(n, N, d, k)_q$ subspace code, where $d \geq 2(k - t + 1)$. Hence, we can use packing designs as codes, and codes as packing designs. If we make the restriction that each 1-subspace is contained in at most one element of the collection we get what we call a partial spread. When considered as a code a partial spread is a $(n, N, 2k, k)_q$ constant dimension code. If we require that each 1-subspace is contained in exactly one subspace then the partial spread is called a spread. Another characterization of spreads is that they are collections of subspaces of the same dimension which partition $\mathbb{F}_q^n$. We will use the following definition of spread codes and partial spread codes.

Definition 3. A subspace code $\mathcal{C}$ of constant dimension, k, is a *partial spread code* if $\mathrm{d}_S(\mathcal{C}) = 2k$. A partial spread code $\mathcal{C}$ which also satisfies $\bigcup_{\mathcal{U}\in\mathcal{C}} \mathcal{U} = \mathbb{F}_q^n$ is called a *spread code.*

It is well known that a spread exists only if k divides n, see [20]. When spreads exist they are optimal subspace codes, meeting the Singelton bound for subspace

codes, [25]. Spreads were originally studied as subspace codes in [25], and later the same authors devise a decoding algorithm for a specific type of spread codes [16].

Unlike spread codes, partial spread codes are not very well studied. Beutelspacher studied partial spreads in [3] and more recently El-Zanati et. al. found maximum partial spreads for the case $q = 2$, $k = 3$ [9]. Additionally, Etzion and Vardy give a construction of a partial spread code in [12, Thm. 11], as do Gorla and Ravagnani in [18]. Currently little is known about the maximum sizes of these codes and so they have been less well studies than spread codes. We will explore partial spread more in depth in Section 4.2.

Chapter 3 Cyclic Orbit Codes and Stabilizer Subfields

In this chapter, we will explore the cardinality and distance of cyclic orbit codes, which were introduced in [26]. We will begin by defining the orbit codes that we will explore more in depth.

3.1 β-Cyclic Orbit Codes

First, we consider the field extension $\mathbb{F}_{q^n}$. For the majority of this chapter, we will consider our subspace codes as being subsets of $\mathbb{PG}(\mathbb{F}_{q^n})$. Recall from Section 2.2 that $\mathbb{F}_q^n \cong \mathbb{F}_{q^n}$ as vector spaces of $\mathbb{F}_q$. Later, we will translate between these two situations more explicitly.

As the name suggests, cyclic orbit codes arise from the orbits of the following group action on $\mathbb{PG}(\mathbb{F}_{q^n})$ by $\mathbb{F}_{q^n}$. Since elements of $\mathbb{PG}(\mathbb{F}_{q^n})$ are subspaces of $\mathbb{F}_{q^n}$, vectors are just elements of the field $\mathbb{F}_{q^n}$. Let $\mathcal{U} \in \mathbb{PG}(\mathbb{F}_{q^n})$ and $\beta \in \mathbb{F}_{q^n}$, then

$$\mathcal{U}\beta := \{u\beta \mid u \in \mathcal{U}\},$$

where $u\beta$ is just the standard multiplication in $\mathbb{F}_{q^n}$. As we can see, $\dim(\mathcal{U}) = \dim(\mathcal{U}\beta)$. Now we have the tools to define cyclic orbit codes.

Definition 4. Fix an element β of $\mathbb{F}_{q^n}^*$. Let $\mathcal{U}$ be a subspace of the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^n}$. The *β-cyclic orbit code* generated by $\mathcal{U}$ is defined as the set

$$\mathrm{Orb}_\beta(\mathcal{U}) := \{\mathcal{U}\beta^i \mid i = 0, 1, \ldots, |\beta| - 1\}. \tag{3.1}$$

If β is primitive, thus $\langle\beta\rangle = \mathbb{F}_{q^n}^*$, we drop the specifier β and simply write $\mathrm{Orb}(\mathcal{U})$ instead of $\mathrm{Orb}_\beta(\mathcal{U})$ and call the code a *cyclic orbit code*. If the specific value of β does not matter we will also simply call the code in (3.1) a *cyclic orbit code*.

A cyclic orbit code is a constant dimension code, because as we noted before, the group action does not affect dimension. We should also mention that when β is primitive we may indeed drop the β notation because any other choice of primitive element will lead to the same code under the isomorphism. Certain β-cyclic orbit codes were introduced as irreducible cyclic orbit codes in [26, 33]. However, the authors consider these codes as subspaces of $\mathbb{F}_q^n$. Here we explore the relationship between the two.

In [26, 33] the authors introduce orbit codes in $\mathbb{F}_q^n$ with respect to a subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$. They use the following group action on $\mathbb{PG}(q,n)$ by $\mathrm{GL}_n(\mathbb{F}_q)$ defined as

$$\mathcal{U}M := \{uM \mid u \in \mathcal{U}\}.$$

If we write $\mathcal{U} = \mathrm{im}\,(U)$ for some $U \in \mathbb{F}_q^{k\times n}$, then $\mathcal{U}M = \mathrm{im}\,(UM)$. The orbit of a subgroup under this action is called an *orbit code*. An orbit code is called *cyclic* if the subgroup is cyclic and *irreducible* if the subgroup is irreducible (see [33, Def. 20] for irreducibility of groups and matrices). As it turns out, every irreducible cyclic matrix group is conjugate to a group of the form $\langle M_f\rangle$, where M_f is the companion matrix of an irreducible polynomial, (again see [33]). As we will see, under the isomorphism φ in (2.4), a restriction of our β-cyclic orbit codes are exactly these codes.

To see this, we let $\beta \in \mathbb{F}_{q^n}^*$ be an irreducible element, i.e. an element such that its minimal polynomial has degree n. In other words $\mathbb{F}_q[\beta] = \mathbb{F}_{q^n}$. (Note this is a restriction on β and that all primitive β are also irreducible.) We write the minimal polynomial of β as $f = x^n + \sum_{i=0}^{n-1} f_i x^i \in \mathbb{F}_q[x]$. Recall from Section 2.2, that $\mathbb{F}_{q^n} \cong \mathbb{F}_q^n$, by the isomorphism φ (2.4). We notice that multiplication by β in $\mathbb{F}_{q^n}$ is the same as multiplication by M_f in $\mathbb{F}_q^n$ under our isomorphism φ.

Additionally, for any subspace $\mathcal{U}$ of $\mathbb{F}_{q^n}$, we can write $\varphi(\mathcal{U})$ as $\varphi(\mathcal{U}) = \mathrm{im}\,(U)$ for a suitable matrix $U \in \mathbb{F}^{k\times n}$ of rank k. Our group action becomes $\varphi(\mathcal{U}\beta) = \mathrm{im}\,(UM_f)$, where M_f is as in (2.5), which is the same action as in [26, 33]. Thus, under the isomorphism (2.4) the orbit code $\mathrm{Orb}_\beta(\mathcal{U})$ simply becomes

$$\{\mathrm{im}\,(UM_f^i) \mid 0 \le i \le |\beta| - 1\}, \tag{3.2}$$

which is exactly an irreducible cyclic orbit code by the definition in [26, 33]. In other words, the action of the cyclic group $\langle\beta\rangle \le \mathbb{F}_{q^n}^*$ on subspaces in $\mathbb{F}_{q^n}$ turns into the action of the cyclic group $\langle M_f\rangle \le \mathrm{GL}_n(\mathbb{F}_q)$ on subspaces in $\mathbb{F}^n$. Thus it makes sense to study our β-cyclic orbit codes in greater depth as they have been characterized in [26].

Though cyclic orbit codes are in general larger than β-cyclic orbit codes, we believe that is worth studying the latter as well because they provide us with a larger pool of codes.

We also wish to mention that in [12, p. 1170], Etzion and Vardy study codes that are closely related to those introduced in Definition 4. They define a *cyclic subspace code* in $\mathbb{F}_{q^n}$ to be a subspace code that is invariant under cyclic shifts, that is, if $\mathcal{U} \in \mathcal{C}$ then $\mathcal{U}\beta \in \mathcal{C}$ for a primitive $\beta \in \mathbb{F}_{q^n}$. We note that $\mathrm{Orb}(\mathcal{U})$ includes all cyclic shifts of $\mathcal{U}$, but $\mathrm{Orb}_\beta(\mathcal{U})$ does not include all cyclic shifts, if β is not primitive. Hence, using

our definitions, a cyclic subspace code is simply a union of cyclic orbit codes, i.e., $\mathcal{C} = \bigcup_{t=1}^{T} \mathrm{Orb}(\mathcal{U}_t)$. In [12] the authors do not require that $\mathcal{C}$ be a constant dimension code, hence $\mathcal{U}_1, \ldots, \mathcal{U}_T$ may have different dimensions. Obviously, cyclic subspace codes are more general than cyclic orbit codes.

We close this section with the following simple fact.

Remark 5. The dual (in the sense of (2.3)) of an orbit code is an orbit code again. Indeed, for any subspace $\mathcal{U} \in \mathbb{F}_q^n$ and matrix $A \in \mathrm{GL}_n(\mathbb{F}_q)$ we have $(\mathcal{U}A)^\perp = \mathcal{U}^\perp (A^\mathsf{T})^{-1}$. Moreover, $A^\mathsf{T} = SAS^{-1}$ for some $S \in \mathrm{GL}_n(\mathbb{F}_q)$, since A and A^T have the same characteristic polynomial [26]. Therefore $\mathrm{Orb}_\beta(\mathcal{U})^\perp$ is linearly isometric to $\mathrm{Orb}_\beta(\mathcal{U}^\perp)$; see also [33, Thm. 18].

As a consequence, we may and will restrict ourselves to orbit codes generated by a subspace $\mathcal{U}$ with $\dim \mathcal{U} \leq n/2$.

3.2 Stabilizer Subfield and Cardinality of β-Cyclic Orbit Codes

In this section, we explore the cardinality of a β-cyclic orbit code. We begin by fixing an element β of $\mathbb{F}_{q^n}^* \backslash \{1\}$ and a k-dimensional subspace $\mathcal{U}$ of $\mathbb{F}_{q^n}$. Consider its β-cyclic orbit code $\mathrm{Orb}_\beta(\mathcal{U})$. We will mainly restrict ourselves to subspaces $\mathcal{U}$ that contain the identity $1 \in \mathbb{F}_{q^n}$, which will simplify later considerations of the cardinality of the orbit code. Notice if $1 \notin \mathcal{U}$ then for any nonzero element $u \in \mathcal{U}$ the subspace $\tilde{\mathcal{U}} := \mathcal{U}u^{-1}$ contains 1. If β is primitive then $u^{-1} \in \langle \beta \rangle$ and $\tilde{\mathcal{U}} \in \mathrm{Orb}(\mathcal{U})$, so we could choose $\tilde{\mathcal{U}}$ and not change the code. Thus $1 \in \mathcal{U}$ is not a restriction at all in this case. However, if β is not primitive, we have a linear isometry between $\mathrm{Orb}_\beta(\mathcal{U})$ and $\mathrm{Orb}_\beta(\tilde{\mathcal{U}})$ given by multiplication by u^{-1}, because $\tilde{\mathcal{U}}\beta^i = \mathcal{U}\beta^i u^{-1} = \mathcal{U}u^{-1}\beta^i$.

Recall that the stabilizer of the subspace $\mathcal{U}$ under the action induced by $\langle \beta \rangle$ is defined as

$$\mathrm{Stab}_\beta(\mathcal{U}) := \{\gamma \in \langle \beta \rangle \mid \mathcal{U}\gamma = \mathcal{U}\} = \{\gamma \in \langle \beta \rangle \mid \mathcal{U}\gamma \subseteq \mathcal{U}\}. \tag{3.3}$$

The stabilizer is clearly a subgroup of $\langle \beta \rangle$. So, there must exist a minimal $N \in \mathbb{N}$ such that $\mathrm{Stab}_\beta(\mathcal{U}) = \langle \beta^N \rangle$. By the properties of cyclic groups, N divides $|\beta|$. Then, by the orbit-stabilizer theorem for group actions,

$$\begin{cases} |\mathrm{Stab}_\beta(\mathcal{U})| = \frac{|\beta|}{N}, \\ \mathrm{Orb}_\beta(\mathcal{U}) = \{\mathcal{U}\beta^i \mid i = 0, \ldots, N-1\}, \quad |\mathrm{Orb}_\beta(\mathcal{U})| = N. \end{cases} \tag{3.4}$$

Since $\mathbb{F}_q^*$ is in the stabilizer of any subspace $\mathcal{U}$, we have $|\mathrm{Orb}_\beta(\mathcal{U})| \leq \frac{q^n-1}{q-1}$, and this upper bound is achieved if and only if β is primitive and $\mathrm{Stab}_\beta(\mathcal{U}) = \mathbb{F}_q^*$. We will

obtain more information about the cardinality based on the given subspace $\mathcal{U}$ with the help of the following notion.

Definition 6. Let $\mathrm{Stab}_\beta^+(\mathcal{U})$ be the smallest subfield of $\mathbb{F}_{q^n}$ containing $\mathbb{F}_q$ and the group $\mathrm{Stab}_\beta(\mathcal{U})$. We call $\mathrm{Stab}_\beta^+(\mathcal{U})$ the *stabilizer subfield* of $\mathcal{U}$ with respect to β.

Note that $\mathrm{Stab}_\beta^+(\mathcal{U})$ is the field extension $\mathbb{F}_q[\beta^N]$, where N is such that $\langle\beta^N\rangle = \mathrm{Stab}_\beta(\mathcal{U})$. If $\gamma \in \mathrm{Stab}_\beta^+(\mathcal{U})$ then $\gamma = \sum_{i=0}^l a_i\gamma_i$, where $\gamma_i \in \mathrm{Stab}_\beta(\mathcal{U})$ and $a_i \in \mathbb{F}_q$. Then $\mathcal{U}\gamma = \mathcal{U}\sum_{i=0}^l a_i\gamma_i \subset \sum_{i=0}^l \mathcal{U}a_i\gamma_i = \sum_{i=0}^l \mathcal{U} = \mathcal{U}$. Hence, $\mathcal{U}$ is a vector space over $\mathrm{Stab}_\beta^+(\mathcal{U})$.

We will drop the subscript β from the stabilizer and the stabilizer subfield and simply write $\mathrm{Stab}(\mathcal{U})$ and $\mathrm{Stab}^+(\mathcal{U})$ when β is primitive to be in line with our notation for $\mathrm{Orb}(\mathcal{U})$ in this case. The identities in (3.3) and (3.4) then read as

$$\begin{cases} \mathrm{Stab}(\mathcal{U}) = \{\gamma \in \mathbb{F}_{q^n}^* \mid \mathcal{U}\gamma = \mathcal{U}\}, \\ \mathrm{Orb}(\mathcal{U}) = \{\mathcal{U}\beta^i \mid i = 0, \ldots, L-1\}, \text{ where } L = \frac{q^n-1}{|\mathrm{Stab}(\mathcal{U})|}. \end{cases} \tag{3.5}$$

In this case, both the stabilizer and the orbit do not depend on the choice of the primitive element β. This case turns out to be much easier to handle than the case of general β-cyclic orbit codes because of the following result about $\mathrm{Stab}^+(\mathcal{U})$.

Lemma 7. *Let $\mathcal{U}$ be a subspace of $\mathbb{F}_{q^n}$ such that $1 \in \mathcal{U}$. Then $\mathrm{Stab}^+(\mathcal{U}) = \mathrm{Stab}(\mathcal{U}) \cup \{0\}$ and $\mathrm{Stab}^+(\mathcal{U})$ is contained in $\mathcal{U}$. Moreover, $\mathcal{U}$ is a vector space over $\mathrm{Stab}^+(\mathcal{U})$ with scalar multiplication being the multiplication of the field $\mathbb{F}_{q^n}$.*

Proof. We know that $\mathrm{Stab}(\mathcal{U}) = \{\gamma \in \mathbb{F}_{q^n}^* \mid \mathcal{U}\gamma = \mathcal{U}\}$ is a subgroup of $\mathbb{F}_{q^n}^*$ and contains $\mathbb{F}_q^*$. Thus, for the first statement it remains to show that $\mathrm{Stab}(\mathcal{U}) \cup \{0\}$ is closed under addition. Let $\gamma, \gamma' \in \mathrm{Stab}(\mathcal{U})$, i.e., $\mathcal{U}\gamma = \mathcal{U} = \mathcal{U}\gamma'$. If $\gamma + \gamma' = 0$, then $\gamma + \gamma' \in \mathrm{Stab}(\mathcal{U}) \cup \{0\}$, and we are done. Now let $\gamma + \gamma' \neq 0$. In this case $\mathcal{U}(\gamma + \gamma') \subseteq \mathcal{U}\gamma + \mathcal{U}\gamma' = \mathcal{U} + \mathcal{U} = \mathcal{U}$, so $\gamma + \gamma' \in \mathrm{Stab}(\mathcal{U})$. All of this shows that $\mathrm{Stab}(\mathcal{U}) \cup \{0\} \subset \mathbb{F}_{q^n}$ is closed under multiplication and addition, making it a subfield, and in fact the smallest subfield containing $\mathrm{Stab}(\mathcal{U})$. So $\mathrm{Stab}^+(\mathcal{U}) = \mathrm{Stab}(\mathcal{U}) \cup \{0\}$. Since $1 \in \mathcal{U}$, we know for $\beta^i \in \mathrm{Stab}(\mathcal{U})$ that $1\beta^i \in \mathcal{U}\beta^i = \mathcal{U}$, so $\mathrm{Stab}^+(\mathcal{U})$ is contained in $\mathcal{U}$. Also $u\beta^i \in \mathcal{U}\beta^i = \mathcal{U}$ so $\mathcal{U}$ is a vector space over $\mathrm{Stab}^+(\mathcal{U})$. ∎

Note that as a result of this statement, if $\mathrm{Stab}(\mathcal{U})$ is the trivial group, then the stabilizer subfield $\mathrm{Stab}^+(\mathcal{U}) = \{0, 1\} = \mathbb{F}_2$, which is only possible if $q = 2$. This also follows from the fact that $\mathbb{F}_q^*$ is contained in the stabilizer of any subspace $\mathcal{U}$.

Another case that we know from this theorem is when n is prime. Then the only proper subfield of $\mathbb{F}_{q^n}$ is $\mathbb{F}_q$. Thus, we have the following corollary.

Corollary 8. *If n is prime, then* $\mathrm{Stab}(\mathcal{U}) = \mathbb{F}_q^*$*, and thus* $|\mathrm{Orb}(\mathcal{U})| = \frac{q^n-1}{q-1}$ *for every proper subspace* $\mathcal{U} \subset \mathbb{F}_{q^n}$*.*

Now we will return to general $\beta \in \mathbb{F}_{q^n}^* \backslash \{1\}$. Since $\langle\beta\rangle \subset \mathbb{F}_{q^n}$, we have the following containments $\mathrm{Stab}_\beta(\mathcal{U}) \subseteq \mathrm{Stab}(\mathcal{U}) \subseteq \mathrm{Stab}^+(\mathcal{U})$, which lead immediately to the following situation for the general case.

Corollary 9. *For any* $\beta \in \mathbb{F}_{q^n} \backslash \{1\}$*, the stabilizer subfield* $\mathrm{Stab}_\beta^+(\mathcal{U})$ *is contained in* $\mathrm{Stab}^+(\mathcal{U})$*. Hence, if* $1 \in \mathcal{U}$ *then* $\mathrm{Stab}_\beta^+(\mathcal{U})$ *is contained in* $\mathcal{U}$ *and* $\mathcal{U}$ *is a vector space over this field.*

The next example shows that the containment $\mathrm{Stab}_\beta^+(\mathcal{U}) \subseteq \mathrm{Stab}^+(\mathcal{U})$ may be strict.

Example 10. Consider $\mathbb{F}_q = \mathbb{F}_3$ and $\mathbb{F}_{q^n} = \mathbb{F}_{3^4}$. Fix the primitive element α with minimal polynomial $x^4 + x + 2$. Consider $\beta := \alpha^{16}$, which has order 5. Let $\mathcal{U}$ be the subfield $\mathbb{F}_{3^2}$ (considered as a subspace of $\mathbb{F}_{3^4}$). Then clearly $\mathrm{Stab}^+(\mathcal{U}) = \mathbb{F}_{3^2}$. Moreover, since $1 \in \mathcal{U}$, any γ satisfying $\mathcal{U}\gamma = \mathcal{U}$ is already in $\mathcal{U}$. But then the relative primeness of the orders of the groups $\langle\beta\rangle$ and $\mathbb{F}_{3^2}^*$ show that $\mathrm{Stab}_\beta(\mathcal{U}) = \{1\}$. As a consequence, $\mathrm{Stab}_\beta^+(\mathcal{U}) = \mathbb{F}_3$. Thus we see that $\mathrm{Stab}_\beta^+(\mathcal{U}) \subsetneq \mathrm{Stab}^+(\mathcal{U})$.

We have the following results pertaining to the cardinality of a β-cyclic orbit code.

Proposition 11. *Let* $\beta \in \mathbb{F}_{q^n}^*$ *and let* $\mathcal{U}$ *be a* k*-dimensional subspace of* $\mathbb{F}_{q^n}$ *such that* $1 \in \mathcal{U}$*. Then*

$$\frac{|\beta|}{\gcd(|\beta|, q^k - 1)} \quad \textit{divides} \quad |\mathrm{Orb}_\beta(\mathcal{U})|.$$

Assume now that k *divides* n*, and thus* $\mathbb{F}_{q^k}$ *is a subfield of* $\mathbb{F}_{q^n}$*.*

(a) If $\mathbb{F}_{q^k}^* \subseteq \langle\beta\rangle$ *then* $\frac{|\beta|}{q^k-1}$ *divides* $|\mathrm{Orb}_\beta(\mathcal{U})|$*.*

(b) $|\mathrm{Orb}_\beta(\mathcal{U})| = \frac{|\beta|}{q^k-1}$ *if and only if* $\mathcal{U} = \mathbb{F}_{q^k}$*.*

Proof. From Corollary 9 we know that $\mathrm{Stab}_\beta^+(\mathcal{U}) = \mathbb{F}_{q^r}$ for some r and that $\mathcal{U}$ is a vector space over $\mathbb{F}_{q^r}$. Thus r divides k and so $q^r - 1$ divides $q^k - 1$. Additionally, since $\mathrm{Stab}_\beta(\mathcal{U})$ is a subgroup of $\mathbb{F}_{q^r}^* \cap \langle\beta\rangle$, its order divides $q^r - 1$ as well as $|\beta|$. All of this shows us that $|\mathrm{Stab}_\beta(\mathcal{U})|$ divides $\gcd(|\beta|, q^k - 1)$, and now the first statement follows from the identities in (3.4).

For (a) note that by assumption, $q^k - 1$ divides $|\beta|$. Thus the statement is just a special case of the previous part.

For (b) set $D := \frac{|\beta|}{q^k-1}$.
"$\Rightarrow$"
With the notation as in (3.4), we have $D = N$. Since $|\beta^N| = \frac{|\beta|}{\gcd(N,|\beta|)} = \frac{|\beta|}{N} = q^k - 1$, the uniqueness of subgroups of a cyclic group gives us $\langle \beta^N \rangle = \mathbb{F}_{q^k}^*$. Now the fact that $\langle \beta^N \rangle = \mathrm{Stab}_\beta(\mathcal{U})$ along with Corollary 9 implies $\mathrm{Stab}_\beta^+(\mathcal{U}) = \mathbb{F}_{q^k} \subseteq \mathcal{U}$. Thus $\mathbb{F}_{q^k} = \mathcal{U}$ due to dimension.
"$\Leftarrow$"
Let $u \in \mathbb{F}_{q^k}^*$. Then $(u\beta^D)^{q^k-1} = u^{q^k-1}\beta^{D\cdot(q^k-1)} = 1 \cdot 1 = 1$. Since the nonzero elements of $\mathbb{F}_{q^k}$ are exactly the roots of $x^{q^k-1} - 1$ in $\mathbb{F}_{q^n}$, we obtain $\mathbb{F}_{q^k}\beta^D = \mathbb{F}_{q^k}$. Hence $|\mathrm{Orb}_\beta(\mathbb{F}_{q^k})| \leq D$. Let $0 \leq i < j < D$ and let $\gamma \in \mathbb{F}_{q^k}\beta^i \cap \mathbb{F}_{q^k}\beta^j$ with $\gamma \neq 0$. Then $\gamma = \gamma_i\beta^i = \gamma_j\beta^j$, for some $\gamma_i, \gamma_j \in \mathbb{F}_{q^k}^*$. But then $\beta^{j-i} = \gamma_i\gamma_j^{-1} \in \mathbb{F}_{q^k}^*$. So $j - i \equiv 0 \bmod D$, which is impossible. Thus $\mathbb{F}_{q^k}\beta^i \cap \mathbb{F}_{q^k}\beta^j = \{0\}$. ■

The last part of the proof along with (2.1) shows the well-known fact $\mathrm{d}_S(\mathrm{Orb}_\beta(\mathbb{F}_{q^k})) = 2k$.

Corollary 12. *Let $\mathcal{U}$ be a k-dimensional subspace of $\mathbb{F}_{q^n}$ such that $1 \in \mathcal{U}$. Then*

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

Furthermore, $\mathrm{d}_S(\mathrm{Orb}(\mathbb{F}_{q^k})) = 2k$.

Note that k divides n because otherwise $(q^n-1)/(q^k-1)$ is not an integer and $\mathbb{F}_{q^n}$ does not contain a subfield of size q^k.

Remark 13. Recall spread codes from Section 2.4. The previous result shows that $\mathrm{Orb}(\mathbb{F}_{q^k})$ is a k-dimensional spread, and $\mathrm{Orb}_\beta(\mathbb{F}_{q^k})$ is a partial spread for any $\beta \in \mathbb{F}_{q^n}^* \backslash \{1\}$. This result is also found in [26, Thm. 11, Cor. 12].

In Lemma 7 we have seen that $\mathcal{U}$ is a vector space over the stabilizer subfield $\mathrm{Stab}^+(\mathcal{U})$, so it makes sence to look at all the subfields of $\mathbb{F}_{q^n}$ over which $\mathcal{U}$ is a vector space. We introduce some convenient terminology.

Definition 14. Let $\mathcal{U}$ be a subspace of $\mathbb{F}_{q^n}$. A subfield $\mathbb{F}_{q^r}$ of $\mathbb{F}_{q^n}$ is called a *friend* of $\mathcal{U}$ if $\mathcal{U}$ is a vector space over $\mathbb{F}_{q^r}$ with scalar multiplication being the multiplication in the field $\mathbb{F}_{q^n}$. The largest friend of $\mathcal{U}$ (with respect to cardinality) is called the *best friend* of $\mathcal{U}$.

Note that since $\mathcal{U}$ is a subspace of the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^n}$, the field $\mathbb{F}_q$ is a friend of $\mathcal{U}$, and thus $\mathcal{U}$ also has a best friend.

Remark 15. For any subspace $\mathcal{U}$ of $\mathbb{F}_{q^n}$ and any friend $\mathbb{F}_{q^r}$ of $\mathcal{U}$ we have $1 \in \mathcal{U} \iff \mathbb{F}_{q^r} \subseteq \mathcal{U}$.

Proposition 16. *Let $\mathcal{U}$ be a subspace of $\mathbb{F}_{q^n}$ with $1 \in \mathcal{U}$. Then the stabilizer subfield $\mathrm{Stab}^+(\mathcal{U})$ is the best friend of $\mathcal{U}$. Furthermore, any friend of $\mathcal{U}$ is contained in the best friend.*

Proof. We know from Lemma 7 that $\mathrm{Stab}^+(\mathcal{U})$ is a friend of $\mathcal{U}$. Moreover, if $\mathbb{F}_{q^l}$ is a friend of $\mathcal{U}$, then $\mathcal{U}\gamma = \mathcal{U}$ for all $\gamma \in \mathbb{F}_{q^l}^*$ by closure of the scalar multiplication. This implies $\mathbb{F}_{q^l}^* \subseteq \mathrm{Stab}(\mathcal{U})$, hence $\mathbb{F}_{q^l} \subseteq \mathrm{Stab}^+(\mathcal{U})$. Thus, $\mathrm{Stab}^+_\beta(\mathcal{U})$ is the largest friend and therefore the best friend of $\mathcal{U}$. ∎

As a consequence, all subspaces in $\mathrm{Orb}(\mathcal{U})$ have the same best friend, say $\mathbb{F}_{q^r}$, and we may therefore call $\mathbb{F}_{q^r}$ the *best friend of the cyclic orbit code*. While stabilizer subfield is the more technical terminology for the best friend, we prefer the term best friend, since we will use the term friend frequently.

Example 10 shows that, unfortunately, we do not have an analogous characterization for $\mathrm{Stab}^+_\beta(\mathcal{U})$, when β is not primitive. This makes understanding the general case more difficult, and shows that the primitive case has additional benefits other than just cardinality concerns.

The identities in (3.4) now read as follows.

Corollary 17. *Let $\mathbb{F}_{q^r}$ be the best friend of $\mathcal{U}$. Then*

$$|\mathrm{Orb}(\mathcal{U})| = \frac{q^n - 1}{q^r - 1} \quad \textit{and} \quad |\mathrm{Stab}(\mathcal{U})| = q^r - 1.$$

This allows us to design of cyclic orbit codes with a prescribed cardinality: we simply have to take a k-dimensional subspace with prescribed best friend, say $\mathbb{F}_{q^r}$. These spaces can be written as $\sum_{i=1}^{t} \alpha_i \mathbb{F}_{q^r}$, where $t = k/r$ and $\alpha_1, \ldots, \alpha_t \in \mathbb{F}_{q^n}$ are linearly independent over $\mathbb{F}_{q^r}$. However, being able to be written in this form only guarantees that $\mathbb{F}_{q^r}$ is a friend not the best friend. Choosing $\alpha_1, \ldots, \alpha_t$ at random will most likely lead to the desired best friend, but does not guarantee that $\mathbb{F}_{q^r}$ is the best friend. If we choose certain $\alpha_1, \ldots, \alpha_t$, a larger subfield may become a friend, thus changing the best friend and cardinality of the cyclic orbit code. One should also note that the dimension, r, of the best friend has to divide $\gcd(k, n)$, which often allows one to easily infer the best friend for a given subspace $\mathcal{U}$. We illustrate this with the following examples.

Example 18. The subspace $\mathcal{U}$ defined below is taken from [12, Ex. 1], where the distance and cardinality of the resulting cyclic orbit code have been determined by straightforward testing and enumeration. Consider $\mathbb{F}_q = \mathbb{F}_2$ and the field $\mathbb{F}_{2^6}$ with primitive element α having minimal polynomial $x^6 + x + 1 \in \mathbb{F}[x]$. Let $\mathcal{U} := \{0, \alpha^0, \alpha^1, \alpha^4, \alpha^6, \alpha^{16}, \alpha^{24}, \alpha^{33}\}$. It is straightforward to check that this is a vector space over $\mathbb{F}_2$ (generated by, for instance, $\{1, \alpha, \alpha^4\}$). Using the isomorphism $\varphi : \sum_{i=0}^{5} a_i \alpha^i \longmapsto (a_0, \ldots, a_5)$ between the vector spaces $\mathbb{F}_{2^6}$ and $\mathbb{F}_2^6$, see (2.4), the subspace $\varphi(\mathcal{U})$ is given by

$$\varphi(\mathcal{U}) = \operatorname{im} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

where $\operatorname{im}(A) := \{xA \mid x \in \mathbb{F}^k\}$ denotes the row space of the matrix $A \in \mathbb{F}^{k \times n}$. Since $\dim(\mathcal{U}) = 3$ it is clear that $\mathcal{U}$ is not a vector space over the subfield $\mathbb{F}_{2^2}$. Furthermore, $\mathcal{U}$ does not coincide with the subfield $\mathbb{F}_{2^3}$ because $\alpha^9 \in \mathbb{F}_{2^3}$, but $\alpha^9 \notin \mathcal{U}$. All of this shows that $\mathbb{F}_2$ is the best friend of $\mathcal{U}$ and thus $|\mathrm{Orb}(\mathcal{U})| = 2^6 - 1 = 63$ by the last corollary.

Example 19. Consider the field $\mathbb{F}_{2^{12}}$ and the primitive element α with minimal polynomial $x^{12} + x^7 + x^6 + x^5 + x^3 + x + 1 \in \mathbb{F}_2[x]$.

(a) Since the minimal polynomial of α over $\mathbb{F}_{2^2}$ has degree 6, it is clear that $\mathcal{U} := \mathbb{F}_{2^2} + \alpha\mathbb{F}_{2^2} + \alpha^3\mathbb{F}_{2^2}$ is a direct sum, and thus $\mathcal{U}$ is a 6-dimensional subspace of the $\mathbb{F}_2$-vector space $\mathbb{F}_{2^{12}}$. Obviously $\mathbb{F}_{2^2}$ is a friend of $\mathcal{U}$. Additionally, $\mathcal{U} \neq \mathbb{F}_{2^6}$ because $\alpha \in \mathcal{U}$, but $\alpha \notin \mathbb{F}_{2^6}$. Along with Proposition 16, all of this shows that $\mathbb{F}_{2^2}$ is the best friend of $\mathcal{U}$ and thus $|\mathrm{Orb}(\mathcal{U})| = (2^{12} - 1)/(2^2 - 1) = 1365$.

(b) Similarly $\mathcal{W} := \mathbb{F}_{2^4} + \alpha\mathbb{F}_{2^2}$ is a 6-dimensional subspace of $\mathbb{F}_{2^{12}}$ with best friend $\mathbb{F}_{2^2}$. Thus $|\mathrm{Orb}(\mathcal{W})| = 1365$.

3.3 The Subspace Distance of Cyclic Orbit Codes

In the previous section we determined the cardinality of a cyclic orbit code in terms of the best friend. Now we turn to finding the minimum distance of these codes, again making use of the best friend.

Since we have a better understanding of the stabilizer when β is primitive, we restrict ourselves to cyclic orbit codes, that is, orbit codes with respect to the entire cyclic group $\mathbb{F}_{q^n}^*$. We begin by fixing a primitive element $\alpha \in \mathbb{F}_{q^n}^*$ and letting $\mathcal{U}$

be a k-dimensional subspace of $\mathbb{F}_{q^n}$. Recall that the orbit code $\mathrm{Orb}(\mathcal{U}) = \mathrm{Orb}_\alpha(\mathcal{U})$ contains a subspace $\mathcal{U}'$ such that $1 \in \mathcal{U}'$. Therefore, we may assume without loss of generality that $1 \in \mathcal{U}$.

We use $\dim_{\mathbb{F}_{q^l}}(\mathcal{U})$ for the dimension of a vector space $\mathcal{U}$ over the field $\mathbb{F}_{q^l}$. We also set $\dim \mathcal{U} := \dim_{\mathbb{F}_q} \mathcal{U}$. Finally, let $\mathbb{F}_{q^r}$ be the best friend of $\mathcal{U}$, and define

$$t := \dim_{\mathbb{F}_{q^r}}(\mathcal{U}) = \frac{k}{r}.$$

From Corollary 17 we know that the cardinality of $\mathrm{Orb}(\mathcal{U})$ is given by $N := \frac{q^n-1}{q^r-1}$. A nice property of orbit codes is that we can compute their distance more efficiently. Since $(\mathcal{U}\alpha^l, \mathcal{U}\alpha^m) = (\mathcal{U}, \mathcal{U}\alpha^{m-l})$, we know

$$\mathrm{d}_S(\mathrm{Orb}(\mathcal{U})) = \min\{(\mathcal{U}, \mathcal{U}\alpha^j) \mid 1 \leq j < |\mathrm{Orb}(\mathcal{U})|\}.$$

Despite this being a more efficient way to compute the distance, we would like to know other ways to compute distance based on the chosen subspace $\mathcal{U}$. In the following subsections we will look at different ways to take the best friend into account when computing the distance of a subspace code.

Bounds on the Subspace Distance via the Stabilizer

We start with a lemma that restricts the possibilities for our distance, based on knowing that $\mathcal{U}$ and all element of its orbit are $\mathbb{F}_{q^r}$ vector spaces.

Lemma 20. *Define* $s := \max_{1 \leq j < N} \dim_{\mathbb{F}_{q^r}}(\mathcal{U} \cap \mathcal{U}\alpha^j)$. *Then*

$$\mathrm{d}_S(\mathrm{Orb}(\mathcal{U})) = 2(k - sr) = 2r(t - s). \tag{3.6}$$

As a consequence,

$$2r \leq \mathrm{d}_S(\mathrm{Orb}(\mathcal{U})) \leq 2k.$$

Recall that the upper bound $\mathrm{d}_S(\mathrm{Orb}(\mathcal{U})) \leq 2k$ is true for all constant dimension codes of dimension $k \leq n/2$.

Proof. Let $1 \leq j < N$. Clearly, $\mathcal{U}\alpha^j$ and thus $\mathcal{U} \cap \mathcal{U}\alpha^j$ are vector spaces over $\mathbb{F}_{q^r}$. Let $s_j := \dim_{\mathbb{F}_{q^r}}(\mathcal{U} \cap \mathcal{U}\alpha^j)$. Since $1 \leq j < N$, we know $\mathcal{U} \neq \mathcal{U}\alpha^j$, and therefore $0 \leq s_j < t$. Thus, $\mathrm{d}_S(\mathcal{U}, \mathcal{U}\alpha^j) = 2(k - \dim(\mathcal{U} \cap \mathcal{U}\alpha^j)) = 2(k - s_j r) \geq 2r(t - s) \geq 2r$. ∎

From this lemma, we observe the usual trade-off between the cardinality of a cyclic orbit code and its (potential) distance: the larger the best friend, the smaller the code, but the better the lower bound for the distance. The most extreme case, namely the best possible distance, is dealt with in the following result.

Corollary 21. *For any cyclic orbit code* $\mathrm{Orb}(\mathcal{U})$ *with best friend* $\mathbb{F}_{q^r}$ *we have*

$$\mathrm{d}_S(\mathrm{Orb}(\mathcal{U})) = 2k \iff r = k \iff \mathcal{U} = \mathbb{F}_{q^k}.$$

If any (hence all) of these properties are true, then $\mathrm{Orb}(\mathcal{U})$ *is a spread code.*

Proof. If $\mathcal{U} = \mathbb{F}_{q^k}$ then obviously, $r = k$. Using the fact that $1 \in \mathcal{U}$, we see that if r=k then $\mathbb{F}_{q^k} \subset \mathcal{U}$, but they must be equal by their dimensions. The implication "$\Longleftarrow$" of the first equivalence has been dealt with in Corollary 12. As for "$\Longrightarrow$", note that Lemma 20 implies that $\mathcal{U}\alpha^j \cap \mathcal{U} = \{0\}$ for all j, hence $\mathrm{Orb}(\mathcal{U})$ is a partial spread. Since $|\mathrm{Orb}(\mathcal{U})| = (q^n-1)/(q^r-1)$, the union of all subspaces in the orbit results in $(q^k-1)(q^n-1)/(q^r-1)$ distinct nonzero points in $\mathbb{F}_{q^n}$. Since $r \leq k$, this implies $r = k$. ■

Now we look as some examples which show examples of how to acheive the best non-spread distance for cyclic orbit codes. We see that according to lemma 20 and corollary 21 the best distance a non-spread cyclic orbit code may achieve is $2(k-r)$.

Example 22. (a) The code in Example 18 is optimal among all non-spread cyclic orbit codes: in [12, p. 1170] the distance has been found as 4, and this is $2(k-1)$.

(b) Consider the code in Example 19(a). In this case $k = 6$ and $r = 2$. One can verify that $\dim_{\mathbb{F}_{2^2}}(\mathcal{U} \cap \mathcal{U}\alpha^j) \leq 1$ for all $1 \leq j < 1365 = |\mathrm{Orb}(\mathcal{U})|$. Hence lemma 20 yields $\mathrm{d}_S(\mathrm{Orb}(\mathcal{U})) = 2(k-r) = 8$, which means the code is optimal among all non-spread cyclic orbit codes with the same length, dimension, and best friend.

There is a specific case where we can always guarantee that a non-spread cyclic orbit code has distance $2(k-r)$.

Example 23. Let $\dim_{\mathbb{F}_{q^r}}(\mathcal{U}) = t = 2$, hence $k = 2r$. Then $2r = 2(k-r)$, and thus $\mathrm{d}_S(\mathrm{Orb}(\mathcal{U})) = 2(k-r)$ due to Lemma 20. Thus any such code is optimal among all non-spread cyclic orbit codes with best friend $\mathbb{F}_{q^r}$.

However, we would like to allow $t > 2$ so we want to find other methods to guarantee non-spread optimal distance. It turns out that this is very difficult but we can find conditions that will lead to a distance less than $2(k-r)$. We begin with a specific construction of "bad" subspaces.

Proposition 24. *Suppose* $\mathcal{U}$ *is of the form* $\mathcal{U} = \bigoplus_{i=0}^{t-1} \alpha^{li}\mathbb{F}_{q^r}$ *for some* $1 \leq l < \frac{q^n-1}{q^r-1}$, *and where* $\mathbb{F}_{q^r}$ *is the best friend of* $\mathcal{U}$. *Then* $(\mathrm{Orb}(\mathcal{U})) = 2r$.

Proof. Since $\alpha^l\mathcal{U} = \bigoplus_{i=1}^{t} \alpha^{li}\mathbb{F}_{q^r}$ we have $\bigoplus_{i=1}^{t-1} \alpha^{li}\mathbb{F}_{q^r} \subseteq \mathcal{U} \cap \alpha^l\mathcal{U}$. Moreover, $l < |\mathrm{Orb}(\mathcal{U})|$ yields $\dim_{\mathbb{F}_{q^r}}(\mathcal{U} \cap \alpha^l\mathcal{U}) \leq t-1 = \dim_{\mathbb{F}_{q^r}}(\bigoplus_{i=1}^{t-1} \alpha^{li}\mathbb{F}_{q^r})$. So $\mathcal{U} \cap \alpha^l\mathcal{U} = \bigoplus_{i=1}^{t-1} \alpha^{li}\mathbb{F}_{q^r}$, and $\dim_{\mathbb{F}_{q^r}}(\mathcal{U} \cap \alpha^l\mathcal{U}) = t-1$, which is the maximum possible intersection between any two distinct subspaces in the cyclic orbit code. Hence in the notation of Lemma 20 we have $s = t-1$, and $\mathrm{d}_S(\mathrm{Orb}(\mathcal{U})) = 2r$. ∎

Notice that in the previous lemma we added the requirement that $\mathbb{F}_{q^r}$ be the best friend of $\mathcal{U}$ because this does not follow from the form of $\mathcal{U}$, as we have mentioned before. Indeed, $\mathcal{U} = \bigoplus_{i=0}^{t-1} \alpha^{li}\mathbb{F}_{q^r}$ only implies that $\mathbb{F}_{q^r}$ is a friend of $\mathcal{U}$, but it may not be the best friend. As an example, in $\mathbb{F}_{2^6}$ with primitive element α we have $\mathbb{F}_{2^2} = \mathbb{F}_2 \oplus \alpha^{21}\mathbb{F}_2$, hence the best friend is $\mathbb{F}_{2^2}$, despite being able to write it as a direct sum of $\mathbb{F}_2$. Notice, however, that we can always write a larger subfield as the direct sum of smaller subfields. The next result shows that this is essentially the only case where we write $\mathcal{U}$ as a direct sum of shifts of $\mathbb{F}_{q^r}$, but $\mathbb{F}_{q^r}$ is not the best friend.

Proposition 25. *Let $\mathcal{U} = \bigoplus_{i=0}^{t-1} \alpha^{il}\mathbb{F}_{q^r}$ for some l, where $t > 1$. Denote by $f \in \mathbb{F}_{q^r}[x]$ the minimal polynomial of α^l over $\mathbb{F}_{q^r}$. Then $\deg(f) \geq t$ and*

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

In other words, $\mathbb{F}_{q^r}$ is the best friend of $\mathcal{U}$ if and only if $\mathcal{U}$ is not a field.

Proof. First, the directness of the sum implies immediately the inequality $\deg(f) \geq t$. As for the chain of equivalences we argue as follows.
1) Assume $\mathcal{U} = \mathbb{F}_{q^{rt}}$. Then $\mathcal{U}$ is a field and the form of $\mathcal{U}$ shows that $\mathcal{U} = \mathbb{F}_{q^r}[\alpha^l]$. This implies $\deg(f) = \dim_{\mathbb{F}_q^r}(\mathcal{U}) = t$.
2) $\deg(f) = t$ yields $\dim_{\mathbb{F}_{q^r}} \mathbb{F}_{q^r}[\alpha^l] = t$, and since $\mathcal{U}$ is contained in this field, we have $\mathcal{U} = \mathbb{F}_{q^r}[\alpha^l]$, by dimensions. This implies $\alpha^l\mathcal{U} = \mathcal{U}$.
3) If $\alpha^l\mathcal{U} = \mathcal{U}$, then $\alpha^l \in \mathrm{Stab}(\mathcal{U})$ and hence α^l is contained in the best friend. Since due to the directness of the sum, α^l is not in $\mathbb{F}_{q^r}$, we conclude that $\mathbb{F}_{q^r}$ is not the best friend of $\mathcal{U}$.
4) Assume that the best friend of $\mathcal{U}$ is $\mathbb{F}_{q^{r'}}$ for some $r' > r$. Set $\dim_{\mathbb{F}_{q^{r'}}} \mathcal{U} = t'$. Then $rt = k = r't'$. We show that $\alpha^l\mathcal{U} = \mathcal{U}$. Assume to the contrary that $\alpha^l\mathcal{U} \neq \mathcal{U}$. Then $\dim_{\mathbb{F}_{q^{r'}}}(\mathcal{U} \cap \alpha^l\mathcal{U}) \leq t'-1$. On the other hand we have $\bigoplus_{i=1}^{t-1} \alpha^{il}\mathbb{F}_{q^r} \subseteq (\mathcal{U} \cap \alpha^l\mathcal{U})$. Considering dimensions over $\mathbb{F}_q$ we obtain the inequality $r(t-1) \leq r'(t'-1)$, and using $rt = r't'$ this yields $r \geq r'$, a contradiction. Thus $\alpha^l\mathcal{U} = \mathcal{U}$, and this implies that $\alpha^{lt} = \sum_{i=0}^{t-1} a_i\alpha^{li}$ for some $a_i \in \mathbb{F}_{q^r}$. But this means that $\deg(f) = t$ and $\mathcal{U} = \mathbb{F}_{q^r}[\alpha^l] = \mathbb{F}_{q^{rt}}$. ∎

Of course, there are also subspaces that are not of the form in Proposition 24 and yet generate cyclic orbit codes with distance as low as $2r$. The following example shows one.

Example 26. Consider $\mathbb{F}_{2^{12}}$ with primitive element α as in Example 19. Let $\mathcal{W} = \mathbb{F}_{2^4} + \alpha\mathbb{F}_{2^2}$. In Example 19(b) we saw that the best friend is $\mathbb{F}_{2^2}$. One can check that $\mathrm{d}_S(\mathrm{Orb}(\mathcal{W})) = 4 = 2r$.

In this example we see that $\mathbb{F}_{2^4}$ is a subspace of $\mathcal{W}$ and that the best friend of $\mathbb{F}_{2^4}$ is itself, which is larger than the best friend of $\mathcal{W}$, $\mathbb{F}_{2^2}$. It turns out that all spaces of this type lead to non-optimal cyclic orbit codes.

Proposition 27. *Suppose there exists a subspace $\mathcal{V}$ of $\mathcal{U}$ with best friend $\mathbb{F}_{q^{r'}}$ for some $r' > r$. Then $\mathrm{d}_S(\mathrm{Orb}(\mathcal{U})) \leq 2(k - r') < 2(k - r)$.*

Proof. Since $\mathbb{F}_{q^{r'}}$ is the best friend of $\mathcal{V}$, Corollary 17 yields

$$|\mathrm{Orb}(\mathcal{V})| = \frac{q^n - 1}{q^{r'} - 1} < \frac{q^n - 1}{q^r - 1} = |\mathrm{Orb}(\mathcal{U})|.$$

So there exists some j such that $\mathcal{V}\alpha^j = \mathcal{V}$, while $\mathcal{U}\alpha^j \neq \mathcal{U}$. Then $\mathcal{V} \subset \mathcal{U} \cap \mathcal{U}\alpha^j$, so $\dim_{\mathbb{F}_{q^r}}(\mathcal{U} \cap \mathcal{U}\alpha^j) \geq \dim_{\mathbb{F}_{q^r}}(\mathcal{V}) \geq \frac{r'}{r}$. Hence $s := \max_{1 \leq j < N} \dim_{\mathbb{F}_{q^r}}(\mathcal{U} \cap \mathcal{U}\alpha^j) \geq \frac{r'}{r}$, and Lemma 20 implies $s \geq \dim_{\mathbb{F}_{q^r}}(\mathcal{U} \cap \mathcal{U}\alpha^j) \geq \frac{r'}{r}$, and $\mathrm{d}_S(\mathrm{Orb}(\mathcal{U})) = 2(k - sr) \leq 2(k - r') < 2(k - r)$. ∎

We would like to stress that the condition in Proposition 27 is not necessary for the distance to be less than $2(k - r)$. As we saw before, codes as in Proposition 24 do not have to have subspace with larger best friends but lead to a distance of $2r$. A specific example of this is the subspace $\mathcal{U}$ of $\mathbb{F}_{2^7}$ generated by 1, α, α^2 (where α is a primitive element of $\mathbb{F}_{2^7}$) has distance $\mathrm{d}_S(\mathrm{Orb}(\mathcal{U})) = 2r = 2 < 2(k - r)$. But since $\mathbb{F}_2$ is the only subfield of $\mathbb{F}_{2^7}$, every subspace of $\mathcal{U}$ has best friend $\mathbb{F}_2$, and the assumption of Proposition 27 is not satisfied.

Unfortunately, we do not know any general construction of cyclic orbit codes with cardinality $(q^n - 1)/(q^r - 1)$ and distance $2(k - r)$, i.e., the best non-spread code case. In [33, p. 7396] it is conjectured that for any n, k, q there exists a cyclic orbit code of cardinality $(q^n - 1)/(q - 1)$ and distance $2(k - 1)$. In the same paper the conjecture is also verified for randomly chosen sets of $(n, k, q) \in \{4, \ldots, 100\} \times \{1, \ldots, 10\} \times \{2, 3\}$.

However for certain extreme cases the conjecture does not hold true.

Example 28. By exhausting all possible 4-dimensional subspaces in $\mathbb{F}_2^8$ via their row echelon form we could verify that no cyclic orbit code exists with parameters

$(n, k, r, q) = (8, 4, 1, 2)$, hence with cardinality 255, and distance 6. While there exists such a code for $(n, k, r, q) = (6, 3, 1, 2)$ and distance 4, it remains open whether there is a cyclic orbit code with parameters $(2k, k, 1, q)$ and distance $2(k-1)$ for any $k > 4$. The usual bounds, see e.g. [37], do not rule out the existence of such codes.

From Lemma 20 we know that there does not exist a cyclic orbit code with parameters $(n, k, r, q) = (8, 4, 2, 2)$, hence with cardinality 85, and distance 6. In fact, it turns out that the largest orbit code of length 8, dimension 4 and with distance 6 is a β-cyclic orbit code for some $\beta \in \mathbb{F}_{2^8}^*$ such that $|\beta| = 51$. The orbit code then also has cardinality 51. Note that this cardinality is not attained by any cyclic orbit code due to Corollary 17.

Example 29. Let us consider cyclic orbit codes in $\mathbb{F}_{2^{12}}$ of dimension $k = 6$ and with best friend $\mathbb{F}_2$. Due to Corollary 17, such a code has cardinality $2^{12} - 1 = 4095$. Because of the above discussion, we have doubts that there exists such a code with distance $2(k-1) = 10$, but we did not perform an exhaustive search. The best code we could find with a random search has distance 8 and is generated by $\mathcal{U} = \mathbb{F}_2 + \alpha\mathbb{F}_2 + \alpha^4\mathbb{F}_2 + \alpha^{10}\mathbb{F}_2 + \alpha^{10}\beta\mathbb{F}_2 + \alpha^8\beta^2\mathbb{F}_2$, where α and β are primitive elements of $\mathbb{F}_{2^{12}}$ and $\mathbb{F}_{2^6}$, respectively.

We close this section with the following positive observation.

Example 30. It can be verified that for $q = 2$ and all $n \in \{6, \ldots, 20\}$, the cyclic orbit code $\mathrm{Orb}(\mathcal{U})$ of dimension $k = 3$ and cardinality $2^n - 1$ with

$$\mathcal{U} = \mathbb{F}_2 + \alpha^2\mathbb{F}_2 + \alpha^3\mathbb{F}_2 \subseteq \mathbb{F}_{2^n}, \text{ where } \langle\alpha\rangle = \mathbb{F}_{2^n}^*,$$

has distance $4 = 2(k-1)$. The same is true (maximal cardinality and distance 4) for $q = 3, 5, 7$ and $n \in \{6, 7, 8\}$ and the analogous subspace $\mathcal{U}$. We did not explore larger values of q and n.

Computing the Subspace Distance via Multisets

In this section, we use multisets to compute distance, rather than computing all subspaces in the code. This idea goes back to Kohnert/Kunz [22, Lem. 1] who made use of it in their search for codes with distance $2(k-1)$, but Rosenthal/Trautmann extended it in [26, Thm. 15, Prop. 16] to the general case. We refine it further by including the use of the best friend, which will allow us to work with a smaller multiset than in [26], and we do not have to distinguish between orbits of size $q^n - 1$ (which can occur only if $q = 2$) and those of smaller size.

As before let $\mathcal{U}$ have best friend $\mathbb{F}_{q^r}$. Lemma 7 yields

$$\mathrm{Stab}(\mathcal{U}) = \langle \alpha^N \rangle = \mathbb{F}_{q^r}^*, \text{ where } N = \frac{q^n - 1}{q^r - 1}. \tag{3.7}$$

Now we consider a new group action $\mathbb{F}_{q^n} \times \langle \alpha^N \rangle \longrightarrow \mathbb{F}_{q^n}$ given by $(v, \gamma) \mapsto v\gamma$. For each $v \in \mathbb{F}_{q^n}^*$ the orbit of v is

$$\mathcal{O}(v) := \{v, v\alpha^N, v\alpha^{2N}, \ldots, v\alpha^{(q^r-2)N}\},$$

and $|\mathcal{O}(v)| = |\langle \alpha^N \rangle| = q^r - 1$, since all elements of the orbit must be distinct. Now we rewrite $v = \alpha^b$ and get that

$$\mathcal{O}(v) = \{\alpha^b, \alpha^{b+N}, \ldots, \alpha^{b+N(q^r-2)}\}.$$

We can see that using modular arithmetic with modulus $q^n - 1$ there is exactly one element in this orbit whose exponent is non-negative and strictly less than N. Hence

$$\mathbb{F}_{q^n}^* = \bigcupdot_{b=0}^{N-1} \mathcal{O}(\alpha^b).$$

Since $\mathcal{U}$ is an $\mathbb{F}_{q^r}$-vector space, the orbit $\mathcal{O}(u)$ is in $\mathcal{U}$ for every $u \in \mathcal{U}$. This shows that

$$\begin{cases} \mathcal{U}\backslash\{0\} = \bigcupdot_{i=1}^{S} \mathcal{O}(\alpha^{b_i}) \text{ for } S = \dfrac{q^k - 1}{q^r - 1} \text{ and} \\ \text{suitable non-negative integers } b_1, \ldots, b_S < N. \end{cases} \tag{3.8}$$

Note that $b_1, \ldots, b_S$ are uniquely determined by $\mathcal{U}$, and if $\alpha^c \in \mathcal{U}$ and $0 \leq c < N$, then $c \in \{b_1, \ldots, b_s\}$.

Now we will use this group action and observations to prove our multiset remark. Recall that a *multiset* is a collection of elements where each element is allowed to appear more than once. We will denote multisets by double braces $\{\{\ldots\}\}$ and the multiplicity of an element $m(J)$, i.e., the number of times J appears in the multiset.

Theorem 31. *Let $\mathcal{U}$ be as above and $b_1, \ldots, b_S$ be as in* (3.8)*. Define the multiset*

$$\mathcal{D} := \{\{b_l - b_m \mod N \mid 1 \leq l, m \leq S, l \neq m\}\},$$

and for $J \in \mathcal{D}$ denote by $m(J)$ the multiplicity of J in $\mathcal{D}$. Furthermore, set $M := \max_{1 \leq J < N}\{m(J)\}$. If $\mathcal{D} = \emptyset$, we define $M := 0$. Then $\dim(\mathcal{U} \cap \mathcal{U}\alpha^J) = \log_q(m(J)(q^r - 1) + 1)$ and

$$\mathrm{d}_S(\mathrm{Orb}(\mathcal{U})) = 2(k - L), \text{ where } L = \log_q(M(q^r - 1) + 1).$$

Proof. We begin by considering the case where $\mathcal{D} = \emptyset$. This happens only if $S = 1$, hence $r = k$ and $\mathcal{U} = \mathbb{F}_{q^k}$. In this case $\mathrm{d}_S(\mathrm{Orb}(\mathcal{U})) = 2k$ as we know from Corollary 21.

Now suppose $\mathcal{D} \neq \emptyset$. Fix $J \in \{1, \ldots, N-1\}$. For all $l \in [S] := \{1, \ldots, S\}$ we have $\alpha^{b_l+J} \in \mathcal{U}\alpha^J$, and thus $\mathcal{O}(\alpha^{b_l+J}) \subset \mathcal{U}\alpha^J$. Hence $(\mathcal{U}\alpha^J)\backslash\{0\} = \dot{\bigcup}_{l\in[S]} \mathcal{O}(\alpha^{b_l+J})$. Since $\mathcal{U} \cap \mathcal{U}\alpha^J$ is an $\mathbb{F}_{q^r}$-vector space contained in $\mathcal{U}$, we have

$$(\mathcal{U} \cap \mathcal{U}\alpha^J)\backslash\{0\} = \dot{\bigcup_{l\in\mathcal{L}_J}} \mathcal{O}(\alpha^{b_l}),$$

where

$$\begin{aligned}\mathcal{L}_J &= \{l \in [S] \mid \mathcal{O}(\alpha^{b_l}) = \mathcal{O}(\alpha^{b_m+J}) \text{ for some } m \in [S]\} \\ &= \{l \in [S] \mid \alpha^{b_l} = \alpha^{b_m+J}\alpha^{\lambda N} \text{ for some } m \in [S] \text{ and } \lambda \in \mathbb{Z}\}.\end{aligned}$$

Note that $\alpha^{b_l} = \alpha^{b_m+J}\alpha^{\lambda N}$ is equivalent to $b_l \equiv b_m + J + \lambda N \mod (q^n - 1)$. Since N is a divisor of $q^n - 1$, we conclude

$$\mathcal{L}_J \subseteq \{l \in [S] \mid b_l - b_m \equiv J \mod N \text{ for some } m \in [S]\}.$$

By assumption there are $m(J)$ pairs (b_l, b_m) so that $b_l - b_m \equiv J \mod N$. Thus, we obtain that $(\mathcal{U} \cap \mathcal{U}\alpha^J)\backslash\{0\}$ is the union of at most $m(J)$ orbits. This shows that $|\mathcal{U} \cap \mathcal{U}\alpha^J| \leq m(J)(q^r - 1) + 1$.

To show equality, note that there are $m(J)$ pairs (b_l, b_m) such that $b_l - b_m \equiv J \mod N$. Pick such a pair (b_l, b_m) and write $b_l = b_m + J + \lambda N$ for some $\lambda \in \mathbb{Z}$. Then $\mathcal{O}(\alpha^{b_l}) = \mathcal{O}(\alpha^{b_m+J+\lambda N}) = \mathcal{O}(\alpha^{b_m+J})$, and so this orbit is in $\mathcal{U} \cap \mathcal{U}\alpha^J$. This shows that there are at least $m(J)$ orbits in the intersection, and we conclude that $|\mathcal{U} \cap \mathcal{U}\alpha^J| = m(J)(q^r - 1) + 1$. Thus $\dim(\mathcal{U} \cap \mathcal{U}\alpha^J) = \log_q(m(J)(q^r - 1) + 1)$.

Finally, $\mathrm{d}_S(\mathrm{Orb}(\mathcal{U})) = 2(k - \max_{0<J<N}\{\dim(\mathcal{U} \cap \mathcal{U}\alpha^J)\})$, which leads to the desired result. ∎

Chapter 4 A Linkage Construction

This chapter will present a new way to build constant-dimension subspace codes, called the linkage construction. These linkage codes are recursive, and therefore use other types of constant-dimension subspace codes as seeds. The main idea of this construction is to link two constant-dimension subspace codes by concatenating their underlying matrices in such a way as to not change the distance of the resulting codes. This process creates a longer, larger code without compromising distance. Since the linkage construction relies heavily on the matrices which represent the subspace code, the following definition will be very helpful in our discussion.

Definition 32. A matrix $M \in \mathbb{F}^{k\times n}$ is called a *matrix representation* of the subspace $\mathcal{U} \subseteq \mathbb{F}^n$ if $\mathcal{U} = \operatorname{im}(M)$. A set of matrices $\mathcal{M} \subseteq \mathbb{F}^{k\times n}$ is called *SC-representing* if $\operatorname{rank}(M) = k$ for all $M \in \mathcal{M}$ and $\operatorname{im}(M) \neq \operatorname{im}(M')$ for all $M \neq M'$. We will denote the induced constant-dimension code $\mathcal{C}(\mathcal{M}) := \{\operatorname{im}(M) \mid M \in \mathcal{M}\}$.

Notice that for any subspace $\mathcal{U} \in \mathcal{G}_q(n,k)$ there exist many matrix representations and we can always find a SC-representing set for any constant-dimension subspace code. For example, we could choose the matrix in Row Reduced Echelon Form.

Additionally, we will often want to project into either the first components of a vector or the last components so the following maps will be helpful. Define the projections

$$\pi_1 : \mathbb{F}^{n_1+n_2} \to \mathbb{F}^{n_1}, (a,b) \mapsto a \text{ and } \pi_2 : \mathbb{F}^{n_1+n_2} \to \mathbb{F}^{n_2}, (a,b) \mapsto b.$$

For a subspace $\mathcal{U} = \operatorname{im}(U_1 \mid U_2) \subseteq \mathbb{F}^{n_1+n_2}$, we define $\mathcal{U}_i = \pi_i(\mathcal{U})$, so $\mathcal{U}_i = \operatorname{im}(U_i)$.

4.1 Linkage Construction Theorem

Now we formalize the idea of the linkage construction. It generalizes the construction in [14, Thm 5.1]. We will present the linkage construction as a theorem. We see in the theorem how to glue the constituant codes together in three components of the linkage code.

Theorem 33. *For $i = 1, 2$ let $\mathcal{M}_i \subset \mathbb{F}^{k\times n_i}$ be SC-representing sets of cardinality N_i. Thus $\mathcal{C}_i = \mathcal{C}(\mathcal{M}_i)$ is a $(n_i, N_i, k)_q$-code. Additionally, let $\mathcal{C}_R$ be an $k \times n_2$ linear rank metric code such that $|\mathcal{C}_R| =: N_R$. Define the subspace code $\widetilde{\mathcal{C}}$ of length $n := n_1 + n_2$ as $\widetilde{\mathcal{C}} = \widetilde{\mathcal{C}}_1 \cup \widetilde{\mathcal{C}}_2 \cup \widetilde{\mathcal{C}}_3$, where*

$$\begin{aligned}
\widetilde{\mathcal{C}}_1 &= \{\text{im } (U \mid 0_{k\times n_2}) \mid U \in \mathcal{M}_1\},\\
\widetilde{\mathcal{C}}_2 &= \{\text{im } (0_{k\times n_1} \mid U) \mid U \in \mathcal{M}_2\},\\
\widetilde{\mathcal{C}}_3 &= \{\text{im } (U \mid M) \mid U \in \mathcal{M}_1, M \in \mathcal{C}_R\backslash\{0\}\}.
\end{aligned}$$

Then $\widetilde{\mathcal{C}}$ is a $(n, N, d, k)_q$ code, where $N = N_2+N_1N_R$ and $d = \min\{\mathrm{d}_S(\mathcal{C}_1), \mathrm{d}_S(\mathcal{C}_2), 2\mathrm{d}_R(\mathcal{C}_R)\}$. We write $\widetilde{\mathcal{C}} = \mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2$ for the resulting linkage code and call $\widetilde{\mathcal{C}}$ the code obtained by linking $\mathcal{C}_1$ and $\mathcal{C}_2$ through $\mathcal{C}_R$.

Proof. The cardinality of $\widetilde{\mathcal{C}}$ is clear, since the sets $\widetilde{\mathcal{C}}_i$ are pairwise disjoint and

$$N_1 + N_2 + N_1(N_R - 1) = N_2 + N_1N_R.$$

It remains to show that $\mathrm{d}_S(\widetilde{\mathcal{C}}) = d$. It is obvious that $\mathrm{d}_S(\widetilde{\mathcal{C}}_i) = \mathrm{d}_S(\mathcal{C}_i)$, for $i = 1, 2$. Additionally, each subspace in $\widetilde{\mathcal{C}}_2$ intersect trivially with each subspace in $\widetilde{\mathcal{C}}_1$ and $\widetilde{\mathcal{C}}_3$, because of the placement of the zero matrix. Thus $\mathrm{d}_S(\mathcal{U}_1, \mathcal{U}_2) = 2k$ for all $\mathcal{U}_1 \in \widetilde{\mathcal{C}}_2$ and $\mathcal{U}_2 \in \widetilde{\mathcal{C}}_1 \cup \widetilde{\mathcal{C}}_3$. Since $2k$ is the maximum distance of a constant dimension k code, we see that $\mathrm{d}_S(\widetilde{\mathcal{C}}_2, \widetilde{\mathcal{C}}_1 \cup \widetilde{\mathcal{C}}_3)$ is greater than $\min\{\mathrm{d}_S(\mathcal{C}_1), \mathrm{d}_S(\mathcal{C}_2), 2\mathrm{d}_R(\mathcal{C}_R)\}$. Thus we must check the distance of $\widetilde{\mathcal{C}}_3$, where we combine the codes, and the distance between $\widetilde{\mathcal{C}}_1$ and $\widetilde{\mathcal{C}}_3$.

We check the distance between $\widetilde{\mathcal{C}}_1$ and $\widetilde{\mathcal{C}}_3$ by letting

$$\mathcal{U} = \text{im } (U \mid 0) \in \widetilde{\mathcal{C}}_1 \text{ and } \mathcal{V} = \text{im } (U' \mid M) \in \widetilde{\mathcal{C}}_3,$$

for some $U \in \mathcal{M}_1$, $U' \in \mathcal{M}_1$ and $M \in \mathcal{C}_R\backslash\{0\}$. If $\operatorname{rank} M = k$ then $\mathrm{d}_S(\mathcal{U}, \mathcal{V}) = 2k$, because of the placement of the zero matrix. So assume $\operatorname{rank} M < k$ but $\operatorname{rank} M \geq \mathrm{d}_R(\mathcal{C}_R)$, by the linearity of the code. By the rank-nullity theorem we get $\dim(\ker(M)) \leq k - \mathrm{d}_R(\mathcal{C}_R)$. We want to relate this to the subspace distance by relating it to the dimension of the intersection of $\mathcal{U}$ and $\mathcal{V}$.

Let $v \in \mathcal{U} \cap \mathcal{V}$. Thus

$$v = w\,(U \mid 0) = w'\,(U' \mid M)\,,$$

which gives us $w'M = w0 = 0$ and $wU = w'U'$. So we see that $w' \in \ker(M)$ and $wU \in \mathcal{U}_1 \cap \mathcal{V}_1$. So we have shown that for every element of $\mathcal{U} \cap \mathcal{V}$ we get a element of $\ker(M)$ as well as an element of $\mathcal{U}_1 \cap \mathcal{V}_1$. So we have shown that

$$\dim(\mathcal{U} \cap \mathcal{V}) \leq \min\{\dim(\mathcal{U}_1 \cap \mathcal{V}_1),\, \dim(\ker(M))\}.$$

Since $\mathcal{U}_1,\ \mathcal{V}_1 \in \mathcal{C}_1$ and using (2.1) we see that,

$$\mathrm{d}_S(\mathcal{U},\mathcal{V}) \geq \max\{\mathrm{d}_S(\mathcal{C}_1), 2\mathrm{d}_R(\mathcal{C}_R)\} \geq \min\{\mathrm{d}_S(\mathcal{C}_1), \mathrm{d}_S(\mathcal{C}_2), 2\mathrm{d}_R(\mathcal{C}_R)\}.$$

Lastly, let

$$\mathcal{U} = \mathrm{im}\ (U \mid M) \in \widetilde{\mathcal{C}_3} \text{ and } \mathcal{V} = \mathrm{im}\ (U' \mid M') \in \widetilde{\mathcal{C}_3},$$

for some $U, U' \in \mathcal{M}_1$ and $M, M' \in \mathcal{C}_R \backslash \{0\}$. Since we do not want $\mathcal{U}$ to be equal to $\mathcal{V}$ we have $U \neq U'$ or $M \neq M'$. Now, we want to compare $\dim(\mathcal{U} \cap \mathcal{V})$ with $\mathrm{d}_R(M, M')$. Let $v \in \mathcal{U} \cap \mathcal{V}$, then

$$v = w\,(U \mid M) = w'\,(U' \mid M')\,.$$

So we get

$$wU = w'U' \in \mathcal{U}_1 \cap \mathcal{V}_1 \text{ and } wM = w'M' \in \mathrm{im}\,(M) \cap \mathrm{im}\,(M').$$

Now we have two cases. If $U \neq U'$, then $\dim(\mathcal{U} \cap \mathcal{V}) \leq \dim(\mathcal{U}_1 \cap \mathcal{V}_1)$, as before. Thus in this case we have

$$\mathrm{d}_S(\mathcal{U},\mathcal{V}) \geq \mathrm{d}_S(\mathcal{C}_1) \geq \min\{\mathrm{d}_S(\mathcal{C}_1), \mathrm{d}_S(\mathcal{C}_2), 2\mathrm{d}_R(\mathcal{C}_R)\}.$$

If $U = U'$, then $w = w'$, since U and U' are full rank. Also $M \neq M'$, which means that $\mathrm{d}_R(M, M') = \mathrm{rank}\,(M - M') \geq \mathrm{d}_R(\mathcal{C}_R)$. Hence $\dim(\ker(M - M')) \leq k - \mathrm{d}_R(\mathcal{C}_R)$. But then we have $wM = wM'$ and hence $w \in \ker(M - M')$. This shows us that, in this case, every element of $\mathcal{U} \cap \mathcal{V}$ gives an element of $\ker(M - M')$. Thus

$$\dim(\mathcal{U} \cap \mathcal{V}) \leq \dim(\ker(M - M')) \leq k - \mathrm{d}_R(\mathcal{C}_R),$$

which implies that $\mathrm{d}_S(\mathcal{U},\mathcal{V}) \geq 2\mathrm{d}_R(\mathcal{C}_R)$. Thus in both cases $\mathrm{d}_S(\mathcal{U},\mathcal{V}) \geq \min\{\mathrm{d}_S(\mathcal{C}_1), \mathrm{d}_S(\mathcal{C}_2), 2\mathrm{d}_R(\mathcal{C}_R)\}$ which finishes our proof.

■

The following example shows how the linkage construction works.

Example 34. For this example, we will work over $\mathbb{F}_2$. Let

$$\mathcal{M}_1 = \mathcal{M}_2 = \left\{ \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \right\} \subseteq \mathbb{F}^{3\times 6}$$

and let

$$\mathcal{M}_1' = \left\{ \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \right\} \subseteq \mathbb{F}^{3\times 6}.$$

Notice that $\mathcal{C}(\mathcal{M}_1) = \mathcal{C}(\mathcal{M}_1')$. Finally, let

$$\mathcal{C}_R = \left\{ 0, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \right\} \subseteq \mathbb{F}^{4\times 8}.$$

A quick check gives us that $\mathcal{C}(\mathcal{M}_1) = \mathcal{C}(\mathcal{M}_1') = \mathcal{C}(\mathcal{M}_2)$ is a $(6, 2, 4, 3)_2$ code and that $\mathcal{C}_R$ is a linear rank metric code, with $\mathrm{d}_R(\mathcal{C}_R) = 3$ and $N_R = 4$. If we let $\mathcal{C}_1 = \mathcal{C}(\mathcal{M}_1)$ and $\mathcal{C}_2 = \mathcal{C}(\mathcal{M}_2)$ then $\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2$ is a $(12, 10, 4, 3)_2$ code. It turns out that $\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2$ has 5 pairs of codewords $(\mathcal{U}, \mathcal{V})$ with distance $\mathrm{d}_S(\mathcal{U}, \mathcal{V}) = 4$. However, if we use $\mathcal{M}_1'$ as the SC-representing set for $\mathcal{C}_1$ then $\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2$ is still a $(12, 10, 4, 3)_2$ code but now we can check that 3 pairs of codewords $(\mathcal{U}, \mathcal{V})$ have distance $\mathrm{d}_S(\mathcal{U}, \mathcal{V}) = 4$. Thus we see that the choice of SC-representing sets gives us different codes. $\mathcal{M}_1 *_{\mathcal{C}_R} \mathcal{M}_2$ may be a more accurate notation, but since the linkage code inherits its properties from the subspace codes, we prefer the notation $\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2$, which will rarely cause any confusion.

This example indicates that there may be an optimal way to choose the matrix representations for the distance distribution for our linkage code. However, at this point in time we do not know what this would be. Since this choice only affects the distance distribution and not any basic of the properties of the code, we will ignore this choice of SC-representing sets in most cases.

It should be noted that the linkage construction should be used for $n \geq 4k$, since we want each $n_i \geq 2k$. Nevertheless, this construction allows us to create codes of large size, as long as there are known codes for $n = 2k, \ldots, 4k - 1$. The following example explores the cardinality of the linkage construction in comparison to codes generated by other constructions.

Example 35. Since many codes are known in the case $q = 2$, $k = 3$ and subspace distance 4, we will construct linkage codes in the case of $n = 12, 13$, and 14. We could continue to construct linkage codes of longer lengths but we don't have codes

to compare to in longer lengths. This is one strength of the linkage constructions, since we can generate a linkage code quickly once a few shorter lengths are known.

In this case we will need the largest codes of size 6,7 and 8, which have cardinality 77, 329, and 1312 respectively, see [5, Tables I and II]. In order to create codes of the largest size, we use an MRD code in $\mathbb{F}^{3\times n_2}$ of rank distance 2, since these are optimal rank metric codes of the appropriate size (see Section 2.3). These codes have size $N_R = 2^{n_2(3-2+1)} = 2^{2n_2}$. Since we can break up $n = 13, 14$ in multiply ways, we show the following table of sizes of linkage codes. The bolded entries are the largest cardinality for each size.

n	n_1	n_2	N_1	N_2	N_R	Linkage
12	6	6	77	77	4096	**315,469**
13	6	7	77	329	16384	1,261,897
13	7	6	329	77	4096	**1,347,661**
14	7	7	329	329	16384	**5,390,665**
14	6	8	77	1312	65536	5,047,584
14	8	6	1312	77	4096	5,374,029

Now we compare the linkage construction to other large constructions. The constructions listed are the multilevel (ML) construction [10], the modified multilevel (MML) construction [11] and the largest codes constructed via computer search [5, 4].

n	Linkage	ML	MML	Largest Known
12	315,469	298,139	305,324	385,515
13	1,347,661	1,192,587	1,221,296	1,597,245
14	5,390,665	4,770,411	4,885,184	5,996,178

Both the multilevel and modified multilevel constructions contain a lifted MRD code. However, the linkage codes created in the table do not contain a lifted MRD code. We also note that the code of length 13 which has 1,597,245 is optimal, since it is a Steiner structure (see [4]).

As we can see the linkage construction beats the multilevel and modified multilevel constructions but does not beat the best known lower bounds.

Despite being smaller than the best known codes, the linkage construction still has many advantages over other constructions, the main one being that it does not require us to generate an entirely new code from scratch for each length. Additionally, cardinality gains can be made without having to start over in each length. When a

gain is made in a smaller length, a gain is also made in the longer linkage codes. Notice that if the cardinality of the seed code $\mathcal{C}_1$ increases by c, then the cardinality of the linkage code increases by cN_R, which can be quite large.

There is another specific linkage case that improves on cardinality of decodable codes. In this case the linkage construction is also decodable and we will explore that later. Here we present this case.

Example 36. Let $\mathcal{C}_1$ be a lifted MRD code of subspace distance 2d and let $\mathcal{C}_R$ be a MRD code of rank distance d. Let $\mathcal{C}_2$ be any decodable subspace code with subspace distance 2d. (Notice we could choose $\mathcal{C}_2$ to be a lifted MRD code.) Construct $\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2$ as in Theorem 33. We will see later on that $\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2$ is decodable. Since $N_1 = q^{(n_1-k)(k-d+1)}$ and $N_R = q^{n_1(k-d+1)}$, we know that

$$|\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2| = N_2 + q^{(n_1-k)(k-d+1)}q^{n_2(k-d+1)} = N_2 + q^{(n-k)(k-d+1)}.$$

We know that $q^{(n-k)(k-d+1)}$ is the cardinality of of a lifted MRD code of dimension k and length n, so the linkage construction will beat the cardinality of such a code in all cases. However, this case is always smaller than the best cardinalities in Example 35. If $\mathcal{C}_2$ is a lifted MRD code then $|\mathcal{C}_2| = q^{(n_2-k)(k-d+1)}$ and

$$|\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2| = q^{(n_2-k)(k-d+1)} + q^{(n-k)(k-d+1)}.$$

So we see that unlike in Example 35 we always get the largest cardinality when n_2 is the largest. The following table compares linking two lifted MRD codes (Link_{MRD}), linking a lifted MRD code with the largest possible code ($\text{Link}_{\text{largest}}$), a lifted MRD code and the extended lifted MRD construction in [30]. This last construction is included since it is a recursive code, which extends a lifted MRD code without compromising distance and seems to be a suitable comparison.

n	n_1	n_2	Link_{MRD}	$\text{Link}_{\text{largest}}$	Lifted MRD	Extended Lifted MRD
12	6	6	262,208	262,221	262,144	266,304
13	6	7	1,048,832	1,048,905	1,048,576	1,065,216
14	6	8	4,195,328	4,195,616	4,194,304	4,260,864

4.2 Partial Spread Linkage Codes

The linkage construction can be used to construct optimal partial spread codes, as well as, to generalize other partial spread constructions. In this section we will explore how to do this. We begin by refining the linkage construction to a special case which is useful to our discussion.

Remark 37. Let f be a primitive polynomial of degree n over $\mathbb{F}_q$ and M_f be its companion matrix. Fix a full rank matrix $V \in \mathbb{F}^{k\times n}$. We define the rank metric code

$$\mathcal{C}_{f,V} := \{VM_f^i \mid i = 0, \dots q^n - 2\} \cup \{0\}.$$

We see that $\mathrm{d}_R(\mathcal{C}_{f,V}) = k$ and $|\mathcal{C}_f| = q^n$ since $\langle M_f\rangle \cup \{0\} \cong \mathbb{F}_{q^n}$. We also note that $\mathcal{C}_{f,V}\backslash\{0\}$ is a SC-representing set of an irreducible cyclic orbit code. Finally, notice that for two subspace codes $\mathcal{C}_1$ and $\mathcal{C}_2$ we have $\mathrm{d}_S(\mathcal{C}_1 *_{\mathcal{C}_{f,V}} \mathcal{C}_2) = \min\{\mathrm{d}_S(\mathcal{C}_1), \mathrm{d}_S(\mathcal{C}_2)\}$, because $\mathrm{d}_S(\mathcal{C}_1), \mathrm{d}_S(\mathcal{C}_2) \leq 2k$.

Recall the concept of spreads and partial spreads from Section 2.4. The remark shows that if we link spreads or partial spreads by a rank metric code $\mathcal{C}_{f,V}$, we obtain again a (partial) spread. Using this special case we are able to generalize two different constructions in the following example.

Example 38.

1. We begin by writing $n = lk + c$ for $0 \leq c < k$ and letting $n_1 = n - (k + c)$ and $n_2 = k + c$. Using the standard map from $\mathbb{F}_{q^{n_1}} \to \mathbb{F}_q^{n_1}$, let $\mathcal{C}_1 = \mathrm{Orb}\mathbb{F}_{q^k} \subseteq \mathbb{F}_q^{n_1}$, which is a k-spread as we saw in Remark 13. Next, let $\mathcal{M}_2 = \{(I_k \mid 0_{k\times c})\}$, which is a partial k-spread. Finally, we set $\mathcal{C}_R = \mathcal{C}_{f,V}$ where $V = (I_k \mid 0_{k\times c})$ and f is a primitive polynomial for $\mathbb{F}_{q^{n_2}}$. Then $\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2$ is a partial spread in $\mathbb{F}_q^n$ and is exactly the partial spread given in [12, Thm. 11]. We have that $|\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2| = 1 + q^{n_2}\frac{q^{n_1}-1}{q^k-1} = \frac{q^n-q^c}{q^k-1} - q^c + 1$.

2. As in (a) let $n = lk+c$ for $0 \leq c < k$, $n_1 = (l-1)k$ and $n_2 = k+c$. Let $p \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree k and M_p be the companion matrix of p. Let $\mathcal{M}_1 = \{(A_1 \mid \dots \mid A_{l-1}) | A_i \in \mathbb{F}_q[M_p], \text{not all } A_i\text{'s zero}\}$. Then $\mathcal{C}_1 = \mathcal{C}(\mathcal{M}_1)$ is a spread called a *Desarguesian spread*[16]. Let $\mathcal{M}_2 = \{(I_k|0_{k\times c})\}$ and $\mathcal{C}_R = \mathcal{C}_f$ where $V = (0_{k\times c}|I_k)$ and f is a primitive polynomial for $\mathbb{F}_{q^{n_2}}$. Again the code $\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2$ is a partial spread in $\mathbb{F}_q^n$. This is the spread constructed in [18, Thm. 13]. As in (a) we have that $|\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2| = 1+q^{n_2}\frac{q^{n_1}-1}{q^k-1} = \frac{q^n-q^c}{q^k-1} - q^c+1$. We can see that the only difference between these constructions is the choice of spread used in the first component. However, in [18], Gorla and Ravagani give a decoding algorithm which makes use of the choice of the Desarguesian spread, where as Etzion and Vardy in [12] do not present a decoding algorithm.

Since we know that the linkage construction generalizes these constructions of partial spreads, we will explore it more in this context. Before we do so we will establish some definitions and facts that we be useful in this discussion.

Definition 39. We say that a partial spread, $\mathcal{C}$, is *maximal* if it is maximal with respect to inclusion. That is, $\mathcal{C}$ is not properly contained in any other partial spread. We say that $\mathcal{C}$ is *maximum* if it has the largest possible cardinality.

In most cases the size of a maximum partial spread is unknown except when $c = 0, 1$, where $c \equiv n \pmod{k}$, or when $q = 2$ and $k = 3$. We will denote the the size of the largest partial k-spread in $\mathcal{G}_q(n, k)$ by

$$\mu_q(n, k).$$

While we do not know $\mu_q(n, k)$ is most cases, we do have the following bounds.

Theorem 40 ([3])**.** *Let $n \equiv c \mod k$. Then*

$$\frac{q^n - q^c}{q^k - 1} - (q^c - 1) \leq \mu_q(n, k).$$

Additionally, if $c = 0$ or $c = 1$ then we get equality, i.e., $\frac{q^n - q^c}{q^k - 1} - (q^c - 1) = \mu_q(n, k)$.

We also have an upper bound for $\mu_q(n, k)$.

Theorem 41 ([8])**.** *Let $n \equiv c \mod k$. Define θ by*

$$\theta = \frac{\sqrt{1 + 4q^k(q^k - q^c)} - (2q^k - 2q^c + 1)}{2}.$$

Then

$$\mu_q(n, k) \leq \frac{q^n - q^c}{q^k - 1} - \lfloor \theta \rfloor - 1.$$

Notice that both constructions in Example 38 meet the lower bound for $\mu_q(n, k)$. We know that for $c = 0, 1$ that the lower bound is sharp; hence, these partial spread constructions are maximal in those cases. However, we know the lower bound is not sharp in one specific case, as seen in the following theorem.

Theorem 42 ([9], Thm. 5)**.** *Let $k = 3$ and $n \geq 8$. Let $n \equiv c \mod k$. Then the maximum cardinality of a partial 3-spread of $\mathbb{F}_2^n$ is*

$$\frac{2^n - 2^c}{7} - c.$$

This theorem is proven by giving a construction, but the linkage construction gives an alternative construction. The following example will be helpful to us in finding maximum spreads.

Example 43. Let $q = 2$, $k = 3$ for all the following examples.

(a) For $n = 6, 9$, k divides n so we can construct a spread, namely the orbit code of $\mathbb{F}_{2^3}$ in $\mathbb{F}_{2^6}$ or $\mathbb{F}_{2^9}$.

(b) For $n = 7$, there is a spread of size 17, see Example 38.

(c) For $n = 8$ there is a partial 3-spread in $\mathbb{F}_2^8$ with cardinality 34, which was found by computer search and is given in [9, Ex. 2].

Since we have maximum partial spread codes to link in this case, we use the linkage construction to construct maximum partial spreads of longer lengths.

Corollary 44. *Let $n \geq 10$ and write $n = 3l + n_2$ for some $l \geq 1$ and $n_2 \geq 7$. Let $n \equiv c \mod 3$, thus $n_2 \equiv c \mod 3$. Let $\mathcal{C}_1$ be a 3 spread in $\mathbb{F}_2^{3l}$. Hence $|C_1| = N_1 = \frac{2^{3l}-1}{7}$. Moreover, let $\mathcal{C}_2$ be a maximum partial 3-spread in $\mathbb{F}_2^{n_2}$, hence $|\mathcal{C}_2| = N_2 = \frac{2^{n_2}-2^c}{7} - c$. Finally, let f be a primitive polynomial for $\mathbb{F}_{q^{n_2}}$, $V \in \mathbb{F}^{k \times n_2}$ be full rank and $\mathcal{C}_R = \mathcal{C}_{f,V}$. Then $\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2$ is a maximum partial 3-spread in $\mathbb{F}_2^n$.*

Proof. The resulting code is a partial spread, since $\mathrm{d}_S(\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2) = \min\{2k, 2k, 2k\} = 2k$. Its cardinality is given by

$$2^{n_2}\frac{2^{3l}-1}{7} + \frac{2^{n_2}-2^c}{7} - c = \frac{2^n - 2^c}{7} - c,$$

which is optimal by Theorem 42. ∎

Using Example 43 and Corollary 44, we can construct an optimal partial spread for all $n \geq 6$, when $q = 2$ and $k = 3$. However, we would still like to know what happens in other cases.

By Theorems 40 and 41, we see that $\mu_q(n,k) = \frac{q^n - q^c}{q^k - 1} - a_q(n,k)$, for some $a_q(n,k) \in \mathbb{Z}_{\geq 1}$. We notice that if we link two maximum partial spreads of lengths $n_1 \equiv c_1 \mod k$ and $n_2 \equiv c_2 \mod k$ by some $\mathcal{C}_{f,V}$, we will always get a cardinality of

$$\frac{q^n - q^{c_2} - q^{n_2}(q^{c_1} - 1)}{q^k - 1} - a_q(n_1,k) - a_q(n_2,k).$$

If we choose $c_1 = 0$ meaning that $k \mid n_1$ and $\mathcal{C}_1$ is an spread then, $n \equiv n_2 \equiv c \mod k$. Thus, if $a_q(n_2,k)$ and $a_q(n,k)$ only depend on c then we will get a maximum partial spread, since our cardinality is

$$\frac{q^n - q^c}{q^k - 1} - a_q(n_2,k) = \frac{q^n - q^c}{q^k - 1} - a_q(n,k).$$

Because we don't know anything about maximum spreads in most cases, the best we can do is find a maximal spread. It turns out that if we link a spread code with a maximal partial spread by $\mathcal{C}_{f,V}$, we will always return a maximal partial spread.

Proposition 45. *Let $\mathcal{C}_1$ be a spread code in $\mathbb{F}_q^{n_1}$, $\mathcal{C}_2$ be a maximal partial spread in $\mathbb{F}_q^{n_2}$ and $\mathcal{C}_R = \mathcal{C}_{f,V}$ for some primitive polynomial f and full rank $V \in \mathbb{F}^{k\times n_2}$. Then $\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2$ is a maximal partial spread in $\mathbb{F}_q^n$.*

Proof. We know that $\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2$ is a partial spread since $\mathrm{d}_S(\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2) = \min\{2k, 2k, 2k\} = 2k$. Thus we only need to show it is maximal. Let $\mathcal{U} \in \mathcal{G}_q(n,k)\backslash(\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2)$, and write $\mathcal{U} = \mathrm{im}\,(X \mid Y)$, for some $X \in \mathbb{F}_q^{k\times n_1}$ and $Y \in \mathbb{F}_q^{k\times n_2}$. We want to show that in all cases $\mathrm{d}_S(\mathcal{U}, \mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2) < 2k$, by showing that $\mathcal{U}$ intersects nontrivially with some codeword.

Case 1: $Y = 0$
Since $Y = 0$, we want to construct an element of $\widetilde{\mathcal{C}_1}$, which will intersect with $\mathcal{U}$. Since $\mathcal{C}_1$ is a spread and must contain every one dimensional subspace in some element of the spread, we know $\mathrm{im}\,(X) \cap \mathrm{im}\,(U_1)$ for some $U_1 \in \mathcal{M}_1$. Thus $\dim(\mathcal{U} \cap \mathrm{im}\,(U_1 \mid 0)) \neq 0$ and $\mathrm{d}_S(\mathcal{U}, \mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2) < 2k$.

Case 2: $X = 0$
In this case, since $X = 0$, we want to construct an element of $\widetilde{\mathcal{C}_2}$ which will intersect with $\mathcal{U}$. Since $\mathcal{C}_2$ is a maximal partial spread, all other subspace must intersect an element of $\mathcal{C}_2$. Hence we can find some $U_2 \in \mathcal{M}_2$ such that $\mathrm{im}\,(Y) \cap \mathrm{im}\,(U_2)$. Thus $\dim(\mathcal{U} \cap \mathrm{im}\,(0 \mid U_2)) \neq 0$ and $\mathrm{d}_S(\mathcal{U}, \mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2) < 2k$.

Case 3: $X \neq 0$ and $Y \neq 0$
We know that $\{VM_f^i \mid i \in \{0, \ldots, q^{n_2} - 2\}\} \cup \{0\}$ is a MRD code with distance k. Thus if $\mathrm{rank}\,(Y) = k$ we must have $\mathrm{d}_R(Y, VM_f^i) < k$ for some i, otherwise we could add Y to our code which contradicts the singleton bound. Thus $\mathrm{rank}\,(Y - VM_f^i) < k$ and there is $v \in \mathbb{F}_q^k$ such that $vY = vVM_f^i$. We also know that $vX \in \mathrm{im}\,(U_1)$ for some $U_1 \in \mathcal{M}_1$, since $\mathcal{C}_1$ is a spread. Thus $v(X \mid Y) \in \mathcal{U} \cap \mathrm{im}\,(U_1 \mid VM_f^i)$, and so $\mathrm{d}_S(\mathcal{U}, \mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2) < 2k$.

Now if $\mathrm{rank}\,(Y) < k$ then there exists $v \in \mathbb{F}_q^k$ such that $vY = 0$. As before, we have $vX \in \mathrm{im}\,(U_1)$ for some $U_1 \in \mathcal{M}_1$. Thus $v(X \mid Y) \in \mathcal{U} \cap \mathrm{im}\,(U_1 \mid 0)$, and $\mathrm{d}_S(\mathcal{U}, \mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2) < 2k$.

So we see that in all cases $\mathrm{d}_S(\mathcal{U}, \mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2) < 2k$. Thus $\mathcal{U}$ cannot be added to the partial spread without compromising the distance, which proves the construction is maximal. ■

We would like to use this proposition on the partial spreads in Example 38, but we must verify that $\mathcal{C}_2 = \{\mathrm{im}\,(I_k \mid 0_{k\times c}\}$ is a maximal partial spread. However, this is trivial, since $k > n_2/2$. Thus we see that both of these constructions from before are maximal partial spreads. Hence, this proposition helps by showing that the construction by Etzion and Vardy in Example 38 (1) is a maximal construction, which they do not show in [12]. Also it is a new abbreviation to the proof of maximality given by Gorla and Ravagnani in [18], for their spreads as seen in Example 38 (2). So we see that linkage partial spread codes nicely generalize all known results on the construction of maximal and maximum partial spreads.

4.3 Decoding of the Linkage Construction

In this section, we want to explore the decodability of the linkage construction. The idea is to utilize the structures of the underlying codes and the structure of the linkage code to decode received words efficiently. We know that if a subspace is close enough to our codeword, that is $\mathrm{d}_S(\mathcal{V},\mathcal{C}) < \frac{\mathrm{d}_S(\mathcal{C})}{2}$, minimum distance decoding will work, see [29]. So the goal is to find an algorithm that will produce the unique closest codeword without having to check the distance between the received word and all codewords. To begin this discussion, we make the following definition.

Definition 46. A subspace $\mathcal{V}$ is *decodable* with respect to the code $\mathcal{C}$ if $\mathrm{d}_S(\mathcal{V},\mathcal{C}) \leq \frac{d-1}{2}$.

For any decodable $\mathcal{V}$ there exists an *unique* subspace $\mathcal{U} \in \mathcal{C}$ such that $\mathrm{d}_S(\mathcal{V},\mathcal{U}) \leq \frac{d-1}{2}$, since d_S is a metric. Our goal for this section is to find an efficient algorithm to find $\mathcal{U} \in \mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2$ for any decodable $\mathcal{V}$.

The natural idea for an efficient algorithm is to decode each projection $\mathcal{V}_i$ in the appropriate seed code and glue it back together. However, in most cases this will not work, because we must make use of both the rank metric and the subspace metric. In order to use the rank metric (which is a matrix metric) we must make a choice of which matrix representation to use for our received subspace. This lemma shows us the relationship of the rank metric and the possible choices.

Lemma 47. *Let $\mathcal{U} \in \mathcal{G}_q(n,K)$ such that $\mathcal{U} = \mathrm{im}\,(U), U \in \mathbb{F}_q^{K\times n}$ and let $\mathcal{V} \in \mathcal{G}_q(n,k) = \mathrm{im}\,(V)$, $V \in \mathbb{F}_q^{K\times n}$ and $K \geq k$, such that $\mathrm{d}_S(\mathcal{U},\mathcal{V}) = d$. Then $\mathrm{d}_R(U,V) \geq \frac{K-k}{2} + \frac{d}{2}$ and there exists $\tilde{V} \in \mathbb{F}_q^{K\times n}$ such that $\mathcal{V} = \mathrm{im}\,(\tilde{V})$ and $\mathrm{d}_R(U,\tilde{V}) = \frac{K-k}{2} + \frac{d}{2}$*

Proof. Since $\mathrm{d}_S(\mathcal{U},\mathcal{V}) = d$, we know that $\dim(\mathcal{U}\cap\mathcal{V}) = \frac{K+k}{2} - \frac{d}{2} =: \ell$. Let $A \in \mathrm{GL}_n(\mathbb{F}_q)$, be a product of elementary matrices, such that $AU = \begin{pmatrix} U_1 \\ U_2 \end{pmatrix}$, where $U_1 \in \mathbb{F}_q^{\ell\times n}$, $U_2 \in \mathbb{F}_q^{(K-\ell)\times n}$ and $\mathrm{im}\,(U_1) = \mathcal{U}\cap\mathcal{V}$. (Note: this can be done since $\mathcal{U}\cap\mathcal{V} \subset \mathcal{U}$, and we can perform a change of basis with row operations.) Then we have

$$\begin{aligned}
\mathrm{d}_R(U,V) &= \mathrm{rank}\,(U-V) \\
&= \mathrm{rank}\,(AU-AV) \\
&= \mathrm{rank}\left(\begin{pmatrix} U_1 \\ U_2 \end{pmatrix} - \begin{pmatrix} V_1' \\ V_2' \end{pmatrix}\right) \\
&= \mathrm{rank}\begin{pmatrix} U_1 - V_1' \\ U_2 - V_2' \end{pmatrix}
\end{aligned}$$

First we know that $\mathcal{V} = \mathrm{im}\,(AV) = \mathrm{im}\begin{pmatrix} V_1' \\ V_2' \end{pmatrix}$, since A is a product of elementary matrices. Thus $\mathrm{im}\,(V_1') \subset \mathcal{V}$. Next, $\mathrm{rank}\,(U_2 - V_2') = K - \ell = \frac{K-k}{2} + \frac{d}{2}$, otherwise we would have $xU_2 = xV_2' \in \mathcal{U}\cap\mathcal{V}$, for some $x \in \mathbb{F}_q^{K-l}$. This is not possible since the rows of U_1 are a basis for the intersection. Thus, $\mathrm{d}_R(U,V) \geq \frac{K-k}{2} + \frac{d}{2}$, since $\mathrm{rank}\,(U_1 - V_1') \geq 0$.

Next we show there exists $\tilde{V}$ such that $\mathcal{V} = \mathrm{im}\,(\tilde{V})$ and $\mathrm{d}_R(U,\tilde{V}) = \frac{K-k}{2} + \frac{d}{2}$. We begin by extending U_1 to a matrix $V = \begin{pmatrix} U_1 \\ V_2 \end{pmatrix} \in \mathbb{F}^{K\times n}$ such that $\mathcal{V} = \mathrm{im}\begin{pmatrix} U_1 \\ V_2 \end{pmatrix}$, which is possible since $\mathrm{im}\,(U_1) = \mathcal{V}\cap\mathcal{U} \subset \mathcal{V}$. Let $\tilde{V} = A^{-1}V$, where A is as before. We see that $\mathrm{im}\,(\tilde{V}) = \mathcal{V}$, since A is a product of elementary matrices. Then we have

$$\begin{aligned}
\mathrm{d}_R(U,\tilde{V}) &= \mathrm{rank}\,(U-\tilde{V}) \\
&= \mathrm{rank}\,(AU-V) \\
&= \mathrm{rank}\begin{pmatrix} 0 \\ U_2 - V_2 \end{pmatrix} \\
&= K - \ell \\
&= \frac{K-k}{2} + \frac{d}{2},
\end{aligned}$$

since $\mathrm{im}\,(U_2 - V_2)$ must not contain any elements of the intersection as before. ∎

However, we notice that $\frac{K-k}{2} + \frac{d}{2}$ may be larger than $\frac{\mathrm{d}_R(\mathcal{C}_R)-1}{2}$, which can lead to problems. This is not the only time we run into problems; the following shows an example of where we see that even if only erasures occur we still cannot decode through projections.

Example 48. For this example, we will work over $\mathbb{F}_2$. Let

$$\mathcal{M}_1 = \mathcal{M}_2 = \left\{ \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \right\} \subseteq \mathbb{F}^{4\times 8}$$

and let

$$\mathcal{C}_R = \left\{ 0, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \right\} \subseteq \mathbb{F}^{4\times 8}.$$

Let $\mathcal{C}_1 = \mathcal{C}_2 = \mathcal{C}(\mathcal{M}_1) = \mathcal{C}(\mathcal{M}_2)$. It is easy to check that $\mathrm{d}_S(\mathcal{C}_1) = \mathrm{d}_S(\mathcal{C}_2) = 6$ and $\mathrm{d}_R(\mathcal{C}_R) = 4$. Then $\mathcal{C} = \mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2$ has distance 6.

Our goal is to create a decodable subspace $\mathcal{V}$, for which decoding by projecting into each component and decoding in the constituent codes does not work. To be more specific, I want to find a $\mathcal{V}$ with closest codeword $\mathcal{U} = \mathrm{im}\,(U_1 \mid M)$ such that for any matrix representation of $\mathcal{V}$, $(V_1 \mid V_2)$, we cannot decode in $\mathcal{C}_R$, i.e., $\mathrm{d}_R(V_2, M) > \frac{\mathrm{d}_R(\mathcal{C}_R)-1}{2}$. This means that if we projected into the second component, no matter how we chose and appropriate matrix for $\mathcal{V}_2$, closest codeword decoding in $\mathcal{C}_R$ will not work.

Let

$$\mathcal{V} = \mathrm{im} \left(\begin{array}{cccccccc|cccccccc} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{array} \right).$$

We can check that $\mathrm{d}_S(\mathcal{V}, \mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2) = 2 \leq \frac{6-1}{2}$ and that

$$\mathcal{U} = \mathrm{im} \left(\begin{array}{cccccccc|cccccccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{array} \right),$$

is the unique closest codeword to $\mathcal{V}$. So we see that $\mathcal{V}$ is a decodable subspace. Next, let

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \in \mathcal{C}_R$$

be the matrix from the second component of the closest codeword. For all matrix representations $(V_1 \mid V_2) \in \mathbb{F}^{4\times 16}$ of $\mathcal{V}$ we can check that $\mathrm{d}_R(V_2, M) > \frac{4-1}{2}$. Hence we cannot use closest codeword decoding in $\mathcal{C}_R$ to find M. Thus, we have a decodable subspace which cannot be decoded by decoding in each separate component.

As we can see there are subspaces where no matrix representation allows for decoding with the rank metric in $\mathcal{C}_R$. The following proposition shows that this is a problem for many linkage codes.

Proposition 49 ([15])**.** *Let $\mathcal{C}$ be as in Theorem 33 and assume $d \geq \mathrm{d}_R(\mathcal{C}_R)+2$. Then there exists a subspace $\mathcal{U} = \mathrm{im}\,(U_1 \mid U_2) \in \mathcal{C}$ and a received word $\mathcal{V} \subseteq \mathbb{F}^n$ such that*

1. *$\mathrm{d}_S(\mathcal{U}, \mathcal{V}) \leq \frac{d-1}{2}$ (that is, $\mathcal{V}$ is decodable),*
2. *$\mathcal{V} \subseteq \mathcal{U}$ (hence only erasures occurred during transmission),*
3. *for any $V_2 \in \mathbb{F}^{k\times n_2}$ such that $\mathrm{im}\,(V_2) = \pi_2(\mathcal{V})$ we have*

$$\mathrm{rank}\,(V_2 - U_2) > \frac{d_R - 1}{2}.$$

In other words, it is not possible to decode $\mathcal{V}$ by making use of the rank metric for the code $\mathcal{C}_R$.

As we can see, for many linkage codes, particularly for codes where $d = 2\mathrm{d}_R(\mathcal{C}_R)$, there is a subspace which cannot be decoded by projecting into components. The issue seems to be integrating the rank metric with the subspace metric. By restricting

to a case where we only use the subspace distance, we would be able to eliminate this difficulty. The following proposition gives a different linkage construction, which only uses subspace codes.

Proposition 50. *For $i = 1, 2$ let $\mathcal{M}_i \subseteq \mathbb{F}^{k\times n_i}$ be a SC-representing set such that $\mathcal{C}_i = \mathcal{C}(\mathcal{M}_i)$ is a $(n_i, N_i, \mathrm{d}_S(\mathcal{C}_i), k)_q$-code. Let $\mathcal{M}_3 \subseteq \mathbb{F}^{k\times n_2}$ be a SC-representing set such that $\mathcal{C}_3 = \mathcal{C}(\mathcal{M}_3)$ is a $(n_2, N_3, \mathrm{d}_S(\mathcal{C}_3), k)_q$-code. Define the subspace code $\widetilde{\mathcal{C}}$ of length $n := n_1 + n_2$ as $\widetilde{\mathcal{C}} = \widetilde{\mathcal{C}}_1 \cup \widetilde{\mathcal{C}}_2 \cup \widetilde{\mathcal{C}}_3$, where*

$$\begin{aligned}
\widetilde{\mathcal{C}}_1 &= \{\mathrm{im}\ (U \mid 0_{k\times n_2}) \mid U \in \mathcal{M}_1\},\\
\widetilde{\mathcal{C}}_2 &= \{\mathrm{im}\ (0_{k\times n_1} \mid U) \mid U \in \mathcal{M}_2\},\\
\widetilde{\mathcal{C}}_3 &= \{\mathrm{im}\ (U_1 \mid U_3) \mid U_1 \in \mathcal{M}_1, U_3 \in \mathcal{M}_3\}.
\end{aligned}$$

Then $\widetilde{\mathcal{C}}$ is a $(n, N, d, k)_q$ code, where $N = N_2 + N_1(N_3+1)$ and $d = \min\{\mathrm{d}_S(\mathcal{C}_1), \mathrm{d}_S(\mathcal{C}_2), \mathrm{d}_S(\mathcal{C}_3)\}$. We denote such a linkage code, $\mathcal{C}_1 *_{\mathcal{C}_3} \mathcal{C}_2$.

Proof. As in the proof of Theorem 33, $\mathrm{d}_S(\widetilde{\mathcal{C}}_1) = \mathrm{d}_S(\mathcal{C}_1)$ and $\mathrm{d}_S(\widetilde{\mathcal{C}}_2) = \mathrm{d}_S(\mathcal{C}_2)$. Also, since $\mathrm{rank}\,(U_3) = k$ for all $U_3 \in \mathcal{M}_3$, we know that $\mathrm{d}_S(\widetilde{\mathcal{C}}_1, \widetilde{\mathcal{C}}_2) = \mathrm{d}_S(\widetilde{\mathcal{C}}_1, \widetilde{\mathcal{C}}_3) = \mathrm{d}_S(\widetilde{\mathcal{C}}_2, \widetilde{\mathcal{C}}_3) = 2k$. So we must only check the distance of $\widetilde{\mathcal{C}}_3$.

Let

$$\mathcal{U} = \mathrm{im}\ (U_1 \mid U_3) \in \widetilde{\mathcal{C}}_3 \text{ and } \mathcal{V} = \mathrm{im}\ (U_1' \mid U_3') \in \widetilde{\mathcal{C}}_3,$$

for some $U_1, U_1' \in \mathcal{M}_1$ and $U_3, U_3' \in \mathcal{M}_3$. Since we do not want $\mathcal{U}$ to be equal to $\mathcal{V}$ we have $U_1 \neq U_1'$ or $U_3 \neq U_3'$. As before we see, for any $v \in \mathcal{U} \cap \mathcal{V}$,

$$v = w\,(U_1 \mid U_3) = w'\,(U_1' \mid U_3') \Rightarrow wU_1 = w'U_1' \text{ and } wU_2 = w'U_2'.$$

So, we get an element of $\mathcal{U}_1 \cap \mathcal{V}_1$, as well as, an element of $\mathcal{U}_2 \cap \mathcal{V}_2$. Thus, $\dim(\mathcal{U} \cap \mathcal{V}) \leq \dim(\mathcal{U}_1 \cap \mathcal{V}_1)$, and $\dim(\mathcal{U} \cap \mathcal{V}) \leq \dim(\mathcal{U}_2 \cap \mathcal{V}_2)$. So we have

$$\mathrm{d}_S(\mathcal{U}, \mathcal{V}) \geq \min\{\mathrm{d}_S(\mathcal{C}_1), \mathrm{d}_S(\mathcal{C}_3)\}.$$

Thus we see that $d = \min\{\mathrm{d}_S(\mathcal{C}_1), \mathrm{d}_S(\mathcal{C}_2), \mathrm{d}_S(\mathcal{C}_3)\}$. ∎

Notice that we can set easily set $\mathcal{M}_2 = \mathcal{M}_3$ and reduce the number of subspace codes needed without changing the distance. This case is worth studying because as we will see shortly it is decodable, but it is also tremendously smaller that the standard linkage construction. As we can see in the following chart the best sizes we get are:

n	Subspace Linkage	Standard Linkage
12	6,083	315,469
13	25,739	1,347,661
14	102,413	5,390,665

However, we cannot efficiently decode in the largest cases, since the links themselves are not efficiently decodable. First, we will show how to decode codes from Proposition 50 then we will explore a larger case of decodable linkage codes.

We begin with a useful lemma.

Lemma 51. *Let $\mathcal{C} = \mathcal{C}_1 *_{\mathcal{C}_3} \mathcal{C}_2$ be as in Proposition 50, and $\mathcal{V} = \text{im}\,(V_1 \mid V_2) \in \mathcal{G}_q(n, K)$, with $(V_1 \mid V_2) \in \mathbb{F}_q^{K\times n}$. Let $\mathrm{d}_S(\mathcal{V},\mathcal{C}) \leq \frac{d-1}{2}$, so there exists a unique $\mathcal{U} = \text{im}\,(U_1 \mid U_2) \in \mathcal{C}$, such that $\mathrm{d}_S(\mathcal{V},\mathcal{U}) \leq \frac{d-1}{2}$. Then following are equivalent:*

(1) $\text{rank}\,(V_i) \leq \frac{K-1}{2}$

(2) $U_i = 0$

for $i = 1, 2$.

Proof. (1) $\Rightarrow$ (2)
Assume $U_i \neq 0$, to get a contradiction, then $\text{rank}\,(U_i) = k$. Note that $\pi_i|_{\mathcal{U}} : \mathcal{U} \to \text{im}\,(U_i)$ and $\pi_i|_{\mathcal{V}} : \mathcal{V} \to \text{im}\,(V_i)$ are surjective. Also $\dim(\mathcal{U}) = \dim(\text{im}\,(U_i)) = k$ so $\pi_i|_{\mathcal{U}}$ is an isomorphism. Thus:

$$\dim(\mathcal{U} \cap \mathcal{V}) = \dim(\pi_i(\mathcal{U} \cap \mathcal{V})) \leq \dim\,(\pi_i(\mathcal{U}) \cap \pi_i(\mathcal{V})) \leq \dim\,(\mathcal{V}_i) = \text{rank}\,(V_i).$$

But, $\text{rank}\,(V_i) \leq \frac{K-1}{2}$, so

$$\begin{aligned}
\mathrm{d}_S(\mathcal{V},\mathcal{U}) &= K + k - 2\dim(\mathcal{V} \cap \mathcal{U}) \\
&\geq K + k - 2\left(\frac{K-1}{2}\right) \\
&= k + 1 \\
&> \frac{d-1}{2},
\end{aligned}$$

since $d \leq 2k$. This is a contradiction.

(2) $\Rightarrow$ (1), $i = 1$
Assume $U_1 = 0$, then $\text{rank}\,(U_2) = k$ since $\mathcal{U} \in \mathcal{C}$. Since $\mathrm{d}_S(\mathcal{U},\mathcal{V}) \leq \frac{d-1}{2} < k$, we have

$$K + k - 2\dim(\mathcal{U} \cap \mathcal{V}) < k \Rightarrow \dim(\mathcal{U} \cap \mathcal{V}) > \frac{K}{2}.$$

Now by using the following matrix $\begin{pmatrix} 0 & U_2 \\ V_1 & V_2 \end{pmatrix}$, we have

$$\begin{aligned} k + \operatorname{rank}(V_1) &\leq \operatorname{rank} \begin{pmatrix} 0 & U_2 \\ V_1 & V_2 \end{pmatrix} \\ &= \dim(\mathcal{U} + \mathcal{V}) \\ &= K + k - \dim(\mathcal{U} \cap \mathcal{V}) \\ &< K + k - \frac{K}{2} \\ &= k + \frac{K}{2}. \end{aligned}$$

Hence $\operatorname{rank}(V_1) < \frac{K}{2} \leq \frac{K-1}{2}$.

For $i = 2$ the proof follows similarly, using the matrix $\begin{pmatrix} U_1 & 0 \\ V_1 & V_2 \end{pmatrix}$.

■

Remark 52. 1. This lemma and proof is very similar to the proof of Lemma 22 in [18], just applied to the linkage construction instead of their partial spread codes.

2. Note that we only need $\mathcal{C}$ to be as in Proposition 50 so that the matrices U_i are full rank. Hence, $\operatorname{rank}(V_1) \leq \frac{K-1}{2} \Leftrightarrow U_1 = 0$ is true for any linkage code, since $\operatorname{rank}(U_1) = k$ for all $U_1 \in \mathcal{M}_1$.

Theorem 53. *Let $\mathcal{C} = \mathcal{C}_1 *_{\mathcal{C}_3} \mathcal{C}_2$ be as in Proposition 50. Let $\mathcal{V} \in \mathcal{G}_q(n, K)$ be a decodable subspace, such that $\mathcal{V} = \operatorname{im}(V_1 \mid V_2)$.*

1. *If $\dim(\mathcal{V}_1) \leq \frac{K-1}{2}$ then $\mathcal{V}_2$ is decodable with respect to $\mathcal{C}_2$. Additionally if $\operatorname{im}(U_2) \in \mathcal{C}_2$ is the unique closest codeword to $\mathcal{V}_2$ then $\mathcal{U} = \operatorname{im}(0 \mid U_2) \in \mathcal{C}$ is the unique closest codeword to $\mathcal{V}$.*

2. *If $\dim(\mathcal{V}_2) \leq \frac{K-1}{2}$ then $\mathcal{V}_1$ is decodable with respect to $\mathcal{C}_1$. Additionally if $\operatorname{im}(U_1) \in \mathcal{C}_1$ is the unique closest codeword to $\mathcal{V}_1$ then $\mathcal{U} = \operatorname{im}(U_1 \mid 0) \in \mathcal{C}$ is the unique closest codeword to $\mathcal{V}$.*

3. *If $\dim(\mathcal{V}_1) > \frac{K-1}{2}$ and $\dim(\mathcal{V}_2) > \frac{K-1}{2}$ then both $\mathcal{V}_1$ and $\mathcal{V}_2$ are decodable with respect to $\mathcal{C}_1$ and $\mathcal{C}_3$ respectively. Additionally if $\operatorname{im}(U_i) \in \mathcal{C}_i$ is the unique*

closest codeword to $\mathcal{V}_i$ for i=1,3 then $\mathcal{U} = \text{im}\,(U_1 \mid U_3) \in \mathcal{C}$ is the unique closest codeword to $\mathcal{V}$.

Proof. First note that these 3 cases are clearly mutually exclusive, since $\dim(\mathcal{V}) = K$. Next let $\mathcal{U} = \text{im}\ (U_1, U_2) \in \mathcal{C}$ be the closest codeword to $\mathcal{V}$, i.e., $\mathrm{d}_S(\mathcal{U} \mid \mathcal{V}) \leq \frac{d-1}{2}$, which must exist since $\mathcal{V}$ is decodable. So we see that $\mathcal{U}_i = \text{im}\,(U_i)$ for $i = 1, 2$.
Case 1: $\dim(\mathcal{V}_1) \leq \frac{K-1}{2}$
By Lemma 51, $U_1 = 0$ and $\mathcal{U} = \text{im}\,(0 \mid U_2)$ for some $U_2 \in \mathcal{M}_2$. Notice:

$$\text{im} \begin{pmatrix} U_1 & U_2 \\ V_1 & V_2 \end{pmatrix} = \text{im} \begin{pmatrix} 0 & U_2 \\ V_{11} & V_{21} \\ 0 & V_{22} \end{pmatrix}$$

where $\text{rank}\,(V_{11}) = \text{rank}\,(V_1) \leq \frac{K-1}{2}$. Then we have

$$\dim(\mathcal{U} \cap \mathcal{V}) = \dim\left(\text{im}\,(U_2) \cap \text{im}\,(V_{22})\right) \leq \dim\left(\text{im}\,(U_2) \cap \text{im}\,(V_2)\right) = \dim(\mathcal{U}_2 \cap \mathcal{V}_2.$$

Hence

$$\begin{aligned} \mathrm{d}_S(\mathcal{U}, \mathcal{V}) &= K + k - 2\dim(\mathcal{U} \cap \mathcal{V}) \\ &\geq K + k - 2\dim(\underbrace{\mathcal{U}_2}_{\dim = k} \cap \underbrace{\mathcal{V}_2}_{\dim \leq K}) \\ &\geq \dim(\mathcal{U}_2) + \dim(\mathcal{V}_2) - 2\dim(\mathcal{U}_2 \cap \mathcal{V}_2) \\ &= \mathrm{d}_S(\mathcal{U}_2, \mathcal{V}_2). \end{aligned}$$

Since $\mathcal{V}$ is decodable, we have $\mathrm{d}_S(\mathcal{U}_2, \mathcal{V}_2) \leq \mathrm{d}_S(\mathcal{U}, \mathcal{V}) \leq \frac{d-1}{2} \leq \frac{\mathrm{d}_S(\mathcal{C}_2)-1}{2}$. Hence $\mathcal{U}_2 \in \mathcal{C}_2$ is the closest codeword to $\mathcal{V}_2$. So $\mathcal{V}_2$ is decodable with respect to $\mathcal{C}_2$, and the unique closest codeword $\mathcal{U}_2 = \text{im}\,(U_2) \in \mathcal{C}_2$ leads to the unique closest codeword $\text{im}\,(0 \mid U_2) \in \mathcal{C}$.
Case 2: $\dim(\mathcal{V}_2) \leq \frac{K-1}{2}$
This follows from a similar argument to Case 1.
Case 3: $\dim(\mathcal{V}_1) > \frac{K-1}{2}$ and $\dim(\mathcal{V}_2) > \frac{K-1}{2}$
By Lemma 51 $U_1 \neq 0$ and $U_2 \neq 0$, so $\text{rank}\,(U_1) = \text{rank}\,(U_2) = k$ by the definition of our code. Thus, $\pi_i|_{\mathcal{U}} : \mathcal{U} \to \mathcal{U}_1$ is an isomorphism. Thus:

$$\dim(\mathcal{U} \cap \mathcal{V}) = \dim(\pi_i(\mathcal{U} \cap \mathcal{V})) \leq \dim\left(\pi_i(\mathcal{U}) \cap \pi_i(\mathcal{V})\right) = \dim(\mathcal{U}_i \cap \mathcal{V}_i).$$

So we have

$$\begin{aligned}
\mathrm{d}_S(\mathcal{U},\mathcal{V}) &= k + K - 2\dim(\mathcal{U}\cap\mathcal{V}) \\
&\geq k + K - 2\dim(\underbrace{\mathcal{U}_i}_{\dim=k} \cap \underbrace{\mathcal{V}_i}_{\dim\leq K}) \\
&\geq \dim\mathcal{U}_i + \dim\mathcal{V}_i - 2\dim(\mathcal{U}_i\cap\mathcal{V}_i) \\
&= \mathrm{d}_S(\mathcal{U}_i,\mathcal{V}_i).
\end{aligned}$$

Since $\mathcal{V}$ is decodable, we have $\mathrm{d}_S(\mathcal{U}_i,\mathcal{V}_i) \leq \mathrm{d}_S(\mathcal{U},\mathcal{V}) \leq \frac{d-1}{2}$. So we see that $\mathcal{V}_i$ is decodable for $i = 1, 2$. Also, by the uniqueness of the closest codeword, we have that if $\mathrm{im}\,(U_i) \in \mathcal{C}_i$ is the unique closest codeword to $\mathcal{V}_i$ for i=1,2 then $\mathcal{U} = \mathrm{im}\,(U_1 \mid U_2) \in \mathcal{C}$ is the unique closest codeword to $\mathcal{V}$. ■

This theorem shows us that the following algorithm will be accurate and efficient as long $\mathcal{C}_1, \mathcal{C}_2$ and $\mathcal{C}_3$ have efficient decoding algorithms.

Algorithm 1: Decoding Algorithm for Special Case from Proposition 50

Data: a decodable K-dimension subspace $\mathcal{V} = \mathrm{im}\ (V_1, V_2)$, $(V_1, V_2) \in \mathbb{F}_q^{K\times n}$
Result: the unique $\mathcal{U} \in \mathcal{C}_1 *_{\mathcal{C}_3} \mathcal{C}_2$ such that $\mathrm{d}_S(\mathcal{V},\mathcal{U}) \leq \frac{d-1}{2}$.
if $\mathrm{rank}\,(V_1) \leq \frac{K-1}{2}$ **then**
  decode $\mathrm{im}\,(V_2)$ in $\mathcal{C}_2$ to $\mathrm{im}\,(U_2)$;
  return $\mathcal{U} = \mathrm{im}\ (0 \mid U_2)$.
else
  if $\mathrm{rank}\,(V_2) \leq \frac{K-1}{2}$ **then**
    decode $\mathrm{im}\,(V_1)$ in $\mathcal{C}_1$ to $\mathrm{im}\,(U_1)$;
    return $\mathcal{U} = \mathrm{im}\ (U_1 \mid 0)$.
  else
    decode $\mathrm{im}\,(V_1)$ in $\mathcal{C}_1$ to $\mathrm{im}\,(U_1)$;
    decode $\mathrm{im}\,(V_2)$ in $\mathcal{C}_3$ to $\mathrm{im}\,(U_3)$;
    return $\mathcal{U} = \mathrm{im}\ (U_1 \mid U_3)$.
  end
end

Since using a subspace codes to link greatly reduces the size of our linkage codes, we would like to be able to efficiently decode larger linkage codes. As we have seen already, we will need to find a special case, where we can harness the structure of the underlying codes, instead of just projecting into compents, as we did in Theorem 53. Recall the special case in Example 36 where we link a lifted rank metric code with any subspace code by a rank metric code. We refine this situation by requiring that $\mathcal{C}_2$ be an efficiently decodable code. In this situation, we can use the structure

of the lifted rank metric code to help us decode. Recall, from Section 2.3, that for a rank metric code $\mathcal{C}_R \subseteq \mathbb{F}_q^{k\times(n-k)}$, we denote a lifted rank rank metric code $\Lambda(\mathcal{C}_R) = \{\mathrm{im}\,(I_k \mid M) \mid M \in \mathcal{C}_R\} \subseteq \mathcal{G}_q(n,k)$. The following theorem will show us how to find the unique closest codeword in this case.

Theorem 54. *Let $\mathcal{C}'_R \subseteq \mathbb{F}_q^{k\times(n_1-k)}$ be a rank metric code and $\mathcal{M}_1 = \{(I_k \mid M) | M \in \mathcal{C}'_R\}$, $\mathcal{M}_2 \subseteq \mathbb{F}_q^{k\times n_2}$ an SC-representing set, and $\mathcal{C}_R \subset \mathbb{F}_q^{k\times n_2}$ a rank metric code. Let $\mathcal{C} = \mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2$ be as in Lemma 33. Let $\mathcal{V} \in \mathcal{G}_q(n,K)$ be a decodable subspace, such that $\mathcal{V} = \mathrm{im}\,(V_1 \mid V_2 \mid V_3)$, where $V_1 \in \mathbb{F}_q^{k\times k}, V_2 \in \mathbb{F}_q^{k\times(n_1-k)}$ and $V_3 \in \mathbb{F}_q^{k\times n_2}$.*

1. *If $\mathrm{rank}\,(V_1 \mid V_2) \leq \frac{K-1}{2}$ then $\mathcal{V}_2 = \mathrm{im}\,(V_3)$ is decodable with respect to $\mathcal{C}_2$. Additionally, if $\mathrm{im}\,(U_3) \in \mathcal{C}_2$ is the unique closest codeword to $\mathcal{V}_2$ then $\mathcal{U} = \mathrm{im}\,(0 \mid 0 \mid U_3) \in \mathcal{C}$ is the unique closest codeword to $\mathcal{V}$.*

2. *If $\mathrm{rank}\,(V_1 \mid V_2) > \frac{K-1}{2}$ then $\mathcal{V}_1 = \mathrm{im}\,(V_1 \mid V_2)$ is decodable with respect to $\mathcal{C}_1$ and $\mathrm{im}\,(V_1 \mid V_3)$ is decodable with respect to $\Lambda(\mathcal{C}_R)$. Additionally, if $\mathrm{im}\,(I_k \mid M_1) \in \mathcal{C}_1$ is the unique closest codeword to $\mathcal{V}_1$ and $\mathrm{im}\,(I_k \mid M_2)$ is the unique closest codeword to $\mathrm{im}\,(V_1 \mid V_3)$ then $\mathcal{U} = \mathrm{im}\,(I_k \mid M_1 \mid M_2) \in \mathcal{C}$ is the unique closest codeword to $\mathcal{V}$.*

Proof. Let $\mathcal{U} = \mathrm{im}\ (U_1 \mid U_2 \mid U_3) \in \mathcal{C}$ be the closest codeword to $\mathcal{V}$, i.e., $\mathrm{d}_S(\mathcal{U},\mathcal{V}) \leq \frac{d-1}{2}$, which must exist since $\mathcal{V}$ is decodable. Note we partition the matrix of $\mathcal{U}$ as we partition the matrix of $\mathcal{V}$.
Case 1: $\dim(\mathrm{im}\,(V_1 \mid V_2)) \leq \frac{K-1}{2}$
As noticed in Remark 52, $(U_1 \mid U_2) = 0$ if and only if $\dim(\mathcal{V}_1) = \dim(\mathrm{im}\,(V_1 \mid V_2)) \leq \frac{K-1}{2}$ still holds for this code. Hence, $(U_1 \mid U_2) = 0$ and $U_3 \in \mathcal{M}_2$. So we see that this case is the same as case 1 in Theorem 53 and

$$\mathrm{d}_S(\mathrm{im}\,(U_3), \mathrm{im}\,(V_3)) \leq \mathrm{d}_S(\mathcal{U},\mathcal{V}) \leq \frac{\mathrm{d}_S(\mathcal{C}_2)-1}{2}.$$

Thus we see that $\mathcal{V}_2 = \mathrm{im}\,(V_3)$ is decodable with respect to $\mathcal{C}_2$, with closest codeword $\mathrm{im}\,(U_3)$. And we see that the closest codeword to $\mathcal{V}$ is $\mathrm{im}\,(0 \mid 0 \mid U_3) \in \mathcal{C}$ by the uniqueness of the closest codeword.
Case 2: $\dim(\mathrm{im}\,(V_1 \mid V_2)) > \frac{K-1}{2}$
First, we observe that $\mathcal{U}_1 = \mathrm{im}\,(U_1 \mid U_2)$, $\mathcal{V}_1 = \mathrm{im}\,(V_1 \mid V_2)$. Then because $\dim(\mathcal{U}_1) > \frac{K-1}{2}$, $\mathcal{U}_1 \in \mathcal{C}_1$ and $(U_1 \mid U_2) \in \mathcal{M}_1$. Thus $(U_1 \mid U_2) = (I_k \mid U_2)$ and $\dim(\mathcal{U}_1) = \dim(\mathcal{U}) = k$. We also know $\dim(\mathcal{V}_1) \leq \dim(\mathcal{V})$ and $\dim(\mathcal{U}_1 \cap \mathcal{V}_1) \geq \dim(\mathcal{U} \cap \mathcal{V})$. So

we have

$$\begin{aligned}
\mathrm{d}_S(\mathcal{U}_1, \mathcal{V}_1) &= \dim(\mathcal{U}_1) + \dim(\mathcal{V}_1) - 2\dim(\mathcal{U}_1 \cap \mathcal{V}_1) \\
&\leq \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2\dim(\mathcal{U} \cap \mathcal{V}) \\
&= \mathrm{d}_S(\mathcal{U}, \mathcal{V}) \\
&\leq \frac{d-1}{2} \\
&\leq \frac{\mathrm{d}_S(\mathcal{C}_1) - 1}{2}
\end{aligned}$$

Hence $\mathcal{V}_1$ is decodable in $\mathcal{C}_1$ and $\mathrm{im}\,(I_k \mid U_2)$ is the unique closest codeword to $\mathcal{V}_1$.

Let $\tilde{\mathcal{U}_2} = \mathrm{im}\,(I_k \mid U_3) \in \Lambda(\mathcal{C}_R)$ and $\tilde{\mathcal{V}_2} = \mathrm{im}\,(V_1 \mid V_3)$. Then by the same argument as before

$$\mathrm{d}_S(\tilde{\mathcal{U}_2}, \tilde{\mathcal{V}_2}) \leq \frac{d-1}{2} \leq \frac{2\mathrm{d}_R(\mathcal{C}_R) - 1}{2}.$$

Hence $\tilde{\mathcal{V}_2}$ is decodable in $\Lambda(\mathcal{C}_R)$ and $\mathrm{im}\,(I_k \mid U_3)$ is the unique closest codeword to $\tilde{\mathcal{V}_2}$. Thus, we see that $\mathcal{U} = \mathrm{im}\,(I_k \mid U_2 \mid U_3)$ must be the closest codeword by uniqueness. ■

By this theorem, we can use the following algorithm to decode such linkage codes.

Algorithm 2: Decoding Algorithm for Special Case from Example 36

Data: a decodable K-dimension subspace $\mathcal{V} = \mathrm{im}\ (V_1 \mid V_2 \mid V_3)$, $(V_1 \mid V_2 \mid) \in \mathbb{F}_q^{K \times n}$

Result: the unique $\mathcal{U} \in \mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2$ such that $\mathrm{d}_S(\mathcal{V}, \mathcal{U}) \leq \frac{d-1}{2}$.

if $\mathrm{rank}\,(V_1 \mid V_2) \leq \frac{K-1}{2}$ **then**
  decode $\mathrm{im}\,(V_3)$ in $\mathcal{C}_2$ to $\mathrm{im}\,(U_3)$;
  return $\mathcal{U} = \mathrm{im}\ (0 \mid 0 \mid U_3)$.
else
  decode $\mathrm{im}\,(V_1 \mid V_2)$ in $\mathcal{C}_1$ to $\mathrm{im}\,(I_k \mid U_2)$;
  decode $\mathrm{im}\,(V_1 \mid V_3)$ in $\Lambda(\mathcal{C}_R)$ to $\mathrm{im}\,(I_k \mid U_3)$;
  return $\mathcal{U} = \mathrm{im}\ (I_k \mid U_2 \mid U_3)$.
end

Recalling that lifted Gabidulin codes can be efficiently decoded, see [35, 29], we can use them to create an efficiently decodable linkage code. This theorem shows that if we link a lifted Gabidulin code with an efficiently decodable $\mathcal{C}_2$ by a Gabidulin code, we have an efficiently decodable linkage code. As we saw in Example 36, we can construct these lifted MRD linkage codes, which have decent cardinality in comparison to other decodable constructions and are larger than standard lifted Gabidulin codes.

So we see that the linkage construction is a useful recursive construction. It allows us to create large and sometimes efficiently decodable codes. Additionally, it nicely generalizes two partial spread constructions and provides a nice framework to study maximum and maximal partial spreads. The linkage construction also leaves room for cardinality improvement, since the linkage construction will improve as other constructions improve.

Bibliography

[1] Rudolf Ahlswede, Ning Cai, Shuo-Yen Robert Li, and Raymond W. Yeung. Network information flow. *IEEE Trans. Inform. Theory*, 46(4):1204–1216, 2000.

[2] Eli Ben-Sasson, Tuvi Etzion, Ariel Gabizon, and Netanel Raviv. Subspace polynomials and cyclic subspace codes. arXiv:1404.7739.

[3] Albrecht Beutelspacher. Partial spreads in finite projective spaces and partial designs. *Math. Z.*, 145(3):211–229, 1975.

[4] Michael Braun, Tuvi Etzion, Patroc Östergård, Alexander Vardy, and Alfred Wassermann. Existence of q-analogs of steiner systems. arXiv:1304.1462v2.

[5] Michael Braun and Jan Reichelt. q-analogs of packing designs. *J. Combin. Des.*, 22(7):306–321, 2014.

[6] Javier de la Cruz, Michael Kiermeier, Alfred Wassermann, and Wolfgang Willems. Algebraic structures of mrd codes. arXiv: 1502.02711.

[7] Ph. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *J. Combin. Theory Ser. A*, 25(3):226–241, 1978.

[8] David A. Drake and J. W. Freeman. Partial t-spreads and group constructible (s, r, μ)-nets. *J. Geom.*, 13(2):210–216, 1979.

[9] S. El-Zanati, H. Jordon, G. Seelinger, P. Sissokho, and L. Spence. The maximum size of a partial 3-spread in a finite vector space over $\mathbb{F}_2$. 54:101–107, 2010.

[10] Tuvi Etzion and Natalia Silberstein. Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams. *IEEE Trans. Inform. Theory*, 55(7):2909–2919, 2009.

[11] Tuvi Etzion and Natalia Silberstein. Codes and designs related to lifted MRD codes. *IEEE Trans. Inform. Theory*, 59(2):1004–1017, 2013.

[12] Tuvi Etzion and Alexander Vardy. Error-correcting codes in projective space. *IEEE Trans. Inform. Theory*, 57(2):1165–1173, 2011.

[13] È. M. Gabidulin. Theory of codes with maximal rank distance. *Probl. Inf. Transm.*, 21:1–12, 1985.

[14] Heide Gluesing-Luerssen, Katherine Morrison, and Carolyn Troha. Cyclic orbit codes and stabilizer subfields. *Adv. Math. Commun.*, 9(2):177–197, 2015.

[15] Heide Gluessing-Luerssen. Private Communications.

[16] Elisa Gorla, Felice Manganiello, and Joachim Rosenthal. An algebraic approach for decoding spread codes. *Adv. Math. Commun.*, 6(4):443–466, 2012.

[17] Elisa Gorla and Alberto Ravagnani. Spaces of matrices with bounded rank and given shape. arXiv:1405.2736.

[18] Elisa Gorla and Alberto Ravagnani. Partial spreads in random network coding. *Finite Fields Appl.*, 26:104–115, 2014.

[19] Bryan Hernandez and Virgilio Sison. Grassmannian codes as lifts of matrix codes derived as images of linear block codes over finite fields. arXiv: 1502.04210.

[20] J. W. P. Hirschfeld. *Projective geometries over finite fields*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, second edition, 1998.

[21] Azadeh Khaleghi, Danilo Silva, and Frank R. Kschischang. Subspace codes. *Cryptography and Coding*, LNCD 5921:1–21, 2009.

[22] Axel Kohnert and Sascha Kurz. Construction of large constant dimension codes with a prescribed minimum distance. In *Mathematical methods in computer science*, volume 5393 of *Lecture Notes in Comput. Sci.*, pages 31–42. Springer, Berlin, 2008.

[23] Ralf Kötter and Frank R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Trans. Inform. Theory*, 54(8):3579–3591, 2008.

[24] Shuo-Yen Robert Li, Raymond W. Yeung, and Ning Cai. Linear network coding. *IEEE Trans. Inform. Theory*, 49(2):371–381, 2003.

[25] Felice Manganiello, Elisa Gorla, and Joachim Rosenthal. Spread codes and spread decoding in network coding. In *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, pages 881–885, July 2008.

[26] Joachim Rosenthal and Anna-Lena Trautmann. A complete characterization of irreducible cyclic orbit codes and their pl ucker embedding. *Designs Codes Cryptography*, 66:275–289, 2013.

[27] Natalia Silberstein and Anna-Lena Trautmann. Subspace codes based on graph matchings, ferrers diagrams and pending blocks. arXiv:1404.6723.

[28] Danilo Silva and Frank R. Kschischang. On metrics for error correction in network coding. *IEEE Trans. Inform. Theory*, 55(12):5479–5490, 2009.

[29] Danilo Silva, Frank R. Kschischang, and Ralf Kötter. A rank-metric approach to error control in random network coding. *IEEE Trans. Inform. Theory*, 54(9):3951–3967, 2008.

[30] Vitaly Skachek. Recursive code construction for random networks. *IEEE Trans. Inform. Theory*, 56(3):1378–1382, 2010.

[31] Anna-Lena Trautmann. Message encoding for spread and orbit codes. arXiv:1401.0615.

[32] Anna-Lena Trautmann. Isometry and automorphisms of constant dimension codes. *Adv. Math. Commun.*, 7(2):147–160, 2013.

[33] Anna-Lena Trautmann, Felice Manganiello, Michael Braun, and Joachim Rosenthal. Cyclic orbit codes. *IEEE Trans. Inform. Theory*, 59(11):7386–7404, 2013.

[34] Anna-Lena Trautmann and Joachim Rosenthal. New improvements on the echelon-ferrers construction. In *Proceeding of the 19th International Symposium on Mathematical Theory of Networks and Systems -MTNS (Budapest, Hungary)*, pages 405–408, Jul 2010.

[35] Antonia Wachter-Zeh, Valentin Afanassiev, and Vladimir Sidorenko. Fast decoding of Gabidulin codes. *Des. Codes Cryptogr.*, 66(1-3):57–73, 2013.

[36] Antonia Wachter-Zeh and Tuvi Etzion. Optimal ferrers diagram rank-metric codes. arXiv:1405.1885.

[37] Shu-Tao Xia and Fang-Wei Fu. Johnson type bounds on constant dimension codes. *Des. Codes Cryptogr.*, 50(2):163–172, 2009.

Vita

Carolyn E. Troha

Education

- **University of Kentucky**, Lexington Kentucky
  M.A. in Mathematics, August 2011
- **College of William and Mary**, Williamsburg, VA
  B.S., Mathematics and Classical Studies, with high honors, *magna cum laude*

Teaching Experience

- **Teaching Assistant**, University of Kentucky August 2009-May 2015

Publications

- (with H. Gluesing-Luerssen and K. Morrison) Cyclic Orbit Codes and Stabilizer Subfields. In *Advances in Mathematics of Communications*. Vol. 9, No. 2, pp. 177-197, 2015.

Awards and Fellowships

- **University of Kentucky**, Lexington Kentucky
  - Edgar Enochs Algebra Scholarship, May 2014
  - Van Meter Fellowship, August 2009 - May 2012
  - Graduate Fellowship for Selected Areas, Spring 2010
- **College of William and Mary**, Williamsburg, VA
  - Phi Beta Kappa, Alpha of Virginia, inducted Fall 2008