CONSTRUCTIONS OF MAXIMUM RANK DISTANCE CODES, CYCLIC CONSTANT DIMENSION CODES, AND SUBSPACE PACKINGS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

KAMIL OTAL

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
CRYPTOGRAPHY

AUGUST 2018

Approval of the thesis:

CONSTRUCTIONS OF MAXIMUM RANK DISTANCE CODES, CYCLIC CONSTANT DIMENSION CODES, AND SUBSPACE PACKINGS

submitted by **KAMIL OTAL** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Cryptography Department, Middle East Technical University** by,

Prof. Dr. Ömür Uğur _____
Director, Graduate School of **Applied Mathematics**

Prof. Dr. Ferruh Özbudak _____
Head of Department, **Cryptography**

Prof. Dr. Ferruh Özbudak _____
Supervisor, **Department of Mathematics & IAM, METU**

Examining Committee Members:

Assoc. Prof. Dr. Ali Doğanaksoy
Department of Mathematics & IAM, METU _____

Prof. Dr. Ferruh Özbudak
Department of Mathematics & IAM, METU _____

Prof. Dr. Gülin Ercan
Department of Mathematics, METU _____

Assoc. Prof. Dr. Sedat Akleylek
Department of Computer Engineering, Ondokuz Mayıs University _____

Assoc. Prof. Dr. Burcu Gülmez Temür
Department of Mathematics, Atılım University _____

Date: _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: KAMIL OTAL

Signature :

ABSTRACT

CONSTRUCTIONS OF MAXIMUM RANK DISTANCE CODES, CYCLIC CONSTANT DIMENSION CODES, AND SUBSPACE PACKINGS

Otal, Kamil
Ph.D., Department of Cryptography
Supervisor : Prof. Dr. Ferruh Özbudak

August 2018, 40 pages

In this thesis, we aim to introduce main contributions to solve three main problems in coding theory.

The first problem investigates the construction of inequivalent maximum rank distance (MRD) codes. Namely, we look for the constructions of the largest possible sets of $m \times n$ matrices over a finite field $\mathbb{F}_q$, such that the rank of the subtraction of any two different matrices in the set cannot be smaller than a certain number. Constructions of such codes under a suitable equivalence notion have taken a worthwhile attention in the last decade due to their applications in many areas, and most of the constructions including also our works have been discovered in last few years. We introduce these outcomes classifying them considering the main and most general equivalence idea. We basically use the language of linearized polynomials in this direction as usual in many works in the literature.

The second problem, which is originated from an application related to the efficiency in random network coding, concerns the construction of large cyclic subspace codes of constant dimension. In this set up, we aim to construct large sets of k-dimensional subspaces of $\mathbb{F}_q^n$ in a way that any two distinct subspaces cannot be close to each other more than a certain number in terms of the subspace distance, and the cyclic shifts of each subspace must be included in the set. We give the only systematic construction

of such sets in the literature utilizing linearized polynomials again but in a slightly different way. We note that the basic structure of this construction was proposed in our another work. Additionally, we summarize the history of the solution and some further remarks.

In the last problem, we focus on the constructions of subspace packings, which are the q-analogue of packing designs. This notion is a natural generalization of constant dimension codes, and has applications in the analysis of different network codes. We give a recursive construction of such codes using a generalization of the linkage construction rather than linearized polynomials. In particular, we make use of the matrix version of MRD codes together with some facts from linear algebra. This result is one of the main outcomes of our recent work.

We express that these problems are different from but substantially related to each other. Connections among them are also expressed in related places. Furthermore, we remark that various areas of mathematics are used to solve these problems in general, e.g. finite geometry, algebraic geometry, algebra, and linear algebra. Therefore, it is not easy to introduce all advances properly with their complete preliminary information here. Moreover, we try to keep our language as simple as possible, and follow the historical journey of the advances. In that way, we target that this thesis can addresses to a more general reader group.

Keywords: linearized polynomials, subspace polynomials, rank metric codes, maximum rank distance (MRD) codes, subspace codes, constant dimension codes, random network coding, subspace packings.

ÖZ

MAKSİMUM RANK UZAKLIKLI KODLARIN, DEVİRLİ SABİT BOYUT KODLARININ, VE ALTUZAY PAKETLEMELERİNİN İNŞASI

Otal, Kamil
Doktora, Kriptografi Bölümü
Tez Yöneticisi : Prof. Dr. Ferruh Özbudak

Ağustos 2018 , 40 sayfa

Bu tezde, kodlama teorisindeki üç ana probleme çözümler sunan temel katkıları tanıtmayı amaçlıyoruz.

İlk problem birbirine denk olmayan maksimum rank uzaklıklı (MRD) kodların inşasını inceliyor. Yani, $\mathbb{F}_q$ üzerindeki $m \times n$ matrislerin mümkün olan en büyük kümesinin inşasını, kümedeki iki farklı matrisin farkının rankı belirli bir sayıdan küçük olamayacak şekilde ele alarak araştırıyoruz. Bu tarz kodların uygun bir denklik fikri altındaki inşaları son on yılda başka alanlardaki uygulamaları sebebiyle kaydadeğer bir ilgi topladı, ve bizim çalışmalarımızı da içeren inşaların çoğu son birkaç yılda keşfedildi. Bu inşa yöntemlerini, temel ve en genel denklik fikrini dikkate alıp sınıflandırarak veriyoruz. Bu doğrultuda, literatürdeki birçok işte de gözlendiği gibi, temel olarak lineerleştirilmiş polinomların dilini kullanıyoruz.

Rastgele ağ kodlamadaki etkin hesaplama ile ilgili bir uygulamadan kaynaklanan ikinci problem, büyük sabit boyutlu ve devirli altuzay kodlarının inşasını dikkate alıyor. Bu kurgu dahilinde, $\mathbb{F}_q^n$'nin k-boyutlu altuzaylarından oluşan büyük bir kümeyi, kümedeki birbirinden farklı iki altuzayın birbirine olan altuzay uzaklığı belirli bir sayıdan daha yakın olmayacak şekilde ve her bir altuzayın devirli kaydırılmışı da küme içinde kalacak şekilde inşa etmeyi amaçlıyoruz. Bu tarz kodların literatürdeki tek sistematik inşasını yine lineerleştirilmiş polinomları ama bu sefer biraz farklı şe-

kilde kullanarak tanıtıyoruz. Belirtmek isteriz ki bu inşanın ana yapısı bizim bir diğer çalışmamızda sunulmuştur. Ek olarak, çözümün tarihini ve bazı ilgili notları özetliyoruz.

Son problemde, paketleme tasarımlarının q-analoğu olan altuzay paketlemelerinin inşasına odaklanıyoruz. Bu fikir sabit boyut kodlarının doğal bir genelleştirmesidir, ve farklı ağ kodlarının analizinde uygulamaları vardır. Bu tarz kodların yinelemeli bir inşasını, lineerleştirilmiş polinomlar yerine "linkage" inşa metodunun bir genelleştirmesini kullanarak veriyoruz. Özellikle, MRD kodların matris versiyonlarından ve lineer cebirdeki bazı araçlardan faydalanıyoruz. Bu inşa yöntemi bizim son çalışmamızdaki ana sonuçlardan biridir.

Bu problemlerin birbirinden farklı ama birbirleriyle oldukça bağlantılı olduğunu belirtiriz. Aralarındaki bağlantılar da ilgili yerlerde veriliyor. Ayrıca not etmek isteriz ki genel olarak matematiğin sonlu geometri, cebirsel geometri, cebir, ve lineer cebir gibi çeşitli alanları bu problemleri çözmek için kullanılmıştır. Bundan dolayı, tüm gelişmeleri gerekli ön bilgilerini de tam bir şekilde burada vererek sunmak kolay değildir. Üstelik, dilimizi mümkün mertebe basit tutmaya çalışıyoruz, ve gelişmelerin tarihi seyrini takip ediyoruz. Bu şekilde, daha genel bir okuyucu grubuna hitap etmeyi hedefliyoruz.

Anahtar Kelimeler: lineerleştirilmiş polinomlar, altuzay polinomları, rank uzaklıklı kodlar, maksimum rank uzaklıklı kodlar, altuzay kodları, sabit boyut kodları, rastgele ağ kodlama, altuzay paketlemeleri.

ACKNOWLEDGMENTS

First and foremost, I would like to extend my sincere thanks to my supervisor Ferruh Özbudak for his patient guidance, enthusiastic encouragement and valuable advices during my Ph.D. education.

My thanks are also to Sedat Akleylek, Ersan Akyıldız, Ali Doğanaksoy, Gülin Ercan, Burcu Gülmez Temür, Ali Ulaş Özgür Kişisel, and Oğuz Yayla for being committee members of my defense.

I wish to record my deep sense of appreciation and thankfulness to all members of Department of Mathematics and Institute of Applied Mathematics at Middle East Technical University. In particular, I am grateful to all my colleagues for their close friendship and pleasant times.

I wish to extend my profound thanks to my teacher Mehpare Bilhan for her generous teaching and warm attitude to all of her students. I owe a debt of gratitude to Murat Cenk, Zülfükar Saygı, and Çetin Ürtiş for their enduring support and encouragement.

I would like to thank the editors and anonymous reviewers of the papers resulting from our studies within my Ph.D. education for their valuable comments and suggestions. Especially, I thank Thomas Honold and the anonymous referees for their suggestions during the review process of my first paper.

I also would like to express my deep gratitude to Tuvi Etzion, Sascha Kurz, Edgar Martinez-Moro, and Wolfgang Willems for three different and invaluable collaborations. It is a great experience for me to work with and learn from them.

I gratefully acknowledge generous financial support from the Scientific and Technological Research Council of Turkey (TÜBİTAK) via programs 2211 and 2214/A. I also acknowledge my participation in and financial support from COST Action IC 1104 chaired by Marcus Greferath and Mario Osvin Pavčević between 2012-2016.

Lastly and most importantly, I wish to express my deepest gratitude to my family for their endless support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

FIGURES

LIST OF ABBREVIATIONS

$\mathbb{Z}$	The set of integers.
$\gcd(a, b)$	The greatest common divisor of a and b.
$\mathrm{lcm}(a, b)$	The least common multiple of a and b.
$a \mid b$	Expresses that b is a multiple of a.
$a \nmid b$	Expresses that b is not a multiple of a.
$\lvert E \rvert$	The size of a set E.
p	A prime number.
q	A power of a prime number.
$\mathbb{F}_q$	The finite field with q elements.
$\mathbb{F}_q^N$	The vector space of dimension N over $\mathbb{F}_q$.
$u \cdot v$	Classical inner product of vectors $u, v \in \mathbb{F}_q^N$.
$U^\perp$	The dual space of a subspace U of $\mathbb{F}_q^N$ with respect to the classical inner product.
$\mathbb{F}_q^{m \times n}$	The set of $m \times n$ matrices over $\mathbb{F}_q$.
$\mathrm{Norm}_{q^n/q}$	The relative norm function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$.
$f \circ g$	The composition $f(g(x))$ of polynomials f and g.

CHAPTER 1

INTRODUCTION

In this chapter, firstly we give an overview on the main goal of coding theory related to our contents. Later, we exemplify this goal introducing our motivating problems. Lastly, we summarize the outline of the other chapters.

1.1 Overview

The main concern in coding theory is to communicate fast and correctly. In this direction, a finite ambient set $\mathcal{A}$ endowed with a distance function (metric) d is taken. The elements of $\mathcal{A}$ are called *words*, some of which are determined as "meaningful", whereas the others are considered "meaningless". Meaningful words are called *codewords* and the set $\mathcal{C}$ of codewords in $\mathcal{A}$ is called a *code* or *dictionary*.

The idea of communication is to convey codewords to some other part on a communication channel. However, the "noise" level of the channel may alter the codewords and turn them into other codewords or meaningless words in $\mathcal{A}$. Therefore, the other part may not understand or misunderstand the original codeword. On the other hand, a corrupted codeword is expected to be in a close neighborhood of the original one. Accordingly, we need to determine $\mathcal{C}$ utilizing the metric function d on $\mathcal{A}$ in a suitable way. Namely, we require that the elements of $\mathcal{C}$ are distributed homogeneously in $\mathcal{A}$ as much as possible. In that way, the receiver can guess that the received word is originally the closest codeword to itself (error correction). In this set up, the minimum distance between any two distinct codewords is called the *minimum distance* of $\mathcal{C}$ and denoted by $d(\mathcal{C})$. Minimum distance of a code is the main security measure

of the code. In particular, for "noisier" channels we need to determine codes with larger minimum distances. However, an increase in $d(\mathcal{C})$ causes a decrease in the size of $\mathcal{C}$ for fixed $\mathcal{A}$. This trade-off yields a sphere packing problem, or an optimization problem in other words.

In addition to construct largest possible codes for a given minimum distance, we can need some further properties on the code depending on needs coming from computations. For instance, if we take $\mathcal{A}$ as a vector space, then choosing $\mathcal{C}$ as a subspace of $\mathcal{A}$ can be quite useful in many applications. Similarly, sometimes we can need to classify codes with respect to an equivalence notion, and discover new codes whenever possible. Such concerns are interesting because of not only their importance in applications but also their attractive theoretical structures.

In this thesis, we focus on the construction of three of such structures, and want to give all known contributions by classifying them and summarizing their history. In particular, the rest of this chapter is devoted to introduce the problems explicitly and highlight the contents of the thesis. We also note that we assume the reader has basic knowledge of linear algebra and finite fields.

1.2 Problem Settings

Let $\mathbb{F}_q^{m\times n}$ denote the set of $m \times n$ matrices over a finite field $\mathbb{F}_q$ of q elements. The function d defined on $\mathbb{F}_q^{m\times n} \times \mathbb{F}_q^{m\times n}$ by

$$d(A, B) := \mathrm{rank}(A - B)$$

satisfies the usual axioms of a metric, and is called the *rank distance* on $\mathbb{F}_q^{m\times n}$.

A subset $\mathcal{C}$ of the ambient space $\mathcal{A} = \mathbb{F}_q^{m\times n}$ including at least two elements and equipped with the rank distance is called a *rank metric code*. The *minimum distance* $d(\mathcal{C})$ of a rank metric code $\mathcal{C}$ is defined by $d(\mathcal{C}) := \min\{d(A, B) : A, B \in \mathcal{C} \text{ and } A \neq B\}$.

Note that, from a given rank metric code, we can produce another one, of the same size and minimum distance, by applying some basic operations. For example, multiplying all codewords from the right by an invertible $n \times n$ matrix we produce such

a second rank metric code. Therefore, new constructions are expected to give really "new" codes considering this issue. In other words, we need to define an equivalence notion between any two codes. The most general and widely used definition of equivalence is determined in [5] considering the set of all rank distance preserving maps under the light of [46, Theorem 3.4]: Two rank metric codes $\mathcal{C}, \mathcal{C}' \subseteq \mathbb{F}_q^{m\times n}$ are called *equivalent* if there exist $X \in GL(m, \mathbb{F}_q)$, $Y \in GL(n, \mathbb{F}_q)$, $Z \in \mathbb{F}_q^{m\times n}$, and an automorphism σ of $\mathbb{F}_q$ acting on the entries of a given matrix in $\mathbb{F}_q^{m\times n}$ such that

$$\begin{aligned} &\mathcal{C}' = X\mathcal{C}^\sigma Y + Z := \{XC^\sigma Y + Z : C \in \mathcal{C}\} \text{ when } m \neq n, \\ &\mathcal{C}' = X\mathcal{C}^\sigma Y + Z \text{ or } \mathcal{C}' = X(\mathcal{C}^t)^\sigma Y + Z \text{ when } m = n, \end{aligned} \tag{1.1}$$

where the superscript t denotes the transposition of matrices. Observe that Z must be the zero matrix if both $\mathcal{C}$ and $\mathcal{C}'$ are additive, i.e. closed under addition. Furthermore, if both $\mathcal{C}$ and $\mathcal{C}'$ are linear over $\mathbb{F}_q$, then σ can be taken as the identity without loss of generality. This equivalence idea have been used in different forms and scopes in several works [5, 23, 25, 27, 29, 30, 33, 34, 36, 37, 38, 45].

Rank metric codes have a well-known upper bound, called *Singleton-like bound*, for a given minimum distance. We state it as follows.

Proposition 1.2.1. *[8] Assume $m \leq n$ without loss of generality. Let $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ be a rank metric code, then $|\mathcal{C}| \leq q^{n(m-d(\mathcal{C})+1)}$.*

An elementary proof for this proposition can be given as follows.

Proof. Let d denote $d(\mathcal{C})$ for short, and $\mathcal{C}' \subseteq \mathbb{F}_q^{(m-d+1)\times n}$ be the set of matrices obtained by deleting the last $d-1$ rows of codewords in $\mathcal{C}$. If $A, B \in \mathcal{C}$ are distinct codewords, then so are their images $A', B' \in \mathcal{C}'$, as $d(A, B) = \operatorname{rank}(A-B) > d-1$. This implies that $|\mathcal{C}| = |\mathcal{C}'|$. Also the inclusion $\mathcal{C}' \subseteq \mathbb{F}_q^{(m-d+1)\times n}$ implies $|\mathcal{C}'| \leq q^{n(m-d+1)}$, which means $|\mathcal{C}| \leq q^{n(m-d+1)}$. □

We call a rank metric code *maximum rank distance (MRD)* if the Singleton-like bound is met. MRD codes exist for all q, m, n and d [8, 16, 35] and have various applications, for example, in random network coding [40], space-time coding [24, 43], distributed storage [39], and cryptography [41].

The number of inequivalent MRD codes increase while the parameters get larger [36]. This result is very similar to the classification of finite groups in group theory. Therefore, the classification and finding new MRD codes problem has gained interest and many constructions appeared especially in the last decade, see for example [4, 9, 11, 21, 23, 29, 30, 33, 34, 37, 38, 45]. We briefly express it as the first motivating problem of the thesis as follows.

Problem 1. *For which parameters and how can we construct new classes of MRD codes with respect to the equivalence idea given in (1.1)?*

Now we give some basic definitions and facts and then introduce the second problem. Note that the finite field $\mathbb{F}_{q^N}$ is also a vector space over $\mathbb{F}_q$. We call the set of all subspaces of $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$ as *projective space* of (vector) dimension N over $\mathbb{F}_q$ and denote by $\mathcal{P}_q(N)$. The set of all k dimensional elements of $\mathcal{P}_q(N)$ is called *Grassmannian space* (or briefly *Grassmannian*) over $\mathbb{F}_q$ and denoted by $\mathcal{G}_q(N,k)$. The metric d on $\mathcal{P}_q(N)$ given by

$$d(U,V) := \dim U + \dim V - 2\dim(U \cap V)$$

is called the *subspace distance*. A subset $\mathcal{C} \subseteq \mathcal{P}_q(N)$ including at least two elements and equipped with this metric is called a *subspace code*. If moreover $\mathcal{C} \subseteq \mathcal{G}_q(N,k)$, then $\mathcal{C}$ is called a *constant dimension code*. We define the *minimum distance* $d(\mathcal{C})$ of a subspace code $\mathcal{C}$ by $d(\mathcal{C}) := \min\{d(U,V) : U,V \in \mathcal{C} \text{ and } U \neq V\}$ naturally. A *cyclic shift* of a subspace $U \subseteq \mathbb{F}_{q^N}$ is given by $\alpha U := \{\alpha u : u \in U\}$, where $\alpha \in \mathbb{F}_{q^N}^*$. Observe that a cyclic shift is a subspace of $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$ of the same dimension. A subspace code $\mathcal{C}$ is called *cyclic* if $\alpha U \in \mathcal{C}$ for all $U \in \mathcal{C}$ and $\alpha \in \mathbb{F}_{q^N}^*$, and *quasi-cyclic* if $\alpha U \in \mathcal{C}$ for all $U \in \mathcal{C}$ and $\alpha \in G$, where G is a multiplicative subgroup of $\mathbb{F}_{q^N}^*$. Quasi-cyclic codes are also known as “(cyclic) orbit codes" (see, for example, [17, 44]).

Remark 1.2.1. *Note that we use d to denote both the subspace distance and the rank distance functions together, but we think that there is a less possibility to confuse them in this thesis. It is because, they are defined on different ambient spaces, also we examine them in separate chapters, Chapter 2 and Chapter 3.*

Subspace codes constitute the main mathematical structure in random network coding by reason of their error correction capabilities shown in [20]. Cyclic subspace codes have a particular interest with their efficient encoding and decoding algorithms. They were firstly presented in [20] from the design theoretical perspective, and then they are defined in [13] as the q-analogue of classical cyclic codes. They are also studied in [44] and [17] from the point of view of group actions. Constructions of such codes is the second main problem of in this thesis, and we state it briefly as follows.

Problem 2. *How can we construct large cyclic subspace codes systematically?*

The third problem considers a generalization of subspace distance but the code does not require to include cyclic shifts of codewords. Now we present the third problem explicitly. Let $1 \leq s \leq k \leq N$ and $\lambda \geq 1$. Also let $\mathcal{C}$ be a set of k-dimensional subspaces of $\mathbb{F}_q^N$ such that any s-dimensional subspace of $\mathbb{F}_q^N$ is covered by at most λ elements of $\mathcal{C}$. In other words, $\mathcal{C}$ satisfies

$$\dim(U_1 \cap \cdots \cap U_{\lambda+1}) \leq s-1$$

for all distinct $U_1, \ldots, U_{\lambda+1} \in \mathcal{C}$. We call such sets *subspace packings*. Subspace packings are q-analogue of packing designs and the construction of large packing designs is an important problem in design theory, see surveys [26, 42]. Similarly, our ultimate purpose is to construct large subspace packings, see survey [2] for example. This problem has a recent application to network coding [14, 15].

Let $A_q(N, k, s; \lambda)$ denote the largest possible size of a subspace packing, we give the mathematical setup of this problem as follows.

Problem 3. *How can we construct large, preferably of size $A_q(N, k, s; \lambda)$, subspace packings?*

1.3 Organization

We give the outline of the other chapters as follows.

Chapter 2 is devoted to contributions related to Problem 1. In particular, Section 2.1 basically gives mathematical background: the introduction of linearized polynomials over finite fields and their fundamental properties in Section 2.1.1, the connection between linearized polynomials and rank metric codes in Section 2.1.2, and lastly a quite fruitful lemma and its proof in Section 2.1.3. We then propose three large families obtained by diverse constructions in Sections 2.2, 2.3, and 2.4 separately. Later on, we list concise information on the other constructions in Section 2.5. Finally, we list some further remarks and comments regarding Problem 1 and its solutions in Section 2.6.

Chapter 3 mainly introduces the unique systematic solution to Problem 2 in the literature. In particular, we utilize subspace polynomials – a special class of linearized problems introduced in Section 3.1. Later we state and prove our main result, Theorem 5, in Section 3.2.

In Chapter 4, we initially present a different approach to Problem 3 in the first section. Later, we state the main theorem, Theorem 6, together with further remarks in Section 4.2. The last section proves Theorem 6 considering the cases separately.

In the last chapter, we briefly discuss the main results of the thesis emphasizing the profiles of the methods to build them.

CHAPTER 2

CONSTRUCTIONS OF MAXIMUM RANK DISTANCE CODES

In this chapter, we introduce all basic constructions of MRD codes. Hence, this chapter can be seen as an updated and slightly extended version of Section 3 of our work [32]. We use the language of linearized polynomials as usual in many recent works (see for example [23, 29, 30, 33, 34, 38, 45]). We introduce such polynomials in Section 2.1 and then give three large families of MRD codes in Sections 2.2, 2.3, and 2.4. We emphasize that the families given in Sections 2.2 and 2.4 are the among our contributions proposed in [30] and [33] respectively. Lastly, we mention other constructions briefly in Section 2.5 and concluding remarks in Section 2.6.

2.1 Preliminaries

This section aims to define and explain one of the main mathematical concepts of the thesis. First subsection is devoted to linearized polynomials, the second subsection gives their connections to rank metric codes, and the last one proposes a very practical tool, Lemma 2.1.1.

2.1.1 Linearized Polynomials

A polynomial $f(x) \in \mathbb{F}_{q^n}[x]$ of the form

$$f(x) = \sum_{i=0}^{l} \alpha_i x^{q^i} \tag{2.1}$$

is called a *q-polynomial* (or, a *linearized polynomial*) over $\mathbb{F}_{q^n}$. We call l the *q-degree* of f if $\alpha_l \neq 0$. Some important properties of such polynomials can be given as follows.

- $f(c\alpha + \beta) = cf(\alpha) + f(\beta)$ for all $c \in \mathbb{F}_q$ and $\alpha, \beta \in \overline{\mathbb{F}}_q$, where $\overline{\mathbb{F}}_q$ denotes the algebraic closure of $\mathbb{F}_q$.
- Each root of f in $\overline{\mathbb{F}}_q$ has the multiplicity q^r where r is the smallest integer satisfying $\alpha_r \neq 0$.
- The roots of f in an extension of $\mathbb{F}_{q^n}$ constitute a vector space over $\mathbb{F}_q$. Specially, the set of roots of f in $\mathbb{F}_{q^n}$ is a subspace of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. This space is called the *kernel* of f and denoted by $\ker(f)$. The *rank* of f is defined by $n - \dim(\ker(f))$ and denoted by $\mathrm{rank}(f)$.

2.1.2 Polynomial Representation of Rank Metric Codes

Let $f(x) \in \mathbb{F}_{q^n}[x]$ be a q-polynomial of q-degree at most $n-1$. Let $\{\epsilon_1, \epsilon_2, \ldots, \epsilon_n\}$ and $\{\delta_1, \delta_2, \ldots, \delta_n\}$ be two ordered bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then, for all $\alpha \in \mathbb{F}_{q^n}$ we have

$$\begin{aligned} f(\alpha) &= f(c_1\delta_1 + c_2\delta_2 + \cdots + c_n\delta_n) \\ &= c_1 f(\delta_1) + c_2 f(\delta_2) + \cdots + c_n f(\delta_n) \\ &= \begin{bmatrix} f(\delta_1) & f(\delta_2) & \ldots & f(\delta_n) \end{bmatrix} \begin{bmatrix} c_1 & c_2 & \ldots & c_n \end{bmatrix}^t \\ &= [\epsilon_1\ \epsilon_2\ \ldots\ \epsilon_n] \begin{bmatrix} f(\delta_1)_{\epsilon_1} & f(\delta_2)_{\epsilon_1} & \ldots & f(\delta_n)_{\epsilon_1} \\ f(\delta_1)_{\epsilon_2} & f(\delta_2)_{\epsilon_2} & \ldots & f(\delta_n)_{\epsilon_2} \\ \vdots & \vdots & \ddots & \vdots \\ f(\delta_1)_{\epsilon_n} & f(\delta_2)_{\epsilon_n} & \ldots & f(\delta_n)_{\epsilon_n} \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} \end{aligned} \tag{2.2}$$

for some $c_i \in \mathbb{F}_q$ for $1 \leq i \leq n$, where $f(\delta_i)_{\epsilon_j}$ denotes the coefficient of ϵ_j when $f(\delta_i)$ is written as a linear combination of $\epsilon_1, \ldots, \epsilon_n$, for all $1 \leq i, j \leq n$. Let F denote the matrix given by $[f(\delta_i)_{\epsilon_j}]_{i,j} \in \mathbb{F}_q^{n\times n}$, equation (2.2) says that there is a one to one correspondence between f and F with respect to the fixed ordered bases $\{\epsilon_1, \epsilon_2, \ldots, \epsilon_n\}$ $\{\delta_1, \delta_2, \ldots, \delta_n\}$. Furthermore, we have $\mathrm{rank}(F) = \mathrm{rank}(f)$. Moreover, the algebra $\mathbb{F}_q^{n\times n}$ with the matrix addition and the matrix multiplication corresponds to the

algebra

$$\mathcal{L}_n := \{\alpha_0 x + \alpha_1 x^q + \cdots + \alpha_{n-1} x^{q^{n-1}} : \alpha_0, \ldots, \alpha_{n-1} \in \mathbb{F}_{q^n}\}$$

with the addition and the composition of polynomials modulo $x^{q^n} - x$, respectively.

Let $f(x) = \sum_{i=0}^{n-1} \alpha_i x^{q^i} \in \mathcal{L}_n$ and let $\{\delta_1, \delta_2, \ldots, \delta_n\}$ given above be a normal basis. Also take $\epsilon_i = \delta_i$ for all $i = 1, \ldots, n$. Then, the correspondence $f \leftrightarrow F$ above implies the correspondence $\widehat{f} \leftrightarrow T^{-1}F^tT$, where $\widehat{f}$ is given by $\widehat{f}(x) = \sum_{i=0}^{n-1} \alpha_{n-i}^{q^i} x^{q^i} \mod x^{q^n} - x$, the subscripts of the coefficients are given modulo n, and T is a particular invertible matrix. Here, $\widehat{f}$ is called the *adjoint* of f.

We consider the algebra $\mathcal{L}_n$ as the ambient space instead of the algebra $\mathbb{F}_q^{n\times n}$ while studying rank metric codes. Accordingly, we can inherit the equivalence notion (1.1) in case σ is identity as follows: Let $\mathcal{C}$ and $\mathcal{C}'$ be two subsets of $\mathcal{L}_n$ (both including at least two elements), then $\mathcal{C}$ and $\mathcal{C}'$ are equivalent if there exist $g_1, g_2, g_3 \in \mathcal{L}_n$ such that $g_1(x)$ and $g_2(x)$ are invertible and

$$\begin{aligned}
\mathcal{C}' &= g_1(x) \circ \mathcal{C} \circ g_2(x) + g_3(x) \\
&:= \{g_1(x) \circ f(x) \circ g_2(x) + g_3(x) \mod x^{q^n} - x : f(x) \in \mathcal{C}\}, \text{ or} \\
\mathcal{C}' &= g_1(x) \circ \widehat{\mathcal{C}} \circ g_2(x) + g_3(x) \\
&:= \{g_1(x) \circ \widehat{f}(x) \circ g_2(x) + g_3(x) \mod x^{q^n} - x : f(x) \in \mathcal{C}\},
\end{aligned} \tag{2.3}$$

where the $\circ$ operation denotes the composition. Note also that, if $\mathcal{C}$ is closed under addition, then the minimum distance $d(\mathcal{C})$ is indeed the minimum non-zero rank of the elements in $\mathcal{C}$. We prefer to represent rank metric codes using $\mathcal{L}_n$ instead of $\mathbb{F}_q^{n\times n}$ as the ambient space, since polynomials are independent of any bases and hence seem to be more brief and neat to represent rank metric codes. Also the arithmetic on polynomials seems easier than the one on matrices.

Note that, from a code $\mathcal{C} \subseteq \mathbb{F}_q^{n\times n}$ of minimum distance d, by deleting the last $n - m$ rows (or columns) for some $m < n$, we can obtain another code $\mathcal{C}' \subseteq \mathbb{F}_q^{m\times n}$ (or $\subseteq \mathbb{F}_q^{n\times m}$) of distance $d-n+m$. We call this procedure *puncturing* and $\mathcal{C}'$ a *punctured code*. Here, if $\mathcal{C}$ is an MRD code then so is $\mathcal{C}'$. Therefore, these constructions can be used to produce MRD codes of rectangular matrices. In the following chapter, we give constructions of MRD codes mainly for $m = n$.

2.1.3 A Useful Tool

We now give an important lemma used to construct three large families of MRD codes introduced in the following three sections. Before stating it, we remember the definition of norm function $\mathrm{Norm}_{q^n/q}$ on $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$: $\mathrm{Norm}_{q^n/q}(x) := x^{1+q+\cdots+q^{n-1}}$. Also we recall that a q-polynomial $f(x) \in \mathbb{F}_{q^n}[x]$ of q-degree l can have at most q^l roots, i.e. $\dim(\ker(f)) \leq l$ by the fundamental theorem of algebra.

Lemma 2.1.1. *[19] Let $f(x) = \alpha_0 x + \alpha_1 x^q + \cdots + \alpha_l x^{q^l} \in \mathbb{F}_{q^n}[x]$ be a q-polynomial of q-degree l, where $0 < l < n$. If $\mathrm{Norm}_{q^n/q}(\alpha_l) \neq (-1)^{nl}\mathrm{Norm}_{q^n/q}(\alpha_0)$, then $\dim(\ker(f)) \leq l - 1$.*

An elementary proof of Lemma 2.1.1, which is also available in [38], can be given as follows.

Proof. Observe that there is a one to one correspondence between an l-dimensional subspace U of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and a monic q-polynomial of q-degree l annihilating U, let us denote this polynomial by m_U. Every linearized polynomial of q-degree l annihilating U is an $\mathbb{F}_{q^n}$-multiple of m_U, and so it suffices to prove the result for any particular linearized polynomial of q-degree l annihilating U. Choose an $\mathbb{F}_q$-basis $\{\delta_1, \ldots, \delta_l\}$ of U, and define a q-polynomial f as follows.

$$f(x) := \det \begin{bmatrix} x & x^q & \ldots & x^{q^l} \\ \delta_1 & \delta_1^q & \ldots & \delta_1^{q^l} \\ \delta_2 & \delta_2^q & \ldots & \delta_2^{q^l} \\ \vdots & \vdots & \ddots & \vdots \\ \delta_l & \delta_l^q & \ldots & \delta_l^{q^l} \end{bmatrix} = \alpha_0 x + \alpha_1 x^q + \cdots + \alpha_l x^{q^l}.$$

Here, clearly f annihilates U, i.e. is a multiple of m_U. On the other hand, expanding along the top row gives that $\alpha_0 = (-1)^l \alpha_l^q$ and so $\mathrm{Norm}_{q^n/q}(\alpha_l) = (-1)^{nl}\mathrm{Norm}_{q^n/q}(\alpha_0)$, which completes the proof. □

2.2 Twisted Gabidulin Codes and their Generalizations

In this section, we give the first construction of MRD codes and its generalizations following their history. Theorem 1 and the following remarks at the end of this section

gives the most general version of this construction.

A natural construction of MRD codes can be given in the language of linearized polynomials as follows:

$$\mathcal{G}_{n,k} := \{\alpha_0 x + \alpha_1 x^q + \cdots + \alpha_{k-1} x^{q^{k-1}} : \alpha_i \in \mathbb{F}_{q^n} \text{ for all } 0 \leq i \leq k-1\}.$$

Observe that the size of $\mathcal{G}_{n,k}$ is clearly q^{nk}. Moreover, the dimension of kernel of the subtraction of any two distinct elements in $\mathcal{G}_{n,k}$ is less than or equal to $k-1$. In other words, $d(\mathcal{G}_{n,k}) \geq n-(k-1)$. These two facts prove that $\mathcal{G}_{n,k}$ is an MRD code. Moreover, $\mathcal{G}_{n,k}$ is a linear subspace of $\mathcal{L}_n$ over $\mathbb{F}_q$, which makes it a mathematically rich and practically useful structure. This set is the first construction of MRD codes in history and has been discovered in [8, 16, 35] independently. It is called *Gabidulin codes* or *Delsarte-Gabidulin codes* in the literature.

Gabidulin codes were generalized in [16] considering all automorphisms of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ as

$$\mathcal{G}_{n,k,s} := \{\alpha_0 x + \alpha_1 x^{q^s} + \cdots + \alpha_{k-1} x^{q^{s(k-1)}} : \alpha_i \in \mathbb{F}_{q^n} \text{ for all } 0 \leq i \leq k-1\},$$

where s is an integer satisfying $\gcd(s,n) = 1$. We reemphasize that all polynomials are considered modulo $x^{q^n} - x$ for along this chapter even if we do not express it explicitly. The main idea used here is the fact that $\mathbb{F}_{q^n} \cap \mathbb{F}_{q^s} = \mathbb{F}_q$. The resulting family is linear again and called *generalized Gabidulin codes*. Note that, for $n \leq 4$, all generalized Gabidulin codes are equivalent to Gabidulin ones. We can give $G_{5,2,1}$ and $G_{5,2,2}$ as an example of the smallest inequivalent couples of such codes. We can show the inequivalence between them as follows: Assume that there are two invertible linearized polynomials $g_1, g_2 \in \mathcal{L}_5$ satisfying, for all $\alpha_0, \alpha_1 \in \mathbb{F}_{q^5}$ there exist $\beta_0, \beta_2 \in \mathbb{F}_{q^n}$ such that

$$\beta_0 x + \beta_1 x^{q^2} \equiv g_1(x) \circ (\alpha_0 x + \alpha_1 x^q) \circ g_2(x) \mod (x^{q^5} - x). \tag{2.4}$$

If we expand the computations on the right hand side in equation (2.4), and equate the coefficients of x^q, x^{q^3}, x^{q^4} to zero, then we see that either $g_1 = 0$ or $g_2 = 0$, i.e. not both are invertible, contradiction. Note that $G_{5,2,1}$ and $G_{5,2,2}$ are both linear, so disproving this assumption is enough to prove the inequivalence between them.

A significant generalization of Gabidulin codes was discovered in [38]. The author relates MRD codes with finite semifields (a generalization of finite fields) and utilizes

Lemma 2.1.1 explicitly. The resulting family is

$$\mathcal{H}_{n,k,s}(\eta,h) := \{\alpha_0 x + \alpha_1 x^{q^s} + \cdots + \alpha_{k-1}x^{q^{s(k-1)}} + \eta\alpha_0^{q^h} x^{q^{sk}} : \alpha_0,\ldots,\alpha_{k-1} \in \mathbb{F}_{q^n}\},$$

where $\gcd(n,s) = 1$, $1 \leq k \leq n-1$ and $\eta \in \mathbb{F}_{q^n}$ satisfies $N_{q^n/q}(\eta) \neq (-1)^{nk}$. This family is called *generalized twisted Gabidulin codes*. Particularly, $\mathcal{H}_{n,k,1}(\eta,h)$ is called *twisted Gabidulin codes*. The multiplicative structure of the norm function together with Lemma 2.1.1 can be directly used to prove that $\mathcal{H}_{n,k,s}(\eta,h)$ is indeed an MRD code. The full classification of this family with respect to the parameters was investigated in [29] for $n = 4$ and $k = 2$, in [38] for $s = 1$ and $(n,k) \neq (4,2)$, and in [23] for arbitrary s values. Explicitly, [23, Theorem 4.4] says the following about the equivalence of such codes: Let $n,k,s,t,g,h \in \mathbb{Z}^+$ satisfying $\gcd(n,s) = \gcd(n,t) = 1$ and $2 \leq k \leq n-2$. Let η and θ be in $\mathbb{F}_{q^n}$ satisfying $\mathrm{Norm}_{q^{ns}/q^s}(\eta) \neq (-1)^{nk}$ and $\mathrm{Norm}_{q^{nt}/q^t}(\theta) \neq (-1)^{nk}$. The codes $\mathcal{H}_{n,k,s}(\eta,g)$ and $\mathcal{H}_{n,k,t}(\theta,h)$ are equivalent if and only if one of the following sets of conditions are satisfied:

1. $s \equiv t$ and $g \equiv h$ modulo n, and there exist $c,d \in (\mathbb{F}_{q^n} \setminus \{0\})$, an automorphism ρ of $\mathbb{F}_q$, and an integer r such that
$$\theta c^{q^h-1} d^{q^{r+h}-q^{r+sk}} = \eta^{\rho q^r}.$$
2. $s \equiv -t$ and $g \equiv -h$ modulo n, and there exist $c,d \in (\mathbb{F}_{q^n} \setminus \{0\})$, an automorphism ρ of $\mathbb{F}_q$, and an integer r such that
$$c^{q^g-1} d^{q^{r+g}-q^{r+sk}} = \eta^{\rho q^r}\theta^{q^{sk}}.$$

In particular, the smallest examples of new codes in this family are semifields given for $q = 3$, $n = 3$ and $k = 1$, and for $q = 4$, $n = 2$ and $k = 1$. On the other hand, this construction does not work for the $q = 2$ and $\eta \neq 0$ case.

The set $\mathcal{H}_{n,k,s}(\eta,h)$ was extended further in [30] for case q is composite. This extension includes also nonlinear but additive codes. The following theorem introduces the corresponding larger family.

Theorem 1. *Let $n,k,s,u,h \in \mathbb{Z}^+$ satisfying $\gcd(n,s) = 1$, $q = q_0^u$ and $k < n$. Let $\eta \in \mathbb{F}_{q^n}$ be satisfying $N_{q^n/q_0}(\eta) \neq (-1)^{nku}$. Then the set*

$$\mathcal{H}_{n,k,s,q_0}(\eta,h) := \{\alpha_0 x + \alpha_1 x^{q^s} + \cdots + \alpha_{k-1}x^{q^{s(k-1)}} + \eta\alpha_0^{q_0^h} x^{q^{sk}} : \alpha_0,\ldots,\alpha_{k-1} \in \mathbb{F}_{q^n}\}$$

is an MRD code of minimum distance $n-k+1$.

Lemma 2.1.1 can be efficiently applied to prove also Theorem 1. The codes in this family is called *additive generalized twisted Gabidulin codes*.

We now elaborate one point as a preparation to show that $\mathcal{H}_{n,k,s,q_0}(\eta,h)$ includes newer codes. Consider $f(x)^{p^i} := x^{p^i} \circ f(x) \mod x^{q^n}-x$, where p is the prime dividing q. If we expand $f(x)^{p^i}$ to the corresponding matrix as in (2.2), then we obtain the matrix $B^{-1}F^{p^i}A$, where A and B are invertible matrices satisfying $[\delta_1^{p^i} \ \ldots \ \delta_n^{p^i}]A = [\delta_1 \ \ldots \ \delta_n]$ and $[\epsilon_1^{p^i} \ \ldots \ \epsilon_n^{p^i}]B = [\epsilon_1 \ \ldots \ \epsilon_n]$. That is, $f(x)^{p^i}$ does not correspond to F^{p^i} directly. In fact, $f(x)^{p^i}$ is not a q-polynomial when $i \not\equiv 0 \mod \log_p(q)$, so it corresponds to another q-polynomial which has the matrix form $B^{-1}F^{p^i}A$ when we fix the ordered bases $\{\epsilon_1,\ldots,\epsilon_n\}$ and $\{\delta_1,\ldots,\delta_n\}$. Nevertheless, it makes sense to write the equivalence between two additive codes $\mathcal{C}$ and $\mathcal{C}'$ in polynomial form as follows: $\mathcal{C} \equiv \mathcal{C}'$ if and only if

$$\mathcal{C}' \ = \ g_1 \circ \mathcal{C}^{p^i} \circ g_2, \quad \text{or} \quad \mathcal{C}' \ = \ g_1 \circ \widehat{\mathcal{C}}^{p^i} \circ g_2$$

for some invertible q-polynomials $g_1, g_2 \in \mathbb{F}_{q^n}[x]$ and a non-negative integer i, even if some elements are not q-polynomials. These p^i-polynomials give an idea about the largest field over which the code is linear. Consequently, we deduce the following result about additive rank metric codes in general: Let $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{L}_n$ be two additive rank metric codes and let $\mathbb{F}_{q_1}, \mathbb{F}_{q_2}$ be the largest subfields of $\mathbb{F}_q$ such that $\mathcal{C}_1$ is $\mathbb{F}_{q_1}$-linear and $\mathcal{C}_2$ is $\mathbb{F}_{q_2}$-linear, then $q_1 = q_2$ if $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent. In that way, when we compare two additive twisted Gabidulin codes, we observe the following: Let $q = q_1^{u_1} = q_2^{u_2}$. Then $\mathcal{H}_{n,k,s,q_1}(\eta,h)$ and $\mathcal{H}_{n,k,s,q_2}(\eta,h)$ are not equivalent when $\gcd(h\log_p q_1, n\log_p q) \neq \gcd(h\log_p q_2, n\log_p q)$.

Remark 2.2.1. *A further generalization of codes in Theorem 1 has been available in a recent preprint [37]. The author mainly utilizes further algebraic properties of skew polynomial rings and particular semifields (Petit's cyclic semifields) in order to construct new MRD codes.*

Remark 2.2.2. *We introduced* $\mathcal{H}_{n,k,s,q_0}(\eta,h)$ *as generalization of Gabidulin codes in this section, but there is another direction of generalization of such codes. We introduce it in Section 2.4 separately.*

2.3 Hughes-Kleinfeld Codes

The family introduced in Section 2.2 has been inspired by a particular family of semifields, twisted semifields. In this section, we introduce another family of MRD codes for even n, constructed from Hughes-Kleinfeld semifields. We can give the main result directly as follows.

Theorem 2. *[45] Let n be an even integer and s be an arbitrary integer satisfying $\gcd(n,s)=1$. Let also $\gamma \in \mathbb{F}_{q^n}$ satisfying $\mathrm{Norm}_{q^n/q}(\gamma)$ is a non-square in $\mathbb{F}_q$. Define*

$$\mathcal{D}_{n,k,s}(\gamma) := \left\{ \alpha_0 x + \left(\sum_{i=1}^{k-1} \beta_i x^{q^{si}} \right) + \gamma \alpha_k x^{q^{sk}} : \beta_1, \ldots, \beta_{k-1} \in \mathbb{F}_{q^n}, \alpha_0, \alpha_k \in \mathbb{F}_{q^{n/2}} \right\}.$$

Then $\mathcal{D}_{n,k,s}(\gamma)$ is an MRD code of size q^{nk} and minimum distance $n-k+1$.

It is easy to prove Theorem 2 using Lemma 2.1.1. In particular, $\mathcal{D}_{n,1,s}(\gamma)$ corresponds to Hughes-Kleinfeld semifields, i.e. it contains new codes for $k=1$. Moreover, it includes new codes for also other $k>1$ values. We use the following definition in order to prove $\mathcal{D}_{n,k,s}(\gamma)$ is new for all parameters. Let

$$N_r(\mathcal{C}) := \{\phi \in \mathcal{L}_n : \phi \circ f \in \mathcal{C} \text{ for all } f \in \mathcal{C}\}$$

for a given $\mathcal{C} \subseteq \mathcal{L}_n$. We call $N_r(\mathcal{C})$ the *right nucleus* of $\mathcal{C}$. If subsets $\mathcal{C}$ and $\mathcal{C}'$ of $\mathcal{L}_n$ are both linear and equivalent to each other, i.e. there exist invertible $g_1, g_2 \in \mathcal{L}_n$ such that $\mathcal{C} = g_1 \circ \mathcal{C}' \circ g_2$, then for any given element $\phi \in N_r(\mathcal{C})$ we observe the following:

$$\mathcal{C} = \phi \circ \mathcal{C} \Leftrightarrow g_1 \circ \mathcal{C}' \circ g_2 = \phi \circ (g_1 \circ \mathcal{C}' \circ g_2) \Leftrightarrow \mathcal{C}' = (g_1^{-1} \circ \phi \circ g_1) \circ \mathcal{C}',$$

and so $g_1^{-1} \circ \phi \circ g_1 \in N_r(\mathcal{C}')$. That means, there is a one to one correspondence between elements of $N_r(\mathcal{C})$ and $N_r(\mathcal{C}')$, and hence their sizes are the same. However, direct computations show that $N_r(\mathcal{D}_{n,k,s}(\gamma)) = \mathbb{F}_{q^{n/2}}$ whereas $N_r(\mathcal{H}_{n,k,s}(\eta,h)) = \mathbb{F}_{q^n}$. In conclusion, we get that Hughes-Kleinfeld type MRD codes are never equivalent to generalized twisted Gabidulin codes.

2.4 Partition Codes

Both families of MRD codes given in Sections 2.2 and 2.3 are generalizations of two semifields and produce additive codes. In this section, we present another family

of MRD codes which is not a generalization of semifields. Furthermore, it includes non-additive MRD codes for most of the parameters. The construction is given as follows.

Theorem 3. *[33] Let I be a subset of $\mathbb{F}_q$, and n, k and s be positive integers such that $k < n$ and $\gcd(n, s) = 1$. Also let*

$$\mathcal{C}^{(1)}_{n,k,s,I} := \left\{ \sum_{i=0}^{k-1} \alpha_i x^{q^{si}} \mod x^{q^n} - x : \alpha_0, \ldots, \alpha_{k-1} \in \mathbb{F}_{q^n}, \mathrm{Norm}_{q^n/q}(\alpha_0) \in I \right\},$$

$$\mathcal{C}^{(2)}_{n,k,s,I} := \left\{ \sum_{i=1}^{k} \beta_i x^{q^{si}} \mod x^{q^n} - x : \beta_1, \ldots, \beta_k \in \mathbb{F}_{q^n}, \mathrm{Norm}_{q^n/q}(\beta_k) \notin (-1)^{n(k+1)} I \right\}.$$

Then $\mathcal{C}_{n,k,s,I} := \mathcal{C}^{(1)}_{n,k,s,I} \cup \mathcal{C}^{(2)}_{n,k,s,I}$ is an MRD code with $d(\mathcal{C}_{n,k,s,I}) = n - k + 1$.

We can use Lemma 2.1.1 again in order to show that minimum distance of $\mathcal{C}_{n,k,s,I}$ is larger than or equal to $n - k + 1$. Besides, we can find the size of $\mathcal{C}_{n,k,s,I}$ using the facts that the norm function is an onto function, and $\mathcal{C}^{(1)}_{n,k,s,I}$ and $\mathcal{C}^{(2)}_{n,k,s,I}$ are disjoint.

For $q = 2$ we see that $\mathcal{C}_{n,k,s,I}$ is a generalized Gabidulin code. On the other hand, $\mathcal{C}_{n,k,s,I}$ is not closed under addition when $q > 2$ and I is not one of $\emptyset, \{0\}, \mathbb{F}_q \setminus \{0\}$ and $\mathbb{F}_q$. Also we see that zero is in $\mathcal{C}_{n,k,s,I}$, i.e. $\mathcal{C}_{n,k,s,I}$ is not affine. These facts impose that $\mathcal{C}_{n,k,s,I}$ is not equivalent to any additive codes when $q > 2$ and I is not one of $\emptyset, \{0\}, \mathbb{F}_q \setminus \{0\}$ and $\mathbb{F}_q$. We remark that $\mathcal{C}_{n,k,s,I}$ includes all known non-additive MRD codes for most of the parameters n and d in the literature.

2.5 Other Constructions

Previous three subsections give three known families of MRD codes, whose constructions work for nearly all parameters n and d. In this section, we mention the other constructions in the literature briefly.

1. The first non-additive MRD codes in history was given in [4] for $n = 3$ and $d = 2$ utilizing some features from finite geometry. Later, this method was generalized in [11] for arbitrary n and $d = n - 1$. We can give the construction

using the language of linearized polynomials as follows: For $\lambda \in \mathbb{F}_{q^n} \setminus \{0\}$, let

$$\begin{aligned}
\pi_\lambda &:= \{(\alpha x) \circ (x + \lambda x^q + \lambda^{1+q} x^{q^2} + \cdots + \lambda^{1+q+\cdots+q^{n-2}} x^{q^{n-1}}) \circ (\beta x) : \\
&\quad \alpha, \beta \in \mathbb{F}_{q^n} \setminus \{0\}\}, \\
J_\lambda &:= \{(\alpha x) \circ (x - \lambda x^{q^{n-1}}) \circ (\beta x) : \alpha, \beta \in \mathbb{F}_{q^n} \setminus \{0\}\}, \\
A_1 &:= \{\alpha x : \alpha \in \mathbb{F}_{q^n} \setminus \{0\}\}, \\
A_2 &:= \{\alpha x^{q^{n-1}} : \alpha \in \mathbb{F}_{q^n} \setminus \{0\}\}.
\end{aligned}$$

We remark that $\pi_{\lambda_1} = \pi_{\lambda_2}$ and $J_{\lambda_1} = J_{\lambda_2}$ when $\mathrm{Norm}(\lambda_1) = \mathrm{Norm}(\lambda_2)$. Hence, for $\mathrm{Norm}(\lambda) = a$, we can use π_a and J_a instead of using the notations π_λ and J_λ, respectively. Thus we get the following result.

Theorem 4. *Let $q > 2$ and $n \geq 3$. For any subset I of $\mathbb{F}_q \setminus \{0, 1\}$, put $\Pi_I = \bigcup_{a \in I} \pi_a$, $\Gamma_I = \bigcup_{b \in \mathbb{F}_q \setminus (I \cup \{0\})} J_b$ and set*

$$\mathcal{A}_{n,I} := \Pi_I \cup \Gamma_I \cup A_1 \cup A_2 \cup \{0\} \subseteq \mathcal{L}_n.$$

Then $\mathcal{A}_{n,I}$ is a non-additive MRD code of minimum distance $n - 1$.

We cannot use Lemma 2.1.1 in order to verify Theorem 4. In fact, further preliminary information mostly from projective geometry is required before the proof, and hence we omit the proof here.

2. A generalization of Theorem 4 is available in [9] for MRD codes of $m \times n$ type with $d = m - 2$ satisfying $m \leq n$.

3. Linear sets are used to construct MRD codes for $n = 6$ and $d = 5$, and for $n = 8$ and $d = 7$ in [6].

4. A generalization of punctured generalized Gabidulin codes was given in [34]. The idea is to produce codes including $m \times n$ matrices, where m is larger than or equal to a nontrivial multiple of n. In general, the authors use linearized polynomials of the form

$$\sum_{i=0}^{k-1} \alpha_i x^{q^i} + \sum_{j=1}^{l} \eta_j \left(\sum_{i=1}^{k-1} \lambda_{i,j} \alpha_i \right) x^{q^{k-1+t_j}},$$

for fixed η_j and $\lambda_{i,j}$ for $i = 0, 1, \ldots, k-1$ and $j = 1, \ldots, l$ taking $\eta_j \in \mathbb{F}_{q^{s_j}} \setminus \mathbb{F}_{q^{s_{j-1}}}$, where $n \leq s_0$ and $\mathbb{F}_q \subseteq \mathbb{F}_{q^{s_0}} \subsetneq \mathbb{F}_{q^{s_1}} \subsetneq \cdots \subsetneq \mathbb{F}_{q^{s_l}} \subseteq \mathbb{F}_{q^m}$.

5. Another investigation of codes including rectangular matrices is available in [25]. In particular, the authors give MRD codes of $m \times 4$ type with $d = 3$ for $m > 4$, and of $m \times 5$ type with $d = 4$ for $m > 7$. They also showed that the codes of these families are not punctured generalized Gabidulin codes.

6. Another study on codes of rectangular type matrices is available in [7]. The authors introduce a construction of MRD codes containing $(rn/2) \times n$ type matrices with $d = n - 1$ for even n.

2.6 Final Remarks

We list some concluding remarks regarding the construction problem of such codes.

- We emphasize that three main constructions in Sections 2.2, 2.3 and 2.4 are constructed under the light of Lemma 2.1.1. Note that a similar notion is available also in [34] for rectangular matrices. Such tools can be seen as an initial point for constructions of MRD codes.

- We also remark that two main constructions in Sections 2.2 are 2.3 are inspired by semifields. Therefore, it makes sense to study on other semifields for further constructions.

- The structure of the codes plays an important role for checking equivalence. For example, testing equivalence between two non-additive MRD codes seems a considerably hard problem.

- MRD codes have various applications in many areas such as coding theory and cryptography. In particular, linear MRD codes are used as encryption keys in some code-based encryption schemes. Observe also that we can construct at least 2^q different partition codes using only the parameter I in Theorem 3. Here, 2^q is an exponential statement in terms of q and independent of n. That is, the set of such codes can be chosen sufficiently large with respect to q, for even small m and n values. However, there are no applications of non-additive MRD codes such as partition codes in cryptography yet.

- MRD codes have connections with some geometrical structures such as linear sets, see [22] for example. That means, the constructions of new MRD codes may help us to understand and enrich other areas in mathematics.

CHAPTER 3

CONSTRUCTIONS OF CYCLIC CONSTANT DIMENSION CODES

In this chapter, we introduce a construction of cyclic constant dimension codes using a particular class of linearized polynomials. This construction is the first and unique systematic construction of such codes up to our knowledge. We also briefly mention the history of generalizations of the method. We remark that our work [31] inherits the main framework of the construction.

3.1 Preliminaries

We have sufficient knowledge about linearized polynomials from Section 2.1. We now present a particular class of such codes. A monic q-polynomial over $\mathbb{F}_{q^N}$ is called a *subspace polynomial* if

- it splits completely over $\mathbb{F}_{q^N}$ (i.e. all roots are in $\mathbb{F}_{q^N}$), and
- has no multiple roots (i.e. the coefficient of x is nonzero).

From the definition we observe a one to one correspondence between a k-dimensional subspace U of $\mathbb{F}_{q^N}$ and a subspace polynomial f of q-degree k satisfying $f(U) = \{0\}$.

Let $U \in \mathcal{G}_q(N, k)$, we assume $1 < k < N$ unless otherwise stated since we omit the trivial cases. Clearly, U is a linear space over $\mathbb{F}_q$, but U can be also a linear space over a larger field. This property affects some important parameters, the $Orb(U) :=$

$\{\alpha U : \alpha \in \mathbb{F}_{q^N}^*\}$ set is called the *orbit* of U, the size of an orbit can be determined as follows.

Proposition 3.1.1. *Let $U \in \mathcal{G}_q(N,k)$. Then, t is the largest number such that U is $\mathbb{F}_{q^t}$-linear if and only if*

$$|Orb(U)| = \frac{q^N - 1}{q^t - 1}.$$

Similar versions of this well-known theorem are available also in [1, 10, 17]. We may prove this theorem in an elementary way as follows.

Proof. $(\Rightarrow)$: Let $\mathbb{F}_{q^t}$ be the largest field over which U is linear. Then we have $|Orb(U)| \leq \frac{q^N-1}{q^t-1}$ since $aU = U$ for all $a \in \mathbb{F}_{q^t}$. Assume that the equality does not hold. Then there exists an $\alpha \in \mathbb{F}_{q^N} \setminus \mathbb{F}_{q^t}$ such that $\alpha U = U$, by pigeon hole principle. It implies U is also $\mathbb{F}_{q^t}(\alpha)-$linear, but $\mathbb{F}_{q^t} \subsetneq \mathbb{F}_{q^t}(\alpha)$ since $\alpha \notin \mathbb{F}_{q^t}$. Hence $\mathbb{F}_{q^t}$ is not the largest field over which U is linear, contradiction. Therefore, the equality must hold, i.e. $|Orb(U)| = \frac{q^N-1}{q^t-1}$.

$(\Leftarrow)$: It can be shown by the $(\Rightarrow)$ part. □

If $t = 1$ in Proposition 3.1.1, then the orbit is called *full length orbit*. Otherwise, the orbit is called *degenerate orbit*.

If we need to work on degenerate orbits in general, we can equivalently work on full length orbits over $\mathbb{F}_{q^t}$ and then carry all the information from $\mathcal{G}_{q^t}(N/t, k/t)$ to $\mathcal{G}_q(N,k)$.

3.2 A Systematic Construction

The following theorem gives a systematic construction of cyclic subspace codes including many full length orbits in $\mathcal{G}_q(N,k)$, when the minimum distance is $2k-2$.

Theorem 5. *Let k and s be positive integers satisfying $1 \leq s < k$ and $\gcd(s,k) = 1$. Consider r polynomials*

$$T_i(x) := x^{q^k} + \theta_i x^{q^s} + \gamma_i x \in \mathbb{F}_{q^n}[x], \quad 1 \leq i \leq r$$

satisfying $\theta_i \neq 0$ *and* $\gamma_i \neq 0$ *for all* $1 \leq i \leq r$*, and*

$$\left(\frac{\gamma_i}{\gamma_j}\right)^{\frac{q^s-1}{q-1}} \neq \left(\frac{\gamma_i}{\gamma_j}\left(\frac{\theta_i}{\theta_j}\right)^{-1}\right)^{\frac{q^k-1}{q-1}} \quad \textit{when } i \neq j. \tag{3.1}$$

Also let

- N_i *be the degree of the splitting field of* T_i *for* $1 \leq i \leq r$*,*
- $U_i \subseteq \mathbb{F}_{q^{N_i}}$ *be the kernel of* T_i *for* $1 \leq i \leq r$*,*
- N *be a multiple of* $\mathrm{lcm}(N_1, ..., N_r)$*.*

Then the code $\mathcal{C} \subseteq \mathcal{G}_q(N, k)$ *given by*

$$\mathcal{C} = \bigcup_{i=1}^{r} \{\alpha U_i : \alpha \in \mathbb{F}_{q^N}^*\}$$

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

Proof. Let $\mathcal{C}_i := \{\alpha U_i : \alpha \in \mathbb{F}_{q^N}^*\}$, for $1 \leq i \leq r$. Then $\mathcal{C} := \bigcup_{i=1}^{r} \mathcal{C}_i$ is a cyclic subset of $\mathcal{G}_q(N, k)$. It is enough to prove

$$\dim(\alpha U_i \cap \beta U_j) \leq 1 \text{ when } i \neq j \text{ or } \frac{\alpha}{\beta} \notin \mathbb{F}_q, \tag{3.2}$$

in order to show that $|\mathcal{C}| = r\frac{q^N-1}{q-1}$ and $d(\mathcal{C}) = 2k-2$. Let $\theta \in \alpha U_i \cap \beta U_j$ for some $1 \leq i, j \leq r$. Then there exist $u \in U_i$ and $v \in U_j$ such that $\theta = \alpha u = \beta v$. Write $\frac{\alpha}{\beta}u$ instead of v, solving the system $T_i(u) = 0$ and $T_j(\frac{\alpha}{\beta}u) = 0$ in terms of u, we obtain

$$\left((\frac{\alpha^{q^k}}{\beta^{q^k}})\theta_i - (\frac{\alpha^{q^s}}{\beta^{q^s}})\theta_j\right) u^{q^s} + \left((\frac{\alpha^{q^k}}{\beta^{q^k}})\gamma_i - (\frac{\alpha}{\beta})\gamma_j\right) u = 0. \tag{3.3}$$

The left hand side of equation (3.3) is clearly a $q-$polynomial in terms of u. Here, computations show that the left hand side is not identically zero because of (3.1). On the other hand, if one of

$$\left((\frac{\alpha^{q^k}}{\beta^{q^k}})\theta_i - (\frac{\alpha^{q^s}}{\beta^{q^s}})\theta_j\right) \qquad \text{and} \qquad \left((\frac{\alpha^{q^k}}{\beta^{q^k}})\gamma_i - (\frac{\alpha}{\beta})\gamma_j\right)$$

is zero, then the result directly holds. Otherwise, i.e. when both are nonzero, we see that any two roots u_1 and u_2 must satisfy

$$\left(\frac{u_1}{u_2}\right)^{q^s-1} = 1,$$

which implies $u_1/u_2 \in \mathbb{F}_q$ since $\gcd(s,k) = 1$. That means, elements u in (3.3) constitute a vector space of dimension at most one. In other words, the proof is completed. □

Remark 3.2.1. *The initial version of Theorem 5 was given in [1] for $\theta_i = \gamma_i^q$ and $s = 1$. Later, it was generalized in [31] to the $s = 1$ case. The current version has been proposed by [3].*

Remark 3.2.2. *Note that Theorem 5 includes only full length orbits. We can insert degenerate orbits into the code keeping the minimum subspace distance. In particular, for k dividing N, it is shown in [3] that we insert also a degenerate orbit coming from the polynomial of type*

$$x^{q^k} - ax \in \mathbb{F}_{q^n}[x].$$

In that way, the size of the code can be slightly increased.

Remark 3.2.3. *Let $T(x) \in \mathbb{F}_{q^N}[x]$ be a subspace polynomial and U be the set of all roots of $T(x)$. There is another subspace $\overline{U} \subseteq \mathbb{F}_{q^N}$ associated with $T(x)$.*

$$u \in \overline{U} \Leftrightarrow T(x) = \left(x^q - \frac{1}{u^{q-1}}x\right) \circ Q(x)$$

for some q-polynomial $Q(x)$ over $\mathbb{F}_{q^N}$. This space can be also characterized by

$$u \in \overline{U} \Leftrightarrow u^q \text{ is a root of } \overline{T}(x) := (\alpha_0 x)^{q^k} + \cdots + (\alpha_{k-1}x)^q + x,$$

where

$$T(x) = x^{q^k} + \alpha_{k-1}x^{q^{k-1}} + \cdots + \alpha_0 x.$$

Here, $\overline{U}$ is called the adjoint space of U [28, Theorems 14, 15 and 16]. Therefore, corresponding to a code $\mathcal{C}$ obtained in Theorem 5, we can construct another code $\overline{\mathcal{C}}$ using the polynomials $\overline{T_i}(x) = \gamma_i^{q^k} x^{q^k} + \theta_i^{q^{k-s}} x^{q^{k-s}} + x$ instead of $T_i(x)$ in Theorem 5. Both $\mathcal{C}$ and $\overline{\mathcal{C}}$ are of the same size, and we call $\overline{\mathcal{C}}$ the adjoint code of $\mathcal{C}$.

CHAPTER 4

CONSTRUCTIONS OF SUBSPACE PACKINGS

In this chapter, we give a recursive solution to Problem 3. The solution is also available in our work [12] where also further information about lower and upper bounds for $A_q(N,k,s;\lambda)$ and computational results are presented.

4.1 Preliminaries

Let $1 \leq \delta \leq k \leq N$ and $\alpha \geq 2$ be integers. Also, let $\mathcal{C}$ be a set of k-dimensional subspaces of $\mathbb{F}_q^N$ such that any α elements of $\mathcal{C}$ span a subspace of dimension at least $k+\delta$ in $\mathbb{F}_q^N$. We denote the largest possible size of $\mathcal{C}$ by

$$B_q(N,k,\delta;\alpha).$$

We have the following equalities.

$$\begin{aligned} A_q(N,k,s;\lambda) &= B_q(N,N-k,k-s+1;\lambda+1),\\ B_q(N,k,\delta;\alpha) &= A_q(N,N-k,N-k-\delta+1;\alpha-1). \end{aligned}$$

These equalities come from a one to one correspondence between a codeword and its dual with respect to the classical inner product given by $(x_1,\ldots,x_N)\cdot(y_1,\ldots,y_N) = \sum_{i=1}^{N} x_i y_i$ for any $(x_1,\ldots,x_N),(y_1,\ldots,y_N) \in \mathbb{F}_q^N$. We can state this correspondence briefly in the following well-known result.

Proposition 4.1.1. *Let $U_1,\ldots,U_\lambda \in \mathcal{G}_q(N,k)$. Then,*

$$(U_1+\cdots+U_\lambda)^\perp = U_1^\perp \cap \cdots \cap U_\lambda^\perp.$$

Proof. The proof can be derived directly for $\lambda = 2$ as follows.

$$\begin{aligned} v \in (U_1 + U_2)^\perp &\Leftrightarrow v \cdot y = 0 \text{ for all } y \in U_1 + U_2 \\ &\Leftrightarrow v \cdot (a_1 u_1 + a_2 u_2) = 0 \text{ for all } a_1, a_2 \in \mathbb{F}_q, u_1 \in U_1, u_2 \in U_2, \\ &\Leftrightarrow a_1(v \cdot u_1) + a_2(v \cdot u_2) = 0 \text{ for all } a_1, a_2 \in \mathbb{F}_q, u_1 \in U_1, u_2 \in U_2, \\ &\Leftrightarrow v \cdot u_1 = 0 \text{ and } v \cdot u_1 = 0 \text{ for all } u_1 \in U_1, u_2 \in U_2, \\ &\Leftrightarrow v \in U_1^\perp \cap U_2^\perp. \end{aligned}$$

We can complete the proof for general λ applying induction. □

Now we give a technical lemma as a property of MRD codes.

Lemma 4.1.1. *Let d, k and N be integers satisfying $2 \leq d \leq k < N$. There are q^N MRD codes $\mathcal{C}_i \subseteq \mathbb{F}_q^{k \times N}$ for $1 \leq i \leq q^N$ satisfying the following.*

- *Minimum rank distance of $\mathcal{C}_i$ is d for all $1 \leq i \leq q^N$,*
- *$\mathcal{C}_i \cap \mathcal{C}_j = \emptyset$ for all $1 \leq i < j \leq q^N$,*
- *Minimum rank distance of $\bigcup_{i=1}^{q^N} \mathcal{C}_i$ is $d - 1$.*

Proof. Recall Gabidulin codes

$$\mathcal{G} = \{\theta_0 x + \theta_1 x^q + \cdots + \theta_{k-d} x^{q^{k-d}} \in \mathbb{F}_{q^N}[x] : \theta_0, \ldots, \theta_{k-d} \in \mathbb{F}_{q^N}\}$$

from Section 2.2. Clearly $\mathcal{G}$ is an MRD code of size $q^{N(k-d+1)}$ and minimum rank distance $N - k + d$. Also note that such codes exist for all d, k and N satisfying $2 \leq d \leq k < N$. Set

$$\mathcal{G}_\theta := \theta x^{q^{k-d+1}} + \mathcal{G}$$

for each $\theta \in \mathbb{F}_{q^N}$. Observe that minimum rank distance of $\mathcal{G}_\theta$ is $N - k + d$, and $\mathcal{G}_\theta \cap \mathcal{G}_\gamma = \emptyset$ for all distinct $\theta, \gamma \in \mathbb{F}_{q^N}$. We delete the last $N - k$ rows of the $N \times N$ type matrix version of $\mathcal{G}_\theta$ (remember the correspondence (2.2)) and create $\mathcal{C}_\theta$ (puncturing) for all $\theta \in \mathbb{F}_{q^N}$. Here, $\mathcal{C}_\theta$ and $\mathcal{C} := \cup_{\theta \in \mathbb{F}_{q^N}} \mathcal{C}_\theta$ are still MRD codes, and have minimum rank distances d and $d - 1$ respectively. □

4.2 A Recursive Construction

In this section, we give a recursive construction for $B_q(N, k, \delta; \alpha)$ and then deduce the corresponding result for $A_q(N, k, s; \lambda)$. Firstly note that we can naturally assume $N \geq k + \delta$, and do so from now on. On the other hand, N can be smaller than $k + 2\delta$ or not. Considering both cases separately, we can give the following result.

Theorem 6. *[12] Let $1 \leq \delta \leq k$, $k + \delta \leq N$ and $2 \leq \alpha \leq q^N + 1$ be integers. Then we have the following.*

1. *If $N < k + 2\delta$, then*

$$B_q(N, k, \delta; \alpha) \geq (\alpha - 1)q^{\max\{k, N-k\}(\min\{k, N-k\}-\delta+1)}.$$

2. *If $N \geq k + 2\delta$, then for an arbitrary t satisfying $\delta \leq t \leq N - k - \delta$, we observe the following.*

   (a) *If $t < k$, then*

$$B_q(N, k, \delta; \alpha) \geq (\alpha-1)q^{k(t-\delta+1)}B_q(N-t, k, \delta; \alpha)+B_q(t+k-\delta, k, \delta; \alpha).$$

   (b) *If $t \geq k$, then*

$$B_q(N, k, \delta; \alpha) \geq (\alpha-1)q^{t(k-\delta+1)}B_q(N-t, k, \delta; \alpha)+B_q(t+k-\delta, k, \delta; \alpha).$$

Remark 4.2.1. *Note that the length of vectors is expected to be greater than or equal to $k+\delta$. However, in Case 2 of Theorem 6, there is a possibility that $t+k-\delta < k+\delta$ for $B_q(t + k - \delta, k, \delta; \alpha)$. In such situations, we consider the following convention.*

$$B_q(t + k - \delta, k, \delta; \alpha) = \min\left\{\alpha - 1, \begin{bmatrix} t + k - \delta \\ k \end{bmatrix}_q\right\}.$$

The reason behind this convention can be understood from the definition.

Corollary 4.2.1. *Let $1 \leq s \leq k \leq N$ and $1 \leq \lambda \leq q^N$ be integers. Then we have the following.*

1. *If $k > 2s - 2$, then*

$$A_q(N, k, s; \lambda) \geq \lambda q^{\max\{k, N-k\}(\min\{k, N-k\}-k+s)}.$$

2. *If $k \leq 2s-2$, then for an arbitrary t satisfying $k-s+1 \leq t \leq s-1$, we observe the following.*

   (a) *If $t < N-k$, then*

$$\begin{aligned} A_q(N,k,s;\lambda) &\geq \lambda q^{(N-k)(t-k+s)} A_q(N-t,k-t,s-t;\lambda) \\ &\quad + A_q(t+N-2k+s-1, t-k+s-1, t-2k-2s-1;\lambda). \end{aligned}$$

   (b) *If $t \geq N-k$, then*

$$\begin{aligned} A_q(N,k,s;\lambda) &\geq \lambda q^{t(N-2k+s)} A_q(N-t,k-t,s-t;\lambda) \\ &\quad + A_q(t+N-2k+s-1, t-k+s-1, t-2k-2s-1;\lambda). \end{aligned}$$

Remark 4.2.2. *Theorem 6 gives a lower bound for $B_q(N,k,\delta;\alpha)$ and so $A_q(N,k,s;\lambda)$. It is natural to investigate how much this bound is good. Computational results in [12], which includes also upper bounds for $A_q(N,k,s;\lambda)$ found by some other methods, show that this bound is quite good for many small parameters. For instance, we can see some good lower bounds obtained by Theorem 6 below.*

- $5377 \leq A_2(8,6,5;4) \leq 5654$,
- $1024 \leq A_2(8,4,2;4) \leq 1224$,
- $768 \leq A_2(8,4,2;3) \leq 901$,
- $512 \leq A_2(8,4,2;2) \leq 578$.

Note also that it is not easy to construct large subspace packings for larger parameters using basic computational trials, hence the recursive construction in Theorem 6 can be used efficiently for this purpose.

4.3 Proof of the Construction

In this section, we prove Theorem 6 case by case. We emphasize that the main idea utilized here is a generalization of the linkage construction (see [18] for example) by the help of Lemma 4.1.1.

4.3.1 Case 1: $N < k + 2\delta$

We now prove Theorem 6 for N values satisfying $k + \delta \leq N < k + 2\delta$. We utilize the following construction for this purpose.

Construction 4.3.1. *Let I_k denote the $k \times k$ identity matrix over $\mathbb{F}_q$ and let $G_1 \subseteq \mathbb{F}_q^{k\times(N-k)}$ be a linear MRD code of minimum rank distance δ. Let $G_2, \ldots, G_{\alpha-1}$ be other (affine) MRD codes of minimum rank distance δ obtained by translating G_1 in a way that*

$$d_R(G_1 \cup \cdots \cup G_{\alpha-1}) = \delta - 1.$$

At this point, we recall that $G_1, \ldots, G_{\alpha-1}$ exist for all $2 \leq \alpha \leq q^{\max\{k,N-k\}} + 1$ by Lemma 4.1.1. Also note that G_i and G_j are disjoint for all $1 \leq i < j \leq \alpha - 1$. Let $G := G_1 \cup \cdots \cup G_{\alpha-1}$. Adding each matrix in G to the end of I_k, we construct $(\alpha - 1)q^{\max\{k,N-k\}(\min\{k,N-k\}-\delta+1)}$ different matrices of size $k \times N$. The resulting matrices are still in row reduce echelon form (RREF). Let $\mathrm{RREF}(\mathcal{C})$ denote the set of such matrices, and let $\mathcal{C}$ be the set of rowspaces of matrices in $\mathrm{RREF}(\mathcal{C})$.

Proposition 4.3.1. *Let $\mathcal{C}$ be the set of k-spaces in Construction 4.3.1. Then we have*

$$\dim(U_1 + \cdots + U_\alpha) \geq k + \delta,$$

for all distinct $U_1, \ldots, U_\alpha \in \mathcal{C}$.

Proof. Given pairwise distinct $U_1, \ldots, U_\alpha \in \mathcal{C}$, let $u_1, \ldots, u_\alpha \in \mathrm{RREF}(\mathcal{C})$ be the corresponding $k \times n$ matrices in RREF. Let also $A_1, \ldots, A_\alpha \in G$ satisfying

$$U_i = \mathrm{rowspace}(u_i) = \mathrm{rowspace}(I_k|A_i)$$

for all $1 \leq i \leq \alpha$. Here, $\dim(U_1 + \cdots + U_\alpha)$ is clearly equal to

$$\mathrm{rank} \begin{array}{|c|c|} \hline I_k & A_1 \\ \hline I_k & A_2 \\ \hline \vdots & \vdots \\ \hline I_k & A_\alpha \\ \hline \end{array}_{\alpha k \times n} . \tag{4.1}$$

Note that $A_1, \ldots, A_\alpha$ must be pairwise distinct by definition. Also note that $A_1, \ldots, A_\alpha \in G = G_1 \cup \cdots \cup G_{\alpha-1}$, i.e. at least two of A_i's must be from the same G_j for some

$1 \leq j \leq \alpha - 1$ (by pigeonhole principle). Without loss of generality, assume A_1 and A_2 are from the same G_j for some $1 \leq j \leq \alpha - 1$. Then clearly (4.1) is equal to

$$\text{rank} \begin{array}{|c|c|} \hline I_k & A_1 \\ \hline 0 & A_2 - A_1 \\ \hline \vdots & \vdots \\ \hline 0 & A_\alpha - A_1 \\ \hline \end{array} \geq \text{rank} \begin{array}{|c|c|} \hline I_k & A_1 \\ \hline 0 & A_2 - A_1 \\ \hline \end{array} \geq k + \delta.$$

□

4.3.2 Case 2a: $N \geq k + 2\delta$ and $t < k$

We now prove Theorem 6 for N and t values satisfying $N \geq k + 2\delta$, $\delta \leq t < k$, and $t \leq N - k - \delta$. We use the construction below for this purpose.

Construction 4.3.2. *Let $\mathcal{C}_{N-t}$ be a subset of k-dimensional subspaces of $\mathbb{F}_q^{N-t}$ such that any α pairwise distinct elements $V_1, \ldots, V_\alpha \in \mathcal{C}_{N-t}$ satisfy $\dim(V_1 + \cdots + V_\alpha) \geq k + \delta$, and $|\mathcal{C}_{N-t}| = B_q(N - t, k, \delta; \alpha)$. Note that $N - t \geq k + \delta$ since $t \leq N - k - \delta$, i.e. it makes sense to take such $\mathcal{C}_{N-t}$.*

1. *For any $V \in \mathcal{C}_{N-t}$, we can find a unique matrix $v \in \mathbb{F}_q^{k \times (N-t)}$ in RREF such that V is the rowspace of v. Create the set $\mathrm{RREF}(\mathcal{C}_{N-t})$ writing each element of $\mathcal{C}_{N-t}$ in this form.*

2. *Let $G_1 \subseteq \mathbb{F}_q^{k \times t}$ be a linear MRD code of minimum rank distance δ. Let $G_2, \ldots, G_{\alpha-1}$ be other (affine) MRD codes of minimum rank distance δ obtained by translating G_1 in a way that*

$$d_R(G_1 \cup \cdots \cup G_{\alpha-1}) = \delta - 1$$

(recall Lemma 4.1.1). Let $G := G_1 \cup \cdots \cup G_{\alpha-1}$. Adding each matrix in G to the end of each $v \in \mathrm{RREF}(\mathcal{C}_{N-t})$, we construct $(\alpha-1)q^{k(t-\delta+1)}|\mathcal{C}_{N-t}|$ different matrices of size $k \times N$. The resulting matrices are still in RREF. We define $\mathcal{C}$ as the set of rowspaces of such matrices.

3. *Additionally, consider $\mathcal{C}_{\text{appendix}} \subseteq \mathcal{G}_q(N, k)$ such that*

   - *the first $N - (t + k - \delta)$ entries of $\mathcal{C}_{\text{appendix}}$ is zero,*

- $\dim(W_1 + \cdots + W_\alpha) \geq k + \delta$ *for all distinct* $W_1, \ldots, W_\alpha \in \mathcal{C}_{\text{appendix}}$,
- $\mathcal{C}_{\text{appendix}}$ *has the largest possible size (i.e.* $|\mathcal{C}_{\text{appendix}}| = B_q(t + k - \delta, k, \delta; \alpha)$*).*

In order to complete our construction, we take the union $\mathcal{C}'$ *of* $\mathcal{C}$ *in Step 2 and* $\mathcal{C}_{\text{appendix}}$ *of Step 3.*

Proposition 4.3.2. *Let* $\mathcal{C}'$ *be the set of* k*-spaces in Construction 4.3.2. Then we have*

$$\dim(U_1 + \cdots + U_\alpha) \geq k + \delta,$$

for all distinct $U_1, \ldots, U_\alpha \in \mathcal{C}'$.

Proof. Firstly note that $\mathcal{C}$ and $\mathcal{C}_{\text{appendix}}$ are disjoint. Given pairwise distinct $U_1, \ldots, U_\alpha \in \mathcal{C}'$, if all $U_1, \ldots, U_\alpha$ are in $\mathcal{C}_{\text{appendix}}$, then the result is clear by definition. Similarly, if one of $U_1, \ldots, U_\alpha$ is in $\mathcal{C}$ and an another one is in $\mathcal{C}_{\text{appendix}}$, then result is immediate again. Now assume $U_1, \ldots, U_\alpha \in \mathcal{C}$ and let $u_1, \ldots, u_\alpha \in \text{RREF}(\mathcal{C})$ be the corresponding $k \times N$ matrices. Let also $v_1, \ldots, v_\alpha \in \text{RREF}(\mathcal{C}_{N-t})$ and $A_1, \ldots, A_\alpha \in G$ satisfying

$$U_i = \text{rowspace}(u_i) = \text{rowspace}([v_i | A_i])$$

for all $1 \leq i \leq \alpha$. Here, $\dim(U_1 + \cdots + U_\alpha)$ is clearly equal to

$$\text{rank} \begin{array}{|c|c|} \hline v_1 & A_1 \\ \hline v_2 & A_2 \\ \hline \vdots & \vdots \\ \hline v_\alpha & A_\alpha \\ \hline \end{array}_{\alpha k \times N} . \tag{4.2}$$

Also, note that the order of $U_1, \ldots, U_\alpha$ in $U_1 + \cdots + U_\alpha$ is not important. Therefore, we can examine statement (4.2) in the following three cases without loss of generality.

1. Assume $v_1 = v_2 = \cdots = v_\alpha$. In this case, $A_1, \ldots, A_\alpha$ must be pairwise distinct by definition. Also note that $A_1, \ldots, A_\alpha \in G = G_1 \cup \cdots \cup G_{\alpha-1}$, i.e. at least two of A_i's must be from the same G_j for some $1 \leq j \leq \alpha - 1$ (by pigeonhole principle). Assume A_1 and A_2 are from the same G_j for some $1 \leq j \leq \alpha - 1$

without loss of generality. Then clearly (4.2) is equal to

$$\text{rank}\begin{array}{|c|c|}\hline v_1 & A_1 \\ \hline 0 & A_2 - A_1 \\ \hline \vdots & \vdots \\ \hline 0 & A_\alpha - A_1 \\ \hline \end{array} \geq \text{rank}\begin{array}{|c|c|}\hline v_1 & A_1 \\ \hline 0 & A_2 - A_1 \\ \hline \end{array} \geq k + \delta.$$

2. Assume $v_i \neq v_j$ for all $1 \leq i < j \leq \alpha$. In this case,

$$\begin{aligned} \text{rank}\begin{array}{|c|c|}\hline v_1 & A_1 \\ \hline v_2 & A_2 \\ \hline \vdots & \vdots \\ \hline v_\alpha & A_\alpha \\ \hline \end{array}_{\alpha k \times n} &\geq \text{rank}\begin{array}{|c|}\hline v_1 \\ \hline v_2 \\ \hline \vdots \\ \hline v_\alpha \\ \hline \end{array}_{\alpha k \times (N-t)} \\ &= \dim(\text{rowspace}(v_1) + \cdots + \text{rowspace}(v_\alpha)) \\ &\geq k + \delta, \end{aligned}$$

by the definition of $\mathcal{C}_{N-t}$.

3. Assume $v_1 \neq v_2 = v_3$ without loss of generality. This case also implies $A_2 \neq A_3$. Note that (4.2) equals

$$\begin{aligned} \text{rank}\begin{array}{|c|c|}\hline v_1 & A_1 \\ \hline v_2 & A_2 \\ \hline 0 & A_3 - A_2 \\ \hline \vdots & \vdots \\ \hline v_\alpha & A_\alpha \\ \hline \end{array} &\geq \text{rank}\begin{array}{|c|c|}\hline v_1 & A_1 \\ \hline v_2 & A_2 \\ \hline 0 & A_3 - A_2 \\ \hline \end{array} \\ &\geq \text{rank}\begin{array}{|c|}\hline v_1 \\ \hline v_2 \\ \hline \end{array} + \text{rank}(A_3 - A_2) \\ &\geq (k+1) + (\delta - 1) \\ &= k + \delta. \end{aligned}$$

□

Remark that $k + \delta \leq N - t$ because we take $t \leq N - k - \delta$. Therefore, Theorem 6 can be reapplied for $B_q(N - t, k, \delta; \alpha)$.

4.3.3 Case 2b: $N \geq k + 2\delta$ and $t \geq k$

This case can be proven similarly as in the proof of Case 2b.

CHAPTER 5

CONCLUSION

The main purpose of this thesis is to give the main results solving Problems 1, 2, and 3 using a simple language and remarking the historical journeys. We express that all three problems are relatively new and motivated mainly from applications. Also note that they have been intensely studied in recent years. Therefore, we hope that the thesis would help researchers to follow recent advances related to these problems in a compact and easy way. In this chapter, we briefly discuss the main results of the thesis emphasizing the profiles of the methods to build them.

The classification of MRD codes gets more complicated when the parameters increase. Fortunately, the rich and neat structure of linearized polynomials plays a fruitful role in solutions of Problem 1. We remark that most of the solutions to Problem 1 have appeared utilizing such polynomials. As a result, we can list the largest solutions as Theorems 1, 2, and 3 thank to Lemma 2.1.1. At this point, we also would like to express that our contribution [30] plays a significant role in creation of Theorem 1, and our another work [33] yields Theorem 3. In addition to these three families, there are some other methods from different areas of mathematics as we observe in Section 2.5.

Cyclic constant dimension codes have a relatively difficult structure since the codewords are larger objects and we also cannot mention binary operations on codes. Theorem 5 tries to overcome this issue relaxing the N parameter and utilizing subspace polynomials. Note that Theorem 5 is the only systematic solution of Problem 2 in the literature, and its eventual structure was presented in our work [31].

The subspace packing problem, Problem 3, investigates the most gigantic structures among the three problems. Fortunately, the neat framework of Gabidulin codes (i.e. Lemma 4.1.1) and the linkage construction can be combined to set up Theorem 6 as a sufficiently useful solution. The one to one correspondence between matrices in RREF and their rowspaces is another important tool to solve the problem. We are glad to note that this theorem is one of the basic results in our work [12].

REFERENCES

[1] E. Ben-Sasson, T. Etzion, A. Gabizon, and N. Raviv, Subspace polynomials and cyclic subspace codes, IEEE Trans. Inf. Theory, 62, pp. 1157–1165, 2016.

[2] M. Braun, M. Kiermaier, and W. Wassermann, q-analogs of designs: subspace designs, in *Network Coding and Subspace Designs, Signals and Communication Technology*, pp. 171–211, Springer, 2018.

[3] B. Chen and H. Liu, Construction of cyclic constant dimension codes, Des. Codes Cryptogr., 86, pp. 1267–1279, 2018.

[4] A. Cossidente, G. Marino, and F. Pavese, Non-linear maximum rank distance codes, Des. Codes Cryptogr., 79, pp. 597–609, 2016.

[5] J. Cruz, M. Kiermaier, A. Wassermann, and W. Willems, Algebraic structures of MRD codes, Adv. Math. Comm., 10, pp. 499–510, 2016.

[6] B. Csajbok, G. Marino, O. Polverino, and C. Zanella, A new family of MRD-codes, arXiv:1707.08487v1 [math.CO].

[7] B. Csajbok, G. Marino, O. Polverino, and F. Zullo, Maximum scattered linear sets and MRD-codes, arXiv:1701.06831v1 [math.CO].

[8] P. Delsarte, Bilinear forms over a finite field, with applications to coding theory, J. Comb. Theory A, 25, pp. 226–241, 1978.

[9] G. Donati and N. Durante, A generalization of the normal rational curve in $PG(d, q^n)$ and its associated non-linear MRD codes, Des. Codes Cryptogr., 86, pp. 1175–1184, 2018.

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

[11] N. Durante and A. Siciliano, Non-linear maximum rank distance codes in the cyclic model for the field reduction of finite geometries, Electr. J. Comb., 24, 2017.

[12] T. Etzion, S. Kurz, K. Otal, and F. Özbudak, Subspace packings, preprint.

[13] T. Etzion and A. Vardy, Error-correcting codes in projective space, IEEE Trans. Inf. Theory, 57, pp. 1165–1173, 2011.

[14] T. Etzion and A. Wachter-Zeh, Vector network coding based on subspace codes outperforms scalar linear network coding, IEEE Trans. Inf. Theory, 64, pp. 2460–2473, 2018.

[15] T. Etzion and H. Zhang, Grassmannian codes with new distance measures for network coding, in *Proc. IEEE Int. Symp. Inf. Theory*, pp. 241–245, 2018.

[16] E. M. Gabidulin, The theory with maximal rank metric distance, Probl. Inform. Transm., 21, pp. 1–12, 1985.

[17] H. Gluesing-Luerssen, K. Morrison, and C. Troha, Cyclic orbit codes and stabilizer subfields, Adv. Math. Comm., 25, pp. 177–197, 2015.

[18] H. Gluesing-Luerssen and C. Troha, Construction of subspace codes through linkage, Adv. Math. Comm., 10, pp. 525–540, 2016.

[19] R. Gow and R. Quinlan, Galois theory and linear algebra, Linear Algebra Appl., 430, pp. 1778–1789, 2009.

[20] R. Kötter and F. R. Kschischang, Coding for errors and erasures in random network coding, IEEE Trans. Inf. Theory, 54, pp. 3579–3591, 2008.

[21] A. Kshevetskiy and E. M. Gabidulin, The new construction of rank codes, in *Proc. IEEE Int. Symp. Inf. Theory*, pp. 2105–2108, 2005.

[22] G. Lunardon, MRD-codes and linear sets, J. Comb. Theory A, 149, pp. 1–20, 2017.

[23] G. Lunardon, R. Trombetti, and Y. Zhou, Generalized twisted Gabidulin codes, J. Comb. Theory A, 159, pp. 79–106, 2018.

[24] P. J. Lusina, E. M. Gabidulin, and M. Bossert, Maximum rank distance codes as space-time codes, IEEE Trans. Inf. Theory, 49, pp. 2757–2760, 2003.

[25] K. Marshall and A.-L. Horlemann-Trautmann, New criteria for MRD and Gabidulin codes and some rank-metric code constructions, Adv. Math. Comm., 11, pp. 533–548, 2017.

[26] W. H. Mills and R. C. Mullin, Coverings and packings, in *Contemporary Design Theory: A Collection of Surveys*, pp. 371–399, Wiley, 1992.

[27] K. Morrison, Equivalence of rank-metric and matrix codes and automorphism groups of Gabidulin codes, IEEE Trans. Inf. Theory, 60, pp. 7035–7046, 2014.

[28] O. Ore, On a special class of polynomials, Trans. Amer. Math. Soc., 35, pp. 559–584, 1933.

[29] K. Otal and F. Özbudak, Explicit constructions of some non-Gabidulin linear MRD codes, Adv. Math. Comm., 10, pp. 589–600, 2016.

[30] K. Otal and F. Özbudak, Additive rank metric codes, IEEE Trans. Inf. Theory, 63, pp. 164–168, 2017.

[31] K. Otal and F. Özbudak, Cyclic subspace codes via subspace polynomials, Des. Codes Cryptogr., 85, pp. 191–204, 2017.

[32] K. Otal and F. Özbudak, Constructions of cyclic subspace codes and maximum rank distance codes, in *Network Coding and Subspace Designs, Signals and Communication Technology*, pp. 43–66, Springer, 2018.

[33] K. Otal and F. Özbudak, Some new non-additive maximum rank distance codes, Finite Fields Appl., 50, pp. 293–303, 2018.

[34] S. Puchinger, J. R. né Nielsen, and J. Sheekey, Further generalisations of twisted Gabidulin codes, arXiv:1703.08093v2 [cs.IT], 2017.

[35] R. M. Roth, Maximum-rank array codes and their application to crisscross error correction, IEEE Trans. Inf. Theory, 37, pp. 328–336, 1991.

[36] K.-U. Schmidt and Y. Zhou, On the number of inequivalent Gabidulin codes, Des. Codes Cryptogr., 86, p. 1973–1982, 2018.

[37] J. Sheekey, New semifields and new MRD codes from skew polynomial rings, arXiv:1806.00251v1 [math.CO].

[38] J. Sheekey, A new family of linear maximum rank distance codes, Adv. Math. Comm., 10, pp. 475–488, 2016.

[39] N. Silberstein, A. Rawat, and S. Vishwanath, Error resilience in distributed storage via rank-metric codes, in *50th Annual Allerton Conference on Communication, Control, and Computing*, pp. 1150–1157, 2012.

[40] D. Silva, F. Kschischang, and R. Kötter, A rank-metric approach to error control in random network coding, IEEE Trans. Inf. Theory, 54, pp. 3951–3967, 2008.

[41] D. Silva and F. R. Kschischang, Universal secure network coding via rank-metric codes, IEEE Trans. Inf. Theory, 57, pp. 1124–1135, 2011.

[42] D. Stinson, R. Wei, and J. Yin, Packings, in *Handbook of Combinatorial Designs, Second Edition*, pp. 550–556, Chapman and Hall/CRC, 2007.

[43] V. Tarokh, N. Seshadri, and A. R. Calderbank, Space-time codes for high data rate wireless communication: performance criterion and code construction, IEEE Trans. Inf. Theory, 44, pp. 744–765, 1998.

[44] A.-L. Trautmann, F. Manganiello, M. Braun, and J. Rosenthal, Cyclic orbit codes, IEEE Trans. Inf. Theory, 59, pp. 7386–7404, 2013.

[45] R. Trombetti and Y. Zhou, A new family of MRD codes in $\mathbb{F}_q^{2n\times 2n}$ with right and middle nuclei $\mathbb{F}_{q^n}$, IEEE Trans. Inf. Theory, to appear.

[46] Z.-X. Wan, *Geometry of matrices, In memory of Professor L.K. Hua (1910-1985)*, World Scientific, 2001.

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Otal, Kamil
Nationality: Turkish (TC)
Date and Place of Birth: 1987, Konya

EDUCATION

Degree	Institution	Year of Graduation
M.S.	Deparment of Mathematics, TOBB ETU	2012
B.S.	Deparment of Mathematics, TOBB ETU	2010
High School	Selçuklu Anadolu Lisesi	2005

PROFESSIONAL EXPERIENCE

Year	Place	Enrollment
2018–Present	TÜBİTAK BİLGEM UEKAE	Senior Researcher
2012–2018	Department of Mathematics, METU	Res. & Teach. Assist.
2010–2012	Department of Mathematics, TOBB ETU	Res. & Teach. Assist.

PUBLICATIONS

International Journal Publications

- K. Otal, F. Özbudak, and W. Willems, Self-duality of generalized twisted Gabidulin codes, Adv. Math. Comm., to appear.

- E. Martínez-Moro, K. Otal, and F. Özbudak, Additive cyclic codes over finite commutative chain rings, Discr. Math., 341, pp. 1873–1884, 2018.
- K. Otal and F. Özbudak, Some new non-additive maximum rank distance codes, Finite Fields Appl., 50, pp. 293–303, 2018.
- K. Otal and F. Özbudak, Cyclic subspace codes via subspace polynomials, Des. Codes Cryptogr., 85, pp. 191–204, 2017.
- K. Otal and F. Özbudak, Additive rank metric codes, IEEE Trans. Inf. Theory, 63, pp. 164–168, 2017.
- K. Otal and F. Özbudak, Explicit constructions of some non-Gabidulin linear MRD codes, Adv. Math. Comm., 10, pp. 589–600, 2016.

International Book Chapters

- K. Otal and F. Özbudak, Constructions of cyclic subspace codes and maximum rank distance codes, in *Network Coding and Subspace Designs, Signals and Communication Technology,* pp. 43–66, Springer, 2018.

International Conference Publications

- K. Otal, Z. Saygı, and Ç. Ürtiş, Cyclotomic numbers and Sidel'nikov sequences, in *ISC TURKEY 2012, Proceedings of 5th International Conference on Information Security and Cryptology,* pp. 175–178, 2012.

Preprints

- T. Etzion, S. Kurz, K. Otal, and F. Özbudak, Subspace packings, preprint.