List decoding of rank-metric and cover-metric codes

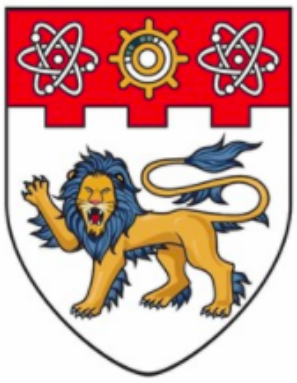
Liu, Shu

2018

Liu, S. (2018). List decoding of rank-metric and cover-metric codes. Doctoral thesis, Nanyang Technological University, Singapore.

http://hdl.handle.net/10356/74108

https://doi.org/10.32657/10356/74108



NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

LIST DECODING OF RANK-METRIC AND COVER-METRIC CODES

SHU LIU

School of Physical and Mathematical Sciences

2018

LIST DECODING OF RANK-METRIC AND COVER-METRIC CODES

SHU LIU

School of Physical and Mathematical Sciences

A thesis submitted to Nanyang Technological University

in partial fulfillment of the requirement for the degree of

Doctor of Philosophy

2018

To My Mommy and Daddy.

Acknowledgements

This thesis contains most of my work as a Ph.D. student in MAS Division, at the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. Many great people helped and contributed to my research, it has been a great and unforgettable time. Hence, I want to express my deepest and sincerest gratitude to them. Words might not be enough.

First of all, my deepest gratitude is extended to my supervisors Prof. Chaoping Xing and Prof. Huaxiong Wang. I would like to thank Prof. Chaoping Xing for bringing me into coding theory, for enthusiastically encouraging me to research, for helping me to open my view, for guiding me to play badminton and for supporting me in uncountable aspects during the past four years. I would also like to thank Prof. Huaxiong Wang from whom I got invaluable guidance and support in so many aspects during my Ph.D. time. I also appreciate their patience and belief in me. I believe it is my great honor to work with them.

I would like to thank my caring and loving family for their faithful support. In my life, my family always supports and encourages me. I am forever indebted to my parents for their concern and love. I dedicate this thesis to them.

The last four years were an unforgettable and enjoyable time for me in Singapore. I am especially grateful to my labmates in SPMS-MAS-0421 and all friends for helping and supporting me.

List of Works

Below is my list of works done during my Ph.D. studies in Nanyang Technological University.

1. Shu Liu, Chaoping Xing and Chen Yuan, List Decodability of Random Subcodes of Gabidulin Codes, In *IEEE Transactions on Information Theory*, 63(1), pp. 159-163, 2017.

2. Shu Liu, Chaoping Xing and Chen Yuan, List Decoding of Cover-metric Codes up to the Singleton Bound, In *IEEE Transactions on Information Theory*, 64(4), pp. 2410-2416, 2018.

3. Shu Liu, On the List Decodability of Self-orthogonal Rank-metric Codes, preprint.

I played an active role in finding the results and writing the following papers:

- List Decodability of Random Subcodes of Gabidulin Codes.
- List Decoding of Cover-metric Codes up to the Singleton Bound.
- On the List Decodability of Self-orthogonal Rank-metric Codes.

Contents

List of Figures

List of Tables

Abstract

A fundamental challenge in coding theory is to efficiently decode the original transmitted message even when a few symbols of the received word are erroneous. Traditionally, unique decoding outputs a unique codeword and can only correct up to half the minimum distance of the code. An alternative notion of decoding called list decoding allows the decoder to output a list of all codewords and permits recovery from errors well beyond the unique decoding barrier. However, the study of list decoding of rank-metric and cover-metric codes has not been as extensive and complete as that of Hamming metric codes.

This thesis presents a detailed investigation of list decoding of rank-metric and cover-metric codes as well as constructions of some codes with good parameters. Our main results consist of four parts. Firstly, we reveal that a random subcode of a Gabidulin code can be list decoded with list decoding radius far beyond half of the minimum distance. Then, we show that the list decoding radius of $\mathbb{F}_q$-linear self-orthogonal rank-metric codes can attain the Gilbert-Varshamov bound with polynomial list size. Furthermore, we successfully construct a new family of $\mathbb{F}_q$-linear MRD codes of large dimension that is not equivalent to any other existing families. Finally, we present that a random cover-metric code can be list decoded up to the Singleton bound and provide explicit constructions attaining this bound.

Chapter 1

Introduction

A sender sent a message through some noisy channel. The encoding process transformed the message to a codeword. This codeword is sent through a noisy channel and modified to a received word. Finally, the decoding process will help the receiver to recover the original message from the received word. This is the whole process of information transmission as depicted in Figure 1.1. A fundamental challenge in coding theory and practice is to efficiently decode the original transmitted message even when a few symbols of the received word are erroneous. In this thesis, we focus on decoding.

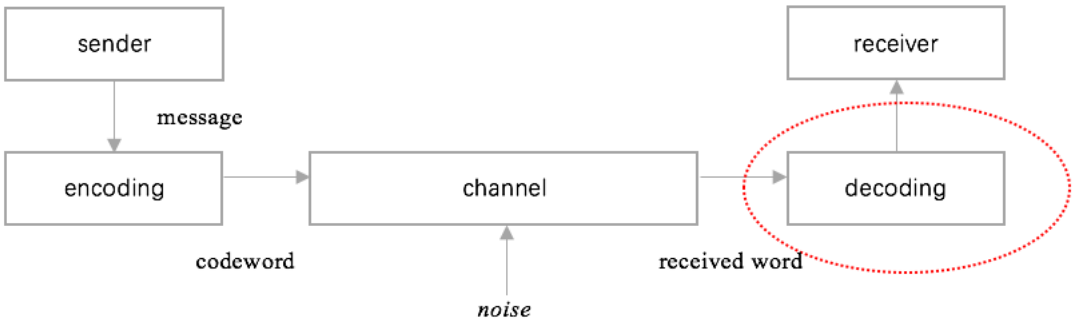


Figure 1.1: Information transmission

This chapter begins by introducing *list decoding* along with applications, history and development of rank-metric codes. We analyze the limitation of unique decoding then introduce list decoding to break the unique decoding barrier. Based on the existing results of list decoding of rank-metric codes, we point out some gaps. Moreover, in order to better

combat crisscross error patterns, we discuss cover-metric codes and its list decodability. Our contributions will be explained in further detail later on in this chapter.

1.1 Decoding

1.1.1 The Decoding Problem for Codes

Unique decoding can correct error up to half the minimum distance of the code and output a unique codeword. However, when the noise affects at least half of the minimum distance of the code, unique decoding does not work anymore. In Figure 1.2, a code of distance d cannot correct $d/2$ errors. The figure shows a received word $\mathbf{r}$ at a distance $d/2$ from two codewords c_1 and c_2. In such a case, the received word $\mathbf{r}$ could have resulted from $d/2$ errors affecting either c_1 or c_2.

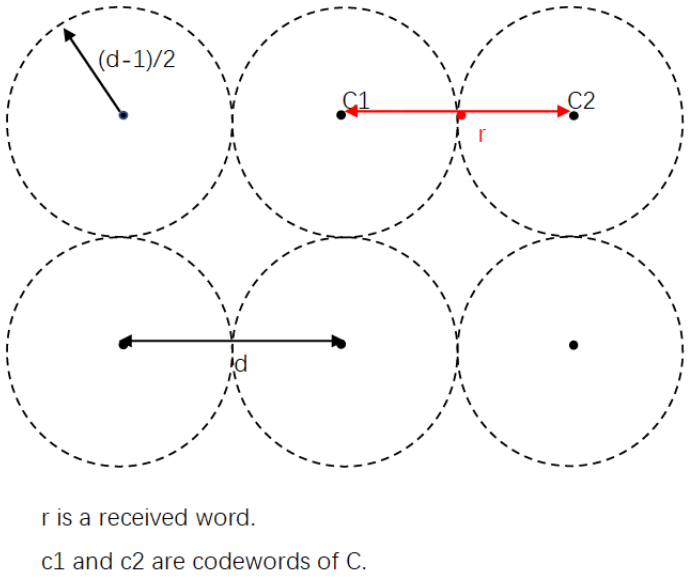


Figure 1.2: A code of distance d cannot correct $d/2$ errors

Thus, it is meaningful to consider the relaxation of unique decoding which permits one to decode beyond the perceived half the distance barrier faced by unique decoding. This relaxed notion of decoding, called *list decoding*, is the subject of this thesis.

1.1.2 List Decoding

In the late 50's, P. Elias [11], [10] and J. M. Wozencraft [66] introduced the concept of list decoding. Intuitively, given a received word, list decoding can output a list of codewords that, if successful, contains the correct transmitted codeword. One of the most common ways to design a list decoding algorithm is to output a list of codewords that are at most e away from the received word (note that a received word is obtained from the original message and some transmission noise), where e is the maximum number of errors assumed to be tolerable by the list decoding algorithm. For a code with minimum distance d, having $e \leq \frac{d-1}{2}$ means that the list size must be 1. Such a decoding algorithm is hence called the unique decoding. Contrary to the unique decoding where the number of output codeword must be equal to 1, by allowing multiple outputs, the decoder can tolerate error beyond half of the minimum distance.

The information rate, list decoding radius and list size are important parameters in list decoding. Since the information rate and list decoding radius are to represent the efficiency of a code and its error correcting ability, respectively, we want those two parameters to be large. On the other hand, list size is to represent the output size of the decoder and a very large list size is undesirable [18, pp. 22, section 1.3, paragraph 3]. This is due to at least two reasons. The first reason is that this list size provides us with a lower bound for the worst-case complexity of the decoding algorithm itself. Hence, if we require the decoding algorithm to be efficient, a polynomial or even a constant list size is of course more desirable. The second reason is because of the usefulness of this list. After the output of this list, the next step is to utilize it to decide what the original transmitted message is. This can be done, for instance, by outputting the codeword corresponding to the smallest error. When the list size is exponentially large, this decision step needs exponential time complexity. Hence, in the study of list decoding, we aim to find some tight upper bounds on the list size.

1.2 Rank-metric Codes

1.2.1 Basics of Rank-metric

Rank-metric codes have found various applications in storage systems, cryptography, space-time coding, network coding, etc. More specifically, in its application in storage systems, some rank-metric codes attaining the Singleton bound can be used to correct criss-cross error [55]. Rank-metric codes can be used to design public key cryptosystems due to its error correcting ability. However, in [16] and [51], R. Overbeck designed brute-force attacks for any Gabidulin code-based public key cryptosystems. In space-time coding, codes are designed to simultaneously take advantage of two dimensions, namely the spatial diversity of antenna elements and coding gain introduced by designed redundancy in the time dimension [14]. The crucial design criterion for space-time codes in asymptotically good channels is the minimum rank between codeword pairs [42]. Based on the properties of rank-metric codes, P. Lusina and E. M. Gabidulin applied rank-metric codes to design space-time codes and derived a Singleton-type bound in [42]. Random network coding is a powerful and useful tool to disseminate information, but it is prone to errors and erasures. Rank-metric codes are useful for error and erasure correction in network coding. For example, the error control problem of random linear network coding can be treated as a noise in the matrix and hence can be resolved, which is similar to the use of subspace code addressed by Kötter and Kschischang in [32]. Due to the properties of rank distance, it is easy to construct a class of subspace codes with constant dimension. Moreover, the problem of minimum distance decoding of subspace codes can be reduced to a problem of decoding rank-metric codes. In particular, Gabidulin codes are well used in [60] and [32].

The concept of rank-metric was first introduced as “arithmetic distance” by Loo-Keng Hua [29] in 1951. In 1978, it was then used by P. Delsarte to design error-correcting codes, their Singleton-like upper bound for the size as well as a class of codes that satisfies this bound in [7]. This class of rank-metric codes was reintroduced by Gabidulin [15] in 1985. Gabidulin further provided several properties of rank-metric codes and an efficient algo-

rithm for decoding them. Because of his significant contribution towards the development of rank-metric codes, the most famous class of rank-metric codes that is constructed by using analogous method in Reed-Solomon codes is called the Gabidulin codes. Similar to the method used for constructing Reed-Solomon codes, Gabidulin code is defined based on the evaluation of non-commutative q-linearized polynomials [46] and [47]. In 1991, R. M. Roth independently discovered rank-metric codes in the attempt to apply it in the correction of crisscross error patterns in [55].

1.2.2 Early Work on List Decoding of Rank-metric Codes

Compared to the numerous results in list decoding of classical codes, there is a relatively small number of literature results regarding efficient list decoding of rank-metric codes. Although the folded Reed-Solomon codes has a good list decodability [22], its counterpart, folded Gabidulin codes does not enjoy similar results. In [43], it was found that the rate for list decodable folded Gabidulin codes tends to 0. Although the list decoding algorithm considered in [27] has an asymptotic list decoding radius that is able to reach the Singleton bound, it is only applicable for matrices with an extremely small row-to-column ratio. Despite these results, C. Xing and C. Yuan provided some positive results where they managed to design a deterministic and a Monte-Carlo decoding algorithms for list decoding radius that can exceed the unique decoding radius in [68].

Since it is difficult to explicitly design efficient list decoding algorithms, researchers consider giving some bounds on the list size of rank-metric codes. There exist some results on the bounds for list decodable rank-metric codes. In [64] and [63], A. Wachter-Zeh gave upper and lower bounds on the list size for rank-metric codes. The upper bound is exponential for any radius exceeding the unique decoding radius. It also provides us with the existence of some rank-metric codes with exponential list size for every radius beyond the unique decoding radius. Consequentially, any list decoding algorithm for Gabidulin code with decoding radius beyond the Johnson bound must have exponential list size in

terms of the length. Hence, we cannot find any upper bound that is polynomial on the length and minimum distance which is analogous to the Johnson bound in Hamming metric. These three bounds gave us insights on the significant differences between rank-metric codes and Hamming metric codes.

In particular, these bounds reveal a gap between unique decoding radius and the Johnson bound for the list decoding of Gabidulin codes (see Figure 1.3). N. Raviv and A. Wachter-Zeh improved the worst-case bound for the list decoding of Gabidulin codes in [54]. One of the consequences of this result is the existence of some sub-family of Gabidulin codes that cannot be efficiently list decoded beyond the unique decoding radius.

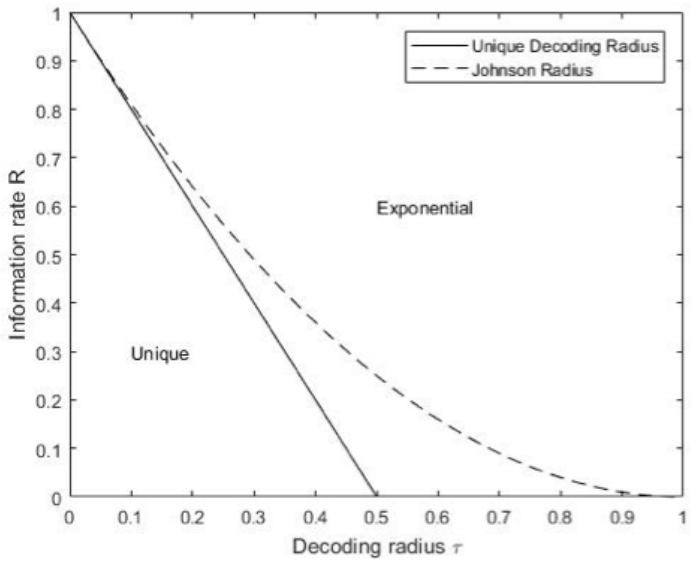


Figure 1.3: A gap between unique decoding radius and the Johnson bound in Gabidulin codes

Ding [8] further improved the study on the list decodability of random rank-metric codes. She proved that the Singleton bound gives the list decoding barrier for random rank-metric codes. Furthermore, she proved that with high probability, a random rank-metric code is list decodable up to this barrier with polynomial list size. When we give the restriction on the choice for the rank-metric codes to be $\mathbb{F}_q$-linear, the list decoding barrier becomes the Gilbert-Varshamov bound. When the $\mathbb{F}_q$-linear code is selected uniformly at random with decoding radius and rate satisfying the Gilbert-Varshamov bound, she proved

that with high probability, it is list decodable with exponential list size (see in Figure 1.4).

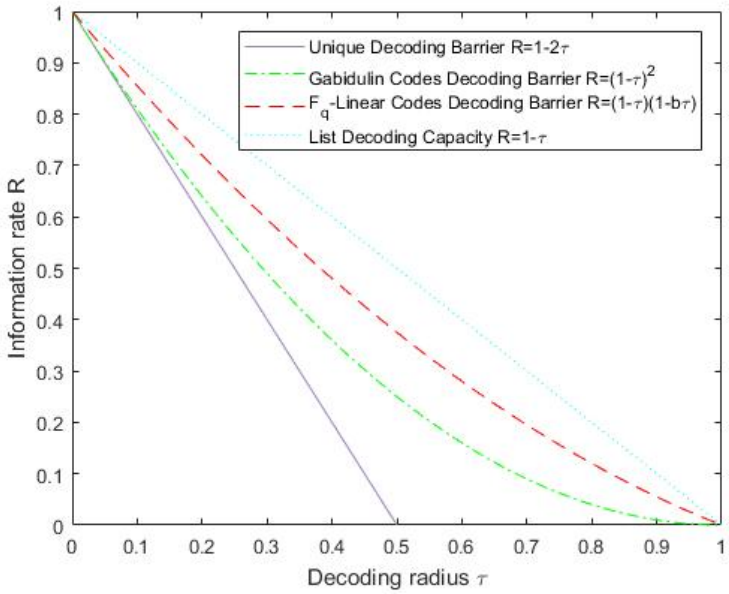


Figure 1.4: Decoding radius of rank-metric codes [8]

There exists no efficient list decoding of Gabidulin codes that can exceed the unique decoding radius [54]. Guruswami and Xing [27] gave an explicit construction of subcodes of some Gabidulin codes, which can be list decoded up to the Singleton bound. Based on those two results, subcodes of Gabidulin codes may be good candidates for list decoding. Hence, S. Liu, C. Xing and C. Yuan showed that with high probability, a random subcode of a Gabidulin code can be list decoded with decoding radius far beyond the unique decoding radius in [38]. This investigation is further discussed in Chapter 3. However, for random $\mathbb{F}_q$-linear rank-metric codes, when the list decoding radius is beyond half of the minimum distance, the list size becomes exponential. Recently, V. Guruswami and N. Resch decreased the list size of $\mathbb{F}_q$-linear rank-metric codes. In [20], the list decodability of random $\mathbb{F}_q$-linear rank-metric codes is shown to match that of a general $\mathbb{F}_q$-linear rank-metric code. A natural question that follows is whether the performance can still be maintained when we further restrict that the random $\mathbb{F}_q$-linear rank-metric codes to be also self-orthogonal. In Chapter 4, we show that the performance of random $\mathbb{F}_q$-linear self-orthogonal rank-metric codes is as good as that of general random $\mathbb{F}_q$-linear rank-metric codes. Specifically, the list

decoding radius can attain the Gilbert-Varshamov bound in [37].

1.2.3 Constructions

Aside from the list decodability of rank-metric codes, another direction that has attracted a lot of attention is the constructions of rank-metric codes which can be observed in [68], [62], [27]. In order to aid the study of constructions, Berger [2] and Morrison [44] discussed the linear and semi-linear isometries for rank-metric codes. Since Gabidulin codes based cryptosystems have proven to be weak due to their structure, so these concepts raise a natural question for the existence of general constructions of maximum rank distance codes that are not equivalent to the well-known Gabidulin codes. Recently, there are several constructions of codes which are not equivalent to Gabidulin codes. These constructions provide us with codes that are linear only over a subfield of the underlying field [62].

One of the foci of this thesis is on the construction of non-Gabidulin MRD codes. In [5], we get the first construction of nonlinear 3×3 MRD codes. [62] and [50] provided us with classes of linear non-Gabidulin MRD codes of dimension 2. An interesting class of non-Gabidulin MRD codes called the Twisted Gabidulin codes was proposed by J. Sheekey in 2015 [57]. He gave a class of codes for arbitrary length n for any dimension from 2 to $n-2$. This class was later expanded to include codes that is not $\mathbb{F}_q$-linear by K. Otal et al. [48]. Inspired by the Twisted Gabidulin codes, G. Lunardon et al. provided an alternative expansion of it called the Generalized Twisted Gabidulin codes [40]. It is natural to consider: Can we construct a new family with large dimension? In Chapter 5, we construct a new family of $\mathbb{F}_q$-linear non-Gabidulin MRD codes for arbitrary $n > 3$ for dimension $n-1$ and 1 which are not equivalent to any existing families.

1.3 Crisscross Errors

In the study of rank-metric, error is assumed to be affecting the entire matrix and is measured by its rank. In the storage of data, it is usually stored in an array of size $n \times m$.

Error usually happens throughout rows or columns (or both) of the array. Hence, the error is confined to a specific subset of rows and columns of the matrix. Such error is called the *crisscross error*. To illustrate this, consider the error pattern in Figure 1.5. This crisscross error pattern is confined to just three rows and two columns.

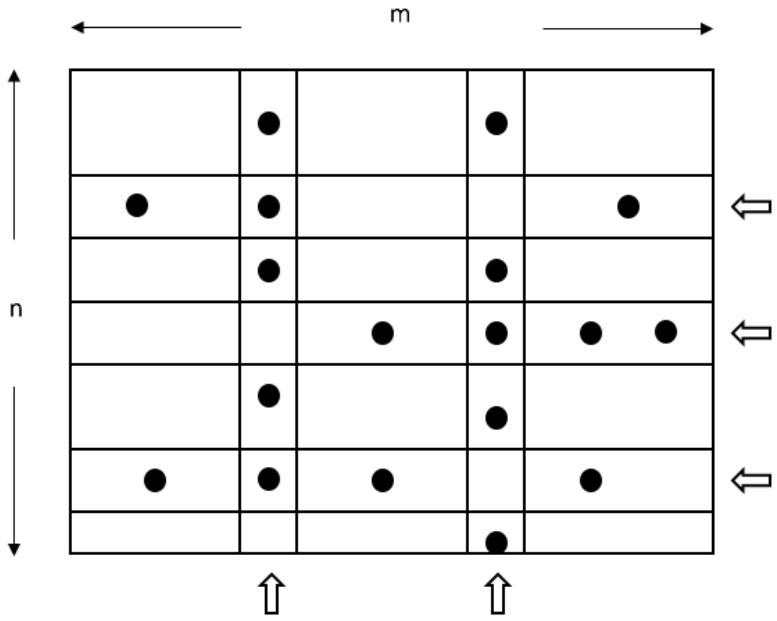


Figure 1.5: Crisscross error pattern

Such error can be found in various data storage and communication systems in [12], [34], [4], [52], [55]. In memory chip arrays, the failures of row (or column) happen because of the malfunction of row drives (or column amplifiers). Such errors can also be found in the high density magnetic tape. Crisscross error correcting codes can be used and applied in hard disc writing processes, orthogonal frequency division multiplexing (OFDM) systems and flash memories, etc.

To combat crisscross error, the cover-metric was proposed and cover-metric codes were defined in [55]. Formally, a cover of a matrix is defined to be a set of rows and columns of the matrix with each of its non-zero entry belonging to either one of the rows or one of the columns in the set. The smallest possible size of such cover is called the cover weight of the corresponding matrix. We give precise definitions in Chapter 2.

1.3.1 The Problem for Rank-metric Codes in Crisscross Errors

R. M. Roth considered correcting crisscross error by rank-metric codes [55] in 1991. Maximum rank distance codes can attain the cover-metric Singleton bound and be used to correct crisscross errors in [13]. Although there are some results about how crisscross errors can be handled by considering them as array codes in rank-metric, rank-metric seems to be "too strong" for the crisscross errors.

Rank-metric codes not only can correct erroneous rows and columns, but they also corrects a certain number of rank errors. Since the rank of a matrix is at most its cover weight, a list decodable rank-metric code is also a list decodable cover-metric code. Based on the existing results, we can convert from rank-metric codes to cover-metric codes. In [27] and [26], it was shown that one can efficiently list decode a rank-metric code up to the Singleton bound if the number of rows over the number of columns is extremely small. Although there have been numerous results on list decoding of rank-metric codes (see for example in [54], [63], [64] and [8]), it is still unknown whether they can even be efficiently list decoded. So, it is undesirable to correct crisscross errors by rank-metric codes. Then, cover-metric codes are defined to correct crisscross errors.

1.3.2 Cover-metric Codes

Cover-metric codes are specifically designed to resolve crisscross errors. We are interested in two problems: One is to find efficient decoding algorithms of cover-metric codes, another is to construct some cover-metric codes with good parameters.

There are many literary results regarding unique decoding and constructions of cover-metric codes. Specifically speaking, the first construction of cover-metric codes was done by Roth in 1991 [55]. They were constructed by utilizing existing maximum distance separable (MDS) codes which can be decodable up to half of the minimum cover distance as well as their decoding algorithms. B. Blaum and J. Bruck later constructed another cover-metric codes along with their decoding algorithms that can correct crisscross errors

with cover weight up to 1 in [3]. Some other constructions include that of D. Lund, E. M. Gabidulin and B. Honary [41] and V. R. Sidorenko [58]. The codes from [55] and [41] were constructed based on maximum rank array codes and can reach the Singleton-like bound for some fixed dimension.

Aside from the deterministic decoding algorithms mentioned above, some probabilistic crisscross error corrections were proposed for a specific family of codes with smaller redundancy in [56]. Investigations on the generalized minimum distance decoding for cover-metric codes have been conducted in [59]. R. Sidorenko and M. Gabidulin [59] showed a generalized minimum distance decoding for correcting array errors. In particular, one can uniquely decode a cover-metric code up to half of its minimum distance.

Due to the limitation of unique decoding, natural questions are: Can cover-metric codes correct more errors? Moreover, can we construct those cover-metric codes of better decoding radii?

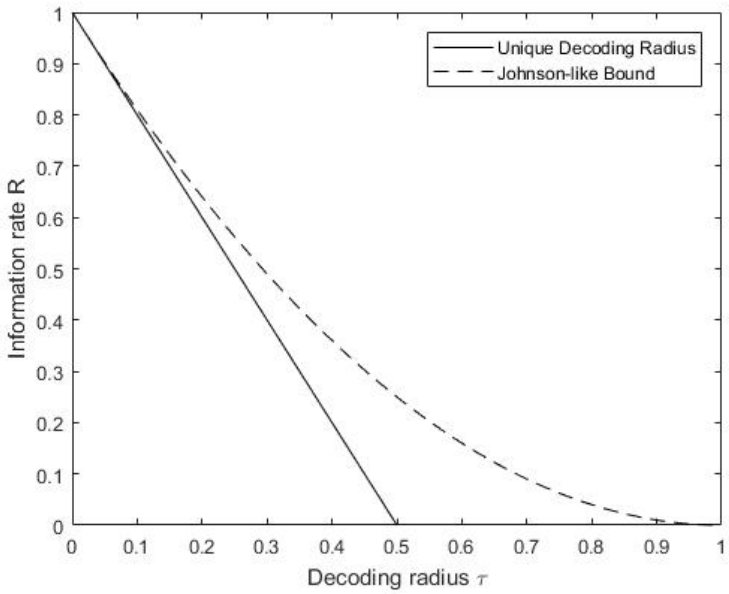


Figure 1.6: Decoding radius of cover-metric codes

1.3.3 List Decoding of Crisscross Errors

The list decoding of cover-metric codes was first considered by A. Wachter-Zeh in [65]. She showed that cover-metric codes can be list decoded up to the Johnson-like bound. She also showed that given a list decodable Hamming metric code, it can be used to construct such list decodable cover-metric code. Since the Johnson-like bound is always less than the Johnson bound, the explicit decoding algorithm in [65] required the list decoding radius to be less than the Johnson bound no matter which Hamming metric codes are used.

Based on the gap that we can observe in Figure 1.6, a natural question that occurs is whether we can make an improvement in the radius beyond the Johnson-like bound. In Chapter 6, we show that a random cover-metric code can be list decoded up to the Singleton bound and provide explicit constructions of cover-metric codes attaining this bound.

Chapter 2

Preliminaries

In this chapter, we review the basic definitions on rank-metric, cover-metric codes and list decoding. In order to avoid introducing too many notations this early on, we only discuss the most fundamental definitions and will defer a formal treatment of further definitions until they are needed.

Throughout this thesis, the following general notations will be used. Let q be a prime power. We denote the finite field with q elements by $\mathbb{F}_q$. Let $\mathbb{F}_q^{n\times m}$ be the set of all $n \times m$ matrices with entries in $\mathbb{F}_q$. The extension field of extension degree m of $\mathbb{F}_q$ is denoted by $\mathbb{F}_{q^m}$. Without loss of generality, we assume $n \leq m$, otherwise we consider the transpose of the matrices. We use ρ as a parameter to describe the ratio $\rho = \frac{n}{m}$ which by assumption is a real number in $(0, 1]$.

2.1 Codes in Rank-metric

2.1.1 Rank-metric and Its Properties

A rank-metric code can be regarded as a set of $n \times m$ matrices over the finite field $\mathbb{F}_q$. Equivalently, it can be interpreted as a set of vectors over the extension field $\mathbb{F}_{q^m}$ of length n. Specifically, if we fix an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$, each column vector of $\mathbb{F}_q^m$ can be identified with an element in $\mathbb{F}_{q^m}$ and vice versa. Hence, each matrix $X \in \mathbb{F}_q^{n\times m}$ can be identified

with a vector $\mathbf{x} \in \mathbb{F}_{q^m}^n$.

We start by defining rank weight and rank distance.

Definition 1. Let $\mathbf{x} = (x_1, x_2, \cdots, x_n)$ and $\mathbf{y} = (y_1, y_2, \cdots, y_n) \in \mathbb{F}_{q^m}^n$ and $X, Y \in \mathbb{F}_q^{n \times m}$ be their corresponding matrices, respectively. The rank weight of $\mathbf{x}$ is the rank of its matrix representation X over $\mathbb{F}_q$, i.e.,

$$\mathrm{wt}_R(\mathbf{x}) = \mathrm{rank}(\mathbf{x}) = \mathrm{rank}(X).$$

The rank distance between $\mathbf{x}$ and $\mathbf{y}$ can be identified by the rank of the difference between the two matrix representations, such that

$$d_R(\mathbf{x}, \mathbf{y}) := \mathrm{rank}(\mathbf{x} - \mathbf{y}) = \mathrm{rank}(X - Y).$$

Lemma 1. *The rank distance as given in Definition 1 is a metric.*

Proof. For any vectors $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{F}_{q^m}^n$ with their corresponding matrices $X, Y, Z \in \mathbb{F}_q^{n \times m}$ respectively,

- Positive definiteness: $d_R(\mathbf{x}, \mathbf{y}) = \mathrm{rank}(X - Y) \geq 0$, where $d_R(\mathbf{x}, \mathbf{y}) = \mathrm{rank}(X - Y) = 0$ if and only if $\mathbf{x} = \mathbf{y}$.
- Symmetry: $d_R(\mathbf{x}, \mathbf{y}) = \mathrm{rank}(X - Y) = \mathrm{rank}(Y - X) = d_R(\mathbf{y}, \mathbf{x})$.
- Triangle inequality: Recall that $\mathrm{rank}(X + Y) \leq \mathrm{rank}(X) + \mathrm{rank}(Y)$. We utilize this fact to show the triangle inequality for this rank distance. Note that

$$\begin{aligned} d_R(\mathbf{x}, \mathbf{z}) &= \mathrm{rank}(X - Z) = \mathrm{rank}(X - Y + Y - Z) \\ &\leq \mathrm{rank}(X - Y) + \mathrm{rank}(Y - Z) = d_R(\mathbf{x}, \mathbf{y}) + d_R(\mathbf{y}, \mathbf{z}). \end{aligned}$$

■

Based on the rank distance, we proceed to define minimum rank distance.

Definition 2. A rank-metric code $\mathcal{C}$ is a subset of $\mathbb{F}_q^{n\times m}$. Then, the minimum rank distance of $\mathcal{C}$ is

$$d_R(\mathcal{C}) := \min\{\mathrm{rank}(X-Y) : X, Y \in \mathcal{C}, X \neq Y\}.$$

The relative minimum rank distance and information rate of a rank-metric code $\mathcal{C}$ are defined by

$$\delta(\mathcal{C}) = \frac{d_R - 1}{n} \quad \text{and} \quad R(\mathcal{C}) = \frac{\log_q |\mathcal{C}|}{mn}.$$

Remark 1. Generally, we define the relative rank distance of $\mathcal{C}$ by $\frac{d_R}{n}$. However, in this thesis, defining it as $\frac{d_R-1}{n}$ sometimes leads to neater formulae.

An $\mathbb{F}_q$-linear rank-metric code $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{n\times m}$. An $[n, k, d_R]$ linear rank-metric code is the notation used to represent a rank-metric code with length n, dimension k and minimum rank distance d_R.

Lemma 2. *(see in [15]) For any rank-metric code $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ of minimum rank distance d_R and length n, it satisfies the following Singleton bound*

$$log_q(|\mathcal{C}|) \leq m(n - d_R + 1).$$

Remark 2. (see in [36, pp. 92-94, section 5.4]) An alternative way to state the Singleton bound for any rank-metric code $\mathcal{C}$ is through the use of its rate and relative minimum rank distance which can be written as

$$R(\mathcal{C}) + \delta(\mathcal{C}) \leq 1,$$

where we choose the relative minimum rank distance as $\delta(\mathcal{C}) = \frac{d_R-1}{n}$ rather than $\frac{d_R}{n}$. The limit for the normalized minimum distance of the code $\mathcal{C}$ is $1 - R(\mathcal{C})$.

A rank-metric code $\mathcal{C}$ that meets the Singleton bound is called a *maximum rank distance* (MRD) code. A well-known class of MRD codes is Gabidulin codes in [15].

We move on to the definition of the dual of a rank-metric code.

Definition 3. For two vectors $\mathbf{x} = (x_1, \cdots, x_n), \mathbf{y} = (y_1, \cdots, y_n) \in \mathbb{F}_{q^m}^n$, let $\langle \mathbf{x}, \mathbf{y} \rangle := \sum_{i=0}^{n-1} x_i y_i$ be their inner product. Let $\mathcal{C}$ be a rank-metric code over $\mathbb{F}_q$. Then,

$$\mathcal{C}^{\perp} := \{\mathbf{x} \in \mathbb{F}_{q^m}^n : \langle \mathbf{x}, \mathbf{c} \rangle = 0, \forall \mathbf{c} \in \mathcal{C}\}$$

is called the dual code of $\mathcal{C}$.

In addition, an alternative way to define a dual of a rank-metric code was proposed in [53].

Definition 4. The Delsarte's dual code of $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ is

$$\mathcal{C}_{Tr}^{\perp} = \{X \in \mathbb{F}_q^{n \times m} : \mathrm{Tr}(CX^T) = 0, \forall C \in \mathcal{C}\}$$

where T is the transpose and $\mathrm{Tr}(X)$ is the trace of the matrix X.

Some straightforward dual properties are summarized in the lemma below.

Lemma 3. *Let $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ be an $\mathbb{F}_q$-linear rank-metric code. Then, we have*

- $(\mathcal{C}^{\perp})^{\perp} = (\mathcal{C}_{Tr}^{\perp})_{Tr}^{\perp} = \mathcal{C}$.
- $\dim_{\mathbb{F}_q}(\mathcal{C}_{Tr}^{\perp}) = mn - \dim_{\mathbb{F}_q}(\mathcal{C})$ *and* $\dim_{\mathbb{F}_{q^m}}(\mathcal{C}^{\perp}) = n - \dim_{\mathbb{F}_{q^m}}(\mathcal{C})$.

Definition 5. Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a linear rank-metric code.

- A generator matrix of $\mathcal{C}$ is a matrix G whose rows form a basis for $\mathcal{C}$.
- A parity check matrix H of $\mathcal{C}$ is a generator matrix for the dual rank-metric code $\mathcal{C}^{\perp}$.

There are several ways for two rank-metric codes to be deemed similar. In the following, we provide the formal definitions of proper and improper equivalence for rank-metric codes.

Definition 6. Let $\mathcal{C}, \mathcal{C}' \subseteq \mathbb{F}_q^{n \times m}$ be two linear rank-metric codes, if

$$\mathcal{C}' = X\mathcal{C}Y := \{XCY : C \in \mathcal{C}\},$$

for some invertible matrices $X \in \mathbb{F}_q^{n\times n}$ and $Y \in \mathbb{F}_q^{m\times m}$, we say that $\mathcal{C}$ is *properly equivalent* to $\mathcal{C}'$.

Definition 7. Let $\mathcal{C}^T$ be the set of transposed matrices of $\mathcal{C}$ and $n = m$. If $\mathcal{C}'$ is (properly) equivalent to $\mathcal{C}^T$, then we call $\mathcal{C}'$ and $\mathcal{C}$ are *improperly equivalent*, that is

$$\mathcal{C}' = X\mathcal{C}^T Y := \{XCY : C \in \mathcal{C}^T\}.$$

There exist similar equivalence ideas discussed in [6], [44], [49] and [57]. In this thesis, we only consider the proper equivalence, for short, equivalence.

2.1.2 Linearized Polynomials

Gabidulin codes are a well-known class of MRD codes which has received a lot of attention because of its good structure and fast decoding algorithm. Gabidulin codes are analogue of classical Reed-Solomon codes.

Linearized polynomials play a significant role in the construction of Gabidulin codes. Thus, before introducing the Gabidulin codes, we first discuss linearized polynomials. Linearized polynomials were firstly studied by Ore in [46]. Let us give the precise definition of linearized polynomials in the following.

Definition 8. A polynomial $f(x)$ over $\mathbb{F}_{q^m}$ is said to be a q-linearized polynomial, if it has the following form:

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

where $a_i \in \mathbb{F}_{q^m}$. The q-degree of $f(x)$ is defined to be e if $a_e \neq 0$. Note that $f(x)$ has no constant term. We denote by $\mathcal{L}_k(x, \mathbb{F}_{q^m})$ the set of all linearized polynomials of q-degree at most $k-1$.

Remark 3. Linearized polynomials can be regarded as $\mathbb{F}_q$-linear maps, that is:

- For any given linearized polynomial $f(x)$, it is obvious that $f(x_1 + x_2) = f(x_1) + f(x_2)$ and $f(x_1) = \lambda f(x_1)$, for any $x_1, x_2 \in \mathbb{F}_{q^m}$ and $\lambda \in \mathbb{F}_q$.

- The ordinary product of linearized polynomials $f_1(x)f_2(x)$ is not a linearized polynomial. However, the composition $f_1(x) \circ f_2(x) = f_1(f_2(x))$ is also a linearized polynomial.

- The set of linearized polynomials with addition $+$ and multiplication operation $\circ$ forms a non-commutative ring.

Definition 9. The symmetric bilinear form b on linearized polynomials is defined by

$$b\left(\sum_{i=0}^{n-1} f_i x^{q^i}, \sum_{i=0}^{n-1} g_i x^{q^i}\right) := \mathrm{Tr}\left(\sum_{i=0}^{n-1} f_i g_i\right),$$

where Tr presents the absolute trace from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, $f_i, g_i \in \mathbb{F}_{q^m}$.

2.1.3 Gabidulin Codes

Equipped with the operations of addition, composition of linearized polynomials and scalar multiplication with elements in $\mathbb{F}_q$, $\mathcal{L}_n(x, \mathbb{F}_{q^m})$ forms an $\mathbb{F}_q$-algebra and is isomorphic to the algebra formed by all $n \times m$ matrices over $\mathbb{F}_q$ [67]. It is well-known that a q-linearized polynomial $f(x)$ defines an $\mathbb{F}_q$-linear map of $\mathbb{F}_{q^m}$ via $\alpha \mapsto f(\alpha)$. Furthermore, if we fix an $\mathbb{F}_q$-linearly independent set $\{\alpha_1, \cdots, \alpha_n\}$ of $\mathbb{F}_{q^m}$, then the linear map defined by $\alpha \mapsto f(\alpha)$ corresponds to the matrix $M_f = (f(\alpha_1), \ldots, f(\alpha_n))^T$, where T denotes the transpose and each $f(\alpha_i)$ is viewed as a row vector of $\mathbb{F}_{q^m}^n$ under a fixed basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Thus, using this map, one establishes a one-to-one correspondence between $\mathcal{L}_n(x, \mathbb{F}_{q^m})$ and $\mathbb{F}_q^{n\times m}$. In fact, this correspondence is an algebra isomorphism. Based on this isomorphism, we give the precise definition of Gabidulin codes in the following.

Definition 10. Let $\{\alpha_1, \cdots \alpha_n\} \subseteq \mathbb{F}_{q^m}$ be an $\mathbb{F}_q$-linearly independent set. A Gabidulin code $\mathcal{G}_k(n, m, q)$ is defined as follows

$$\mathcal{G}_k(n, m, q) = \{M_f : f(x) \text{ is a } q\text{-linearized polynomial over } \mathbb{F}_{q^m} \text{ of } q\text{-degree at most } k-1\}.$$

The information rate of the Gabidulin code is $R = k/n$.

Remark 4. We can define a Gabidulin code in $\mathbb{F}_q^{n\times m}$ to be a linear $[n, k]$ block code over $\mathbb{F}_{q^m}$ by the generator matrix

$$G = \begin{bmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ {\alpha_1}^q & {\alpha_2}^q & \cdots & {\alpha_n}^q \\ \vdots & \vdots & \ddots & \vdots \\ {\alpha_1}^{q^{k-1}} & {\alpha_2}^{q^{k-1}} & \cdots & {\alpha_n}^{q^{k-1}} \end{bmatrix},$$

where the elements $\alpha_1, \cdots, \alpha_n \in \mathbb{F}_{q^m}$ are linearly independent over $\mathbb{F}_q$.

Firstly, we assume the input of the Gabidulin encoder to be a message vector, such as

$$\mathbf{u} = [u_0, u_1, \cdots, u_{k-1}],$$

which contains k message symbols in the field $\mathbb{F}_{q^m}$. Let $f_{\mathbf{u}}(x)$ present the corresponding q-linearized polynomial $\sum_{i=0}^{k-1} u_i x^{q^i}$. Then, we have the corresponding codeword $V = (\mathbf{u}G)^T$ to be equal to

$$[f_{\mathbf{u}}(\alpha_1), f_{\mathbf{u}}(\alpha_2), \cdots, f_{\mathbf{u}}(\alpha_n)]^T,$$

where V can be regarded as a matrix in $\mathbb{F}_q^{n\times m}$ over the finite field $\mathbb{F}_q$.

Remark 5. Since any Gabidulin code in $\mathbb{F}_q^{n\times m}$ has rate $R = \frac{k}{n}$ and minimum rank distance $d_R = n - k + 1$, it achieves the Singleton bound and hence it is a maximum rank distance (MRD) code.

2.1.4 List Decoding of Rank-metric Codes

For list decoding, given a received word, the aim is to output a list of all codewords that contains the original message by a rank-metric ball of certain radius around the received word. The radius of the rank-metric ball corresponds to the number of errors corrected by the list decoding procedure. Hence it is of interest to quantify the maximum number of

codewords in a rank-metric ball of certain radius, or equivalently, to quantify the largest number of errors that can be list decoded with lists of a certain size.

A rank-metric ball in Figure 2.1 is analogous to the Hamming ball in the classical block codes. The formal definition is given in the following.

Definition 11. Let $\tau \in (0,1)$ and $X \in \mathbb{F}_q^{n\times m}$. The rank-metric ball centered at X and radius τn is defined by

$$\mathcal{B}_R(X,\tau n) := \{Y \in \mathbb{F}_q^{n\times m} : d_R(X,Y) \leq \tau n\}.$$

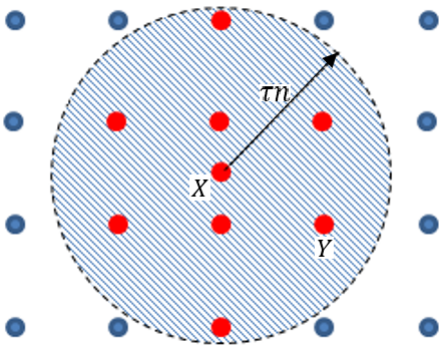


Figure 2.1: Rank-metric ball

Next we introduce the Gaussian binomial coefficient to help us in estimating the size of a rank-metric ball.

For any vector space V over $\mathbb{F}_q$ of dimension n, we denote by $\begin{bmatrix} n \\ k \end{bmatrix}_q$, the number of subspaces of V with dimension k. This is called the *Gaussian binomial coefficient* and it has the following explicit formula,

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i}.$$

It can be verified that this formula $\begin{bmatrix} n \\ k \end{bmatrix}_q$ has the following bounds that can be used as estimation [17],

$$q^{k(n-k)} \leq \begin{bmatrix} n \\ k \end{bmatrix}_q \leq 4q^{k(n-k)}.$$

Definition 12. For an integer $\mathcal{L} \geq 1$ and a real $\tau \in (0, 1)$, a rank-metric code $\mathcal{C}$ is said to be $(\tau, \mathcal{L})^R$-list decodable if for every $X \in \mathbb{F}_q^{n \times m}$

$$|\mathcal{B}_R(X, \tau n) \cap \mathcal{C}| \leq \mathcal{L}.$$

Any non-trivial bound on the list decoding capability can provide us some insights on rank-metric codes with good list decodability. A. Wachter-Zeh firstly gave lower and upper bounds on the list size of rank-metric codes [64]. A lower bound is showed in the theorem below.

Theorem 1. *(see in [64]) Let $\mathcal{G}_k(n, m, q)$ be a Gabidulin code of minimum rank distance $d_R = n - k + 1$ over $\mathbb{F}_{q^m}$. Let the list decoding radius $\tau n < d_R$, then there exists a word $r \in \mathbb{F}_{q^m}^n$ such that*

$$\mathcal{L} \geq |\mathcal{B}_R(X, \tau n) \cap \mathcal{G}_k(n, m, q)| \geq q^m q^{\tau n(m+n) - \tau^2 n^2 - m d_R}.$$

The proof of the above theorem is based on the evaluation of linearized polynomials, which is inspired by bounding technique performed to analyze the list size of Reed-Solomon codes [31], [1].

Remark 6. When $n = m$, the list size can be rewritten as

$$\mathcal{L} \geq q^n q^{2n^2\tau - \tau^2 n^2 - n d_R}.$$

It implies when the list decoding radius $\tau n \geq n - \sqrt{n(n - d_R + \epsilon)}$, $0 \leq \epsilon < 1$, the list size must be exponential in n. In particular, the list decoding radius τ becomes the Johnson bound, when $\epsilon = 0$,

Theorem 2. *(see in [64]) Let $\lfloor \frac{d_R - 1}{2} \rfloor \leq \tau n < d_R$. Then, for any (n, M, d_R) rank-metric*

code $\mathcal{C}$, the maximum list size is upper bounded by

$$\begin{aligned}\mathcal{L} &\leq |\mathcal{B}_R(X, \tau n) \cap \mathcal{C}| \\ &\leq 1 + 4 \cdot \left(\tau n - \left\lfloor \frac{d_R - 1}{2} \right\rfloor \right) \cdot q^{(2\tau n - d_R + 1)\left(n - \left\lfloor \frac{d_R - 1}{2} \right\rfloor\right) - 1}.\end{aligned}$$

Unfortunately, for any list decoding radius beyond unique decoding radius $\tau n = \lfloor \frac{d_R - 1}{2} \rfloor$, this upper bound is exponential. In addition, A. Wachter-Zeh showed that there exists a rank-metric code with exponential list size for any radius larger than unique decoding radius in [64].

2.2 Codes in Cover-metric

2.2.1 Definitions and Properties

Crisscross error is considered when the corruption occurs in rows or columns (or both) of data stored in arrays. Such error can be found in various data storage and communication systems [12], [4], [52], [55]. To combat this error, the cover-metric was proposed and cover-metric codes were defined in [55].

The cover-metric code is a set of $n \times m$ $(n \leq m)$ matrices over $\mathbb{F}_q$. Firstly, we define the cover of a matrix.

Definition 13. The cover of an $n \times m$ matrix $A = (a_{ij})_{i,j=0}^{n-1,m-1}$ is a pair (X, Y) with $X \subseteq \{0, 1, \ldots, n-1\}$ and $Y \subseteq \{0, 1, \ldots, m-1\}$ such that, whenever $a_{ij} \neq 0$, we have $i \in X$ or $j \in Y$ for all $0 \leq i \leq n-1, 0 \leq j \leq m-1$. The size of a cover (X, Y) is defined to be $|X| + |Y|$.

Based on the definition of the cover of a matrix, we consider the following definition of cover weight of a matrix.

Definition 14. The cover weight (or "term rank") of $A \in \mathbb{F}_q^{n \times m}$, denoted by $\mathrm{wt}_{\mathsf{C}}(A)$, is the minimum size of all covers of A. Obviously, the cover weight $\mathrm{wt}_{\mathsf{C}}(A) \leq n$, where C

denotes the cover-metric, which is different to rank-metric and Hamming metric.

Note that the cover of a matrix with minimum size may not be unique. It is not difficult to verify that this defines a metric in the space $\mathbb{F}_q^{n\times m}$, called cover-metric. Thus, we define the cover distance by

$$d_{\mathsf{C}}(A,B) := \mathrm{wt}_{\mathsf{C}}(A-B).$$

For example, let us consider a 3×7 binary matrix A in Figure 2.2. The matrix A has two covers of weight 3, namely $\{7,8,9\}$ and $\{7,2,4\}$, we can not find any cover with weight less than 3. It follows that $\mathrm{wt}_{\mathsf{C}}(A)=3$.

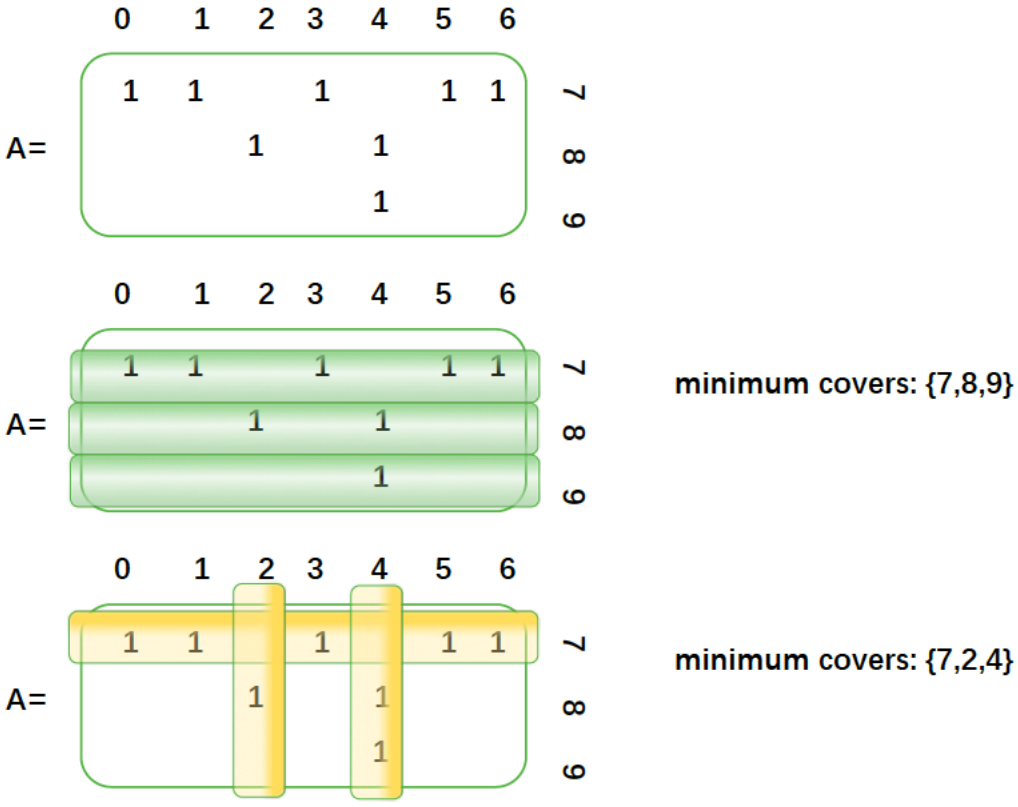


Figure 2.2: The cover of a matrix with minimum size may not be unique

Definition 15. An $(n\times m, M, d_{\mathsf{C}})_q^{\mathsf{C}}$ cover-metric code C is a set of matrices in $\mathbb{F}_q^{n\times m}$, with cardinality M and minimum cover distance d_{C}, where d_{C} is defined as the following

$$d_{\mathsf{C}} := \min_{A,B\in\mathsf{C},A\neq B} d_{\mathsf{C}}(A,B) = \min_{A,B\in\mathsf{C},A\neq B} \mathrm{wt}_{\mathsf{C}}(A-B).$$

A cover-metric code over $\mathbb{F}_q$ is said to be $\mathbb{F}_q$-linear if it forms an $\mathbb{F}_q$-vector space under matrix addition and scalar multiplication. By $[n \times m, k, d_{\mathsf{C}}]_q^{\mathsf{C}}$, we denote an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{n\times m}$ of dimension k and minimum cover distance d_{C}. In this case, we have $d_{\mathsf{C}} = \min_{A\in\mathsf{C},A\neq 0} \mathrm{wt}_{\mathsf{C}}(A)$.

Similar to the rank-metric codes, we define rate and relative minimum cover distance of an $(n \times m, M, d_{\mathsf{C}})_q^{\mathsf{C}}$ cover-metric code C by

$$R(\mathsf{C}) = \frac{\log_q |\mathsf{C}|}{mn} \text{ and } \delta(\mathsf{C}) = \frac{d_{\mathsf{C}} - 1}{n}.$$

There exists a trade-off between the information rate and the relative minimum cover distance.

Lemma 4. *(see in [55]) The Singleton bound of any $[n \times m, k, d_{\mathsf{C}}]_q^{\mathsf{C}}$ cover-metric code over $\mathbb{F}_q$ is defined by*

$$mn - k \geq (d_{\mathsf{C}} - 1)m.$$

In [55], [13], it was shown that any linear cover-metric code C must obey the Singleton bound. Actually, this is also true for nonlinear cover-metric codes. In Chapter 6, we show that every cover-metric code $\mathcal{C}$ must obey the Singleton bound $R(\mathsf{C}) + \delta(\mathsf{C}) \leq 1$.

2.2.2 List Decoding of Cover-metric Codes

Unique decoding of cover-metric codes has been extensively studied in [3], [56], [59]. In order to break this limit, one has to consider list decoding. Since it is difficult to have an efficient list decoding of crisscross errors in rank-metric codes, so we consider list decoding of cover-metric codes.

Similar to the rank-metric ball, given a cover distance as the radius, the cover-metric ball is used to cover matrices in it.

Definition 16. For a matrix $X \in \mathbb{F}_q^{n\times m}$ and a real number r, the cover-metric ball of center

X and radius r is defined by

$$\mathcal{B}_{\mathsf{C}}(X, r) := \{Y \in \mathbb{F}_q^{n\times m} : d_{\mathsf{C}}(X, Y) \leq r\}.$$

Definition 17. A cover-metric code $\mathsf{C} \subseteq \mathbb{F}_q^{n\times m}$ is said to be $(\tau, \mathcal{L})^{\mathsf{C}}$-list decodable, if for every $X \in \mathbb{F}_q^{n\times m}$, we have

$$|\mathcal{B}_{\mathsf{C}}(X, \tau n) \cap \mathsf{C}| \leq \mathcal{L}.$$

Chapter 3

List Decodability of Random Subcodes of Gabidulin Codes

This chapter is based on the work in [38]. Efficient list decoding of rank-metric codes seems to be more difficult compared with that of classical block codes although list decodability of random rank-metric codes is completely determined by Ding [8]. For example, it was shown by Raviv and Wachter-Zeh [54] that the list decoding radius of Gabidulin codes is the same as the unique decoding radius, i.e., half of the minimum distance for some instances of parameters. On the other hand, Guruswami and Xing [27] gave an explicit construction of subcodes of Gabidulin codes, which can be list decoded up to the Singleton bound. This implies that subcodes of Gabidulin codes are good candidates for list decoding. In this chapter, we confirm that, with overwhelming probability, a random subcode of a Gabidulin code can be list decoded with decoding radius far beyond half of the minimum distance.

3.1 Introduction

Although Ding [8] has completely determined the list decodability of random rank-metric codes, explicitly designing efficient list decoding algorithms for rank-metric codes

seems to have more complications than that of classical block codes. The analog of a Reed-Solomon code is a Gabidulin code. There exist efficient list decoding algorithms of Reed-Solomon codes beyond half of the minimum distance. However, no efficient list decoding of Gabidulin codes beyond half of the minimum distance has been found. In fact, it was proved in [54] that it is impossible to list decode square Gabidulin codes beyond half of the minimum distance for some instances of parameters. Since there is little hope to list decode Gabidulin codes beyond half of the minimum distance, i.e., unique decoding radius, people have been looking for some variants of Gabidulin codes. It has been shown in [27] that one could list decode subcodes of Gabidulin codes up to the Singleton bound. This implies that subcodes of Gabidulin codes are good candidates for list decoding.

In this chapter we study the list decodability of random subcodes of Gabidulin codes. It has been shown that the subcode of a Gabidulin code can be efficiently list decoded up to the Singleton bound $1 - R - \epsilon$ [27] and [25]. Hence, it seems reasonable to deduce that the subcode of a Gabidulin code may meet our demands of list decoding. To better understand the properties of these subcodes, we need to study the list decodability of random subcodes of a Gabidulin code. It has been shown in [8] that with high probability list decoding radius of a random linear rank-metric code meets the Gilbert-Varshamov bound. When the list decoding radius is beyond this bound, any rank-metric codes have exponential list size. The question arises: "Can we derive a similar bound for subcodes of a Gabidulin code?" Any meaningful upper bounds and lower bounds will help us investigate subcodes of Gabidulin codes with good list decoding radius. In this chapter, we derive several lower bounds for random subcodes of Gabidulin codes. Our bounds indicate that, with high probability, a random subcode of a Gabidulin code has decoding radius beyond the unique decoding radius. Furthermore, for some rate regime, the decoding radius of a random subcode of a Gabidulin code achieves the Gilbert-Varshamov bound which is optimal for list decoding radius (see in [8]). As a consequence, we are able to show that our lower bound meets the Singleton bound when the ratio ρ of the number of rows over the number of columns is $O(\epsilon)$ (here rows and columns refer to those of matrices in rank-metric codes). Our results

confirm the existence of a subcode of a Gabidulin code with better parameters than the code in [27] where the ratio $\rho = O(\epsilon^2)$.

This chapter is organized as follows. Firstly, we recall list decoding of rank metric codes. Then, we derive two lower bounds of subcodes of Gabidulin codes. One lower bound deals with the case where the rate of a subcode is close to that of the mother Gabidulin code. Other lower bound studies the case where the rate of a subcode is a bit far from that of the mother Gabidulin code. In the third section, we investigated list decodability of $\mathbb{F}_{q^m}$-linear subcodes of Gabidulin codes. Some conclusions were discussed in the last section.

3.2 Background

Ding [8] provides us with a bound for list decodability of a random rank-metric code that follows the Gilbert-Varshamov bound.

Lemma 5. *(see in [8]) Let the ratio $\rho = \frac{n}{m}$ be a constant. Let $m, n, \mathcal{L}$ be positive integers satisfying $\mathcal{L} = \text{poly}(mn)$. Then a $(\tau n, \mathcal{L})^R$-list decodable linear rank-metric code of rate R must satisfy the Gilbert-Varshamov bound*

$$R \leq (1-\tau)(1-\rho\tau).$$

On the other hand, for any given small $\epsilon > 0$, with high probability a random rank-metric code of rate R is $(\tau n, O(1/\epsilon))^R$-list decodable if $R = (1-\tau)(1-\rho\tau) - \epsilon$.

If $\rho = 1$, then the Gilbert-Varshamov bound becomes $R \leq (1-\tau)^2$, i.e.,

$$\tau \leq 1 - \sqrt{R}.$$

A direct consequence of the above lemma is the following.

Corollary 1. *Regardless of the ratio $\rho = \frac{n}{m}$, a $(\tau n, \mathcal{L})^R$-list decodable rank-metric code in*

$\mathbb{F}_q^{n\times m}$ *with rate* R *and list size* $\mathcal{L} = \text{poly}(mn)$ *must satisfy the Singleton bound*

$$R \leq 1 - \tau.$$

On the other hand, for any given small $\epsilon > 0$, *with high probability a random rank-metric code of rate* R *and ratio* $\rho = \frac{n}{m} = O(\epsilon)$ *in* $\mathbb{F}_q^{n\times m}$ *is* $(\tau n, O(1/\epsilon))^R$*-list decodable if the* $R = 1 - \tau - \epsilon$.

3.3 Random Subcodes of Gabidulin Codes

In this section, we study the list decodability of random subcodes of Gabidulin codes. In particular, we show that random subcodes of Gabidulin codes can be list decoded beyond the unique decoding radius. From now on, R and ρ denotes the rate k/n and ratio n/m for the Gabidulin code $\mathcal{G}_k(n, m, q)$, respectively. Furthermore, we use r to denote the rate of a subcode of the Gabidulin code $\mathcal{G}_k(n, m, q)$.

In the rest of this section, we discuss list decoding radius of a random subcode of the Gabidulin code $\mathcal{G}_k(n, m, q)$ depending on its rate regime, i.e., $(i) R - \rho R(1 - R) \leq r < R$; or $(ii) 0 < r < R - \rho R(1 - R)$.

3.3.1 Case 1. $R - \rho R(1 - R) \leq r < R$

In this section, we consider lower bounds on the list decoding radius, when $R - \rho R(1 - R) \leq r < R$. Theorems 3 and 4 are our main results. To reach the results, we first bound the list size for Gabidulin codes in the Lemma 6.

Lemma 6. *(see in [63]) Let the Gabidulin code* $\mathcal{G}_k(n, m, q)$ *over* $\mathbb{F}_{q^m}$ *with* $n \leq m$ *and* $d_R = n - k + 1$ *be given. Let* $\tau n \leq 1 - R$. *Then, for any word* $\mathbf{v} \in \mathbb{F}_{q^m}^n$, *the maximum list size* $\mathcal{L}$ *is bounded by*

$$\mathcal{L} \;=\; \max_{\mathbf{v}\in\mathbb{F}_{q^m}^n} |\mathcal{B}_R(\mathbf{v}, \tau n) \cap \mathcal{G}_k(n, m, q)| \leq q^{(2\tau n - d)(n - \frac{d}{2}) + O(n)}.$$

In the following, we use the upper bound to establish an estimation on the list size of a random subcode of a Gabidulin code.

Theorem 3. *Let $\rho = \frac{n}{m}$ be a constant. Consider a Gabidulin code $\mathcal{G}_k(n, m, q)$ of rate R. For every $0 < \epsilon < 1$, when r and R satisfy $R - \rho R(1 - R) \leq r < R$, we define the list decoding radius*

$$\tau = \frac{R - r}{\rho(1 + R)} + \frac{1 - R}{2} - \epsilon. \tag{3.1}$$

Then, with a probability at least $1 - q^{-\Omega(mn)}$, a subcode $\mathcal{C}$ of the Gabidulin code $\mathcal{G}_k(n, m, q)$ of rate r is $(\tau n, O(1/\epsilon))^R$-list decodable for sufficiently large n and m.

Proof. First of all, combining equation (3.1) with the assumption $r \geq R - \rho R(1 - R)$, we can obtain

$$\begin{aligned} \tau &\leq \frac{\rho R(1 - R)}{\rho(1 + R)} + \frac{1 - R}{2} - \epsilon \\ &= \left(\frac{R}{1 + R} + \frac{1}{2}\right)(1 - R) - \epsilon < 1 - R. \end{aligned}$$

Let $\mathcal{L} + 1 = \frac{1}{\rho(1+R)\epsilon}$. The subcode $\mathcal{C}$ of size q^{rmn} is selected uniformly at random from a Gabidulin code $\mathcal{G}_k(n, m, q)$. Given a vector $\mathbf{v} \in \mathbb{F}_{q^m}^n$, by Lemma 6, we bound the probability that one codeword $c \in \mathcal{C}$ is contained in $\mathcal{B}_R(\mathbf{v}, \tau) \cap \mathcal{G}_k(n, m, q)$.

$$\begin{aligned} \Pr[c \in \mathcal{B}_R(\mathbf{v}, \tau n) \cap \mathcal{G}_k(n, m, q)] &= \frac{|\mathcal{B}_R(\mathbf{v}, \tau n) \cap \mathcal{G}_k(n, m, q)|}{|\mathcal{G}_k(n, m, q)|} \\ &\leq q^{(2\tau n - d)(n - \frac{d}{2}) - Rmn + O(n)}. \end{aligned} \tag{3.2}$$

If $\mathcal{C}$ is not $(\tau n, \mathcal{L})^R$-list decodable, there exists a vector $\mathbf{v} \in \mathbb{F}_{q^m}^n$ and a subset $S \subseteq \mathcal{C}$ with $|S| = \mathcal{L} + 1$ such that $S \subseteq \mathcal{B}_R(\mathbf{v}, \tau n) \cap \mathcal{G}_k(n, m, q)$. For a given vector $\mathbf{v} \in \mathbb{F}_{q^m}^n$ and the corresponding S, let $E_{\mathbf{v},S}$ denote the event that all codewords c in S is in $\mathcal{B}_R(\mathbf{v}, \tau n) \cap$

$\mathcal{G}_k(n,m,q)$. By Equation (3.2), we have

$$\begin{aligned}\Pr[E_{\mathbf{v},S}] &\leq \left(\frac{|\mathcal{B}_R(\mathbf{v},\tau n)\cap\mathcal{G}_k(n,m,q)|}{|\mathcal{G}_k(n,m,q)|}\right)^{\mathcal{L}+1}\\ &\leq q^{((2\tau n-d)(n-\frac{d}{2})-Rmn+O(n))(\mathcal{L}+1)}.\end{aligned}$$

Taking the union bound over all q^{mn} choices for $\mathbf{v}$ and S over any $(\mathcal{L}+1)$-subsets of $\mathcal{C}$, we have

$$\begin{aligned}\sum_{\mathbf{v},S}\Pr[E_{\mathbf{v},S}] &\leq q^{[(2\tau n-d)(n-\frac{d}{2})-Rmn+O(n)](\mathcal{L}+1)}q^{mn}\binom{|\mathcal{C}|}{\mathcal{L}+1}\\ &\leq q^{[(2\tau n-d)(n-\frac{d}{2})-Rmn+O(n)](\mathcal{L}+1)}q^{mn}|\mathcal{C}|^{\mathcal{L}+1}\\ &= q^{[(2\tau n-d)(n-\frac{d}{2})-Rmn+O(n)](\mathcal{L}+1)+mn+rmn(\mathcal{L}+1)}\\ &\leq q^{(\mathcal{L}+1)mn[\frac{\rho}{2}(2\tau-1+R)(1+R)-R+r+\frac{1}{\mathcal{L}+1}+O(\frac{1}{m})]}\\ &\leq q^{(\mathcal{L}+1)mn(-\epsilon)} \qquad (3.3)\\ &= q^{-\Omega(mn)}. \qquad (3.4)\end{aligned}$$

The inequality 3.3 holds since

$$\begin{aligned}\tau &\leq \frac{1-R}{2}+\frac{(R-r)}{\rho(1+R)}-\epsilon\\ &= \frac{1-R}{2}+\frac{(R-r)}{\rho(1+R)}-\frac{1}{\rho(1+R)(\mathcal{L}+1)}.\end{aligned}$$

Thus, a subcode $\mathcal{C}$ of the Gabidulin code $\mathcal{G}_k(n,m,q)$ with rate r is not $(\tau n, O(1/\epsilon))^R$-list decodable with an exponentially small probability. ■

Remark 7. When the ratio $\rho = \frac{n}{m} = 1$, we call Gabidulin codes as square Gabidulin codes, which have received a lot of interest [63]. In this case, the list decoding radius τ is monotonously increasing for $r \geq R - \rho R(1-R) = R^2$ in (3.1). Thus, for any r, the

decoding radius τ attains the maximal possible value when $R = \sqrt{r}$:

$$\tau = \frac{\sqrt{r} - r}{1 + \sqrt{r}} + \frac{1 - \sqrt{r}}{2} = \left(\frac{\sqrt{r}}{1 + \sqrt{r}} + \frac{1}{2} \right) (1 - \sqrt{r}) - \epsilon. \tag{3.5}$$

In [54], it is shown that it is impossible for a square Gabidulin code with parameters $[12, 6, 7]$ to be list decoded beyond the unique decoding radius $\frac{1-r}{2}$. Note that omitting the ϵ in Equation (3.5), considering a subcode of a square Gabidulin code enables the list decoding radius to be bigger than the unique decoding bound in Table 3.1. However, it is also easy to verify that the bound given is still worse than the Gilbert-Varshamov bound $1 - \sqrt{r}$.

Table 3.1: Square Gabidulin codes vs. subcodes of square Gabidulin codes

Codes	Decoding radius τ	List size $\mathcal{L}$
Square Gabidulin codes [54]	$\frac{1-r}{2}$	1
Subcodes of square Gabidulin codes	$> \frac{1-r}{2}$	$O(1/\epsilon)$

Inspired by the work of V. Guruswami et al. [19], we consider list decodability of random linear subcodes of Gabidulin codes. We prove that by replacing random subcodes with random linear subcodes, the list size grows to $\exp(O(1/\epsilon))$.

Theorem 4. *Let the ratio $\rho = \frac{n}{m}$ be a constant. Consider a Gabidulin code $\mathcal{G}_k(n, m, q)$ of rate R. Then, for $R - \rho R(1 - R) \leq r < R$ and every $0 < \epsilon < 1$ and τ given in* (3.1)*, with a probability at least $1 - q^{-\Omega(mn)}$ an $\mathbb{F}_q$-linear subcode $\mathcal{C}_q$ of the Gabidulin code $\mathcal{G}_k(n, m, q)$ of rate r is $(\tau n, \exp(O(1/\epsilon)))^R$-list decodable with rate r for sufficiently large n and m.*

Proof. Let $\log_q(\mathcal{L} + 1) = \frac{1}{\rho(1+R)\epsilon}$. Then the list size $\mathcal{L} + 1 = \exp(O(1/\epsilon))$.

Given a Gabidulin code $\mathcal{G}_k(n, m, q)$, we select rmn $\mathbb{F}_q$-linear independent codewords uniformly at random from $\mathcal{G}_k(n, m, q)$. The linear subcode $\mathcal{C}_q$ of the Gabidulin code $\mathcal{G}_k(n, m, q)$

spanned by these codewords has rate r. Moreover, any $\mathbb{F}_q$-linear independent codewords in $\mathcal{C}_q$ are selected uniformly at random, i.e., they are chosen to be mutually independent. If a random linear subcode $\mathcal{C}_q$ is not $(\tau n, \mathcal{L})^R$-list decodable, there exists a vector $\mathbf{v} \in \mathbb{F}_{q^m}^n$ and a subset $S \subseteq \mathcal{C}_q$ with $|S| = \mathcal{L} + 1$ such that $S \subseteq \mathcal{B}_R(\mathbf{v}, \tau n) \cap \mathcal{G}_k(n, m, q)$. There are $\mathcal{L}' = \lceil \log_q(\mathcal{L} + 1) \rceil$ codewords in S, which are $\mathbb{F}_q$-linear independent and selected to be mutually independent. Let S' be the $\mathbb{F}_q$-linear span of these $\mathcal{L}'$ codewords. Thus, $S \subseteq S$. Let notations be the same as in Theorem 3. Then

$$\begin{aligned} \Pr[E_{\mathbf{v},S}] \leq \Pr[E_{\mathbf{v},S'}] &\leq \left(\frac{|\mathcal{B}_R(\mathbf{v}, \tau n) \cap \mathcal{G}_k(n, m, q)|}{|\mathcal{G}_k(n, m, q)|} \right)^{\mathcal{L}'} \\ &\leq q^{((2\tau n - d)(n - \frac{d}{2}) - Rmn + O(n))(\mathcal{L}')}. \end{aligned}$$

Taking the union bound over all q^{mn} choices for $\mathbf{v}$ and S' over any $\mathcal{L}'$-dimensional $\mathbb{F}_q$-linear subspaces of $\mathcal{C}$, we have

$$\begin{aligned} \sum_{\mathbf{v},S'} \Pr[E_{\mathbf{v},S'}] &\leq q^{\lfloor (2\tau n - d)(n - \frac{d}{2}) - Rmn + O(n) \rfloor \cdot \mathcal{L}'} q^{mn} \binom{|\mathcal{C}|}{\mathcal{L}'} \\ &\leq q^{\mathcal{L}' mn \lfloor \frac{\rho}{2}(2\tau - 1 + R)(1 + R) - R + r + \frac{1}{\mathcal{L}'} + O(\frac{1}{m}) \rfloor \rfloor} \\ &\leq q^{\log_q(\mathcal{L}+1) mn \lfloor \frac{\rho}{2}(2\tau - 1 + R)(1 + R) - R + r + \frac{1}{\log_q(\mathcal{L}+1)} + O(\frac{1}{m}) \rfloor} \\ &\leq q^{\log_q(\mathcal{L}+1) mn(-\epsilon)} \\ &= q^{-\Omega(mn)}. \end{aligned}$$

So, an $\mathbb{F}_q$-linear subcode of the Gabidulin code is not $(\tau n, \exp(O(1/\epsilon)))^R$-list decodable with an exponentially small probability. ■

3.3.2 Case 2. $0 < r < R - \rho R(1 - R)$

In this subsection, we show that if, $r < R - \rho R(1 - R)$, most subcodes and linear subcodes of Gabidulin codes with rate r and decoding radius τ meet the asymptotic Gilbert-Varshamov bound.

Lemma 7. *Let the Gabidulin code $\mathcal{G}_k(n, m, q)$ with $n \leq m$ and $d_R = n - k + 1$ be given. Let $\tau \geq 1 - R$. Then, for any word $\mathbf{v} \in \mathbb{F}_{q^m}^n$, we have*

$$|\mathcal{B}_R(\mathbf{v}, \tau n)| \leq \begin{bmatrix} n \\ n - \tau n \end{bmatrix}_q q^{m(k-n+\tau n)}.$$

Proof. Consider a Gabidulin code $\mathcal{G}_k(n, m, q)$ with the $\mathbb{F}_q$-linearly independent elements $\alpha_1, \cdots, \alpha_n \in \mathbb{F}_{q^m}$.

Then for any $\mathbf{v} = (v_1, \cdots, v_n) \in \mathbb{F}_{q^m}^n$ and a codeword $\mathbf{c} = (f(\alpha_1), \cdots, f(\alpha_n)) \in \mathcal{G}_k(n, m, q)$, we have $\mathbf{c} \in \mathcal{B}_R(\mathbf{v}, \tau n)$ if

$$\mathrm{rank}_{\mathbb{F}_q}(f(\alpha_1) - v_1, f(\alpha_2) - v_2, \ldots, f(\alpha_n) - v_n) \leq \tau n.$$

Now suppose that $w_i = f(\alpha_i) - v_i$ for $i = 1, \cdots, n$ and $\mathcal{M} = (w_1, \cdots, w_n)$. By the assumption that $\mathrm{rank}_{\mathbb{F}_q}(\mathcal{M}) \leq \tau n$, there is an $(n - \tau n)$-dimension subspace Λ of $\mathbb{F}_q^n$ as the null space of $\mathcal{M}$ with basis $\{\lambda_1, \cdots, \lambda_{n-\tau n}\}$. By definition, the number of choices of such Λ is at most $\begin{bmatrix} n \\ n-\tau n \end{bmatrix}_q$.

Fix Λ with basis $(\lambda_1, \cdots, \lambda_{n-\tau n})$. Denote $\lambda_j = (\lambda_{j,1}, \cdots, \lambda_{j,n})$. We can then obtain that $f(x)$ satisfies the following requirements

$$f\left(\sum_{l=1}^{n} \lambda_{j,l}\alpha_l\right) = \sum_{l=1}^{n} \lambda_{j,l} v_l, \quad j = 1, \ldots, n - \tau n.$$

Hence, the list of codewords inside the rank-metric ball $\mathcal{B}_R(\mathbf{v}, \tau n)$ is determined by the number of q-linearized polynomials f that maps the $(n - \tau n)$-dimensional space Λ to the images determined above. Due to the q-degree of f being at most $k - 1$, there are at most $q^{m(k-n+\tau n)}$ such f. This in turns bounds the number of possible codewords in $\mathcal{B}_R(\mathbf{v}, \tau n)$ from above by $\begin{bmatrix} n \\ n-\tau n \end{bmatrix}_q q^{m(k-n+\tau n)}$. ■

Based on the Lemma 7 above, we can estimate the list size of a random subcode of a Gabidulin code, when the list decoding radius is larger than $1 - R$.

Theorem 5. *Let $\rho = \frac{n}{m}$ be a constant. Consider a Gabidulin code $\mathcal{G}_k(n, m, q)$ of rate R. For $0 < r < R - \rho R(1 - R)$ and every sufficiently small $\epsilon > 0$, if r satisfies*

$$r = (1 - \tau)(1 - \rho\tau) - \epsilon, \tag{3.6}$$

then with a probability at least $1 - q^{-\Omega(mn)}$, a subcode $\mathcal{C}$ of the Gabidulin code $\mathcal{G}_k(n, m, q)$ of rate r is $(\tau n, O(1/\epsilon))^R$-list decodable for sufficiently large n and m.

Proof. Let ϵ be chosen such that $\epsilon < R - \rho R(1 - R) - r$. Such ϵ exists since we assumed that $r < R - \rho R(1 - R)$.

Claim 1. $\tau > 1 - R$.

Proof. Suppose otherwise; $\tau \leq 1 - R$. Then equation (3.6) gives us that

$$\begin{aligned} r &\geq R(1 - \rho(1 - R)) - \epsilon \\ &= R - \rho R(1 - R) - \epsilon > r \end{aligned}$$

which results in a contradiction. ■

Let $\mathcal{L} + 1 = \frac{1}{\epsilon}$. We select a subcode $\mathcal{C}$ with size $|\mathcal{C}| = q^{rmn}$ uniformly at random from a Gabidulin code $\mathcal{G}_k(n, m, q)$. If $\mathcal{C}$ is not $(\tau n, \mathcal{L})^R$-list decodable, there exists a vector $\mathbf{v} \in \mathbb{F}_{q^m}^n$ and a subset $S \subseteq \mathcal{C}$ with $|S| = \mathcal{L} + 1$ such that $S \subseteq \mathcal{B}_R(\mathbf{v}, \tau n) \cap \mathcal{G}_k(n, m, q)$. For a given vector $\mathbf{v} \in \mathbb{F}_{q^m}^n$ and the corresponding S, let $E_{\mathbf{v},S}$ denote the event that all codewords c in S is in $\mathcal{B}_R(\mathbf{v}, \tau n) \cap \mathcal{G}_k(n, m, q)$. This probability of $E_{\mathbf{v},S}$ is upper bounded by Lemma 7, we have

$$\begin{aligned} \Pr[E_{\mathbf{v},S}] &\leq \left(\frac{|\mathcal{B}_R(\mathbf{v}, \tau n) \cap \mathcal{G}_k(n, m, q)|}{|\mathcal{G}_k(n, m, q)|} \right)^{\mathcal{L}+1} \\ &\leq \left(\begin{bmatrix} n \\ n - \tau n \end{bmatrix}_q q^{m(k-n+\tau n)} q^{-km} \right)^{\mathcal{L}+1} \\ &\leq q^{n(\tau n - \tau^2 n + \tau m - m)(\mathcal{L}+1)}. \end{aligned}$$

We take the union bound over all $\mathbf{v} \in \mathbb{F}_{q^m}^n$ and S over any $(\mathcal{L}+1)$-subsets of $\mathcal{C}$. It follows that

$$\begin{aligned}
\sum_{\mathbf{v},S} \Pr[E_{\mathbf{v},S}] &\leq q^{n(\tau n - \tau^2 n + \tau m - m)(\mathcal{L}+1)} q^{mn} \binom{|\mathcal{C}|}{\mathcal{L}+1} \\
&\leq q^{n(\tau n - \tau^2 n + \tau m - m)(\mathcal{L}+1)} q^{mn} q^{rmn(\mathcal{L}+1)} \\
&\leq q^{(\mathcal{L}+1)mn(-\epsilon)} \\
&= q^{-mn}.
\end{aligned}$$

Using the fact that $r = (1-\tau)(1-\rho\tau)-\epsilon$, when $\tau \geq 1-R$, the probability that a random rate r subcode $\mathcal{C}$ of $\mathcal{G}_k(n,m,q)$ is not $(\tau n, O(1/\epsilon))^R$-list decodable with an exponentially small probability. ■

Remark 8. Theorem 5 reveals that random subcodes of Gabidulin codes can be list decoded up to the Gilbert-Varshamov bound with polynomial list size, when $r < R - \rho R(1-R)$. In particular, random subcodes of square Gabidulin codes can be list decoded up to the Gilbert-Varshamov bound $\tau = 1 - \sqrt{r}$ when $r \leq R^2$, while Gabidulin codes can be list decoded only up to the unique decoding radius $\frac{1-R}{2}$.

Taking a special case $\rho = O(\epsilon)$, Theorem 5 implies the following Singleton Bound.

Corollary 2. *If the ratio $\rho = \frac{n}{m} = \epsilon$, then the decoding radius of a random subcode $\mathcal{C}$ with rate r of a Gabidulin code is $((1-r-2\epsilon)n, O(1/\epsilon))^R$-list decodable.*

Proof. By (3.6), we have

$$r = (1-\tau)(1-\epsilon\tau) - \epsilon \geq 1 - \tau - \epsilon\tau(1-\tau) - \epsilon \geq 1 - \tau - 2\epsilon.$$

■

Compared to the result in [26] , we would like to emphasize that the result above confirms the existence of a subcode of Gabidulin codes with a larger ratio ρ; $\rho = O(\epsilon)$ instead of the $O(\epsilon^2)$ considered in the previous result in Table 3.2.

Table 3.2: Bigger ratio $\rho = O(\epsilon)$ vs. $\rho = O(\epsilon^2)$

Codes	Ratio $\boldsymbol{\rho}$	Decoding radius $\boldsymbol{\tau}$	List size $\mathcal{L}$
Guruswami, Wang & Xing's subcodes of Gabidulin codes [26]	$O(\epsilon^2)$	Singleton bound	$\exp(O(1/\epsilon))$
Subcodes of Gabidulin codes	$O(\epsilon)$	Singleton bound	$O(1/\epsilon)$

We can obtain an analogous result for random linear subcodes of Gabidulin codes in this scenario using similar approach to the proofs of Theorem 4 and 5.

Theorem 6. *Let $\rho = \frac{n}{m}$ be a constant. Consider a Gabidulin code $\mathcal{G}_k(n, m, q)$ of rate R. For $0 < r < R - \rho R(1-R)$ and every sufficiently small $\epsilon > 0$, if τ satisfies* (3.6)*, then with a probability at least $1 - q^{-\Omega(mn)}$, a linear subcode $\mathcal{C}_q$ of the Gabidulin code $\mathcal{G}_k(n, m, q)$ of rate r is $(\tau n, \exp(O(1/\epsilon)))^R$-list decodable for sufficiently large n and m.*

3.4 $\mathbb{F}_{q^m}$-Linear Subcodes of Gabidulin Codes

It is common to view a rank-metric code $\mathcal{C}$ as a subset of $\mathbb{F}_{q^m}^n$ and then insist that such a code to be $\mathbb{F}_{q^m}$-linear. A natural question is if a random $\mathbb{F}_{q^m}$-linear subspace $\mathcal{C}_{q^m} \subseteq \mathbb{F}_{q^m}^n$ is rank-metric list decodable. In this section, we focus on the list decoding of random $\mathbb{F}_{q^m}$-linear subcodes of Gabidulin codes.

Let $\mathcal{G}_k(n, m, q)$ be a Gabidulin code over $\mathbb{F}_{q^m}$ with the generator matrix $G \in \mathbb{F}_{q^m}^{k \times n}$. Further, let the code $\mathcal{C}_{q^m}$ be an $\mathbb{F}_{q^m}$-linear subcode of Gabidulin codes with dimension k'. Then, up to the reordering of the codewords elements, we can express $\mathcal{C}_{q^m}$ from its generator matrix which can be presented as

$$\mathcal{C}_{q^m} = \{\mathbf{v} \cdot [I_{k'}|X] \cdot G | \mathbf{v} \in \mathbb{F}_{q^m}^{k'}, X \in \mathbb{F}_{q^m}^{k' \times (k-k')}\}.$$

We recall that $\mathcal{G}_k(n, m, q)$, a Gabidulin code of length n and dimension k over $\mathbb{F}_{q^m}$, consists of evaluations of q-degree $k-1$ linearized polynomials $f(x)$. That is, $\mathcal{G}_k(n, m, q)$

can be identified with the set of all $k-1$ q-degree linearized polynomials over $\mathbb{F}_{q^m}$,

$$\mathcal{G}_k(n,m,q) := \left\{ \sum_{i=0}^{k-1} f_i x^{q^i} \,\middle|\, f_i \in \mathbb{F}_{q^m} \right\}.$$

Let $X = (x_{i,j})_{i=0,\cdots,k'-1;j=0,\cdots,k-k'-1}$ be such that $[I_{k'}|X] \cdot G$ is a generator matrix of the code $\mathcal{C}_{q^m}$ after reordering. Then

$$\mathcal{C}_{q^m} = \left\{ \sum_{i=0}^{k'-1} f_i x^{q^i} \,\middle|\, f_0, \cdots, f_{k'-1} \in \mathbb{F}_{q^m}, f_\ell = \sum_{j=0}^{k'-1} x_{j,\ell-k'} f_j,\ k' \le \ell \le k-1 \right\}.$$

Remark 9. Let $\mathcal{C}_{q^m}$ be an $\mathbb{F}_{q^m}$-linear subcode of Gabidulin code and a codeword $c \in \mathcal{C}_{q^m}$. Then, we have the following conditional probability

$$\begin{aligned}
& Pr(c \in \mathcal{C}_{q^m} | c \in \mathcal{B}_R(v, \tau n) \cap \mathcal{G}_k(n,m,q)) \\
= \;& Pr\left(f_\ell = \sum_{j=0}^{k'-1} x_{j,\ell-k'} f_j,\ k' \le \ell \le k-1 \right) \\
= \;& \prod_{\ell=k'}^{k-1} Pr\left(f_\ell = \sum_{j=0}^{k'-1} x_{j,\ell-k'} f_j \right) \\
= \;& \left(\frac{1}{q^m} \right)^{k-k'}.
\end{aligned}$$

3.4.1 Case 1. $R - \frac{\rho}{2}R(1-R) \le r < R$

By using the upper bound from Lemma 6 to estimate the list size of an $\mathbb{F}_{q^m}$-linear subcode of a Gabidulin code in the case $R - \frac{\rho}{2}R(1-R) \le r < R$, we have the following result.

Theorem 7. *Let the ratio $\rho = \frac{n}{m}$ be a constant and $\mathcal{G}_k(n,m,q)$ be a Gabidulin code of rate R with $R - \frac{\rho}{2}R(1-R) \le r < R$. For every $0 < \epsilon < 1$, in the case $R - \frac{\rho}{2}R(1-R) \le r < R$, we define the list decoding radius*

$$\tau = \frac{2(R-r)}{\rho(1+R)} + \frac{1-R}{2} - \epsilon.$$

Then, with a high probability at least $1 - q^{-\Omega(mn)}$*, an* $\mathbb{F}_{q^m}$*-linear subcode* $\mathcal{C}_{q^m}$ *of the Gabidulin code* $\mathcal{G}_k(n, m, q)$ *is* $(\tau n, \exp(O(1/\epsilon)))^R$*-list decodable for sufficiently large* n *and* m *and information rate* r*.*

Proof. Let $\log_{q^m}(\mathcal{L}+1) = \frac{1}{\rho(1+R)\epsilon}$. Then the list size is $\mathcal{L}+1 = \exp(O(1/\epsilon))$.

We select rmn $\mathbb{F}_{q^m}$-linearly independent codewords uniformly at random from a given Gabidulin code $\mathcal{G}_k(n, m, q)$. The $\mathbb{F}_{q^m}$-linear subcode $\mathcal{C}_{q^m}$ of size q^{rmn} is selected uniformly at random from a Gabidulin code $\mathcal{G}_k(n, m, q)$. The $\mathbb{F}_{q^m}$-linear subcode $\mathcal{C}_{q^m}$ of the Gabidulin code $\mathcal{G}_k(n, m, q)$ spanned by these codewords have rate r. Any $\mathbb{F}_{q^m}$-linear independent codewords in $\mathcal{C}_{q^m}$ are selected uniformly at random.

Given a vector $\mathbf{v} \in \mathbb{F}_{q^m}^n$, by Lemma 6 we estimate the probability that one codeword $c \in \mathcal{C}_{q^m}$ is contained in $\mathcal{B}_R(\mathbf{v}, \tau n) \cap \mathcal{C}_{q^m}$,

$$\begin{aligned}
& Pr[c \in \mathcal{B}_R(\mathbf{v}, \tau n) \cap \mathcal{C}_{q^m}] \\
= \;& Pr[c \in \mathcal{C}_{q^m} \cap \mathcal{B}_R(\mathbf{v}, \tau n) \cap \mathcal{G}_k(n, m, q)] \\
= \;& Pr[c \in \mathcal{C}_{q^m} | c \in \mathcal{B}_R(\mathbf{v}, \tau n) \cap \mathcal{G}_k(n, m, q)] \cdot Pr[c \in \mathcal{B}_R(\mathbf{v}, \tau n) \cap \mathcal{G}_k(n, m, q)] \\
= \;& \left(\frac{1}{q^m}\right)^{k-k'} \cdot \frac{|\mathcal{B}_R(\mathbf{v}, \tau n) \cap \mathcal{G}_k(n, m, q)|}{|\mathcal{G}_k(n, m, q)|} \\
\leq \;& q^{m(k'-k)+(2\tau n-d)(n-\frac{d}{2})-Rmn+O(n)}. \qquad (3.7)
\end{aligned}$$

If $\mathcal{C}_{q^m}$ is not $(\tau n, \mathcal{L})^R$-list decodable implies the existence of $\mathbf{v} \in \mathbb{F}_{q^m}^n$ and $S \subseteq \mathcal{C}_{q^m}$ such that $|S| = \mathcal{L}+1$ and any content of S is at most τn away from $\mathbf{v}$. By Pigeonhole Principle, the maximum possible size of a set containing $\mathbb{F}_{q^m}$-linearly independent elements of S is at least $\mathcal{L}' := \lceil \log_{q^m}(\mathcal{L}+1) \rceil$. Let S' be the space spanned by such $\mathcal{L}'$ codewords. It is apparent that $S \subseteq S'$. Then, by Equation 3.7, we have

$$\begin{aligned}
Pr[E_{\mathbf{v},S}] \;&\leq\; Pr[E_{\mathbf{v},S'}] \\
&\leq\; \left(\left(\frac{1}{q^m}\right)^{k-k'} \frac{|\mathcal{B}_R(\mathbf{v}, \tau n) \cap \mathcal{G}_k(n, m, q)|}{|\mathcal{G}_k(n, m, q)|}\right)^{\mathcal{L}'} \\
&\leq\; q^{(m(k'-k)+(2\tau n-d)(n-\frac{d}{2})-Rmn+O(n))\mathcal{L}'}.
\end{aligned}$$

Noting that $\mathbf{v}$ can be one of any q^{mn} elements of $\mathbb{F}_{q^m}^n$ while S' can be selected among all possible $\mathcal{L}'$-dimensional $\mathbb{F}_{q^m}$-linear subspaces of $\mathcal{C}_{q^m}$, we can use union bound to estimate the total probability to be

$$\begin{aligned}
\sum_{\mathbf{v},S'} Pr[E_{\mathbf{v},S'}] &\leq q^{(m(k'-k)+(2\tau n-d)(n-\frac{d}{2})-Rmn+O(n))\mathcal{L}'} q^{mn} \binom{|\mathcal{C}_{q^m}|}{\mathcal{L}'} \\
&\leq q^{(m(k'-k)+(2\tau n-d)(n-\frac{d}{2})-Rmn+O(n))\mathcal{L}'+mn+rmn\mathcal{L}'} \\
&\leq q^{\mathcal{L}'mn[\frac{k'-k}{n}+\frac{\rho}{2}(2\tau-1+R)(1+R)-R+r+\frac{1}{\mathcal{L}'}+O(\frac{1}{m})]} \\
&\leq q^{\mathcal{L}'mn(-\epsilon)} \qquad (3.8) \\
&= q^{-\Omega(mn)}.
\end{aligned}$$

The last inequality confirms our claim that the probability for an $\mathbb{F}_{q^m}$-linear subcode $\mathcal{C}_{q^m}$ of $\mathcal{G}_k(n,m,q)$ of rate r not to be $(\tau n, \exp(O(1/\epsilon)))^R$-list decodable with an exponentially small probability. ■

3.4.2 Case 2. $0 < r < R - \frac{\rho}{2}R(1-R)$

Based on Lemma 7 and similar arguments in Theorem 7, in the case $0 < r < R - \frac{\rho}{2}R(1-R)$ we can provide a bound on the decoding radius for $\mathbb{F}_{q^m}$-linear subcodes of Gabidulin codes.

Theorem 8. *Let the ratio $\rho = \frac{n}{m}$ be a constant and $\mathcal{G}_k(n,m,q)$ be a Gabidulin code of rate R. For every $0 < \epsilon < 1$, in the case $0 < r < R - \frac{\rho}{2}R(1-R)$, if information rate r and list decoding radius τ satisfy*

$$r = \frac{(1-\tau)(1-\rho\tau)+R}{2} - \epsilon.$$

Then, with a probability at least $1 - q^{-\Omega(mn)}$, an $\mathbb{F}_{q^m}$-linear subcode $\mathcal{C}_{q^m}$ of the Gabidulin code $\mathcal{G}_k(n,m,q)$ of rate r is $(\tau n, \exp(O(1/\epsilon)))^R$-list decodable for sufficiently large n and m.

3.5 Conclusion

In this chapter, we investigated the list decodability of subcodes of Gabidulin codes. We discovered that random subcodes and linear subcodes of Gabidulin codes can be list decoded beyond the unique decoding radius in Table 3.3 and Table 3.4. Our results reveal that list decodability of subcodes depends on the ratio $\rho = \frac{n}{m}$ and its rate. More precisely speaking, for $0 < r < R - \rho R(1-R)$, random subcodes of Gabidulin codes can be list decoded up to the Gilbert-Varshamov bound; while for $R - \rho R(1-R) \leq r < R$, list decodability of subcodes of Gabidulin codes is worse than the former case, but is still beyond the half of the minimum distance. For $\mathbb{F}_{q^m}$-linear cases, subcodes of Gabidulin codes can be list decoded with list decoding radius beyond the unique decoding radius, but the lists size are exponential.

Table 3.3: List decoding of ($\mathbb{F}_q$-linear) subcodes of Gabidulin codes

	$r \in [R\text{-}\rho R(1\text{-}R), R)$		$r \in (0, R\text{-}\rho R(1\text{-}R))$	
Random codes	Decoding radius τ	List size $\mathcal{L}$	Decoding radius τ	List size $\mathcal{L}$
Subcodes of Gabidulin codes	$> \frac{1\text{-}r}{2}$	$O(1/\epsilon)$	GV-bound	$O(1/\epsilon)$
$\mathbb{F}_q$-linear subcodes of Gabidulin codes	$> \frac{1\text{-}r}{2}$	$\exp(O(1/\epsilon))$	GV-bound	$\exp(O(1/\epsilon))$

Table 3.4: List decoding of $\mathbb{F}_{q^m}$-linear subcodes of Gabidulin codes

	$r \in [R\text{-}\frac{\rho}{2}R(1\text{-}R), R)$		$r \in (0, R\text{-}\frac{\rho}{2}R(1\text{-}R))$	
Random codes	Decoding radius τ	List size $\mathcal{L}$	Decoding radius τ	List size $\mathcal{L}$
$\mathbb{F}_{q^m}$-linear subcodes of Gabidulin codes	$> \frac{1\text{-}r}{2}$	$\exp(O(1/\epsilon))$	$> \frac{1\text{-}r}{2}$	$\exp(O(1/\epsilon))$

In particular, when $\rho = O(\epsilon)$, the list decoding radius can achieve the Singleton bound. Due to this promising result, we believe that subcodes of Gabidulin codes can be used as a

very good source in our attempt to find rank-metric codes with large list decoding radius.

There are some future research directions that we believe can be interesting to consider. Firstly, the existence of subcode of Gabidulin code with large decoding radius is only shown without actually constructing it. It may be interesting to explicitly construct such codes along with their efficient list decoding algorithms. Secondly, although the list decoding radius can be made to be far beyond half of the minimum distance, the result on linear subcode of Gabidulin codes that we have are still with exponential list size. A natural improvement is then to decrease this list size while keeping the radius to be beyond the unique decoding radius.

Chapter 4

On the List Decodability of Linear Self-orthogonal Rank-metric Codes

This chapter is based on the work in [37]. In [20], V. Guruswami and N. Resch proved that a random $\mathbb{F}_q$-linear rank-metric code is list decodable with list decoding radius attaining the Gilbert-Varshamov bound. On the other hand, in Hamming metric, random linear self-orthogonal codes can be list decoded to the Gilbert-Varshamov bound with polynomial list size [30]. Because of the potential applications of linear self-orthogonal rank-metric codes in network coding and cryptography [60], [51] and [16], we focus on investigating their list decodability.

In this chapter, we prove that with high probability, an $\mathbb{F}_q$-linear self-orthogonal rank-metric code over $\mathbb{F}_q^{n\times m}$ of rate $R = (1-\tau)(1-\frac{n}{m}\tau) - \epsilon$ is list decodable up to fractional radius $\tau \in (0,1)$ and small $\epsilon \in (0,1)$ with list size $O(1/\epsilon)$. In addition, we show that an $\mathbb{F}_{q^m}$-linear self-orthogonal rank-metric code of rate up to the Gilbert-Varshamov bound is $(\tau n, \exp(O(\frac{1}{\epsilon})))^R$-list decodable. In the future research, it is interesting to consider decreasing the list size of $\mathbb{F}_{q^m}$-linear case.

4.1 Introduction

In the late 50's, P. Elias [11] and J. M. Wozencraft [66] independently introduced list decoding. Compared with unique decoding, list decoding can output a list of codewords which contains the correct transmitted codeword rather than output a unique codeword. Consequentially, the list size of list decoding can be bigger than 1 and list decoding radius can be beyond unique decoding barrier.

The goal of list decoding is to determine the optimal trade-offs between the information rate, list decoding radius and list size. As we mentioned in Chapter 1, we want the information rate and list decoding radius to be large. On the contrary, a very large list size is undesirable.

There have been some interesting findings on the list decodability for random $\mathbb{F}_q$-linear rank-metric codes [20] and [45]. An interesting direction is to see whether this new result can be applied to improve results on specific $\mathbb{F}_q$-linear rank-metric codes. Due to its potential application in many fields, the specific $\mathbb{F}_q$-linear rank-metric codes that we are interested in is the $\mathbb{F}_q$-linear self-orthogonal rank-metric codes. A natural question that follows is whether a random $\mathbb{F}_q$-linear self-orthogonal rank-metric codes still can be list decoded up to the Gilbert-Varshamov bound with polynomial list size. Moreover, based on $\mathbb{F}_q$-linear case, we investigate how well one can list decode random $\mathbb{F}_{q^m}$-linear self-orthogonal rank-metric codes.

This chapter is organized as follows. Firstly, we give some definitions and notations about linear self-orthogonal rank-metric codes and quadratic form. Then, we describe how to construct $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$-linear self-orthogonal rank-metric codes based on the quadratic form and analyze their list decodability. Ultimately, we draw a conclusion.

4.2 Preliminaries

4.2.1 Linear self-orthogonal rank-metric codes

Rank-metric codes can mainly be interpreted in two different representations. The first representation is to deem each codeword as matrices in $\mathbb{F}_q^{n\times m}$. Alternatively, we can interpret each element of a rank-metric code as a vector in $\mathbb{F}_{q^m}^n$. In the first representation of codewords as matrices, linear codes are considered to be linear over $\mathbb{F}_q$. On the other hand, the linearity considered when seeing a rank-metric code as a set of vectors is assumed to be $\mathbb{F}_{q^m}$ linearity. The two different representations of rank-metric codes provide us with two different ways of defining inner product, which have been discussed in Chapter 2, and these present two possible ways in defining self-orthogonal rank-metric codes ($\mathbb{F}_q$-linear and $\mathbb{F}_{q^m}$-linear).

$\mathbb{F}_q$-linear self-orthogonal rank-metric codes

To properly define an $\mathbb{F}_q$-linear self-orthogonal rank-metric code, first we briefly provide the definitions and notations of matrix representation for rank-metric codes. A rank-metric code $\mathcal{C}$ contains $n \times m$ matrices over $\mathbb{F}_q$ for integers n, m and prime power q. Through the use of matrix transpose, for simplicity, we can just assume that n is at most m.

The (Delsarte) dual of $\mathcal{C}$ is then defined to be

$$\mathcal{C}^{\perp} = \{X \in \mathbb{F}_q^{n\times m} | \mathrm{Tr}(CX^T) = 0, \forall C \in \mathcal{C}\}.$$

Based on this definition of the Delsarte dual, an $\mathbb{F}_q$-linear rank-metric code $\mathcal{C}$ is said to be self-orthogonal if $\mathcal{C} \subseteq \mathcal{C}^{\perp}$. A property of $\mathbb{F}_q$-linear self-orthogonal rank-metric code that is readily verified is that its $\mathbb{F}_q$-dimension should be at most $\frac{nm}{2}$ and hence its rate R must be in the range $0 < R \leq 1/2$.

$\mathbb{F}_{q^m}$-linear self-orthogonal rank-metric codes

Pick $\mathbb{F}_{q^m}$, the extension field of $\mathbb{F}_q$ with degree m. The ring isomorphism between $\mathbb{F}_{q^m}$ and $\mathbb{F}_q^m$ through the use of a fixed $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$ implies the possibility to identify a rank-metric codes over $\mathbb{F}_q^{n\times m}$ as a collection of vectors over $\mathbb{F}_{q^m}^n$. For any two vectors $\mathbf{x} = (x_1, \cdots x_n)$ and $\mathbf{y} = (y_1, \cdots, y_n) \in \mathbb{F}_{q^m}^n$, we say they are orthogonal to each other if $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^n x_i y_i = 0$. $\mathbf{x}$ is then called a self-orthogonal vector if it is orthogonal to itself. The definition of self-orthogonality can be naturally extended to a set $\{v_1, \cdots, v_t\}$ where this set is self-orthogonal if $\langle v_i, v_j \rangle = 0$ for any choices of i and j.

Clearly, this suggests an alternative way to define a dual $\mathcal{C}^\perp$ of a rank-metric code $\mathcal{C} \in \mathbb{F}_{q^m}^n$, namely the collection of codewords that are orthogonal through the standard inner product to all codewords in $\mathcal{C}$. Analogous to the previous definition, we call an $\mathbb{F}_{q^m}$-linear rank-metric code $\mathcal{C}$ to be self-orthogonal given that $\mathcal{C} \subseteq \mathcal{C}^\perp$. Consequentially, an $\mathbb{F}_{q^m}$-linear rank-metric code $\mathcal{C}$ can only be self orthogonal if its $\mathbb{F}_{q^m}$-dimension does not exceed $\frac{n}{2}$ or it has rate $0 \leq R \leq 1/2$. We will devote the remainder of this section to investigate when both definition of duals can coincide.

In order to do that, we first need to review some basic concepts of algebra. Recall that for the field $\mathbb{F}_{q^m}$, there are m different $\mathbb{F}_q$-linear automorphisms which are the Frobenius automorphisms $x \mapsto x^{q^i}$ for $i = 0, \cdots, m-1$. Based on these automorphisms, we can then define the field trace $\mathrm{tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ which sends x to $\sum_{i=0}^{m-1} x^{q^i}$. We also recall that for any given $\mathbb{F}_q$-basis $\mathcal{B} = (\beta_1, \cdots, \beta_m)$ of $\mathbb{F}_{q^m}$, there always exists a dual bases $\mathcal{B}^* := (\beta_1^*, \cdots \beta_m^*)$ satisfying $\mathrm{tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta_i \beta_j^*) = \delta_{i,j}$, where $\delta_{i,j}$ is the Kronecker delta function. Now if β_i coincides with β_i^* for all i, $\mathcal{B}$ is called a self-dual basis. Note that the existence of a self-dual $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$ is equivalent to the condition that q is even or both q and m are odd [45]. We are ready to conduct our investigations.

Lemma 8. *Let q and m be chosen such that $\mathbb{F}_{q^m}$ has a self dual basis $\mathcal{B} = (\beta_1, \cdots, \beta_m)$.*

Furthermore, pick any two rank-metric codes $\mathcal{C}_1$ and $\mathcal{C}_2$ over $\mathbb{F}_q^{n\times m}$. Then

$$\mathrm{Tr}(\mathcal{C}_1\mathcal{C}_2^T) = \{\mathrm{Tr}(XY^T) : X \in \mathcal{C}_1, Y \in \mathcal{C}_2\} = \{0\}$$

if and only if

$$\langle \mathcal{C}_1, \mathcal{C}_2 \rangle = \{\langle \mathbf{x}, \mathbf{y} \rangle : \mathbf{x} \in \mathcal{C}_1, \mathbf{y} \in \mathcal{C}_2\} = \{0\}.$$

Note that we assume $\mathcal{C}_i$ to be in its matrix representation for the earlier equation and vector representation for the latter.

Proof. Let $\mathbf{a} = (a_1, \cdots, a_n) \in \mathcal{C}_1$ and $\mathbf{b} = (b_1, \cdots b_n) \in \mathcal{C}_2$. We further let $a_i = \sum_{j=1}^m a_{i,j}\beta_j$ and $b_i = \sum_{k=1}^m b_{i,k}\beta_k$ for all $i = 1, 2 \cdots, n$. Assuming $\langle \mathcal{C}_1, \mathcal{C}_2 \rangle = \{0\}$, we have

$$0 = \langle \mathbf{a}, \mathbf{b} \rangle = \sum_{i=1}^n a_i b_i \;\; = \;\; \sum_{i=1}^n \left(\sum_{j=1}^m a_{i,j}\beta_j \right) \left(\sum_{k=1}^m b_{i,k}\beta_k \right) = \sum_{i=1}^n \sum_{j=1}^m \sum_{k=1}^m a_{i,j} b_{i,k} \beta_j \beta_k.$$

Applying the field trace function to both sides, we have

$$0 = \mathrm{tr}\langle \mathbf{a}, \mathbf{b} \rangle = \sum_{i=1}^n \sum_{j=1}^m \sum_{k=1}^m a_{i,j} b_{i,k} \mathrm{tr}(\beta_j \beta_k) = \sum_{i=1}^n \sum_{j=1}^m a_{i,j} b_{i,j}.$$

Note that by assumption, the matrices $A = (a_{i,j}), B = (b_{i,j})$ with size $n \times m$ are the matrix representations of $\mathbf{a}$ and $\mathbf{b}$ respectively. Noting that $\mathrm{Tr}(AB^T) = \sum_{i=1}^n \sum_{j=1}^m a_{i,j} b_{i,j}$, the last equality implies that $\mathrm{Tr}(AB^T) = 0$. Since $\mathbf{a}$ and $\mathbf{b}$ are arbitrary elements of $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively, we have the conclusion $\mathrm{Tr}(\mathcal{C}_1\mathcal{C}_2^T) = \{0\}$ from the assumption that $\langle \mathcal{C}_1, \mathcal{C}_2 \rangle = \{0\}$.

On the other direction can be easily proved. Suppose that $\mathrm{Tr}(AB^T) = 0$ for all $A = (a_{i,j}) \in \mathcal{C}_1$ and $B = (b_{i,j}) \in \mathcal{C}_2$. Hence, we have $B \in \mathcal{C}_1^\perp$ or $\langle A, B \rangle = 0$ for all $A \in \mathcal{C}_1$ and $B \in \mathcal{C}_2$ which ultimately implies that $\langle \mathcal{C}_1, \mathcal{C}_2 \rangle = \{0\}$. ■

4.2.2 Quadratic forms

We say $f(x)$ is an n-variate quadratic form over $\mathbb{F}_q$, if it is a degree 2 homogeneous multinomial of n variables with coefficients from $\mathbb{F}_q$. The general formula that f should be

$$f(x) = f(x_1, x_2, \cdots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j, a_{ij} \in \mathbb{F}_q.$$

Note that an n-variate quadratic form f over $\mathbb{F}_q$ can be expressed as multiplication of matrices. Assuming $\mathbf{x} = (x_1, \cdots, x_n)^T$ and $A = (a_{i,j})_{i,j=1,\cdots,n}$ over $\mathbb{F}_q$, $f(x)$ can then be rewritten as $f(x) = x^T A x$.

Two quadratic forms f and g of n_1 and n_2 indeterminates respectively are called equivalent provided that we can find a full rank $n_1 \times n_2$ matrix M over $\mathbb{F}_q$ satisfying $f(xM) = g(x)$. Note that equivalence implies the same number of roots.

Equivalence enables two quadratic forms of different number of indeterminates to be closely related to each other. Given a non-zero quadratic form $f(x)$, the smallest number of indeterminates that a quadratic form $g(x)$ can have while still being equivalent to $f(x)$ is a parameter of $f(x)$ that is called to be its rank. By convention, we let the rank of the zero quadratic form be 0. A non-zero quadratic form $f(x)$ is said to be non-degenerate if its rank is equal to the number of its indeterminates.

To aid our analysis in this chapter, the number of roots of a quadratic form $f(x)$ is a topic of interest. We combine several results in [35, pp. 278-287, section 6.2] as a lemma to consider two cases (over $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$).

Lemma 9. *(see in [35, pp. 278-287, section 6.2]) Let $f(x) := f(x_1, x_2, \cdots, x_n)$ be a quadratic form with rank r over $\mathbb{F}_q$ (or $\mathbb{F}_{q^m}$). $N(f(x) = 0)$ denotes the number of roots of $f(x) = 0$ in $\mathbb{F}_q^{n \times m}$ (or $\mathbb{F}_{q^m}^n$). If $r = 0$, then we have $N(f(x) = 0) = q^{mn}$. If $r \geq 1$, then we have the following results:*

If $f(x)$ is defined over $\mathbb{F}_q$ with solutions in $\mathbb{F}_q^{n\times m}$,

$$N(f(x)=0)=\begin{cases} q^{mn-1}, & \text{if } r \text{ is odd.} \\ q^{mn-1}\pm(q-1)q^{mn-r/2-1}, & \text{if } r \text{ is even.} \end{cases}$$

Alternatively, if $f(x)$ is defined over $\mathbb{F}_{q^m}$ with solutions in $\mathbb{F}_{q^m}^n$,

$$N(f(x)=0)=\begin{cases} q^{m(n-1)}, & \text{if } r \text{ is odd.} \\ q^{m(n-1)}\pm(q^m-1)q^{m(n-r/2-1)}, & \text{if } r \text{ is even.} \end{cases}$$

4.3 Construction of Random Self-orthogonal Rank-metric Codes

4.3.1 $\mathbb{F}_q$-linear self-orthogonal rank-metric codes construction

In this part, we construct $\mathbb{F}_q$-linear self-orthogonal rank-metric codes based on quadratic forms.

Let $A=[a_{ij}], 1\le i\le n, 1\le j\le m$ be a word. If A is self-orthogonal, then

$$\mathrm{Tr}(AA^T)=\sum_{i=1}^{n}\sum_{j=1}^{m}a_{ij}a_{ij}=0.$$

Considering the standard bijection from $[n]\times[m]$ to $[nm]$, where $[n]=\{1,\cdots,n\}, [m]=\{1,\cdots,m\}$, we can rewrite the double index (i,j) to a single index to obtain

$$\mathrm{Tr}(AA^T) \;=\; \sum_{i=1}^{n}\sum_{j=1}^{m}a_{ij}a_{ij}=\sum_{\ell=1}^{mn}a_\ell^2=0.$$

Construction

- Step 1. Choose a nonzero random solution $A_1\in\mathbb{F}_q^{n\times m}$ of the quadratic equation $x_1^2+x_2^2+\cdots+x_{mn}^2=0$.

By Lemma 9 we can obtain that the above equation has at least q^{mn-2} solutions, so a self-orthogonal word A_1 can be found.

- Step 2. Obtain a linearly independent set $\{A_1, A_2, \cdots, A_{k-1}, A_k\}$ of random self-orthogonal matrices given $A_1, \cdots, A_{k-1}$.

  Firstly, we assume that a linearly independent set $\{A_1, A_2, \cdots, A_{k-1}\}$ of random self-orthogonal matrices has already been found, i.e. $\mathrm{Tr}(A_i A_j^T) = \sum_{\ell=1}^{mn} a_{i\ell} a_{j_\ell} = 0, 1 \leq i, j \leq k-1$. Then, if we want to find the k-th matrix A_k, we need to find a solution of the following equations

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1,mn}x_{mn} = 0, \\ \vdots \\ a_{k-1,1}x_1 + a_{k-1,2}x_2 + \cdots + a_{k-1,mn}x_{mn} = 0, \\ x_1^2 + x_2^2 + \cdots + x_{mn}^2 = 0. \end{cases} \tag{4.1}$$

Take the first $k-1$ equations above in to the last one, we have a quadratic equation $g(x_{i_1}, x_{i_2}, \cdots, x_{i_{mn-k+1}})$ of $mn-k+1$ variables. So, $N(g(x_{i_1}, x_{i_2}, \cdots, x_{i_{mn-k+1}}) = 0)$ is the number of solutions of the equation (4.1). The cardinality of $\mathrm{span}\{A_1, A_2, \cdots, A_{k-1}\}$ is equal to $q^{mn(k-1)}$. $N(g(x_{i_1}, x_{i_2}, \cdots, x_{i_{mn-k+1}}) = 0) > q^{mn(k-1)}$, thus we can randomly choose a solution A_k of (4.1), as long as it is not contained in $\mathrm{span}\{A_1, A_2, \cdots, A_{k-1}\}$.

So, we can obtain a linearly independent set $\{A_1, A_2, \cdots, A_{k-1}, A_k\}$ of random self-orthogonal matrices.

Moreover, by Lemma 9, the number of solution $N(g(x_{i_1}, x_{i_2}, \cdots, x_{i_{mn-k+1}}) = 0)$ of $g(x_{i_1}, x_{i_2}, \cdots, x_{i_{mn-k+1}}) = 0$ is at least q^{mn-k-1}. Thus, the set can always be constructed as long as $k \leq (mn-1)/2$.

4.3.2 $\mathbb{F}_{q^m}$-linear self-orthogonal rank-metric codes construction

We study how to construct $\mathbb{F}_{q^m}$-linear self-orthogonal rank-metric codes. The idea is similar to the construction of $\mathbb{F}_q$-linear self-orthogonal rank-metric codes. Constructing a random $\mathbb{F}_{q^m}$-linear self-orthogonal rank-metric code is equivalent to find a linearly independent set $\{x_1, x_2, \cdots, x_k\}$ of random $\mathbb{F}_{q^m}$-linear self-orthogonal vectors, where $x_i \in \mathbb{F}_{q^m}, 1 \leq i \leq k$.

Choose a nonzero random solution $x_1 = (x_{11}, x_{12}, \cdots, x_{1n}) \in \mathbb{F}_{q^m}^n$ of the quadratic equation $z_1^2 + z_2^2 + \cdots + z_n^2 = 0$. This equation has at least $q^{m(n-2)}$ roots, so a self-orthogonal x_1 can be found. The same method as the construction $\mathbb{F}_q$-linear self-orthogonal rank-metric codes can be conducted. Then, we can confirm there exists a linearly independent set $\{x_1, x_2, \cdots, x_{k-1}, x_k\}$ of $\mathbb{F}_{q^m}$-linear self-orthogonal vectors. In addition, by calculation we have such x_k as long as $k \leq (n-1)/2$.

4.4 List Decoding of Self-orthogonal Rank-metric Codes

4.4.1 List decoding of $\mathbb{F}_q$-linear self-orthogonal rank-metric codes

In this part, we investigate the list decodability of $\mathbb{F}_q$-linear self-orthogonal rank-metric codes. We show that rate and decoding radius of $\mathbb{F}_q$-linear self-orthogonal rank-metric codes can achieve the Gilbert-Varshamov bound. From now on, the information rate $\frac{\log_q |\mathcal{C}|}{mn}$ and the ratio $\frac{n}{m}$ are denoted by R and ρ, respectively.

Our main result of list decoding of $\mathbb{F}_q$-linear self-orthogonal rank-metric codes can be found in the Theorem 9. With the help of studying and discussing the weight distribution of certain rank-metric code, we can deal with it.

Lemma 10. *(see in [20]) For all integers $n \leq m$, every $\tau \in (0, 1)$ and $\ell = O(\sqrt{nm})$, there exists a constant $C_{\tau,q} > 1$ such that if $X_1, \cdots, X_\ell$ are selected independently and uniformly*

at random from $B_R(0, \tau n)$, *then we have*

$$Pr[|\operatorname{span}\{X_1, \cdots, X_\ell\} \cap B_R(0, \tau n)| \geq C_{\tau,q} \cdot \ell] \leq q^{-(3-O(1))mn}$$

From the above lemma, it reveals that randomly picking ℓ words from $B_R(0, \tau n)$, there exists more than $\Omega(\ell)$ words in the span of ℓ words lies in the $B_R(0, \tau n)$ happens with a very small probability, where the parameter ℓ depends on the list size $\mathcal{L}$.

Then, we consider the following result on the probability that a random dimension k $\mathbb{F}_q$-linear rank-metric code contains a dimension $k-1$ $\mathbb{F}_q$-linear self-orthogonal subcode and a given set $\{X_1, \cdots, X_\ell\} \subseteq \mathbb{F}_q^{n\times m}$ of linearly independent vectors. Let $\mathcal{C}_k^*$ present the set of dimension k $\mathbb{F}_q$-linear rank-metric codes, where every code contains a dimension $k-1$ $\mathbb{F}_q$-linear self-orthogonal subcode.

Lemma 11. *(see in [30]) For any* $\mathbb{F}_q$*-linearly independent words* $X_1, X_2, \cdots, X_\ell$ *in* $\mathbb{F}_q^{n\times m}$ *with* $\ell \leq k < mn/2$, *the probability of a random code* $\mathcal{C}^*$ *from* $\mathcal{C}_k^*$ *contains* $\{X_1, X_2, \cdots, X_\ell\}$ *is*

$$Pr_{\mathcal{C}^*\in\mathcal{C}_k^*}[\{X_1, X_2, \cdots, X_\ell\} \subseteq \mathcal{C}] \leq \begin{cases} q^{((k+\ell-mn-1)\ell+2k-1)}, & if\ q\ is\ even; \\ q^{((k+\ell-mn-2)\ell+4k-2)}, & if\ q\ is\ odd. \end{cases} \tag{4.2}$$

Thus, we have

$$Pr_{\mathcal{C}^*\in\mathcal{C}_k^*}[\{X_1, X_2, \cdots, X_\ell\} \subseteq \mathcal{C}] \leq q^{((k+\ell-mn-2)\ell+4k-1)}. \tag{4.3}$$

Based on the Lemma 10 and Lemma 11, we prove Theorem 9.

Theorem 9. *Let* q *be prime power and* $\tau \in (0, 1)$. *For small* $\epsilon > 0$, *an* $\mathbb{F}_q$*-linear self-orthogonal rank-metric code* $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ *of rate* $R = (1-\tau)(1-\rho\tau)-\epsilon$ *is* $(\tau n, O(1/\epsilon))^R$*-list decodable with a probability at least* $1 - q^{-2mn}$ *for large enough* n *and* m.

Proof. Pick $M = 5C_{\tau,q}$, where $C_{\tau,q}$ is the constant in Lemma 10. Set $\mathcal{L} = \lceil \frac{M}{\epsilon} \rceil$ and n to be large enough.

Let $\mathcal{C}$ be an $\mathbb{F}_q$-linear self-orthogonal rank-metric codes with $\dim_{\mathbb{F}_q}(\mathcal{C}) = Rmn$ in $\mathbb{F}_q^{n\times m}$, so the size $|\mathcal{C}| = q^{Rmn}$. We want to show that with high probability, $\mathcal{C}$ is $(\tau n, \frac{M}{\epsilon})^R$-list decodable. In other words, the code $\mathcal{C}$ is not $(\tau n, \frac{M}{\epsilon})^R$-list decodable with negligible probability, we aim to show that

$$Pr_{\mathcal{C}\in\mathcal{C}_{Rmn}}[\exists X \in \mathbb{F}_q^{n\times m},\ |B_R(X, \tau n) \cap \mathcal{C}| \geq \mathcal{L}] < q^{-2mn}, \tag{4.4}$$

where $\mathcal{C}_{Rmn}$ denotes the set of $\mathbb{F}_q$-linear self-orthogonal rank-metric codes with dimension Rmn.

Let $X \in \mathbb{F}_q^{n\times m}$ be picked uniformly at random, define

$$\triangle := Pr_{\mathcal{C}\in\mathcal{C}_{Rmn}, X\in\mathbb{F}_q^{n\times m}}[|B_R(X, \tau n) \cap \mathcal{C}| \geq \mathcal{L}]$$

For (4.4), it suffices to prove

$$\triangle < q^{-2mn} \cdot q^{-(1-R)mn} \tag{4.5}$$

The inequality (4.5) is derived from (4.4). For every $\mathbb{F}_q$-linear code $\mathcal{C}$, due to"bad" case X such that ($|B_R(X, \tau n) \cap \mathcal{C}| \geq \mathcal{L}$), there are at least q^{Rmn} such "bad" X.

Since $\mathcal{C}$ is $\mathbb{F}_q$-linear, we have

$$\begin{aligned}
\triangle =& Pr_{\mathcal{C}\in\mathcal{C}_{Rmn}, X\in\mathbb{F}_q^{n\times m}}[|B_R(X, \tau n) \cap \mathcal{C}| \geq \mathcal{L}] \\
=& Pr_{\mathcal{C}\in\mathcal{C}_{Rmn}, X\in\mathbb{F}_q^{n\times m}}[|B_R(0, \tau n) \cap (\mathcal{C} + X)| \geq \mathcal{L}] \\
\leq& Pr_{\mathcal{C}\in\mathcal{C}_{Rmn}, X\in\mathbb{F}_q^{n\times m}}[|B_R(0, \tau n) \cap \mathrm{span}_{\mathbb{F}_q}(\mathcal{C} + X)| \geq \mathcal{L}] \\
\leq& Pr_{\mathcal{C}^*\in\mathcal{C}^*_{Rmn+1}}[|B_R(0, \tau n) \cap \mathcal{C}^*| \geq \mathcal{L}],
\end{aligned}$$

where $\mathcal{C}^*$ is a dimension $Rmn+1$ random $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{n\times m}$ containing $\mathrm{span}_{\mathbb{F}_q}(\mathcal{C}+X)$. More specifically, if X is not in $\mathcal{C}$, then $\mathcal{C}^* = \mathrm{span}_{\mathbb{F}_q}(\mathcal{C}, X)$; otherwise $\mathcal{C}^* = \mathrm{span}_{\mathbb{F}_q}(\mathcal{C}, Y)$, where word Y is randomly picked from $\mathbb{F}_q^{n\times m}\backslash\mathcal{C}$.

For each integer $\log_q \mathcal{L} \leq \ell \leq \mathcal{L}$, let $\mathcal{F}_\ell$ be the set of all tuples $(X_1, X_2, \cdots, X_\ell) \in B_R(0, \tau n)^\ell$ such that $X_1, X_2, \cdots, X_\ell$ are linearly independent and $|\mathrm{span}(X_1, \cdots, X_\ell) \cap B_R(0, \tau n)| \geq \mathcal{L}$.

Let $\mathcal{F} = \bigcup_{\ell=\lceil log_q \mathcal{L} \rceil}^{\mathcal{L}} \mathcal{F}_\ell$. For each $X = (X_1, \cdots, X_\ell) \in \mathcal{F}$, let $\{X\}$ and (X) denote the set $\{X_1, \cdots, X_\ell\}$ and the tuple $(X_1, \cdots, X_\ell)$, respectively.

We claim that if $|B_R(0, \tau n) \cap \mathcal{C}^*| \geq \mathcal{L}$, there must exist $(X) \in \mathcal{F}$ such that $\{X\} \subseteq \mathcal{C}^*$. Indeed, let $\{H\}$ be a maximal linearly independent subset of $B_R(0, \tau n) \cap \mathcal{C}^*$. If $|\{H\}| < \mathcal{L}$, then we have $\{X\} = \{H\}$. Otherwise, we have $\{X\}$ to be any subset of $\{H\}$ of size $\mathcal{L}$. Thus,

$$
\begin{aligned}
\triangle \leq & Pr_{\mathcal{C}^* \in \mathcal{C}^*_{Rmn+1}}[|B_R(0, \tau n) \cap \mathcal{C}^*| \geq \mathcal{L}] \\
\leq & \sum_{(X) \in \mathcal{F}_\ell} Pr_{\mathcal{C}^* \in \mathcal{C}^*_{Rmn+1}}[\{X\} \subseteq \mathcal{C}^*] \\
= & \sum_{\ell=\lceil log_q \mathcal{L} \rceil}^{\mathcal{L}} \sum_{(X) \in \mathcal{F}_\ell} Pr_{\mathcal{C}^* \in \mathcal{C}^*_{Rmn+1}}[\{X\} \subseteq \mathcal{C}^*] \\
= & \sum_{\ell=\lceil log_q \mathcal{L} \rceil}^{\mathcal{L}} |\mathcal{F}_\ell| Pr_{\mathcal{C}^* \in \mathcal{C}^*_{Rmn+1}}[\{X\} \subseteq \mathcal{C}^*] \\
\leq & \sum_{\ell=\lceil log_q \mathcal{L} \rceil}^{L} |\mathcal{F}_\ell| q^{(((Rmn+1)+\ell-mn-2)\ell+4(Rmn+1)-1)}.
\end{aligned}
$$

The last inequality is from the Lemma 11. We want to get a good bound of our probability, so we need to take a reasonable good upper bound for $|\mathcal{F}_\ell|$. Following the idea in [20], we bound the size of $\mathcal{F}_\ell$ relying on the value of the parameter ℓ.

- Case 1. $\ell < \frac{5}{\epsilon}$

  In this case, we have $\frac{|\mathcal{F}_\ell|}{|B_R(0,\tau n)|^\ell}$ is a lower bound on the probability that matrices $X_1, X_2, \cdots, X_\ell$ chosen independently and uniformly at random from the rank-metric ball $B_R(0, \tau n)$ are

  $$| \mathrm{span}\{X_1, \cdots, X_\ell\} \cup B_R(0, \tau n) | \geq \mathcal{L}.$$

By Lemma 10, the probability is at most q^{-2mn}, thus

$$|\mathcal{F}_\ell| \leq |B_R(0,\tau n)^\ell| \cdot q^{-2mn} \leq \left(4q^{mn(\tau+\tau\rho-\tau^2\rho)}\right)^\ell \cdot q^{-2mn}.$$

- Case 2. $\ell \geq \frac{5}{\epsilon}$

  We have the simple bound of

$$|\mathcal{F}_\ell| \leq |B_R(0,\tau n)^\ell| \leq \left(4q^{mn(\tau+\tau\rho-\tau^2\rho)}\right)^\ell.$$

Finally, taking the value of $R = (1-\tau)(1-\rho\tau) - \epsilon$ into the inequality below,

$$\begin{aligned}
\triangle \leq & \sum_{\ell=\lceil log_q \mathcal{L} \rceil}^{\mathcal{L}} |\mathcal{F}_\ell| q^{(((Rmn+1)+\ell-mn-2)\ell+4(Rmn+1)-1)} \\
\leq & \sum_{\ell=\lceil log_q \mathcal{L} \rceil}^{\lceil \frac{5}{\epsilon} \rceil - 1} |\mathcal{F}_\ell| q^{(((Rmn+1)+\ell-mn-2)\ell+4(Rmn+1)-1)} + \sum_{\ell=\lceil \frac{5}{\epsilon} \rceil}^{\mathcal{L}} |\mathcal{F}_\ell| q^{(((Rmn+1)+\ell-mn-2)\ell+4(Rmn+1)-1)} \\
= & q^{-2mn} q^{4Rmn} \cdot \sum_{\ell=\lceil log_q \mathcal{L} \rceil}^{\lceil \frac{5}{\epsilon} \rceil - 1} 4^\ell q^{mn\ell(\tau+\tau\rho-\tau^2\rho+R-1)} + q^{4Rmn} \cdot \sum_{\ell=\lceil \frac{5}{\epsilon} \rceil}^{\mathcal{L}} 4^\ell q^{mn\ell(\tau+\tau\rho-\tau^2\rho+R-1)} \\
= & q^{-2mn} q^{4Rmn} \cdot \sum_{\ell=\lceil log_q \mathcal{L} \rceil}^{\lceil \frac{5}{\epsilon} \rceil - 1} 4^\ell q^{mn\ell(-\epsilon)} + q^{4Rmn} \cdot \sum_{\ell=\lceil \frac{5}{\epsilon} \rceil}^{L} 4^\ell q^{mn\ell(-\epsilon)} \\
\leq & q^{-2mn} q^{4Rmn} \cdot \sum_{\ell=\lceil log_q \mathcal{L} \rceil}^{\lceil \frac{5}{\epsilon} \rceil - 1} 4^\ell q^{mn\ell(-\epsilon)} + q^{4Rmn} \cdot \sum_{\ell=\lceil \frac{5}{\epsilon} \rceil}^{\mathcal{L}} 4^\ell q^{-5mn} \\
\leq & q^{-2mn}.
\end{aligned}$$

Thus, an $\mathbb{F}_q$-linear self-orthogonal rank-metric code with rate $R = (1-\tau)(1-\rho\tau) - \epsilon$ is not $(\tau n, O(1/\epsilon))^R$-list decodable with an exponentially small probability at most q^{-2mn}. ■

Then, we consider two special cases, when the ratio $\rho = 1$ and ϵ.

Remark 10. When the ratio $\rho = \frac{n}{m} = 1$, our results reveal that a square $\mathbb{F}_q$-linear self-orthogonal rank-metric codes can be list decoded up to the Johnson bound with polynomial

list size. On the other hand, when the ratio $\rho = \epsilon$, a random $\mathbb{F}_q$-linear self-orthogonal rank-metric codes is list decodable with list decoding radius up to the Singleton bound.

4.4.2 List decoding $\mathbb{F}_{q^m}$-linear self-orthogonal rank-metric codes

We consider the probability that a random dimension k $\mathbb{F}_{q^m}$-linear code contains a self-orthogonal $k-1$ dimensional subcode and a given set $\{v_1, v_2, \cdots, v_\ell\} \subseteq \mathbb{F}_{q^m}^n$ of linearly independent vectors. Let $\mathcal{C}_k^*$ present the set of $\mathbb{F}_{q^m}$-linear codes in which every code contains an $\mathbb{F}_{q^m}$-linear $k-1$ dimensional self-orthogonal subcode.

Lemma 12. *(see in [30]) For any $\mathbb{F}_{q^m}$-linearly independent vectors $x_1, x_2, \cdots, x_\ell$ in $\mathbb{F}_{q^m}^n$ with $\ell \leq k < n/2$, the probability of a random code $\mathcal{C}^*$ from $\mathcal{C}_k^*$ contains $\{x_1, x_2, \cdots, x_\ell\}$ is*

$$Pr_{\mathcal{C}^* \in \mathcal{C}_k^*}[\{x_1, x_2, \cdots, x_\ell\} \subseteq \mathcal{C}] \leq q^{m((k+\ell-n-2)\ell+4k-1)}. \tag{4.6}$$

Theorem 10. *Let q be prime power and $\tau \in (0,1)$. For small $\epsilon > 0$, an $\mathbb{F}_{q^m}$-linear self-orthogonal rank-metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of $R = (1-\tau)(1-\rho\tau) - \epsilon$ is $(\tau n, \exp(O(1/\epsilon)))^R$-list decodable with high probability $1 - q^{-2mn}$ for large enough n and m.*

Proof. Put $\mathcal{L} = \lceil \frac{1}{\epsilon} \rceil$ and assume n is large enough. Let $\mathcal{C}$ be an $\mathbb{F}_{q^m}$-linear self-orthogonal rank-metric codes with $\dim_{\mathbb{F}_{q^m}} = Rn$ in $\mathbb{F}_{q^m}^n$, so the size $|\mathcal{C}| = q^{Rmn}$. We want to show that $\mathcal{C}$ is $(\tau n, 1/\epsilon)^R$-list decodable, we aim to show that

$$Pr_{\mathcal{C} \in \mathcal{C}_{Rn}}[\exists x \in \mathbb{F}_{q^m}^n,\ |B_R(x, \tau n) \cap \mathcal{C}| \geq \mathcal{L}] < q^{-2mn}, \tag{4.7}$$

where $\mathcal{C}_{Rn}$ denotes the set of $\mathbb{F}_{q^m}$-linear self-orthogonal rank-metric codes with dimension Rn.

Let $x \in \mathbb{F}_{q^m}^n$ be picked uniformly at random, define

$$\triangle := Pr_{\mathcal{C} \in \mathcal{C}_{Rn}, x \in \mathbb{F}_{q^m}^n}[|B_R(x, \tau n) \cap \mathcal{C}| \geq \mathcal{L}]$$

To prove inequality (4.7), we need to show that

$$\triangle < q^{-2mn} \cdot q^{-(1-R)mn} \tag{4.8}$$

The inequality (4.8) is derived from (4.7). For every $\mathbb{F}_{q^m}$-linear $\mathcal{C}$, due to "bad" case x such that $|B_R(x, \tau n) \cap \mathcal{C}| \geq \mathcal{L}$, there are at least q^{Rmn} such "bad" x.

Since $\mathcal{C}$ is linear, we have

$$\begin{aligned}
\triangle =& Pr_{\mathcal{C} \in \mathcal{C}_{Rn}, x \in \mathbb{F}_{q^m}^n}[|B_R(x, \tau n) \cap \mathcal{C}| \geq \mathcal{L}] \\
=& Pr_{\mathcal{C} \in \mathcal{C}_{Rn}, x \in \mathbb{F}_{q^m}^n}[|B_R(0, \tau n) \cap (\mathcal{C} + x)| \geq \mathcal{L}] \\
\leq& Pr_{\mathcal{C} \in \mathcal{C}_{Rn}, x \in \mathbb{F}_{q^m}^n}[|B_R(0, \tau n) \cap \mathrm{span}_{\mathbb{F}_{q^m}}(\mathcal{C} + x)| \geq \mathcal{L}] \\
\leq& Pr_{\mathcal{C}^* \in \mathcal{C}^*_{Rn+1}}[|B_R(0, \tau n) \cap \mathcal{C}^*| \geq \mathcal{L}],
\end{aligned}$$

where $\mathcal{C}^*$ is a random $Rn+1$ dimensional $\mathbb{F}_{q^m}$-subspace of $\mathbb{F}_{q^m}^n$ containing $\mathcal{C}$ (If $x \notin \mathcal{C}$,then $\mathcal{C}^* = \mathrm{span}_{\mathbb{F}_{q^m}}(\mathcal{C}, x)$; otherwise $\mathcal{C}^* = \mathrm{span}_{\mathbb{F}_{q^m}}(\mathcal{C}, y)$, where y is picked randomly from $\mathbb{F}_{q^m}^n \backslash \mathcal{C}$).

For each integer ℓ, $\log_{q^m} \mathcal{L} \leq \ell \leq \mathcal{L}$. Let $\mathcal{F}_\ell$ be the set of all tuples $(x_1, \cdots, x_\ell) \in B_R(0, \tau n)^\ell$ such that $x_1, \cdots, x_\ell$ are linearly independent and

$$|\mathrm{span}(x_1, \cdots, x_\ell) \cap B_R(0, \tau n)| \geq \mathcal{L}.$$

Hence,

$$|\mathcal{F}_t| \leq |B_R(0, \tau n)^t| \leq \left(4q^{mn(\tau + \tau b - \tau^2 b)}\right)^\ell.$$

Let $\mathcal{F} = \bigcup_{\ell = \lceil log_{q^m} \mathcal{L} \rceil}^{\mathcal{L}} \mathcal{F}_\ell$. For each $x = (x_1, \cdots, x_\ell) \in \mathcal{F}$, let $\{x\}$ denote the set $\{x_1, \cdots, x_\ell\}$.

We claim that if $|B_R(0, \tau n) \cap \mathcal{C}^*| \geq \mathcal{L}$, there must exist $x \in \mathcal{F}$ such that $\{x\} \subseteq \mathcal{C}^*$.

Thus, we have

$$\begin{aligned}
\triangle \leq & Pr_{\mathcal{C}^* \in \mathcal{C}^*_{Rn+1}}[|B_R(0, \tau n) \cap \mathcal{C}^*| \geq \mathcal{L}] \\
\leq & \sum_{x \in \mathcal{F}_\ell} Pr_{\mathcal{C}^* \in \mathcal{C}^*_{Rn+1}}[\{x\} \subseteq \mathcal{C}^*] \\
= & \sum_{\ell = \lceil log_{q^m} \mathcal{L} \rceil}^{\mathcal{L}} \sum_{x \in \mathcal{F}_\ell} Pr_{\mathcal{C}^* \in \mathcal{C}^*_{Rn+1}}[\{x\} \subseteq \mathcal{C}^*] \\
= & \sum_{\ell = \lceil log_{q^m} \mathcal{L} \rceil}^{\mathcal{L}} |\mathcal{F}_\ell| Pr_{\mathcal{C}^* \in \mathcal{C}^*_{Rn+1}}[\{v\} \subseteq \mathcal{C}^*]
\end{aligned}$$

By taking $R = (1-\tau)(1-\rho\tau) - \epsilon$, we can obtain

$$\begin{aligned}
\triangle \leq & Pr_{\mathcal{C}^* \in \mathcal{C}^*_{Rn+1}}[|B_R(0, \tau n) \cap \mathcal{C}^*| \geq \mathcal{L}] \\
\leq & \sum_{\ell = \lceil log_{q^m} \mathcal{L} \rceil}^{\mathcal{L}} \left(4q^{mn(\tau+\tau\rho-\tau^2\rho)}\right)^\ell Pr_{\mathcal{C}^* \in \mathcal{C}^*_{Rn+1}}[\{x\} \subseteq \mathcal{C}^*] \\
\leq & \sum_{\ell = \lceil log_{q^m} \mathcal{L} \rceil}^{\mathcal{L}} \left(4q^{mn(\tau+\tau\rho-\tau^2\rho)}\right)^\ell q^{m((Rn+1)+\ell-n-2)\ell+4(Rn+1)-1)} \\
\leq & 4^\ell \cdot \sum_{\ell = \lceil log_{q^m} \mathcal{L} \rceil}^{\mathcal{L}} q^{mn\ell(\tau+\tau b-\tau^2\rho+R-1)} \\
\leq & q^{-2mn}.
\end{aligned}$$

Thus, an $\mathbb{F}_{q^m}$-linear self-orthogonal rank-metric code with rate $R = (1-\tau)(1-\rho\tau) - \epsilon$ is not $(\tau n, \exp(O(1/\epsilon)))^R$-list decodable with an exponentially small probability at most q^{-2mn}.

■

4.5 Conclusion

We investigate the list decodability of $\mathbb{F}_q$- and $\mathbb{F}_{q^m}$-linear self-orthogonal rank-metric codes. Our results reveal that a random $\mathbb{F}_q$-linear self-orthogonal rank-metric codes can be list decoded up to the Gilbert-Varshamov bound with polynomial list size. By using the same methods for $\mathbb{F}_{q^m}$-linear rank-metric codes, our results reveal that the $\mathbb{F}_{q^m}$-linear self-orthogonal rank-metric codes is list decodable up to $R = (1-\tau)(1-\rho\tau) - \epsilon$ with exponential list size.

In the future research, it is interesting to consider decreasing the list size of $\mathbb{F}_{q^m}$-linear self-orthogonal rank-metric codes and $\mathbb{F}_{q^m}$-linear rank-metric codes in general. Moreover, the study on this chapter only considered the list decodability of random rank-metric codes. Hence, can we efficiently list decode $\mathbb{F}_{q^m}$-linear rank-metric codes?

Chapter 5

A New Family of $\mathbb{F}_q$-Linear Maximum Rank Distance Codes

Gabidulin codes are the most prominent family of maximum rank distance (MRD) codes that have been used in many fields. However, their structured form is problematic in the cryptographic application [51] and [28]. A natural following challenge is then to see if other families of MRD codes which are not equivalent to Gabidulin codes can be constructed. In the last three years, people have made some progress on this topic in [62], [5], [57], [40], [50] and [48]. However, all the known families of $\mathbb{F}_q$-linear non-Gabidulin MRD codes of length n have dimension and co-dimension less than $n-1$ except for $n=3$. Our construction extends the idea used to construct Twisted Gabidulin codes [57] in two ways: (i) dimension of our codes is extended from $1<k<n-1$ to $k=n-1$ and $k=1$; (ii) the leading coefficient of linearized polynomials can be controlled by any other coefficients, while in [57] the leading coefficient of the linearized polynomials is controlled only by the constant term. In this chapter, we present a new family of $\mathbb{F}_q$-linear MRD codes of dimension $k=n-1$ for all n, which are not equivalent to any currently known families of MRD codes. Furthermore, our family along with its dual extends Twisted Gabidulin codes and Generalized Twisted Gabidulin codes to dimension $k=n-1$ and $k=1$, which fills the gap in [57].

5.1 Introduction

A rank-metric code is a set of $m \times n$ matrices over a finite field $\mathbb{F}_q$, or alternatively, vectors of length m over the extension field $\mathbb{F}_{q^n}$. Rank-metric codes that attain the Singleton bound are called maximum rank distance (MRD) codes. Gabidulin codes are the most well-known MRD codes, which were introduced by Delsarte and Gabidulin [7], [15]. Due to its structure [51], [28] showed Gabidulin codes based cryptosystems have proven to be weak. So, it is interesting to find non-Gabidulin MRD codes.

Known results: By a non-Gabidulin MRD code, we mean an MRD code that is not equivalent to a Gabidulin code. Recently there have been some research in this area. In [5], nonlinear 3×3 MRD codes were firstly proposed. In [62], [50], classes of linear non-Gabidulin MRD codes with dimension 2 were presented. In 2015, an interesting class of non-Gabidulin MRD codes was proposed in [57]. This class of codes has arbitrary size n and dimension from 2 to $n-2$. Otal et al [48] constructed a family of MRD codes, which coincides with the family in [57] when it is $\mathbb{F}_q$-linear. Thus, it remains an open question: *are there any $\mathbb{F}_q$-linear non-Gabidulin MRD codes of size n and dimension $n-1$ or 1 for $n > 3$, which are not equivalent to the existing families*?

Our result: The main purpose of this chapter is to solve the open question above. Specifically speaking, we generalize the idea of construction in [57] in two ways: (i) dimension of our codes extends the possible dimension k to include 1 and $n-1$; (ii) the leading coefficient of the linearized polynomials can be controlled by any other coefficients. Moreover, we investigate the equivalences of our family and its dual with existing families.

This chapter is organized as follows. Firstly, we give and introduce some preliminaries on Twisted Gabidulin codes, Equivalence and Dickson matrices. Secondly, we give a construction of a new family of $\mathbb{F}_q$-linear MRD codes. Then, we show that most codes in this family are not equivalent to Gabidulin codes and Generalized Gabidulin codes. Based on the Delsarte dual of our family, we give some results on Twisted Gabidulin codes and Generalized Twisted Gabidulin codes. Lastly, we give a conclusion.

5.2 Background

Based on Gabidulin codes $\mathcal{G}_k$, we introduce the *Generalized Gabidulin codes* in the following.

Definition 18. Let n, k, s and q be positive integers such that $\gcd(n, s) = 1$ and q be a power of prime. Then the set

$$\mathcal{G}_{k,s} = \left\{ \sum_{i=0}^{k-1} f_i x^{q^{si}} : f_i \in \mathbb{F}_{q^n} \right\},$$

is an $\mathbb{F}_q$-linear MRD code of size q^{nk}, which we call a Generalized Gabidulin code.

Recently, J. Sheekey constructed the *Twisted Gabidulin codes* [57]. In order to define the Twisted Gabidulin codes, we first recall the definition of norm function.

Definition 19. Let $\alpha \in \mathbb{F}_{q^n}$. The norm of α over $\mathbb{F}_q$, denoted by $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$, is given by

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \prod_{i=0}^{n-1} \alpha^{q^i}.$$

Definition 20. (see in [57]) Let n, k, h be positive integers and $k < n$. Let η be in $\mathbb{F}_{q^n}$ such that $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\eta) \neq (-1)^{kn}$. Then the set

$$\mathcal{H}_k(\eta, h) = \left\{ \sum_{i=0}^{k-1} f_i x^{q^i} + \eta f_0^{q^h} x^{q^k} : f_i \in \mathbb{F}_{q^n} \right\},$$

is an $\mathbb{F}_q$-linear MRD code of size q^{nk}, which is called a Twisted Gabidulin code.

Inspired by Twisted Gabidulin codes, Lunardon et al [40] defined *Generalized Twisted Gabidulin codes*.

Definition 21. (see in [40]) Let n, k, s, h be positive integers satisfying $\gcd(n, s) = 1$ and $k < n$. Let η be in $\mathbb{F}_{q^n}$ such that $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\eta) \neq (-1)^{nk}$. Then the set

$$\mathcal{H}_{k,s}(\eta, h) = \left\{ \sum_{i=0}^{k-1} f_i x^{q^{si}} + \eta f_0^{q^h} x^{q^{sk}} : f_i \in \mathbb{F}_{q^n} \right\},$$

is an $\mathbb{F}_q$-linear MRD code of size q^{nk}, which is called a Generalized Twisted Gabidulin code.

By [45], all Gabidulin codes are improperly automorphic. Hence, given a code, if it is equivalent to a Gabidulin code $\mathcal{G}$, then it must be properly equivalent to $\mathcal{G}$. In this chapter, we only need to consider the proper equivalence, for short, equivalence.

If we identify the codes $\mathcal{C}$ and $\mathcal{C}'$ with two sets $\mathcal{L}$ and $\mathcal{L}'$ of q-linearized polynomials, respectively, then $\mathcal{C}$ is equivalent to $\mathcal{C}'$ if and only if

$$\begin{aligned} \mathcal{L} &= A(x) \circ \mathcal{L}' \circ B(x) \\ &= \{A(x) \circ f(x) \circ B(x) : f(x) \in \mathcal{L}'\}, \end{aligned}$$

where $A(x)$ and $B(x)$ are invertible q-linearized polynomials corresponding to the matrices A and B, respectively. Throughout this chapter, we will use a set of linearized polynomials to represent a rank-metric code.

Then, we review some basic properties about Dickson matrices.

Definition 22. The Dickson matrix D_L associated with a q-linearized polynomial $L(x) = \sum_{i=0}^{n-1} f_i x^{q^i}$, $f_i \in \mathbb{F}_{q^n}$ is

$$D_L = \begin{pmatrix} f_0 & f_1 & \cdots & f_{n-1} \\ f_{n-1}^q & f_0^q & \cdots & f_{n-2}^q \\ \vdots & \vdots & \ddots & \vdots \\ f_1^{q^{n-1}} & f_2^{q^{n-1}} & \cdots & f_0^{q^{n-1}} \end{pmatrix}.$$

The relations between linearized polynomials and Dickson matrices have been well studied [67].

Proposition 1. *(see in [67]) For any linearized polynomials $L(x) \in \mathcal{L}_n(\mathbb{F}_{q^n})$, we have*

$$\mathrm{rank}_{\mathbb{F}_q} L(x) = \mathrm{rank}_{\mathbb{F}_{q^n}} D_L,$$

where $\mathrm{rank}_{\mathbb{F}_q} L(x)$ *is defined to be the rank of the corresponding matrix.*

5.3 Construction of New $\mathbb{F}_q$-Linear Maximum Rank Distance Codes

In this section, we present our family of $\mathbb{F}_q$-linear MRD codes.

Theorem 11. *Let* i, g, h *be integers such that* $0 \leq i \leq n-2, g = \gcd(i+1, n)$ *and* $h \equiv 0 \pmod{g}$. *Fixing* $\eta \in \mathbb{F}_{q^n} \setminus \{0\}$ *with* $N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^g}}(\eta) \neq 1$, *the set*

$$\mathcal{F}_{(i,h)} := \left\{ \sum_{j=0}^{n-2} f_j x^{q^j} + \eta f_i^{q^h} x^{q^{n-1}} : f_j \in \mathbb{F}_{q^n} \right\}$$

gives an $\mathbb{F}_q$*-linear MRD code of size* $q^{n(n-1)}$.

Proof. It is obvious that $\mathcal{F}_{(i,h)}$ is $\mathbb{F}_q$-linear. We prove it is an MRD code. Since $\mathcal{F}_{(i,h)}$ is linear, we need to prove that for any $f(x) \in \mathcal{F}_{(i,h)} \setminus \{0\}$, $d_R(f(x)) = \mathrm{rank}_{\mathbb{F}_q} f(x) \geq 2$.

Consider the Dickson matrix D_f corresponding to $f(x)$,

$$D_f = \begin{bmatrix} f_0 & \cdots & f_i & \cdots & \eta f_i^{q^h} \\ \eta^q f_i^{q^{h+1}} & \cdots & f_{i-1}^q & \cdots & f_{n-2}^q \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ f_{n-i-1}^{q^{i+1}} & \cdots & \eta^{q^{i+1}} f_i^{q^{h+i+1}} & \cdots & f_{n-i-2}^{q^{i+1}} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ f_1^{q^{n-1}} & \cdots & f_{i-(n-1)}^{q^{n-1}} & \cdots & f_0^{q^{n-1}} \end{bmatrix}.$$

By Proposition 1, $\mathrm{rank}_{\mathbb{F}_q} f(x) = \mathrm{rank}_{\mathbb{F}_{q^n}} D_f$. So, it is sufficient to show that $\mathrm{rank}_{\mathbb{F}_{q^n}} D_f \geq 2$. Since $f(x) \neq 0$, there exists $j, 0 \leq j \leq n-1$, such that $f_j \neq 0$. Thus, each row of D_f cannot be $\mathbf{0}$. Let $\mathbf{r}_t$ denote the t-th row of D_f. Suppose there exists $\ell, 0 \leq \ell \leq n-1$, such that $f_\ell = 0$, then we can obtain that the $(\ell+1)$-th coordinate of $\mathbf{r}_1$ is 0. Since $f_j \neq 0$, the $(\ell+1)$-th coordinate of $\mathbf{r}_{\ell-j+1}$ is $f_j^{q^{\ell-j}} \neq 0$. It implies that $\mathbf{r}_1$ cannot be a multiple of

$\mathbf{r}_{\ell-j+1}$. Therefore, $\mathrm{rank}_{\mathbb{F}_{q^n}} D_f \geq 2$. Now, we consider when $f_j \neq 0$, for all j. Suppose $\mathrm{rank}_{\mathbb{F}_{q^n}} D_f = 1$, then for any $j \neq k$, there exists $\lambda_{j,k} \in \mathbb{F}_{q^n}$, such that $\mathbf{r}_j = \lambda_{j,k} \cdot \mathbf{r}_k$. In particular, consider $\mathbf{r}_1$ and $\mathbf{r}_{i+2}$, then

$$\lambda_{1,i+2} = \frac{f_0}{f_{n-i-1}^{q^{i+1}}} = \frac{f_1}{f_{n-i}^{q^{i+1}}} = \cdots = \frac{f_i}{\eta^{q^{i+1}} f_i^{q^{h+i+1}}} = \cdots = \frac{\eta f_i^{q^h}}{f_{n-i-2}^{q^{i+1}}}.$$

That is, we have

$$\frac{f_i}{\eta^{q^{i+1}} f_i^{q^{h+i+1}}} = \frac{f_j}{f_{j-i-1}^{q^{i+1}}} = \frac{\eta f_i^{q^h}}{f_{n-i-2}^{q^{i+1}}},$$

for $j \in \{0, 1, \cdots, n-2\} \setminus \{i\}$. Thus, we can obtain

$$\begin{aligned} & \frac{f_i}{\eta^{q^{i+1}} f_i^{q^{h+i+1}}} \cdots \left(\frac{f_i}{\eta^{q^{i+1}} f_i^{q^{h+i+1}}} \right)^{q^{(k-1)(i+1)}} \\ = \; & \frac{\eta f_i^{q^h}}{f_{n-i-2}^{q^{i+1}}} \cdot \left(\frac{f_{n-i-2}}{f_{n-1-2(i+1)}^{q^{i+1}}} \right)^{q^{i+1}} \cdots \left(\frac{f_{n-1-(k-1)(i+1)}}{f_{n-1-k(i+1)}^{q^{i+1}}} \right)^{q^{(k-1)(i+1)}}. \end{aligned} \tag{5.1}$$

Note that (5.1) is true for any value of k. Let $k = \frac{n}{g} - 1$, where $g = \gcd(i+1, n)$. In this case,

$$n - 1 - \left(\frac{n}{g} - 1 \right)(i+1) \equiv i \pmod{n},$$

so $f_{n-1-k(i+1)} = f_i$. As $h \equiv 0 \pmod{g}$, we have $N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^g}}(f_i) = N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^g}}(f_i^{q^h})$. Thus, $N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^g}}(\eta) = 1$. This contradicts with the assumption $N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^g}}(\eta) \neq 1$. Therefore, the conclusion follows. ■

By investigating a generalization of the family of non-Gabidulin MRD codes in [57], Lunardon et al [40] found the family in [57] is a proper subset of their new family. Utilizing the same idea, we generalize our new family.

Definition 23. Let s be a positive integer with $\gcd(n, s) = 1$. We define a family of MRD

codes as

$$\mathcal{F}_{(i,h;s)} := \left\{ \sum_{j=0}^{n-2} f_j x^{q^{sj}} + \eta f_i^{q^h} x^{q^{s(n-1)}} : f_j \in \mathbb{F}_{q^n} \right\},$$

where $\eta \in \mathbb{F}_{q^n}$ satisfies $N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^g}}(\eta) \neq 1$.

Lemma 13. *The family $\mathcal{F}_{(i,h;s)}$ is equivalent to the family $\mathcal{F}_{(s(i+1)-1,h)}$.*

Proof. Since $\gcd(n, s) = 1$, the set $\{0, s, 2s, \cdots, (n-1)s\}$ can be rearranged to the set $\{0, 1, 2, \cdots, n-1\}$. Thus, the family $\mathcal{F}_{(i,h;s)}$ can be rewritten as

$$\mathcal{F}_{(i,h;s)} = \mathcal{F}_{(s(i+1)-1,h)} \circ x^{q^{n-s+1}}.$$

Hence, $\mathcal{F}_{(i,h;s)}$ is equivalent to $\mathcal{F}_{(s(i+1)-1,h)}$. ■

By using this generalization method for our new family, we can not obtain a bigger family. Hence, we focus on studying the relationship between our family $\mathcal{F}_{(i,h)}$ and the existing families, namely Gabidulin codes, Generalized Gabidulin codes, Twisted Gabidulin codes and Generalized Twisted Gabidulin codes.

5.4 Comparison with (Generalized) Gabidulin Codes

5.4.1 Comparison with Gabidulin codes

In this subsection, we consider the equivalence of the new family $\mathcal{F}_{(i,h)}$ to the Gabidulin code $\mathcal{G}_{n-1}$ in Theorem 12 and Theorem 13.

Theorem 12. *Let $\mathcal{F}_{(i,h)}$ be the family defined in Theorem 11 with $h \neq 0$ and $h \neq n-i-1$, $0 \leq i \leq n-2$. Then, the new family $\mathcal{F}_{(i,h)}$ is not equivalent to the Gabidulin code $\mathcal{G}_{n-1}$.*

Proof. Suppose $\mathcal{F}_{(i,h)}$ is equivalent to the Gabidulin code $\mathcal{G}_{n-1}$, there exist non-zero invertible polynomials $A(x) = \sum_{\ell=0}^{n-1} a_\ell x^{q^\ell}$, $a_\ell \in \mathbb{F}_{q^n}$ and $B(x) = \sum_{j=0}^{n-1} b_j x^{q^j}$, $b_j \in \mathbb{F}_{q^n}$ such

that $A(x) \circ \mathcal{F}_{(i,h)} \circ B(x) = \mathcal{G}_{n-1}$ for any $f(x) = \sum_{t=0}^{n-2} f_t x^{q^t} + \eta f_i^{q^h} x^{q^{n-1}} \in \mathcal{F}_{(i,h)} \setminus \{0\}$,

$$\begin{aligned} A(x) \circ f(x) \circ B(x) &= \sum_{\ell=0}^{n-1} a_\ell x^{q^\ell} \circ \left(\sum_{t=0}^{n-2} f_t x^{q^t} + \eta f_i^{q^h} x^{q^{n-1}} \right) \circ \sum_{j=0}^{n-1} b_j x^{q^j} \\ &= \sum_{\ell=0}^{n-1} a_\ell \sum_{t=0}^{n-2} f_t^{q^\ell} \sum_{j=0}^{n-1} b_j^{q^{t+\ell}} x^{q^{\ell+t+j}} + \sum_{\ell=0}^{n-1} a_\ell \eta^{q^\ell} f_i^{q^{h+\ell}} \sum_{j=0}^{n-1} b_j^{q^{n-1+\ell}} x^{q^{n-1+j+\ell}}, \end{aligned}$$

the coefficient of $x^{q^{n-1}}$ in $A(x) \circ f(x) \circ B(x)$ is 0. Thus, for any $f_t \in \mathbb{F}_{q^n}$, $0 \le t \le n-2$, we have

$$\begin{aligned} a_0 \left(f_0 b_{n-1} + f_1 b_{n-2}^q + f_2 b_{n-3}^{q^2} + \cdots + f_{n-2} b_1^{q^{n-2}} + \eta f_i^{q^h} b_0^{q^{n-1}} \right) &+ \\ a_1 \left(f_0^q b_{n-2}^q + f_1^q b_{n-3}^{q^2} + f_2^q b_{n-4}^{q^3} + \cdots + f_{n-2}^q b_0^{q^{n-1}} + \eta^q f_i^{q^{h+1}} b_{n-1} \right) &+ \\ \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots &+ \\ a_{n-1} \left(f_0^{q^{n-1}} b_0^{q^{n-2}} + f_1^{q^{n-2}} b_{n-1} + f_2^{q^{n-2}} b_{n-2}^q + \cdots + f_{n-2}^{q^{n-1}} b_2^{q^{n-3}} + \eta^{q^{n-1}} f_i^{q^{h-1}} b_1^{q^{n-2}} \right) &= 0. \end{aligned}$$

For any $s \in \{0, 1, \cdots, n-2\} \setminus \{i\}$, letting $f_t = 0$, $t \neq s$, we can obtain

$$a_0 b_{n-1-s}^{q^s} f_s + a_1 b_{n-2-s}^{q^{s+1}} f_s^q + \cdots + a_{n-1} b_{n-s}^{q^{s-1}} f_s^{q^{n-1}} = 0. \tag{5.2}$$

Since (5.2) is true for any $f_s \in \mathbb{F}_{q^n}$, we have that for any $\alpha \in \mathbb{F}_{q^n}$, α is a root of the following linearized polynomial of q-degree $n-1$,

$$a_0 b_{n-1-s}^{q^s} x + a_1 b_{n-2-s}^{q^{s+1}} x^q + \cdots + a_{n-1} b_{n-s}^{q^{s-1}} x^{q^{n-1}} = 0.$$

There is only possible if it is the zero polynomial, i.e.

$$a_\ell b_{n-1-s-\ell} = 0, \tag{5.3}$$

where $0 \le \ell \le n-1$ and $s \in \{0, 1, \cdots, n-2\} \setminus \{i\}$.

Let $f_t = 0, t \in \{0, 1, \cdots, n-2\} \setminus \{i\}$, we obtain

$$\left(a_0 b_{n-i-1}^{q^i} + \eta^{q^{n-h}} b_h^{q^{n-h-1}} a_{n-h}\right) f_i + \cdots + \left(a_{n-1} b_{n-i}^{q^i-1} + \eta^{q^{n-h-1}} b_{h+1}^{q^{n-h-2}} a_{n-h-1}\right) f_i^{q^{n-1}} = 0 \quad (5.4)$$

Since (5.4) is true for any $f_i \in \mathbb{F}_{q^n}$, we have for any $\alpha \in \mathbb{F}_{q^n}$, α is a root of a linearized polynomial of q-degree $n-1$,

$$\left(a_0 b_{n-i-1}^{q^i} + \eta^{q^{n-h}} b_h^{q^{n-h-1}} a_{n-h}\right) x + \cdots + \left(a_{n-1} b_{n-i}^{q^i-1} + \eta^{q^{n-h-1}} b_{h+1}^{q^{n-h-2}} a_{n-h-1}\right) x^{q^{n-1}} = 0.$$

Therefore,

$$a_0 b_{n-i-1}^{q^i} + \eta^{q^{n-h}} b_h^{q^{n-h-1}} a_{n-h} = 0 \quad (5.5)$$

$$\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots$$

$$a_h b_{n-i-h-1}^{q^{i+h}} + \eta b_0^{q^{n-1}} a_0 = 0 \quad (5.6)$$

$$\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots$$

$$a_{n-1} b_{n-i}^{q^i-1} + \eta^{q^{n-h-1}} b_{h+1}^{q^{n-h-2}} a_{n-h-1} = 0.$$

Without loss of generality, we can assume that $a_0 \neq 0$. By (5.3), it implies $b_{n-1-s} = 0$ for $s \in \{0, \cdots, n-2\} \setminus \{i\}$. From (5.5) and (5.6) we can deduce that $b_{n-1-i} = 0$ and $b_0 = 0$ with $h \neq n-i-1$ and $h \neq 0$. Thus, all coefficients of $B(x)$ are zeros. It contradicts the assumption that $B(x)$ is nonzero. Thus, the new family $\mathcal{F}_{(i,h)}$ is not equivalent to the Gabidulin code $\mathcal{G}_{n-1}$. ■

In the following, we consider the equivalence of the family $\mathcal{F}_{(i,h)}$ to $\mathcal{G}_{n-1}$ when $h = 0$ or $h = n-i-1$.

Lemma 14. *Let n, i, g, h, η be the values defined along with the construction of $\mathcal{F}_{(i,h)}$ in Theorem 11. Define $A(x) = \sum_{s=0}^{\frac{n}{g}-1} a_s x^{q^{gs}}$, where $a_0 = 1$, $a_s = \eta a_{s+\frac{i+1}{g}}^{q^{n-1-i}}$ for all $s \in \{1, 2, \ldots, \frac{n}{g}-1\}$. Then we have $a_{\frac{i+1}{g}} - \eta^{-q^{i+1}} a_0^{q^{i+1}} \neq 0$.*

Proof. Suppose $a_{\frac{i+1}{g}} = \eta^{-q^{i+1}} a_0^{q^{i+1}}$, we have $a_s = \eta a_{s+\frac{i+1}{g}}^{q^{n-1-i}}$ for all $s \in \{0, 1, \cdots, \frac{n}{g} - 1\}$. As $a_0 = 1 \neq 0$, we have $a_s \neq 0$. Combining the equalities $a_s = \eta a_{s+\frac{i+1}{g}}^{q^{n-1-i}}$ for all $s \in \{0, 1 \cdots, \frac{n}{g} - 1\}$, we have $a_0 = \eta^{\sum_{t=0}^{\frac{n}{g}-1} q^{t(-1-i)}} \cdot a_0 = N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^g}}(\eta) \cdot a_0$, therefore $N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^g}}(\eta) = 1$ which contradicts the assumption of $N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^g}}(\eta) \neq 1$. Thus, $a_{\frac{i+1}{g}} - \eta^{-q^{i+1}} a_0^{q^{i+1}} \neq 0$. ■

Lemma 15. *Let the polynomial $A(x)$ be defined in the Lemma 14, then $A(x)$ is invertible.*

Proof. We define the polynomial

$$C(x) = \frac{1}{a_{\frac{i+1}{g}}^{q^{n-1-i}} - \eta^{-1} a_0} x^{q^{n-1-i}} \circ (x - \eta^{-q^{i+1}} x^{q^{i+1}}).$$

A straightforward calculation gives the equality $C(x) \circ A(x) = x$ proving the invertibility of $A(x)$. ■

Theorem 13. *Let $\mathcal{F}_{(i,h)}$ be defined in Theorem 11. If $h = n - i - 1$ or $h = 0$, then $\mathcal{F}_{(i,h)}$ is equivalent to the Gabidulin code $\mathcal{G}_{n-1}$.*

Proof. For $h = n - i - 1$, we let the polynomial $A(x)$ be defined as in Lemma 14 and the invertible polynomial $B(x) = x$. We prove that $A(x) \circ \mathcal{G}_{n-1} \circ B(x) = \mathcal{F}_{(i,h)}$.

Let $\mathcal{F}^*_{(i,h)} = A(x) \circ \mathcal{G}_{n-1} \circ B(x)$. We firstly prove $\mathcal{F}^*_{(i,h)} \subseteq \mathcal{F}_{(i,h)}$. Suppose $f^*(x) = A(x) \circ g(x) \circ B(x) \in \mathcal{F}^*_{(i,h)}$, where $g(x) \in \mathcal{G}_{n-1}$. So, we have

$$f^*(x) = \sum_{s=0}^{\frac{n}{g}-1} a_s \sum_{t=0}^{n-2} g_t^{q^{gs}} x^{q^{gs+t}}. \tag{5.7}$$

Let $gs + t \equiv i \pmod{n}$. Since $i \equiv g - 1 \pmod{g}$, we have $t \equiv g - 1 \pmod{g}$. This implies that the coefficient of x^{q^i} in (5.7) is the same as the coefficient of x^{q^i} in $\sum_{s=0}^{\frac{n}{g}-1} a_s \sum_{t=1}^{\frac{n}{g}-1} g_{tg-1}^{q^{gs}} x^{q^{g(s+t)-1}}$. Assuming $i + 1 = p_1 g$, for some positive integer p_1, the coefficient of x^{q^i} of $f^*(x)$ is $\sum_{t=1}^{\frac{n}{g}-1} a_{p_1-t} g_{tg-1}^{q^{(p_1-t)g}}$. Let $n = p_2 g$, for some positive integer p_2, the coefficient of $x^{q^{n-1}}$ of $f^*(x)$ is $\sum_{t=1}^{\frac{n}{g}-1} a_{p_2-t} g_{tg-1}^{q^{(p_2-t)g}}$.

If $f^*(x) \in \mathcal{F}_{(i,h)}$, we have $f^*_{n-1} - \eta f_i^{*q^{n-1-i}} = 0$. Since $n-1-i = (p_2-p_1)g$,

$$f^*_{n-1} - \eta f_i^{*q^{n-1-i}} = \sum_{t=1}^{\frac{n}{g}-1} \left(a_t - \eta a_{t+\frac{i+1}{g}}^{q^{n-1-i}} \right) g_{(p_2-t)g-1}^{q^{tg}}.$$

By Lemma 14, we have $a_t = \eta a_{t+\frac{i+1}{g}}^{q^{n-1-i}}$, $t \in \{1, 2, \cdots, \frac{n}{g}-1\}$. Thus, the above equation is equal to 0 proving $\mathcal{F}^*_{(i,h)} \subseteq \mathcal{F}_{(i,h)}$.

Note that $|\mathcal{G}_{n-1}| = |\mathcal{F}_{(i,h)}| = q^{n(n-1)}$, and $|\mathcal{F}^*_{(i,h)}| = |A(x) \circ \mathcal{G}_{n-1}| = |\mathcal{G}_{n-1}|$, since $A(x)$ is invertible. Therefore, $|\mathcal{F}^*_{(i,h)}| = |\mathcal{F}_{(i,h)}|$. This implies that $\mathcal{F}_{(i,h)}$ is equivalent to the Gabidulin code $\mathcal{G}_{n-1}$.

The proof of the case when $h = 0$ is similar to that of $h = n-i-1$, by showing $\mathcal{F}_{(i,h)} = C(x) \circ \mathcal{G}_{n-1} \circ D(x)$, where $C(x) = x$ and $D(x) = \sum_{s=0}^{\frac{n}{g}-1} d_s x^{q^{gs}}$, $d_0 = 1$, $d_s = \eta^{q^{gs}} d_{s+\frac{i+1}{g}}$ for all $s \in \{1, \cdots, \frac{n}{g}-1\}$. Hence, the new family $\mathcal{F}_{(i,h)}$ is equivalent to the Gabidulin code $\mathcal{G}_{n-1}$, if $h = n-i-1$ or $h = 0$. ■

5.4.2 Comparison with Generalized Gabidulin codes

Lemma 16. *The Gabidulin code $\mathcal{G}_{n-1}$ is equivalent to the Generalized Gabidulin code $\mathcal{G}_{n-1,s}$.*

Proof. It can be verified that $\mathcal{G}_{n-1} \circ x^{q^{n-s+1}} = \mathcal{G}_{n-1,s}$. ■

Due to this equivalence, the following corollary follows.

Corollary 3. *Let $\mathcal{F}_{(i,h)}$ be defined in Theorem 11. The family $\mathcal{F}_{(i,h)}$ is not equivalent to the Generalized Gabidulin code $\mathcal{G}_{n-1,s}$ when $h \neq 0$ and $h \neq n-i-1$ with $0 \leq i \leq n-2$. When $h = n-i-1$ or $h = 0$, $\mathcal{F}_{(i,h)}$ is equivalent to $\mathcal{G}_{n-1,s}$.*

5.5 The Delsarte Dual of the Family $\mathcal{F}_{(i,h)}$

In this section, we focus on the Delsarte dual of $\mathcal{F}_{(i,h)}$. It helps us to confirm that our family is indeed a new family and not equivalent to the Delsarte dual of the existing families

with same dimension.

Theorem 14. *Let $\mathcal{F}_{(i,h)}$ be defined in Theorem 11. Then, the Delsarte dual of $\mathcal{F}_{(i,h)}$ is the dimension* 1 *code*

$$\mathcal{F}_{(i,h)}^{\perp} = \{f^* x^{q^i} - \eta^{-1} f^{*q^h} x^{q^{n-1}} : f^* \in \mathbb{F}_{q^n}\}.$$

Proof. By the Definition, we can get $\mathcal{F}_{(i,h)}^{\perp}$ from a straightforward calculation. ■

Now, we learn the comparison of the dual $\mathcal{F}_{(i,h)}^{\perp}$ with the Gabidulin code $\mathcal{G}_1$ and the Generalized Gabidulin code $\mathcal{G}_{1,s}$. Note that the Gabidulin code $\mathcal{G}_1$ is equal to the Generalized Gabidulin code $\mathcal{G}_{1,s}$. Hence, we only need to compare the family $\mathcal{F}_{(i,h)}^{\perp}$ with $\mathcal{G}_1$.

Corollary 4. *The family $\mathcal{F}_{(i,h)}^{\perp}$ is not equivalent to the Gabidulin code $\mathcal{G}_1$ when $h \neq 0$ and $h \neq n-i-1$. When $h = n-i-1$ or $h = 0$, $\mathcal{F}_{(i,h)}^{\perp}$ is equivalent to $\mathcal{G}_1$.*

Proof. It can be shown that proving equivalence of two codes is the same as proving the equivalence of their respective Delsarte dual. Furthermore, Lemma 2 [57] tells us that the Delsarte dual of $\mathcal{G}_1$ is equivalent to $\mathcal{G}_{n-1}$, by noting the results in Theorem 12 and Theorem 13 we complete our proof. ■

5.6 Note on Twisted and Generalized Twisted Gabidulin Codes

Firstly, we note that when the family [48] is $\mathbb{F}_q$-linear, it coincides with the Generalized Twisted Gabidulin codes. Since our family is $\mathbb{F}_q$-linear, it is sufficient to just compare it with $\mathbb{F}_q$-linear MRD codes. Hence, we only focus on Twisted Gabidulin codes and Generalized Twisted Gabidulin codes. In [57] Theorem 7, Sheekey claims that Generalized Twisted Gabidulin codes $\mathcal{H}_{k,s}(\eta, h)$ are not equivalent to Gabidulin codes $\mathcal{G}_k$ and Generalized Gabidulin codes $\mathcal{G}_{k,s}$ unless $k \in \{1, n-1\}$ and $h \in \{0, 1\}$. On the other hand, the

equivalences to Gabidulin codes for the dimension $k = 1$ or $n-1$, $h = 0$ or 1 are still open. Our proof uses the following proposition.

Proposition 2. *(see in [40]) Let n, k, s, h be positive integers satisfying $\gcd(n, s) = 1$, $k < n$ with $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\eta) \neq (-1)^{nk}, \eta \in \mathbb{F}_{q^n}$. The Delsarte dual code of $\mathcal{H}_{k,s}(\eta, h)$ is equivalent to the code $\mathcal{H}_{n-k,s}(-\eta^{q^{n-ks}}, n-h)$.*

Fixing $i = 0$, our new family $\mathcal{F}_{(i,h)}$ along with its dual $\mathcal{F}_{(i,h)}^{\perp}$ extends the family $\mathcal{H}_k(\eta, h)$ to dimension $k = 1$ and $k = n-1$. By Theorem 12 and Theorem 13, we give answers for those open problems.

Corollary 5. *Consider the Twisted Gabidulin Code $\mathcal{H}_k(\eta, h)$ with $1 \leq k \leq n-1$ and $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\eta) \neq (-1)^{kn}$. For $h \in \{0, \cdots, n-1\}$, we have*

- *If $k = 1, \mathcal{H}_1(\eta, h)$ is not equivalent to $\mathcal{G}_1$ if and only if $h \notin \{0, 1\}$.*
- *If $k = 2, \cdots, n-2, \mathcal{H}_k(\eta, h)$ is not equivalent to $\mathcal{G}_k$ for all h in [57].*
- *If $k = n-1, \mathcal{H}_{n-1}(\eta, h)$ is not equivalent to $\mathcal{G}_{n-1}$ if and only if $h \notin \{0, n-1\}$.*

Proof. By fixing $i = 0$, we have the family $\mathcal{F}_{(0,h)}$ to be equal to $\mathcal{H}_{n-1}(\eta, h)$. Based on Theorem 12 and Theorem 13, we accomplish the proof of the dimension $k = n-1$. To prove the case when $k = 1$, we use the fact that $\mathcal{H}_1(\eta, h)^{\perp}$ is equivalent to $\mathcal{H}_{n-1}(-\eta^{q^{n-1}}, n-h)$ by Proposition 2 with $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(-\eta^{q^{n-1}}) = N(-1) \cdot N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\eta^{q^{n-1}}) \neq 1$. The result follows by applying the result we proved earlier for the case $k = n-1$. ■

Remark 11. In [57], it was shown that the family $\mathcal{H}_k(\eta, h)$ is not equivalent to $\mathcal{G}_k$ unless $k \in \{1, n-1\}$ and $h \in \{0, 1\}$. However, our corollary shows that the condition $k \in \{1, n-1\}$ and $h \in \{0, 1\}$ does not guarantee that $\mathcal{H}_k(\eta, h)$ is equivalent to $\mathcal{G}_k$. For instance, when $k = n-1$ and $h = 1$ for all n, the Twisted Gabidulin code $\mathcal{H}_{n-1}(\eta, h)$ is not equivalent to $\mathcal{G}_{n-1}$ from the above corollary.

Lastly, we investigate the Generalized Twisted Gabidulin code $\mathcal{H}_{k,s}(\eta, h)$ of dimension $k = n-1$ and $k = 1$.

Corollary 6. *Consider the Generalized Twisted Gabidulin code* $\mathcal{H}_{k,s}(\eta, h)$ *with* $\gcd(s, n) = 1$, $1 \leq k \leq n-1$ *and* $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\eta) \neq (-1)^{kn}$. *Then, for* $h \in \{0, \cdots, n-1\}$, *we have*

- *If* $k = 1, \mathcal{H}_{1,s}(\eta, h)$ *is not equivalent to* $\mathcal{G}_{1,s}$ *if and only if* $h \notin \{0, s\}$.
- *If* $k = 2, \cdots, n-2, \mathcal{H}_{k,s}(\eta, h)$ *is not equivalent to* $\mathcal{G}_{k,s}$ *for all* h *in [40].*
- *If* $k = n-1, \mathcal{H}_{n-1,s}(\eta, h)$ *is not equivalent to* $\mathcal{G}_{n-1,s}$ *if and only if* $h \notin \{0, n-s\}$.

Proof. Fixing $i = 0$, the family $\mathcal{F}_{(0,h;s)}$ is equal to $\mathcal{H}_{n-1,s}(\eta, h)$. We know the family $\mathcal{F}_{(0,h;s)}$ is equivalent to $\mathcal{F}_{(s-1,h)}$ by Lemma 14, and $\mathcal{G}_{n-1,s}$ is equivalent to $\mathcal{G}_{n-1}$ by Lemma 16. Thus, we have $\mathcal{H}_{n-1,s}(\eta, h)$ not to be equivalent to $\mathcal{G}_{n-1,s}$ when $h \neq 0, n-s$ and to be equivalent otherwise by Theorem 12 and Theorem 13. When $k = 1$, we know that $\mathcal{H}_{1,s}(\eta, h)^{\perp}$ is equivalent to $\mathcal{H}_{n-1,s}(-\eta^{q^{n-s}}, n-h)$ by Proposition 2 with $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(-\eta^{q^{n-s}}) = N(-1) \cdot N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\eta^{q^{n-s}}) \neq 1$. The family $\mathcal{H}_{n-1,s}(-\eta^{q^{n-s}}, n-h)$ is equal to the family $\mathcal{F}_{(0,n-h;s)}$, and $\mathcal{F}_{(0,n-h;s)}$ is equivalent to $\mathcal{F}_{(s-1,n-h)}$ by Lemma 14. The Delsarte dual of $\mathcal{G}_1$ is equivalent to $\mathcal{G}_{n-1}$. The result follows by applying the result we proved earlier for the case $k = n-1$. ■

5.7 Conclusion

In this chapter, we constructed a new family $\mathcal{F}_{(i,h)}$ of $\mathbb{F}_q$-linear MRD codes by considering the last coefficient to be an $\mathbb{F}_q$-linear function of one of the other coefficients. The new family is not equivalent to the Gabidulin code and the Generalized Gabidulin code with $h \neq 0$ and $h \neq n-i-1$ and is equivalent otherwise, which is summarized in Table 5.1.

Table 5.1: Comparsion with (Generalized) Gabidulin Codes

Our family $\mathcal{F}_{(i,h)}$	Gabidulin codes $\mathcal{G}_{n-1}$	Generalized Gabidulin codes $\mathcal{G}_{n-1,s}$
$h \neq 0, n-i-1$	Not equivalent	Not equivalent
$h = 0, n-i-1$	Equivalent	Equivalent

Comparing the Delsarte dual of $\mathcal{F}_{(i,h)}$ with the existing families, we obtain similar result to give us another family of MRD codes of dimension 1. Furthermore, our family $\mathcal{F}_{(i,h)}$ along with its dual $\mathcal{F}_{(i,h)}^{\perp}$ extends Twisted Gabidulin codes and Generalized Twisted Gabidulin codes to dimension $k = 1$ and $k = n - 1$, which fills the gap [57]. The results are summarized in Table 5.2.

Table 5.2: Note on (Generalized) Twisted Gabidulin Codes

k	h	$\mathcal{H}_k(\eta, h)$
1	$\neq 0,1$	Not equivalent to $\mathcal{G}_1$
$2, \cdots, n-2$	all	Not equivalent $\mathcal{G}_k$ [40]
$n-1$	$\neq 0, n-1$	Not equivalent $\mathcal{G}_{n-1}$
k	h	$\mathcal{H}_{k,s}(\eta, h)$
1	$\neq 0, s$	Not equivalent to $\mathcal{G}_{1,s}$
$2, \cdots, n-2$	all	Not equivalent $\mathcal{G}_{k,s}$ [57]
$n-1$	$\neq 0, n-s$	Not equivalent $\mathcal{G}_{n-1,s}$

For $i \neq 0$, we conjecture our family are not equivalent to Twisted Gabidulin codes and Generalized Twisted Gabidulin codes of the same dimension.

Chapter 6

List Decoding of Cover-metric Codes up to the Singleton Bound

This chapter is based on the work in [39]. A. Wachter-Zeh [65] showed that every cover-metric code can be list decoded up to the Johnson-like bound. Furthermore, it was shown that efficient list decoding of cover-metric codes up to the Johnson-like bound can be performed in [65]. From the work of [65], one natural question is whether the Johnson-like bound can be improved. In this chapter, we give a confirmative answer to this question by showing that cover-metric codes can be list decoded with the Singleton bound as their list decoding radius. Our contributions consist of three parts. Firstly, we prove that the list decodability of cover-metric codes does not exceed the Singleton bound. Secondly, our results reveal that a random cover-metric code can be list decoded up to the Singleton bound with high probability, which is better than the Johnson-like bound. Thirdly, by applying some existing decoding algorithms for Hamming metric and rank-metric codes, we present explicit constructions of cover-metric codes that can be efficiently list decoded up to the Singleton bound.

6.1 Introduction

The columns and rows of data stored in an array can be corrupted by crisscross errors. Such error can be found in various communication systems and data storages such as hard disc write processes, orthogonal frequency division multiplexing (OFDM) systems and flash memories [12], [4], [52] and [55]. To better combat this error, the cover-metric was proposed and cover-metric codes were defined in [55]. The cover-metric code is a set of $n \times m$ matrices over $\mathbb{F}_q$ (throughout this chapter, we assume $n \leq m$, otherwise we can consider the transpose of matrices).

Unique decoding of cover-metric codes has been extensively studied and investigated in [3], [56] and [59]. In particular, one can uniquely decode a cover-metric code up to half of its minimum distance d_{C}. The rate R and relative distance δ are defined to be $\frac{\log_q |\mathsf{C}|}{mn}$ and $\frac{d_{\mathsf{C}}-1}{n}$, respectively. By the Singleton bound $R + \delta \leq 1$ [55], the decoding radius τn ($\tau \in (0, 1)$) satisfies $\tau \leq \delta/2 \leq (1 - R)/2$. Thus $(1 - R)/2$ is the upper bound of unique decoding radius. To surpass this limit, one has to consider list decoding. List decoding of cover-metric codes was firstly considered in [65]. It was shown that cover-metric code can be list decoded up to a Johnson-like bound $\tau_J = 1 + \frac{n}{m} - \sqrt{(1 + \frac{n}{m})(1 + \frac{n-d_{\mathsf{C}}}{m})}$. In the case where $m = n$, we get the Johnson-like bound $\tau_J = 2 - \sqrt{2(2 - \delta)}$. Then, a question arises whether one can do better in the list decoding issue of cover-metric codes. In other words, can cover-metric codes be list decoded beyond the Johnson-like bound?

Previous results

List decoding of cover-metric codes was first considered in [65]. One of the open problems in [65] is: What is the limit of the list decoding radius of cover-metric codes? There are mainly two results in [65]. The first result shows that cover-metric code can be list decoded up to the Johnson-like bound. Secondly, it was shown that every list decodable Hamming metric code with list decoding radius τ_{H} can be used to efficiently construct a cover-metric code with decoding radius $\min\{\tau_{\mathsf{H}}, \tau_J\}$. Thus, in the case of $n = m$, one

can list decode cover-metric codes up to the bound $\min\{1-\sqrt{R}, 2-\sqrt{2(2-\delta)}\}$. The explicit construction in [65] reaching this bound is to write the Reed-Solomon codes into the matrix via a diagonal construction. Since $2-\sqrt{2(2-\delta)} \leq 2-\sqrt{2(1+R)} < 1-\sqrt{R}$ for $R \in [0,1)$ and $\delta \in (0,1]$, the explicit decoding algorithm in [65] gave list decoding radius that is strictly less than $1-\sqrt{R}$ no matter which Hamming metric codes are used.

On the other hand, the rank weight of a matrix is at most its cover weight. As a result, the rank-metric codes under cover-metric automatically attain the Singleton bound [56]. We note that such codes can be constructed over any finite field. However, they may not even be list decodable [54]. Another consequence is that a list decodable rank-metric code is also a list decodable cover-metric code. In [27] and [26], it was shown that one can efficiently list decode a rank-metric code up to the Singleton bound if the ratio $\rho = \frac{n}{m}$ (the number of rows over the number of columns) is sufficiently small. Thus, such a code is also list decodable up to the Singleton bound under the cover-metric errors. This already answers our question when the ratio ρ is sufficiently small.

Our results

To see whether we can list decode cover-metric codes beyond the Johnson-like bound, we first investigate the list decodable cover-metric codes and then study the list decoding of random cover-metric codes. Our results consist of three parts. Firstly, we show that the list decodability of the cover-metric codes does not exceed the Singleton bound regardless of alphabet size q and the ratio $\rho = \frac{n}{m}$. Secondly, we show that, regardless of the alphabet size and the ratio ρ, a random cover-metric code can be list decoded up to the Singleton bound with high probability, which is better than the Johnson-like bound. Thirdly, by applying existing decoding algorithms for Hamming metric codes, one can efficiently list decode cover-metric codes up to the Singleton bound if either the alphabet size depends on m, the size of the matrix or the list size is not a polynomial in m (although the list size is almost a polynomial in m). Unlike the case of rank-metric codes, the explicit construction

of cover-metric codes is independent of the ratio ρ.

Organization

This chapter is organized as follows. Firstly, we show the Singleton bound of cover-metric codes. Secondly, we derive a limit to the list decoding of the cover-metric codes, i.e., the Singleton bound. Furthermore, we show that a random cover-metric code can be list decoded up to the Singleton bound. Then, we present explicit constructions of cover-metric codes that can be list decoded up to the Singleton bound. Finally ,we draw a conclusion.

6.2 Preliminaries

Let $\mathbf{x}$ be a vector in $\mathbb{F}_q^n$. The Hamming weight of $\mathbf{x}$ is denoted by $\mathrm{wt}_{\mathsf{H}}(\mathbf{x})$. A q-ary Hamming metric code $\mathbf{C}$ of length n is a subset of $\mathbb{F}_q^n$. The code $\mathbf{C}$ is called $(\tau n, \mathcal{L})^{\mathsf{H}}$-list decodable if for every word $\mathbf{u} \in \mathbb{F}_q^n$, the intersection of $\mathbf{C}$ with the Hamming ball $\{\mathbf{x} \in \mathbf{C} : \ \mathrm{wt}_{\mathsf{H}}(\mathbf{x} - \mathbf{u}) \leq \tau \mathbf{n}\}$ has size at most $\mathcal{L}$, here the parameter $\mathcal{L}$ is called the list size. The previous definition of cover-metric, we define in the Chapter 2.

In [55] and [13], it was shown that any linear cover-metric code C must obey the Singleton bound, i.e, $R(\mathsf{C}) + \delta(\mathsf{C}) \leq 1$. In fact, this is also true for nonlinear cover-metric codes.

Lemma 17. *Every cover-metric code* C *must obey the Singleton bound:* $R(\mathsf{C}) + \delta(\mathsf{C}) \leq 1$.

Proof. Let $\mathsf{C} \subseteq \mathbb{F}_{\mathsf{q}}^{\mathsf{n} \times \mathsf{m}}$ be a cover-metric code of minimum distance d. Remove the last $d-1$ columns of every matrix in C to get a cover-metric code $\mathsf{C}' \subseteq \mathbb{F}_q^{(n-d_{\mathsf{C}}+1)\times m}$. It is clear that $|\mathsf{C}'| = |\mathsf{C}|$ as $d(\mathsf{C}) \geq \mathsf{d_C}$ and we remove only $d-1$ columns. Thus, we have

$$R(\mathsf{C}) = \frac{\log_{\mathsf{q}} |\mathsf{C}|}{\mathsf{mn}} = \frac{\log_{\mathsf{q}} |\mathsf{C}'|}{\mathsf{mn}} \leq \frac{\log_{\mathsf{q}} \left|\mathbb{F}_{\mathsf{q}}^{(\mathsf{n}-\mathsf{d_C}+1)\times \mathsf{m}}\right|}{\mathsf{mn}} = \frac{\mathsf{m}(\mathsf{n}-\mathsf{d_C}+1)}{\mathsf{mn}} = 1 - \delta(\mathsf{C}).$$

■

By $[n \times m, k, d_{\mathsf{C}}]_q^{\mathsf{C}}$, we denote an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{n \times m}$ of minimum cover distance d_{C} and dimension k. In this case, we have $d_{\mathsf{C}} = \min_{A \in \mathcal{C}, A \neq 0} \mathrm{wt}_{\mathsf{C}}(A)$. In contrast, we denote by $[n, k, d]_q^{\mathsf{H}}$ an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ of minimum Hamming distance d and dimension k.

6.3 List Decodability of Cover-metric Codes

6.3.1 Limit of list decodability

In this subsection, we show that list decoding of every cover-metric code cannot exceed the Singleton bound. The idea of our proof is based on counting matrices in a cover-metric ball. Let us fix a positive ratio $\rho = \frac{n}{m}$ throughout this chapter. Thus, when the number n of rows tends to ∞, the number m of columns tends to ∞ as well.

Lemma 18. *Given a matrix $A \in \mathbb{F}_q^{n \times m}$, the size of the cover-metric ball $\mathcal{B}_{\mathsf{C}}(A, d)$ is upper bounded by*

$$|\mathcal{B}_{\mathsf{C}}(A, d)| \leq (d+1) \times 2^{(m+n)H_2\left(\frac{d}{m+n}\right)} q^{md},$$

where $H_2(x)$ is the binary entropy function, where $H_2(x) := -x \log_2(x) - (1-x) \log_2(1-x)$.

Proof. Let B be a matrix in $\mathcal{B}_{\mathsf{C}}(A, d)$ and consider a minimum cover (X, Y) of $A - B$. Let $r = |X| + |Y|$ with $|X| = i$ and $|Y| = j$. The maximum number of nonzero entries covered by X and Y is $nj + mi - ij \leq mi + mj - ij \leq mr$. Thus, if we fix X and Y, the total number of matrices B is upper bounded by q^{mr}. Since there are $\binom{n}{i}$ different row sets Y

and $\binom{m}{j}$ different column sets X. It follows that the size of $\mathcal{B}_{\mathsf{C}}(A,d)$ is upper bounded by

$$\begin{aligned}|\mathcal{B}_{\mathsf{C}}(A,d)| &\leq \sum_{r=0}^{d}\sum_{i+j=r}\binom{n}{i}\binom{m}{j}q^{mr}\\ &= \sum_{r=0}^{d}\binom{m+n}{r}q^{mr}\\ &\leq (d+1)\times 2^{(m+n)H_2\left(\frac{d}{m+n}\right)}q^{md}.\end{aligned}$$

■

Denote by $A_q(m,n,\delta n)$ the maximum cardinality of cover-metric codes with minimum cover distance δn in $\mathbb{F}_q^{n\times m}$. By [55] and [56], one knows the exact values of $A_q(m,n,\delta n)$, i.e., $A_q(m,n,\delta n)=q^{m(n-\delta n+1)}$.

On the other hand, it is interesting to look at the Gilbert-Varshamov bound for the cover-metric codes. The Gilbert-Varshamov bound is an upper bound for the list decoding radius of codes under both Hamming metric codes [24] and linear rank-metric codes [8]. Thus, any codes under Hamming metric or rank-metric (given that it is linear) that are list decoded beyond this bound will output an exponential list size. A natural question raises that the Gilbert-Varshamov bound may also be the limit to the list decoding of cover-metric codes (indeed it is true, see Theorems 16 and 17).

Proposition 3 (Gilbert-Varshamov Bound)**.**

$$\lim_{n\to\infty}\frac{\log_q A_q(m,n,\delta n)}{mn}\geq 1-\delta.$$

Proof. Since there are at most $(\delta n+1)\times 2^{(m+n)H_2\left(\frac{\delta n}{m+n}\right)}q^{\delta mn}$ matrices within δn cover distance from a given matrix, by using the standard Gilbert-Varshamov arguments, we have

$$A_q(m,n,\delta n)\geq\frac{q^{mn}}{(\delta n+1)\times 2^{(m+n)H_2\left(\frac{\delta n}{m+n}\right)}q^{\delta mn}}.$$

Taking $\log_q$ and dividing mn on both sides gives

$$\begin{aligned}\frac{\log_q A_q(m,n,\delta n)}{mn} &\geq 1-\delta-\left(\frac{1}{m}+\frac{1}{n}\right)H_2\left(\frac{\delta n}{m+n}\right)-\frac{1}{mn}\log_q(\delta n+1)\\ &\geq 1-\delta-\left(\frac{1}{m}+\frac{1}{n}\right)-\frac{1}{mn}\log_q(\delta n+1).\end{aligned}$$

The second inequality follows from the binary entropy function $H_2(x)$ takes values between 0 and 1. Let n tend to infinity and we can obtain the desired result. ■

The above result shows that the asymptotic Gilbert-Varshamov bound coincides with the Singleton bound for cover-metric codes. In contrast, the asymptotic Gilbert-Varshamov bound and the Singleton bound are different for both Hamming metric and rank-metric codes.

To study the list decodability of cover-metric codes, we derive a lower bound on the size of a cover-metric ball.

Lemma 19. *Given a matrix $A \in \mathbb{F}_q^{n\times m}$, the size of the cover-metric ball $\mathcal{B}_{\mathsf{C}}(A,d)$ is lower bounded by*

$$|\mathcal{B}_{\mathsf{C}}(A,d)| \geq q^{md}.$$

Proof. To prove this bound, we count the number of matrices with all nonzero entries in the first d columns and all zero entries in the last $n-d$ columns. Every such matrix belongs to the ball $\mathcal{B}_{\mathsf{C}}(O,d)$, where O presents for the zero matrix. The total number of such matrices is q^{md}. The desired result follows from the fact that $\mathcal{B}_{\mathsf{C}}(A,d) = \mathcal{B}_{\mathsf{C}}(O,d)$. ■

Remark 12. Note that we did not try to optimize the bounds in Lemmas 18 and 19 as they give the same asymptotic bound. Namely, if d/n tends to a fixed real $\delta \in (0,1)$, we have that

$$\lim_{n\to\infty}\frac{\log_q|\mathcal{B}_{\mathsf{C}}(A,d)|}{mn} = \delta$$

by Lemmas 18 and 19.

Let us conclude this subsection by showing the list decodability of cover-metric codes.

Theorem 15. *A cover-metric code of rate R in $\mathbb{F}_q^{n\times m}$ is $(\tau n, \mathcal{L})^{\mathsf{C}}$-list decodable with list size $\mathcal{L} = \mathrm{poly}(m,n)$[1] then $\tau \leq 1 - R$.*

Proof. Let $\mathcal{C}$ be a cover-metric code of rate R in $\mathbb{F}_q^{n\times m}$. Suppose that $\mathcal{C}$ is $(\tau n, \mathcal{L})^{\mathsf{C}}$-list decodable with $\tau > 1 - R$. Then, there is a real $\epsilon \in (0,1)$ such that $\tau \geq 1 - R + \epsilon$.

Consider the matrix indexed by $\mathbb{F}_q^{n\times m} \times \mathcal{C}$ where the (B, A)-th entry δ_{BA} satisfies

$$\delta_{BA} = \begin{cases} 1 & \text{if } A \in \mathcal{B}_{\mathsf{C}}(B, \tau n) \\ 0 & \text{otherwise.} \end{cases}$$

In rows if we count the total number of $1's$ of this matrix, it is given by $\sum_{B\in\mathbb{F}_q^{n\times m}} |\mathcal{B}_{\mathsf{C}}(B,\tau n)\cap \mathcal{C}|$. On the other hand, if we count the total number of $1's$ of this matrix in columns, it is given by $\sum_{A\in\mathcal{C}} |\mathcal{B}_{\mathsf{C}}(A,\tau n)|$. Thus, we have

$$\sum_{B\in\mathbb{F}_q^{n\times m}} |\mathcal{B}_{\mathsf{C}}(B,\tau n)\cap\mathcal{C}| = \sum_{A\in\mathcal{C}} |\mathcal{B}_{\mathsf{C}}(A,\tau n)| = |\mathcal{C}||\mathcal{B}_{\mathsf{C}}(O,\tau n)| \geq q^{Rmn}\times q^{\tau mn},$$

where the second equality follows from that $|\mathcal{B}_{\mathsf{C}}(A,\tau n)|$ is independent of the center, and the last inequality follows from Lemma 19.

By the Pigeonhole Principle, there exists $C \in \mathbb{F}_q^{n\times m}$ such that

$$|\mathcal{B}_{\mathsf{C}}(C,\tau n)\cap\mathcal{C}| \geq q^{Rmn+\tau mn-mn} \geq q^{\epsilon mn}. \tag{6.1}$$

■

The above theorem tells that any cover-metric codes cannot be list decoded beyond the Singleton bound. In the next section, we will show that a random cover-metric code can actually be list decoded up to the Singleton bound with high probability.

[1] $\mathrm{poly}(m,n)$ means a polynomial in both m and n.

6.3.2 List decoding of random cover-metric codes

In this subsection, we investigate the list decodability of random cover-metric codes. Our results reveal that with high probability, random codes can be list decoded up to the Singleton bound. In particular, most cover-metric codes with rate R can be list decoded up to the Singleton bound $\tau = 1 - R - \epsilon$ with constant list size $O(1/\epsilon)$, while most $\mathbb{F}_q$-linear cover-metric codes with rate R can be list decoded up to the Singleton bound $\tau = 1 - R - \epsilon$ with list size $\exp(O(1/\epsilon))$.

Theorem 16. *For every small $\epsilon \in (0, 1)$, with a probability at least $1 - 2^{-mn/2}$, a random cover-metric code $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ of rate R is $((1 - R - \epsilon)n, O(1/\epsilon))^{\mathsf{C}}$-list decodable for all $n \geq \frac{8}{\epsilon}$.*

Proof. Let $\mathcal{L} = \left\lceil \frac{2}{\epsilon} \right\rceil - 1$. We choose sufficiently large positive integers m, n satisfying $m \geq n \geq \frac{8}{\epsilon}$. Pick a cover-metric code $\mathcal{C}$ with size q^{Rmn} uniformly at random. We calculate the probability that $\mathcal{C}$ is not $(\tau n, \mathcal{L})^{\mathsf{C}}$-list decodable.

If $\mathcal{C}$ is not $(\tau n, \mathcal{L})^{\mathsf{C}}$-list decodable, there exists a matrix $A \in \mathbb{F}_q^{n\times m}$ and a subset $\mathcal{S} \subseteq \mathcal{C}$ with $|\mathcal{S}| = \mathcal{L} + 1$ such that $\mathcal{S} \subseteq \mathcal{B}_{\mathsf{C}}(A, \tau n)$. Given a matrix $A \in \mathbb{F}_q^{n\times m}$, by Lemma 18, the probability that one codeword $C \in \mathcal{C}$ is contained in $\mathcal{B}_{\mathsf{C}}(A, \tau n)$ is

$$Pr[C \in \mathcal{B}_{\mathsf{C}}(A, \tau n)] = \frac{|\mathcal{B}_{\mathsf{C}}(A, \tau n)|}{q^{mn}} \leq (\tau n + 1) \times 2^{(m+n)H_2\left(\frac{\tau n}{m+n}\right)} q^{m(\tau n - n)}. \tag{6.2}$$

Let $E_{A,\mathcal{S}}$ be the event that all codewords in $\mathcal{S}$ are contained in $\mathcal{B}_{\mathsf{C}}(A, \tau n)$. By Equation (6.2), we have

$$Pr[E_{A,S}] \leq \left(\frac{|\mathcal{B}_{\mathsf{C}}(A, \tau n)|}{q^{mn}}\right)^{\mathcal{L}+1} \leq \left((\tau n + 1) \times 2^{(m+n)H_2\left(\frac{\tau n}{m+n}\right)} q^{m(\tau n - n)}\right)^{\mathcal{L}+1}.$$

Taking the union bound over all q^{mn} choices for A and $\mathcal{S}$ over any $(\mathcal{L} + 1)$-subsets of $\mathcal{C}$, we

have

$$\begin{aligned}
\sum_{A,\mathcal{S}} Pr[E_{A,\mathcal{S}}] &\leq q^{mn}\binom{|\mathcal{C}|}{\mathcal{L}+1}\Big((\tau n+1)\times 2^{(m+n)H_2\left(\frac{\tau n}{m+n}\right)}q^{m(\tau n-n)}\Big)^{\mathcal{L}+1} \\
&\leq q^{mn}|\mathcal{C}|^{\mathcal{L}+1}(\tau n+1)^{\mathcal{L}+1}\times 2^{(m+n)H_2\left(\frac{\tau n}{m+n}\right)(\mathcal{L}+1)}q^{m(\tau n-n)(\mathcal{L}+1)} \\
&\leq q^{mn}q^{Rmn(\mathcal{L}+1)}(\tau n+1)^{\mathcal{L}+1}\times 2^{(m+n)(\mathcal{L}+1)}q^{m(\tau n-n)(\mathcal{L}+1)} \\
&= 2^{2mn(\mathcal{L}+1)\left(\frac{1}{n}+\frac{1}{m}\right)}q^{mn(\mathcal{L}+1)\left(R+\tau-1+\frac{1}{\mathcal{L}+1}\right)} \leq 2^{mn\cdot\frac{2}{\epsilon}\cdot\frac{\epsilon}{4}}q^{-mn} \\
&\leq 2^{-\frac{1}{2}mn}.
\end{aligned}$$

■

If we replace arbitrary random cover-metric codes with random $\mathbb{F}_q$-linear cover-metric codes in the above lemma, we get the same decoding radius, but with the list size becoming $\exp(O(1/\epsilon))$.

Theorem 17. *For every small $\epsilon \in (0,1)$, with a probability at least $1-2^{-mn/2}$, a random $\mathbb{F}_q$-linear cover-metric code $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ of rate R is $((1-R-\epsilon)n, \exp(O(1/\epsilon)))^{\mathsf{C}}$-list decodable for all $n \geq \frac{8}{\epsilon}$.*

Proof. Let $\mathcal{L} = q^{\lceil\frac{2}{\epsilon}\rceil}-1$. Then we have $\log_q(\mathcal{L}+1) = \lceil\frac{2}{\epsilon}\rceil$ and $\mathcal{L} = \exp(O(\frac{1}{\epsilon}))$. We choose sufficiently large integers m, n satisfying $m, n \geq \frac{8}{\epsilon}$. Pick Rmn $\mathbb{F}_q$-linearly independent matrices uniformly at random from $\mathbb{F}_q^{n\times m}$. The $\mathbb{F}_q$-linear cover-metric code $\mathcal{C}$ spanned by these matrices has rate R. If $\mathcal{C}$ is not $(\tau n, \mathcal{L})^{\mathsf{C}}$-list decodable, then there exists a matrix $A \in \mathbb{F}_q^{n\times m}$ and a subset $\mathcal{S} \subseteq \mathcal{C}$ with $|\mathcal{S}| = \mathcal{L}+1$ such that $\mathcal{S} \subseteq \mathcal{B}_{\mathsf{C}}(A, \tau n)$. There are at least $\mathcal{L}' = \log_q(\mathcal{L}+1) = \lceil\frac{2}{\epsilon}\rceil$ codewords in $\mathcal{S}$, which are $\mathbb{F}_q$-linearly independent. Let $\mathcal{S}'$ be the $\mathbb{F}_q$-linear span of these $\mathcal{L}'$ codewords, thus $\mathcal{S}' \subseteq \mathcal{S}$. Then,

$$\begin{aligned}
Pr[E_{A,\mathcal{S}}] \leq Pr[E_{A,\mathcal{S}'}] &= \left(\frac{|\mathcal{B}_{\mathsf{C}}(A,\tau n)|}{q^{mn}}\right)^{\mathcal{L}'} \\
&\leq \Big((\tau n+1)\times 2^{(m+n)H_2\left(\frac{\tau n}{m+n}\right)}q^{m(\tau n-n)}\Big)^{\mathcal{L}'}.
\end{aligned}$$

Taking the union bound over all q^{mn} choices for A and any $\mathcal{L}'$ $\mathbb{F}_q$-linearly independent

matrices from $\mathcal{C}$, we can derive the following probability.

$$\begin{aligned}
\sum_{\mathbf{v},S} Pr[E_{A,\mathcal{S}}] &\leq q^{mn}\binom{|\mathcal{C}|}{\mathcal{L}'}\Big((\tau n+1)\times 2^{(m+n)H_2\left(\frac{\tau n}{m+n}\right)}q^{m(\tau n-n)}\Big)^{\mathcal{L}'} \\
&\leq q^{mn}|\mathcal{C}|^{\mathcal{L}'}(\tau n+1)^{\mathcal{L}'}\times 2^{(m+n)H_2\left(\frac{\tau n}{m+n}\right)\mathcal{L}'}q^{m(\tau n-n)\mathcal{L}'} \\
&\leq q^{mn}q^{Rmn\mathcal{L}'}(\tau n+1)^{\mathcal{L}'}\times 2^{(m+n)\mathcal{L}'}q^{m(\tau n-n)\mathcal{L}'} \\
&= 2^{2mn\mathcal{L}'\left(\frac{1}{n}+\frac{1}{m}\right)}q^{mn\mathcal{L}'(R+\tau-1+\frac{1}{\mathcal{L}'})} \leq 2^{mn\cdot\frac{2}{\epsilon}\cdot\frac{\epsilon}{4}}q^{-mn} \\
&\leq 2^{-\frac{1}{2}mn}.
\end{aligned}$$

■

6.4 Explicit Constructions

Our arguments in the previous section show that random cover-metric codes can be list decoded up to the Singleton bound regardless of the field size q and the ratio ρ. The main purpose of this section is to explicitly list decode cover-metric codes up to the Singleton bound by converting either rank-metric codes or Hamming metric codes to cover-metric codes. However, in order to efficiently list decode cover-metric codes up to the Singleton bound, one has to sacrifice either the ratio ρ or the field size q. In [65], although the Johnson-like bound holds for cover-metric codes over any finite field, the explicit construction reaching this bound also requires that the field size is a function of the matrix size.

Let us firstly state the result by converting rank-metric codes to cover-metric codes.

Theorem 18. *For every small real $\epsilon > 0$ and $\rho = O(\epsilon^2)$, there exists a q-ary cover-metric code of rate R in $\mathbb{F}_q^{\rho m\times m}$ which is $((1-R-\epsilon)n, \exp(O(1/\epsilon)))^{\mathsf{C}}$-list decodable. Furthermore, the algorithm can be performed in time $\mathrm{poly}(m, \frac{1}{\epsilon})$.*

Proof. By [27] and [26], there exists a q-ary rank-metric code $\mathcal{C}$ of rate R in $\mathbb{F}_q^{\rho m\times m}$ which is $((1-R-\epsilon)n, \exp(O(1/\epsilon)))^{\mathsf{R}}$-list decodable and the algorithm can be performed in time $\mathrm{poly}(m, \frac{1}{\epsilon})$. It is clear that $\mathcal{C}$ is also $((1-R-\epsilon)n, \exp(O(1/\epsilon)))^{\mathsf{C}}$-list decodable by using

the same decoding algorithm since all the codewords in a ball $\mathcal{B}_{\mathsf{C}}(A, \tau n)$ are contained in the rank-metric ball $\mathcal{B}_{\mathsf{R}}(A, \tau n)$. ■

In the rest of this section, we show that by converting a list decodable Hamming metric code to a list decodable cover-metric code, we can list decode cover-metric codes up to the Singleton bound.

Theorem 19. *Let* $\mathbf{C}$ *be a Hamming metric code of length* mn *over* $\mathbb{F}_q$*. If* $\mathbf{C}$ *is* $(\tau n, \mathcal{L})^{\mathsf{H}}$*-list decodable with time complexity* $D_{\mathsf{H}}(\mathbf{C})$*. Then, there exists a cover-metric code* $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ *such that* $\mathcal{C}$ *is* $(\tau n, \mathcal{L})^{\mathsf{C}}$*-list decodable with the same time complexity.*

Proof. We convert each codeword in $\mathbf{C}$ into an $n \times m$ matrix by placing the first m coordinates as the first row, the second m coordinates as the second row, and so on. Thus, we form a cover-metric code $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$. We will show that $\mathcal{C}$ is the cover-metric code with desired list decodability and time complexity. The decoding algorithm works as follows.

1. Let B be the received matrix and form a vector $\boldsymbol{b} \in \mathbb{F}_q^{mn}$ by placing the first row of B as the first coordinates, the second row of B as the second m coordinates and so on.

2. Use the list decoding algorithm of $\mathbf{C}$ to decode vector $\boldsymbol{b}$ to list $\mathbf{L}$ of size $\mathcal{L}$.

3. Convert each codeword in $\mathcal{L}$ into a matrix in $\mathcal{C}$.

From the above description of our decoding algorithm, the list size is still $\mathcal{L}$. Now we have to show that any matrix within cover distance τn from B is contained in this list.

Let a matrix $C \in \mathcal{C}$ with $d_{\mathsf{C}}(B, C) \leq \tau n$. There must exist i rows and j columns covering all the errors such that $i + j \leq \tau n$. We count the maximum number of entries which may be corrupted. The number is at most $nj + mi - ij \leq \tau mn$. Note that when we convert an $n \times m$ matrix into a vector of length mn, the error in Hamming metric is exactly the number of corrupted entries. The list decoding algorithm of $\mathbf{C}$ will output codewords within Hamming distance τmn from $\boldsymbol{b}$. It follows that this matrix is in the list of our list decoding algorithm. ■

We have shown that a Hamming metric list decodable code of length mn can be converted to a cover-metric code in $\mathbb{F}_q^{n\times m}$ with the same list decoding radius. However, in most cases, Hamming metric codes may not have the length equal to mn. The following lemma shows that by deleting a negligible set of coordinates one can obtain the desired length mn.

Theorem 20. *Fix a real $\rho \in (0,1)$. Suppose that there exists a Hamming metric code of length N and rate R that is $(\tau_{\mathsf{H}}N, \mathcal{L})^{\mathsf{H}}$-list decodable. Then, there exists a cover-metric code in $\mathbb{F}_q^{n\times m}$ of rate at least $R - 3\sqrt{\frac{1}{\rho N}}$ which is $(\tau_{\mathsf{C}}n, \mathcal{L})^{\mathsf{C}}$-list decodable, where $m = \lfloor\sqrt{N/\rho}\rfloor$, $n = \lfloor\rho m\rfloor$ and $\tau_{\mathsf{C}} = \tau_{\mathsf{H}} - 3\sqrt{\frac{1}{\rho N}}$.*

Proof. Let $\mathbf{A} \subseteq \mathbb{F}_q^N$ be a Hamming metric code of rate R that is a $(\tau_{\mathsf{H}}N, \mathcal{L})^{\mathsf{H}}$-list decodable code. Put $m = \lfloor\sqrt{N/\rho}\rfloor$ and $n = \lfloor\rho m\rfloor$. Then $mn \leq \rho m^2 \leq N$ and $mn \geq (\rho m - 1)m \geq (\rho(\sqrt{N/\rho} - 1) - 1)(\sqrt{N/\rho} - 1) \geq N - 3\sqrt{N/\rho}$. Deleting the last $N - mn$ coordinates of every codeword in $\mathbf{A}$ gives a Hamming metric code $\mathbf{C}$ of length mn of size at least $|\mathbf{A}|/q^{N-mn}$. Now we convert $\mathbf{C}$ into a cover-metric code $\mathcal{C}$ of $\mathbb{F}_q^{n\times m}$. The rate of $\mathcal{C}$ is the same as the one of $\mathbf{C}$ which is equal to

$$R(\mathcal{C}) = \frac{\log_q |\mathbf{C}|}{mn} \geq \frac{\log_q(|\mathbf{A}|/q^{N-mn})}{N} \times \frac{N}{mn} \geq R - \frac{N-mn}{N} \geq R - 3\sqrt{\frac{1}{\rho N}}.$$

Once we receive a matrix $B \in \mathbb{F}_q^{n\times m}$ with at most τ_{C} fraction of errors, we convert it into a vector $\boldsymbol{b} \in \mathbb{F}_q^{mn}$. We add all zeros to $\boldsymbol{b}$ to form a vector $\mathbf{a}$ of length N. Thus, there are at most $\tau_{\mathsf{C}}mn + N - mn \leq \tau_{\mathsf{H}}N$ errors in $\mathbf{a}$. Now one can list decode $\mathbf{a}$ to obtain $\mathcal{L}$ codewords of $\mathbf{A}$ and hence $\mathcal{L}$ codewords of $\mathcal{C}$. ■

Now we can apply various list decodable Hamming metric codes in literature to Theorem 21 to obtain list decodable cover-metric codes. Let us firstly apply Reed-Solomon codes and algebraic geometry codes with list decoding radius achieving the Johnson bound.

Theorem 21. *(i) For a real $\epsilon \in (0,1)$, one can list decode q-ary cover-metric codes in $\mathbb{F}_q^{n\times m}$ of rate R from Reed-Solomon codes with decoding radius $1 - \sqrt{R} - \epsilon$ and list size $O(\frac{1}{\epsilon})$. The decoding algorithm can be performed in time $O\left(\frac{(m)^6 \log^3 q}{\epsilon^5}\right)$.*

(ii) For a real $\epsilon \in (0,1)$ and $q = \Omega\left(\frac{1}{\epsilon^2}\right)$, one can list decode q-ary cover-metric codes in $\mathbb{F}_q^{n\times m}$ of rate R from algebraic geometry codes with decoding radius $1-\sqrt{R}-\epsilon$ and list size $O(\frac{1}{\epsilon})$. The decoding algorithm can be performed in time $\mathrm{poly}(m, \frac{1}{\epsilon})$.

Proof. By [23], we know that one can list decode a q-ary Reed-Solomon code of rate R_1 and length N up to the Johnson bound $\tau_{\mathsf{H}} := 1-\sqrt{R_1}-\epsilon_1$ with list size $O(\frac{1}{\epsilon_1})$ and time $O\left(\frac{N^3 \log^3 q}{\epsilon_1^5}\right)$. Fix a real $\rho \in (0,1)$. Let $R = R_1 - 3\sqrt{1/(\rho N)}$ and

$$\tau_{\mathsf{C}} = \tau_{\mathsf{H}} - 3\sqrt{1/(\rho N)} = 1 - \sqrt{R + 3\sqrt{1/(\rho N)}} - \epsilon_1 - 3\sqrt{1/(\rho N)} = 1 - \sqrt{R} - \epsilon,$$

where $\epsilon = \epsilon_1 + O(\sqrt{1/(N)})$. As $N = \Theta(mN)$, we obtain the desired result of (i) from Theorem 21.

With a similar argument, we can obtain the result of (ii) by applying algebraic geometry codes [23]. ■

Next, we apply the folded Reed-Solomon codes [9] and algebraic geometry codes [27] with Hamming metric list decoding radius achieving the Singleton bound to get cover-metric codes with list decoding radius achieving the Singleton bound as well.

Theorem 22. *(i) For every real $\rho \in (0,1)$ and small $\epsilon > 0$, there exists a q-ary cover-metric code of rate R in $\mathbb{F}_q^{\rho m\times m}$ with $q = m^{O(1/\epsilon^2)}$ which is $\left((1-R-\epsilon)n, (1/\epsilon)^{O(1/\epsilon)}\right)^{\mathsf{C}}$-list decodable. Furthermore, the algorithm can be performed in time* $\mathrm{poly}(mn, \frac{1}{\epsilon})$.
(ii) For every real $\rho \in (0,1)$, small $\epsilon > 0$ and prime power $q = \exp(O(1/\epsilon^2))$, there exists a q-ary cover-metric code of rate R in $\mathbb{F}_q^{\rho m\times m}$ which is $\left((1-R-\epsilon)n, \ell := 2^{2^{(\log^* m)^2}}\right)^{\mathsf{C}}$-list decodable. Furthermore, the algorithm can be performed in time $(mn)^{O(1)}(1/\epsilon)^{O(\ell)}$, where $\log^* m$ denotes the number of iterated logarithms to the base 2 needed to reach a number below 1.

Proof. By [9], there exists an explicit construction of codes over $\mathbb{F}_q$ with length N and rate R_1 which is $\left((1-R_1-\epsilon_1)n, (1/\epsilon_1)^{O(1/\epsilon_1)}\right)^{\mathsf{H}}$-list decodable. The alphabet size is $m^{O(1/\epsilon_1^2)}$ and the list decoding algorithm runs in time $\mathrm{poly}(mn, \frac{1}{\epsilon})$. Fix $\rho \in (0,1)$. Let $\epsilon = \epsilon_1 +$

$6\sqrt{1/(\rho N)}$ and $R = R_1 - 3\sqrt{1/(\rho N)}$. As $N = \Theta(mN)$, we obtain the desired result of (i) from Theorem 22.

Using a similar argument, we can obtain the result of (ii) by applying list decoding of algebraic geometry codes given in [27]. ■

We give a table to illustrate some concrete parameters for our explicit constructions reaching the Johnson bound and the Singleton bound. We emphasize that it is just a theoretical estimation applicable to the case when the matrix size m is sufficiently large.

Table 6.1: Explicit constructions reaching the Johnson bound and the Singleton bound

Rate R	Radius $1-\sqrt{R}-\epsilon$	List size	ϵ	Rate R	Radius $1-R-\epsilon$	List size	ϵ
0.1	0.68	100	0.01	0.1	0.89	100^{100}	0.01
0.1	0.64	20	0.05	0.1	0.85	20^{20}	0.05
0.4	0.37	100	0.01	0.4	0.59	100^{100}	0.01
0.4	0.32	20	0.05	0.4	0.55	20^{20}	0.05
0.6	0.23	100	0.01	0.6	0.39	100^{100}	0.01
0.6	0.19	20	0.05	0.65	0.35	20^{20}	0.05

Remark 13. We have applied various decoding algorithms from rank-metric codes or Hamming metric codes to obtain explicit list decoding algorithms for cover-metric codes to attain the Singleton bound (see Thorems 18 and 22). There are various list decoding algorithms for Hamming metric codes in literature. By Theorems 19 and 20, we can covert these list decoding algorithms to those for cover-metric codes. However, as we mentioned before, we pay attention to the list decoding of cover-metric codes with decodability up to the Singleton bound. Therefore, we selected only those explicit list decoding of Hamming metric codes achieving the Singleton bound. On the other hand, if we choose binary Hamming metric codes for instance, we can only list decode cover-metric codes up to the Blokh-Zyablov bound (see in [21]).

Although we understand that the case $\rho = 1$ is interesting, there are no list decoding algorithms for rank-metric codes with decoding radius achieving the Singleton bound. If

we choose a rank-metric code with the ratio ρ independent of ϵ (for instance $\rho = 1$), we get cover-metric codes with decoding radius far away from the Singleton bound (see in [68]).

6.5 Conclusion

In this chapter, we study and investigate list decoding of cover-metric codes. We show that the list decodability of cover-metric codes cannot exceed the Singleton bound. Furthermore, we show that most random cover-metric codes can be list decoded up to the Singleton bound and the list decoding radius is independent of the ratio $\rho = \frac{n}{m}$ and alphabet size in Table 6.2. We further show that there exist cover-metric codes that can be efficiently

Table 6.2: List decodability of random ($\mathbb{F}_q$-linear) cover-metric codes

Random codes	Decoding radius τ	List size $\mathcal{L}$
cover-metric codes	Singleton bound	$O(1/\epsilon)$
$\mathbb{F}_q$-linear cover-metric codes	Singleton bound	$\exp(O(1/\epsilon))$

Table 6.3: Converting from rank-metric codes to cover-metric codes

Ratio ρ	Decoding radius τ	List size $\mathcal{L}$	Decoding algorithm running time
$O(\epsilon^2)$	Singleton bound	$\exp(O(1/\epsilon))$	$\text{poly}(m, 1/\epsilon)$

list decoded with list decoding radius up to the Singleton bound and the Johnson bound. Although our efficient list decoding algorithm can list decode up to the Singleton bound and the Johnson bound, either the ratio ρ is very small, or the alphabet size q is a function of the matrix size m or the list size is not a polynomial in m (although it is almost polynomial in m) in Table 6.3 and Table 6.4.

Finally, we draw a graph to compare our results with the Johnson-like bound in Figure 6.1.

Table 6.4: Converting from Hamming metric codes to cover-metric codes

	Field $\mathbf{q}$	Decoding radius $\boldsymbol{\tau}$	List size $\mathcal{L}$	Decoding algorithm running time
Ours	q	Johnson bound	$O(1/\epsilon)$	$O(m^6 \log^3 q\ /\epsilon^5)$
Ours	$\Omega(1/\epsilon^2)$	Johnson bound	$O(1/\epsilon)$	$\text{poly}(m, 1/\epsilon)$
[65]	q	Johnson-like bound	$O(1/\epsilon)$	$\text{poly}(m, 1/\epsilon)$
Ours	$m^{O(1/\epsilon^2)}$	Singleton bound	$(1/\epsilon)^{O(1/\epsilon)}$	$\text{poly}(mn, 1/\epsilon)$
Ours	$\exp(O(1/\epsilon^2))$	Singleton bound	$l := 2^{2^{(log*m)}}$	$(mn)^{O(1)}(1/\epsilon)^{O(l)}$

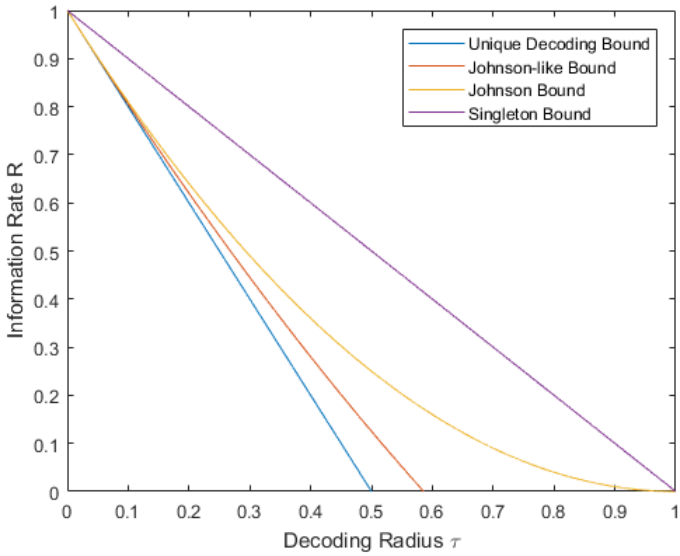


Figure 6.1: Decoding radius of cover-metric codes

The open question is how to efficiently list decode cover-metric codes up to the Singleton bound with constant alphabet size, polynomial list size and ratio $\rho = 1$.

Chapter 7

Conclusions

In this thesis, we have addressed some issues on list decoding. We began by presenting investigations on list decoding along with the study of rank-metric codes. Then, we moved on to consider the crisscross errors which occur more commonly in the array for message storage. To better combat crisscross errors, the cover-metric codes were also proposed and considered in Chapter 2.

The challenge of list decoding of rank-metric codes is believed to be more difficult than that for classical block codes. It is quite difficult to efficiently list decode some Gabidulin codes beyond the unique decoding barrier in [54]. On the other hand, several results (see for examples in [27] and [68]) have shown that by only considering some subsets of Gabidulin codes, the performance can improve. In the view of this, we dedicate Chapter 3 to investigate the prospect of this line of thought. As results for this investigation, we proposed some lower bounds for random subcodes of Gabidulin codes. Moreover, given a random subcode of Gabidulin code, it is list decodable with decoding radius far beyond the unique decoding bound with probability negligibly close to 1. The improvement is more significant when the rate of the subcode is a bit far from that of the mother Gabidulin code where it can attain the Gilbert-Varshamov bound. In particular, for any small positive ϵ, when the ratio $\rho = O(\epsilon)$, we can show that the existence of a subcode which has decoding radius even reaching the Singleton bound. These findings confirm how good of candidates of sub-

codes of Gabidulin codes can be. Some possible improvements that may be interesting to be considered are the explicit construction of such codes along with efficient list decoding algorithms. Furthermore, can we decrease the list size for linear subcodes of Gabidulin codes?

Recently, the improvement on the list decodability of $\mathbb{F}_q$-linear rank-metric codes in [20] along with the good performance and properties of list decoding of self-orthogonal codes in Hamming metric [30] leads us to consider whether $\mathbb{F}_q$-linear self-orthogonal rank-metric codes also perform as well as the two former families. We answer this question in Chapter 4. Our investigation produces the result that with high probability, a random $\mathbb{F}_q$-linear self-orthogonal rank-metric code of rate $R = (1-\tau)(1-\rho\tau) - \epsilon$, for small $\epsilon \in (0,1)$ is $(\tau n, O(1/\epsilon))^R$-list decodable. When we further restrict the chosen random rank-metric code to also be $\mathbb{F}_{q^m}$-linear, the list decoding radius can achieve the Gilbert-Varshamov bound albeit its list size being exponential $\exp(O(\frac{1}{\epsilon}))$. An interesting improvement that can be considered is can we efficiently list decode $\mathbb{F}_{q^m}$-linear rank-metric codes?

The focus of the previous two chapters, Chapters 3 and 4, have been the list decodability of rank-metric codes. Another direction for rank-metric codes that we have considered is to construct a new family of MRD codes, which is not equivalent to the Gabidulin codes and any other existing families. Despite the numerous results in this field, aside from the special case the length $n = 3$, all other constructions have not reached the dimension to be $n - 1$. In our investigation, we extended the idea from the Twisted Gabidulin codes [57]. As a result, for any n, we succeeded in the construction of a new family of $\mathbb{F}_q$-linear MRD codes of dimension $n - 1$ that are not equivalent to any other existing constructions. Chapter 5 is dedicated to the discussion of this construction along with the investigation of its equivalence and dual.

In the consideration of the crisscross errors, using rank-metric codes as decoding tools may not be so appropriate. Apart from it being "too strong", the prospect of finding an efficient list decoder for rank-metric codes beyond the unique decoding radius is not too hopeful. Due to the limitations of list decoding of rank-metric codes, we try to combat

the crisscross errors with the help of cover-metric codes. In Chapter 6, inspired by the result in [65], we prove that the list decodability of cover-metric codes does not exceed the Singleton bound. Moreover, with high probability, a random cover-metric code can be list decoded up to the Singleton bound which is better than the Johnson-like bound. Furthermore, we present explicit constructions of cover-metric codes that can be efficiently list decoded up to the Singleton bound and the Johnson bound. In the future research, it is interesting to consider: How to efficiently list decode cover-metric codes up to the Singleton bound with constant field size q, polynomial list size and the ratio $\rho = 1$?

Bibliography

[1] E. Ben-Sasson, S. Kopparty, and J. Radhakrishnan, Subspace Polynomials and Limits to List Decoding of ReedSolomon Codes, *IEEE Transactions on Information Theory*, 56(1), pp. 113-120, 2009.

[2] T. P. Berger. Isometries for rank distance and permutation group of Gabidulin codes, *IEEE Transactions on Information Theory*, 49(11), pp. 3016-3019, 2003.

[3] M. Blaum and J. Bruck, MDS array codes for correcting a Single crisscross error, *IEEE Transactions on Information Theory*, 46(3), pp. 1068-1077, 2000.

[4] M. Blaum, R. J. Mceliece, Coding protection for magnetic tapes: a generalization of the Patel-Hong code, *IEEE Transactions on Information Theory*, 31(5), pp. 690-693, 1985.

[5] A. Cossidente, G. Marino, and F. Pavese, Non-Gabidulin maximum rank distance codes, *Designs, Codes and Cryptography*, 79(3), pp. 579-609, 2016.

[6] J. Cruz, M. Kiermaier, A. Wassermann, and W. Willems, Algebraic structures of MRD codes, *Advances in Mathematics of Communications*, 10(3), pp. 499-510, 2016.

[7] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory, *Journal of Combinatorial Theory, Series A*, 25(3), pp. 226-241, 1978.

[8] Y. Ding, On List-Decodability of Random Rank Metric Codes and Subspace Codes, *IEEE Transactions on Information Theory*, 61(1), pp. 51-59, 2015.

[9] Z. Dvir and S. Lovett, Subspace evasive sets, *Proceedings of the 44th ACM Symposium on Theory of Computing*, pp. 351–358, 2012.

[10] P. Elias, Error-correcting codes for list decoding, *IEEE Transactions on Information Theory*, 37(1), pp. 5-12, 1991.

[11] P. Elias, List decoding for noisy channels, Research Laboratory of Electronics, Massachusetts Institute of Technology, 1957.

[12] S. A. Elking, D. P. Siewiorek, Reliability and performance of error correcting memory and register arrays, *IEEE Transactions on Computers*, C-29(10), pp. 920-927, 1980.

[13] E. M. Gabidulin, Optimum Codes Correcting Lattice Errors, *Problems of Information Transmission,* 21(2), pp. 103-108, 1985.

[14] E. M. Gabidulin. Rank-metric codes and applications, http://iitp.ru/upload/content/839/Gabidulin.pdf.

[15] E. M. Gabidulin, Theory of codes with maximal rank distance, *Problems of Information Transmission*, 21(1), pp. 3-16, 1985.

[16] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov, Ideals over a non-commutative ring and their application in cryptology, Workshop on the theory and application of cryptographic techniques Brighton, pp. 482-489, 1991.

[17] M. Gadouleau and Z. Y. Yan, Packing and covering properties of rank metric codes, *IEEE Transactions on Information Theory*, 54(9), pp. 3873-3883, 2008.

[18] V. Guruswami, List Decoding of Error-Correcting Codes, Springer, US, 2001.

[19] V. Guruswami, J. Hastad and S. Kopparty, On the list-decodability of random linear codes, *Proceedings of the 42nd Annual ACM Symposium on Theory of Computing (STOC)*, pp. 409-416, 2010.

[20] V. Guruswami, N. Resch, On the List-Decodability of Random Linear Rank Metric Codes, preprint, 2017.

[21] V. Guruswami and A. Rudra, Better binary list-decodable codes via multilevel concatenation, *IEEE Transactions on Information Theory,* 55(1), pp. 19-26, 2009.

[22] V. Guruswami and A. Rudra, Explicit codes achieving list decoding capacity: error correction with optimal redundancy, *IEEE Transactions on Information Theory*, 54(1), pp. 135-150, 2008.

[23] V. Guruswami and M. Sudan, Improved Decoding of Reed-Solomon and Algebraic-Geometry Codes, *IEEE Transactions on Information Theory*, 145(6), pp. 1757-1767, 1999.

[24] V. Guruswami and S. Vadhan, A lower bound on list size for list decoding, *IEEE Transactions on Information Theory*, 56(11), pp. 5681-5688, 2010.

[25] V. Guruswami and C. Wang, Explicit rank-metric and subspace codes list-decodable with optimal redundancy, *Electronic Colloquium on Computational Complexity*, vol. 20, 2013.

[26] V. Guruswami, C. Wang and C. Xing, Explicit list-decodable rank-metric and subspace codes via subspace designs, *IEEE Transactions on Information Theory*, 62(5), pp. 2707-2718, 2016.

[27] V. Guruswami and C. Xing, List decoding Reed-Solomon, Algebraic-Geometric, and Gabidulin subcodes up to the Singleton bound, *Proceedings of the 45th ACM Symposium on Theory of Computing (STOC'13)*, pp. 843-852, 2013.

[28] A. Horlemann-Trautmann, K. Marshall and J. Rosenthal, Considerations for rank-based cryptosystems, *IEEE International Symposium on Information Theory (ISIT)*, Jul. 2016.

[29] L. K. Hua, A theorem on matrices over a fields and its applications, *Chinese mathematical society*, 1(2), pp. 109-163, 1951.

[30] L. Jin, C. Xing and X. Zhang, On the List-Decodability of Random Self-Orthogonal Codes, *IEEE Transactions on Information Theory*, 61(2), pp. 820-828, 2015.

[31] J. Justesen and T. Hoholdt, Bounds on list decoding of MDS codes, *IEEE Transactions on Information Theory*, 47(4), pp. 1604-1609, 2001.

[32] R. Kötter and F. R. Kschischang, Coding for errors and erasures in random network coding, *IEEE Transactions on Information Theory*, 54(8), pp. 3579-3591, 2008.

[33] A. Kshevetskiy and E. Gabidulin, The new construction of rank codes, *IEEE International Symposium on Information Theory (ISIT)*, Sep. 2005.

[34] L. Levine, W. Meyers, Special Feature: Semiconductor memory reliability with error detecting and correcting codes, 9(10), pp. 43-50, 1976.

[35] R. Lidl and H. Neiderriter, *Finite Fields,* Cambridge, U.K. Cambridge University. Press, 1997.

[36] S. Ling and C. Xing, *Coding Theory A First Course*, 2004: Cambridge University.

[37] S. Liu, On the List Decodability of Self-orthogonal Rank Metric Codes, preprint, 2018.

[38] S. Liu, C. Xing and C. Yuan, List Decodability of Random Subcodes of Gabidulin Codes, *IEEE Transactions on Information Theory*, 63(1), pp. 159-163, 2017.

[39] S. Liu, C. Xing and C. Yuan, List Decoding of Cover Metric Codes up to the Singleton Bound, *IEEE Transactions on Information Theory*, 64(4), pp. 2410-2416, 2018.

[40] G. Lunardon, R. Trombetti, Y. Zhou, Generalized Twisted Gabidulin Codes, *http://arxiv.org/pdf/1507.07855v2.pdf*, 2015.

[41] D. Lund, E. M. Gabidulin, and B. Honary, A new family of optimal codes correcting term rank errors, *IEEE International Symposium on Information Theory (ISIT)*, Jun. 2000.

[42] P. Lusina, E. M. Gabidulin and M. Bossert, Maximum rank distance codes as space-time codes, *IEEE Transactions on Information Theory*, 49(10), pp. 2757-2760, 2003.

[43] H. Mahdavifar and A. Vardy, List-decoding of subspace codes and rank-metric codes up to Singleton bound, *IEEE International Symposium on Information Theory (ISIT)*, Jul. 2012.

[44] K. Morrison, Equivalence for rank metric and matrix codes and automorphism groups of Gabidulin codes, *IEEE Transactions on Information Theory*, 60(11), pp. 7035-7046, 2014.

[45] G. Nebe, W. Willems, On self-dual MRD codes, *Advances in Mathematics of Communication*, 10(3), pp. 633-642, 2016.

[46] O. Ore, On a special class of polynomials, *Transactions American Mathematical Society*, 35(3), pp. 559-584,1933.

[47] O. Ore, Theory of Non-Commutative Polynomials, *Annals of Mathematics*, 34(3), pp. 480-508, 1933.

[48] K. Otal, F. Özbudak, Additive Rank Metric Codes, *IEEE Transactions on Information Theory*, 63(1),pp. 164-168, 2017.

[49] K. Otal, F. Özbudak, Explicit constructions of some non-Gabidulin linear Maximum Rank Distance codes, *Advances in Mathematics of Communications*, 10(3), pp. 589-600, 2016.

[50] K. Otal, F. Özbudak, Some Non-Gabidulin MRD Codes, *Algebraic combinatorics and applications*, 2015.

[51] R. Overbeck, Brute-force attacks public key cryptosystem based on Gabidulin codes, *Journal of Cryptography*, 21(2), pp. 280-301, 2008.

[52] P. Prunsinkiewicz, S. Budkowski, A double track error correction code for magnetic tape, *IEEE Transactions on Computers*, C-25(6), pp. 642-645, 1976.

[53] A. Ravagnani, Rank metric codes and their duality theory, *Design, Codes and Cryptography*, 80(1), pp. 197-216, 2016.

[54] N. Raviv and A. Wachter-Zeh, Some Gabidulin codes cannot be list decoded efficiently at any radius, IEEE Transactions on Information Theory, 62(4), pp. 1605-1615, 2016.

[55] R. M. Roth, Maximum Rank Array Codes and their Application to Crisscross Error Correction, *IEEE Transactions on Information Theory*, 37(2), pp. 328-336, 1991.

[56] R. M. Roth, Probabilistic Crisscross Error Correction, *IEEE Transations on Information Theory*, 43(5), pp. 1425-1438, 1997.

[57] J. Sheekey, A new family of linear maximum rank distance codes, *Advances in Mathematics of Communication*, vol.10, pp. 475-488, 2016.

[58] V. R. Sidorenko, Class of correcting codes for errors with a lattice configuration, *Problemy Peredachi Informatsii*, 12(3), pp. 165171, March 1976.

[59] V. R. Sidorenko, M. Bossert, and E. M. Gabidulin, Generalized Minimum Distance Decoding for Correcting Array Errors, *International Zurich Seminar on Communications (IZS)*, Mar. 2010.

[60] D. Silva, F. R. Kschischang and R. Köetter, A rank-metric approach to error control in random network coding, *IEEE Transactions on Information Theory*, 54(9), pp. 3951-3967, 2008.

[61] M. Sudan, Decoding of Reed-Solomon Codes beyond the Error-Correction Bound, *Journal of Complexity*, 13(1), pp. 180-193, 1997.

[62] A. Trautmann, K. Marshall, New Criteria for MRD and Gabidulin codes and some Rank-Metric code constructions, *Advances in Mathematics of Communications*, 11(3), pp. 533-548, 2017.

[63] A. Wachter-Zeh, Bounds on list decoding Gabidulin codes, in *International Workshop on Algebraic and Combinatorial Coding Theory*, pp. 329-334, 2012.

[64] A. Wachter-Zeh, Bounds on list decoding of rank-metric codes, *IEEE Transactions on Information Theory*, 59(11), pp. 7268-7277, 2013.

[65] A. Wachter-Zeh, List decoding of crisscross errors, *IEEE Transactions on Information Theory*, 63(1), pp. 142-149, 2017 .

[66] J. M. Wozencraft, List decoding, Quarterly Progress Report, Research Laboratory of Electronics, MIT, 48, pp. 90-95, 1958.

[67] B. Wu, Z. Liu, Linearized polynomials over finite fields revisited, *Finite Fields and Their Applications*, vol. 22, pp. 79-100, 2013.

[68] C. Xing and C. Yuan, A new class of rank-metric codes and their list decoding beyond the unique decoding radius, *IEEE Transactions on Information Theory*, 2017.