Algebraic Theory of Rank-Metric Codes: Representations, Invariants and Density Results

Dissertation

zur

Erlangung der naturwissenschaftlichen Doktorwürde
(Dr. sc. nat.)

vorgelegt der

Mathematisch-naturwissenschaftlichen Fakultät

der

Universität Zürich

von

alessandro neri

aus

Italien

Promotionskommission

Prof. Dr. Joachim Rosenthal (Vorsitz)

Prof. Dr. Valentin Feray

Prof. Dr. Eimear Byrne

Zürich, 2019

Abstract

Rank-metric codes are a family of codes introduced for the first time by Delsarte in 1978. They have been shown to have many applications in several areas. In particular, they gained a lot of interest due to their use in random network coding. These codes are linear subspaces of the space of matrices over a finite field, but they can also be seen as subspaces of vectors over an extension field. The metric considered is the one induced by the rank. Codes that are optimal with respect to this metric are called *Maximum Rank Distance (MRD) codes.* Rank-metric codes have been shown to have interesting connections in other areas of mathematics, such as finite geometry, combinatorics, nonassociative algebra and complexity theory. This is mainly due to the rich algebraic structure that they have, in particular if one considers MRD codes.

In this thesis we investigate on the algebraic properties of rank-metric codes, considering them both in matrix and in vector representation. First, we give an overview on known results. Then, we study the encoding of rank-metric codes in terms of their generator matrix and in terms of three-dimensional tensors. Indeed, if one considers rank-metric codes as subspaces of vectors, then it is natural to represent them via their generator matrix. An analogue for the spaces of matrices is given by a three-dimensional tensor. We show how these objects have many of the properties of the defining code. We focus then on Gabidulin codes, which is the most prominent and studied family of MRD codes. We characterize all the canonical representations arising from the generator matrix. While it is well-known that Gabidulin codes can be represented via a Moore matrix, it was unclear how their generator matrix in standard form looks like. We completely answer this question, giving rise to a new notion of q-analogue of Cauchy matrices.

For what concerns rank-metric codes in the vector representation, we give an algebraic description of MRD codes in terms of their generator matrix. We show that it corresponds to a Zariski open set in the algebraic closure of the underlying field. This implies some density results, leading to probability estimations that a random code is MRD. In particular, we show that if the field is big enough, almost all the codes are MRD, but only few of them belong to the family of Gabidulin codes. This motivates researchers in looking for new MRD constructions.

The investigation of rank-metric codes as spaces of matrices via three-dimensional tensors leads to the notion of tensor rank of a code. This is a new parameter that was never considered before, giving a connection to algebraic complexity theory. Since the tensor rank gives a measure on the complexity of storage and encoding of a rank-metric code, we investigate on codes which have the smallest possible tensor rank.

Furthermore, we study the properties of some new invariants of vector codes. These invariants are a generalization of some parameters already considered in literature, and give a criterion for testing code inequivalence. Moreover, we show how we can use them in order to derive new characterization and enumerative results.

Finally, we illustrate some applications of rank-metric codes in biometric authentication and in distributed storage.

Contents

Preface

Introduction

The rise of coding theory was due to cope with the difficulty to send information through a channel in presence of noise. In the 40's, Shannon seminal paper [105] laid the foundation of the mathematical framework of information and coding theory. After that, the theory of error-correcting codes has been quickly developed, especially thanks to Hamming's work [48], that can be considered as the starting point of algebraic coding theory. In this work, the mathematical framework of block codes endowed with the *Hamming distance* was proposed. The metric defined by such a distance is the main tool to allow the algebraic study of coding theory.

In the most general framework, algebraic coding theory is the theory of subsets of a vector space over a finite field $\mathbb{F}$ endowed with a distance function. The most studied distance in coding theory is the Hamming distance, which is defined as a map $d : \mathbb{F}^n \times \mathbb{F}^n \longrightarrow \mathbb{R}$, such that $d(u, v) = |\{i \in \mathbb{F}^n : u_i \neq v_i\}|$ for any $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in \mathbb{F}^n$. However, in this dissertation, the function considered is the *rank distance*. The well-known chain of inequalities

$$|\operatorname{rk}(A) - \operatorname{rk}(B)| \leq \operatorname{rk}(A + B) \leq \operatorname{rk}(A) + \operatorname{rk}(B)$$

defines a metric on the space of $n \times m$ matrices over a (finite) field $\mathbb{F}$. Codes with this metric have been considered in error control theory for the first time by Delsarte in [30], although similar notions can be traced back to [54]. Few years later, Gabidulin introduced the rank distance on vectors over a field extension of $\mathbb{F}$ and studied the relations between this vector representation and the matrix representation given by Delsarte [36].

In both the frameworks described, *rank-metric codes* have been shown to have many interesting applications. Roth was the first to use them for crisscross error correction in [96]. Then, Silva, Kschischang and Kötter proposed a scheme that uses rank-metric codes for error correction in network coding [58, 111, 109]. After these groundbreaking papers, many researchers, not only from the coding theory community, focused their attention on rank-metric codes. More recently, many other applications have been investigated, such as in distributed storage systems [108], construction and decoding of space-time codes [39, 13, 70], and low-rank matrix recovery [35, 78]. However, one of the most appealing and important research directions is oriented towards code-based cryptography.

Rank-metric codes in general, and MRD codes in particular, are also well-studied from a theoretical point of view. Their notion can be found also in other areas of mathematics, and not only in algebraic coding theory. Their connection with semifields is well-known and studied [106], and the recent construction of twisted Gabidulin codes is a generalization of the twisted semifields introduced by Albert [1]. Also, MRD codes have been studied in connection to linear sets and other objects arising in finite geometry [73]. Finally, some combinatorial techniques had led to new results in rank-metric codes and their duality theory [92, 9, 18]. For these reasons, rank-metric codes have brought together researchers from coding theory, finite geometry, combinatorics and algebra, leading to a fast improvement of their mathematical theory in the last decade.

Personal Contributions

In this thesis, we give a treatise on rank-metric codes. We explain in details the rich algebraic structure that they possess, and that comes from their representations. Invariants and density results arising from the algebraic description are carefully described. Moreover, part of the dissertation is devoted to the study of codes having optimal parameters, namely *maximum rank distance (MRD) codes*, and their general properties. The most studied family of MRD codes is the one of *Gabidulin codes*, which we analyze in detail. Furthermore, the theory of rank-metric codes gives rise to an interesting connection with three-dimensional tensors, that provides a link to algebraic complexity theory. Finally, we briefly describe few applications of rank-metric codes.

The aim of this work is to combine the existing literature on rank-metric codes with the personal contributions in [16, 79, 81, 82, 83, 84, 53, 80], in order to provide a complete and original overview on the topic.

With the purpose of characterizing the encoding schemes for rank-metric codes, in [16] Byrne, Ravagnani, Sheekey and the author developed a theory for the representation of matrix rank-metric codes as three-dimensional tensors. More specifically, every k-dimensional $\mathbb{F}_q$-subspace $\mathcal{C}$ of $\mathbb{F}_q^{n\times m}$ can be represented via a *generator tensor* $T \in \mathbb{F}_q^k \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^m \cong \mathbb{F}_q^{k\times n\times m}$. Such a tensor T identifies an encoding map $\mathcal{E}_T : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^{n\times m}$ such that $\mathrm{Im}(\mathcal{E}_T) = \mathcal{C}$. This representation is the analogue of the generator matrix for linear codes in $\mathbb{F}_q^n$. Moreover, the analogous notion of a parity check matrix is determined. It is shown how one can read information on the parameters of a code from these two new objects. In the same paper, a new parameter of rank-metric codes, arising from the tensor representation, is investigated. It is the *tensor rank*. It is important to remark that this parameter has no analogue in the linear block case; it gives an idea of "how complex" the rank-metric code is, and it measures how many bits are needed in order to store the code. For this reason, codes with small tensor rank are investigated, and some constructions are proposed. The study of the tensor rank of a rank-metric code leads to a new connection between the theory of rank-metric codes and algebraic complexity theory. As an example, one can see that the tensor rank of a 1-dimensional Gabidulin code in $\mathbb{F}_q^{n\times m}$ corresponds to the complexity of multiplication between two polynomials in $\mathbb{F}_q[x]$ whose degrees are upper-bounded by n and m, respectively.

The author spent much effort in investigating the algebraic structure of MRD codes. Among them, the family of generalized Gabidulin codes is still the most interesting from an algebraic point of view. These codes can be considered the analogue of generalized Reed-Solomon (GRS) codes for the rank metric, since they both correspond to the evaluation of some special set of polynomials. In this direction, another analogy emerges in the generator matrices of these codes. While the canonical generator matrix for GRS codes can be described via a Vandermonde matrix, the analogous generator matrix for a generalized Gabidulin code is given by the Moore matrix. In 1985, Roth and Seroussi gave a characterization of the generator matrix in reduced row echelon form for GRS codes, showing that GRS codes are in 1-to-1 correspondence with *generalized Cauchy matrices* [98]. In [79], the author found a parametrization of the generator matrix in reduced row echelon form of generalized Gabidulin codes. The matrix obtained is of the form $(I_k \mid X)$, where X can be considered as the q-analogue of generalized Cauchy matrices, leading to a new definition of *θ-Cauchy matrices.* In the same paper, some applications of this parametrization are given. Among them, it is worth to mention the development of a new criterion for determining whether a given rank-metric code is a generalized Gabidulin code. The result only requires $\mathcal{O}(k^2mn)$ field operations, where k is the dimension and n is the length of the given code. It is also shown that it improves by an exponential speed-up the best previously known criterion.

In [81], Horlemann-Trautmann, Randrianarisoa, Rosenthal and the author showed that the properties for a code $C \subseteq \mathbb{F}_{q^m}^n$ of being MRD and non-Gabidulin are generic. This means that over a large field extension a randomly chosen generator matrix generates an MRD code that is not a Gabidulin code in $\mathbb{F}_{q^m}^n$ with probability approaching 1, when m increases. Moreover, upper and lower bounds on the respective probabilities in dependence on the extension degree are derived. This result motivates many researchers to look for new constructions of MRD codes and, since then, some new families have been discovered. There, it is also shown that for any length and dimension there exists a linear non-Gabidulin MRD code, if the extension degree is large enough. Although this can be considered as a trivial observation implied by Sheekey's construction whenever $q \geq 3$, for $q = 2$ it gives an important result, since there are essentially no construction of linear MRD codes over $\mathbb{F}_{2^m}$ except for the Gabidulin one.

When one considers new rank-metric codes constructions, it is needed to check whether the new codes are equivalent to any other known construction. For this purpose, one wants to develop some criteria to check code equivalence. A first criterion was introduced in [51]. This criterion was based on the dimension of the σ-sum of a code $C \subseteq \mathbb{F}_{q^m}^n$, that is the subspace $C + \sigma(C)$, where $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. In [82], Puchinger, Horlemann-Trautmann and the author gave a generalization of this idea, by considering the $\mathbb{F}_{q^m}$-subspace generated by the code and the application of several powers of the automorphism σ to it. The sequence of the dimensions of such subspaces is called σ-sequence and is an invariant of a rank-metric code, which provides an easy checkable criterion for determining code inequivalence. Furthermore, the study of σ-sequences has important implications in code-based cryptography. Indeed, they serve as distinguishers for retrieving the structure of the rank-metric code used in the McEliece-type cryptosystem. In the same paper, the σ-sequences of Gabidulin and twisted Gabidulin codes are computed. In the subsequent work [83] by the same authors, it is shown how to apply the theory of these invariants in order to obtain some lower bounds on the number of equivalence classes of Gabidulin and twisted Gabidulin codes. In some special cases, the exact number of such equivalence classes is provided. Moreover, a characterization result for Gabidulin codes is given in terms of the σ-sequences.

The remaining works focus on some applications of rank-metric codes. In [84], Rosenthal, Schipani and the author proposed an authentication scheme based on Gabidulin codes and linearized polynomials. The motivation is that rank-metric codes can correct more errors which have particular structures (i.e. matrices with small rank), and in some frameworks they could outperform authentication schemes based on Hamming metric. In [80], Horlemann-Trautmann and the author used MRD codes for constructing *partial MDS codes.* These codes are used in distributed storage, and they are a special family of locally repairable codes that achieve the maximum capacity of erasure correction from an information theoretical point of view. Moreover, an algebraic description and a characterization result for a special class of PMDS codes are given in the paper [53] by the same authors.

Outline

In order to make this dissertation as self-contained as possible, we recall some preliminary results in Chapter 1. We start with the basics on finite fields, with a particular focus on trace, norm and q-polynomials. Then, we give an overview on three-dimensional tensors, their characterizations and representations. Finally, we conclude with a brief description of linear block codes and some results on generalized Reed-Solomon codes.

In Chapter 2 we introduce rank-metric codes. We give some basic notions and results, and study both matrix and vector codes in terms of their parameters, duality and code equivalence. The link between the two representations is also explained. Moreover, we define *maximum rank distance codes*, which are codes with optimal parameters with respect to the Singleton bound.

Chapter 3 focuses on the encoding and the representation of rank-metric codes. On one hand, we see that vector codes can be represented via the *generator matrix*, which is a well-known concept in coding theory. On the other hand, matrix codes can be represented as three-dimensional tensors. Roughly speaking, one can think about a sort of cube built gluing together a basis of matrices for the code. This representation is known as *generator tensor*, and was introduced in [16]. In that paper, we show that this leads to interesting results in terms of encoding and storage complexity, as explained in Subsection 3.2.1. Morever, we describe how to extrapolate information about a code from any of its generator matrices (respectively tensors).

The family of *Gabidulin codes* is the central topic of Chapter 4. All the most important properties are explained and a complete description of their representation is given, following the results in [79]. In the present dissertation, Gabidulin codes are explained in a more general way. In spite of the usual definitions using q-polynomials, we define them using the group algebra on the Galois group of the defining field extension. This makes (almost) all the results true even for fields of any characteristic. This generalization is explained in Section 4.5.

Genericity results are then discussed in Chapter 5. Section 5.1 is based on [81], in which Neri, Horlemann-Trautmann, Randrianarisoa and Rosenthal showed that in the vector representation, maximum rank distance codes are dense in the set of all rank-metric codes which are linear over the extension field, while Gabidulin codes are rare. This implies that a randomly chosen linear code is very likely a maximum rank distance code but not a Gabidulin code, if the degree of the extension field is big enough. Quite surprisingly, a similar result does not hold for matrix codes which are linear over the base field. This was proved independently by Antrobus and Gluesing-Luerssen in [18] and by Byrne and Ravagnani in [2], and it is briefly explained in Section 5.2.

In Chapter 6, the relation between rank-metric codes and three-dimensional tensors is furtherly investigated [16]. This connection leads also to a connection between rank-metric codes and linear block codes. In particular, the notion of *tensor rank of a code* is central to this chapter. This is because the smaller the tensor rank, the lower the storage and encoding complexity. This motivates the study of *minimum tensor rank codes*, which we face in Section 6.2. Those codes are extremal codes with respect to a Singleton-like bound for the tensor rank.

Chapter 7 contains an intensive study of some new invariants, introduced in [82] and additionally investigated in [83]. These invariants are based on the dimensions of the σ-sums and the σ-intersections of a vector code C. More specifically, we show that the sequence of dimensions of the linear spaces, generated by C together with itself under several applications of a field automorphism, is an invariant for the whole equivalence class of the code. The same also holds for the dimensions of the intersections of such spaces. Moreover, we compute such sequences of dimensions for the known classes of Gabidulin and twisted Gabidulin codes. As a result, we derive upper and lower bounds on the number of inequivalent codes. Finally, we derive a characterization theorem for Gabidulin codes, which is partially based on these invariants.

Finally, in Chapter 8 we focus on applications of rank-metric codes. We briefly describe the most common uses of these codes for communication and security purposes. Then, we analyze two specific aspects. We describe a fuzzy authentication model based on Gabidulin codes, which was proposed in [84] for authentication using approximate matching under a certain metric of similarity. Afterwards, we deal with *partial MDS codes*, a family of codes used for distributed storage. Based on [53, 80], we give an algebraic description of these codes, a characterization result and a general construction that involves maximum rank distance codes.

Chapter 1

Preliminaries

In this chapter we give some preliminary notions that will be useful in the whole dissertation. We introduce the basics of finite fields, the trace and norm maps, and some additional results on the theory of q-analogues. Afterwards, we revise some theory of tensors, in particular the three-dimensional ones. Finally, we give an overview on classical coding theory with the Hamming metric, with a particular focus on the family of generalized Reed-Solomon codes.

Notation: Let $\mathcal{X}, \mathcal{Y}$ be two sets and $f : \mathcal{X} \to \mathcal{Y}$ be a map. For any $\mathcal{S} \subseteq \mathcal{Y}$ we denote the preimage of $\mathcal{S}$ under the map f by $f^{-1}(\mathcal{S})$, i.e.

$$f^{-1}(\mathcal{S}) := \{x \in \mathcal{X} \mid f(x) \in \mathcal{S}\}.$$

We will widely use this notation in the present dissertation. Moreover, for any positive integer i we let $[i] := \{1, \ldots, i\}$.

1.1 Finite Fields

The following definitions and results can be found in any textbook on finite fields, e.g. [68]. We denote the finite field of cardinality q by $\mathbb{F}_q$. It is well-known that it exists if and only if q is a prime power. Moreover, if it exists, $\mathbb{F}_q$ is unique up to isomorphism. An extension field of extension degree m is denoted by $\mathbb{F}_{q^m}$. An important property of finite fields is the existence of a primitive element. This means that there always exists $\gamma \in \mathbb{F}_q$ that is a generator of $\mathbb{F}_q^*$, i.e.

$$\mathbb{F}_q = \{0\} \cup \{\gamma^i \mid 0 \leq i \leq q-2\}.$$

We now recall some basic theory on finite fields and the trace function. It is well-known that the extension field $\mathbb{F}_{q^m}/\mathbb{F}_q$ is a Galois extension and

$$\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \{\sigma : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m} \text{ field automorphism } \mid \sigma_{|_{\mathbb{F}_q}} = \mathrm{id}\}$$

is a cyclic group. One of its generators is given by the q-Frobenius automorphism $\bar{\theta}$, defined as

$$\begin{aligned} \bar{\theta} : \mathbb{F}_{q^m} &\longrightarrow \mathbb{F}_{q^m} \\ \alpha &\longmapsto \alpha^q. \end{aligned}$$

1.1.1 Trace over Finite Fields and its Duality

We study here the trace map of a finite field extension, and the duality theory that follows from that.

Definition 1.1. Let $\mathbb{F}_{q^m}/\mathbb{F}_q$ be a finite extension of fields. For $\alpha \in \mathbb{F}_{q^m}$, the *trace* of α with respect to the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ is defined by

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) := \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)} \sigma(\alpha) = \sum_{i=0}^{m-1} \bar{\theta}^i(\alpha) = \sum_{i=0}^{m-1} \alpha^{q^i},$$

We will refer to the function

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$$

as the *trace map* of $\mathbb{F}_{q^m}/\mathbb{F}_q$.

For every generator θ of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, we denote by ψ_θ the map given by

$$\begin{aligned} \psi_\theta : \mathbb{F}_{q^m} &\longrightarrow \mathbb{F}_{q^m} \\ \alpha &\longmapsto \theta(\alpha) - \alpha. \end{aligned}$$

The following result relates the trace with the maps ψ_θ.

Lemma 1.2. *The trace function satisfies the following properties:*

1. $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$ *for all* $\alpha \in \mathbb{F}_{q^m}$.
2. $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ *is an* $\mathbb{F}_q$*-linear surjective transformation from* $\mathbb{F}_{q^m}$ *to* $\mathbb{F}_q$.
3. ψ_θ *is an* $\mathbb{F}_q$*-linear transformation from* $\mathbb{F}_{q^m}$ *to itself.*
4. *For every generator* θ *of* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, $\psi_\theta(\alpha) = 0$ *if and only if* $\alpha \in \mathbb{F}_q$.
5. *(Additive Hilbert's Theorem 90 for finite fields)* $\ker(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}) = \mathrm{Im}(\psi_\theta)$ *for every generator* θ *of* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ *and has cardinality* q^{m-1}.

Proof. A partial proof of this result can be found in [68, Chapter 2, Section 3]. For a complete proof we refer to [81, Lemma 2]. □

The trace map has many important properties. One of them is that it can be used to define an isomorphism between $\mathbb{F}_{q^m}$ and $\mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_{q^m}, \mathbb{F}_q)$.

Definition 1.3. The $\mathbb{F}_q$-bilinear map defined as

$$\begin{aligned} \mathrm{tr} : \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} &\longrightarrow \mathbb{F}_q \\ (\alpha, \beta) &\longmapsto \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha\beta), \end{aligned}$$

is called the *trace form* of the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$.

Observe that for every $\alpha \in \mathbb{F}_{q^m}$, we can associate an $\mathbb{F}_q$-linear map $T_\alpha \in \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_{q^m}, \mathbb{F}_q)$, defined as

$$\begin{aligned} T_\alpha : \mathbb{F}_{q^m} &\longrightarrow \mathbb{F}_q \\ \beta &\longmapsto \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha\beta). \end{aligned}$$

Theorem 1.4. *The trace form of $\mathbb{F}_{q^m}/\mathbb{F}_q$ is a symmetric non degenerate $\mathbb{F}_q$-bilinear form. Moreover it induces a duality isomorphism given by*

$$\begin{aligned} \Psi : \mathbb{F}_{q^m} &\longrightarrow \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_{q^m}, \mathbb{F}_q) \\ \alpha &\longmapsto T_\alpha. \end{aligned}$$

Proof. For the proof one can see [68, Theorem 2.24]. □

The following results directly follow from Theorem 1.4.

Corollary 1.5. *For every $\alpha \in \mathbb{F}_{q^m}^*$ the map T_α is non identically zero, and hence* $\dim_{\mathbb{F}_q}(\ker(T_\alpha)) = m - 1$.

Corollary 1.6. *For every $\alpha, \beta \in \mathbb{F}_{q^m}$ and $\lambda, \mu \in \mathbb{F}_q$, we have*

$$T_{\lambda\alpha+\mu\beta} = \lambda T_\alpha + \mu T_\beta.$$

Since the trace form induces a duality isomorphism, we can naturally define the notion of dual basis.

Definition 1.7. Given an $\mathbb{F}_q$-basis $\alpha_1, \ldots, \alpha_m$ of $\mathbb{F}_{q^m}$ and $\beta_1, \ldots, \beta_m \in \mathbb{F}_{q^m}$, we say that $\beta_1, \ldots, \beta_m$ is a *dual basis* of $\alpha_1, \ldots, \alpha_m$ with respect to the trace form, if for all $i, j \in [m]$

$$\mathrm{tr}(\alpha_i, \beta_j) = \delta_{i,j} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

Remark 1.8. Given an $\mathbb{F}_q$-basis $\alpha_1, \ldots, \alpha_m$ of $\mathbb{F}_{q^m}$, the existence and uniqueness of its dual basis follow by Theorem 1.4 and the fact that $\mathbb{F}_{q^m}$ is a finite dimensional $\mathbb{F}_q$-vector space.

Lemma 1.9. *For every $\alpha_1, \ldots, \alpha_k, \beta \in \mathbb{F}_{q^m}$,*

$$\ker(T_{\alpha_1}) \cap \ldots \cap \ker(T_{\alpha_k}) \subseteq \ker(T_\beta)$$

if and only if $\beta \in \langle \alpha_1, \ldots, \alpha_k \rangle$.

Proof. Suppose $\beta \in \langle \alpha_1, \dots, \alpha_k \rangle$. By Corollary 1.6, there exist $\lambda_1, \dots, \lambda_k \in \mathbb{F}_q$ such that $T_\beta = \lambda_1 T_{\alpha_1} + \ldots + \lambda_k T_{\alpha_k}$. Hence, if $x \in \ker(T_{\alpha_1}) \cap \ldots \cap \ker(T_{\alpha_k})$, then

$$T_\beta(x) = \lambda_1 T_{\alpha_1}(x) + \ldots + \lambda_k T_{\alpha_k}(x) = 0 + \ldots + 0 = 0,$$

and therefore $x \in \ker(T_\beta)$.

On the other hand, suppose $\beta \notin \langle \alpha_1, \dots, \alpha_k \rangle$. Let $s := \dim_{\mathbb{F}_q} \langle \alpha_1, \dots, \alpha_k \rangle$. Without loss of generality we can assume that $\langle \alpha_1, \dots, \alpha_k \rangle = \langle \alpha_1, \dots, \alpha_s \rangle$. Now, complete $\alpha_1, \dots, \alpha_s, \beta$ to an $\mathbb{F}_q$-basis $\alpha_1, \dots, \alpha_s, \beta, \gamma_1, \dots \gamma_{m-s-1}$ of $\mathbb{F}_{q^m}$ and consider its dual basis with respect to the trace form $\tilde{\alpha}_1, \dots, \tilde{\alpha}_s, \tilde{\beta}, \tilde{\gamma}_1, \dots \tilde{\gamma}_{m-s-1}$. Therefore, $T_{\alpha_i}(\tilde{\beta}) = 0$ for every $i \in [s]$ and $T_\beta(\tilde{\beta}) = 1$, i.e.

$$\tilde{\beta} \in \ker(T_{\alpha_1}) \cap \ldots \cap \ker(T_{\alpha_k}) \setminus \ker(T_\beta).$$

□

Theorem 1.10. *For every $\alpha_1, \dots, \alpha_k \in \mathbb{F}_{q^m}$,*

$$\dim_{\mathbb{F}_q}(\ker(T_{\alpha_1}) \cap \ldots \cap \ker(T_{\alpha_k})) = m - \dim_{\mathbb{F}_q} \langle \alpha_1, \dots, \alpha_k \rangle.$$

Proof. Let $s := \dim_{\mathbb{F}_q} \langle \alpha_1, \dots, \alpha_k \rangle$. Without loss of generality we can suppose $\langle \alpha_1, \dots, \alpha_k \rangle = \langle \alpha_1, \dots, \alpha_s \rangle$. By Lemma 1.9, we have $\ker(T_{\alpha_{s+1}}), \dots, \ker(T_{\alpha_k}) \supseteq \ker(T_{\alpha_1}) \cap \ldots \cap \ker(T_{\alpha_s})$, and hence

$$\ker(T_{\alpha_1}) \cap \ldots \cap \ker(T_{\alpha_k}) = \ker(T_{\alpha_1}) \cap \ldots \cap \ker(T_{\alpha_s}).$$

Therefore, it is enough to prove the statement when $\alpha_1, \dots, \alpha_k$ are linearly independent over $\mathbb{F}_q$. We use induction on k. If $k = 1$ then $\dim_{\mathbb{F}_q}(\ker(T_{\alpha_1})) = m - 1$ by Corollary 1.5.

Suppose now that the statement is true for $k - 1$, i.e.

$$\dim_{\mathbb{F}_q}(S) = m - k + 1,$$

where $S := \ker(T_{\alpha_1}) \cap \ldots \cap \ker(T_{\alpha_{k-1}})$. Then, by Lemma 1.9, $S \not\subseteq \ker(T_{\alpha_k})$, i.e. $S + \ker(T_{\alpha_k}) = \mathbb{F}_{q^m}$. Therefore,

$$\begin{aligned} \dim_{\mathbb{F}_q}(S \cap \ker(T_{\alpha_k})) &= \dim_{\mathbb{F}_q}(S) + \dim_{\mathbb{F}_q}(\ker(T_{\alpha_k})) - \dim_{\mathbb{F}_q}(S + \ker(T_{\alpha_k})) \\ &= m - k + 1 + m - 1 - m \\ &= m - k. \end{aligned}$$

□

Now, let $\alpha_1, \dots, \alpha_k \in \mathbb{F}_{q^m}$ be $\mathbb{F}_q$-linearly independent and complete them to a basis $\alpha_1, \dots, \alpha_m$ of $\mathbb{F}_{q^m}$. Let $\beta_1, \dots, \beta_m$ be its dual bases. Then for every $i = 1, \dots, k$ we have $T_{\alpha_i}(\beta_j) = 0$ for every $j = k+1, \dots, m$, i.e. $\beta_j \in \ker(T_{\alpha_1}) \cap \ldots \cap \ker(T_{\alpha_k})$. Moreover, by Theorem 1.10, we get $\dim_{\mathbb{F}_q}(\ker(T_{\alpha_1}) \cap \ldots \cap \ker(T_{\alpha_k})) = m - k$, and hence

$$\ker(T_{\alpha_1}) \cap \ldots \cap \ker(T_{\alpha_k}) = \langle \beta_{k+1}, \dots, \beta_m \rangle.$$

We can now define the trace-orthogonal space of a subspace as follows.

Definition 1.11. Let $S := \langle \alpha_1, \dots, \alpha_k \rangle$ be an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$. Then the *trace-orthogonal* space of S is defined as the $\mathbb{F}_q$-subspace

$$S^\times := \ker(T_{\alpha_1}) \cap \ldots \cap \ker(T_{\alpha_k}).$$

Proposition 1.12. *The subspace $S^\times$ is well-defined, i.e. it does not depend on the choice of the set of generators.*

Proof. Let $\{\alpha_1, \dots, \alpha_k\}$ and $\{\alpha'_1, \dots, \alpha'_t\}$ be two sets of generators for a subspace S. We want to prove that $\ker(T_{\alpha_1}) \cap \ldots \cap \ker(T_{\alpha_k}) = \ker(T_{\alpha'_1}) \cap \ldots \cap \ker(T_{\alpha'_t})$. For every $i = 1, \dots, k$, $\alpha_i \in \langle \alpha'_1, \dots, \alpha'_t \rangle$ and therefore, by Lemma 1.9, it holds that $\ker(T_{\alpha_i}) \supseteq \ker(T_{\alpha'_1}) \cap \ldots \cap \ker(T_{\alpha'_t})$. Hence,

$$\ker(T_{\alpha_1}) \cap \ldots \cap \ker(T_{\alpha_k}) \supseteq \ker(T_{\alpha'_1}) \cap \ldots \cap \ker(T_{\alpha'_t}).$$

The opposite inclusion is analogous. □

We already know the relation between the image of the map ψ_θ and the kernel of the trace map (see Lemma 1.2). The following Lemma characterizes the preimage of any element in $\mathbb{F}_{q^m}$ under the map ψ_θ.

Lemma 1.13. *Let $\alpha \in \mathbb{F}_{q^m}$ and θ be a generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Then*

1.
$$|\psi_\theta^{-1}(\{\alpha\})| = \begin{cases} q & \text{if } \alpha \in \ker(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}) \\ 0 & \text{if } \alpha \notin \ker(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}). \end{cases}$$

2. *Let $\alpha \in \ker(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q})$. If $x_1, x_2 \in \psi_\theta^{-1}(\{\alpha\})$, then $x_1 - x_2 \in \mathbb{F}_q$, or equivalently, there exists an $x \in \mathbb{F}_{q^m}$ such that*

$$\psi_\theta^{-1}(\{\alpha\}) = \{x + \lambda \mid \lambda \in \mathbb{F}_q\}.$$

Moreover such an x is of the form

$$x = -\frac{1}{\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma)} \left(\alpha\theta(\gamma) + (\alpha + \theta(\alpha))\theta^2(\gamma) + \ldots + (\alpha + \ldots + \theta^{m-2}(\alpha))\theta^{m-1}(\gamma)\right),$$

where $\gamma \in \mathbb{F}_{q^m}$ *is such that* $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma) \neq 0$*.*

Proof. 1. If $\alpha \notin \ker(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q})$, then, by part 5 of Lemma 1.2, we have $\psi_\theta^{-1}(\{\alpha\}) = \emptyset$. On the other hand, if $\alpha \in \ker(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q})$, then $|\psi_\theta^{-1}(\{\alpha\})| = |\ker(\psi_\theta)|$, since ψ_θ is an $\mathbb{F}_q$-linear map. By part 2 of Lemma 1.2,

$$q^{m-1} = |\ker(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q})| = |\mathrm{Im}(\psi_\theta)| = \frac{|\mathbb{F}_{q^m}|}{|\ker(\psi_\theta)|},$$

and therefore we get $|\psi_\theta^{-1}(\{\alpha\})| = q$.

2. For the first part, let $x_1, x_2 \in \psi_\theta^{-1}(\{\alpha\})$. Hence, $\psi_\theta(x_1) - \psi_\theta(x_2) = 0$, and by linearity of ψ_θ, we get $\psi_\theta(x_1 - x_2) = 0$. By part 4 of Lemma 1.2, we get $x_1 - x_2 \in \mathbb{F}_q$. Finally, showing that $\psi_\theta(x) = \alpha$ is a straightforward computation.

□

We conclude this section with a useful result on the linear independence of preimages of ψ_θ.

Lemma 1.14. *Let* $\alpha_1, \dots, \alpha_k \in \ker(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q})$ *and* θ *be a generator of* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$*. Suppose moreover that* $\beta_1, \dots, \beta_k \in \mathbb{F}_{q^m}$ *are such that* $\theta(\beta_i) - \beta_i = \alpha_i$*. Then, the elements* $\alpha_1, \dots, \alpha_k$ *are linearly independent over* $\mathbb{F}_q$ *if and only if the elements* $1, \beta_1, \dots, \beta_k$ *are linearly independent over* $\mathbb{F}_q$*.*

Proof. Suppose $\lambda_1, \dots, \lambda_k \in \mathbb{F}_q$ and consider the sum

$$\sum_{i=1}^{k} \lambda_i \alpha_i = \sum_{i=1}^{k} \lambda_i(\theta(\beta_i) - \beta_i) = \theta\left(\sum_{i=1}^{k} \lambda_i \beta_i\right) - \sum_{i=1}^{k} \lambda_i \beta_i = \psi_\theta\left(\sum_{i=1}^{k} \lambda_i \beta_i\right).$$

This means that a non-trivial combination of the α_i's is zero if and only if a non-trivial combination of the β_i's belongs to $\ker \psi_\theta$. This is equivalent, by part 4 of Lemma 1.2, to $\sum_i \lambda_i \beta_i \in \mathbb{F}_q$, i.e. $1, \beta_1, \dots, \beta_k$ are linearly dependent over $\mathbb{F}_q$. □

1.1.2 Norm over Finite Fields

In this subsection, we study the multiplicative counterpart of the trace map, that is the norm. It is given by the product of all the conjugates under the Galois group action, and it has properties that are similar to the trace's ones.

Definition 1.15. Let $\mathbb{F}_{q^m}/\mathbb{F}_q$ be a finite extension of fields. For $\alpha \in \mathbb{F}_{q^m}$, the *norm* of α with respect to the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ is defined by

$$\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) := \prod_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)} \sigma(\alpha) = \prod_{i=0}^{m-1} \bar{\theta}^i(\alpha) = \prod_{i=0}^{m-1} \alpha^{q^i},$$

We will refer to the function

$$\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$$

as the *norm map* of $\mathbb{F}_{q^m}/\mathbb{F}_q$.

For any θ generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, we define the map

$$\begin{aligned} \xi_\theta : \mathbb{F}_{q^m}^* &\longrightarrow \mathbb{F}_{q^m}^* \\ \alpha &\longmapsto \tfrac{\alpha}{\theta(\alpha)}. \end{aligned}$$

Lemma 1.16. *The norm map of $\mathbb{F}_{q^m}/\mathbb{F}_q$ satisfies the following properties:*

1. $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$ *for all* $\alpha \in \mathbb{F}_{q^m}$.
2. $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = 0$ *if and only if* $\alpha = 0$.
3. $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ *restricted to* $\mathbb{F}_{q^m}^*$ *is a group homomorphism from* $\mathbb{F}_{q^m}^*$ *to* $\mathbb{F}_q^*$.
4. ξ_θ *is a group homomorphism from* $\mathbb{F}_{q^m}^*$ *to itself.*
5. *For every generator* θ *of* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, $\xi_\theta(\alpha) = 1$ *if and only if* $\alpha \in \mathbb{F}_q^*$.
6. *(Hilbert's Theorem 90 for finite fields)* $\ker(\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}) = \mathrm{Im}(\xi_\theta)$ *for every generator* θ *of* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ *and has cardinality* $\frac{q^m-1}{q-1}$.

Proof. The proof is straightforward. It can be partially found in [68, Theorem 2.28]. □

Lemma 1.17. *Let* $\alpha \in \mathbb{F}_{q^m}^*$ *and* θ *be a generator of* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. *Then*

1. $$|\xi_\theta^{-1}(\{\alpha\})| = \begin{cases} q-1 & \text{if } \alpha \in \ker(\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}) \\ 0 & \text{if } \alpha \notin \ker(\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}). \end{cases}$$

2. *Let* $\alpha \in \ker(\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q})$. *If* $x_1, x_2 \in \xi_\theta^{-1}(\{\alpha\})$, *then* $\frac{x_1}{x_2} \in \mathbb{F}_q^*$, *or equivalently, there exists an* $x \in \mathbb{F}_{q^m}$ *such that*

$$\xi_\theta^{-1}(\{\alpha\}) = \left\{\lambda x \mid \lambda \in \mathbb{F}_q^*\right\}.$$

Moreover such an x *is of the form* $x = \chi(\gamma)$, *where*

$$\chi = \sum_{i=0}^{m-1} \left(\prod_{j=1}^{i} \theta^{j-1}(\alpha) \right) \theta^i,$$

and $\gamma \in \mathbb{F}_{q^m}^*$ *is such that* $\chi(\gamma) \neq 0$.

The proof of Lemma 1.17 is straightforward and can be found in any Algebra book. Note that there always exists an element $\gamma \in \mathbb{F}_{q^m}^*$ such that $\chi(\gamma) \neq 0$. This is due to the fact that, by Artin's Theorem of linear independence of characters, χ is a non-zero character.

1.1.3 Gaussian Binomials and Moore Matrices

We denote by $\mathrm{GL}_n(q) := \{A \in \mathbb{F}_q^{n\times n} \mid \mathrm{rk}(A) = n\}$ the general linear group of degree n over $\mathbb{F}_q$. Furthermore, given a finite field $\mathbb{F}_q$, we consider the Grassmannian $\mathrm{Gr}(k, \mathbb{F}_q^n)$, that is the set of all k-dimensional subspaces of the vector space $\mathbb{F}_q^n$ over $\mathbb{F}_q$. It is well known that its cardinality is given by the Gaussian binomial $\begin{bmatrix} n \\ k \end{bmatrix}_q$, defined as

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i} = \frac{\prod_{i=0}^{k-1}(q^n - q^i)}{|\,\mathrm{GL}_k(q)|}.$$

Lemma 1.18. *Let k, n be two integers such that $0 < k \leq n/2$, and let $\mathcal{U}$ be a k-dimensional vector subspace of $\mathbb{F}_q^n$. Then, for every $r = 0, \dots, k$, the number of k-dimensional subspaces that intersect $\mathcal{U}$ in a $(k-r)$-dimensional subspace is*

$$\begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2}.$$

Proof. There are $\begin{bmatrix} k \\ k-r \end{bmatrix}_q$ many subspaces $\mathcal{U}'$ of $\mathcal{U}$ of dimension $(k-r)$ that can be the intersection space. Now, in order to complete $\mathcal{U}'$ to a k-dimensional vector space, intersecting $\mathcal{U}$ only in $\mathcal{U}'$, we have $\prod_{i=0}^{r-1}(q^n - q^{k+i})$ choices for the remaining basis vectors. For a fixed basis of $\mathcal{U}'$, the number of bases spanning the same subspace is given by the number of $k \times k$ matrices of the form

$$\begin{pmatrix} I_{k-r} & 0 \\ A & B \end{pmatrix},$$

where $A \in \mathbb{F}_q^{r\times(k-r)}$ and $B \in \mathrm{GL}_r(q)$. This number is equal to $q^{r(k-r)}|\,\mathrm{GL}_r(q)| = \prod_{i=0}^{r-1}(q^k - q^{k-r+i})$. Hence, the final count is given by

$$\begin{bmatrix} k \\ k-r \end{bmatrix}_q \frac{\prod_{i=0}^{r-1}(q^n - q^{k+i})}{\prod_{i=0}^{r-1}(q^k - q^{k-r+i})} = \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2}.$$

□

In the rest of this section, we will introduce the *Moore matrix*, which is the q-analogue of the Vandermonde matrix, and state some of its most important properties.

Definition 1.19. Let $1 \leq k \leq n$ be integers. For a vector $v = (v_1, \dots, v_n) \in \mathbb{F}_{q^m}^n$ and $\theta \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, we denote by $M_{k,\theta}(v)$ the *θ-Moore matrix*, which is defined as

$$M_{k,\theta}(v) := \begin{pmatrix} v_1 & v_2 & \dots & v_n \\ \theta(v_1) & \theta(v_2) & \dots & \theta(v_n) \\ \vdots & & & \vdots \\ \theta^{k-1}(v_1) & \theta^{k-1}(v_2) & \dots & \theta^{k-1}(v_n) \end{pmatrix}.$$

The following results give a relation between the rank of a Moore matrix and the q-rank of the defining vector. The next Theorem is a generalization of [68, Corollary 2.38] and a consequence of [62, Corollary 4.13].

Theorem 1.20. *Let $\mathbb{F} \subseteq \mathbb{L}$ be a Galois field extension, $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{F})$ and $\mathbb{E} = \mathbb{L}^\sigma$ be the fixed field of σ, i.e. $\mathbb{E} = \{\alpha \in \mathbb{L} \mid \sigma(\alpha) = \alpha\}$. For $g \in \mathbb{L}^n$, consider the σ-Moore matrix $M_{s,\sigma}(g) \in \mathbb{L}^{s\times n}$ whose (i, j)-entry is $\sigma^{i-1}(g_j)$. Then $\mathrm{rk}(M_{s,\sigma}(g)) = \min\{s, r\}$, where $r = \dim_{\mathbb{E}}\langle g_1, \dots, g_n\rangle_{\mathbb{E}}$.*

Corollary 1.21. *Let θ be a generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ and $g \in \mathbb{F}_{q^m}^n$. Then $\mathrm{rk}(M_{s,\theta}(g)) = \min\{s, r\}$, where $r = \dim_{\mathbb{F}_q}\langle g_1, \dots, g_n\rangle_{\mathbb{F}_q}$.*

1.2 Linearized Polynomials

In this section we recall some basic notions on linearized polynomials. For a deeper understanding on this topic, the interested reader is referred to [119].

Linearized polynomials over finite fields have been intensively studied. They are a special type of polynomials defined over a finite field of characteristic p, with the property that the only monomials involved are x^i's, where i is a power of p. In general, let q be a power of a prime p, and m be a positive integer. One can consider *q-polynomials* over an extension field $\mathbb{F}_{q^m}$; they are polynomials in $\mathbb{F}_{q^m}[x]$ that involve only monomials of the form x^{q^i}, for some non-negative integers i. Their importance is due to the fact that, seen as functions corresponding to their evaluation, they are $\mathbb{F}_q$-linear maps from $\mathbb{F}_{q^m}$ to itself. On the other hand, any $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^m}$ to itself can be represented as a q-polynomial of degree at most q^{m-1}. Let $\mathcal{L}(\mathbb{F}_{q^m})$ denote the set of q-polynomials with coefficients in $\mathbb{F}_{q^m}$. We have that $\mathcal{L}(\mathbb{F}_{q^m})$ is closed under addition and composition. Together with these two operations, $\mathcal{L}(\mathbb{F}_{q^m})$ is a non-commutative ring. However, when one only cares about the evaluation in $\mathbb{F}_{q^m}$, can reduce to study the set

$$\mathcal{L}_m(\mathbb{F}_{q^m}) := \mathcal{L}(\mathbb{F}_{q^m})/(x^{q^m} - x).$$

This is due to the fact that $a^{q^m} = a$ for every $a \in \mathbb{F}_{q^m}$, and the set $(x^{q^m} - x)$ is a two-sided ideal. In this framework, one can easily verify that

$$\mathcal{L}_m(\mathbb{F}_{q^m}) \cong M_n(\mathbb{F}_q).$$

However, this can be seen as a consequence of the following more general setting. Let $\mathbb{F}/\mathbb{E}$ be a Galois field extension with cyclic finite Galois group

$$G := \mathrm{Gal}(\mathbb{F}/\mathbb{E}) = \langle\theta\rangle.$$

Then, $\mathbb{F}$ is a finite $\mathbb{E}$-vector space and the group algebra $\mathbb{F}[G] = \mathbb{F}[\theta]$ is a ring endowed with the addition and the composition. More in details, the elements $f, g \in \mathbb{F}[G]$ are of the form

$f=\sum_{i=0}^{m-1} f_i\theta^i$, $g=\sum_{i=0}^{m-1} g_i\theta^i$, for some $f_i, g_i \in \mathbb{F}$. The addition is defined by $f+g=\sum_{i=0}^{m-1}(f_i+g_i)\theta^i$; the composition is defined on monomials by $(f_i\theta^i)\circ(g_j\theta^j)=f_i\theta^i(g_j)\theta^{i+j}$, and then extended by linearity. In this framework, we also have that

$$\mathbb{F}[G]\cong \mathrm{End}_{\mathbb{E}}(\mathbb{F})=\{\phi:\mathbb{F}\to\mathbb{F}\mid \phi \text{ is } \mathbb{E}\text{-linear }\}.$$

This is a consequence of the more general duality theory of the trace map of finite cyclic Galois extensions, which follows from the additive version of Hilbert's Theorem 90.

For this reason, we will widely use these notions also in the context of finite fields. Let $\mathbb{F}_{q^m}/\mathbb{F}_q$ be a field extension and $G:=\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ be its Galois group. Let θ be a generator of G. We have

$$\mathbb{F}_{q^m}[G]=\mathbb{F}_{q^m}[\theta]\cong \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^m})\cong \mathcal{L}_m(\mathbb{F}_{q^m}).$$

If $\theta : a\mapsto a^{q^s}$, for some integer s coprime to m, then the isomorphism between $\mathbb{F}_{q^m}[\theta]$ and $\mathcal{L}_m(\mathbb{F}_{q^m})$ is given by

$$\sum_{i=0}^{m-1} f_i\theta^i \longmapsto \sum_{i=0}^{m-1} f_i x^{q^{si}}.$$

In order to simplify the notation and make clear this connection, we will write x^{θ^i} instead of $x^{q^{si}}$, so that

$$\mathcal{L}_m(\mathbb{F}_{q^m})=\left\{\sum_{i=0}^{m-1} f_i x^{\theta^i}\mid f_i\in\mathbb{F}_{q^m}\right\}.$$

1.3 3-Tensors

We recall some definitions and results from tensor algebra. The interested reader is referred to [15, 24] for more details. In this section, $\mathbb{F}$ denotes an arbitrary field.

Definition 1.22. Let U and V be vector spaces over $\mathbb{F}$. We define the *tensor product* $U\otimes V$ of U and V to be the $\mathbb{F}$-vector space of all elements of the form $\sum_{i=1}^{\ell} u_i\otimes v_i$, with $u_i\in U$ and $v_i\in V$ for which the following holds:

1. $\lambda(u\otimes v)=(\lambda u)\otimes v=u\otimes(\lambda v)$,
2. $(u_1+u_2)\otimes v=u_1\otimes v+u_2\otimes v$,
3. $u\otimes(v_1+v_2)=u\otimes v_1+u\otimes v_2$.

Equivalently, a tensor product of $\mathbb{F}$-spaces U and V, denoted by $U\otimes V$, is defined as a pair (T,φ), where $\varphi: U\times V\to T$ is a bilinear map to the $\mathbb{F}$-space T such that, for any bilinear map $f:U\times V\to W$ to an $\mathbb{F}$-space W, there exists a unique $\mathbb{F}$-linear map $\hat{f}:T\longrightarrow W$ satisfying $f=\hat{f}\circ\varphi$. We say that (T,φ) satisfies the *universal mapping property.* The existence and uniqueness of (T,φ), and hence the well-definedness of $U\otimes V$, can be shown by its construction as a quotient space of the free $\mathbb{F}$-linear space on $U \times V$ (see, for example, [24, Chapter 10]). Tensors of the form $u \otimes v$ are called *simple* tensors (also called *fundamental* or *pure* tensors in the literature). Arbitrary elements of $U \otimes V$ are expressed as sums of simple tensors: $\sum_{i=1}^{\ell} u_i \otimes v_i$, with $u_i \in U$ and $v_i \in V$. Since the tensor product of a pair of spaces is itself a vector space, we may construct the tensor product $(U \otimes V) \otimes W = U \otimes (V \otimes W)$, for $\mathbb{F}$-spaces U, V, W, which we therefore express as $U \otimes V \otimes W$. The corresponding map associated with such a tensor product is a trilinear map $\varphi : U \times V \times W \longrightarrow U \otimes V \otimes W$. It is important to remark that all the maps that will be given in this section are well-defined, which is a consequence of the universal mapping property.

If $\{u_1, \ldots, u_k\}$, $\{v_1, \ldots, v_n\}$ and $\{w_1, \ldots, w_m\}$ are bases of U, V and W, respectively, then a basis of $U \otimes V \otimes W$ is given by

$$\{u_i \otimes v_j \otimes w_\ell \mid 1 \leq i \leq k,\ 1 \leq j \leq n,\ 1 \leq \ell \leq m\}.$$

In particular, $\dim_{\mathbb{F}}(U \otimes V \otimes W) = \dim_{\mathbb{F}}(U) \dim_{\mathbb{F}}(V) \dim_{\mathbb{F}}(W)$.

In this dissertation we shall be mainly interested in tensor products of the form

$$\mathbb{F}^k \otimes \mathbb{F}^n \otimes \mathbb{F}^m,$$

whose elements are called 3-tensors, 3rd-order tensors, or triads. The elements of this space can be represented as 3-dimensional arrays. As with matrices (2nd-order tensors), one can define a 3-dimensional array of size $k \times n \times m$ as a function

$$X : [k] \times [n] \times [m] \longrightarrow \mathbb{F},$$

which we represent as

$$X = (X_{ij\ell} \mid 1 \leq i \leq k,\ 1 \leq j \leq n,\ 1 \leq \ell \leq m). \tag{1.1}$$

These representations of the tensor $X = \sum_{r=1}^{R} u_r \otimes v_r \otimes w_r$ are related by

$$X_{ij\ell} = \sum_{r=1}^{R} u_{ir} v_{jr} w_{\ell r},$$

where $u_r = (u_{ir} \mid 1 \leq i \leq k)$, $v_r = (v_{jr} \mid 1 \leq j \leq n)$, and $w_r = (w_{\ell r} \mid 1 \leq \ell \leq m)$. We hence identify $\mathbb{F}^k \otimes \mathbb{F}^n \otimes \mathbb{F}^m$ with the space $\mathbb{F}^{k \times n \times m}$. The representation of X as an element of $\mathbb{F}^{k \times n \times m}$ is called its *coordinate tensor*.

For the remainder of the dissertation, given vectors $z_r \in \mathbb{F}^N$, we will write z_{jr} to denote the j-th coefficient of z_r for each r. That is, $z_r := (z_{jr} \mid 1 \leq j \leq N)$.

We introduce the following maps, which define multiplication of 3-tensors with vectors (corresponding to $s = 1$) and matrices ($s > 1$).

$$m_1 : \mathbb{F}^{s\times k} \times \mathbb{F}^{k\times n\times m} \longrightarrow \mathbb{F}^{s\times n\times m} : (A, X) \mapsto m_1(A, X) = \sum_i (Au_i) \otimes v_i \otimes w_i,$$

$$m_2 : \mathbb{F}^{s\times n} \times \mathbb{F}^{k\times n\times m} \longrightarrow \mathbb{F}^{k\times s\times m} : (B, X) \mapsto m_2(B, X) = \sum_i u_i \otimes (Bv_i) \otimes w_i,$$

$$m_3 : \mathbb{F}^{s\times m} \times \mathbb{F}^{k\times n\times m} \longrightarrow \mathbb{F}^{k\times n\times s} : (C, X) \mapsto m_3(C, X) = \sum_i u_i \otimes v_i \otimes (Cw_i),$$

for any $X = \sum_i u_i \otimes v_i \otimes w_i \in \mathbb{F}^{k\times n\times m}$.

Let $X \in \mathbb{F}^{N_1\times N_2\times N_3}$. For each $i \in \{1, 2, 3\}$ and for any $A \in \mathbb{F}^{s\times \ell},\ B \in \mathbb{F}^{\ell\times N_i}$ it is easy to see that

$$m_i(AB, X) = m_i(A, m_i(B, X)). \tag{1.2}$$

Indeed, $\mathrm{GL}_{N_i}(q)$ acts on the set of tensors $\mathbb{F}^{N_1\times N_2\times N_3}$.

Remark 1.23. Notice that, in the case that $s = 1$, the operation m_1 yields a 3-tensor of the form $\sum_i \lambda_i \otimes v_i \otimes w_i$, for some scalars $\lambda_i \in \mathbb{F}$, which can be identified with the 2-tensor $\sum_i (\lambda_i v_i) \otimes w_i \in \mathbb{F}^{n\times m}$ ($\mathbb{F} \otimes V$ and V are isomorphic). Similarly, m_2 and m_3 yield 2-tensors for the case $s = 1$. With abuse of notation, in this case we will consider the images of the m_i to be in the space of matrices over $\mathbb{F}$.

Definition 1.24. Let $X \in \mathbb{F}^{N_1\times N_2\times N_3}$. For each $i \in \{1, 2, 3\}$, we define the i-th *slice space* of X to be the $\mathbb{F}$-span of $\{m_i(e_j, X) \mid 1 \leq j \leq N_i\}$, that is,

$$\mathrm{ssp}_i(X) := \langle m_i(e_1, X), \ldots, m_i(e_{N_i}, X)\rangle.$$

We write $\dim_i(X)$ to denote the dimension of $\mathrm{ssp}_i(X)$ as an $\mathbb{F}$-vector space. We say that $\mathrm{ssp}_i(X)$ is *nondegenerate* if $\dim_i(X) = N_i$, in which case we say that X is *i-nondegenerate.*

If $X = \sum_{r=1}^{R} u_r \otimes v_r \otimes w_r \in \mathbb{F}^{k\times n\times m}$, then clearly

$$\mathrm{ssp}_1(X) = \left\langle \sum_{r=1}^{R} u_{jr} v_r \otimes w_r \mid 1 \leq j \leq k \right\rangle,$$

where for each r, $u_r = (u_{jr} \mid 1 \leq j \leq k) \in \mathbb{F}^k$. In particular, $\mathrm{ssp}_1(X)$ is the $\mathbb{F}$-span of k matrices

$$A_j = \sum_r u_{jr} v_r \otimes w_r = m_1(e_j, X) \in \mathbb{F}^{n\times m},$$

of rank at most R, which form a basis of $\mathrm{ssp}_1(X)$ if X is 1-nondegenerate.

We also point out the simple fact that for every basis $g_1, \dots, g_{N_i}$ of $\mathbb{F}^{N_i}$ we have

$$\mathrm{ssp}_i(X) = \langle m_i(g_1, X), \dots, m_i(g_{N_i}, X)\rangle.$$

In particular, for every $G \in \mathrm{GL}_{N_i}(q)$ we have

$$\mathrm{ssp}_i(X) = \mathrm{ssp}_i(m_i(G, X)).$$

Of particular interest in this work, is the 1st slice space $\mathrm{ssp}_1(X)$ of a nondegenerate 3-tensor $X \in \mathbb{F}_q^{k\times n\times m}$, which will be a k-dimensional subspace of matrices in $\mathbb{F}_q^{n\times m}$.

A notable parameter of a tensor that relates to algebraic complexity is its *tensor rank*, which we now define.

Definition 1.25. Let $X \in \mathbb{F}^{k\times n\times m}$. The *tensor rank* of X is the minimum integer R such that there exist $u_r \in \mathbb{F}^k, v_r \in \mathbb{F}^n, w_r \in \mathbb{F}^m$ with

$$X = \sum_{r=1}^{R} u_r \otimes v_r \otimes w_r.$$

We write $\mathrm{trk}(X)$ to denote the tensor rank of X. A representation of the X as sum of $R = \mathrm{trk}(X)$ simple tensors is called a *minimal rank form* of X.

The reader will easily verify that

$$\mathrm{trk}(m_1(A, X)) \leq \mathrm{trk}(X), \tag{1.3}$$

for any $A \in \mathbb{F}^{s\times k}$ (with analogous statements for elements in the image of m_2 and m_3). Moreover, it is straightforward to check that the tensor rank is invariant under any permutation of the spaces $\mathbb{F}^k, \mathbb{F}^n, \mathbb{F}^m$.

The following result gives various characterizations of the tensor rank; see for example [15, Proposition 14.45]. As we will use the construction of these characterizations in Lemma 6.6, we include a proof.

Proposition 1.26. *Let $X \in \mathbb{F}^{k\times n\times m}$ and let $R > 0$ be an integer. The following are equivalent.*

1. $\mathrm{trk}(X) \leq R$.

2. *There exist $A_1, \dots, A_R \in \mathbb{F}^{n\times m}$ of rank 1 such that $\mathrm{ssp}_1(X) \subseteq \langle A_1, \dots, A_R\rangle$.*

3. *There exist diagonal matrices $D_1, \dots, D_k \in \mathbb{F}^{R\times R}$, and matrices $P \in \mathbb{F}^{n\times R}$, $Q \in \mathbb{F}^{m\times R}$ such that*

$$\mathrm{ssp}_1(X) = P\langle D_1, \dots, D_k\rangle Q^\top := \langle PD_1Q^\top, \dots, PD_kQ^\top\rangle.$$

Proof. Suppose that $\operatorname{trk}(X) \leq R$. Then $X = \sum_{r=1}^{R} u_r \otimes v_r \otimes w_r$ for some vectors $u_r \in \mathbb{F}^k$, $v_r \in \mathbb{F}^n$, $w_r \in \mathbb{F}^m$ and

$$\operatorname{ssp}_1(X) = \left\langle \sum_r u_{jr} v_r \otimes w_r \mid 1 \leq j \leq k \right\rangle \subseteq \langle v_r \otimes w_r \mid 1 \leq r \leq R \rangle.$$

Conversely, if $\operatorname{ssp}_1(X)$ is contained in the span of R rank 1 matrices $A_r = v_r \otimes w_r$, then for all $1 \leq j \leq k$ there exist $u_{jr} \in \mathbb{F}$ satisfying $m_1(e_j, X) = \sum_{r=1}^{R} u_{jr} v_r \otimes w_r$. Therefore $X = \sum_{r=1}^{R} u_r \otimes v_r \otimes w_r$ and $\operatorname{trk}(X) \leq R$.

Again suppose that $X = \sum_{r=1}^{R} u_r \otimes v_r \otimes w_r$ for some $u_r \in \mathbb{F}^k, v_r \in \mathbb{F}^n, w_r \in \mathbb{F}^m$. Let

$$D_j = \operatorname{diag}(u_{jr}, 1 \leq r \leq R).$$

So the diagonal elements of D_j are the j-th coefficients of the u_r. Set

$$P = (v_{jr} \mid 1 \leq j \leq n, 1 \leq r \leq R), \qquad Q = (w_{jr} \mid 1 \leq j \leq m, 1 \leq r \leq R).$$

Then $P D_j Q^\top = \sum_{r=1}^{R} u_{jr} v_r \otimes w_r$ for each j and hence $\operatorname{ssp}_1(X) = P\langle D_1, \dots, D_k \rangle Q^\top$. Conversely, given the existence of matrices P, Q, D_i satisfying (3), the tensor X can be constructed as $\sum_{r=1}^{R} u_r \otimes v_r \otimes w_r$, where v_r is the r-th column of P, w_r is the r-th column of Q and u_{jr} is the r-th element of the main diagonal of D_j for each j. □

Example 1.27. The following example, adapted from [65], illustrates the preceding definitions and propositions. Consider the tensor $X = e_1 \otimes (e_1 \otimes e_1 + e_2 \otimes e_2) + e_2 \otimes (e_1 \otimes e_2 + e_2 \otimes e_3)$ in $\mathbb{F}^2 \otimes \mathbb{F}^2 \otimes \mathbb{F}^3$, where $\mathbb{F}$ is any field of characteristic not two. Then

$$\operatorname{ssp}_1(X) = \left\langle \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle.$$

Then X can be written as the sum of the three rank one tensors

$$\begin{aligned} X_1 &= e_1 \otimes e_1 \otimes (e_1 - e_3) \\ X_2 &= \frac{1}{2}(e_1 + e_2) \otimes (e_1 + e_2) \otimes (e_2 + e_3) \\ X_3 &= \frac{1}{2}(-e_1 + e_2) \otimes (e_1 - e_2) \otimes (e_2 - e_3), \end{aligned}$$

which corresponds to the fact that $\operatorname{ssp}_1(X)$ is contained in

$$\left\langle \begin{pmatrix} 1 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & -1 \\ 0 & -1 & 1 \end{pmatrix} \right\rangle.$$

The matrices P, Q are given by

$$P = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \end{pmatrix}; \qquad Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ -1 & 1 & -1 \end{pmatrix},$$

and $D_1 = \operatorname{diag}(1, 1/2, -1/2)$, $D_2 = \operatorname{diag}(0, 1/2, 1/2)$.

It was shown in [50] that computing the tensor rank of a 3-tensor over a finite field is NP-complete. However, we have the following bound on the tensor rank, which was proved by Kruskal; see [60, Corollary 1].

Theorem 1.28 (Kruskal's tensor rank bound)**.** *Let $X \in \mathbb{F}^{k\times n\times m}$ be* 1*-nondegenerate. Then*

$$\operatorname{trk}(X) \geq \dim_1(X) + \min\{\operatorname{trk}(m_1(u, X)) \mid u \in \mathbb{F}^k \setminus \{0\}\} - 1.$$

We will see later in Chapters 3 and 6 that this inequality will assume an important role in the framework of rank-metric codes.

Another operation that is important in the context of tensors, is the so-called *contraction* with respect to some indices. Since in this work we will only need one particular contraction, we will not define this concept in general, but only for the following case.

Definition 1.29. Let $k, k', n, m \in \mathbb{N}$, and let

$$X = \sum_i u_i \otimes v_i \otimes w_i \in \mathbb{F}^{k\times n\times m}, \qquad Y = \sum_j u'_j \otimes v'_j \otimes w'_j \in \mathbb{F}^{k'\times n\times m}$$

be tensors. We define the *double-dot product* between X and Y, as the 2-tensor (i.e., the matrix) $X : Y \in \mathbb{F}_q^{k\times k'}$ given by

$$X : Y = \sum_{i,j} (v_i \cdot v'_j)(w_i \cdot w'_j) u_i \otimes u'_j,$$

where the *dot product* between two vectors $a, b \in \mathbb{F}_q^N$ is defined to be $a \cdot b := \sum_{i=1}^N a_i b_i$.

In terms of their coordinate tensor representations, if we write $X = (X_{ij\ell})$ and $Y = (Y_{sj\ell})$, then it is straightforward to see that the double-dot product $X : Y$ will have coordinate representation defined by

$$(X : Y)_{is} = \sum_{j,\ell} X_{ij\ell} Y_{sj\ell}, \qquad \text{for } 1 \leq i \leq k, 1 \leq s \leq k'.$$

The definition also extends when one (or even both) of the tensors is a 2-tensor, i.e. a matrix, considering $A \in \mathbb{F}^{n\times m}$ as an element in $\mathbb{F}^{1\times n\times m}$. In particular, for two matrices $A, B \in \mathbb{F}^{n\times m}$, we have

$$A : B = \operatorname{Tr}(AB^\top),$$

that is, the double-dot product between two matrices corresponds to their trace-product. Moreover, it is straightforward to prove that, for $A \in \mathbb{F}^{s\times k}$, $B \in \mathbb{F}^{s\times k'}$, $X \in \mathbb{F}^{k\times n\times m}$, and $Y \in \mathbb{F}^{k'\times n\times m}$ we have

$$\begin{aligned} &m_1(A,X) : Y = A(X : Y),\\ &X : m_1(B,Y) = (X : Y)B^{\top}. \end{aligned} \tag{1.4}$$

1.4 Codes in the Hamming Metric and GRS Codes

In classical coding theory the most studied and well-known class of codes is definitely represented by generalized Reed-Solomon codes. These codes were introduced in [93] and through the years were deeply studied by many authors. Their importance is due to the fact that they are maximum distance separable, and possess very fast algorithms for their encoding and decoding procedures [47, 59]. The interested reader is referred to [75, 95, 115] for more details on the theory or error-correcting codes. In this section we are going to briefly describe them, focusing in particular on their generator matrices.

Definition 1.30. Let n be a positive integer. The *Hamming weight* is defined on $\mathbb{F}_q^n$ as

$$\mathrm{wt}_H(v) = |\{i \in [n] \mid v_i \neq 0\}|.$$

The *Hamming distance* d_H on $\mathbb{F}_q^n$ is defined as

$$\begin{array}{rccc} d_H : & \mathbb{F}_q^n \times \mathbb{F}_q^n & \longrightarrow & \mathbb{N} \\ & (u,v) & \longmapsto & \mathrm{wt}_H(u-v). \end{array}$$

It is well-known that d_H defines indeed a metric on $\mathbb{F}_q^n$. With this metric, classical coding theory was developed in the last 70 years, focusing on many different classes of codes. In this section we will only consider linear codes.

Definition 1.31. Let $0 < k \leq n$ be two positive integers. A *linear code* C of dimension k and length n over a finite field $\mathbb{F}_q$ is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$ equipped with the Hamming distance. The *minimum distance* of C is the integer

$$d_H(C) := \min\left\{d_H(u,v) \mid u,v \in C, u \neq v\right\}.$$

A matrix $G \in \mathbb{F}_q^{k\times n}$ is called a *generator matrix* for the code C if $C = \mathrm{rowsp}(G)$, where $\mathrm{rowsp}(G)$ denotes the subspace generated by the rows of G, called the *row space* of G.

We will refer to a linear code $C \subseteq \mathbb{F}_q^n$ of dimension k as an $[n,k]_q$ block code. When also the minimum distance d is known, we will call it an $[n,k,d]_q$ block code. Sometimes, the word "block" will be omitted.

It is well known that the minimum distance d of any linear code of dimension k and length n satisfies the following inequality:

$$d \leq n - k + 1.$$

This bound is known as Singleton bound [112].

Definition 1.32. A code meeting the Singleton bound is called a *maximum distance separable (MDS) code.*

Among all the possible generator matrices of an MDS code, there exists one in a special form. Indeed, it is easy to verify that every MDS code of length n and dimension k has a generator matrix of the form $G = (I_k \mid X)$, where $X \in \mathbb{F}_q^{k\times(n-k)}$ and I_k denotes the $k \times k$ identity matrix. Such a generator matrix is said to be in *standard form*, or equivalently, in *systematic form.* Moreover, MDS codes can be characterized using their generator matrix in standard form. Let $\mathbb{F}$ be a field. Recall that a matrix $X \in \mathbb{F}^{r\times s}$ is said to be *superregular* if all its minors are non-zero.

Theorem 1.33. *Let C be an $[n, k]_q$ block code with generator matrix $(I_k \mid X)$. Then, C is MDS if and only if X is a superregular matrix.*

Now we introduce the most prominent family of MDS codes. Let $0 < k \leq n$ be two positive integers, and consider the set of polynomials over $\mathbb{F}_q$ of degree strictly less than k, namely

$$\mathbb{F}_q[x]_{<k} := \{f(x) \in \mathbb{F}_q[x] \mid \deg f < k\}.$$

Definition 1.34. Suppose that $n \leq q$, and consider $\alpha_1, \dots, \alpha_n \in \mathbb{F}_q$ pairwise distinct elements, and $b_1, \dots, b_n \in \mathbb{F}_q^*$. The code

$$C = \{(b_1 f(\alpha_1), b_2 f(\alpha_2), \dots, b_n f(\alpha_n)) \mid f \in \mathbb{F}_q[x]_{<k}\}$$

is called *Generalized Reed-Solomon (GRS) code* and it is denoted by $\mathrm{GRS}_k(\alpha, b)$, where $\alpha = (\alpha_1, \dots, \alpha_n)$ and $b = (b_1, \dots, b_n)$.

It is well-known that the canonical generator matrix for $C = \mathrm{GRS}_k(\alpha, b)$ is given by the *weighted Vandermonde matrix* that is

$$\begin{pmatrix} b_1 & b_2 & \dots & b_n \\ b_1\alpha_1 & b_2\alpha_2 & \dots & b_n\alpha_n \\ b_1\alpha_1^2 & b_2\alpha_2^2 & \dots & b_n\alpha_n^2 \\ \vdots & \vdots & & \vdots \\ b_1\alpha_1^{k-1} & b_2\alpha_2^{k-1} & \dots & b_n\alpha_n^{k-1} \end{pmatrix} = V_k(\alpha)\mathrm{diag}(b),$$

where $V_k(\alpha)$ is the classical Vandermonde matrix, and $\mathrm{diag}(b)$ denotes the diagonal matrix whose diagonal entries are given by $b_1, \dots, b_n$. This generator matrix is obtained by choosing the set of monomials $\left\{1, x, x^2, \ldots, x^{k-1}\right\}$ as an $\mathbb{F}_q$-basis of $\mathbb{F}_q[x]_{<k}$, and then evaluating each of them in the points $\alpha_1, \ldots, \alpha_n$. This is why we refer to it as the *canonical generator matrix.*

The following result can be found in any coding theory book.

Theorem 1.35. *Let* $1 \leq k \leq n$ *be integers,* $\alpha, b \in \mathbb{F}_q^n$ *as in Definition 1.34 and let* $C = \mathrm{GRS}_k(\alpha, b)$*. Then,* $\dim(C) = k$ *and* $d_H(C) = n-k+1$*, i.e. GRS codes are MDS.*

In 1985 Roth and Seroussi [98] studied the generator matrix in standard form of a GRS code, giving a complete characterization.

Definition 1.36. Let r, s be positive integers, $x_1, \ldots, x_r, y_1, \ldots, y_s \in \mathbb{F}_q$, $c_1, \ldots, c_r$, $d_1, \ldots, d_s \in \mathbb{F}_q^*$ be elements such that

(a) $x_1, \ldots, x_r$ pairwise distinct,

(b) $y_1, \ldots, y_s$ pairwise distinct,

(c) $y_i \in \mathbb{F}_q \setminus \{x_1, \ldots, x_r\}$, for $i = 1, \ldots, s$.

The matrix $A \in \mathbb{F}_q^{r \times s}$ defined by

$$a_{i,j} = \frac{c_i d_j}{x_i - y_j}$$

is called *Generalized Cauchy (GC) matrix.*

Theorem 1.37. *[98, Theorem 1]*

1. *If* $C = \mathrm{GRS}_{n,k}(\alpha, b)$*, then* C *has a generator matrix in standard form* $(I_k \mid X)$*, where* $X \in \mathbb{F}_q^{k \times (n-k)}$ *is a GC matrix.*

2. *If* $X \in \mathbb{F}_q^{k \times (n-k)}$ *is a GC matrix then the code* $C = \mathrm{rs}(I_k \mid X)$ *is a Generalized Reed-Solomon code.*

Theorem 1.37 gives a correspondence between GRS codes of dimension k and length n over $\mathbb{F}_q$, and $k \times (n-k)$ GC matrices over $\mathbb{F}_q$. Moreover, in [97], a characterization of GC matrices in terms of their entries was given. We are now going to reformulate this result for our purpose, in order to underline that it gives a way to determine whether a code is a GRS code in terms of its generator matrix in standard form.

Let $A \in (\mathbb{F}_q^*)^{r \times s}$ with entries $a_{i,j}$. We denote by $A^{(-1)}$ the $r \times s$ matrix over $\mathbb{F}_q^*$ whose entries are $a_{i,j}^{-1}$.

Theorem 1.38. *[97, Lemma 7] Let* $X \in \mathbb{F}_q^{k \times (n-k)}$ *and let* C *be the linear code whose generator matrix in standard form is* $(I_k \mid X)$*. Then,* C *is a GRS code if and only if*

(i) *every entry* $x_{i,j}$ *is non-zero,*

(ii) *every* 2×2 *minor of* $X^{(-1)}$ *is non-zero,*

(iii) $\mathrm{rk}(X^{(-1)}) = 2$.

Chapter 2

Rank-Metric Codes

Rank-metric codes have received a lot of attention in the last decades, due to their applications in network coding, distributed storage and post-quantum cryptography. Originally introduced independently by Delsarte [30] in 1978 and Gabidulin [36] in 1985, these codes were first considered for applications by Roth [96] in 1991, who used them for correcting crisscross errors. In his seminal paper, Delsarte showed that the parameters of these codes must satisfy a Singleton-like bound on the cardinality. Codes meeting this bound with equality are called *maximum rank distance* (or shortly *MRD) codes*. Delsarte also provided a first construction of a family of MRD codes, which was then explained by Gabidulin in terms of evaluations of q-polynomials. These codes were then generalized in [61] and they are known as *(generalized) Gabidulin codes*.

In recent years, rank-metric codes in general, and MRD codes in particular, have been investigated both for their applications and for their links with other mathematical areas. Their connection with semifields has been recently pointed out in [106]. Indeed, the recent construction of twisted Gabidulin codes is a generalization of the twisted semifields introduced by Albert [1]. Furthermore, MRD codes have been studied in connection to important geometric objects, such as linear sets [73]. In addition, some combinatorial techniques had led to new results in rank-metric codes and their duality theory [92, 9, 18].

In this chapter, we give some basic notions and results on rank-metric codes. We study these codes both as spaces of matrices with coefficient in a finite field $\mathbb{F}_q$, and as spaces of vectors over an extension field $\mathbb{F}_{q^m}$. We describe carefully the notions of duality and code equivalence, explaining how they are related in the two different representations.

2.1 Vector Codes

In [36], Gabidulin introduces a class of rank-metric codes that are linear over the extension field $\mathbb{F}_{q^m}$. They are defined as follows.

Definition 2.1. Let $\mathbb{F}_{q^m}$ be an extension field of $\mathbb{F}_q$, and let $g = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$. We define the $\mathbb{F}_{q^m}$*-support of* g *over* $\mathbb{F}_q$ the $\mathbb{F}_q$-subspace

$$\mathrm{supp}_q(g) := \langle g_1, \ldots, g_n \rangle_{\mathbb{F}_q}.$$

Moreover, we denote by $\mathrm{rk}_q(g) = \dim_{\mathbb{F}_q}(\mathrm{supp}_q(g))$, which is called the *$q$-rank of g*.

Definition 2.2. The *rank distance* between $u, v \in \mathbb{F}_{q^m}^n$ is defined as $d(u, v) := \mathrm{rk}_q(u - v)$. A *(vector) rank-metric code* is an $\mathbb{F}_{q^m}$-linear subspace $C \subseteq \mathbb{F}_{q^m}^n$. If $C \neq \{0\}$, then the *minimum distance* of C is the integer

$$d(C) := \min\{\mathrm{rk}_q(u) \mid u \in C,\ u \neq 0\} = \min\{d(u, v) \mid u, v \in C,\ u \neq v\}.$$

It is easy to verify that the map $d : \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n \to \mathbb{N}$ defines a metric on $\mathbb{F}_{q^m}^n$. From now on, we will refer to a vector rank-metric code $C \subseteq \mathbb{F}_{q^m}^n$ of dimension k as an $[n, k]_{q^m}$ code. When also the minimum distance d is known, we will call it an $[n, k, d]_{q^m}$ code.

Let V, W be vector spaces over a field $\mathbb{F}$. Recall that a map $\varphi : V \longrightarrow W$ is called *semilinear*, if there exists $\tau \in \mathrm{Aut}(\mathbb{F})$ such that, for all $x, y \in V$ and $\lambda \in \mathbb{F}$, it holds that

1. $f(x + y) = f(x) + f(y)$.
2. $f(\lambda x) = \tau(\lambda) f(x)$.

When $V = W$, then the set of semilinear maps which are invertible is a group, called *general semilinear group* and denoted by $\Gamma\mathrm{L}(V)$. Furthermore, $\Gamma\mathrm{L}(V) \cong \mathrm{GL}(V) \rtimes \mathrm{Aut}(\mathbb{F})$.

Definition 2.3. Two vector rank-metric codes $C, C' \subseteq \mathbb{F}_{q^m}^n$ are *(semilinearly) equivalent* if there exists an $\mathbb{F}_{q^m}$-semilinear isometry $\varphi : (\mathbb{F}_{q^m}^n, d) \to (\mathbb{F}_{q^m}^n, d)$ such that $\varphi(C) = C'$.

Let $q = p^r$ for a prime p, and denote by $\mathrm{Aut}(\mathbb{F}_{q^m}) = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ the *automorphism group* of $\mathbb{F}_{q^m}$.

The semilinear rank isometries on $\mathbb{F}_{q^m}^n$ are induced by the semilinear isometries on $\mathbb{F}_q^{n \times m}$ and are hence well-known, see e.g. [8, 77, 118].

Theorem 2.4. *[8, Corollary 1][77, Proposition 2] The semilinear $\mathbb{F}_q$-rank isometries on $\mathbb{F}_{q^m}^n$ are of the form*

$$(\lambda, A, \sigma) \in \left(\mathbb{F}_{q^m}^* \times \mathrm{GL}_n(q)\right) \rtimes \mathrm{Aut}(\mathbb{F}_{q^m}),$$

acting on $\mathbb{F}_{q^m}^n$ via

$$(v_1, \ldots, v_n)(\lambda, A, \sigma) = (\sigma(\lambda v_1), \ldots, \sigma(\lambda v_n))A.$$

In particular, if $C \subseteq \mathbb{F}_{q^m}^n$ is a vector code with minimum rank distance d, then $C' = \sigma(\lambda C)A$ is a vector code with minimum rank distance d.

If $C, C' \in \mathbb{F}_{q^m}^n$ are equivalent vector rank-metric codes, then we will write $C \sim_v C'$, or simply $C \sim C'$.

Recall that the *standard inner-product* (or *dot product*) of $u, v \in \mathbb{F}_{q^m}^n$ is $\langle u; v\rangle := \sum_{i=1}^n u_i v_i$. It is well-known and easy to see that the map $(u, v) \mapsto \langle u; v\rangle$ defines an $\mathbb{F}_{q^m}$-bilinear, symmetric and nondegenerate form on $\mathbb{F}_{q^m}^n$. Sometimes, we will also denote the standard inner-product between two vectors u, v by $u \cdot v$.

Definition 2.5. The *dual* of a $[n, k]_{q^m}$ vector rank-metric code C is

$$C^\perp := \{u \in \mathbb{F}_{q^m}^n \mid \langle u; v\rangle = 0 \text{ for all } v \in C\}.$$

Note that $C^\perp$ is an $[n, n-k]_{q^m}$ code.

2.2 Matrix Codes

Definition 2.6. The *rank distance* between $X, Y \in \mathbb{F}_q^{n\times m}$ is defined as $d(X, Y) := \mathrm{rk}(X - Y)$. A *(matrix) rank-metric code* is an $\mathbb{F}_q$-linear subspace $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$. If $\mathcal{C} \neq \{0\}$, then the *minimum distance* of $\mathcal{C}$ is the integer

$$d(\mathcal{C}) := \min\{\mathrm{rk}(X) \mid X \in \mathcal{C},\ X \neq 0\} = \min\{d(X, Y) \mid X, Y \in \mathcal{C},\ X \neq Y\}.$$

It is easy to check that the map $d : \mathbb{F}_q^{n\times m} \times \mathbb{F}_q^{n\times m} \to \mathbb{N}$ defines a metric on $\mathbb{F}_q^{n\times m}$. From now on, we will refer to a rank-metric code $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ of dimension k as an $[n \times m, k]_q$ code. When also the minimum distance d is known, we will call it an $[n \times m, k, d]_q$ code.

Also in the rank metric, one can define the notion of equivalence of codes.

Definition 2.7. Two rank-metric codes $\mathcal{C}, \mathcal{C}' \subseteq \mathbb{F}_q^{n\times m}$ are *(semilinearly) equivalent* if there exists an $\mathbb{F}_q$-semilinear isometry $\varphi : (\mathbb{F}_q^{n\times m}, d) \to (\mathbb{F}_q^{n\times m}, d)$ such that $\varphi(\mathcal{C}) = \mathcal{C}'$.

If $\mathcal{C}, \mathcal{C}' \in \mathbb{F}_q^{n\times m}$ are equivalent rank-metric codes, then we will write $\mathcal{C} \sim_m \mathcal{C}'$, or simply $\mathcal{C} \sim \mathcal{C}'$.

As a semilinear isometry of $\mathbb{F}_q^{n\times m}$ is necessarily bijective, equivalent codes have the same dimension and minimum distance. According to [54, 118], in which all the $\mathbb{F}_q$-semilinear isometries are classified, we have the following result.

Theorem 2.8. *[54, 118] Let $\mathcal{C}, \mathcal{C}' \subseteq \mathbb{F}_q^{n\times m}$ be two rank-metric codes. Then, $\mathcal{C} \sim \mathcal{C}'$ if and only if there exist invertible matrices $A \in \mathrm{GL}_n(q)$, $B \in \mathrm{GL}_m(q)$ and a field automorphism $\tau \in \mathrm{Aut}(\mathbb{F}_q)$ such that*

$$\mathcal{C}' = A\tau(\mathcal{C})B := \{A\tau(X)B \mid X \in \mathcal{C}\},$$

or, when $m = n$,

$$\mathcal{C}' = A\tau(\mathcal{C})^\top B := \left\{A\tau(X)^\top B \mid X \in \mathcal{C}\right\}.$$

Recall that the *trace-product* of $X, Y \in \mathbb{F}_q^{n\times m}$ is $\langle X; Y\rangle := \mathrm{Tr}(XY^\top)$. It is well-known and easy to see that the map $(X,Y) \mapsto \mathrm{Tr}(XY^\top)$ defines an $\mathbb{F}_q$-bilinear, symmetric and nondegenerate form on $\mathbb{F}_q^{n\times m}$.

Definition 2.9. The *dual* of an $[n \times m, k]_q$ code is

$$\mathcal{C}^\perp := \{X \in \mathbb{F}_q^{n\times m} \mid \langle X; Y\rangle = 0 \text{ for all } Y \in \mathcal{C}\}.$$

Note that $\mathcal{C}^\perp$ is an $[n \times m, nm - k]_q$ code.

Remark 2.10. We denoted by $\mathcal{C}^\perp$ the dual codes in both vector and matrix frameworks. This is not really an abuse of notation, since for row vectors u, v we have $\langle u; v\rangle = \sum_i u_i v_i = \mathrm{Tr}(uv^\top)$.

We also define the column support and row support of a rank-metric code. See [45] for a detailed analysis of the various definitions of rank-support proposed in the literature. For this purpose, it is important to introduce the notion of row space and column space of a matrix $A \in \mathbb{F}^{k\times n}$, where $\mathbb{F}$ is a field. They are defined as the $\mathbb{F}$-subspace generated by the rows, respectively the columns, of A, and denoted by $\mathrm{rowsp}(A)$ and $\mathrm{colsp}(A)$.

Definition 2.11. Let $\mathcal{C}$ be a rank-metric code. The *column support* and the *row support* of $\mathcal{C}$ are defined to be the $\mathbb{F}_q$-subspaces of $\mathbb{F}_q^n$ and $\mathbb{F}_q^m$, respectively, defined by

$$\mathrm{csupp}(\mathcal{C}) := \sum_{M\in\mathcal{C}} \mathrm{colsp}(M), \qquad \mathrm{rsupp}(\mathcal{C}) := \sum_{M\in\mathcal{C}} \mathrm{rowsp}(M),$$

where the sums are sums of vector subspaces. The code $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ is said to be *nondegenerate* if $\mathrm{csupp}(\mathcal{C}) = \mathbb{F}_q^n$ and $\mathrm{rsupp}(\mathcal{C}) = \mathbb{F}_q^m$.

2.3 Maximum Rank Distance Codes

The following result is the rank-metric analogue of the Singleton bound for codes with the Hamming metric.

Theorem 2.12. *[30, Theorem 5.4] Let $n \leq m$ be two positive integers and $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ be a non-zero code. Then*

$$\dim_{\mathbb{F}_q}(\mathcal{C}) \leq m(n - d(\mathcal{C}) + 1).$$

Definition 2.13. A code $\mathcal{C}$ is *maximum rank distance* (*MRD*) if it meets the bound of Theorem 2.12, or if it is the zero code.

In this framework, it is easy to see that a vector code $C \subseteq \mathbb{F}_{q^m}^n$ is MRD if and only if

$$d(C) = n - \dim_{\mathbb{F}_{q^m}}(C) + 1.$$

The property of being MRD satisfies a duality statement, both for vector and matrix codes with their respective duality notions defined in Definitions 2.5 and 2.9.

Theorem 2.14. *[30, 36]*

1. *Let C be an $[n,k]_{q^m}$ MRD code. Then $C^\perp$ is an $[n,n-k]_{q^m}$ MRD code.*
2. *Let $\mathcal{C}$ be an $[n\times m,k]_q$ MRD code. Then $\mathcal{C}^\perp$ is an $[n\times m,nm-k]_q$ MRD code.*

2.4 Operations on Codes

In this section we focus on operations on rank-metric codes, on both vector and matrix representations. In particular, we analyze the puncturing and shortening, which are related by a duality statement in both the frameworks.

2.4.1 Vector Codes

For any matrix $G\in\mathbb{F}_{q^m}^{k\times n}$, and set $I\subseteq[n]$ satisfying $0<|I|<n$, we denote by $G^I\in\mathbb{F}_{q^m}^{k\times|I|}$ the submatrix whose columns are those of G indexed by I, and by $\bar{I}$ the complement of I in $[n]$, i.e. $\bar{I}=[n]\setminus I$.

Definition 2.15. Let C be an $[n,k]_{q^m}$ code and $A\in\mathrm{GL}_n(q)$. Let $I\subseteq[n]$ satisfy $0<|I|<n$, We define the *punctured* and *shortened* codes of C with respect to A and I by

$$\Pi(C,A,I):=\left\{(cA)^{\bar{I}}\mid c\in C\right\}\subseteq\mathbb{F}_{q^m}^{n-|I|},\quad \Sigma(C,A,I):=\left\{(cA)^{\bar{I}}\mid c\in C,(cA)^I=0\right\}\subseteq\mathbb{F}_{q^m}^{n-|I|}.$$

Proposition 2.16. *Let C be an $[n,k]_{q^m}$ code, and let $2\leq d\leq n$. The following are equivalent.*

1. *$d(C)\geq d$.*
2. *For every $A\in\mathrm{GL}_n(q)$ and $I\subseteq[n]$ satisfying $|I|\leq d-1$, the punctured code $\Pi(C,A,I)$ has dimension k.*

Proof. Let $A\in\mathrm{GL}_n(q)$ and $I\subseteq[n]$ with $|I|\leq d-1$, and consider the map

$$\begin{array}{rcl} f_{A,I}:\mathbb{F}_{q^m}^n & \longrightarrow & \mathbb{F}_{q^m}^{n-|I|} \\ c & \longmapsto & (cA)^{\bar{I}}. \end{array}$$

For any non-zero $c\in C$, we have $\mathrm{rk}_q(cA)=\mathrm{rk}_q(c)\geq d$. Moreover, $\mathrm{rk}_q((cA)^{\bar{I}})\geq\mathrm{rk}_q(cA)-|I|\geq 1$. Therefore, $\ker(f_{A,I})\cap C=\{0\}$ and $f_{A,I}$ restricted to C is injective.

On the other hand, suppose $d(C)=r\leq d-1$, and let $c\in C$ such that $\mathrm{rk}_q(c)=r$, and let $\langle v_1,\dots,v_r\rangle=\mathrm{supp}_q(c)$. There exists $A\in\mathrm{GL}_n(q)$ such that $cA=(v_1,\dots,v_r,0,\dots,0)$. Taking $I=[r]$, we get that $f_{A,I}(c)=0$, and $\ker(f_{A,I})\cap C\supseteq\langle c\rangle$. Therefore, with this choice of A and I, the dimension of $\Pi(C,A,I)$ is at most $k-1$, which yields a contradiction.

□

The following result is known for classical Hamming metric codes. We could not find a reference for this statement, but it directly follows from the classical case.

Theorem 2.17. *Let $C \subseteq \mathbb{F}_{q^m}^n$ be a vector rank-metric code, $A \in \mathrm{GL}_n(q)$ and $I \subseteq [n]$ with $0 < |I| < n$. Then*

$$\Pi(C, A, I)^{\perp} = \Sigma(C^{\perp}, (A^{\top})^{-1}, I).$$

Proposition 2.18. *Let C be an $[n,k]_{q^m}$ code and let $2 \leq d \leq n$. The following are equivalent.*

1. *$d(C) \geq d$.*

2. *For every $I \subseteq [n]$ with $|I| = n - d + 1$, for every $A \in \mathrm{GL}_n(q)$, $\Sigma(C, A, I) = \{0\}$.*

Proof. From Proposition 2.16, $d(C) \geq d$ if and only if, for every I with $|I| = n - d + 1$ and $A \in \mathrm{GL}_n(q)$, $\Pi(C, A, \bar{I})$ and C are isomorphic under the map $f_{A,\bar{I}}$, which was defined in the proof of the same Proposition. The kernel of this map is in one-to-one correspondence with $\Sigma(C, A, I)$, which shows the desired equivalence. □

2.4.2 Matrix Codes

Let $M \in \mathbb{F}_q^{n \times m}$. For any $I \subseteq [n]$, $J \subseteq [m]$ satisfying $0 < |I| < n$, $0 < |J| < m$, respectively, we denote by $M_I \in \mathbb{F}_q^{|I| \times m}$ the matrix whose rows are those of M indexed by I and by $M^J \in \mathbb{F}_q^{n \times |J|}$ the submatrix whose columns are those of M indexed by J.

Definition 2.19. Let $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ be a matrix rank-metric code and let $A \in \mathrm{GL}_n(q)$, $B \in \mathrm{GL}_m(q)$. Let $I \subseteq [n]$, $J \subseteq [m]$ satisfy $0 < |I| < n$, $0 < |J| < m$. We define the *row-punctured* and *row-shortened* codes of $\mathcal{C}$ with respect to A and I by

$$\Pi^r(\mathcal{C}, A, I) := \{(AM)_{\bar{I}} \mid M \in \mathcal{C}\}, \quad \Sigma^r(\mathcal{C}, A, I) := \{(AM)_{\bar{I}} \mid M \in \mathcal{C}, (AM)_I = 0\}.$$

We define the *column-punctured* and *column-shortened* codes of $\mathcal{C}$ with respect to B and J by

$$\Pi^c(\mathcal{C}, B, J) := \left\{(MB)^{\bar{J}} \mid M \in \mathcal{C}\right\}, \quad \Sigma^c(\mathcal{C}, B, J) := \left\{(MB)^{\bar{J}} \mid M \in \mathcal{C}, (MB)^J = 0\right\}.$$

Clearly,

$$\Pi^r(\mathcal{C}, A, I) = A_{\bar{I}}\mathcal{C} \text{ and } \Pi^c(\mathcal{C}, B, J) = \mathcal{C}B^{\bar{J}}. \tag{2.1}$$

In particular every row-punctured code of $\mathcal{C}$ has the form $A\mathcal{C}$ for some $\ell \times n$ matrix A of rank ℓ and every column-punctured code has the form $\mathcal{C}B$ for some $m \times s$ matrix B of rank s.

Proposition 2.20. *Let $\mathcal{C}$ be an $[n \times m, k]_q$ code, and let $2 \leq d \leq \min\{n, m\}$. The following are equivalent.*

1. *$d(\mathcal{C}) \geq d$.*

2. *For every $A \in \mathrm{GL}_n(q)$ and $I \subseteq [n]$ satisfying $|I| \leq d-1$, the row-punctured code $\Pi^r(\mathcal{C}, A, I)$ has dimension k.*

3. *For every $B \in \mathrm{GL}_m(q)$ and $J \subseteq [m]$ satisfying $|J| \leq d-1$, the column-punctured code $\Pi^c(\mathcal{C}, B, J)$ has dimension k.*

Proof. Let $A \in \mathrm{GL}_n(q)$ and let $I \subseteq [n]$ such that $|I| \leq d-1$. The $\mathbb{F}_q$-linear epimorphism

$$\begin{aligned} f : \mathcal{C} &\longrightarrow \Pi^r(\mathcal{C}, A, I) \\ M &\longmapsto (AM)_{\bar{I}}, \end{aligned}$$

has non-trivial kernel if and only if $\mathrm{rk}(AM)_{\bar{I}} > 0$ for every non-zero $M \in \mathcal{C}$. Since

$$\mathrm{rk}((AM)_{\bar{I}}) \geq \mathrm{rk}(M) - |I| \geq \mathrm{rk}(M) - d + 1,$$

f is an isomorphism if and only if $d(\mathcal{C}) \geq d$. This establishes the equivalence of (1) and (2). Similarly, (1) and (3) are equivalent. □

Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ be a rank-metric code. There is a duality result involving shortening and puncturing, similarly to the Hamming metric and the vector rank-metric cases.

Theorem 2.21. *[17, Theorem 3.5] Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ be a rank-metric code, $A \in \mathrm{GL}_n(q)$, $B \in \mathrm{GL}_m(q)$. Let $I \subseteq [n]$ with $0 < |I| < n$ and let $J \subseteq [m]$ with $0 < |J| < m$.*

$$\Pi^r(\mathcal{C}, A, I)^\perp = \Sigma^r(\mathcal{C}^\perp, (A^\top)^{-1}, I), \qquad \Pi^c(\mathcal{C}, B, J)^\perp = \Sigma^c(\mathcal{C}^\perp, (B^\top)^{-1}, J).$$

Proposition 2.22. *Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ be a rank-metric code and let $2 \leq d \leq \min\{n, m\}$. The following are equivalent.*

1. *$d(\mathcal{C}) \geq d$.*

2. *For every $I \subseteq [n]$ with $|I| = n - d + 1$, for every $A \in \mathrm{GL}_n(q)$, $\Sigma^r(\mathcal{C}, A, I) = \{0\}$.*

3. *For every $J \subseteq [m]$ with $|J| = m - d + 1$, for every $B \in \mathrm{GL}_m(q)$, $\Sigma^c(\mathcal{C}, B, J) = \{0\}$.*

Proof. From Proposition 2.20, $d(\mathcal{C}) \geq d$ if and only if $\Pi^r(\mathcal{C}, A, \bar{I})$ and $\mathcal{C}$ are isomorphic under the map : $M \mapsto (AM)_I$. The kernel of this map is in one-to-one correspondence with $\Sigma^r(\mathcal{C}, A, I)$, which shows the equivalence of (1) and (2). The equivalence of (1) and (3) follows similarly. □

2.5 Relations between Vector Codes and Matrix Codes

To obtain a matrix code from a vector code, it suffices to use the fact that $\mathbb{F}_{q^m}^n$ and $\mathbb{F}_q^{n\times m}$ are isomorphic as $\mathbb{F}_q$-linear spaces. An isomorphism can be constructed as follows. Let $\Gamma = \{\gamma_1, \dots, \gamma_m\}$ be a basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$. For $v \in \mathbb{F}_{q^m}^n$, denote by $\Gamma(v) \in \mathbb{F}_q^{n\times m}$ the matrix whose

(i,j) entry is the j-th coordinate of v_i over the basis Γ. Then the map $v \mapsto \Gamma(v)$ is an $\mathbb{F}_q$-isomorphism. We denote by $\Gamma(C)$ the image of a vector rank-metric code $C \subseteq \mathbb{F}_{q^m}^n$ under Γ, i.e., we let $\Gamma(C) = \{\Gamma(v) \mid v \in C\}$.

Lemma 2.23. *Let $C \subseteq \mathbb{F}_{q^m}^n$ be a non-zero vector code. The minimum distance of $\Gamma(C)$ does not depend on the choice of the basis Γ for $\mathbb{F}_{q^m}/\mathbb{F}_q$. Moreover, for any such basis we have*

$$\dim_{\mathbb{F}_q}(\Gamma(C)) = m \cdot \dim_{\mathbb{F}_{q^m}}(C).$$

Another notion of support for vectors in $\mathbb{F}_{q^m}^n$ can be defined, in addition to the one given in Definition 2.1.

Definition 2.24. Let $C \subseteq \mathbb{F}_{q^m}^n$ be a vector rank-metric code, $v \in \mathbb{F}_{q^m}^n$ and Γ be a basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$. The $\mathbb{F}_q$*-support of* v is defined as $\mathrm{supp}(v) = \mathrm{colsp}(\Gamma(v))$. Moreover, the $\mathbb{F}_q$*-support of the code* C is the $\mathbb{F}_q$-space

$$\mathrm{supp}(C) := \sum_{v \in C} \mathrm{supp}(v).$$

The following result is an easy computation.

Proposition 2.25. *The support of a codeword is well-defined, i.e. it does not depend on the choice of the basis Γ of $\mathbb{F}_{q^m}/\mathbb{F}_q$.*

Notice that by definition, if $C \subseteq \mathbb{F}_{q^m}^n$, then $\mathrm{supp}(C) = \mathrm{csupp}(\Gamma(C))$ for every basis Γ of $\mathbb{F}_{q^m}/\mathbb{F}_q$.

2.5.1 Code Equivalence

At this point, one could wonder if the definitions of equivalent codes for vector and matrix codes are compatible. The answer was given by Sheekey and Van de Voorde in [107].

Proposition 2.26. *[107, Proposition 2.5] Let $C,\, C' \subseteq \mathbb{F}_{q^m}^n$ be two vector-codes. Then, $C \sim_v C'$ if and only if for any fixed basis Γ of $\mathbb{F}_{q^m}/\mathbb{F}_q$, it holds $\Gamma(C) \sim_m \Gamma(C')$.*

Moreover, an improvement in one direction was recently proved in [46].

Proposition 2.27. *[46, Proposition 1.15] Let $C, C' \in \mathbb{F}_{q^m}^n$ be vector rank-metric codes. Let Γ, Γ' be basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$. If $C \sim_v C'$ then $\Gamma(C) \sim_m \Gamma'(C')$*

Combining the two results, one can easily derive the following.

Theorem 2.28. *Let $C,\, C' \subseteq \mathbb{F}_{q^m}^n$ be two vector-codes, and let Γ, Γ' be two bases of $\mathbb{F}_{q^m}/\mathbb{F}_q$. Then, $C \sim_v C'$ if and only if $\Gamma(C) \sim_m \Gamma'(C')$.*

2.5.2 Duality

Given a vector rank-metric code $C \subseteq \mathbb{F}_{q^m}^n$ and a basis Γ of $\mathbb{F}_{q^m}/\mathbb{F}_q$, it is natural to ask whether the matrix codes $\Gamma(C^\perp)$ and $\Gamma(C)^\perp$ are the same. The answer is negative in general.

Example 2.29. [92, Example 18] Let $q = 3$, $n = m = 2$ and $\mathbb{F}_{3^2} = \mathbb{F}_3[\gamma]$, with $\gamma^2 + 1 = 0$. Consider now the vector rank-metric code C generated by $g = (\gamma, 2)$, and the basis $\Gamma = \{1, \gamma\}$ of $\mathbb{F}_{3^2}/\mathbb{F}_3$. With these assumptions, we have that $C^\perp$ is the vector rank-metric code generated by $h = (1, \gamma)$, and

$$\begin{aligned}\Gamma(C) &= \left\langle \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right\rangle, \\ \Gamma(C^\perp) &= \left\langle \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \right\rangle.\end{aligned}$$

However, $\langle I_2; 2I_2 \rangle = 1 \neq 0$, therefore $I_2 \notin \Gamma(C)^\perp$ and $\Gamma(C)^\perp \neq \Gamma(C^\perp)$.

Example 2.29 shows that in general $\Gamma(C^\perp) \neq \Gamma(C)^\perp$ for an $\mathbb{F}_{q^m}$-$[n, k]$ code and a basis Γ of $\mathbb{F}_{q^m}/\mathbb{F}_q$. However, the following result shed lights on the duality of the matrix representation.

Theorem 2.30. *[92, Theorem 21] Let C be an $[n, k]_{q^m}$ rank-metric code, and let Γ be a basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$ and Γ' be its dual basis with respect to the trace form. Then*

$$\Gamma(C^\perp) = \Gamma'(C)^\perp.$$

In particular, $\Gamma(C^\perp) \sim \Gamma(C)^\perp$.

Chapter 3

Encoding and Representation of Rank-Metric Codes

In coding theory, two important issues concern the encoding and the storage of a code. In the most general case, given a finite set $\mathcal{A}$ and a positive integer n, a block code C is a subset of $\mathcal{A}^n$, endowed with a distance function (usually the Hamming one). The space of messages $\mathcal{M}$ is then embedded in $\mathcal{A}^n$, via an injective encoding map E, such that $E(\mathcal{M}) = C$. The need to have fast encoding and efficient representation of codes led to look at algebraic structures on all the defining objects (the alphabet, the space of messages and the code), and on the encoding map E. For this reason, one usually only considers the alphabet as a field of q elements, the space of messages as the vector space $\mathbb{F}_q^k$, and the encoding map as a linear function, which leads to the study of linear codes. In this framework, we can locate the *generator matrix* of an $[n, k]_q$ code C, which serves as a representation in order to store C, and also as an encoding map. However, one can also read the parameters of the defining code from its algebraic structure. This generator matrix can also be constructed for a vector rank-metric code, and in analogous ways, one can extrapolate information on the code from it. In the case of matrix rank-metric codes, there is a similar object that one can use for storing, encoding and reading the parameters of the code. This is the case of the *generator tensor*, which was introduced and studied in [16] by Byrne, Neri, Ravagnani and Sheekey. This also lead to the investigation of a new parameter, that is the *tensor rank* of an $[n \times m, k]_q$ code $\mathcal{C}$, which gives a measure on the storage and encoding complexity of $\mathcal{C}$.

3.1 Vector Codes

In the Hamming metric case, linear codes are usually represented via their generator matrix, which represents the encoding map from the space of messages into the ambient space. Since this representation does not depend on the metric defined on the space, the same representation holds for vector rank-metric codes.

More specifically, for a given $[n,k]_{q^m}$ code C, an encoder is an $\mathbb{F}_{q^m}$-monomorphism

$$E : \mathbb{F}_{q^m}^k :\longrightarrow \mathbb{F}_{q^m}^n.$$

The space of all such encoding maps is contained in the space $\mathrm{Hom}_{\mathbb{F}_{q^m}}(\mathbb{F}_{q^m}^k, \mathbb{F}_{q^m}^n)$, which is an $\mathbb{F}_{q^m}$-vector space of dimension kn isomorphic to $\mathbb{F}_{q^m}^{k\times n}$ as $\mathbb{F}_{q^m}$-vector space. The isomorphism is given by:

$$\begin{array}{rcl}\mathcal{E} : \mathbb{F}_{q^m}^{k\times n} & \longrightarrow & \mathrm{Hom}_{\mathbb{F}_{q^m}}(\mathbb{F}_{q^m}^k, \mathbb{F}_{q^m}^n) \\ G & \longmapsto & E_G,\end{array}$$

where

$$\begin{array}{rcl}E_G : \mathbb{F}_{q^m}^k & \longrightarrow & \mathbb{F}_{q^m}^n \\ u & \longmapsto & uG.\end{array}$$

Definition 3.1. Let C be an $[n,k]_{q^m}$ code. A *generator matrix* for C is an element $G \in \mathbb{F}_{q^m}^{k\times n}$ such that $\mathrm{rowsp}(G) = C$.

Note that the generator matrix for an $[n,k]_{q^m}$ code C is not unique. However, there is a special generator matrix which is unique, that is the one in *reduced row echelon form.* A very special reduced row echelon form is the one given by $(I_k \mid X)$.

Definition 3.2. A generator matrix of the form $G = (I_k \mid X)$ is said to be in *standard form* (also called *systematic form*). The matrix X of this representation is the *non-systematic part* of G. We will denote by C_X the code $\mathrm{rowsp}(I_k \mid X)$.

Note that not all the codes have a generator matrix in standard form. However, it is easy to see that every $[n,k]_{q^m}$ code C is equivalent to a code C' which has a generator matrix in standard form.

Definition 3.3. Let C be an $[n,k]_{q^m}$ code. A *parity check matrix* for C is an element $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$ such that $\ker(H) = C$.

In classical coding theory with the Hamming metric, it is well-known that generator matrix and parity check matrix satisfy a duality property. Since the bilinear form defining the dual code is the same in the case of vector rank-metric codes (that is the standard inner-product), then also for an $[n,k]_{q^m}$ code C, we have that a matrix $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$ is a parity check matrix for C if and only if it is a generator matrix for $C^\perp$.

We now express the shortened code of an $[n,k]_{q^m}$ code C in terms of the parity check matrix. Let G be a generator matrix for C, $I \subseteq [n]$ and $A \in \mathrm{GL}_n(q)$. For a codeword $c \in C$, there exists a unique $u \in \mathbb{F}_{q^m}^k$ such that $c = uG$. Then

$$(cA)^{\bar{I}} = c(A^{\bar{I}}) = uGA^{\bar{I}} = u(GA^{\bar{I}}).$$

In particular,

$$\Pi(C, A, I) = \mathrm{rowsp}(GA^{\bar{I}}) \tag{3.1}$$

This implies that $GA^{\bar{I}}$ is a generator matrix for $\Pi(\mathcal{C}, A, I)$ if and only if $\mathrm{rk}(GA^{\bar{I}}) = k$.

Using these facts and the duality result of Theorem 2.17, we get some corollaries.

Corollary 3.4. *Let $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$ be the parity check matrix of an $[n, k]_{q^m}$ code $\mathcal{C}$, let $A \in \mathrm{GL}_n(q)$ and $I \subseteq [n]$.*

$$\mathrm{rowsp}(HA^{\bar{I}}) = (\Sigma(C, (A^\top)^{-1}, I))^\perp.$$

Proof. Since H is a generator matrix for $\mathcal{C}^\perp$, by (3.1), we have that $\mathrm{rowsp}(HA^{\bar{I}}) = \Pi(\mathcal{C}^\perp, A, I)$. Then, the statement follows from Theorem 2.17. □

Corollary 3.5. *Let C be an $[n, k]_{q^m}$ code, d be an integer such that $2 \leq d \leq n$, and $G \in \mathbb{F}_{q^m}^{k\times n}$ be a generator matrix for C. The following are equivalent.*

1. *$d(C) \geq d$.*
2. *For every $A \in \mathrm{GL}_n(q)$ and $I \subseteq [n]$ satisfying $|I| \leq d - 1$, $GA^{\bar{I}}$ is the generator matrix of $\Pi(C, A, I)$.*
3. *For every $A \in \mathbb{F}_q^{(n-d+1)\times n}$ of rank $n - d + 1$, $\mathrm{rk}(GA^\top) = k$.*

Proof. The equivalence between 2 and 3 has already been observed above. The fact that 1 and 3 are equivalent follows from Proposition 2.16 and (3.1). □

Corollary 3.6. *Let C be an $[n, k]_{q^m}$ code and let $2 \leq d \leq n$, and let $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$ be a parity check matrix for C. The following are equivalent.*

1. *$d(C) \geq d$.*
2. *For every $A \in \mathbb{F}_q^{(d-1)\times n}$, $\mathrm{rowsp}(HA^\top) = \mathbb{F}_{q^m}^{d-1}$.*

Proof. It follows from Corollary 3.4, (3.1) and Proposition 2.18. □

3.1.1 Generator and Parity Check Matrices of MRD Codes

As a direct consequence of Corollary 3.5, we present some criteria on the generator matrix and on the parity check matrix of an $[n, k]_{q^m}$ code, that allow to verify whether the code is MRD. First, we state the criterion given in the seminal paper of Gabidulin [36].

Proposition 3.7. *[36] Let C be an $[n, k]_{q^m}$ code, and $G \in \mathbb{F}_{q^m}^{k\times n}$ be a generator matrix for C. Then, C is MRD if and only if for every $A \in \mathrm{GL}_n(q)$, the code $\mathrm{rowsp}(GA)$ endowed with the Hamming metric, is an MDS code.*

The following criterion was given in [51, Corollary 2.12], and it is based on Proposition 3.7. It was finally improved in [81]. First we define the sets

$$\mathcal{E}_q(k,n) := \left\{E \in \mathbb{F}_q^{k\times n} \mid \mathrm{rk}(E) = k\right\}, \tag{3.2}$$

$$\mathcal{T}_q(k,n) := \{E \in \mathcal{E}_q(k,n) \mid E \text{ is in reduced row echelon form } \}. \tag{3.3}$$

Proposition 3.8 (MRD criterion)**.** *Let C be an $[n,k]_{q^m}$ code. Let $G \in \mathbb{F}_{q^m}^{k\times n}$ be a generator matrix and $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$ be a parity check matrix for C. The following are equivalent.*

1. *C is MRD.*
2. *$\mathrm{rk}(GE^\top) = k$ for all $E \in \mathcal{E}_q(k,n)$.*
3. *$\mathrm{rk}(HE^\top) = n-k$ for all $E \in \mathcal{E}_q(n-k,n)$.*
4. *$\mathrm{rk}(GE^\top) = k$ for all $E \in \mathcal{T}_q(k,n)$.*
5. *$\mathrm{rk}(HE^\top) = n-k$ for all $E \in \mathcal{T}_q(n-k,n)$.*

Another criterion was given in [51], involving the multiplication of the generator matrix by upper-triangular matrices. Consider the set of all upper-triangular matrices with all 1's on the diagonal, namely

$$\mathrm{U}_n(q) := \left\{A \in \mathbb{F}_q^{n\times n} \mid a_{i,j} = 0 \text{ for } i > j, a_{i,i} = 1 \text{ for } i \in [n]\right\}.$$

The next theorem is a reformulation of [51, Corollary 3.3].

Theorem 3.9. *[51] Let C be an $[n,k]_{q^m}$ code with generator matrix G. Then, C is MRD if and only if for every $A \in \mathrm{U}_q(n)$, the code $\mathrm{rowsp}(GA)$, endowed with the Hamming metric, is an MDS block code.*

We now study the generator matrix in standard (or systematic) form of MRD codes.

Lemma 3.10. *[79, Lemma 8] Let C be an $[n,k]_{q^m}$ MRD code. Then*

1. *C has a generator matrix in standard form, that is $C = \mathrm{rowsp}(I_k \mid X)$, for some $X = (x_{i,j}) \in \mathbb{F}_{q^m}^{k\times(n-k)}$.*
2. *$\mathrm{rk}_q(1, x_{i,1}, \dots, x_{i,n-k}) = n-k+1$, for every $i \in [k]$.*
3. *$\mathrm{rk}_q(1, x_{1,j}, \dots, x_{k,j}) = k+1$, for every $j \in [n-k]$.*

Proof. 1. An $[n,k]_{q^m}$ MRD code is also MDS, if considered endowed with the Hamming distance. This follows from the fact that $\mathrm{rk}_q(v) \leq \mathrm{wt}_H(v)$ and from the Singleton bound. Since the statement holds for MDS codes, we conclude.

2. Suppose that $\mathrm{rk}_q(1, x_{i,1}, \ldots, x_{i,n-k}) < n-k+1$ for some $i \in [k]$, and consider the non-zero codeword
$$e_i \left(\begin{array}{c|c} I_k & X \end{array} \right) = (0, \ldots, 0, 1, 0, \ldots, 0, x_{i,1}, \ldots, x_{i,n-k}).$$
The q-rank of this codeword is strictly less than $n-k+1$, and therefore C_X can not be MRD.

3. In this case we consider the code $C_X^\perp$. Since a generator matrix for this code is $(-X^T \mid I_{n-k})$, we get that $C_X^\perp \sim C_{-X^T}$. By the part 2 of this Lemma, we have that C_{-X^T} is not MRD and therefore the same holds for $C_X^\perp$. Hence, by Theorem 2.14, we can conclude that C_X is not MRD.

□

Observe that by Lemma 3.10 every $[n,k]_{q^m}$ MRD code can be represented in a unique way as a code of the form C_X for some $X \in \mathbb{F}_{q^m}^{k\times(n-k)}$. We will widely use this notation later in this work.

The following result derives from Theorem 3.9; it can be considered as the analogue in the rank metric of Theorem 1.33, since it gives conditions for a code C_X to be MRD, based only on the matrix X.

Theorem 3.11. *Let $X \in \mathbb{F}_{q^m}^{k\times(n-k)}$. The following are equivalent:*

1. *C_X is MRD.*
2. *For every $A \in \mathrm{GL}_k(q), B \in \mathrm{GL}_{n-k}(q), C \in \mathbb{F}_q^{k\times(n-k)}$, the matrix $AXB + C$ is superregular.*
3. *For every $A \in \mathrm{U}_k(q), B \in \mathrm{U}_{n-k}(q), C \in \mathbb{F}_q^{k\times(n-k)}$, the matrix $AXB + C$ is superregular.*

Proof. 2. ⇒ 3. This is clear, since $\mathrm{U}_r(q) \subseteq \mathrm{GL}_r(q)$ for any positive integer r.

1. ⇒ 2. Suppose that C_X is MRD, and let $A \in \mathrm{GL}_k(q), B \in \mathrm{GL}_{n-k}(q), C \in \mathbb{F}_q^{k\times(n-k)}$. Then we consider the matrix $\widetilde{G} = (I_k \mid X)M$, where
$$M := \begin{pmatrix} A^{-1} & A^{-1}C \\ 0 & B \end{pmatrix} \in \mathrm{GL}_n(q).$$
Then it is easy to see that $\mathrm{rowsp}(\widetilde{G}) = C_{\widetilde{X}}$, where $\widetilde{X} = AXB + C$. Then the statement follows from Proposition 3.7 and the characterization of MDS codes given in Theorem 1.33.

3. ⇒ 1. Suppose that 3 holds. Every matrix $M \in \mathrm{U}_n(q)$ can be written in the form
$$M := \begin{pmatrix} A & AC \\ 0 & B \end{pmatrix} \in \mathrm{GL}_n(q),$$

for some $A \in \mathrm{U}_k(q), B \in \mathrm{U}_{n-k}(q), C \in \mathbb{F}_q^{k\times(n-k)}$. Moreover, $\mathrm{rowsp}((I_k \mid X)M) = C_{\widetilde{X}}$, where $X = A^{-1}XB + C$. Since the map $A \longmapsto A^{-1}$ is a bijection from $\mathrm{U}_k(q)$ into itself, we conclude that C_X is an MRD code using Theorem 1.33 and Theorem 3.9. □

Even though Theorem 3.11 is an easy consequence of known results, it can not be found in any published scientific work. Thus, it is an original contribution of this dissertation.

3.2 Matrix Codes: Tensor Representation

The results presented in this section are taken from the paper [16] by Byrne, Neri, Ravagnani and Sheekey.

In the theory of rank-metric codes, a natural representation of an $[n \times m, k]_q$ code is given by a *generator tensor* for it. It will become evident that this representation offers greater efficiency in terms of complexity of encoding and storage of the encoder.

The generator tensor essentially determines an encoding from the information space $\mathbb{F}_q^k$ to the ambient matrix space $\mathbb{F}_q^{n\times m}$. More specifically, for a given $[n \times m, k]_q$ code $\mathcal{C}$, an encoder is an $\mathbb{F}_q$-monomorphism

$$E : \mathbb{F}_q^k :\longrightarrow \mathbb{F}_q^{n\times m}.$$

The space of all such encoding maps is contained in the space $\mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_q^k, \mathbb{F}_q^{n\times m})$, which is an $\mathbb{F}_q$-vector space of dimension knm. Moreover, we have that

$$\mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_q^k, \mathbb{F}_q^{n\times m}) \cong \mathbb{F}_q^{k\times n\times m}$$

as $\mathbb{F}_q$-vector spaces. The isomorphism is explicitly given by:

$$\begin{array}{rcl} \mathcal{E} : \mathbb{F}_q^{k\times n\times m} & \longrightarrow & \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_q^k, \mathbb{F}_q^{n\times m}) \\ X & \longmapsto & E_X, \end{array}$$

where

$$\begin{array}{rcl} E_X : \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^{n\times m} \\ g & \longmapsto & m_1(g, X). \end{array}$$

This yields an analogue of the notion of a generator matrix for rank-metric codes, in the form of a 3-tensor.

Definition 3.12. Let $\mathcal{C}$ be an $[n \times m, k]_q$ code. A *generator tensor* for the code $\mathcal{C}$ is an element $X \in \mathbb{F}_q^{k\times n\times m}$ such that $\mathrm{ssp}_1(X) = \mathcal{C}$.

Clearly, with respect to this definition, any generator tensor for a code is necessarily 1-nondegenerate. The complexity of realizing a code $\mathcal{C}$ as the slice space of a tensor X depends on the tensor rank of X and hence it is of interest to give expressions of generating tensors as minimal sums of simple tensors, and moreover to obtain constructions of codes whose generating tensors have least possible tensor rank.

Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ be a non-zero code, and let X_1, X_2 be generating tensors for $\mathcal{C}$. By Proposition 1.26 we have that

$$\begin{aligned}\mathrm{trk}(X_1) &= \min\{R \in \mathbb{N} \mid \exists\, A_1, \dots, A_R \text{ with } \mathrm{rk}(A_i) = 1, \mathcal{C} \subseteq \langle A_1, \dots, A_R\rangle\} \\ &= \mathrm{trk}(X_2).\end{aligned}$$

Therefore the following holds.

Proposition 3.13. *Let X_1 and X_2 be two generator tensors for the same $[n \times m, k]_q$ code $\mathcal{C}$. Then*

$$\mathrm{trk}(X_1) = \mathrm{trk}(X_2).$$

Furthermore, if $\mathcal{C}$ is not the zero code, then this number equals the minimum $R > 0$ such that $\mathcal{C}$ is contained in the span of R rank 1 matrices.

Definition 3.14. Let $\mathcal{C}$ be an $[n \times m, k]_q$ code. The *tensor rank* of $\mathcal{C}$, denoted by $\mathrm{trk}(\mathcal{C})$, is defined to be the tensor rank of any generator tensor of $\mathcal{C}$.

If $\mathcal{C}$ and $\mathcal{C}'$ are a pair of codes satisfying $\mathcal{C}' = \varphi(\mathcal{C})$ for an isometry φ, and let $\{A_1, \dots, A_R\}$ be a set of rank 1 matrices such that $\mathcal{C} \subseteq \langle A_1, \dots, A_R\rangle$. Then $\mathcal{C}' \subseteq \langle \varphi(A_1), \dots, \varphi(A_R)\rangle$, and the matrices $\varphi(A_i)$'s have also rank 1. Therefore, Proposition 3.13 also implies that the tensor rank is invariant under code equivalence.

Proposition 3.15. *Let $\mathcal{C}, \mathcal{C}' \in \mathbb{F}_q^{n\times m}$ with $\mathcal{C} \sim_m \mathcal{C}'$. Then $\mathrm{trk}(\mathcal{C}) = \mathrm{trk}(\mathcal{C}')$.*

Let $\mathcal{C}$ be an $[n \times m, k]_q$ code with generator tensor $X \in \mathbb{F}^{k\times n\times m}$. By the definition of a generator tensor, we have that $\dim_1(X) = \dim_{\mathbb{F}_q}(\mathcal{C})$. However, $\dim_2(X)$ and $\dim_3(X)$ also have an important role, as explained by the following result.

Proposition 3.16. *Let $\mathcal{C}$ be an $[n \times m, k]_q$ code with generator tensor $X \in \mathbb{F}_q^{k\times n\times m}$. Then*

$$\dim_2(X) = \dim(\mathrm{csupp}(\mathcal{C})), \qquad \dim_3(X) = \dim(\mathrm{rsupp}(\mathcal{C})).$$

Proof. Let $A_1, \dots, A_k$ be a basis of $\mathcal{C}$. Then $Y = \sum_{i=1}^k e_i \otimes A_i$ is a generator tensor for $\mathcal{C}$. For any $y \in \mathbb{F}_q^n$, we have that $m_2(y, Y) = \sum_{i=1}^k e_i \otimes (yA_i) = 0$ if and only if $yA_i = 0$ for each $i = 1, \dots, k$. This is true if and only if

$$y \in \bigcap_{i=1}^k \mathrm{colsp}(A_i)^\perp = \left(\sum_{i=1}^k \mathrm{colsp}(A_i)\right)^\perp = \mathrm{csupp}(\mathcal{C})^\perp.$$

In particular $\mathrm{csupp}(\mathcal{C})^\perp$ is the kernel of the map

$$m_2(\cdot, Y) : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^{k\times m} : y \mapsto m_2(y, Y),$$

hence $\dim(\text{csupp}(\mathcal{C})) = \dim_2(Y) = \dim \text{ssp}_2(\mathcal{C}) = \dim_2(X)$.

The proof of the statement for $\dim_3(X)$ is analogous. □

Remark 3.17. As a consequence, the property of a rank-metric code $\mathcal{C}$ of being nondegenerate can be read from its generator tensor. Indeed, $\mathcal{C}$ is nondegenerate if and only if any of its generator tensors is both 2-nondegenerate and 3-nondegenerate.

Remark 3.18. We note that some of the results of this section have been previously considered in the case of $m = n = k$, due to the fact that MRD codes in this situation are in one-to-one correspondence with *finite semifields*, that is, nonassociative division algebras. Indeed, tensors and rank-metric codes in this case correspond to algebras which are not necessarily associative. Knuth [57] considered the cubical array of a semifield, which is precisely the coordinate tensor introduced in (1.1). The explicit tensor correspondence was outlined in [69] and developed in [63], where the tensor rank was proposed as an interesting invariant of a finite semifield, or equivalently its corresponding slice space.

3.2.1 Complexity

We have demonstrated how the encoding map from $\mathbb{F}_q^k$ to the ambient space $\mathbb{F}_q^{n\times m}$ is represented for a rank metric code by a 3-tensor, namely its generator tensor. Let $X = \sum_{r=1}^{R} u_r \otimes v_r \otimes w_r$ be a generator tensor for an $[n \times m, k, d]_q$ code $\mathcal{C}$ of tensor rank R. The message $a \in \mathbb{F}_q^k$ is encoded via

$$a \mapsto m_1(a, X) = \sum_{r=1}^{R} (a \cdot u_r) v_r \otimes w_r = V \operatorname{diag}(aU) W^T,$$

where $U = (u_r \mid 1 \leq r \leq R)$, $V = (v_r \mid 1 \leq r \leq R)$ and $W = (w_r \mid 1 \leq r \leq R)$. We say that X is in standard form if $U = (I_k \mid U')$, $V = (I_n \mid V')$ and $W = (I_m \mid W')$ for matrices U', V', W' of the required sizes.

X has storage complexity $R(k + n + m)$ in the general case and requires storing up to $R(k+n+m) - k^2 - n^2 - m^2$ symbols in $\mathbb{F}_q$ if X is in standard from. Note that the expression of the codeword $c = m_1(a, X)$ as an $\mathbb{F}_q$-linear combination of the rank one matrices $v_r \otimes w_r$ is unique. Thus, it is sufficient to compute aU in order to represent elements of $\mathcal{C}$, once the generator tensor X is known. The tensor encoding therefore requires kR multiplications and $(k-1)R$ additions over $\mathbb{F}_q$ for arbitrary U of rank k and $k(R-k)$ multiplications and $(k-1)(R-k)$ additions if U is in standard form.

Of course, being an $\mathbb{F}_q$-space, we could also choose to use a generator matrix to represent the encoding map. This can be achieved by representing each element of $\mathbb{F}_q^{n\times m}$ as a vector of length $\mathbb{F}_q^{nm}$ by the obvious $\mathbb{F}_q$-isomorphism

$$(M_{ij}) \mapsto (M_{11} \cdots M_{1n} | \cdots | M_{m1} \cdots M_{mn}).$$

Then choose a $k \times nm$ generator matrix G as the encoder. The storage complexity of G is knm and if G is in systematic form it requires $k(nm-k)$ symbols in $\mathbb{F}_q$. The encoding complexity of the computation $x \mapsto xG$ for G in standard form then requires $k(nm-k)$ multiplications and $(k-1)(nm-k)$ additions. We remark that the $k \times nm$ matrix G can simply be obtained from the coordinate tensor representation of X via

$$G_{it} := X_{ij\ell}, \tag{3.4}$$

where $t = (j-1)m + \ell$ for $1 \leq j \leq n$, $1 \leq \ell \leq m$. We summarize these observations in Table 3.1.

	$k \times nm$ Generator Matrix	$k \times n \times m$ Generator Tensor
Storage	$k(mn-k)$	$R(k+n+m) - k^2 - n^2 - m^2$
Encoding Additions	$(k-1)(nm-k)$	$(k-1)(R-k)$
Encoding Multiplications	$k(nm-k)$	$k(R-k)$

Table 3.1: Complexities

Since $R \leq nm$, the generator tensor approach in most cases offers complexity lower than that required by the generator matrix encoder. The number of symbols in $\mathbb{F}_q$ required to store the standard form generator matrix G exceeds that of the standard generator tensor X if and only if

$$R < \frac{knm + n^2 + m^2}{k+n+m}.$$

3.2.2 Parity Check Tensor

We define a *parity check tensor* of a rank-metric code.

Definition 3.19. Let $\mathcal{C}$ be an $[n \times m, k]_q$ code and let $Y \in \mathbb{F}_q^{(mn-k)\times n \times m}$. We say that Y is a *parity check tensor* for $\mathcal{C}$ if

$$\mathcal{C} = \left\{ M \in \mathbb{F}^{n \times m} \mid Y : M = 0 \right\}.$$

Recall that for a pair of matrices $M = (m_{ij})$ and $N = (n_{ij})$ in $\mathbb{F}_q^{n \times m}$,

$$\langle M; N \rangle = \mathrm{Tr}(MN^\top) = \sum_{i,j} m_{ij} n_{ij}.$$

This operation coincides with the tensor double-dot product when applied to matrices, i.e.

$$M : N = \langle M; N \rangle.$$

From this, let $\mathcal{C}$ be an $[n \times m, k]_q$ code, $X \in \mathbb{F}_q^{k \times n \times m}$ be a generator tensor for $\mathcal{C}$, and $Y \in \mathbb{F}_q^{(mn-k)\times n \times m}$ be a parity check tensor for $\mathcal{C}$. Let moreover $G \in \mathbb{F}_q^{k \times nm}$ be constructed from X

as in (3.4), and $H \in \mathbb{F}_q^{(nm-k)\times nm}$ be a parity check matrix for the $[nm, k]_q$ block code generated by G. Then, it holds that

$$X : Y = 0 \text{ if and only if } GH^\top = 0,$$

i.e. the definition of parity check tensor is compatible with the defiition of parity check matrices if one uses the identification in (3.4).

Proposition 3.20. *Let $Y \in \mathbb{F}^{(mn-k)\times n\times m}$, and let $\mathcal{C}$ be an $[n \times m, k]_q$ code. Then, Y is a generator tensor for $\mathcal{C}^\perp$ if and only if it is a parity check tensor for $\mathcal{C}$.*

Proof. Y is a parity check tensor for $\mathcal{C}$ if and only if $Y : M = 0$ for all $M \in \mathcal{C}$. From (1.4), this holds if and only if

$$0 = g(Y : M) = m_1(g, Y) : M$$

for all $g \in \mathbb{F}_q^{nm-k}$ and $M \in \mathcal{C}$, which holds if and only if $\mathcal{C}^\perp = \{m_1(g, Y) \mid g \in \mathbb{F}_q^{nm-k}\}$. □

Corollary 3.21. *Let $X \in \mathbb{F}^{k\times n\times m}$ be a generator tensor for an $[n \times m, k]_q$ code $\mathcal{C}$. A 1-nondegenerate tensor $Y \in \mathbb{F}^{(mn-k)\times n\times m}$ is a parity check tensor for $\mathcal{C}$ if and only if*

$$X : Y = 0.$$

Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ be a rank-metric code. We now express the shortened code of a rank-metric code in terms of its parity check tensor.

Let X be a generator tensor for $\mathcal{C} \in \mathbb{F}_q^{n\times m}$ and let $M \in \mathcal{C}$. Then $M = m_1(\alpha, X)$ for unique $\alpha \in \mathbb{F}_q^k$. Let $I \subseteq [n]$ and let $A \in \mathrm{GL}_n(q)$. Then

$$(AM)_I = A_I M = m_2(A_I, M) = m_2(A_I, m_1(\alpha, X)) = m_1(\alpha, m_2(A_I, X)),$$

where we have identified matrices $H \in \mathbb{F}_q^{N\times M}$ with 3-tensors $1 \otimes H \in \mathbb{F}_q^{1\times N\times M}$. In particular,

$$\Pi^r(\mathcal{C}, A, I) = \mathrm{ssp}_1(m_2(A_{\bar{I}}, X)). \tag{3.5}$$

Similarly, for any $J \subseteq [m]$ and $B \in \mathrm{GL}_m(q)$, we have

$$\Pi^c(\mathcal{C}, B, J) = \mathrm{ssp}_1(m_3((B^{\bar{J}})^\top, X)). \tag{3.6}$$

Clearly, $m_2(A_{\bar{I}}, X)$ is a generator tensor for $\Pi^r(\mathcal{C}, A, I)$ (respectively $m_3((B^{\bar{J}})^\top, X)$ is a generator tensor for $\Pi^c(\mathcal{C}, B, J)$) if and only if it is 1-nondegenerate.

Corollary 3.22. *Let $Y \in \mathbb{F}_q^{(nm-k)\times n\times m}$ be a parity check tensor of an $[n \times m, k]_q$ code $\mathcal{C}$, let $A \in \mathrm{GL}_n(q)$ and let $B \in \mathrm{GL}_m(q)$. Let $I \subseteq [n]$ and $J \subseteq [m]$. Then*

1. $\mathrm{ssp}_1(m_2(((A^\top)^{-1})_{\bar{I}}, Y)) = (\Sigma^r(\mathcal{C}, A, I))^\perp$.

2. $\mathrm{ssp}_1(m_3((B^{\bar{J}})^\top, Y)) = (\Sigma^c(\mathcal{C}, B, J))^\perp$.

Proof. By the duality statement of Theorem 2.21, we have

$$\Sigma^r(\mathcal{C}, A, I) = \Pi^r(\mathcal{C}^\perp, (A^\top)^{-1}, I)^\perp.$$

By Proposition 3.20, Y is a generator tensor for $\mathcal{C}^\perp$ and so by (3.5) we have

$$\mathrm{ssp}_1(m_2(((A^\top)^{-1})_{\bar{I}}, Y)) = \Pi^r(\mathcal{C}^\perp, (A^\top)^{-1}, I),$$

showing that (1) holds. The proof that (2) holds is similar. □

Proposition 2.20, combined with (2.1), (3.5) and (3.6) immediately yield the following result.

Corollary 3.23. *Let $X \in \mathbb{F}_q^{k\times n\times m}$ be a generator tensor of an $[n \times m, k]_q$ code $\mathcal{C}$, and let $2 \le d \le \min\{n, m\}$. The following are equivalent.*

1. *$d(C) \ge d$.*
2. *For every $A \in \mathrm{GL}_n(q)$ and $I \subseteq [n]$ satisfying $|I| \le d-1$, $m_2(A_{\bar{I}}, X)$ is a generator tensor of $\Pi^r(\mathcal{C}, A, I)$.*
3. *For every $B \in \mathrm{GL}_m(q)$ and $J \subseteq [m]$ satisfying $|J| \le d-1$, $m_3((B^{\bar{J}})^\top, X)$ is a generator tensor of $\Pi^c(\mathcal{C}, B, J)$.*
4. *For every $A \in \mathbb{F}_q^{(n-d+1)\times n}$ of rank $n-d+1$, $\dim_1(m_2(A, X)) = k$.*
5. *For every $B \in \mathbb{F}_q^{(m-d+1)\times m}$ of rank $m-d+1$, $\dim_1(m_3(B, X)) = k$.*

As a direct consequence of Propositions 3.22 and 2.22, we get the following result that relates the minimum distance of a rank-metric code with any of its parity check tensors.

Corollary 3.24. *Let $Y \in \mathbb{F}_q^{(nm-k)\times n\times m}$ be a parity check tensor of an $[n \times m, k]_q$ code $\mathcal{C}$, and let $2 \le d \le \min\{n, m\}$. The following are equivalent.*

1. *$d(\mathcal{C}) \ge d$.*
2. *For every $A \in \mathbb{F}_q^{(d-1)\times n}$ of full rank, $\mathrm{ssp}_1(m_2(A, Y)) = \mathbb{F}_q^{(d-1)\times m}$.*
3. *For every $B \in \mathbb{F}_q^{(d-1)\times m}$ of full rank, $\mathrm{ssp}_1(m_3(B, Y)) = \mathbb{F}_q^{n\times(d-1)}$.*

Chapter 4

Gabidulin Codes

The most studied and important construction of MRD codes is still the one proposed in the seminal works [30, 36, 96], and then generalized in [61]. These codes are known as *Gabidulin codes*, and they represent the rank analogue of the well-known *generalized Reed-Solomon (GRS) codes*. As GRS codes, Gabidulin codes are evaluation codes. However, they are defined over a field extension $\mathbb{F}_{q^m}/\mathbb{F}_q$, whose Galois group is cyclic with generator θ. Here, the evaluation is done on a particular subset of *θ-polynomials* in n points that are linearly independent over $\mathbb{F}_q$. The structure of evaluation codes allowed the development of many efficient decoding algorithms in the last years [110, 116]. In this framework, another analogy emerges regarding the generator matrices of these two families of codes. The canonical generator matrix of GRS codes is obtained by the evaluation of the canonical basis $\{1, x, \dots, x^{k-1}\}$, that gives as a result the *weighted Vandermonde matrix*, a matrix given by the product of a Vandermonde with a non-singular diagonal matrix. The rank analogue of the weighted Vandermonde matrix is given by the θ-Moore matrix. Such a matrix is the canonical generator matrix of a θ-Gabidulin code, obtained via the evaluation of the canonical basis $\{x, x^{\theta}, x^{\theta^2}, \dots, x^{\theta^{k-1}}\}$. As already explained in Section 1.4, there is another important generator matrix of GRS codes that is well-known in the literature. In 1985 Roth and Seroussi gave a characterization of the generator matrix in standard form for these codes ([98]), showing that GRS codes are in correspondence with *generalized Cauchy matrices* (see also [33]). Explicitly, the generator matrix in standard form of a GRS code is given by $(I_k \mid X)$, where I_k is the $k \times k$ identity matrix, and X is a generalized Cauchy matrix. On the other hand, every matrix $(I_k \mid X)$, where X is a generalized Cauchy matrix, generates a GRS code.

In this chapter, we first introduce the family of Gabidulin codes, recalling definitions, properties and some known results. Furthermore, we give a characterization of the generator matrix in standard form of Gabidulin codes. As a consequence, this also allows us to define a rank analogue of generalized Cauchy matrices, whose definition coincides with the q-analogue of generalized Cauchy matrices. This result is obtained making a wide use of properties of finite fields, in particular the trace map, and of some new results appeared very recently [51, 81]. In addition to the theoretical result that almost completes the picture of the analogies between GRS and Gabidulin codes, this has also a useful impact from a practical point of view. Using the structure of the rank analogue of a generalized Cauchy matrix, we derive a subfamily of Gabidulin codes whose generator matrix is made by an identity block and a Toeplitz/Hankel block. This new family of codes seems to be suitable for fast algorithms for erasure correction and syndrome decoding as well as for encoding. It is well-known, indeed, that the matrix-vector multiplication with a Toeplitz/Hankel matrix can be performed in a fast way. Moreover, from the characterization obtained, we also derive a new criterion to determine whether a given code is a Gabidulin code. This new criterion is faster to compute than any other previously known. Indeed, for a given rank metric code of dimension k and length n over a finite field $\mathbb{F}_{q^m}$, it only requires $\mathcal{O}(k^2nm)$ field operations.

The results contained in this chapter are taken from the paper [79] by Neri.

Notation: Given a matrix (resp. a vector) $A \in \mathbb{F}_{q^m}^{k\times n}$ and $\theta \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, we denote by $\theta(A)$ the matrix obtained by applying θ to every entry of the matrix (resp. the vector) A. Analogously, given a code $C \subseteq \mathbb{F}_{q^m}^n$, we define

$$\theta(C) := \{\theta(c) \mid c \in C\}.$$

Moreover we consider the map Ψ_θ defined as

$$\begin{array}{rccc}\Psi_\theta : \mathbb{F}_{q^m}^{k\times(n-k)} & \longrightarrow & \mathbb{F}_{q^m}^{k\times(n-k)} \\ X & \longmapsto & \theta(X) - X.\end{array}$$

Observe that Ψ_θ is the function that maps every entry $x_{i,j}$ of the matrix X to $\psi_\theta(x_{i,j})$.

4.1 Definition and Properties

As we did for the previous chapters, let q be a prime power and k, n, m be positive integers. Suppose we are looking for $[n,k]_{q^m}$ MRD codes. It can be easily shown that a necessary condition for the existence of MRD codes is $n \leq m$. Furthermore, the condition $n \leq m$ is also sufficient. MRD vector codes (and therefore MRD matrix codes) exist for every set of parameters. The first construction was found by Delsarte [30] and independently by Gabidulin [36] and Roth [96]. It was then generalized in [61].

Definition 4.1. Let θ be a generator of $G = \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. We denote by $\mathcal{G}_{k,\theta}$ the $\mathbb{F}_{q^m}$-subspace of the group algebra $\mathbb{F}_{q^m}[\theta] = \mathbb{F}_{q^m}[G]$ generated by the first k powers of θ, that is

$$\mathcal{G}_{k,\theta} := \left\{ f_0\mathrm{id} + f_1\theta + \ldots + f_{k-1}\theta^{k-1} \mid f_i \in \mathbb{F}_{q^m} \right\}.$$

In the language of θ-polynomials, the set $\mathcal{G}_{k,\theta}$ corresponds to the set

$$\mathcal{L}_{k,\theta} := \left\{ f_0 x + f_1 x^{\theta} + \ldots + f_{k-1} x^{\theta^{k-1}} \mid f_i \in \mathbb{F}_{q^m} \right\}.$$

Definition 4.2. Let $g = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ be a vector such that $\mathrm{rk}_q(g) = n$. Let moreover $1 \leq k \leq n \leq m$. The θ-Gabidulin code $\mathcal{G}_{k,\theta}(g)$ is defined as

$$\mathcal{G}_{k,\theta}(g) := \{(f(g_1), \ldots, f(g_n)) \mid f \in \mathcal{G}_{k,\theta}\}.$$

Remark 4.3. In the literature, it is often referred to Gabidulin codes to denote $\bar{\theta}$-Gabidulin codes, where $\bar{\theta}$ is the q-Frobenius automorphism, i.e. the map that sends any $\alpha \in \mathbb{F}_{q^m}$ to its q-th power α^q. Gabidulin codes with this special automorphism $\bar{\theta}$ were the ones first introduced and studied in [30, 36, 96]. The general case with any θ generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ was later studied by Kshevetskiy and Gabidulin in [61], and these codes are known as *generalized Gabidulin codes.* However, in the whole dissertation, we will never distinguish between the two constructions, since there is nothing really special with $\bar{\theta}$-Gabidulin codes.

Theorem 4.4. *[30, 36] Let $g \in \mathbb{F}_{q^m}^n$ be a vector such that $\mathrm{rk}_q(g) = n$. The minimum rank distance of the θ-Gabidulin code $\mathcal{G}_{k,\theta}(g)$ is $d = n - k + 1$, i.e. $\mathcal{G}_{k,\theta}(g)$ is an MRD code.*

The following result gives an explicit expression for the dual of a θ-Gabidulin code, which is in turn a θ-Gabidulin code.

Proposition 4.5. *[36, Sections 2 and 4][61, Subsection IV.C] Let $g \in \mathbb{F}_{q^m}^n$ be a vector such that $\mathrm{rk}_q(g) = n$ and $C = \mathcal{G}_{k,\theta}(g)$ be a θ-Gabidulin code. Then $C^{\perp} = \mathcal{G}_{n-k,\theta}(h)$ where h is any non-zero vector in the code $\mathcal{G}_{n-1,\theta}(\theta^{-(n-k-1)}(g))^{\perp}$. Moreover, $\mathrm{rk}_q(h) = n$.*

In the following, $\mathrm{Gr}(k, \mathbb{F}_{q^m}^n)$ denotes the k-dimensional Grassmannian of $\mathbb{F}_{q^m}^n$, that is the set of all the k-dimensional $\mathbb{F}_{q^m}$-subspaces of $\mathbb{F}_{q^m}^n$. Moreover, let $\mathrm{Gab}_q(k, n, m, \theta)$ be the set of all $[n, k]_{q^m}$ θ-Gabidulin codes, i.e.

$$\mathrm{Gab}_q(k, n, m, \theta) := \left\{ \mathcal{U} \in \mathrm{Gr}(k, \mathbb{F}_{q^m}^n) \mid \mathcal{U} = \mathcal{G}_{k,\theta}(g) \text{ for some } g \in \mathbb{F}_{q^m}^n \text{ with } \mathrm{rk}_q(g) = n \right\}.$$

One can also find the exact number of θ-Gabidulin codes for a given θ. In [8], Berger provided the following result.

Theorem 4.6. *[8, Theorem 2] Let $u, v \in \mathbb{F}_{q^m}^n$ be two vectors such that $\mathrm{rk}_q(u) = \mathrm{rk}_q(v) = n$. Then, for any θ generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, $\mathcal{G}_{k,\theta}(u) = \mathcal{G}_{k,\theta}(v)$ if and only if $u = \lambda v$ for some $\lambda \in \mathbb{F}_{q^m}^*$.*

Corollary 4.7. *Let k, n, m be integers such that $2 \leq k \leq n - 2$ and $n \leq m$, and let θ be a* *generator of* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. *Then,*

$$|\,\mathrm{Gab}_q(k,n,m,\theta)| = \prod_{i=1}^{n-1}(q^m - q^i).$$

In general a θ-Gabidulin code C can be also a σ-Gabidulin code for another generator σ of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. We will prove in Theorem 7.28 that this can not happen for many σ's. However, it is straightforward to see that a θ-Gabidulin code is always also a θ^{-1}-Gabidulin code.

Proposition 4.8. *Let θ be a generator of the Galois group $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ and $g \in \mathbb{F}_{q^m}^n$ such that $\mathrm{rk}_q(g)$. Then $\mathcal{G}_{k,\theta}(g) = \mathcal{G}_{k,\theta^{-1}}(\theta^{k-1}(g))$.*

Proposition 4.8, together with Corollary 4.7, provides an upper bound on the total number of Gabidulin codes. A lower bound on this number will be provided in Chapter 7. Let $F = \{\theta \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) \mid \theta \text{ is a generator of } \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)\}$, and

$$\begin{aligned}\mathrm{Gab}_q(k,n,m) &:= \left\{\mathcal{U} \in \mathrm{Gr}(k, \mathbb{F}_{q^m}^n) \mid \mathcal{U} \text{ is a } \theta\text{-Gabidulin code for some } \theta \in F\right\}\\ &= \bigcup_{\theta\in F} \mathrm{Gab}_q(k,n,m,\theta).\end{aligned}$$

Corollary 4.9. *Let k,n,m be integers such that $2 \le k \le n-2$ and $n \le m$. Then,*

$$|\mathrm{Gab}_q(k,n,m)| \le \frac{\phi(m)}{2}\prod_{i=1}^{n-1}(q^m - q^i).$$

Proof. It directly follows from Corollary 4.7 and Proposition 4.8. □

However, one can expect that some of those Gabidulin codes will be equivalent to each other. Then the natural question is "how many inequivalent Gabidulin codes do exist?". Recently, Schmidt and Zhou provided a lower bound on this number.

Theorem 4.10. *[101, Theorem 1.2] For any k,n,m integers such that $1 \le k \le n-1$ and $2 \le n \le m-2$, the number of inequivalent Gabidulin codes of dimension k in $\mathbb{F}_{q^m}^n$ is at least*

$$\frac{1}{m}\begin{bmatrix} m \\ n\end{bmatrix}_q \frac{q-1}{q^m-1}.$$

4.2 Canonical Generator Matrix

The most used generator matrix of a θ-Gabidulin code $\mathcal{G}_{k,\theta}(g)$ is given by the θ-Moore matrix $M_{s,\theta}(g)$. This generator matrix is said to be *canonical* or *monomial*, since it is obtained by evaluating the basis $\{\mathrm{id}, \theta, \dots, \theta^{k-1}\}$ of $\mathcal{G}_{k,\theta}$ in the points $g_1, \dots, g_n$. In terms of θ-polynomials, the θ-Moore matrix is obtained by evaluating in g the monomial basis $\{x, x^\theta, \dots, x^{\theta^{k-1}}\}$ of $\mathcal{L}_{k,\theta}$.

Definition 4.11. Let $v \in \mathbb{F}_{q^m}^n$ and θ be a generator of $\operatorname{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. The *$\theta$-Moore matrix of order k in g* is the matrix defined by

$$M_{k,\theta}(v) := (\theta^{i-1}(v_j))_{i,j} \in \mathbb{F}_{q^m}^{k\times n}.$$

Now, if one picks the q-Frobenius automorphism $\bar{\theta}$, which maps every α to its q-th power α^q, the $\bar{\theta}$-Moore matrix will be of the form

$$M_{k,\bar{\theta}} := \left(g_j^{q^{i-1}}\right)_{i,j},$$

that is how it is usually described in the literature. This particular matrix was deeply used in the theory of finite fields and normal bases. Already at the beginning of the 20th century, Dickson used the structure of Moore matrices for finding the modular invariants of the general linear group over a finite field [32] (Moore was actually Dickson's doctoral advisor, Ed.). For all these reasons, the θ-Moore matrix is considered the q-analogue of a (weighted) Vandermonde matrix.

An important criterion for an $[n,k]_{q^m}$ code C to be a θ-Gabidulin code was given in [51], and it is based on the intersection of the code C with $\theta(C)$, where θ is a generator of $\operatorname{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$.

Theorem 4.12. *[51, Theorem 4.8] Let $0 < k < n \leq m$ be integers, C be an $[n,k]_{q^m}$ MRD code, and θ be a generator of $\operatorname{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Then, C is a θ-Gabidulin code if and only if*

$$\dim(C \cap \theta(C)) = k-1.$$

Theorem 4.12 can be reformulated in the following way, based on the generator matrix in standard form of C.

Theorem 4.13 (Gabidulin criterion)**.** *[81, Lemma 19] Let $0 < k < n \leq m$ be integers and let $X \in \mathbb{F}_{q^m}^{k\times(n-k)}$ such that C_X is an $[n,k]_{q^m}$ MRD code. Then, C_X is a Gabidulin code if and only if there exists θ generator of $\operatorname{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, such that*

$$\operatorname{rk}(\Psi_\theta(X)) = 1.$$

Proof. We know from Theorem 4.12 that an MRD code C_X is a θ-Gabidulin code if and only if

$\dim(C \cap \theta(C)) = k - 1$. We get

$$\begin{aligned} & \dim(C \cap \theta(C)) = k-1 \\ \iff & \operatorname{rk}\left(\begin{array}{c|c} I_k & X \\ I_k & \theta(X) \end{array}\right) = k+1 \\ \iff & \operatorname{rk}\left(\begin{array}{c|c} I_k & X \\ 0 & \theta(X)-X \end{array}\right) = k+1 \\ \iff & \operatorname{rk}(\Psi_\theta(X)) = 1. \end{aligned}$$

□

Theorem 4.13 will be one of the most important results on which this chapter is based. The criterion starts with the assumption that we already know that the code is MRD. However, in Section 4.3 we will derive a new criterion that does not have such assumption and it is definitely easier to verify.

As a consequence of Theorem 2.4, we have an interesting result, that will be useful in the next section.

Corollary 4.14. *Let $X \in \mathbb{F}_{q^m}^{k\times(n-k)}$, and $\tilde{X} = X + B$ for some matrix $B \in \mathbb{F}_q^{k\times(n-k)}$. Let moreover s be a positive integer coprime to m.*

1. *If the code C_X is MRD, then also $C_{\tilde{X}}$ is MRD.*
2. *If the code C_X is a θ-Gabidulin code, then also $C_{\tilde{X}}$ is a θ-Gabidulin code.*

Proof. 1. Let $G = (I_k \mid X)$, be the generator matrix for C_X, and let $\widetilde{G} = (I_k \mid \tilde{X})$ be the generator matrix for $C_{\tilde{X}}$. Then, $\widetilde{G} = GM$ where

$$M = \begin{pmatrix} I_k & B \\ 0 & I_{n-k} \end{pmatrix} \in \mathrm{GL}_n(q).$$

By Lemma 2.4, $C_{\tilde{X}} \sim C_X$ is MRD.

2. By Theorem 4.4 the code C_X is MRD, and so it is $C_{\tilde{X}}$ by part 1 of this Corollary. Moreover we have

$$\Psi_\theta(\tilde{X}) = \Psi_\theta(X+B) = \Psi_\theta(X),$$

and we conclude using Theorem 4.13.

□

4.3 Standard Form of Gabidulin Codes

Similarly to the work of Roth and Seroussi for GRS codes [98], in this section we characterize the matrices $X \in \mathbb{F}_{q^m}^{k\times(n-k)}$ such that the code C_X is a Gabidulin code, and we refer to this family of matrices as *θ-Cauchy matrices.* In order to do that, we rely on Theorem 4.13 which tells that $\mathrm{rk}(\Psi_\theta(X)) = 1$. Therefore, we start with a rank-one matrix A and determine the conditions such that A belongs to the image of the map Ψ_θ. Finally, we impose that the resulting matrices X with $\Psi_\theta(X) = A$, are such that the code C_X is MRD and get the desired characterization.

Moreover, we also give an analogue of Theorem 1.38 for θ-Gabidulin codes. This result represents a new criterion that allows to determine whether a given code in standard form is a Gabidulin code, which is faster than the one given in Theorem 4.13.

As in the whole work, we fix positive integers $0 < k < n \leq m$. For every θ generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, we consider the following sets:

$$\begin{aligned}\mathbb{G}(\theta) &:= \{X \in \mathbb{F}_{q^m}^{k\times(n-k)} \mid C_X \in \mathrm{Gab}_q(k,n,m,\theta)\},\\ \mathcal{R}_1^* &:= \left\{A \in (\mathbb{F}_{q^m}^*)^{k\times(n-k)} \mid \mathrm{rk}(A) = 1\right\},\\ \mathcal{K} &:= \left(\ker\left(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}\right)\right)^{k\times(n-k)}.\end{aligned}$$

Throughout the rest of the chapter, given a set $\mathcal{T} \subseteq \mathbb{F}_{q^m}^{k\times(n-k)}$, we denote by $\Psi_\theta^{-1}(\mathcal{T})$ the preimage of the set $\mathcal{T}$, i.e.

$$\Psi_\theta^{-1}(\mathcal{T}) = \left\{A \in \mathbb{F}_{q^m}^{k\times(n-k)} \mid \Psi_\theta(A) \in \mathcal{T}\right\}.$$

In the same way, for a set $\mathcal{S} \subseteq \mathbb{F}_{q^m}^{k\times(n-k)}$, $\Psi_\theta(\mathcal{S})$ denotes the set of images of the elements in $\mathcal{S}$ through Ψ_θ, i.e.

$$\Psi_\theta(\mathcal{S}) = \{\Psi_\theta(A) \mid A \in \mathcal{S}\}.$$

Lemma 4.15. *For every θ generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, the following properties hold.*

1. $\Psi_\theta(\mathbb{F}_{q^m}^{k\times(n-k)}) = \mathcal{K}$.
2. *Let $A \in \mathbb{F}_{q^m}^{k\times(n-k)}$. If $A \in \mathcal{K}$ and $X \in \Psi_\theta^{-1}(\{A\})$, then*

$$\Psi_\theta^{-1}(\{A\}) = \left\{X + B \mid B \in \mathbb{F}_q^{k\times(n-k)}\right\}.$$

In particular,

$$|\Psi_\theta^{-1}(\{A\})| = \begin{cases} 0 & \text{if } A \notin \mathcal{K} \\ q^{k(n-k)} & \text{if } A \in \mathcal{K}. \end{cases}$$

3. $\Psi_\theta(\mathbb{G}(\theta)) \subseteq \mathcal{R}_1^* \cap \mathcal{K}$, *or, equivalently,* $\mathbb{G}(\theta) \subseteq \Psi_\theta^{-1}(\mathcal{R}_1^* \cap \mathcal{K})$.

4. *Let $A \in \mathcal{R}_1^* \cap \mathcal{K}$ and $X \in \Psi_\theta^{-1}(\{A\})$. If $X \in \mathbb{G}(\theta)$ then the whole preimage of $\{A\}$ is contained in $\mathbb{G}(\theta)$, i.e.*
$$\Psi_\theta^{-1}(\{A\}) \subseteq \mathbb{G}(\theta).$$

Proof.

1. Since Ψ_θ is the function that maps every entry $x_{i,j}$ of the matrix X to $\psi_\theta(x_{i,j})$, we have that $A \in \Psi_\theta(\mathbb{F}_{q^m}^{k\times(n-k)})$ if and only if every entry $a_{i,j}$ of A belongs to $\mathrm{Im}(\psi_\theta)$. By part 5 of Lemma 1.2 this is true if and only if every $a_{i,j}$ belongs to $\ker\left(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}\right)$.

2. If $A \notin \mathcal{K}$, then, by part 1 of this Lemma, this means that $\Psi_\theta^{-1}(A) = \emptyset$. Otherwise, again by part 1, $\Psi_\theta^{-1}(A) \neq \emptyset$. In this case every entry $a_{i,j}$ belongs to $\mathrm{Im}(\psi_\theta)$, and by part 2 of Lemma 1.13,
$$\psi_\theta^{-1}(\{a_{i,j}\}) = \{x_{i,j} + \lambda \mid \lambda \in \mathbb{F}_q\}$$
for some $x_{i,j} \in \mathbb{F}_{q^m}$. Since this holds for every entry, we get the desired result.

3. Let $X \in \mathbb{G}(\theta)$. By Theorem 4.13, $\Psi_\theta(X)$ has rank equal to 1. Moreover, by Lemma 3.10, all the entries of $\Psi_\theta(X)$ are in $\mathbb{F}_{q^m}^*$. Finally, by part 1 of this Lemma, we have $\Psi_\theta(X) \in \mathcal{K}$ and this concludes the proof.

4. It directly follows from part 2 of this Lemma and part 2 of Corollary 4.14.

□

As a consequence of part 4 of Lemma 4.15, given a matrix $X \in \mathbb{F}_{q^m}^{k\times(n-k)}$, we have that the property of C_X being Gabidulin only depends on the image $\Psi_\theta(X)$. It is now crucial to investigate the matrices that belong to the image of the map Ψ_θ, and, by part 3 of Lemma 4.15, in particular $\mathcal{R}_1^* \cap \mathcal{K}$.

By definition, every element in $\mathcal{R}_1^* \cap \mathcal{K}$ has rank one, and it is well-known that every rank-one matrix can be written as the product of a non-zero column vector by a non-zero row vector. Moreover, for a fixed rank-one matrix over $\mathbb{F}_{q^m}$, there are exactly q^m-1 different parametrizations of this form.

The following result is straightforward and directly follows from the considerations above and the definitions of $\mathcal{R}_1^*$ and $\mathcal{K}$.

Lemma 4.16. *The set $\mathcal{R}_1^* \cap \mathcal{K}$ can be written in the following way*
$$\begin{aligned}\mathcal{R}_1^* \cap \mathcal{K} &= \left\{\alpha^\top\beta \mid \alpha \in \mathbb{F}_{q^m}^k, \beta \in \mathbb{F}_{q^m}^{n-k}, \alpha_i\beta_j \in \ker(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}) \text{ for all } i,j\right\}\\ &= \left\{\alpha^\top\beta \mid \alpha \in \mathbb{F}_{q^m}^k, \beta \in \mathbb{F}_{q^m}^{n-k}, \beta_j \in \mathrm{supp}_q(\alpha)^\times \text{ for all } j\right\}\\ &= \left\{\alpha^\top\beta \mid \alpha \in \mathbb{F}_{q^m}^k, \beta \in \mathbb{F}_{q^m}^{n-k}, \mathrm{supp}_q(\beta) \subseteq \mathrm{supp}_q(\alpha)^\times\right\}.\end{aligned}$$

Moreover, every element in $\mathcal{R}_1^* \cap \mathcal{K}$ has $q^m - 1$ distinct representations of this form.

This result gives a convenient way to represent $\mathcal{R}_1^* \cap \mathcal{K}$ with the set

$$V_{k,n} := \left\{ (\alpha, \beta) \in \mathbb{F}_{q^m}^k \times \mathbb{F}_{q^m}^{n-k} \mid \operatorname{supp}_q(\beta) \subseteq \operatorname{supp}_q(\alpha)^\times \right\}.$$

Notice that, since we have $q^m - 1$ distinct representations for a matrix in $\mathcal{R}_1^* \cap \mathcal{K}$ and the entries are all non-zero, we can always choose the representation with $\beta_1 = 1$.

At this point, given $(\alpha, \beta) \in V_{k,n}$ and a matrix $X \in \Psi_\theta^{-1}(\{\alpha^\top \beta\})$, we have, by Theorem 4.13 and by the definition of $\mathbb{G}(\theta)$, that C_X is MRD if and only if $X \in \mathbb{G}(\theta)$, i.e. if and only if C_X is a θ-Gabidulin code.

Lemma 4.17. *Let $(\alpha, \beta) \in V_{k,n}$, and let*

$$X \in \Psi_\theta^{-1}(\{\alpha^\top \beta\}).$$

1. *If $\operatorname{rk}_q(\alpha) < k$, then $X \notin \mathbb{G}(\theta)$, i.e. C_X is not MRD.*

2. *If $\operatorname{rk}_q(\beta) < n - k$, then $X \notin \mathbb{G}(\theta)$, i.e. C_X is not MRD.*

Proof.

1. The entries of the first column of $\alpha^\top \beta$ are $\alpha_1\beta_1, \dots, \alpha_k\beta_1$, that are $\mathbb{F}_q$-linearly dependent by hypothesis. By Lemma 1.14 this means that the entries of the first column of X together with the element 1, are $\mathbb{F}_q$-linearly dependent. At this point we conclude by Lemma 3.10.

2. The entries of the first row of $\alpha^\top \beta$ are $\alpha_1\beta_1 \dots, \alpha_1\beta_{n-k}$, that are $\mathbb{F}_q$-linearly dependent by hypothesis. Then we conclude again using Lemma 1.14 and Lemma 3.10.

□

Finally, we can state our desired result.

Theorem 4.18 (Standard form of Gabidulin codes)**.** *[79] Suppose $X \in \mathbb{F}_{q^m}^{k \times (n-k)}$ is a matrix such that $C_X \in \operatorname{Gab}_q(k, n, m, \theta)$. Then $X \in \Psi_\theta^{-1}(\{\alpha^\top \beta\})$ for some $\alpha \in \mathbb{F}_{q^m}^k, \beta \in \mathbb{F}_{q^m}^{n-k}$ such that*

(a) $\operatorname{rk}_q(\alpha) = k$,

(b) $\operatorname{rk}_q(\beta) = n - k$,

(c) $\operatorname{supp}_q(\beta) \subseteq \operatorname{supp}_q(\alpha)^\times$.

Moreover, if $\alpha \in \mathbb{F}_{q^m}^k, \beta \in \mathbb{F}_{q^m}^{n-k}$ satisfy properties (a), (b), (c) and $X \in \Psi_\theta^{-1}(\{\alpha^\top \beta\})$, then $C_X \in \operatorname{Gab}_q(k, n, m, \theta)$.

Proof. Let C_X be a Gabidulin code. We have that $\Psi_\theta(X)$ is of the form $\alpha^\top \beta$ for some α, β by part 3 of Lemma 4.15 and Lemma 4.16. Part (c) follows from the fact that if C_X is a Gabidulin code, then all the entries of $\Psi_\theta(X)$ belong to $\ker(\operatorname{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q})$. Finally part (a) and (b) follow from Lemma 4.17.

On the other hand, we can count the number of matrices $X \in \Psi_\theta^{-1}(\{\alpha^\top \beta\})$ for $\alpha \in \mathbb{F}_{q^m}^k, \beta \in \mathbb{F}_{q^m}^{n-k}$ satisfying properties (a), (b), (c). For α we have $\prod_{i=0}^{k-1}(q^m - q^i)$ possible choices, while for β we have $\prod_{i=0}^{n-k-1}(q^{m-k} - q^i)$ choices. Moreover, we need to divide by $q^m - 1$ since, by Lemma 4.16, we have $q^m - 1$ choices of (α, β) that give the same matrix $\alpha^\top \beta$. Since for every $\alpha^\top \beta \in \mathcal{R}_1^* \cap \mathcal{K}$ we have, by part 2 of Lemma 4.15, $q^{k(n-k)}$ many matrices in the preimage under the map Ψ_θ, we finally obtain

$$\begin{aligned} |\Psi_\theta^{-1}(\mathcal{R}_1^* \cap \mathcal{K})| =& \frac{q^{k(n-k)}}{q^m - 1} \prod_{i=0}^{k-1}(q^m - q^i) \prod_{i=0}^{n-k-1} (q^{m-k} - q^i) \\ =& \prod_{i=1}^{k-1}(q^m - q^i) \prod_{i=0}^{n-k-1} (q^m - q^{i+k}) \\ =& \prod_{i=1}^{n-1}(q^m - q^i). \end{aligned}$$

By Corollary 4.7, this number is equal to the number of distinct θ-Gabidulin codes. Therefore, by a counting argument, it follows that conditions (a), (b), (c) are also sufficient. □

Theorem 4.18 gives a characterization of the generator matrix in standard form of a Gabidulin code. In [98], Roth and Seroussi showed that there is a one-to-one correspondence between generalized Reed-Solomon (GRS) codes and generalized Cauchy (GC) matrices. In that paper, it is shown that a code in the Hamming metric, whose generator matrix in standard form is $(I_k \mid X)$, is a GRS code if and only if X is a GC matrix (see Theorem 1.37). Since Gabidulin codes are the analogue of GRS codes for the rank metric, it becomes natural to give the definition of a rank analogue of Cauchy matrices according to Theorem 4.18.

Let $\gamma \in \mathbb{F}_{q^m}$ such that $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma) \neq 0$ and θ be a generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. We define the function π_θ as

$$\begin{aligned} \pi_\theta : \mathbb{F}_{q^m} &\longrightarrow \mathbb{F}_{q^m} \\ \alpha &\longmapsto \frac{-1}{\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma)} \sum_{i=0}^{m-2} \left(\theta^{i+1}(\gamma) \sum_{j=0}^{i} (\theta^j(\alpha)) \right). \end{aligned} \tag{4.1}$$

Recall that, by Lemma 1.13, for $\alpha \in \ker(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q})$, $\pi_\theta(\alpha)$ gives one of the elements in the preimage of α under ψ_θ, i.e. $\psi_\theta(\pi_\theta(\alpha)) = \alpha$ and $\pi_\theta(\psi_\theta(\alpha)) = \alpha + \lambda$ for some $\lambda \in \mathbb{F}_q$. Moreover, every element in $\psi_\theta^{-1}(\{\alpha\})$ is of the form $\pi_\theta(\alpha) + \lambda$.

Definition 4.19. Let $\alpha \in \mathbb{F}_{q^m}^t, \beta \in \mathbb{F}_{q^m}^r$ such that

(A) $\mathrm{rk}_q(\alpha) = t$,

(B) $\mathrm{rk}_q(\beta) = r$,

(C) $\mathrm{supp}_q(\beta) \subseteq \mathrm{supp}_q(\alpha)^\times$.

Let moreover θ be a generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ and $B \in \mathbb{F}_q^{t\times r}$. A $t \times r$ *θ-Cauchy matrix* $C_\theta(\alpha, \beta, B)$ is a matrix of the form

$$C_\theta(\alpha,\beta,B) = \begin{pmatrix} \pi_\theta(\alpha_1\beta_1) & \pi_\theta(\alpha_1\beta_2) & \cdots & \pi_\theta(\alpha_1\beta_r) \\ \pi_\theta(\alpha_2\beta_1) & \pi_\theta(\alpha_2\beta_2) & \cdots & \pi_\theta(\alpha_2\beta_r) \\ \vdots & \vdots & & \vdots \\ \pi_\theta(\alpha_t\beta_1) & \pi_\theta(\alpha_t\beta_2) & \cdots & \pi_\theta(\alpha_t\beta_r) \end{pmatrix} + B.$$

Remark 4.20. Definition 4.19 directly arises from the characterization of the generator matrix in standard form of a Gabidulin code. However, one can see that θ-Cauchy matrices introduced in this work are the rank analogue of GC matrix. Indeed, conditions (A), (B) and (C) represent the q-analogues of conditions (a), (b) and (c) of Definition 1.36.

With this definition, we can reformulate Theorem 4.18 in the following way, that puts emphasis on the correspondence between θ-Gabidulin codes and θ-Cauchy matrices.

Theorem 4.21. *[79] Let $X \in \mathbb{F}_{q^m}^{k\times(n-k)}$ and let θ be a generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. The code C_X is a θ-Gabidulin code if and only if the matrix X is a θ-Cauchy matrix.*

From Theorem 4.18 we have an immediate consequence, that relates θ-Cauchy matrices with θ-Moore matrices.

Corollary 4.22. *Let $0 < k < n \leq m$ be positive integers and θ be a generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Let $g = (g_1, \dots, g_n) \in \mathbb{F}_{q^m}^n$ be a vector such that $\mathrm{rk}_q(g) = n$. Then the matrix*

$$M_{k,\theta}(g_1,\dots,g_k)^{-1}M_{k,\theta}(g_{k+1},\dots,g_n)$$

is a $k \times (n-k)$ θ-Cauchy matrix.

Moreover, if R is a $t \times r$ θ-Cauchy matrix, then there exists $g = (g_1, \dots, g_{t+r}) \in \mathbb{F}_{q^m}^{t+r}$ with $\mathrm{rk}_q(g) = t + r$ such that

$$R = M_{t,\theta}(g_1,\dots,g_t)^{-1}M_{t,\theta}(g_{t+1},\dots,g_{t+r}).$$

Now, we want to determine the basis of the linearized polynomial space $\mathcal{L}_{k,\theta}$ that corresponds to the generator matrix in standard form. In order to do that, we introduce the following notion.

Definition 4.23. Let $h = (h_1, \dots, h_\ell) \in \mathbb{F}_{q^m}^\ell$ be a vector such that $\mathrm{rk}_q(h) = \ell$, and let θ be a generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. We define the *associated polynomial* $p_{h,\theta}$ to h as

$$p_{h,\theta}(x) = \det(M_{\ell+1,\theta}(h_1,\dots,h_\ell,x)).$$

Obviously $p_{h,\theta}(x)$ is a linearized θ-polynomial and in particular it belongs to $\mathcal{L}_{\ell+1,\theta}$. Observe that, by the properties of θ-Moore matrices, it can be deduced that the set of roots of $p_{h,\theta}(x)$ in $\mathbb{F}_{q^m}$ is equal to the $\mathbb{F}_q$-subspace $\mathrm{supp}_q(h)$. Moreover, if $h, h' \in \mathbb{F}_{q^m}^{\ell}$ are two vectors such that $\mathrm{rk}_q(h) = \mathrm{rk}_q(h') = \ell$ and $\mathrm{supp}_q(h) = \mathrm{supp}_q(h')$, then

$$p_{h,\theta}(x) = \det(E) p_{h',\theta}(x),$$

where $E \in \mathbb{F}_q^{\ell \times \ell}$ is the change-of-basis matrix from $\{h'_1, \ldots, h'_\ell\}$ to $\{h_1, \ldots, h_\ell\}$. (see [68, Chapter 3, Section 4] for more details).

Remark 4.24. Let $C = \mathcal{G}_{k,\theta}(g)$ be a θ-Gabidulin code. Consider the vectors

$$g^{(i)} := (g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_k) \in \mathbb{F}_{q^m}^{k-1} \quad \text{for } i = 1, \ldots, k,$$

and define the θ-polynomials

$$f_i(x) := p_{g^{(i)},\theta}(g_i)^{-1} p_{g^{(i)},\theta}(x) \quad \text{for } i = 1, \ldots, k.$$

It follows from the definition that for every $i, j \in \{1, \ldots, k\}$, we have $f_i(x) \in \mathcal{L}_{k,\theta}$ and

$$f_i(g_j) = \delta_{i,j} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

Therefore the generator matrix in standard form for the θ-Gabidulin code C is obtained evaluating the basis $\{f_1(x), \ldots, f_k(x)\}$ of $\mathcal{L}_{k,\theta}$ in the points $g_1, \ldots, g_n$.

4.3.1 A New Criterion for Gabidulin Codes

The next result represents the analogue of Theorem 1.38 for the rank metric, and its proof follows directly from Theorem 4.18.

Theorem 4.25 (New Gabidulin Criterion I)**.** *[79] Let $X = (x_{i,j})_{i,j} \in \mathbb{F}_{q^m}^{k \times (n-k)}$ and θ be a generator of* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$*. Then, $C_X \in \mathrm{Gab}_q(k, n, m, \theta)$ if and only if*

(i) the first row of $\Psi_\theta(X)$ has q-rank $n-k$,

(ii) the first column of $\Psi_\theta(X)$ has q-rank k,

(iii) $\mathrm{rk}(\Psi_\theta(X)) = 1$.

This theorem can be reformulated also in the following way.

Theorem 4.26 (New Gabidulin Criterion II)**.** *[79] Let $X = (x_{i,j})_{i,j} \in \mathbb{F}_{q^m}^{k \times (n-k)}$ and θ be a generator of* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$*. Then, $C_X \in \mathrm{Gab}_q(k, n, m, \theta)$ if and only if* *(i')* $\mathrm{rk}_q(1, x_{1,1}, \dots, x_{1,n-k}) = n - k + 1$,

(ii') $\mathrm{rk}_q(1, x_{1,1}, \dots, x_{k,1}) = k + 1$,

(iii) $\mathrm{rk}(\Psi_\theta(X)) = 1$.

Proof. By Lemma 1.14 we have that conditions (i') and (ii') are equivalent to conditions (i) and (ii). This means that the statement is equivalent to Theorem 4.25. □

In addition to representing a natural analogue of Theorem 1.38 for the rank metric framework, Theorem 4.25 also gives a new criterion to recognize whether a given code in standard form is a Gabidulin code. Observe that, contrary to Theorem 4.13, which gives a criterion subject to a previous verification that the code is MRD, this result is independent on this assumption, and it could be verified more easily. Indeed, according to Proposition 3.8, checking whether a code is MRD requires the computation of $\begin{bmatrix} n \\ k \end{bmatrix}_q = \mathcal{O}(q^{k(n-k)})$ matrix products and ranks, while this new criterion only requires to check the linear independence of two sets of elements and the computation of the rank of one matrix.

More generally, suppose we have an $[n, k]_{q^m}$ code C given by one of its generator matrices $G \in \mathbb{F}_{q^m}^{k \times n}$, and a generator θ of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. We can check whether C is a θ-Gabidulin code with the following algorithm. First we compute the reduced row echelon form of G. If it is not of the form $(I_k \mid X)$, then by Lemma 3.10, C is not MRD and hence it is not a θ-Gabidulin code for any θ. Hence, suppose we get a matrix of the form $(I_k \mid X)$. We can use Theorem 4.25, computing the matrix $\Psi_\theta(X)$ and its rank, and then computing the q-ranks of the first row and of the first column. It is easy to see that the computational cost of this algorithm is given by the cost of computing the reduced row echelon form of G, that can be done via Gaussian elimination. Therefore, we have just provided a procedure that verifies if a given code is a Gabidulin code with $\mathcal{O}(k^2nm)$ operations over $\mathbb{F}_{q^m}$, where the factor m arises because we have to check it for all the $\phi(m)$ generators of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. This cost can also be improved if one uses faster algorithms for computing the reduced row echelon form of a matrix.

Example 4.27. Let $q = 3$, $k = 3$ and $n = m = 6$. Consider the finite field $\mathbb{F}_{3^6} = \mathbb{F}_3(a)$, where a is a primitive element that satisfies the relation $a^6 + 2a^4 + a^2 + 2a + 2 = 0$. Consider the $\mathbb{F}_{3^6}$-linear code $C \subseteq \mathbb{F}_{3^6}^6$ with generator matrix

$$G = \begin{pmatrix} a^2 & a^{54} & a^{591} & a^{277} & a^{160} & a^{634} \\ a^{67} & a^{701} & a^{443} & a^{45} & a^{486} & a^{209} \\ a^{320} & a^{199} & a^{650} & a^{361} & a^{701} & a^{562} \end{pmatrix}.$$

We put G in reduced row echelon form, and obtain the matrix $(I_3 \mid X)$ with

$$X = \begin{pmatrix} a^{180} & a^{373} & a^{714} \\ a^{14} & a^{588} & a^{561} \\ a^{370} & a^{702} & a^{442} \end{pmatrix}.$$

$$\Psi_{\bar{\theta}}(X) = \begin{pmatrix} a^{72} & a^{226} & a^{406} \\ a^{98} & a^{252} & a^{432} \\ a^{144} & a^{298} & a^{478} \end{pmatrix},$$

where $\bar{\theta}$ is the 3-Frobenius automorphism. We can observe that this matrix has rank one. Moreover, the elements of the first row of $\Psi_{\bar{\theta}}(X)$ are linearly independent over $\mathbb{F}_3$ and the same holds for the elements of the first column. Thus, by Theorem 4.25, C is a $\bar{\theta}$-Gabidulin code.

4.3.2 Recovering the Parameters of the Code from the θ-Cauchy Matrix

In order to complete the picture of the correspondence between Gabidulin codes and θ-Cauchy matrices, we need to find the relations between the points $g_1, \dots, g_n$ in which the set $\mathcal{L}_{k,\theta}$ (or, equivalently, $\mathcal{G}_{k,\theta}$) is evaluated, and the vectors $\alpha \in \mathbb{F}_{q^m}^k$, $\beta \in \mathbb{F}_{q^m}^{n-k}$ and matrix $B \in \mathbb{F}_q^{k\times(n-k)}$ that define the corresponding θ-Cauchy matrix. Observe that, by Lemma 4.16 and Theorem 4.6, we can always suppose $\beta_1 = g_1 = 1$. In the rest of this subsection we will always use this assumption.

As a preliminary result, we prove that knowing the entries of a θ-Cauchy matrix is equivalent to knowing its defining parameters α, β and B. If one knows the latter, then it is trivial that the entries of the θ-Cauchy matrix can be easily computed. For the other way around we have the following result.

Proposition 4.28. *Let $X \in \mathbb{F}_{q^m}^{t\times r}$ be a θ-Cauchy matrix. Then it is possible to recover the parameters $\alpha \in \mathbb{F}_{q^m}^t, \beta \in \mathbb{F}_{q^m}^r$ and $B \in \mathbb{F}_q^{t\times r}$ from the entries of X.*

Proof. It follows from the definition of π_θ and from Lemma 1.13 that $\psi_\theta(x_{i,1}) = \alpha_i$ (since $\beta_1 = 1$), and $\psi_\theta(x_{i,j}) = \alpha_i\beta_j$ for $j = 2, \dots, r$. From that, we can recover α and β. Finally, the matrix B can be easily obtained, since

$$B = X - \begin{pmatrix} \pi_\theta(\alpha_1\beta_1) & \pi_\theta(\alpha_1\beta_2) & \cdots & \pi_\theta(\alpha_1\beta_r) \\ \pi_\theta(\alpha_2\beta_1) & \pi_\theta(\alpha_2\beta_2) & \cdots & \pi_\theta(\alpha_2\beta_r) \\ \vdots & \vdots & & \vdots \\ \pi_\theta(\alpha_t\beta_1) & \pi_\theta(\alpha_t\beta_2) & \cdots & \pi_\theta(\alpha_t\beta_r) \end{pmatrix}.$$

□

Suppose we have a θ-Gabidulin code $C = \mathcal{G}_{k,\theta}(g)$. Then we can efficiently obtain the corresponding θ-Cauchy matrix by computing the reduced row echelon form of the θ-Moore matrix

$M_{k,\theta}(g)$. The cost of this reduction is $\mathcal{O}(k^2n)$ field operations over the finite field $\mathbb{F}_{q^m}$. If we want a more explicit way to do it (but less efficient), then we can compute the basis $\{f_1(x),\dots,f_k(x)\}$ of $\mathcal{L}_{k,\theta}$ as described in Remark 4.24, and evaluate it in the points $g_1,\dots,g_n$. In order to recover the parameters $\alpha\in\mathbb{F}_{q^m}^k$, $\beta\in\mathbb{F}_{q^m}^{n-k}$ and $B\in\mathbb{F}_q^{k\times(n-k)}$, one can use Proposition 4.28.

On the other hand, we have that the two sets of parameters that we want to put in relation are connected by Corollary 4.22 as follows:

$$M_{k,\theta}(g_1,\dots,g_k)C_\theta(\alpha,\beta,B)=M_{k,\theta}(g_{k+1},\dots,g_n).$$

From this matrix equation we can deduce how to get the g_i's from α,β and B. Since $\beta_1=1$, from the first column of the matrix product we get

$$\sum_{j=1}^{k} g_j(\pi_\theta(\alpha_j)+b_{j,1})=g_{k+1} \tag{4.2}$$

and, in general, for $\ell=0,\dots,k-1$,

$$\sum_{j=1}^{k}\theta^\ell(g_j)(\pi_\theta(\alpha_j)+b_{j,1})=\theta^\ell(g_{k+1}). \tag{4.3}$$

If we apply θ to equation (4.3) for $\ell-1$ and we subtract (4.3) to it, we get the set of equations

$$\begin{aligned}0&=\sum_{j=1}^{k}\theta^\ell(g_j)(\theta(\pi_\theta(\alpha_j)+b_{j,1})-(\pi_\theta(\alpha_j)+b_{j,1}))\\&=\sum_{j=1}^{k}\theta^\ell(g_j)\alpha_j,\end{aligned} \tag{4.4}$$

for every $\ell=1,\dots,k-1$, where the last identity follows from part 2 of Lemma 1.13.

We can repeat this process with any other column of the matrix product, and we get, for $i=2,\dots,n-k$,

$$\sum_{j=1}^{k} g_j(\pi_\theta(\alpha_j\beta_i)+b_{j,i})=g_{k+i} \tag{4.5}$$

and

$$0=\sum_{j=1}^{k}\theta^\ell(g_j)\alpha_j\beta_i.$$

However, this set of equations is the same as (4.4), therefore we do not consider it. Now, we can show that equations (4.2), (4.4) and (4.5) are exactly what we need for our purpose.

By Proposition 4.28, we can recover the vectors α and β and the matrix B from X. Moreover, applying $\theta^{-\ell}$ to every equation in (4.4), we get a linear system

$$\begin{pmatrix} \theta^{-1}(\alpha_2) & \theta^{-1}(\alpha_3) & \cdots & \theta^{-1}(\alpha_k) \\ \theta^{-2}(\alpha_2) & \theta^{-2}(\alpha_3) & \cdots & \theta^{-2}(\alpha_k) \\ \vdots & \vdots & & \vdots \\ \theta^{-k+1}(\alpha_2) & \theta^{-k+1}(\alpha_3) & \cdots & \theta^{-k+1}(\alpha_k) \end{pmatrix} \begin{pmatrix} g_2 \\ \vdots \\ g_k \end{pmatrix} = - \begin{pmatrix} \theta^{-1}(\alpha_1) \\ \theta^{-2}(\alpha_1) \\ \vdots \\ \theta^{-k+1}(\alpha_1) \end{pmatrix} \tag{4.6}$$

with $g_2, \ldots, g_k$ unknowns. The matrix defining the linear system (4.6) is a $(k-1) \times (k-1)$ matrix with coefficients in $\mathbb{F}_{q^m}$. In particular, this matrix is equal to the θ^{-1}-Moore matrix $M_{k-1,\theta^{-1}}(\theta^{-1}(\alpha_2), \ldots, \theta^{-1}(\alpha_k))$, and since $\alpha_2, \ldots, \alpha_k$ are $\mathbb{F}_q$-linearly independent it has full rank. The unique solution of this linear system allows to compute $g_2, \ldots, g_k$, and for computing $g_{k+1}, \ldots, g_n$ one can use (4.2) and (4.5).

4.4 Gabidulin Codes in Hankel and Toeplitz Form

In this section we use the characterization of the generator matrix in standard form for a Gabidulin code given in Section 4.3 for the construction of particular subclasses of these codes. Indeed, we will prove that there exist Gabidulin codes C_X such that X is a Hankel matrix or a Toeplitz matrix.

For our purpose, we first need a technical result.

Lemma 4.29. *Let $\gamma \in \mathbb{F}_{q^m}$ be a primitive element, i.e. such that $\mathbb{F}_{q^m}^* = \langle \gamma \rangle$. Then there exists $\ell \in \mathbb{N}$ such that*

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma^\ell) = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma^{\ell+1}) = \ldots = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma^{\ell+m-2}) = 0.$$

Proof. Since γ is a primitive element, then $\mathbb{F}_{q^m} = \mathbb{F}_q(\gamma)$ and $1, \gamma, \gamma^2, \ldots, \gamma^{m-1}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$. Consider the $\mathbb{F}_q$-linear map $L \in \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_{q^m}, \mathbb{F}_q)$ defined as

$$L(\gamma^i) = \begin{cases} 0 & \text{for } 0 \leq i \leq m-2 \\ 1 & \text{for } i = m-1. \end{cases}$$

L is a non zero element in $\mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_{q^m}, \mathbb{F}_q)$, and by Theorem 1.4, there exists $\beta \in \mathbb{F}_{q^m}^*$ such that $L = T_\beta$. At this point, since γ is a primitive element, there exists $\ell \in \mathbb{N}$ such that $\beta = \gamma^\ell$. In this way, we have that for all $i = 0, \ldots, m-2$,

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma^{\ell+i}) = T_{\gamma^\ell}(\gamma^i) = L(\gamma^i) = 0$$

and this concludes the proof. □

Definition 4.30. An $r \times s$ matrix $A = (A_{i,j})$ over a field $\mathbb{F}$ is called *Toeplitz matrix* if there exists a vector $a = (a_{1-r}, a_{2-r}, \dots, a_{s-1}) \in \mathbb{F}^{r+s-1}$ such that

$$A_{i,j} = a_{j-i}.$$

An $r \times s$ matrix $A = (A_{i,j})$ over a field $\mathbb{F}$ is called *Hankel matrix* if there exists a vector $a = (a_0, a_1, \dots, a_{r+s-2}) \in \mathbb{F}^{r+s-1}$ such that

$$A_{i,j} = a_{i+j-2}.$$

A special kind of square Toeplitz matrices is given by circulant matrices.

Definition 4.31. An $r \times r$ matrix $A = (A_{i,j})$ over a field $\mathbb{F}$ is called *circulant matrix* if there exists a vector $a = (a_0, \dots, a_{r-1})$ such that

$$A_{i,j} = a_{j-i(\bmod r)}.$$

Theorem 4.32. *For every $0 < k < n \leq m$ and every θ generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, there exists a θ-Gabidulin code C_X such that X is a Hankel matrix.*

Proof. Let $\gamma \in \mathbb{F}_{q^m}$ be a primitive element. By Lemma 4.29 there exist $\ell \in \mathbb{N}$ such that

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma^{\ell}) = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma^{\ell+1}) = \ldots = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma^{\ell+m-2}) = 0. \tag{4.7}$$

Let $\alpha \in \mathbb{F}_{q^m}^k$, $\beta \in \mathbb{F}_{q^m}^{n-k}$ be defined as

$$\begin{aligned}\alpha &= (\gamma^{\ell}, \gamma^{\ell+1}, \dots, \gamma^{\ell+k-1}),\\ \beta &= (1, \gamma, \dots, \gamma^{n-k-1}),\end{aligned}$$

and consider the matrix $\alpha^{\top}\beta$. We now check that α, β satisfy properties (a), (b), (c) of Theorem 4.18. Indeed, γ is a primitive element, and therefore $1, \gamma, \dots, \gamma^{m-1}$ are linearly independent, as well as $\gamma^{\ell}, \dots, \gamma^{\ell+m-1}$. In particular, properties (a) and (b) are satisfied. Moreover, for every $i = 0, \dots, k-1$, $j = 0, \dots, n-k-1$,

$$T_{\gamma^{\ell+i}}(\gamma^j) = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma^{\ell+i+j}) = 0,$$

where the last inequality holds by (4.7). Therefore also property (c) is verified.

Now we have that every matrix $X \in \Psi_{\theta}^{-1}(\{\alpha^{\top}\beta\})$ is a θ-Cauchy matrix and hence it is of the form

$$X = \begin{pmatrix} \pi_\theta(\gamma^{\ell}) & \pi_\theta(\gamma^{\ell+1}) & \cdots & \pi_\theta(\gamma^{\ell+n-k-1}) \\ \pi_\theta(\gamma^{\ell+1}) & \pi_\theta(\gamma^{\ell+2}) & \cdots & \pi_\theta(\gamma^{\ell+n-k}) \\ \vdots & \vdots & & \vdots \\ \pi_\theta(\gamma^{\ell+k-1}) & \pi_\theta(\gamma^{\ell+k}) & \cdots & \pi_\theta(\gamma^{\ell+n-2}) \end{pmatrix} + B,$$

for an arbitrary $B \in \mathbb{F}_q^{k\times(n-k)}$. Choosing B as a Hankel matrix completes the proof. □

Theorem 4.33. *For every $0 < k < n \leq m$ and every θ generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, there exists a θ-Gabidulin code C_X such that X is a Toeplitz matrix.*

Proof. Following the same proof of Theorem 4.32 with

$$\begin{aligned}\alpha &= (\gamma^{\ell+n-k-1}, \gamma^{\ell+n-k}, \dots, \gamma^{\ell+n-2}),\\ \beta &= (1, \gamma^{-1}, \gamma^{-2}, \dots, \gamma^{-n+k+1}),\end{aligned}$$

the matrix obtained is of the form

$$X = \begin{pmatrix} \pi_\theta(\gamma^{\ell+n-k-1}) & \pi_\theta(\gamma^{\ell+n-k-2}) & \cdots & \pi_\theta(\gamma^{\ell}) \\ \pi_\theta(\gamma^{\ell+n-k}) & \pi_\theta(\gamma^{\ell+n-k-1}) & \cdots & \pi_\theta(\gamma^{\ell+1}) \\ \vdots & \vdots & & \vdots \\ \pi_\theta(\gamma^{\ell+n-2}) & \pi_\theta(\gamma^{\ell+n-3}) & \cdots & \pi_\theta(\gamma^{\ell+k-1}) \end{pmatrix} + B,$$

for an arbitrary $B \in \mathbb{F}_q^{k\times(n-k)}$. As above, choosing B in Toeplitz form concludes the proof. □

These two theorems allow to define two subfamilies of Gabidulin codes, the *Hankel Gabidulin codes* and the *Toeplitz Gabidulin codes*. In the following lemma we can see that this structure on the generator matrix in standard form is hard to improve if we still require the code to be MRD.

Lemma 4.34. *Suppose that n is even and $k = \frac{n}{2}$. Let $X \in \mathbb{F}_{q^m}^{k\times k}$ be a circulant matrix, and let d be the minimum rank distance of the code C_X. Then $d \leq 2$.*

In particular, for $n \geq 4$, there does not exist any $[n, \frac{n}{2}]_{q^m}$ MRD code C_X with X circulant matrix.

Proof. Since the matrix X is circulant, then the sum of the elements on each of its columns is constant. Let γ be such a sum. Then, the non-zero codeword of the code C_X

$$(1, \dots, 1)\left(\begin{array}{c|c} I_k & X \end{array}\right) = (1, \dots, 1, \gamma, \dots, \gamma)$$

has q-rank at most 2. In particular, if $n \geq 4$ we have

$$n - k + 1 = \frac{n}{2} + 1 > 2 \geq d$$

and therefore, the code C_X can not be MRD. □

This result possibly suggests that, at least in the case $k = \frac{n}{2}$, it is very difficult to require more structure on the non-systematic part of the generator matrix in standard form of an MRD code. However, it would be very interesting to find new families of Gabidulin, or more generally MRD codes with structured generator matrices.

We conclude this chapter with a small example.

Example 4.35. Consider the case $q = 2$, $k = 3$, $n = m = 6$ and $s = 1$. We construct a Hankel Gabidulin code of dimension 3 and length 6 over the finite field $\mathbb{F}_{2^6} = \mathbb{F}_2(a)$, where a is a primitive element that satisfies $a^6 + a^4 + a^3 + a + 1 = 0$. One can find, by Lemma 4.29, five consecutive powers of a that belong to $\ker(\mathrm{Tr}_{\mathbb{F}_{2^6}/\mathbb{F}_2})$, that are a^i for $i = 14, 15, \dots, 18$. Then, we set the vectors

$$\alpha = (a^{14}, a^{15}, a^{16}), \quad \beta = (1, a, a^2).$$

Moreover, we choose the matrix B to be the zero matrix, and the map

$$\begin{array}{rcl} \pi_{\bar{\theta}} : \mathbb{F}_{2^6} & \longrightarrow & \mathbb{F}_{2^6} \\ z & \longmapsto & \dfrac{-1}{\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma)} \displaystyle\sum_{i=0}^{4} \left(\gamma^{2^{i+1}} \sum_{j=0}^{i} z^{2^j} \right), \end{array}$$

where $\gamma = a^3$, and $\bar{\theta}$ is the 2-Frobenius automorphism. We then get the following $\bar{\theta}$-Cauchy matrix

$$X := C_{\bar{\theta}}(\alpha, \beta, 0) = \begin{pmatrix} \pi_{\bar{\theta}}(a^{14}) & \pi_{\bar{\theta}}(a^{15}) & \pi_{\bar{\theta}}(a^{16}) \\ \pi_{\bar{\theta}}(a^{15}) & \pi_{\bar{\theta}}(a^{16}) & \pi_{\bar{\theta}}(a^{17}) \\ \pi_{\bar{\theta}}(a^{16}) & \pi_{\bar{\theta}}(a^{17}) & \pi_{\bar{\theta}}(a^{18}) \end{pmatrix} = \begin{pmatrix} a^{57} & a^7 & a^{13} \\ a^7 & a^{13} & a^{37} \\ a^{13} & a^{37} & a^{36} \end{pmatrix}.$$

By Theorem 4.32 the code C_X is a $\bar{\theta}$-Gabidulin code. Moreover we can recover the evaluation points $g_1, \dots, g_6$ of the code. We can suppose $g_1 = 1$, and recover $g_2 = a^{45}$ and $g_3 = a^{15}$ using the linear system (4.6). Finally, using equations (4.2) and (4.5) we get $g_4 = a^{46}$, $g_5 = a^{14}$ and $g_6 = a^{28}$. Therefore, our Hankel Gabidulin code is

$$C_X = \mathcal{G}_{3,\bar{\theta}}(1, a^{45}, a^{15}, a^{46}, a^{14}, a^{28}).$$

4.5 Gabidulin Codes over Fields of any Characteristic

In this section we want to briefly describe what happens if we switch from finite fields to fields of any characteristic. In particular, what follows aims to explain the reasons of our notations and definitions in terms of generators of the Galois group, which are not common in literature.

Recently, a new theory of rank-metric codes over fields of any characteristic was developed by Augot, Loidreau and Robert in [4, 3, 5], which was also shown to be useful in low-rank matrix completion problem [78]. We describe here the general idea. Let $\mathbb{F}$ be a field, and let $\mathbb{L}$ be an extension field of degree m, such that $\mathbb{L}/\mathbb{F}$ is a Galois extension and $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ is a cyclic group.

One can consider vector rank-metric codes as k-dimensional $\mathbb{L}$-subspaces of $\mathbb{L}^n$, endowed with the rank distance. Such distance is defined by the $\mathbb{F}$-rank of a vector $v \in \mathbb{L}^n$, that is

$\mathrm{rk}_{\mathbb{F}}(v) := \dim_{\mathbb{F}} \mathrm{supp}_{\mathbb{F}}(v)$, where

$$\mathrm{supp}_{\mathbb{F}}(v) = \langle v_1, \ldots, v_n \rangle_{\mathbb{F}}.$$

The minimum distance $d(C)$ of a code C is analogously defined. Codes of dimension k and minimum distance d in $\mathbb{L}^n$ are denoted $[n, k, d]_{\mathbb{L}}$ codes or simply $[n, k]_{\mathbb{L}}$ codes. Also in this more general setting, the Singleton-like bound holds. For a non-zero code $C \subseteq \mathbb{L}^n$, we have

$$d(C) \leq n - \dim_{\mathbb{L}}(C) + 1. \tag{4.8}$$

Whenever $n \leq m$, it is possible to construct codes meeting the bound in (4.8) with equality, which are also called MRD codes. The construction is the same as the one for Gabidulin codes. We take a generator θ of $G := \mathrm{Gal}(\mathbb{L}/\mathbb{F})$, and a vector $g = (g_1, \ldots, g_n)$ with $\mathrm{rk}_{\mathbb{F}}(g) = n$. Moreover, we define the $\mathbb{L}$-subspace $\mathcal{G}_{k,\theta}$ of the group algebra $\mathbb{L}[\theta] = \mathbb{L}[G]$ as

$$\mathcal{G}_{k,\theta} := \langle \mathrm{id}, \theta, \ldots, \theta^{k-1} \rangle_{\mathbb{L}} = \left\{ f_0 \mathrm{id} + f_1 \theta + \ldots + f_{k-1} \theta^{k-1} \mid f_i \in \mathbb{L} \right\}.$$

The code $\mathcal{G}_{k,\theta}(g) := \{(f(g_1), \ldots, f(g_n)) \mid f \in \mathcal{G}_{k,\theta}\}$ is called *θ-Gabidulin-like code.* Theorem 4.4 holds also in this framework, that is, Gabidulin-like codes are MRD. The statement follows from Theorem 1.20.

We want to point out that almost all the results contained in this chapter are true for this more general setting. It is straightforward to prove that Proposition 4.5, Theorem 4.6 and Proposition 4.8 still hold. When we say “almost”, it is because obviously cardinality results such as Corollaries 4.7 and 4.9 do not make sense in this context. However, it is still true that the set of $[n, k]_{\mathbb{L}}$ θ-Gabidulin-like codes is in 1-to-1 correspondence with the set of

$$\{g \in \mathbb{L}^n \mid \mathrm{rk}_{\mathbb{F}}(g) = n\}/_{\sim}, \tag{4.9}$$

where $\sim$ is the equivalence relation defined as follows:

$$v \sim u \iff \exists\ \lambda \in \mathbb{L}^* \text{ such that } v = \lambda u.$$

Also Theorems 4.12 and 4.13 and Corollary 4.14 are true in this setting, if we replace $\mathbb{F}_{q^m}$ with $\mathbb{L}$ and $\mathbb{F}_q$ with $\mathbb{F}$. This is because the proofs of those results do not depend on the field, and they are based on Theorem 1.20. Indeed, the canonical generator matrix of a θ-Gabidulin-like code is still a θ-Moore matrix.

The only open problem we leave is if θ-Gabidulin-like codes have the same parametrization for the generator matrix in standard form as the one given in Theorem 4.18. The proof of that result is based on a cardinality argument, which is not possible to use in this case. However, we believe that also this result holds. Indeed, that parametrization strongly relies on the duality theory of the trace map given by the additive version of Hilbert's Theorem 90, which is a result that holds for every cyclic Galois extension. Therefore, our belief is that it should be possible to define a bijection between the set defined in (4.9) and the set $\Psi_\theta^{-1}(V)$, where

$$V = \left\{\alpha^\top \beta \mid \alpha \in \mathbb{L}^k, \beta \in \mathbb{L}^{n-k}, \mathrm{rk}_{\mathbb{F}}(\alpha) = k, \mathrm{rk}_{\mathbb{F}}(\beta) = n-k, \mathrm{supp}_{\mathbb{F}}(\beta) \subseteq \mathrm{supp}_{\mathbb{F}}(\alpha)^\times\right\}$$

and Ψ_θ is the map that acts on the set of $k \times (n-k)$ matrices as $\theta - \mathrm{id}$ entrywise.

Once proved the analogue of Theorem 4.18 (if it is true), it would be interesting to see if one can construct θ-Gabidulin-like codes in Hankel or Toeplitz form. The construction given for the finite field case is based on the existence of a primitive element, which we do not have in case of infinite fields.

Finally, we want to remark that also almost all the definitions and results in Chapter 7 can be generalized to this framework. The only results which are not true in that chapter are the cardinality results in which q is involved. For instance, we can not give an analogue to Theorem 7.28 nor to part 2 of Theorem 7.29, but the same result holds for part 1 of the same Theorem.

Chapter 5

Genericity Results in the Rank Metric

The question, if there are other general constructions of MRD codes that are not equivalent to Gabidulin codes, has been of large interest recently. Some constructions of non-Gabidulin MRD codes can be found e.g. in [25, 29, 106, 86, 74, 114], where many of the derived codes, when seen as block codes in $\mathbb{F}_{q^m}^n$, are not linear over $\mathbb{F}_{q^m}$ but only linear over some subfield of it. For some small parameter sets, constructions of $[n,k]_{q^m}$ non-Gabidulin MRD codes were presented in [51, 28, 26, 27], and for $q \neq 2$, a general family of those codes appears in [106, 74]. For m very large and any q, a new family was given in [90]. These last two families will be studied in Chapter 7. On the other hand, for $k \in \{1, 2, n-2, n-1\}$ all the $[n,k]_{2^n}$ MRD codes are Gabidulin codes (see Theorem 7.32 from [88]). In general, it remains an open question for which parameters non-Gabidulin MRD codes exist, and if so, how many such codes there are.

In the first section of this chapter, we show that the properties of being MRD (maximum rank distance) and non-Gabidulin are generic among the $[n,k]_{q^m}$ codes. These results imply that, over a large field extension degree, a randomly chosen generator matrix generates an MRD and a non-Gabidulin code with high probability. Moreover, an upper, respectively lower, bound on the respective probabilities in dependence on the extension degree are given. Finally, we show that for any length n and dimension k there exists an $[n,k]_{q^m}$ non-Gabidulin MRD code, if the extension degree m is large enough.

In the second section, we analyze the properties of being MRD among the $[n \times m, k]_q$ codes. Contrary to what happens for vector codes, it was shown in [18, 2], that in this case the results are different, and it is not true that a random code is MRD with high probability.

5.1 Vector Codes

The results contained in this section were published by Neri, Horlemann-Trautmann, Randrianarisoa and Rosenthal in [81]. However the estimates in Subsection 5.1.4 have been slightly improved in the present dissertation.

5.1.1 The Zariski Topology over Finite Fields

Consider the polynomial ring $\mathbb{F}_q[x_1, \dots, x_r]$ over the base field $\mathbb{F}_q$ and denote by $\bar{\mathbb{F}}_q$ the algebraic closure of $\mathbb{F}_q$, necessarily an infinite field. For a subset $S \subseteq \mathbb{F}_q[x_1, \dots, x_r]$ one defines the *algebraic set*

$$V(S) := \{x \in \bar{\mathbb{F}}_q^r \mid f(x) = 0, \forall f \in S\}.$$

It is well-known that the algebraic sets inside $\bar{\mathbb{F}}_q^r$ form the *closed sets* of a topology, called the *Zariski topology* [49, Ch. I, Sec. 1]. The complements of the Zariski-closed sets are the *Zariski-open* sets.

Definition 5.1. A subset $G \subset \bar{\mathbb{F}}_q^r$ is called a *generic set* if G contains a non-empty Zariski-open set.

If the base field is the field of real numbers $\mathbb{R}$, (or complex numbers $\mathbb{C}$) then a generic set inside $\mathbb{R}^r$ (respectively inside $\mathbb{C}^r$) is necessarily dense and its complement is contained in an algebraic set of dimension at most $r - 1$.

Over a finite field $\mathbb{F}_q$ one has to be a little bit more careful. Indeed for every subset $T \subset \mathbb{F}_q^r$ one finds a set of polynomials $S \subseteq \mathbb{F}_q[x_1, \dots, x_r]$ such that

$$\{x \in \mathbb{F}_q^r \mid f(x) = 0, \forall f \in S\} = T.$$

This follows simply from the fact that a single point inside $\mathbb{F}_q^r$ forms a Zariski-closed set and any subset $T \subset \mathbb{F}_q^r$ is a finite union of points. However if one has an algebraic set $V(S)$, as defined at the beginning of this subsection, then the number of $\mathbb{F}_{q^m}$-rational points defined through

$$V(S; \mathbb{F}_{q^m}) := \{x \in \mathbb{F}_{q^m}^r \mid f(x) = 0, \forall f \in S\}$$

becomes in proportion to the cardinality of the whole vector space $\mathbb{F}_{q^m}^r$ smaller, as the extension degree m increases. This is a consequence of the Schwartz-Zippel Lemma (or Schwartz-Zippel-DeMillo-Lipton [102, 120, 31] which we will formulate, for our purposes, over a finite field. The lemma itself will be crucial for our probability estimations in Subsection 5.1.3. We use the following version of the Schwartz-Zippel Lemma.

Lemma 5.2 (Schwartz-Zippel). *[67, Lemma 1.1] Let $f \in \mathbb{F}_q[x_1, x_2, \dots, x_r]$ be a non-zero polynomial of total degree $d \geq 0$. Let $\mathbb{F}_{q^m}$ be an extension field and let $F \subseteq \mathbb{F}_{q^m}$ be a finite set. Let $\alpha_1, \alpha_2, \dots, \alpha_r$ be selected at random independently and uniformly from F. Then*

$$\Pr\big(f(\alpha_1, \alpha_2, \dots, \alpha_r) = 0\big) \leq \frac{d}{|F|}.$$

5.1.2 Topological Results

The idea of this section is to show that the properties of being MRD and non-Gabidulin are generic properties.

Recall that, by Lemma 3.10, every $[n,k]_{q^m}$ MRD code in $\mathbb{F}_{q^m}^n$ has a unique representation by its generator matrix $G \in \mathbb{F}_{q^m}^{k\times n}$ in standard/systematic form

$$G = (I_k \mid X).$$

Thus, we have a one-to-one correspondence between the set of $[n,k]_{q^m}$ MRD codes and a subset of the set of matrices $\mathbb{F}_{q^m}^{k\times(n-k)}$. Therefore we want to investigate how many matrices $X \in \mathbb{F}_{q^m}^{k\times(n-k)}$ give rise to an MRD or a Gabidulin code, when plugged into the above form of a systematic generator matrix.

However, in order to make sense of the definition of genericity, we need to do this investigation over the algebraic closure of $\mathbb{F}_{q^m}$. In particular, we will show that the set of matrices fulfilling the MRD criterion of Proposition 3.8, and the subset of these matrices not fulfilling the Gabidulin criterion of Theorem 4.13, are generic sets over the algebraic closure.

We first show that the set of generator matrices fulfilling the MRD criterion of Proposition 3.8 is generic.

Theorem 5.3. *Let $1 \leq k \leq n-1$. The set*

$$S_{\mathrm{MRD}} := \{X \in \bar{\mathbb{F}}_{q^m}^{k\times(n-k)} \mid \det((I_k \mid X)E^\top) \neq 0, \forall\, E \in \mathcal{T}_q(k,n)\}$$

is a generic subset of $\bar{\mathbb{F}}_{q^m}^{k\times(n-k)}$.

Proof. We need to show that S_{MRD} contains a non-empty Zariski-open set. In fact, we will show that S_{MRD} is a non-empty Zariski-open set. The non-emptiness follows from the existence of Gabidulin codes for every set of parameters. Hence it remains to show that it is Zariski-open.

In the following, for any set S, we denote its complement by S^C. If we denote the entries of $X \in \bar{\mathbb{F}}_{q^m}^{k(n-k)}$ by $x_1, \dots, x_{k(n-k)}$, then, for a given $E \in \mathcal{T}_q(k,n)$, we have $\det((I_k \mid X)E^\top) \in \mathbb{F}_q[x_1, \dots, x_{k(n-k)}]$. Hence we can write

$$\begin{aligned} S_{\mathrm{MRD}} &= \bigcap_{E\in\mathcal{T}_q(k,n)} \{X \in \bar{\mathbb{F}}_{q^m}^{k\times(n-k)} \mid \det((I_k \mid X)E^\top) \neq 0\} \\ &= \bigcap_{E\in\mathcal{T}_q(k,n)} V(\det((I_k \mid X)E^\top))^C, \end{aligned}$$

i.e., it is a finite intersection of Zariski-open sets. Therefore, S_{MRD} is a Zariski-open set. □

Remark 5.4. In Theorem 5.3 we chose the MRD criterion of Proposition 3.8 to show that the set of matrices $X \in \bar{\mathbb{F}}_{q^m}^{k\times(n-k)}$ satisfying that criterion is generic. One can do the same by using the MRD criterion of Horlemann-Trautmann and Marshall from [51, Corollary 3.3].

We now turn to Gabidulin codes. The following theorem shows that the set of generator matrices not fulfilling the Gabidulin criterion of Theorem 4.13 is generic over the algebraic closure.

Theorem 5.5. *Let $1 \leq k \leq n-1$ and θ be a generator of* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$*. Moreover, let $S_{\mathrm{MRD}} \subseteq \bar{\mathbb{F}}_{q^m}^{k\times(n-k)}$ be as defined in Theorem 5.3. The set*

$$S_{\mathrm{Gab},\theta} := \{X \in \bar{\mathbb{F}}_{q^m}^{k\times(n-k)} \mid \mathrm{rk}(\Psi_\theta(X)) = 1\} \cap S_{\mathrm{MRD}}$$

is a Zariski-closed subset of the Zariski-open set S_{MRD}.

Proof. Let $X \in S_{\mathrm{Gab},\theta}$. Since $X \in S_{\mathrm{MRD}}$, it follows from Lemma 3.10 that $X_{i,j} \notin \mathbb{F}_q$ for $i = 1,\dots,k$ and $j = 1,\dots,n-k$. Then the condition $\mathrm{rk}(\Psi_\theta(X)) = 1$ is equivalent to $\mathrm{rk}(\Psi_\theta(X)) < 2$, which in turn is equivalent to the condition that all 2×2-minors of $\Psi_\theta(X)$ are zero. If we denote the entries of $X \in \bar{\mathbb{F}}_{q^m}^{k(n-k)}$ as the variables $x_1,\dots,x_{k(n-k)}$, then these 2×2-minors of $\Psi_\theta(X)$ are elements of $\mathbb{F}_q[x_1,\dots,x_{k(n-k)}]$. This is due to the fact that $\theta(x) = x^{q^s}$ for some integer $s < m$ and therefore $\psi_\theta(x_i)$ is a polynomial of degree q^s. Let us call the set of all these minors S'. Then

$$\begin{aligned} S_{\mathrm{Gab},\theta} &= \left\{X \in \bar{\mathbb{F}}_{q^m}^{k\times(n-k)} \mid f(x_1,\dots,x_{k(n-k)}) = 0, \forall f \in S'\right\} \cap S_{\mathrm{MRD}} \\ &= V(S') \cap S_{\mathrm{MRD}}. \end{aligned}$$

Hence it is a Zariski-closed subset of $S_{\mathrm{MRD}} \subseteq \bar{\mathbb{F}}_{q^m}^{k\times(n-k)}$. □

Theorem 5.5 implies that the complement in S_{MRD} of $S_{\mathrm{Gab},\theta}$, i.e. the set of $k\times(n-k)$ matrices over $\bar{\mathbb{F}}_{q^m}$ that fulfill the MRD criterion but do not fulfill the Gabidulin criterion, is a Zariski-open subset of S_{MRD}. Thus, if it is non-empty, then the complement of $S_{\mathrm{Gab},\theta}$ is a generic set. The non-emptiness of this set will be shown in the following subsection, in Theorem 5.12.

In other words, over the algebraic closure, a randomly chosen generator matrix fulfills the MRD criterion and does not fulfill the Gabidulin criterion with probability 1. In the next subsection, we will clarify what this exactly means in terms of probability.

5.1.3 Probability Estimations

In the previous subsection we have used the Zariski topology to show that a randomly chosen linear code over $\bar{\mathbb{F}}_{q^m}$ fulfills most likely the MRD criterion but not the Gabidulin criterion. Intuitively this tells us that over a finite, but large, extension field of $\mathbb{F}_q$ a randomly chosen linear code is most likely an MRD code but not a Gabidulin code. In this section we derive some bounds on the probability that this statement is true, in dependence of the field extension degree m.

Here we give a lower bound on the probability that a random $[n,k]_{q^m}$ code in $\mathbb{F}_{q^m}^n$ is MRD.

For $E \in \mathcal{T}_q(k,n)$ we define the polynomial

$$f_E(x_1,\dots,x_{k(n-k)}) := \det((I_k \,|\, X)E^\top) \in \mathbb{F}_{q^m}[x_1,\dots,x_{k(n-k)}],$$

and we furthermore define

$$f^*(x_1,\dots,x_{k(n-k)}) := \operatorname{lcm}\left\{f_E(x_1,\dots,x_{k(n-k)}) \,|\, E \in \mathcal{T}_q(k,n)\right\},$$

where, as before, the entries of X are the variables $x_1,\dots,x_{k(n-k)}$. We can easily observe the following.

Proposition 5.6. *The set of $[n,k]_{q^m}$ non-MRD codes is in one-to-one correspondence with the algebraic set*

$$V(\{f^*\};\mathbb{F}_{q^m}) = \left\{(v_1,\dots,v_{k(n-k)}) \in \mathbb{F}_{q^m}^{k(n-k)} \,|\, f^*(v_1,\dots,v_{k(n-k)}) = 0\right\}.$$

Proof. It follows from Proposition 3.8 that the set of $[n,k]_{q^m}$ non-MRD codes is in one-to-one correspondence with the algebraic set

$$\begin{aligned} V &= \bigcup_{E\in\mathcal{T}_q(k,n)} \left\{(v_1,\dots,v_{k(n-k)}) \in \mathbb{F}_{q^m}^{k(n-k)} \mid f_E(v_1,\dots,v_{k(n-k)}) = 0\right\} \\ &= \left\{(v_1,\dots,v_{k(n-k)}) \in \mathbb{F}_{q^m}^{k(n-k)} \mid \prod_{E\in\mathcal{T}_q(k,n)} f_E(v_1,\dots,v_{k(n-k)}) = 0\right\} \\ &= \left\{(v_1,\dots,v_{k(n-k)}) \in \mathbb{F}_{q^m}^{k(n-k)} \mid f^*(v_1,\dots,v_{k(n-k)}) = 0\right\} \\ &= V(\{f^*\};\mathbb{F}_{q^m}), \end{aligned}$$

where the second and the third equalities follow from the well-known fact that

$$V(\{f\};\mathbb{F}_{q^m}) \cup V(\{g\};\mathbb{F}_{q^m}) = V(\{fg\};\mathbb{F}_{q^m}) = V(\{\operatorname{lcm}(f,g)\};\mathbb{F}_{q^m})$$

for any $f,g \in \mathbb{F}_q[x_1,\dots,x_{k(n-k)}]$. □

Note that in the definition of an algebraic set, it suffices to use the square-free part of the defining polynomial(s). In the above definition of V however, $f^*(x_1,\dots,x_{k(n-k)})$ is already square-free, as we show in the following.

Lemma 5.7. *For every $E \in \mathcal{T}_q(k,n)$ the polynomial $f_E(x_1,\dots,x_{k(n-k)})$ is square-free. In particular, the polynomial $f^*(x_1,\dots,x_{k(n-k)})$ is square-free.*

Proof. Every variable x_i is contained in at most one row of the matrix $(I_k \,|\, X)E^\top$. Hence, in the polynomial $f_E(x_1,\dots,x_{k(n-k)})$ the degree with respect to every variable is at most 1. Thus, $f_E(x_1,\dots,x_{k(n-k)})$ cannot have multiple factors. □

We now determine an upper bound on the degree of the defining polynomial f^*.

Lemma 5.8. *Let $E \in \mathcal{T}_q(k,n)$ and let $\mathcal{U}_0$ be the subspace of $\mathbb{F}_q^n$ defined by*

$$\mathcal{U}_0 := \operatorname{rowsp}(I_k \mid 0) = \left\{(u_1,\dots,u_n) \in \mathbb{F}_q^n \mid u_{k+1} = u_{k+2} = \ldots = u_n = 0\right\}.$$

Then

$$\deg f_E = k - \dim\left(\operatorname{rowsp}(E) \cap \mathcal{U}_0\right).$$

Proof. Let $r := k - \dim\left(\operatorname{rowsp}(E) \cap \mathcal{U}_0\right)$ with $0 \le r \le k$. We can write

$$E^\top = \left(\begin{array}{c} E_1 \\ \hline E_2 \end{array}\right),$$

where $E_1 \in \mathbb{F}_q^{k\times k}, E_2 \in \mathbb{F}_q^{(n-k)\times k}$. Since $\dim\left(\operatorname{rowsp}(E) \cap \mathcal{U}_0\right) = k-r$, we have $\operatorname{rk}(E_2) = r$. Thus, there exists a matrix $R \in \mathrm{GL}_k(q)$ such that the first r columns of E_2R are linearly independent and the last $k-r$ columns are zero. Then

$$f_E(x_1,\dots,x_{k(n-k)}) = \det((I_k \mid X)E^\top) = \det(R)^{-1}\det(E_1R + XE_2R).$$

The last $k-r$ columns of the matrix XE_2R are zero, i.e., the last $k-r$ columns of E_1R+XE_2R do not contain any of the variables x_i's. On the other hand, the entries of the first r columns are polynomials in $\mathbb{F}_q[x_1,\dots,x_{k(n-k)}]$ of degree 1, since

$$E_1R + XE_2R = \left(\sum_{\ell=1}^{k}(E_1)_{i,\ell}R_{\ell,j} + \sum_{\ell=1}^{k}\sum_{\ell'=1}^{n-k} X_{i,\ell'}(E_2)_{\ell',\ell}R_{\ell,j}\right)_{i,j}.$$

Hence we have $\deg f_E \le r$.

Now consider the matrix E_2R. We can write

$$E_2R = \left(\begin{array}{c|c} \tilde{E}_2 & 0 \end{array}\right)$$

where $\tilde{E}_2$ is an $(n-k)\times r$ matrix of rank r. Hence

$$XE_2R = \left(\begin{array}{c|c} X\tilde{E}_2 & 0 \end{array}\right).$$

First we prove that the entries of the matrix $X\tilde{E}_2$ are algebraically independent over $\mathbb{F}_q$. Fix $1 \le i \le k$ and denote by $(X\tilde{E}_2)_i$ the i-th row of the matrix $X\tilde{E}_2$. Then, consider the polynomials $(X\tilde{E}_2)_{i,j}$, for $j = 1,\dots,r$, that only involve the variables $x_{(i-1)(n-k)+1},\dots,x_{i(n-k)}$. The Jacobian of these polynomials is $\tilde{E}_2^\top$, whose rows are linearly independent over $\mathbb{F}_q$. Therefore the elements in every row are algebraically independent over $\mathbb{F}_q$.[1] Moreover, different rows involve different

[1] The Jacobian criterion for algebraic independence of polynomials over $\mathbb{C}$ can be found in [66, Ch. I, Sec. 5].

variables, hence we can conclude that the entries of the matrix $X\tilde{E}_2$ are algebraically independent over $\mathbb{F}_q$.

At this point consider the set of all $r \times r$ minors of $X\tilde{E}_2$. These minors are all different and hence linearly independent over $\mathbb{F}_q$, otherwise a non-trivial linear combination of them that gives 0 would produce a non-trivial polynomial relation between the entries of $X\tilde{E}_2$. Now observe that the degree r term of f_E is a linear combination of these minors. If we write

$$E_1 R = \left(\, * \, \middle| \, \tilde{E}_1 \, \right),$$

where $\tilde{E}_1 \in \mathbb{F}_q^{k \times (k-r)}$, then the coefficients of this linear combination are given by the $(k-r) \times (k-r)$ minors of $\tilde{E}_1$, multiplied by $\det(R)^{-1}$. Since $E^\top R$ has rank k and the last $k-r$ columns of $E_2 R$ are 0, it follows that the columns of $\tilde{E}_1$ are linearly independent, and hence at least one of the coefficients of the linear combination is non-zero. This proves that the degree r term of f_E is non-zero, and hence $\deg f_E = r$. □

We can now give the main result of this subsection, an upper bound on the probability that a random generator matrix generates an MRD code:

Theorem 5.9. *Let $X \in \mathbb{F}_{q^m}^{k \times (n-k)}$ be randomly chosen. Then*

$$\Pr\big(\, C_X \textit{ is an MRD code } \big) \geq 1 - \sum_{r=0}^{k} r \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2} q^{-m}.$$

Proof. For every $r = 0, 1, \ldots, k$ we define the set

$$\mathcal{T}_{q,r} = \{E \in \mathcal{T}_q(k,n) \mid \dim\left(\mathcal{U}_0 \cap \operatorname{rowsp}(E)\right) = k - r\},$$

where

$$\mathcal{U}_0 := \operatorname{rowsp}(I_k \mid 0) = \big\{(u_1, \ldots, u_n) \in \mathbb{F}_q^n \mid u_{k+1} = u_{k+2} = \ldots = u_n = 0\big\}.$$

By Lemma 1.18 we have

$$|\mathcal{T}_{q,r}| = \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2}.$$

Moreover, by Lemma 5.8, if $E \in \mathcal{T}_{q,r}$, then $\deg f_E = r$. Hence, by the definition of f^*, we have

$$\deg f^* \leq \sum_{E \in \mathcal{T}_q(k,n)} \deg f_E = \sum_{r=0}^{k} \sum_{E \in \mathcal{T}_{q,r}} \deg f_E = \sum_{r=0}^{k} r \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2}.$$

With Lemma 5.2, the statement follows.

□

In positive characteristic, it remains true that the linear independence of the rows of the Jacobian matrix of a set of polynomials implies the algebraic independence of them.

Remember that we know how to construct MRD codes, namely as Gabidulin codes, for any set of parameters. Hence the probability that a randomly chosen generator matrix generates an MRD code is always greater than zero. However, the lower bound of Theorem 5.9 is not always positive. In particular, for

$$m \leq k(n-k) + \log_q k$$

we get

$$\begin{aligned}
&1 - \sum_{r=0}^{k} r \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2} q^{-m} \\
=&1 - q^{-m} \left(\sum_{r=1}^{k} r \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2} \right) \\
\leq&1 - q^{-m} \left(k \sum_{r=1}^{k} \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2} \right) \\
\overset{(*)}{=}&1 - q^{-m} \begin{bmatrix} n \\ k \end{bmatrix}_q \\
\leq&1 - q^{-m} \left(k q^{k(n-k)} \right) \leq 0,
\end{aligned}$$

where $(*)$ follows from the q-Vandermonde identity. This implies that the bound is not tight (and not sensible) in these cases.

A similar result on the density of $[n,k]_{q^m}$ MRD codes was found later by Byrne and Ravagnani in [18]. The proof involves different techniques, and was part of a general method developed for proving density results in coding theory. Here, we just state their asymptotical results.

Theorem 5.10. *[18, Corollary 5.5] Let k be an integer with $1 \leq k \leq n$. Let $\mathcal{F}$ be the family of $[n,k]_{q^m}$ codes, and $\mathcal{F}'$ be the family of $[n,k]_{q^m}$ non-MRD codes. Then*

$$\frac{|\mathcal{F}'|}{|\mathcal{F}|} = \Theta(q^{-m}) \quad \textit{for} \quad m \longrightarrow +\infty.$$

5.1.4 Existence of non-Gabidulin MRD Codes

We can now use the probability estimates we got in Theorem 5.9 to give implicit and explicit results about the existence of $[n,k]_{q^m}$ MRD codes that are not Gabidulin codes for almost every set of parameters. We first write a probabilistic result concerning Gabidulin codes which directly follows from Corollary 4.7. This result improves the probabilistic estimate of [81, Theorem 31] by a factor of $2q^{(k-1)(n-k-1)}$.

Theorem 5.11. *Let $X \in \mathbb{F}_{q^m}^{k\times(n-k)}$ be randomly chosen. Then*

$$\Pr\left(C_X \textit{ is a Gabidulin code }\right) \leq \frac{\phi(m)}{2} q^{-m(n-k-1)(k-1)} \prod_{i=1}^{n-1}(1-q^{i-m}),$$

where ϕ denotes the Euler-ϕ function.

Proof. By Corollary 4.9 there are at most $\frac{\phi(m)}{2}\prod_{i=1}^{n-1}(q^m - q^i)$ Gabidulin codes, and by Lemma 3.10, all of them have a generator matrix in standard form. Since there are exactly $q^{mk(n-k)}$ many codes in standard form, the proof is complete. □

Theorem 5.12. *1. For any prime power q, and for any $1 < k < n-1$, there exists an integer $M(q,k,n)$ such that, for every $m \geq M(q,k,n)$, there exists an $[n,k]_{q^m}$ MRD code that is not a Gabidulin code.*

2. An integer $M(q,k,n)$ with this property can be found as the minimum integer solution of the inequality

$$1 - \sum_{r=0}^{k} r \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2} q^{-m} > \frac{m-1}{2} q^{-m(n-k-1)(k-1)} \tag{5.1}$$

taken over all $m \in \mathbb{N}$.

Proof. For fixed q, k and n consider the function

$$\begin{aligned} F(m) &= \sum_{r=0}^{k} r \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2} q^{-m} + \frac{m-1}{2} q^{-m(n-k-1)(k-1)} \\ &= aq^{-m} + \frac{m-1}{2} q^{-cm}, \end{aligned}$$

where

$$a := \sum_{r=0}^{k} r \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2}, \quad c := (n-k-1)(k-1).$$

Since $k \neq 1$ and $k \neq n-1$, we have $c > 0$. In this case $F(m)$ is the sum of two non-increasing functions and hence it is non-increasing. Therefore, the function $1 - F(m)$ is non-decreasing. Moreover, it is easy to see that

$$\lim_{m\to+\infty} 1 - F(m) = 1.$$

This means that the set of the solutions of Inequality (5.1) is non-empty. Then it has a minimum solution $M(q,k,n)$. Since the function $1 - F(m)$ is non-decreasing, every $m \geq M(q,k,n)$ is also a solution of (5.1). Hence, by Theorems 5.9 and 5.11, we have the following chain of inequalities for every $m \geq M(q,k,n)$,

$$\begin{aligned}\Pr\big(C_X \text{ is an MRD code}\big) \geq 1 - aq^{-m} > \frac{m-1}{2}q^{-cm}\\ \geq \Pr\big(C_X \text{ is a Gabidulin code}\big),\end{aligned}$$

which concludes the proof. □

The theorem above proves the existence of infinitely many integers m such that there exists an $[n,k]_{q^m}$ MRD code which is not Gabidulin. These integers are given implicitly as the solutions of Inequality 5.1. In the following we derive such integers explicitly, in order to give an idea of the magnitude of the extension degree needed to have non-Gabidulin MRD codes.

We first need some auxiliary results: For $b \in \mathbb{N}$ we consider the sequence $\{Q(b)\}_{b\in\mathbb{N}}$ defined as

$$Q(b) := \prod_{i=1}^{b}\left(1 - \frac{1}{2^i}\right).$$

Lemma 5.13. *$\{Q(b)\}_{b\in\mathbb{N}}$ is a decreasing positive sequence, such that*

$$\lim_{b\to+\infty} Q(b) = C \simeq 0.2887.$$

In particular, for every $b \in \mathbb{N}$, $Q(b) > \frac{1}{4}$.

Proof. The sequence $\{Q(b)\}_{b\in\mathbb{N}}$ is trivially positive and decreasing. Its decimal expansion, which gives rise to the above approximation, can be found in [113] with ID number A048651. □

Lemma 5.14. *Let a, b be two positive integers with $0 < b \leq a$. Then*

$$\begin{bmatrix} a \\ b \end{bmatrix}_q \leq \frac{1}{Q(b)}q^{b(a-b)}.$$

Proof. We have

$$\begin{bmatrix} a \\ b \end{bmatrix}_q = \prod_{i=0}^{b-1}\frac{q^{a-i}-1}{q^{b-i}-1} \leq \prod_{i=0}^{b-1}\frac{q^{a-i}}{q^{b-i}-\left(\frac{q}{2}\right)^{b-i}} = \frac{1}{Q(b)}q^{b(a-b)}.$$

□

We can now state the explicit version of the existence of $[n,k]_{q^m}$ non-Gabidulin MRD codes:

Theorem 5.15. *Let q be a prime power, and let k, n be two integers such that $1 < k < n-1$. If*

$$m \geq k(n-k) + \min\{\lceil \log_q(4k+1)\rceil, \lceil \log_q(4(n-k)+1)\rceil,$$

then there exists an $[n,k]_{q^m}$ MRD code that is not Gabidulin.

Proof. We will prove the statement for the case $n \geq 2k$ and $m \geq k(n-k) + \lceil \log_q(4k+1) \rceil$. The other case, $n < 2k$ and $m \geq k(n-k) + \lceil \log_q(4(n-k)+1) \rceil$, then follows by duality, using Theorem 2.14 and Proposotion 4.5.

As in the proof of Theorem 5.12, consider the function

$$F(m) = \sum_{r=0}^{k} r \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2} q^{-m} + \frac{(m-1)}{2} q^{-m(n-k-1)(k-1)}.$$

We need to show that $F(m) < 1$ for $m \geq k(n-k) + \lceil \log_q(4k+1) \rceil$. We divide the proof into two cases.

Case $n \geq 5$. We have

$$\begin{aligned} \sum_{r=0}^{k} r \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2} q^{-m} &\leq k q^{-m} \sum_{r=0}^{k} \begin{bmatrix} k \\ r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2} \\ &= k \begin{bmatrix} n \\ k \end{bmatrix}_q q^{-m} \\ &< 4kq^{k(n-k)-m}, \end{aligned} \tag{5.2}$$

where the last inequality follows from Lemma 5.14 and Lemma 5.13. Moreover,

$$\frac{(m-1)}{2} q^{-m(n-k-1)(k-1)} = q^{-m(k(n-k)-n+1)+\log_q(m-1)-\log_q(2)}. \tag{5.3}$$

Furthermore, we observe that

$$n + k^2 + \frac{1}{2} - kn \leq 0 \iff n \geq \frac{k^2 + \frac{1}{2}}{k-1} \iff n \geq k + 1 + \frac{3}{2(k-1)},$$

which is fulfilled by the conditions $k \leq n/2$ and $n \geq 5$. Therefore,

$$\begin{aligned} &\big(-m(k(n-k)-n+1) + \log_q(m-1) - \log_q(2)\big) - (k(n-k)-m) \\ &= m(n + k^2 - kn) + \log_q\left(\frac{m-1}{2}\right) + k^2 - kn \\ &\leq m\big(n + k^2 - kn + \frac{1}{2}\big) + k^2 - kn - \frac{1}{2} \\ &\leq 0. \end{aligned}$$

Combining this with Inequality (5.2) and Equality (5.3) we get

$$F(m) < 4kq^{k(n-k)-m} + q^{-m(k(n-k)-n+1)+\log_q(m-1)-\log_q(2)} \leq (4k+1)q^{k(n-k)-m}.$$

Hence, we can conclude that for $m \geq k(n-k) + \lceil \log_q(4k+1) \rceil$, it holds that $F(m) < 1$, i.e., there exists a non-Gabidulin MRD code.

Case $n = 4$. This implies that $k = 2$ and $m \geq 4 + \lceil \log_q(9) \rceil$. For these fixed values of k and n, we consider $F(m) = G(q, m)$ as a function of q and m. We get

$$G(q,m) = \frac{2q^4 + q^3 + 2q^2 + q}{q^m} + \frac{m-1}{2q^m},$$

which is a decreasing function in both q and m. Hence, if we fix q, we have that

$$G(q, 4 + \lceil \log_q(9) \rceil) \geq G(q, m),$$

for every $m \geq 4 + \lceil \log_q(9) \rceil$. So we need to show that $G(q, 4 + \lceil \log_q(9) \rceil) < 1$ for every prime power q. We have

$$\begin{aligned} G(q, 4 + \lceil \log_q(9) \rceil) &= \frac{2q^4 + q^3 + 2q^2 + q}{q^{4+\lceil \log_q(9) \rceil}} + \frac{3 + \lceil \log_q(9) \rceil}{2q^{4+\lceil \log_q(9) \rceil}} \\ &\leq \frac{2q^4 + q^3 + 2q^2 + q}{9q^4} + \frac{3 + \lceil 2\log_q(3) \rceil}{18q^4} =: K(q). \end{aligned}$$

We observe that $K(q)$ is a decreasing function in q. Therefore,

$$G(q, 4 + \lceil \log_q(9) \rceil) \leq K(q) \leq K(2) = \frac{107}{288} < 1,$$

which concludes the proof.

□

Remark 5.16. In the previous theorem, the condition $1 < k < n - 1$ is not a real restriction, since one can easily see that all MRD codes of dimension $k = 1$ or $k = n-1$ are Gabidulin codes, see e.g. [51, Thm. 5.1].

5.2 Matrix Codes

We have seen in the previous section (Theorems 5.9 and 5.10) that for $[n,k]_{q^m}$ codes, the proportion of MRD codes among all the $[n,k]_{q^m}$ codes goes to 1, as m goes to infinity. However, it is surprising that the situation for $[n \times m, k]_q$ codes is quite different. This behaviour was shown independently in [2] and in [18].

Let $2 \leq d \leq n \leq m$ be integers, and set $k := m(n - d + 1)$. Denote by $\mathcal{Z}_{q,m}$ the set of $[n \times m, k]_q$ codes, and by $\widehat{\mathcal{Z}}_{q,m}$ the set of $[n \times m, k, d]_q$ codes, which are therefore MRD, and define the number

$$s_m(q) := \left| \left\{ A \in \mathbb{F}_q^{m \times m} \mid A \text{ has no eigenvalues in } \mathbb{F}_q \right\} \right|.$$

With this notation, we can state the crucial results showing that $[n \times m, k]_q$ MRD codes are not dense. The following theorem was proved by Byrne and Ravagnani in [18].

Theorem 5.17. *[18, Corollaries 6.2 and 6.4] Let $2 \leq d \leq n \leq m$ be integers and $k := m(n-d+1)$.*

1. *For every $\epsilon > 0$ there exists $q_\epsilon \in \mathbb{N}$ such that*

$$\frac{|\widehat{\mathcal{Z}}_{q,m}|}{|\mathcal{Z}_{q,m}|} \leq \frac{1}{2} + \epsilon, \quad \textit{for every } q \geq q_\epsilon.$$

2. *For every $\epsilon > 0$ there exists $m_\epsilon \in \mathbb{N}$ such that*

$$\frac{|\widehat{\mathcal{Z}}_{q,m}|}{|\mathcal{Z}_{q,m}|} \leq \frac{1}{2}\left(\frac{q^2-3q+3}{(q-1)^2}\right) + \epsilon, \quad \textit{for every } m \geq m_\epsilon.$$

The asymptotical behaviour in q has been investigated further by Antrobus and Gluesing-Luerssen. The following theorem gives a more precise upper bound on the proportion of $[n, k]_{q^m}$ MRD codes, and it is based on [2, Theorem 7.5].

Theorem 5.18. *Let $2 \leq d \leq n \leq m$ be integers and $k := m(n-d+1)$. Then*

$$\frac{|\widehat{\mathcal{Z}}_{q,m}|}{|\mathcal{Z}_{q,m}|} \leq s_m(q)^{(n-d+1)(d-1)} \begin{bmatrix} mn \\ k \end{bmatrix}_q^{-1},$$

which in turn converges to

$$\left(\sum_{j=0}^{m} \frac{(-1)^j}{j!}\right)^{(n-d+1)(d-1)},$$

when q goes to infinity.

Furthermore, when $n = 2$, the upper bound is asymptotically met, as shown in [2, Proposition 7.4].

Theorem 5.19. *Let $2 = d = n \leq m$ be integers and $k = m$. Then*

$$\frac{|\widehat{\mathcal{Z}}_{q,m}|}{|\mathcal{Z}_{q,m}|} = s_m(q) \begin{bmatrix} 2m \\ m \end{bmatrix}_q^{-1}.$$

Moreover,

$$\lim_{q \to +\infty} \frac{|\widehat{\mathcal{Z}}_{q,m}|}{|\mathcal{Z}_{q,m}|} = \sum_{j=0}^{m} \frac{(-1)^j}{j!} \approx \frac{1}{e}.$$

Chapter 6

Codes and Tensors: Tensor Rank Extremal Codes

In this chapter, we deepen the relation between rank-metric codes and tensors, focusing more on the tensor rank. We have already seen in Chapter 3 rank-metric codes in the framework of 3-tensors, and how generator tensor and parity check tensor of an $\mathbb{F}_q$-linear space of matrices describe the properties of such space. An important and well-studied parameter of a tensor is given by its *tensor rank*, which is also central to algebraic complexity theory [14, 15, 60]. The tensor rank considered here is the minimum number of simple tensors that appear in the expression of a tensor as a sum of simple tensors. It extends the notion of matrix rank and gives a measure of the complexity of tensor multiplication. Precise computation of tensor rank is elusive for an arbitrary tensor; indeed computing the rank of a 3-tensor over a finite field is NP-complete [50]. We propose that the tensor rank is a significant parameter in the theory of rank-metric codes. This extends the notion of the tensor rank of a rank-metric code corresponding to a finite semifield [63]. As seen in Chapter 3, a rank-metric code in $\mathbb{F}_q^{n\times m}$ is a *slice space* of an associated *generator tensor*, just as a code in $\mathbb{F}_q^n$ is the row-space of a generator matrix. The smaller the tensor rank of the generator tensor, the more efficient the encoding. Therefore, it is of interest to obtain codes whose generator tensors have minimum tensor rank.

Lower bounds on tensor rank have been known for some time [60]. As seen in Definition 3.14, the notion of tensor rank can be extended to an $[n \times m, k, d]_q$ code $\mathcal{C}$, and this quantity satisfies the relation

$$\mathrm{trk}(\mathcal{C}) \geq k + d - 1. \tag{6.1}$$

Coding theorists will immediately notice the similarity of this inequality to the Singleton bound. We will refer to a code meeting this bound as a *minimum tensor rank* (MTR) code. It is known that any (nondegenerate) tensor of rank R gives rise to a linear block code of length R, and in particular that any lower bound on the length of a linear block code provides an immediate lower bound on the tensor rank [14, 15]. Therefore, it can be deduced that any MTR code gives a construction of an MDS block code. A central problem posed in this chapter is to address the inverse problem: given an MDS block code of length R, find a construction of an MTR code with tensor rank R. We solve this problem for a range of parameter sets. Moreover, we introduce the *generalized ranks* of a rank-metric code, which turn out to be an invariant of code equivalence. In particular, such values can be used to distinguish between inequivalent codes and, remarkably, even between MRD codes that otherwise share many invariants. Furthermore, generalized tensor ranks lead to a refinement of the tensor rank bound, from which the existing tensor rank bound (6.1) can be deduced. The coding theoretic arguments used in these proofs are very simple and compact.

The results presented in this chapter are taken from the paper [16] by Byrne, Neri, Ravagnani and Sheekey.

6.1 A Connection with Linear Block Codes

In [14], the authors draw a connection between tensor rank and linear block codes (See [15, Chapter 18] for a detailed exposition). This connection provides a lower bound on the tensor rank in terms of the length of a block code, hence one can apply coding theoretic bounds to get an estimate for $\mathrm{trk}(X)$. First, we define the following number from coding theory.

Definition 6.1. For positive integers k, d we define

$$N_q(k,d) := \min\{N \in \mathbb{N} \mid \text{there exists an } [N,k,d]_q \text{ block code }\}.$$

We will associate a linear block code with a rank-metric code as follows. Let $\mathcal{C}$ be an $[n\times m,k]_q$ code with tensor rank R. By Proposition 1.26, we can define the following.

Definition 6.2. Let $\mathcal{C}$ be an $[n \times m, k]_q$ code with $k \geq 1$ and tensor rank R. A set $\mathcal{A} = \{A_1, \dots, A_R\} \subset \mathbb{F}_q^{n\times m}$ of rank 1 matrices such that $\mathcal{C} \subseteq \langle \mathcal{A} \rangle$ is called an *R-basis* for $\mathcal{C}$.

Let $\mathcal{A} = \{A_1, \dots, A_R\} \subset \mathbb{F}_q^{n\times m}$ be a linearly independent set of matrices of rank 1. We define an $\mathbb{F}_q$-linear isomorphism (c.f. [15, Theorem 18.4]):

$$\begin{array}{rcl} \psi_{\mathcal{A}} : \langle \mathcal{A} \rangle & \longrightarrow & \mathbb{F}_q^R \\ \sum\limits_{i=1}^{R} \mu_i A_i & \longmapsto & \sum\limits_{i=1}^{R} \mu_i e_i, \end{array}$$

where e_i denotes the i-th vector of the standard basis.

Definition 6.3. Let $\mathcal{C}$ be an $[n \times m, k]_q$ code with tensor rank R and let $\mathcal{A}$ be an R-basis for $\mathcal{C}$. We define the linear block code $C_{\mathcal{A}}$ to be the image of $\mathcal{C}$ under $\psi_{\mathcal{A}}$:

$$C_{\mathcal{A}} := \psi_{\mathcal{A}}(\mathcal{C}),$$

endowed with the Hamming distance.

Given a generator tensor $X = \sum_{r=1}^{R} u_r \otimes v_r \otimes w_r$ of an $[n \times m, k]_q$ code $\mathcal{C}$, any element M of $\mathcal{C}$ can be expressed as

$$M = m_1(a, X) = \sum_{r=1}^{R} a \cdot u_r(v_r \otimes w_r)$$

for some $a \in \mathbb{F}_q^k$. For $A_r = v_r \otimes w_r$, the image of the element M under $\psi_{\mathcal{A}}$ is $(a \cdot u_r \mid 1 \leq r \leq R)$. In other words, we have that $C_{\mathcal{A}}$ is simply the $[R, k]_q$ block code with $k \times R$ generator matrix $(u_r \mid 1 \leq r \leq R)$.

Theorem 6.4 ([14]). *Let $\mathcal{C}$ be an $[n \times m, k, d]_q$ code with tensor rank R. Let $\mathcal{A} = \{A_1, \ldots, A_R\}$ be an R-basis for $\mathcal{C}$. Then the following hold.*

1. *For every $M \in \mathcal{C}$, $\mathrm{rk}(M) \leq \mathrm{wt}_H(\psi_{\mathcal{A}}(M))$.*
2. *$C_{\mathcal{A}}$ is an $[R, k, \geq d]_q$ block code.*
3. *$\mathrm{trk}(\mathcal{C}) \geq N_q(k, d)$.*

Proof. Let $M \in \mathcal{C}$, and let $s = \mathrm{rk}(M)$. Then any expression of M as sum of rank one matrices requires at least s such matrices in the sum. In particular, $M = \sum_{i=1}^{R} \lambda_i A_i$ for some $\lambda_i \in \mathbb{F}_q$ with at least s of the values λ_i non-zero. Then clearly $s \leq \mathrm{wt}_H(\psi_{\mathcal{A}}(M)) \leq R$, proving the first statement. The next two statements follow immediately. □

Definition 6.5. Let $\mathcal{C}$ be an $[n \times m, k, d]_q$ code. We say that $\mathcal{C}$ is *tensor rank extremal* if $\mathrm{trk}(\mathcal{C}) = N_q(k, d)$. Moreover, we say that $\mathcal{C}$ is *minimum tensor rank*, or *MTR* in short, if it meets the bound of Theorem 1.28, that is, if

$$\mathrm{trk}(\mathcal{C}) = k + d(\mathcal{C}) - 1.$$

Indeed, any lower bound on $N_q(k, d)$ provides a lower bound on the tensor rank, so the connection to linear block codes can be exploited. In particular, if $\mathcal{C}$ meets the tensor-rank bound, that is, if $R = k + d - 1$, then the code $C_{\mathcal{A}}$ is an $[R, k, R - k + 1]_q$ block code and thus it is MDS.

For any pair of full-rank matrices $V \in \mathbb{F}^{n \times R}$ and $W \in \mathbb{F}^{m \times R}$, define the $\mathbb{F}_q$-linear map

$$\begin{aligned} \phi_{V,W} : \mathbb{F}_q^R &\longrightarrow \mathbb{F}_q^{n \times m} \\ x &\longmapsto V \operatorname{diag}(x) W^\top. \end{aligned}$$

Let v_r, w_r denote the r-th columns of V and W, respectively, and let $\mathcal{A} = \{A_r \mid 1 \leq r \leq R\}$, with $A_r = v_r \otimes w_r$ for each r. Then

$$\phi_{V,W}(\psi_{\mathcal{A}}(M)) = M, \tag{6.2}$$

for each M in the span of $\mathcal{A}$. This is easy to see, indeed, if $M = \sum_{r=1}^{R} \lambda_r A_r$ for some $\lambda_r \in \mathbb{F}_q$, then we have

$$\begin{aligned} \phi_{V,W}(\psi_{\mathcal{A}}(M)) &= \phi_{V,W}\left(\sum_{r=1}^{R} \lambda_r e_r\right) \\ &= \phi_{V,W}(\lambda) \\ &= V\,\mathrm{diag}(\lambda)W^\top \\ &= \sum_{r=1}^{R} \lambda_r v_r \otimes w_r \\ &= \sum_{r=1}^{R} \lambda_r A_r = M. \end{aligned}$$

This yields the following result.

Lemma 6.6. *Let $\mathcal{C}$ be a nondegenerate $[n \times m, k]_q$ code. Suppose that $\mathcal{C} = V\langle\mathcal{D}\rangle W^\top$ for some set $\mathcal{D} = \{D_1, \ldots, D_k\}$ of diagonal matrices in $\mathbb{F}_q^{R\times R}$ and matrices $V \in \mathbb{F}_q^{n\times R}$ and $W \in \mathbb{F}_q^{m\times R}$ of ranks n, m respectively. Let v_r, w_r denote the r-th columns of V and W, respectively, and define $\mathcal{A} = \{A_r \mid 1 \leq r \leq R\}$ such that $A_r = v_r \otimes w_r$ for each r. Then $\phi_{V,W}(\psi_{\mathcal{A}}(\mathcal{C})) = \mathcal{C}$.*

In the next section, we shall be concerned with tensor rank extremal codes (those meeting the bound of Theorem 6.4) and in particular with constructions of codes meeting Kruskal's tensor rank bound of Theorem 1.28. One approach will be to view a rank-metric code $\mathcal{C}$ in $\mathbb{F}_q^{n\times m}$ as the image of an $\mathbb{F}_q$-linear block code under $\phi_{V,W}$. Then

$$\phi_{V,W}^{-1}(\mathcal{C}) := \left\{c \in \mathbb{F}_q^R \mid V\,\mathrm{diag}(c)W^\top \in \mathcal{C}\right\},$$

is an $[R, k]_q$ block code C and in fact we have $C = \psi_{\mathcal{A}}(\mathcal{C})$ where $\mathcal{A} = \{A_r \mid 1 \leq r \leq R\}$ such that $A_r = v_r \otimes w_r$ for each r.

We therefore have, using (6.2) and/or Lemma 6.6, the following rewriting of Theorem 6.4.

Corollary 6.7. *Let $\mathcal{C}$ be an $[n \times m, k, d]_q$ code with tensor rank R. Let $\mathcal{D} = \{D_1, \ldots, D_k\}$ be a k-set of $R \times R$ diagonal matrices such that $\mathcal{C} = V\langle\mathcal{D}\rangle W^\top$ for matrices $V \in \mathbb{F}_q^{n\times R}, W \in \mathbb{F}_q^{m\times R}$ of ranks n, m, respectively. The following hold.*

1. *For every $M \in \mathcal{C}$, $\mathrm{rk}(M) \leq \mathrm{wt}_H(\phi_{V,W}^{-1}(M))$.*
2. *$\phi_{V,W}^{-1}(\mathcal{C})$ is an $[R, k, \geq d]_q$ block code.*
3. *If $\mathcal{C}$ is tensor rank extremal, then the code $\phi_{V,W}^{-1}(\mathcal{C})$ is an $[R, k, d]_q$ code of length $N_q(k, d)$. In particular, if $\mathcal{C}$ is MTR then the code $\phi_{V,W}^{-1}(\mathcal{C})$ is an MDS code.*

We have also obtained a new proof of the tensor-rank bound.

Corollary 6.8 (Tensor-rank bound)**.** *Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ be a rank-metric code. Then*

$$\operatorname{trk}(\mathcal{C}) \geq \dim(\mathcal{C}) + d(\mathcal{C}) - 1. \tag{6.3}$$

6.2 Tensor Rank Extremal Codes

In this section we consider existence questions on tensor rank extremal and MTR codes. Let k, d be positive integers. We wish to determine for which n, $m \in \mathbb{N}$ there exists an $[n \times m, k, d]_q$ code $\mathcal{C}$ of tensor rank $R = N_q(k, d)$ and in particular, those for which $R = k + d - 1$.

Our approach to this problem relies on Corollary 6.7, which gives a way to obtain block codes of minimal length from tensor rank extremal codes and hence MDS codes from MTR codes. A natural problem is to determine in which cases we can do the converse.

Problem 1. *Let n, m be positive integers and let R, k, d be positive integers satisfying $R = N_q(k, d)$. Find an $[R, k, d]_q$ block code C and a pair of matrices $V \in \mathbb{F}_q^{n\times R}, W \in \mathbb{F}_q^{m\times R}$ such that the code $\phi_{V,W}(C)$ is an $[n \times m, k, d]_q$ code with tensor rank R (i.e., is a tensor rank extremal code).*

An interesting special case is given by the following.

Problem 2. *Let n, m be positive integers and let R, k, d be positive integers satisfying $R = k + d - 1$. Find an $[R, k]_q$ MDS code C and a pair of matrices $V \in \mathbb{F}_q^{n\times R}, W \in \mathbb{F}_q^{m\times R}$ such that the code $\phi_{V,W}(C)$ is an $[n \times m, k, d]_q$ code with tensor rank R (i.e. is an MTR code).*

The answer to these problems clearly depends on n and m. Indeed, one immediately observes that both n and m can not be smaller than d. Moreover, we can use the Singleton-like bound of Theorem 2.12 to deduce that n, m have to satisfy

$$k \leq \min\{n(m - d + 1), m(n - d + 1)\}.$$

Definition 6.9. Let C be an $[R, k, d]_q$ block code of length $R = N_q(k, d)$. Let $V \in \mathbb{F}_q^{n\times R}$ and let $W \in \mathbb{F}_q^{m\times R}$. We say that (C, V, W) is an *extremal triple* if it is a solution to Problem 1, i.e. if $\phi_{V,W}(C)$ is a tensor rank extremal code.

With this notation, given positive integers k, d, we wish to determine for which $n, m \in \mathbb{N}$ there exist matrices $V \in \mathbb{F}_q^{n\times R}, W \in \mathbb{F}_q^{m\times R}$ and an $[R = N_q(k, d), k, d]_q$ block code C such that (C, V, W) is an extremal triple. It is clear from the definition that this happens if and only if

$$\operatorname{rk}(V \operatorname{diag}(c) W^\top) \geq d, \tag{6.4}$$

for every $c \in C \setminus \{0\}$.

We fix some further notation. For an arbitrary matrix $Y \in \mathbb{F}_q^{\ell \times R}$ and element $c \in \mathbb{F}_q^R$, we write $C_Y = \mathrm{rowsp}(Y)$ and $C_{Y_c} = \mathrm{rowsp}(Y \operatorname{diag}(c))$. The following result will be useful in addressing this problem.

Lemma 6.10. *Let $V \in \mathbb{F}_q^{n \times R}, W \in \mathbb{F}_q^{m \times R}$ and let $c \in \mathbb{F}_q^R$. Then*

$$\mathrm{rk}(V \operatorname{diag}(c) W^T) = \mathrm{rk}(V) - \dim(C_V \cap C_{W_c}^{\perp}) = \mathrm{rk}(W) - \dim(C_W \cap C_{V_c}^{\perp}).$$

Proof. Suppose first that V and W both have full rank. For any $c \in C$, the rank of $V \operatorname{diag}(c) W^{\top}$ is the rank of the associated bilinear form on

$$\begin{aligned} \varphi : \mathbb{F}_q^n \times \mathbb{F}_q^m &\longrightarrow \mathbb{F}_q \\ (x, y) &\longmapsto xV \operatorname{diag}(c) W^{\top} y^{\top}. \end{aligned}$$

Such a rank is equal to

$$n - \dim \ker_L(\varphi) = m - \dim \ker_R(\varphi),$$

where $\ker_L(\varphi)$ and $\ker_R(\varphi)$ denote the left kernel and the right kernel of φ, respectively. Now, V has full rank, and so $\mathbb{F}_q^n$ and C_V are isomorphic. Therefore,

$$\begin{aligned} \ker_L(\varphi) &= \{x \in \mathbb{F}_q^n \mid xV \operatorname{diag}(c) W^{\top} y^{\top} = 0, \ \forall\, y \in \mathbb{F}_q^m\} \\ &\cong \{v \in C_V \mid v \operatorname{diag}(c) W^{\top} = 0\} \\ &= C_V \cap C_{W_c}^{\perp}. \end{aligned}$$

Similarly, $\ker_R(\varphi) \cong C_W \cap C_{V_c}^{\perp}$. Now consider the case $\mathrm{rk}\, V = s \leq n$ and $\mathrm{rk}\, W = t \leq m$. There exist full rank matrices $A \in \mathbb{F}_q^{s \times R}$ and $B \in \mathbb{F}_q^{t \times R}$ such that AV and BW are full rank matrices with the same row-spaces as V and W, respectively. Then, apply the above argument with AV in place of V and with BW in place of W to complete the proof. □

It is clear that, if for given parameters k, d we have a tensor rank extremal code in $\mathbb{F}_q^{n \times m}$, then we can construct a tensor rank extremal code in a larger ambient space for the same parameters k, d. In terms of extremal triples, we can express this observation as follows.

Lemma 6.11. *Let C be an $[R = N_q(k, d), k, d]_q$ block code. Let $V \in \mathbb{F}_q^{n \times R}$ and $W \in \mathbb{F}_q^{m \times R}$ such that (C, V, W) is an extremal triple. Then for all integers $n' \geq n$, $m' \geq m$ and for all the matrices $V' \in \mathbb{F}_q^{n' \times R}, W' \in \mathbb{F}_q^{m' \times R}$ such that $\mathrm{rowsp}(V) \subseteq \mathrm{rowsp}(V')$ and $\mathrm{rowsp}(W) \subseteq \mathrm{rowsp}(W')$, (C, V', W') is an extremal triple.*

Proof. Let (C, V, W) be an extremal triple. Let $V' \in \mathbb{F}_q^{n' \times R}, W' \in \mathbb{F}_q^{m' \times R}$ such that $\mathrm{rowsp}(V) \subseteq \mathrm{rowsp}(V')$ and $\mathrm{rowsp}(W) \subseteq \mathrm{rowsp}(W')$. Then, there exist $A \in \mathbb{F}_q^{n' \times n'}, B \in \mathbb{F}_q^{m' \times m'}$ such that

$$AV' = \begin{pmatrix} V \\ \tilde{V} \end{pmatrix}, \quad BW' = \begin{pmatrix} W \\ \tilde{W} \end{pmatrix}.$$

for some $\tilde{V} \in \mathbb{F}_q^{(n'-n)\times R}$ and $\tilde{W} \in \mathbb{F}_q^{(m'-m)\times R}$ Therefore, for every $v \in C \setminus \{0\}$

$$\mathrm{rk}(V'D_vW'^\top) = \mathrm{rk}(AV'D_vW'^\top B^\top) = \mathrm{rk}\begin{pmatrix} VD_vW^\top & VD_v\tilde{W}^\top \\ \tilde{V}D_vW^\top & \tilde{V}D_v\tilde{W}^\top \end{pmatrix} \geq \mathrm{rk}(VD_vW^\top) \geq d.$$

□

In particular, this means that in our analysis of Problem 1 we may assume, without loss of generality, that V and W are full rank matrices.

First we observe that in the case that at least one integer among n and m is greater or equal than R, then it is easy to construct an extremal triple. Suppose that $n \geq R$. Let C be an $[R = N_q(k,d), k, d]_q$ block code and let V, W be any full-rank matrices. By Sylvester's inequality, we get that, for every $c \in C \setminus \{0\}$,

$$\mathrm{rk}(V\,\mathrm{diag}(c)W^\top) \geq \mathrm{rk}(V) + \mathrm{rk}(W\,\mathrm{diag}(c)) - R = \mathrm{rk}(W\,\mathrm{diag}(c)).$$

For the case $m \geq R$, all columns of W are linearly independent and so $\mathrm{rk}(W\,\mathrm{diag}(c)) = \mathrm{wt}_H(c) \geq d$. For the case $R < m$, $\mathrm{rk}(W\,\mathrm{diag}(c)) \geq \mathrm{rk}(W) - (R - \mathrm{wt}_H(c)) = \mathrm{wt}_H(c) \geq d$. In either case the inequality of (6.4) is satisfied and clearly holds similarly with the assumption $m \geq R$. It therefore only remains to consider the case $m, n < R$.

Proposition 6.12. *Let C be an $[R = N_q(k,d), k, d]_q$ block code. Let $n, m \in \mathbb{N}$ such that $d \leq n, m < R$ and $V \in \mathbb{F}_q^{n\times R}, W \in \mathbb{F}_q^{m\times R}$. Then, the following are equivalent.*

1. *(C, V, W) is an extremal triple.*
2. *For every $c \in C \setminus \{0\}$, $\dim(C_{V_c}^\perp \cap C_W) \leq \mathrm{rk}(W) - d$.*
3. *For every $c \in C \setminus \{0\}$, $\dim(C_V \cap C_{W_c}^\perp) \leq \mathrm{rk}(V) - d$.*
4. *For every $c \in C \setminus \{0\}$, $\dim(C_{V_c}^\perp + C_W) \geq R - \mathrm{rk}(V) + d$.*
5. *For every $c \in C \setminus \{0\}$, $\dim(C_V + C_{W_c}^\perp) \geq R - \mathrm{rk}(W) + d$.*
6. *For every $c \in C \setminus \{0\}$, $\dim(C_{V_c} + C_W^\perp) \geq R - \mathrm{rk}(W) + d$.*
7. *For every $c \in C \setminus \{0\}$, $\dim(C_V^\perp + C_{W_c}) \geq R - \mathrm{rk}(V) + d$.*
8. *For every $c \in C \setminus \{0\}$, $\dim(C_{V_c} \cap C_W^\perp) \leq \dim(C_{V_c}) - d$.*
9. *For every $c \in C \setminus \{0\}$, $\dim(C_V^\perp \cap C_{W_c}) \leq \dim(C_{W_c}) - d$.*

Proof. As we observed before, $\phi_{V,W}(C)$ has tensor rank at most R and dimension k and so is tensor rank extremal if and only if it has minimum rank distance d. Therefore, from Lemma 6.10, the equivalence of the first three statements is immediate. The equivalences between (2) and (4) and between (3) and (5) are a direct consequence of the dimension formula for the sum of two subspaces, which is $\dim(X+Y)+\dim(X\cap Y)=\dim(X)+\dim(Y)$.

The equivalences between (2) and (6) and between (3) and (7) follow from the fact that $(X\cap Y)^\perp = X^\perp + Y^\perp$ and that $\dim(X^\perp)=R-\dim(X)$, for every X,Y subspaces of $\mathbb{F}_q^R$, while the equivalences between (6) and (8) and between (7) and (9) follow again from the dimension formula for the sum of two subspaces. □

Proposition 6.13. *Let k,d,n,m,R be positive integers satisfying $d\leq n,m<R$ and $R=N_q(k,d)$. Let C be an $[R,k,d]_q$ block code and let $V\in\mathbb{F}_q^{n\times R}, W\in\mathbb{F}_q^{m\times R}$ such that C_V and C_W are MDS codes of dimension n and m, respectively. If $n+m\geq R+d$, then (C,V,W) is an extremal triple.*

Proof. Let $c\in C\setminus\{0\}$, with $\mathrm{wt}_H(v)=w\geq d$. Since C_V and C_W are MDS codes, we have $\mathrm{rk}(V\,\mathrm{diag}(v))=\min\{n,w\}$ and $\mathrm{rk}(\mathrm{diag}(v)W^\top)=\min\{m,w\}$. By the Frobenius rank inequality, we have

$$\mathrm{rk}(V\,\mathrm{diag}(c)W^\top)\geq \mathrm{rk}(V\,\mathrm{diag}(c))+\mathrm{rk}(\mathrm{diag}(c)W^\top)-\mathrm{rk}(\mathrm{diag}(c))=\min\{n,w\}+\min\{m,w\}-w.$$

It is easy to check that in all cases, under the assumption that $m+n\geq R+d$, the right hand side of this inequality is at least d. □

We conclude this part with a particular construction of an extremal triple involving doubly-extended generalized Reed-Solomon codes or Cauchy codes [33, 104], which hence is a partial solution to Problem 2. Before doing this, we briefly recall some notation. For each $s\in\mathbb{N}$, let $\mathbb{F}_q[x,y]_{s-1}$ denote the $\mathbb{F}_q$-space of homogeneous polynomials with degree equal to $s-1$ together with the zero polynomial. Let $\mathbb{P}^1(\mathbb{F}_q)=\mathbb{F}_q\cup\{\infty\}$ denote the projective line over $\mathbb{F}_q$. For any

$$f(x,y)=\sum_{j=0}^{s-1} f_j x^j y^{s-1-j}\in\mathbb{F}_q[x,y]_{s-1}$$

we define the map

$$\begin{array}{rcl} f:\mathbb{P}^1(\mathbb{F}_q) & \longrightarrow & \mathbb{F}_q \\ Q & \longmapsto & f(Q):=\begin{cases} f(Q,1) & \text{if } Q\in\mathbb{F}_q, \\ f(1,0) & \text{if } Q=\infty. \end{cases} \end{array}$$

Let $N\in\mathbb{N}$. For any $\alpha=(\alpha_1,\ldots,\alpha_N)\in(\mathbb{P}^1(\mathbb{F}_q))^N$ define the evaluation map

$$\begin{array}{rcl} \mathrm{ev}_\alpha:\mathbb{F}_q[x,y]_{s-1} & \longrightarrow & \mathbb{F}_q^N \\ f(x,y) & \longmapsto & (f(\alpha_1),\ldots,f(\alpha_N)). \end{array}$$

Definition 6.14 (see [33])**.** Let $1\leq k\leq N-1$ and let $\beta=(\beta_1,\ldots,\beta_N)\in\mathbb{F}_q^N$ and let $\alpha_1,\ldots,\alpha_N$

be pairwise distinct elements of $\mathbb{P}^1(\mathbb{F}_q)$. The *Cauchy code* $C_k(\alpha, \beta)$ is defined to be the set

$$C_k(\alpha,\beta) := \{(\beta_1 f(\alpha_1), \dots, \beta_N f(\alpha_N)) \mid f \in \mathbb{F}_q[x,y]_{k-1}\}.$$

Observe that in our definition we allow the coefficients of β to be zero, while the standard definition requires each $\beta \in (\mathbb{F}_q^*)^N$. In particular, the Cauchy code as defined here is MDS if $\beta \in (\mathbb{F}_q^*)^N$.

Let $*$ denote the *Schur product* (or *Hadamard product*) of two vectors, which is the vector obtained after component-wise multiplication of two vectors of the same length. Then we have the expression

$$C_k(\alpha,\beta) = \{\beta * \mathrm{ev}_\alpha(f) \mid f \in \mathbb{F}_q[x,y]_{k-1}\}.$$

The following result gives a construction of MTR codes of dimension k and minimum rank distance d, provided that $d < k$. We will see later that in the case $d \geq k$ we can always find a construction of MTR codes for every $m, n \geq d$. Therefore, the case analyzed here is the non-trivial one.

Theorem 6.15. *Let $0 < d < k < R$ be positive integers satisfying $R = k + d - 1$ and let $\alpha = (\alpha_1, \dots, \alpha_R) \in (\mathbb{P}^1(\mathbb{F}_q))^R$ be a vector such that the α_i's are pairwise distinct. Let $f(x,y) \in \mathbb{F}_q[x,y]$ be an irreducible homogeneous polynomial of degree k. Let $C = C_k(\alpha, \mathbf{1})$, let $V \in \mathbb{F}_q^{k\times R}$ be a parity check matrix of $C_{R-k}(\alpha, \mathrm{ev}_\alpha(f))$ and let $W \in \mathbb{F}_q^{d\times R}$ be a generator matrix of $C_d(\alpha, \mathbf{1})$. Then (C, V, W) is an extremal triple.*

Proof. In order to prove that (C, V, W) is an extremal triple, we use the characterization given in Proposition 6.12, showing that for every $c \in C \setminus \{0\}$ we have $\dim(C_V^\perp \cap C_{W_c}) \leq \dim(C_{W_c}) - d$. Let $c \in C \setminus \{0\}$. Since C is an MDS code with minimum distance d, then $\mathrm{wt}_H(c) \geq d$. Moreover, the code C_{W_c} is obtained from C_W by multiplying the i-th coordinate of every codeword by c_i, that is, $C_{W_c} = C_d(\alpha, c)$. Since C_W is an MDS code of dimension d, we have $\dim(C_{W_c}) = d$. We therefore need to show that

$$C_V^\perp \cap C_{W_c} = \{0\}.$$

Now $c = \mathrm{ev}_\alpha(g)$ for some non-zero $g(x,y) \in \mathbb{F}_q[x,y]_{k-1}$, and so $C_{W_v} = C_d(\alpha, \mathrm{ev}_\alpha(g))$. Let $b \in C_V^\perp \cap C_{W_c}$. There exist $\mu \in \mathbb{F}_q[x,y]_{R-k-1}$, $\lambda \in \mathbb{F}_q[x,y]_{d-1}$ such that $b = \mathrm{ev}_\alpha(f) * \mathrm{ev}_\alpha(\mu) = \mathrm{ev}_\alpha(g) * \mathrm{ev}_\alpha(\lambda)$, i.e.

$$b_i = f(\alpha_i)\mu(\alpha_i) = g(\alpha_i)\lambda(\alpha_i), \qquad \text{for } i = 1, \dots, R.$$

From the fact that $\deg f\mu < R$ and $\deg g\lambda < R$, we obtain $f\mu = g\lambda$. Therefore, since f is irreducible, f divides g or λ. But $\deg g < k$ and $\deg \lambda < d$. This implies $\lambda = 0$ and $b = 0$. □

Example 6.16. Let $q = 8$, $R = 7$, $k = 5$ and let $d = R - k + 1 = 3$. Let ω be a generator of $\mathbb{F}_8^*$ and let $\alpha = (1, \omega, \dots, \omega^6)$. The polynomial $f(x) = x^5 + x^2 + 1$ is irreducible in $\mathbb{F}_8[x]$. Let C be the $[7,5,3]_8$ Reed-Solomon code $C_5(\alpha,\mathbf{1})$. Let

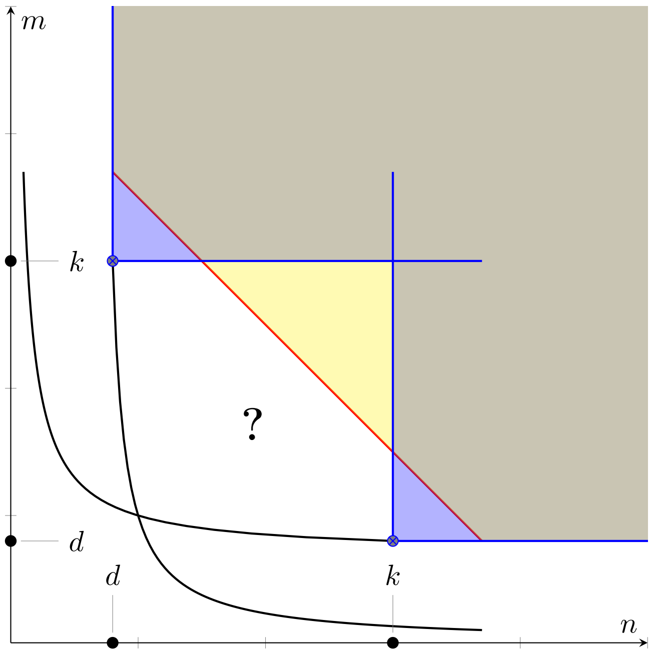
$$V=\begin{bmatrix}1&0&0&0&0&\omega^6&\omega^2\\0&1&0&0&0&\omega^3&\omega^5\\0&0&1&0&0&\omega^6&\omega^3\\0&0&0&1&0&\omega^5&\omega^4\\0&0&0&0&1&\omega^4&\omega^2\end{bmatrix},\qquad W=\begin{bmatrix}1&0&0&\omega^3&\omega&1&\omega^2\\0&1&0&\omega^6&\omega^6&1&\omega^2\\0&0&1&\omega^5&\omega^4&1&\omega^4\end{bmatrix}.$$

V is a parity check matrix of $C_2(\alpha, ev_\alpha(f)) = C_2(\alpha,(1,\omega,\omega^2,\omega^4,\omega^4,\omega^2,\omega))$, and W is a generator matrix of $C_3(\alpha,\mathbf{1})$. It can be checked that for each $c\in C$, we have $C_2(\alpha, ev_\alpha(f))\cap C_3(\alpha,c)=\{0\}$. (C,V,W) is an extremal triple and the rank-metric code $\mathcal{C}=\phi_{V,W}(C)$ is an MTR $[5\times 3,5,3]_8$ code of tensor rank 7 and is in fact MRD.

Remark 6.17. The storage complexity cost of the generator tensor for this class of MTR codes is at most $3kd-2k-d$. This bound is exceeded by the bound on the cost of encoding using a generator matrix as described in Subsection 3.2.1 (which is $k^2(d-1)$) for all $k>d$. The generator tensor encoding cost requires at most $k(d-1)$ multiplications and $(k-1)(d-1)$ additions, while the encoding cost given by a generator matrix requires up to $k^2(d-1)$ multiplications and $(k-1)k(d-1)$ additions.

Remark 6.18. The next figure gives a graphical description of the parameters for which Problem 2 is solved. That is, it represents the parameters for which we do have constructions of MTR codes, the parameters for which we know no MTR codes exist, and the parameters for which the problem is still open. We suppose that $d<k$ are fixed integers, and the axis show increasing n and m (the number of rows and the number of columns of the ambient matrix space). The black hyperbolae represent the Singleton-like bounds, and therefore below them there does not exist any MTR codes. The blue shading represents the construction of MTR codes described in Theorem 6.15 and its transpose. Moreover, by Lemma 6.11, the right-upper quarter-planes having those points as corner points have also a construction of MTR codes. The red line represents the solutions provided by Proposition 6.13, and again by Lemma 6.11; for each point on it, the right-upper quarter-plane starting from it has solution. As we can see, the area in between the Singleton-like bounds, the red line and the two upper-right quarter-planes starting from the blue dots is not solved yet. For this reason, in the following we will investigate codes which are not necessarily MTR, but have “small” tensor rank relative to their dimension and minimum distance.

Existence of MTR Codes



6.2.1 Tensor Rank of Gabidulin Codes

In this subsection, we study the tensor rank of Gabidulin codes. We will give a precise computation of their tensor rank when the dimension of the code over the extension field is 1, and a non-trivial upper bound when this dimension is strictly greater than 1. In order to do this, we recall some well-known results on tensors over finite fields. In the literature, the computation of tensor rank of tensors over finite field was mainly studied for complexity purposes. Indeed, the tensor rank of some special tensors reveals the lowest complexity of some operations, such as multiplication between polynomials or between matrices. The interested reader is referred to [15] for a more complete exposition.

First, we need the following result, which ensures that the tensor rank of a vector code is well defined.

Proposition 6.19. *Let C be an $[n,k]_{q^m}$ code, and let $\Gamma = \{\gamma_1, \dots, \gamma_m\}$, $\Gamma' = \{\gamma'_1, \dots, \gamma'_m\}$ be two bases of $\mathbb{F}_{q^m}/\mathbb{F}_q$. Then* $\mathrm{trk}(\Gamma(C)) = \mathrm{trk}(\Gamma'(C))$.

Proof. By Proposition 2.26, we have that $\Gamma(C)$ and $\Gamma'(C)$ are equivalent codes in $\mathbb{F}_q^{n\times m}$, so the result follows by Proposition 3.15. □

Therefore, by Proposition 6.19, the notion of tensor rank of a vector code is well-defined, and we will denote by $\mathrm{trk}(C)$ the tensor rank of any of its matrix representations.

Let $f \in \mathbb{F}_q[x]$ be a fixed polynomial of degree k. The map

$$\begin{array}{rcl} \mathbb{F}_q[x]_{<m} \times \mathbb{F}_q[x]_{<n} & \longrightarrow & \mathbb{F}_q[x]_{<k} \\ (g,h) & \longmapsto & gh \mod f, \end{array}$$

is clearly bilinear, and so can be represented by a tensor, which we denote by $T_{m,n,k} \in \mathbb{F}_q^{m\times n\times k}$. We have the following result on the tensor rank of $T_{m,n,k}$.

Proposition 6.20 ([15, Propositions 14.47, 14.48])**.** *$T_{m,n,k}$ over $\mathbb{F}_q$ has tensor rank at least $m+n-1$, and has tensor rank exactly $m+n-1$ if and only if $q \geq m+n-2$.*

Lemma 6.21. *Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m, and let $\alpha \in \mathbb{F}_{q^m}$ be a root of f. Let $C = \langle (1,\alpha,\dots,\alpha^{m-1})\rangle_{\mathbb{F}_{q^m}}$ and let $\Gamma = \{1,\alpha,\dots,\alpha^{m-1}\}$. The tensor $T_{m,m,m}$ is the generator tensor of the m-dimensional code $\Gamma(C)$.*

Proof. Let M_f denote the companion matrix of the polynomial f. Then the map $h \mapsto gh \mod f$ has an associated matrix $g(M_f)$ with respect to the basis $\{1,x,\dots,x^{m-1}\}$. Thus,

$$\mathrm{ssp}_1(T_{m,m,m}) = \{g(M_f) \mid g \in \mathbb{F}_q[x]_{<m}\} = \langle I, M_f,\dots,M_f^{m-1}\rangle = \Gamma(C). \qquad \square$$

As an immediate corollary, we have a similar statement for the one-dimensional Gabidulin codes in $\mathbb{F}_{q^m}^n$.

Corollary 6.22. *Let $n \leq m$ be positive integers, and f be an irreducible polynomial of degree m. Then, the tensor $T_{m,n,m}$ is the generator tensor of a one-dimensional Gabidulin code in $\mathbb{F}_{q^m}^n$.*

Proof. Denote by X the matrix associated to the map from $\mathbb{F}_q[x]_{<m}$ to $\mathbb{F}_q[x]_{<n}$ defined by

$$\sum_{i=0}^{m-1} a_i x^i \longmapsto \sum_{i=0}^{n-1} a_i x^i,$$

with respect to the basis $\{1,x,\dots,x^{m-1}\}$ and $\{1,x,\dots,x^{n-1}\}$. Let moreover $\alpha \in \mathbb{F}_{q^m}$ be a root of f. Then it is clear by definition that $\mathrm{ssp}_1(T_{m,n,m}) = \mathrm{ssp}_1(T_{m,m,m})X = \Gamma(C)X$, where C is the one-dimensional Gabidulin code in $(\mathbb{F}_{q^m})^m$ generated by the vector $(1,\alpha,\dots,\alpha^{m-1})$ and $\Gamma := \{1,\alpha,\dots,\alpha^{m-1}\}$. Now, for every $v \in C$ and every $i = 0,\dots,m-1$, $\Gamma(\alpha^i v) \in C$. Therefore, for every $\beta \in \mathbb{F}_{q^m}, v \in C$, we have $\Gamma(\beta v)X \in \Gamma(C)X$, which means that $\Gamma(C)X$ is equivalent to an $\mathbb{F}_{q^m}$-linear code in $\mathbb{F}_{q^m}^n$ of dimension 1. All such codes are Gabidulin codes. □

Using the results above, we give an upper bound on the tensor rank of some special Gabidulin codes.

Proposition 6.23. *Let $n \leq m$ and let $q \geq m+n-2$. For every $K \leq m$, there exists a K-dimensional $\bar{\theta}$-Gabidulin code in $\mathbb{F}_{q^m}^n$ of tensor rank at most $\min\{mn, K(m+n-1)\}$, where $\bar{\theta}$ denotes the q-Frobenius automorphism.*

Proof. It is clear that every code in $\mathbb{F}_{q^m}^n$ has tensor rank at most mn. Choose as a K-dimensional $\bar{\theta}$-Gabidulin code the code $C \subseteq \mathbb{F}_{q^m}^n$ defined as an evaluation code on $g = (1, \gamma, \dots, \gamma^{n-1})$, where γ is a primitive element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Therefore, the code C is the $\mathbb{F}_q$-span of K one-dimensional Gabidulin codes of the form $C_i = \langle(1, \bar{\theta}^i(\gamma), \bar{\theta}^i(\gamma^2), \dots, \bar{\theta}^i(\gamma^{n-1}))\rangle$. For each $i = 1, \dots, K$, consider the basis

$$\Gamma_i = \{1, \bar{\theta}^i(\gamma), \bar{\theta}^i(\gamma^2), \dots, \bar{\theta}^i(\gamma^{n-1})\}.$$

Then, $\Gamma_i(C_i) = \mathrm{ssp}_1(T_{m,n,m})$, which has tensor rank exactly $m + n - 1$ by Proposition 6.20. □

Remark 6.24. The rank of the tensor $T_{m,m,m}$ for $q < 2m - 1$ has been studied in connection with the algebraic complexity of multiplication in $\mathbb{F}_{q^m}$. This problem remains open in general. We refer to [64] for the case $m = 3$, and [7] for bounds in the case $q = 2$.

6.2.2 Codes with Small Tensor Rank

In this subsection we give some constructions of codes with tensor rank bounded by above. In order to do that, we rely on the results given in the previous subsection about the tensor rank of Gabidulin codes. Before proceeding with these constructions, we give an auxiliary lemma.

Lemma 6.25. *Let $\mathcal{C}$ be an $[n \times m, k, d]_q$ code with tensor rank R. Then there exists a subcode $\mathcal{D} \subset \mathcal{C}$ such that* $\dim(\mathcal{D}) = k - 1$, *$d(\mathcal{D}) \geq d$ and* $\mathrm{trk}(\mathcal{D}) \leq R - 1$.

Proof. Let $\mathcal{C}$ be a rank-metric code with tensor rank R, and let $\mathcal{A} = \{A_1, \dots, A_R\}$ be an R-basis for $\mathcal{C}$. Consider the code $C_{\mathcal{A}}$ as defined in Definition 6.3. Without loss of generality, we may assume that $C_{\mathcal{A}}$ is systematic in the first k coordinates and so it has a generator matrix of the form

$$G = (I_k \mid M).$$

Now, let $\tilde{D}$ be the subcode of $C_{\mathcal{A}}$ generated by all but the first row of G. The code

$$\mathcal{D} := \phi_{\mathcal{A}}^{-1}(\tilde{D})$$

clearly has dimension $k - 1$ and minimum distance $\geq d$. Moreover, since $\tilde{D} \subset \langle e_2, \dots, e_R\rangle$, we have $\mathcal{D} \subseteq \langle A_2, \dots, A_R\rangle$. Therefore $\mathrm{trk}(\mathcal{D}) \leq R - 1$. □

Proposition 6.26. *Let k, d, n, m be positive integers with $d \leq n \leq m$ and let $\rho = \min\{s \in \mathbb{N} \mid s(s - d + 1) \geq k\}$. If $\rho \leq n$ then there exists an $[n \times m, k, \geq d]_q$ code $\mathcal{C}$ such that*

$$\mathrm{trk}(\mathcal{C}) \leq k + \min\{\rho(d-1), (\rho - d + 1)(\rho - 1)\},$$

provided that $q \geq 2\rho - 2$.

Proof. Let $K = \rho - d + 1$. There exists a Gabidulin code $C \subseteq \mathbb{F}_{q^\rho}^\rho$ of dimension K, minimum distance d, and by Proposition 6.23, tensor rank at most $\min\{\rho^2, K(2\rho-1)\} = \min\{\rho^2, (\rho - d + 1)(2\rho-1)\}$. Let Γ' be a basis for $\mathbb{F}_{q^\rho}/\mathbb{F}_q$. Then, the code $\Gamma'(C)$ is a $[\rho \times \rho, K\rho, d]_q$ code and can be embedded in $\mathbb{F}_q^{n\times m}$. Applying Lemma 6.25 $K\rho - k$ times, we get an $[n \times m, k, \geq d]_q$ code $\mathcal{C}$ with $\mathrm{trk}(\mathcal{C}) \leq k + \min\{\rho(d-1), (\rho - d + 1)(\rho - 1)\}$. □

We now present a result that uses the same principle of the previous construction, which yields a different upper bound.

Theorem 6.27. *Let k, d, n, m be positive integers with $d \leq n \leq m$, and $k \leq m(n-d+1)$. Then there exists an $[n \times m, k, \geq d]_q$ code $\mathcal{C}$ such that*

$$\mathrm{trk}(\mathcal{C}) \leq k + \min\left\{m(d-1), \left\lceil \frac{k}{m} \right\rceil \left(\left\lceil \frac{k}{m} \right\rceil + d - 2\right)\right\},$$

provided $q \geq m + \lceil \frac{k}{m} \rceil + d - 3$.

Proof. Let $\mu = \min\{s \in \mathbb{N} \mid m(s-d+1) \geq k\} = \lceil \frac{k}{m} \rceil + d - 1$. By hypothesis, $\mu \leq n$. Let $K = \mu - d + 1$. There exists a Gabidulin code $C \subseteq \mathbb{F}_{q^m}^\mu$ of dimension K, minimum distance d and, by Proposition 6.23, tensor rank at most $\min\{m\mu, K(m+\mu-1)\} = \min\{m\mu, (\mu - d + 1)(m + \mu - 1)\}$. Let Γ be a basis for $\mathbb{F}_{q^m}/\mathbb{F}_q$. Then the code $\Gamma(C)$ is a $[\mu \times m, Km, d]_q$ code, which can be embedded in $\mathbb{F}_q^{n\times m}$. Again, we iteratively apply Lemma 6.25 $Km - k$ times to get an $[n \times m, k, \geq d]_q$ code $\mathcal{C}$ such that

$$\begin{aligned}\mathrm{trk}(\mathcal{C}) &\leq \min\{m\mu, (\mu - d + 1)(m + \mu - 1)\} - (\mu - d + 1)m + k \\ &= k + \min\{m(d-1), (\mu - d + 1)(\mu - 1)\} \\ &= k + \min\left\{m(d-1), \left\lceil \frac{k}{m} \right\rceil \left(\left\lceil \frac{k}{m} \right\rceil + d - 2\right)\right\}.\end{aligned}$$

□

Remark 6.28. In Proposition 6.26, the essential idea was to take a Gabidulin code whose elements are representable as square matrices, embed it in $\mathbb{F}_q^{n\times m}$ and iteratively obtain subcodes with decreasing tensor rank. In Theorem 6.27 we applied the same principle, but this time chose a Gabidulin code whose elements are representable as rectangular matrices. In the first case the initial code is a subspace of $\mathbb{F}_q^{\rho\times\rho}$, while in the second the code is a subspace of $\mathbb{F}_q^{\mu\times m}$. We can compare the two bounds in the following way. Clearly $\rho \leq m$ so the first part of the bound of Proposition 6.26 is better than the first part of the bound in Theorem 6.27. For the second parts of these bounds, we get the opposite relation. This can be easily verified since $\lceil \frac{k}{m} \rceil = \mu - d + 1$ and $\mu \leq \rho$.

Remark 6.29. In fact, we stated this result in the most general case, even though we are more interested in those parameters k, d, n, m that are not covered by the constructions of MTR codes given at the beginning of this section. As a consequence of this result, we get the existence of MTR codes for the same parameters as those arising in Theorem 6.15, even though the constructions are quite different.

Corollary 6.30. *Let d, k, n, m be positive integers with $d \leq n \leq m$ and $k \leq m$. Then there exists an $[n \times m, k, d]_q$ MTR code $\mathcal{C}$, provided that $q \geq m + d - 2$*

Proof. If $k \leq m$, then by Theorem 6.27 we get an $[n \times m, k, d]_q$-code $\mathcal{C}$ such that $\mathrm{trk}(\mathcal{C}) \leq k+d-1$ and we deduce the result by the tensor rank bound. □

Remark 6.31. Observe that in Corollary 6.30 we require $q \geq m+d-2$, whereas the construction provided by Theorem 6.15 depends on the existence of a Cauchy code of length $k+d-1$, which we always have for $q \geq k+d-2$.

6.3 Generalized Tensor Ranks of a Code

In the sequel, we denote by $\mathcal{U}$ the set of subspaces of $\mathbb{F}_q^{n \times m}$ that are generated by matrices of rank one.

Definition 6.32. Let $\mathcal{C}$ be an $[n \times m, k]_q$ code with $k \geq 1$, and let $1 \leq r \leq k$ be an integer. The *r-th generalized tensor rank* of C is

$$d_r(\mathcal{C}) = \min\{\dim(U) \mid U \in \mathcal{U},\ \dim(\mathcal{C} \cap U) \geq r\}.$$

It is easy to check that the set of generalized tensor ranks form a code invariant.

Proposition 6.33. *Equivalent codes have the same generalized tensor ranks.*

The next result summarizes the main properties of the generalized ranks and explains the terminology. It also gives a new proof of the tensor rank bound (Corollary 6.8).

Theorem 6.34. *Let $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ be a k-dimensional code with $k \geq 1$. The following hold.*

1. *$d_1(\mathcal{C}) = d(\mathcal{C})$.*
2. *$d_k(\mathcal{C}) = \mathrm{trk}(\mathcal{C})$.*
3. *For all $1 \leq r \leq \min\{k, mn-1\}$ we have $d_r(\mathcal{C}) < d_{r+1}(\mathcal{C})$.*
4. *For all $1 \leq r \leq k$ we have $d_r(\mathcal{C}) \geq d(\mathcal{C}) + r - 1$. In particular, $\mathrm{trk}(\mathcal{C}) \geq d(\mathcal{C}) + k - 1$.*
5. *For all $1 \leq r \leq k$ we have $d_r(\mathcal{C}) \leq \mathrm{trk}(\mathcal{C}) - k + r$.*

Proof. 1. Let $M \in \mathcal{C}$ be a matrix with $d = d(\mathcal{C}) = \mathrm{rk}(M)$. Write $M = M_1 + \cdots + M_d$, where each $M_i \in \mathbb{F}_q^{n \times m}$ has rank one. Then $U = \langle M_1, \ldots, M_d \rangle$ attains the minimum in the definition of $d_1(\mathcal{C})$.

2. This follows from Proposition 3.13.

3. Let $U \in \mathcal{U}$ with $\dim(\mathcal{C} \cap U) \geq r+1$ and $\dim(U) = d_{r+1}(\mathcal{C})$. Let $U' \subseteq U$ be a hyperplane of U with $U' \in \mathcal{U}$. Since $U' + (U \cap \mathcal{C}) \subseteq U$, we have

$$\begin{aligned}
\dim(U' \cap \mathcal{C}) &= \dim(U' \cap (U \cap \mathcal{C})) \\
&= \dim(U') + \dim(U \cap \mathcal{C}) - \dim(U' + (U \cap \mathcal{C})) \\
&\geq \dim(U') + (r+1) - \dim(U) \\
&= \dim(U) - 1 + (r+1) - \dim(U) \\
&= r.
\end{aligned}$$

   By definition, this implies that $d_r(\mathcal{C}) \leq \dim(U') = d_{r+1}(\mathcal{C}) - 1$.

4. This follows combining 1, 2, and 3.

5. This follows from 2 and 3. □

An interesting application of generalized tensor ranks is the distinction of inequivalent codes, as the following example shows.

Example 6.35. Let $q = 2$ and $n = m = 4$. Let $\mathcal{C}_1, \mathcal{C}_2$ be the $[4 \times 4, 4]_2$ codes given by

$$\mathcal{C}_1 := \left\langle \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \right\rangle,$$

$$\mathcal{C}_2 := \left\langle \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} \right\rangle.$$

It can be checked that their generalized tensor ranks are $(4,6,8,9)$ and $(4,6,7,9)$, respectively. In particular, $\mathcal{C}_1$ and $\mathcal{C}_2$ are not equivalent.

A natural question is whether generalized tensor ranks satisfy a duality property analogous to that of generalized rank weights [91, Corollary 38]. More generally, one may ask if the generalized tensor ranks of a code $\mathcal{C}$ determine those of the dual code $\mathcal{C}^\perp$. The answer to this question is negative in general. In the following example, we exhibit two codes that have the same generalized tensor ranks, but whose duals have different generalized tensor ranks.

Example 6.36. Let $q = 2$ and $n = m = 4$. Let $\mathcal{C}_2$ be the $[4\times 4, 4]_2$ code defined in Example 6.35, and let $\mathcal{C}_3$ be the $[4 \times 4, 4]_2$ code defined as

$$\mathcal{C}_3 := \left\langle \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \right\rangle .$$

Then $\mathcal{C}_2$ and $\mathcal{C}_3$ have the same dimension, the same minimum distance, and the same generalized tensor ranks, namely, $(4, 6, 7, 9)$. However, the tensor rank of $\mathcal{C}_2^\perp$ is 14, and that of $\mathcal{C}_3^\perp$ is 13.

Chapter 7

New Invariants for Vector Codes

When looking for new MRD code constructions, it is important to understand if the new codes are equivalent to any of the already known codes. For this reason, it is helpful to have easily computable criteria to check if codes belong to a given family. For Gabidulin codes, such a criterion, based on the dimension of the intersection of the code with itself under some field automorphism, was given in [51] (see Theorem 4.12). In this chapter we generalize this result to more than just one application of the field automorphism, and derive results about the number of equivalence classes of certain MRD codes. The theory developed here partially answers to an open problem given by Zullo in [121, Chapter 6, Section 3], on finding efficient ways for testing code equivalence of rank-metric codes. Motivated by this aim, in this chapter we define invariants of vector codes, which are based on these dimensions. We study deeply the theory and the properties that they possess, and compute them for some classes of known codes. Such theory has also implications in code-based cryptography. This is due to the fact that these invariants serve as distinguishers for retrieving the structure of the rank-metric code used in the McEliece-type cryptosystem. Furthermore, we show how these sequences are helpful to prove other results in the theory of rank metric codes. Indeed, using the tools defined in this chapter, we prove lower and upper bounds on the number of inequivalent Gabidulin codes. In particular, the lower bound that we found, is better than the one proved by Schmidt and Zhou in [101] for some choice of the parameters. In the case when the length n of the code is equal to the degree m of the extension field, we derive the exact number of inequivalent Gabidulin and Twisted Gabidulin codes. Finally, we give a characterization theorem for Gabidulin codes which involves the sequences described in this chapter.

The results contained in this chapter are based on the work in preparation [83] by Neri, Puchinger and Horlemann-Trautmann, which is the extended version of the conference proceedings [82] published by the same authors.

7.1 Known MRD Constructions

Gabidulin codes are not the only known MRD codes. There are some other families of codes which attain the Singleton-like bound of Theorem 2.12, that have been discovered in the last few years. Here we give an overview on some of these families.

Definition 7.1. Let θ be a generator of $G = \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, h be an integer such that $0 \leq h < m$ and $\eta \in \mathbb{F}_{q^m}$. We denote by $\mathcal{H}_{k,\theta}^{\eta,h}$ the $\mathbb{F}_q$-subspace of the group algebra $\mathbb{F}_{q^m}[\theta] = \mathbb{F}_{q^m}[G]$ given by

$$\mathcal{H}_{k,\theta}^{\eta,h} := \left\{ f_0 \mathrm{id} + f_1\theta + \ldots + f_{k-1}\theta^{k-1} + \eta\theta^h(f_0)\theta^k \mid f_i \in \mathbb{F}_{q^m} \right\}.$$

In the language of θ-polynomials, the set $\mathcal{H}_{k,\theta}^{\eta,h}$ corresponds to the set

$$\mathcal{M}_{k,\theta}^{\eta,h} := \left\{ f_0 x + f_1 x^{\theta} + \ldots + f_{k-1}x^{\theta^{k-1}} + \eta\theta^h(f_0)x^{\theta^k} \mid f_i \in \mathbb{F}_{q^m} \right\}.$$

Definition 7.2. Let $g = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ be a vector such that $\mathrm{rk}_q(g) = n$. Let, moreover, $1 \leq k \leq n \leq m$, and $\eta \in \mathbb{F}_{q^m}$ such that $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\eta) \neq (-1)^{km}$. The *$\theta$-twisted Gabidulin code* of parameters η and h is defined as

$$\mathcal{H}_{k,\theta}^{\eta,h}(g) := \left\{ (f(g_1), \ldots, f(g_n)) \mid f \in \mathcal{H}_{k,\theta}^{\eta,h} \right\}.$$

Proposition 7.3. *[106] Let $g \in \mathbb{F}_{q^m}^n$ be a vector such that $\mathrm{rk}_q(g) = n$ and $\eta \in \mathbb{F}_{q^m}$ such that $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\eta) \neq (-1)^{km}$. The θ-twisted Gabidulin code $\mathcal{H}_{k,\theta}^{\eta,h}(g)$ has cardinality q^{km} and minimum distance $d = n - k + 1$, i.e. $\mathcal{H}_{k,\theta}^{\eta,h}(g)$ is an MRD code.*

Remark 7.4. Observe that in general a θ-twisted Gabidulin code is not $\mathbb{F}_{q^m}$-linear, but only $\mathbb{F}_q$-linear. However, we can easily note that it is $\mathbb{F}_{q^m}$-linear if and only if $h = 0$. In such a case, we will denote the set $\mathcal{H}_{k,\theta}^{\eta,0}$ by $\mathcal{H}_{k,\theta}^{\eta}$, and the corresponding code by $\mathcal{H}_{k,\theta}^{\eta}(g)$. Therefore, with the hypothesis of Proposition 7.3, the code $\mathcal{H}_{k,\theta}^{\eta}(g)$ is an $[n, k, n-k+1]_{q^m}$ code, and it is given by

$$\left\langle g + \eta\theta^k(g), \theta(g), \ldots, \theta^{k-1}(g) \right\rangle_{\mathbb{F}_{q^m}}.$$

This family of codes was given by Sheekey in [106], and it was first introduced only considering the q-Frobenius automorphism $\bar{\theta}$. In [106, Remark 9] and [74], it was generalized to any generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Further generalizations were given in [86], where the codes obtained are only linear over the prime field, in [90], where more than one twist is considered and in [38]. We now give an overview on the last two constructions.

From now on we fix the following notation. Let $1 \leq k \leq n \leq m$ be integers. Choose $\ell \in \mathbb{N}$, which we call the *number of twists*. Let $\boldsymbol{h} \in \{0, \ldots, k-1\}^\ell$ and $\boldsymbol{t} \in \{1, \ldots, n-k\}^\ell$ such that the h_i's are distinct and the t_i's are distinct. Furthermore, let $\boldsymbol{\eta} \in (\mathbb{F}_{q^m})^\ell$ and θ be a generator of $G = \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. We denote by $\mathcal{P}_{k,\theta}^{\boldsymbol{\eta},\boldsymbol{t},\boldsymbol{h}}$ the $\mathbb{F}_{q^m}$-subspace of the group algebra $\mathbb{F}_{q^m}[\theta] = \mathbb{F}_{q^m}[G]$

given by

$$\mathcal{P}_{k,\theta}^{\boldsymbol{\eta},\boldsymbol{t},\boldsymbol{h}} := \left\{ f_0 \mathrm{id} + f_1\theta + \ldots + f_{k-1}\theta^{k-1} + \sum_{j=1}^{\ell} \eta_j f_{h_j} \theta^{k-1+t_j} \mid f_i \in \mathbb{F}_{q^m} \right\}.$$

Definition 7.5. With the notation above, let moreover $g \in \mathbb{F}_{q^m}^n$ with $\mathrm{rk}_q(g) = n$. The *generalized θ-twisted Gabidulin code* $\mathcal{P}_{k,\theta}^{\boldsymbol{\eta},\boldsymbol{t},\boldsymbol{h}}(g)$ is defined as

$$\mathcal{P}_{k,\theta}^{\boldsymbol{\eta},\boldsymbol{t},\boldsymbol{h}}(g) := \left\{ (f(g_1), \ldots, f(g_n)) \mid f \in \mathcal{P}_{k,\theta}^{\boldsymbol{\eta},\boldsymbol{t},\boldsymbol{h}} \right\}.$$

Observe that the set $\mathcal{P}_{k,\theta}^{\boldsymbol{\eta},\boldsymbol{t},\boldsymbol{h}}$ corresponds to the subset of θ-polynomials given by

$$\left\{ f_0 x + f_1 x^{\theta} + \ldots + f_{k-1} x^{\theta^{k-1}} + \sum_{j=1}^{\ell} \eta_j f_{h_j} x^{\theta^{k-1+t_j}} \mid f_i \in \mathbb{F}_{q^m} \right\}.$$

Moreover, generalized θ-twisted Gabidulin codes are $\mathbb{F}_{q^m}$-linear by definition. In particular, the code $\mathcal{P}_{k,\theta}^{\boldsymbol{\eta},\boldsymbol{t},\boldsymbol{h}}(g)$ can be written as

$$\left\langle \left\{ \theta^{h_i}(g) + \eta_i \theta^{k-1+t_i}(g) \mid i \in [\ell] \right\} \cup \left\{ \theta^i(g) \mid i \in \{0, \ldots, k-1\} \setminus \{h_1, \ldots, h_\ell\} \right\} \right\rangle_{\mathbb{F}_{q^m}}.$$

In general, there is a sufficient MRD condition if the g_i's are chosen from a subfield $\mathbb{F}_{q^r} \subseteq \mathbb{F}_{q^m}$ with $r2^{\ell} \mid m$ and a suitable choice of the η_i [90] (see also [89, Chapter 7] for more details). Note that this gives codes of length $n \leq 2^{-\ell} m$. It is an open problem whether longer MRD codes exist for arbitrary $\boldsymbol{t}$ and $\boldsymbol{h}$. In the special case $\ell = 1$, we write $t := \boldsymbol{t} = t_1 \in \mathbb{N}$ and $h := \boldsymbol{h} = h_1 \in \mathbb{N}_0$.

Here we give the last construction, due to Gabidulin in [38]. In that paper, he gave a new family of codes, dividing the construction in two cases, which we distinguish in Definitions 7.7 and 7.9.

Definition 7.6. Let $1 \leq k \leq m$ be integers with $m - k > k$, let θ be a generator of $G = \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ and $\eta \in \mathbb{F}_{q^m}$. We denote by $\mathcal{N}_{k,\theta}^{\eta,I}$ the $\mathbb{F}_{q^m}$-subspace of the group algebra $\mathbb{F}_{q^m}[\theta] = \mathbb{F}_{q^m}[G]$ given by

$$\mathcal{N}_{k,\theta}^{\eta,I} := \left\langle \left\{ \theta^i + \theta^i(\eta)\theta^{k+i} \mid i \in \{0, \ldots, k-1\} \right\} \right\rangle_{\mathbb{F}_{q^m}}.$$

Definition 7.7. With the same notation of Definition 7.6, let moreover $g \in \mathbb{F}_{q^m}^n$ with $\mathrm{rk}_q(g) = n$. The *new θ-Gabidulin code of first kind* $\mathcal{N}_{k,\theta}^{\eta,I}(g)$ is defined as

$$\mathcal{N}_{k,\theta}^{\eta,I}(g) := \left\{ (f(g_1), \ldots, f(g_n)) \mid f \in \mathcal{N}_{k,\theta}^{\eta,I} \right\}.$$

Observe that the new θ-Gabidulin codes of first kind can be seen as a special case of generalized θ-twisted Gabidulin codes in the sense of Definition 7.5, with

$$\ell = k, \quad h_i = i-1, \quad t_i = i, \quad \text{and} \quad \eta_i = \theta^{i-1}(\eta)$$

for $i \in [k]$.

Definition 7.8. Let $1 \leq k \leq m$ be integers with $m-k \leq k$, let θ be a generator of $G = \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ and $\eta \in \mathbb{F}_{q^m}$. We denote by $\mathcal{N}_{k,\theta}^{\eta,II}$ the $\mathbb{F}_{q^m}$-subspace of the group algebra $\mathbb{F}_{q^m}[\theta] = \mathbb{F}_{q^m}[G]$ given by

$$\mathcal{N}_{k,\theta}^{\eta,II} := \left\langle \left\{ \theta^i + \theta^i(\eta)\theta^{k+i} \mid i \in \{0,\ldots,m-k-1\} \right\} \cup \left\{ \theta^i \mid m-k \leq i < k \right\} \right\rangle_{\mathbb{F}_{q^m}}.$$

Definition 7.9. With the same notation of Definition 7.8, let moreover $g \in \mathbb{F}_{q^m}^n$ with $\mathrm{rk}_q(g) = n$. The *new θ-Gabidulin code of second kind* $\mathcal{N}_{k,\theta}^{\eta,II}(g)$ is defined as

$$\mathcal{N}_{k,\theta}^{\eta,II}(g) := \left\{ (f(g_1),\ldots,f(g_n)) \mid f \in \mathcal{N}_{k,\theta}^{\eta,II} \right\}.$$

Also the new θ-Gabidulin codes of second kind can be seen as a special case of generalized θ-twisted Gabidulin codes in the sense of Definition 7.5, with

$$\ell = m-k, \quad h_i = i-1, \quad t_i = i, \quad \text{and} \quad \eta_i = \theta^{i-1}(\eta)$$

for $i \in [m-k]$.

Proposition 7.10. *[38] Let $1 \leq k \leq m$ be integers, θ be a generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, $g \in \mathbb{F}_{q^m}^n$ with $\mathrm{rk}_q(g) = n$. Suppose, moreover, that $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\eta) \neq (-1)^{km}$.*

1. *If $m-k > k$, then the new θ-Gabidulin code of first kind $\mathcal{N}_{k,\theta}^{\eta,I}(g)$ is an $[n,k]_{q^m}$ MRD code.*
2. *If $m-k \leq k$, then the new θ-Gabidulin code of second kind $\mathcal{N}_{k,\theta}^{\eta,II}(g)$ is an $[n,k]_{q^m}$ MRD code.*

7.2 Invariants

Let $\theta \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. In recent works, it has been noticed that the dimension of the code $C + \theta(C)$ is an invariant of an $[n,k]_{q^m}$ code C under code equivalences ([51, 89, 23]). In [51], this dimension was used to derive a criterion for checking whether a given code is Gabidulin or not (see Theorem 4.12). In [89], it was used to show that some generalized θ-twisted Gabidulin codes are inequivalent to known constructions. Moreover, in [43], Giuzzi and Zullo considered the dimensions of $C \cap \theta(C)$ and $C \cap \theta(C) \cap \theta^2(C)$, in order to give a distinguisher for twisted Gabidulin codes. We generalize these invariants here.

Lemma 7.11. *1. Let $0 < s_1 < \ldots < s_r < m$ be positive integers, θ be a generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ and let C_1, C_2 be two equivalent $[n,k]_{q^m}$ codes. Then, $\mathcal{S}_1 := C_1 + \theta^{s_1}(C_1) + \ldots + \theta^{s_r}(C_1)$ and $\mathcal{S}_2 := C_2 + \theta^{s_1}(C_2) + \ldots + \theta^{s_r}(C_2)$ are equivalent. In particular, $\dim \mathcal{S}_1 = \dim \mathcal{S}_2$.*

2. Let $0 < t_1 < \ldots < t_r < m$ be positive integers, θ be a generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ and let C_1, C_2 be two equivalent $[n,k]_{q^m}$ codes. Then, $\mathcal{T}_1 := C_1 \cap \theta^{t_1}(C_1) \cap \ldots \cap \theta^{t_r}(C_1)$ is equivalent to $\mathcal{T}_2 := C_2 \cap \theta^{t_1}(C_2) \cap \ldots \cap \theta^{t_r}(C_2)$. In particular, $\dim \mathcal{T}_1 = \dim \mathcal{T}_2$.

Proof. Since C_1 and C_2 are equivalent, there exist $\tau \in \mathrm{Aut}(\mathbb{F}_{q^m})$, $A \in \mathrm{GL}_n(\mathbb{F}_q)$ such that $C_1 = \tau(C_2)A$. Therefore,

$$\begin{aligned} C_1 + \theta^{s_1}(C_1) + \ldots + \theta^{s_r}(C_1) &= \tau(C_2)A + \theta^{s_1}(\tau(C_2))\theta^{s_1}(A) + \ldots + \theta^{s_r}(\tau(C_2))\theta^{s_r}(A) \\ &\overset{(*)}{=} \tau(C_2)A + \tau(\theta^{s_1}(C_2))A + \ldots + \tau(\theta^{s_r}(C_2))A \\ &= \tau(C_2 + \theta^{s_1}(C_2) + \ldots + \theta^{s_r}(C_2))A, \end{aligned}$$

and

$$\begin{aligned} C_1 \cap \theta^{t_1}(C_1) \cap \ldots \cap \theta^{t_r}(C_1) &= \tau(C_2)A \cap \theta^{t_1}(\tau(C_2))\theta^{t_1}(A) \cap \ldots \cap \theta^{t_r}(\tau(C_2))\theta^{t_r}(A) \\ &\overset{(*)}{=} \tau(C_2)A \cap \tau(\theta^{t_1}(C_2))A \cap \ldots \cap \tau(\theta^{t_r}(C_2))A \\ &= \tau(C_2 \cap \theta^{t_1}(C_2) \cap \ldots \cap \theta^{t_r}(C_2))A, \end{aligned}$$

where the equalities $(*)$ follow from the fact that $\mathrm{Aut}(\mathbb{F}_{q^m})$ is a cyclic group, therefore abelian, $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) \subseteq \mathrm{Aut}(\mathbb{F}_{q^m})$ and θ leaves all the elements in $\mathbb{F}_q$ fixed. □

Lemma 7.11 implies that if two $[n,k]_{q^m}$ codes C_1, C_2 have different dimensions of $\mathcal{S}_1$ and $\mathcal{S}_2$ (or of $\mathcal{T}_1$ and $\mathcal{T}_2$), then they must be inequivalent. Hence, checking the dimensions of $\mathcal{S}_1$ and $\mathcal{S}_2$ (or of $\mathcal{T}_1$ and $\mathcal{T}_2$) for different choices of the powers s_i gives a sufficient condition for codes to be inequivalent. It is notable that computing the dimension of $C + \theta^{s_1}(C) + \ldots + \theta^{s_r}(C)$ of a code C with generator matrix G can be done by computing the rank of the $(r+1)k \times n$ matrix $(G^\top, \theta^{s_1}(G)^\top, \ldots, \theta^{s_r}(G)^\top)^\top$, which costs at most $\mathcal{O}(\max\{r^2k^2n, n^2rk\})$ field operations. The dimension of $C \cap \theta^{s_1}(C) \cap \ldots \cap \theta^{s_r}(C)$ can be found by computing the rank of the $(r+1)(n-k) \times n$ matrix $(H^\top, \theta^{t_1}(H)^\top, \ldots, \theta^{t_r}(H)^\top)^\top$, where H is a parity check matrix of C. This costs at most $\mathcal{O}(\max\{r^2(n-k)^2n, n^2(n-k)r\})$ field operations.

In the following, we restrict to the special case of consecutive $s_i = t_i = i$, since in this case, we have additional interesting properties. Motivated by Lemma 7.11, we introduce the following setting and definitions. Let $\mathcal{P}_{q^m}(n)$ denote the set of all $\mathbb{F}_{q^m}$-subspaces of $\mathbb{F}_{q^m}^n$. For any automorphism $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ and integer $0 \le i \le n$, we consider the maps

$$\begin{array}{rccl} \mathcal{S}_i^\sigma: & \mathcal{P}_{q^m}(n) & \longrightarrow & \mathcal{P}_{q^m}(n) \\ & C & \longmapsto & \sum\limits_{j=0}^{i} \sigma^j(C), \end{array}$$

$$\begin{array}{rccl} \mathcal{T}_i^\sigma: & \mathcal{P}_{q^m}(n) & \longrightarrow & \mathcal{P}_{q^m}(n) \\ & C & \longmapsto & \bigcap\limits_{j=0}^{i} \sigma^j(C), \end{array}$$

and the integers

$$\begin{array}{rlrl} s_i^\sigma(C) &:= \dim(\mathcal{S}_i^\sigma(C)), & t_i^\sigma(C) &:= \dim(\mathcal{T}_i^\sigma(C)), \\ \Delta_i^\sigma(C) &:= s_{i+1}^\sigma(C) - s_i^\sigma(C), & \Lambda_i^\sigma(C) &:= t_i^\sigma(C) - t_{i+1}^\sigma(C). \end{array}$$

Definition 7.12. With the notation above:

1. $s_i^\sigma(C)$ is called the *i-th σ-sum-dimension of C*, and $\Delta_i^\sigma(C)$ the *i-th σ-sum-increment of C*.
2. $t_i^\sigma(C)$ is called the *i-th σ-intersection-dimension of C*, and $\Lambda_i^\sigma(C)$ the *i-th σ-intersection-decrease of C*.

As a consequence of Lemma 7.11, we get that the sequences $\{s_i^\sigma(C)\}$, $\{\Delta_i^\sigma(C)\}$, $\{t_i^\sigma(C)\}$ and $\{\Lambda_i^\sigma(C)\}$ are invariants of linear rank metric codes, i.e. they are stable under code equivalence.

A first property that we show is that the maps $\mathcal{S}_i^\sigma$ and $\mathcal{T}_i^\sigma$ are connected by a duality relation, which is explained in the followng result.

Proposition 7.13. *Let C be an $[n,k]_{q^m}$ code. Then $\mathcal{T}_i^\sigma(C)^\perp = \mathcal{S}_i^\sigma(C^\perp)$. In particular, $t_i^\sigma(C) = n - s_i^\sigma(C^\perp)$ and $\Lambda_i^\sigma(C) = \Delta_i^\sigma(C^\perp)$.*

Proof. Since $\sigma(C^\perp) = \sigma(C)^\perp$, we get

$$\mathcal{T}_i^\sigma(C)^\perp = \left(\bigcap_{j=0}^{i} \sigma^j(C)\right)^\perp = \sum_{j=0}^{i} \left(\sigma^j(C)^\perp\right) = \sum_{j=0}^{i} \left(\sigma^j(C^\perp)\right) = \mathcal{S}_i^\sigma(C^\perp).$$

The equalities $t_i^\sigma(C) = n - s_i^\sigma(C^\perp)$ and $\Lambda_i^\sigma(C) = \Delta_i^\sigma(C^\perp)$ immediately follow, using the fact that $\dim(U^\perp) = n - \dim(U)$, for any $U \in \mathcal{P}_{q^m}(n)$. □

Proposition 7.14. *Let $C \subseteq \mathbb{F}_{q^m}^n$ be an $[n,k]_{q^m}$ code. Then:*

1. *$k = s_0^\sigma(C) \le s_1^\sigma(C) \le \ldots \le s_{n-k}^\sigma(C) \le n$.*
2. *$\mathcal{S}_i^\sigma \circ \mathcal{S}_j^\sigma = \mathcal{S}_{i+j}^\sigma$.*
3. *$s_i^\sigma(C) = s_{i+1}^\sigma(C)$ if and only if $\mathcal{S}_i^\sigma(C)$ has a basis of elements in $\mathbb{F}_q^n$.*

4. *If $s_i^\sigma(C) = s_{i+1}^\sigma(C)$ then $s_{i+j}^\sigma(C) = s_i^\sigma(C)$ for all $j \geq 0$.*

5. *$s_{n-k}^\sigma(C) = s_{n-k+j}^\sigma(C)$ for all $j \geq 0$.*

6. *$k \geq \Delta_0^\sigma(C) \geq \Delta_i^\sigma(C) \geq \ldots \geq \Delta_{n-k}^\sigma(C) = 0$.*

Proof. 1. Follows from $\mathcal{S}_i^\sigma(C) \subseteq \mathcal{S}_{i+1}^\sigma(C) \subseteq \mathbb{F}_{q^m}^n$.

2. It holds that $\mathcal{S}_i^\sigma(\mathcal{S}_j^\sigma(C)) = \sum_{\ell=0}^{i} \sigma^\ell(\mathcal{S}_j^\sigma(C)) = \sum_{\ell=0}^{i}\sum_{r=0}^{j} \sigma^{\ell+r}(C) = \sum_{h=0}^{i+j} \sigma^h(C) = \mathcal{S}_{i+j}^\sigma(C)$.

3. Suppose $s_i^\sigma(C) = s_{i+1}^\sigma(C)$, then $\mathcal{S}_i^\sigma(C) = \mathcal{S}_{i+1}^\sigma(C)$, and by part 2, we get $\mathcal{S}_1^\sigma(\mathcal{S}_i^\sigma(C)) = \mathcal{S}_i^\sigma(C)$. This is true if and only if $\sigma(\mathcal{S}_i^\sigma(C)) = \mathcal{S}_i^\sigma(C)$, and we can conclude using [51, Lemma 4.5].

4. $s_i^\sigma(C) = s_{i+1}^\sigma(C)$ implies that $\sigma(\mathcal{S}_i^\sigma(C)) = \mathcal{S}_i^\sigma(C)$, and therefore, $\mathcal{S}_{i+j}^\sigma(C) = \sigma^j(\mathcal{S}_i^\sigma(C)) = \mathcal{S}_i^\sigma(C)$ for all $j \geq 0$.

5. Given an $[n,k]_{q^m}$ code C, let $r^\sigma(C) = \min\{i \mid s_i^\sigma(C) = s_{i+1}^\sigma(C)\}$. If $r^\sigma(C) \leq n-k$, then by part 4 we can conclude. Suppose by contradiction that $r^\sigma(C) > n-k$. Then we get a chain $k = s_0^\sigma(C) < s_1^\sigma(C) < \ldots < s_{n-k}^\sigma(C) < s_{n-k+1}^\sigma(C)$. This implies that $s_i^\sigma(C) \geq k+i$, and in particular $s_{n-k+1}^\sigma(C) \geq k+n-k+1 = n+1$, but this is impossible since $\mathcal{S}_{n-k+1}^\sigma(C) \subseteq \mathbb{F}_{q^m}^n$.

6. First we prove that $\Delta_1^\sigma(C) \leq k$. We have $\mathcal{S}_1^\sigma(C) = C + \sigma(C)$ and thus $s_1^\sigma(C) = \dim(C + \sigma(C)) \leq \dim(C) + \dim(\sigma(C)) = s_0^\sigma(C) + k$. Now, suppose $s_{i+1}^\sigma(C) = s_i^\sigma(C) + \ell$. Then $\dim(\mathcal{S}_i^\sigma(C) + \sigma(\mathcal{S}_i^\sigma(C))) = \dim(\mathcal{S}_i^\sigma(C)) + \ell$. This implies that $\sigma(\mathcal{S}_i^\sigma(C)) = W + U$, where $W \subseteq \mathcal{S}_i^\sigma(C)$, $U \cap \mathcal{S}_i^\sigma(C) = \{0\}$ and $\dim U = \ell$. Hence, $\mathcal{S}_{i+2}^\sigma(C) = \mathcal{S}_1^\sigma(\mathcal{S}_{i+1}^\sigma(C)) = \mathcal{S}_{i+1}^\sigma(C) + \sigma(\mathcal{S}_{i+1}^\sigma(C)) = \mathcal{S}_i^\sigma(C) + U + \sigma(\mathcal{S}_i^\sigma(C)) + \sigma(U)$. However, $U \subseteq \sigma(\mathcal{S}_i^\sigma(C))$, and therefore $\mathcal{S}_{i+2}^\sigma(C) = \mathcal{S}_i^\sigma(C) + \sigma(\mathcal{S}_i^\sigma(C)) + \sigma(U) = \mathcal{S}_{i+1}^\sigma(C) + \sigma(U)$. Since $\dim \sigma(U) = \dim(U) = \ell$, we conclude. □

It is easy to see from the definition and from Proposition 7.14, that the $\Delta_i^\theta(C)$'s and the $s_i^\theta(C)$'s satisfy the following relations:

$$\begin{gathered} \Delta_i^\sigma(C) = s_{i+1}^\sigma(C) - s_i^\sigma(C), \quad s_i^\sigma(C) = k + \textstyle\sum_{j=0}^{i-1} \Delta_j^\sigma(C), \\ s_0^\sigma(C) = k, \quad \Delta_{n-k}^\sigma(C) = 0. \end{gathered} \tag{7.1}$$

Now we state an analogous result for the σ-intersection sequences $\{t_i^\sigma(C)\}$ and $\{\Lambda_i^\sigma(C)\}$ of an $[n,k]_{q^m}$ code C.

Proposition 7.15. *Let $C \subseteq \mathbb{F}_{q^m}^n$ be an $[n,k]_{q^m}$ code. Then:*

1. *$k = t_0^\sigma(C) \geq t_1^\sigma(C) \geq \ldots \geq t_k^\sigma(C) \geq 0$.*

2. *$\mathcal{T}_i^\sigma \circ \mathcal{T}_j^\sigma = \mathcal{T}_{i+j}^\sigma$.*

3. $t_i^\sigma(C) = t_{i+1}^\sigma(C)$ *if and only if* $\mathcal{T}_i^\sigma(C)$ *has a basis of elements in* $\mathbb{F}_q^n$.

4. *If* $t_i^\sigma(C) = t_{i+1}^\sigma(C)$ *then* $t_{i+j}^\sigma(C) = t_i^\sigma(C)$ *for all* $j \geq 0$.

5. $t_k^\sigma(C) = t_{k+j}^\sigma(C)$ *for all* $j \geq 0$.

6. $k \geq \Lambda_0^\sigma(C) \geq \Lambda_1^\sigma(C) \geq \ldots \geq \Lambda_k^\sigma(C) = 0$.

Proof. It directly follows from Proposition 7.14 and the duality result of Proposition 7.13. □

From Proposition 7.15, we also get that the $\Lambda_i^\theta(C)$'s and the $t_i^\theta(C)$'s satisfy the following relations:

$$\begin{gathered}\Lambda_i^\sigma(C) = t_i^\sigma(C) - t_{i+1}^\sigma(C), \quad t_i^\sigma(C) = k - \textstyle\sum_{j=0}^{i-1} \Delta_j^\sigma(C), \\ t_0^\sigma(C) = k, \quad \Lambda_k^\sigma(C) = 0.\end{gathered} \tag{7.2}$$

Remark 7.16. The sequence $\{\mathcal{S}_i^\sigma(C)\}_{i=0}^m$ was already considered in [87], and following works, to retrieve the structure of a Gabidulin code (i.e., the vector g) from an obfuscated generator matrix thereof, which led to an efficient attack on a cryptosystem based on Gabidulin codes. To the best of our knowledge, it has so far not been used to study inequivalences of rank-metric codes.

Proposition 7.17. *Let* C *be an* $[n,k]_{q^m}$ *code. Then:*

1. $t_1^\sigma(C) = 2k - s_1^\sigma(C)$.

2. $\Delta_0^\sigma(C) = \Lambda_0^\sigma(C)$.

Proof.

1. We have $\mathcal{T}_1^\sigma(C) = \mathcal{C} \cap \sigma(C)$ and thus $t_1^\sigma(C) = \dim(C \cap \sigma(C)) = \dim(C) + \dim(\sigma(C)) - s_1^\sigma(C) = 2k - s_1^\sigma(C)$.

2. $\Delta_0^\sigma(C) = s_1^\sigma(C) - s_0^\sigma(C) = s_1^\sigma(C) - k = k - t_1^\sigma(C) = t_0^\sigma(C) - t_1^\sigma(C) = \Lambda_0^\sigma(C)$.

□

In the following subsections, we explicitly compute the sequences $\{s_i^\sigma(C)\}_{i=0}^m$ and $\{t_i^\sigma(C)\}_{i=0}^m$ for θ-Gabidulin and θ-twisted Gabidulin codes. For these families of codes, in the case $n = m$, this implies the exact number of pairwise inequivalent codes in the respective code family. For θ-Gabidulin codes, some lower and upper bounds on this number will be also provided. This will be explained in details in Subsection 7.3.1.

7.2.1 The Sequences for Gabidulin Codes

In the following, we are going to study the properties of the sequences introduced above in the case when the code considered is a Gabidulin code.

Proposition 7.18. *Let* $C := \mathcal{G}_{k,\theta}(g)$ *be a* θ*-Gabidulin code and* $i \in \mathbb{N}$.

1. *If* $0 \le \ell \le k$, *then* $\mathcal{S}_i^{\theta^\ell}(C) = \mathcal{S}_{i\ell}^{\theta}(C) = \mathcal{G}_{k+i\ell,\theta}(g)$ *and* $s_i^{\theta^\ell}(C) = \min\{k+i\ell, n\}$.
2. *If* $m-k \le \ell < m$, *then* $\mathcal{S}_i^{\theta^\ell}(C) = \mathcal{G}_{k+i(m-\ell),\theta^{-1}}(\theta^{k-1}(g))$ *and* $s_i^{\theta^\ell}(C) = \min\{k+i(m-\ell), n\}$.
3. *If* $k < \ell \le n-k$, *then* $s_1^{\theta^\ell}(C) = 2k$.
4. *If* $\ell > k$ *and* $\ell > n-k$, *then* $s_1^{\theta^\ell}(C) \ge k+n-\ell$.
5. *If* $k < m-\ell \le n-k$, *then* $s_1^{\theta^\ell}(C) = 2k$.
6. *If* $m-\ell > k$ *and* $m-\ell > n-k$, *then* $s_1^{\theta^\ell}(C) \ge k+n-m+\ell$.
7. *If* $m = n$, *and* $0 \le \ell \le m-1$, *then* $s_1^{\theta^\ell}(C) = \min\{r, n\}$, *where*

$$r = \begin{cases} k+\ell & \text{if } 0 \le \ell \le k \\ k+m-\ell & \text{if } m-k \le \ell \le m-1 \\ 2k & \text{if } k+1 \le \ell \le m-k-1 \end{cases} .$$

Proof. 1. Let $0 \le \ell \le k$. Then $\mathcal{S}_i^{\theta^\ell}(C) = \langle g, \theta(g), \dots, \theta^{k-1}(g), \theta^k(g), \dots, \theta^{k+i\ell-1}(g)\rangle = \mathcal{G}_{k+i\ell,\theta}(g)$. The computation of $s_i^{\theta^\ell}(C)$ follows from Corollary 1.21.

2. If $m-k \le \ell \le m-1$, then one considers that $\mathcal{G}_{k,\theta}(g) = \mathcal{G}_{k,\theta^{-1}}(\theta^{k-1}(g))$, by Proposition 4.8 and applying $\theta^\ell = (\theta^{-1})^{m-\ell}$, with $0 \le m-\ell \le k$. The computation of $s_i^{\theta^\ell}(C)$ follows again from Corollary 1.21.

3. If $\ell > k$ and $k \le n-\ell$, then $\mathcal{S}_1^{\theta^\ell}(C) = \langle g, \theta(g), \dots, \theta^{k-1}(g), \theta^\ell(g), \dots, \theta^{\ell+k-1}(g)\rangle$ and by Corollary 1.21 it has dimension $2k$.

4. If $\ell > k$ and $k+\ell > n$, then $\mathcal{S}_1^{\theta^\ell}(C) \supseteq \langle g, \theta(g), \dots, \theta^{k-1}(g), \theta^\ell(g), \dots, \theta^{n-1}(g)\rangle$, which has dimension $k+n-\ell$, by Corollary 1.21.

5. The claim follows considering that $\mathcal{G}_{k,\theta}(g) = \mathcal{G}_{k,\theta^{-1}}(\theta^{k-1}(g))$ and $\theta^\ell = (\theta^{-1})^{m-\ell}$ by Proposition 4.8, and using part 3.

6. The claim follows considering that $\mathcal{G}_{k,\theta}(g) = \mathcal{G}_{k,\theta^{-1}}(\theta^{k-1}(g))$ and $\theta^\ell = (\theta^{-1})^{m-\ell}$ by Proposition 4.8, and using part 4.

7. If $0 \le \ell \le k$ or $m-k \le \ell \le m-1$, the claim holds by parts 1 and 2. On the other hand, the case $k+1 \le \ell \le m-k-1$ follows from parts 3 and 5.

□

Proposition 7.19. *Let* $C := \mathcal{G}_{k,\theta}(g)$ *be a* θ*-Gabidulin code and* $i \in \mathbb{N}$.

1. *If* $0 \le \ell \le k$, *then* $\mathcal{T}_i^{\theta^\ell}(C) = \mathcal{T}_{i\ell}^{\theta}(C) = \mathcal{G}_{r,\theta}(\theta^{k-r}(g))$ *and* $t_i^{\theta^\ell}(C) = r$, *where* $r = \max\{k - i\ell, 0\}$.

2. *If $m-k \leq \ell < m$, then $\mathcal{T}_i^{\theta^\ell}(C) = \mathcal{G}_{r,\theta^{-1}}(\theta^{r-1}(g))$ and $s_i^{\theta^\ell}(C) = r$ where $r = \max\{k - i(m-\ell), 0\}$.*

3. *If $k < \ell \leq n-k$, then $t_1^{\theta^\ell}(C) = 0$.*

4. *If $\ell > k$ and $\ell > n-k$, then $t_1^{\theta^\ell}(C) \leq k-n+\ell$.*

5. *If $k < m-\ell \leq n-k$, then $t_1^{\theta^\ell}(C) = 0$.*

6. *If $m-\ell > k$ and $m-\ell > n-k$, then $t_1^{\theta^\ell}(C) \leq k-n+m-\ell$.*

7. *If $m = n$, and $0 \leq \ell \leq m-1$, then $t_1^{\theta^\ell}(C) = \min\{r, n\}$, where*

$$r = \begin{cases} k-\ell & \text{if } 0 \leq \ell \leq k \\ k-m+\ell & \text{if } m-k \leq \ell \leq m-1 \\ 0 & \text{if } k+1 \leq \ell \leq m-k-1 \end{cases}.$$

Proof. 1. It is enough to prove it for $i = 1$, then the claim follows by induction, since $\mathcal{T}_{i+1}^{\theta^\ell} = \mathcal{T}_1^{\theta^\ell} \circ \mathcal{T}_i^{\theta^\ell}$ by part 2 of Proposition 7.15. We have $\mathcal{T}_1^{\theta^\ell}(C) = \langle g, \ldots, \theta^{k-1}(g)\rangle \cap \langle \theta^\ell(g), \ldots, \theta^{k+\ell-1}(g)\rangle \supseteq \langle \theta^\ell(g), \ldots, \theta^{k-1}(g)\rangle$. The equality follows by comparing the dimensions, using part 1 of Proposition 7.17, and part 1 of Proposition 7.14.

2. It follows form part 1, Proposition 4.8, and writing $\theta^\ell = (\theta^{-1})^{m-\ell}$.

3.–7. They follow from part 1 of Proposition 7.17. and parts 3–7 of Proposition 7.14.

□

7.2.2 The Sequences for Twisted Gabidulin Codes

In this subsection we analyze the family of $[n,k]_{q^m}$ twisted Gabidulin codes, i.e. those which are linear over $\mathbb{F}_{q^m}$. We first give some results on θ-twisted Gabidulin codes.

Lemma 7.20. *Let θ be a generator of* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$*, $g \in \mathbb{F}_{q^m}^n$ with $\mathrm{rk}_q(g) = n$, and let $D :=$* $\det(M_{n,\theta}(g))$*. Then there exist $\lambda_0, \ldots, \lambda_{n-1} \in \mathbb{F}_{q^m}^n$ with $\lambda_0 = (-1)^{n-1}\frac{\theta(D)}{D}$ such that*

$$\theta^n(g) = \sum_{i=0}^{n-1} \lambda_i \theta^i(g).$$

Proof. By Corollary 1.21 we have

$$\mathbb{F}_{q^m}^n = \langle g, \theta(g), \ldots, \theta^{n-1}(g)\rangle = \langle \theta(g), \theta^2(g), \ldots, \theta^n(g)\rangle.$$

This means that $\theta^n(g)=\sum_{i=0}^{n-1}\lambda_i\theta^i(g)$, with $\lambda_0\in\mathbb{F}_{q^m}^*$. Moreover, we can compute

$$\begin{aligned}\theta(D)&=\theta(\det(M_{n,\theta}(g)))=\det(\theta(M_{n,\theta}(g)))=\det(M_{n,\theta}(\theta(g)))\\&=\det\begin{pmatrix}\theta(g)\\\theta^2(g)\\\vdots\\\theta^n(g)\end{pmatrix}=\det\begin{pmatrix}\theta(g)\\\theta^2(g)\\\vdots\\\sum_i\lambda_i\theta^i(g)\end{pmatrix}=\sum_{i=0}^{n-1}\lambda_i\det\begin{pmatrix}\theta(g)\\\theta^2(g)\\\vdots\\\theta^i(g)\end{pmatrix}\\&=\lambda_0\det\begin{pmatrix}\theta(g)\\\theta^2(g)\\\vdots\\g\end{pmatrix}=\lambda_0(-1)^{n-1}\det\begin{pmatrix}g\\\theta(g)\\\vdots\\\theta^{n-1}(g)\end{pmatrix}=\lambda_0(-1)^{n-1}D.\end{aligned}$$

Since by Corollary 1.21 $D\neq 0$, we get the desired result. □

Theorem 7.21. *Let k,n,m be positive integers such that $2\leq k\leq n-2$ and $n\leq m$. Let $g\in\mathbb{F}_{q^m}^n$ with $\mathrm{rk}_q(g)=n$, $\eta\in\mathbb{F}_{q^m}^*$ with $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\eta)\neq(-1)^{km}$ and consider the θ-twisted Gabidulin code $C:=\mathcal{H}_{k,\theta}^{\eta}(g)$. Then, for any non-zero $h\in\mathcal{G}_{n-1,\theta}(\theta^{-(n-k-1)}(g))^\perp$, we have $C^\perp=\mathcal{H}_{n-k,\theta}^{\eta'}(h)$, where*

$$\eta'=(-1)^n\eta\frac{\theta^{k-n+1}(D)}{\theta^{k-n}(D)}\frac{\theta^{k-n}(\langle\theta^{n-k}(h);g\rangle)}{\langle\theta^{n-k}(h);g\rangle},$$

and $D:=\det(M_{n,\theta}(g))$. Moreover $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\eta')=(-1)^{nm}\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\eta)$.

Proof. Let $h\in\mathbb{F}_{q^m}^n$ be any non-zero vector in $\mathcal{G}_{n-1,\theta}(\theta^{-(n-k-1)}(g))^\perp$. This means that

$$\langle h;\theta^i(g)\rangle=0,\ \text{for any } k+1-n\leq i\leq k-1. \tag{7.3}$$

Therefore, for any $1\leq i\leq n-k-1$, $0\leq j\leq k$, we have that $\langle\theta^i(h);\theta^j(g)\rangle=\theta^i(\langle h;\theta^{j-i}(g)\rangle)=0$, since $k+1-n\leq j-i\leq k-1$. We only need to check the condition on η' such that $h+\eta'\theta^{n-k}(h)\in C^\perp$. First we get that both h and $\theta^{n-k}(h)$ are orthogonal to $\theta^j(g)$, for $1\leq j\leq k-1$ by (7.3). Finally, we have

$$\begin{aligned}\langle h+\eta'\theta^{n-k}(h);g+\eta\theta^k(g)\rangle&=\langle h;g\rangle+\eta\langle h;\theta^k(g)\rangle+\eta'\langle\theta^{n-k}(h);g\rangle+\eta\eta'\langle\theta^{n-k}(h);\theta^k(g)\rangle\\&=0+\eta\langle h;\theta^k(g)\rangle+\eta'\langle\theta^{n-k}(h);g\rangle+0.\end{aligned}$$

We observe that $\langle\theta^{n-k}(h);\theta^k(g)\rangle\neq 0$, otherwise we would have h orthogonal to a basis of $\mathbb{F}_{q^m}^n$.

Hence, $h+\eta'\theta^{n-k}(h)\in C^\perp$ if and only if

$$\begin{aligned}\eta' &= -\eta\frac{\langle h;\theta^k(g)\rangle}{\langle\theta^{n-k}(h);g\rangle}\\ &= -\eta\frac{\theta^{k-n}(\langle\theta^{n-k}(h);\theta^n(g)\rangle)}{\langle\theta^{n-k}(h);g\rangle}\\ &= -\eta\frac{\theta^{k-n}(\sum_{i=0}^{n-1}\lambda_i\langle\theta^{n-k}(h);\theta^i(g))}{\langle\theta^{n-k}(h);g\rangle}\\ &= -\eta\frac{\theta^{k-n}(\lambda_0\langle\theta^{n-k}(h);g\rangle}{\langle\theta^{n-k}(h);g\rangle}\\ &= (-1)^n\eta\frac{\theta^{k-n+1}(D)}{\theta^{k-n}(D)}\frac{\theta^{k-n}(\langle\theta^{n-k}(h);g\rangle)}{\langle\theta^{n-k}(h);g\rangle},\end{aligned}$$

where the last three equalities follow from Lemma 7.20, and (7.3). The computation of the norm derives from Lemma 1.16. □

Let F be the set of generators of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. We denote by $\mathrm{TGab}_q(k,n,m,\theta)$ the set of all $[n,k]_{q^m}$ θ-twisted Gabidulin codes, and by $\mathrm{TGab}_q(k,n,m)$ the set of all $[n,k]_{q^m}$ twisted Gabidulin codes i.e.

$$\begin{aligned}\mathrm{TGab}_q(k,n,m,\theta) := \big\{\mathcal{U}\in\mathrm{Gr}(k,\mathbb{F}_{q^m}^n)\mid \mathcal{U}=\mathcal{H}_{k,\theta}^{\eta}(g) \text{ for some } \eta\in\mathbb{F}_{q^m}^* \text{ and } g\in\mathbb{F}_{q^m}^n\\ \text{with } \mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\eta)\neq(-1)^{km} \text{ and } \mathrm{rk}_q(g)=n\big\},\end{aligned}$$

$$\begin{aligned}\mathrm{TGab}_q(k,n,m) :&= \big\{\mathcal{U}\in\mathrm{Gr}(k,\mathbb{F}_{q^m}^n)\mid \mathcal{U} \text{ is a } \theta\text{-twisted Gabidulin code for some } \theta\in F\big\}\\ &=\bigcup_{\theta\in F}\mathrm{TGab}_q(k,n,m,\theta).\end{aligned}$$

As for θ-Gabidulin codes, one can find the exact number of θ-twisted Gabidulin codes for given θ generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$.

Theorem 7.22. *Let $u,v\in\mathbb{F}_{q^m}^n$ be two vectors such that $\mathrm{rk}_q(u)=\mathrm{rk}_q(v)=n$. Then, for any θ generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ and $\eta,\eta'\in\mathbb{F}_{q^m}^*$, $\mathcal{H}_{k,\theta}^{\eta}(u)=\mathcal{H}_{k,\theta}^{\eta'}(v)$ if and only if there exists $\lambda\in\mathbb{F}_{q^m}^*$ such that $u=\lambda v$ and $\eta'=\eta\frac{\theta^k(\lambda)}{\lambda}$.*

Proof. We divide the proof in three cases.

Case $3\le k\le\frac{n}{2}$: Suppose that $C:=\mathcal{H}_{k,\theta}^{\eta}(u)=\mathcal{H}_{k,\theta}^{\eta'}(v)$. Then $\theta(u)$ can be written as

$$\theta(u)=\sum_{i=1}^{k-1}\lambda_i\theta^i(v)+\lambda_k(v+\eta'\theta^k(v)),$$

for some $\lambda_i\in\mathbb{F}_{q^m}$ not all zeros. Let $r:=\max\{i\in[k]\mid\lambda_i\neq0\}$. If $r=k$, then we would have $\theta(\theta(u))=\theta(\lambda_k(v+\eta'\theta^k(v)))+\theta(\sum_{i=1}^{k-1}\lambda_i\theta^i(v))\in C$, but this is not possible, since we would have

$C = \langle v + \eta'\theta^k(v), \theta(v), \dots, \theta^{k-1}(v), \theta^{k+1}(v) + \mu\theta^k(v)\rangle$, for some $\mu \in \mathbb{F}_{q^m}$, which has dimension $k+1$ by Corollary 1.21. Then $r < k$. Suppose that $r > 1$, then $0 < k-r < k$ and $\theta^{k-r}(\theta(u)) \in C$, and we obtain

$$\theta^{k-r}(\theta(u)) = \sum_{i=1}^{r} \theta^{k-r}(\lambda_i)\theta^{k-r+i}(v) \in C.$$

Also in this case, we obtain $C = \langle v, \theta(v), \dots, \theta^{k-1}(v), \theta^k(v)\rangle$, which has dimension $k+1$ by Corollary 1.21. Hence the only possibility is $r = 1$, i.e. $\theta(u) = \lambda_1\theta(v)$, or equivalently, $u = \lambda v$ for some $\lambda \in \mathbb{F}_{q^m}^*$. It remains to study the conditions on η and η'. At this point we have $C = \langle v + \eta'\theta^k(v), \theta(v), \dots, \theta^{k-1}(v)\rangle = \langle \lambda v + \eta\theta^k(\lambda)\theta^k(v), \theta(v), \dots, \theta^{k-1}(v)\rangle$. Therefore, $v + \eta'\theta^k(v) = \mu\lambda v + \mu\eta\theta^k(\lambda)\theta^k(v) + \sum_{i=1}^{k-1}\mu_i\theta^i(v)$, for some $\mu, \mu_i \in \mathbb{F}_{q^m}$, which we can rewrite as

$$(1-\mu\lambda)v - \sum_{i=1}^{k-1}\mu_i\theta^i(v) + (\eta' - \mu\eta\theta^k(\lambda))\theta^k(v) = 0.$$

By Corollary 1.21, $v, \theta(v), \dots, \theta^k(v)$ are linearly independent (since obviously $k < n$), hence $\mu_i = 0$ for every $i \in [k-1]$, $\mu = \lambda^{-1}$ and $\eta' = \frac{\theta^k(\lambda)}{\lambda}\eta$.

Case $k = 2$: Suppose $C = \langle u + \eta\theta^2(u), \theta(u)\rangle = \langle v + \eta'\theta^2(v), \theta(v)\rangle$. Then $\theta(u)$ can be written as linear combination of $v + \eta'\theta^2(v), \theta(v)$, i.e. $\theta(u) = \lambda_1\theta(v) + \lambda_2 v + \lambda_2\eta'\theta^2(v)$. Then one can write

$$\begin{aligned} u + \eta\theta^2(u) =& \theta^{-1}(\lambda_2)\theta^{-1}(v) + \theta^{-1}(\lambda_1)v + (\theta(\lambda_2) + \theta^{-1}(\lambda_2)\theta^{-1}(\eta'))\theta(v) + \\ & \theta(\lambda_1)\theta^2(v) + \theta(\lambda_2)\theta(\eta')\theta^3(v). \end{aligned}$$

By Corollary 1.21 we deduce that $\lambda_2 = 0$, and therefore, $\theta(u) = \lambda_1\theta(v)$, or equivalently, $u = \lambda v$ for some $\lambda \in \mathbb{F}_{q^m}^*$. The relation between η and η' is derived in the same way as done in the proof of the case $3 \le k \le \frac{n}{2}$.

Case $k > \frac{n}{2}$: It follows by the duality result in Theorem 7.21, and the cases $k = 2$ and $3 \le k \le \frac{n}{2}$. □

Corollary 7.23. *Let k, n, m be integers such that $2 \le k \le n-2$ and $n \le m$, and let θ be a generator of* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. *Then,*

$$|\,\mathrm{TGab}_q(k,n,m,\theta)| = \left(1 - \frac{1}{q-1}\right)\prod_{i=0}^{n-1}(q^m - q^i),$$

Proof. We have exactly $\prod_{i=0}^{n-1}(q^m - q^i)$ many choices for the vector g and $(q^m-1) - \frac{q^m-1}{q-1}$ choices for the element η with norm different from $(-1)^{km}$. By Theorem 7.22, the total number has to be divided by the number of non-zero multiple of g, which is $q^m - 1$. □

The following result is a straightforward computation.

Proposition 7.24. *Let θ be a generator of the Galois group $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ and $g \in \mathbb{F}_{q^m}^n$ such that $\mathrm{rk}_q(g)$, and $\eta \in \mathbb{F}_{q^m}^*$. Then $\mathcal{H}_{k,\theta}^{\eta}(g) = \mathcal{H}_{k,\theta^{-1}}^{\eta^{-1}}(\theta^k(g))$.*

Corollary 7.25. *Let k, n, m be integers such that $2 \leq k \leq n-2$ and $n \leq m$. Then,*

$$|\,\mathrm{TGab}_q(k,n,m)| \leq \frac{\phi(m)}{2}\left(1 - \frac{1}{q-1}\right)\prod_{i=0}^{n-1}(q^m - q^i).$$

Proof. It directly follows from Corollary 7.23 and Proposition 7.24. □

Proposition 7.26. *Let $g \in \mathbb{F}_{q^m}^n$ with $\mathrm{rk}_q(g) = n$, and $C := \mathcal{H}_{k,\theta}^{\eta}(g)$ be a θ-twisted Gabidulin code, where $\eta \in \mathbb{F}_{q^m}^*$ with $N(\eta) \neq (-1)^{km}$.*

1. *If $1 \leq \ell \leq k-1$, then $\mathcal{S}_i^{\theta^\ell}(C) = \mathcal{G}_{k+i\ell+1,\theta}(g)$ and $s_i^{\theta^\ell}(C) = \min\{k+i\ell+1, n\}$.*
2. *If $m-k+1 \leq \ell < m$, then $\mathcal{S}_i^{\theta^\ell}(C) = \mathcal{G}_{k+i(m-\ell)+1,\theta^{-1}}(\theta^k(g))$ and $s_i^{\theta^\ell}(C) = \min\{k+i(m-\ell)+1, n\}$.*
3. *If $k \leq \ell \leq n-k-1$, then $s_1^{\theta^\ell}(C) = 2k$.*
4. *If $\ell \geq k$ and $\ell > n-k-1$, then $s_1^{\theta^\ell}(C) \geq k+n-\ell-1$.*
5. *If $k \leq m-\ell \leq n-k-1$, then $s_1^{\theta^\ell}(C) = 2k$.*
6. *If $m-\ell \geq k$ and $m-\ell > n-k-1$, then $s_1^{\theta^\ell}(C) \geq k+n-m+\ell-1$.*
7. *If $m = n$, and $1 \leq \ell \leq m-1$, then $s_1^{\theta^\ell}(C) = \min\{r, m\}$, where*

$$r = \begin{cases} k+\ell+1 & \text{if } 1 \leq \ell \leq k-1 \\ k+m-\ell+1 & \text{if } m-k+1 \leq \ell \leq m-1 \\ 2k & \text{if } k \leq \ell \leq m-k \end{cases}.$$

Proof.

1. Let $1 \leq \ell \leq k-1$ and $i = 1$. Then,

$$\mathcal{S}_1^{\theta^\ell}(C) = \langle g + \eta\theta^k(g), \ldots, \theta^{k-1}(g), \theta^\ell(g) + \theta^\ell(\eta)\theta^{k+\ell}(g), \theta^{\ell+1}(g), \ldots, \theta^{k+\ell-1}(g)\rangle,$$

which is contained in $\mathcal{G}_{k+\ell+1,\theta}(g)$. Moreover, we have that $\mathcal{S}_1^{\theta^\ell}(C) \supseteq \{\theta(g), \ldots, \theta^{\ell+k-1}(g)\}$. Furthermore, it contains $g + \eta\theta^k(g)$ and $\theta^\ell(g) + \theta^\ell(\eta)\theta^{k+\ell}(g)$. Since $1 \leq \ell \leq k-1$, then it contains $\theta^k(g)$, and $\theta^\ell(g)$, and therefore $g, \theta^{k+\ell}(g) \in \mathcal{S}_1^{\theta^\ell}(C)$, and we deduce $\mathcal{S}_1^{\theta^\ell}(C) = \mathcal{G}_{k+\ell+1,\theta}(g)$. If $i > 1$, by part 2 of Proposition 7.14, we have $\mathcal{S}_i^{\theta^\ell}(C) = \mathcal{S}_{i-1}^{\theta^\ell}(\mathcal{S}_1^{\theta^\ell}(C))$, and we conclude using part 1 of Proposition 7.18.

2. Observe that $\mathcal{H}_{k,\theta}^{\eta}(g) = \mathcal{H}_{k,\theta^{-1}}^{\eta^{-1}}(\theta^k(g))$ by Proposition 7.24, and that $\theta^\ell = (\theta^{-1})^{m-\ell}$, with $1 \leq m-\ell \leq k-1$. Then, the claim follows from part 1.

3. If $\ell \geq k$ and $k \leq n-\ell-1$, then

$$\mathcal{S}_1^{\theta^\ell}(C) = \langle g+\eta\theta^k(g), \theta(g) \dots, \theta^{k-1}(g), \theta^\ell(g) + \theta^\ell(\eta)\theta^{\ell+k}(g), \theta^{\ell+1}(g), \dots, \theta^{\ell+k-1}(g)\rangle$$

   and by Corollary 1.21 it has dimension $2k$.

4. If $\ell > k$ and $k+\ell > n-1$, then

$$\mathcal{S}_1^{\theta^\ell}(C) \supseteq \langle g+\eta\theta^k(g), \dots, \theta^{k-1}(g), \theta^{\ell+1}(g), \dots, \theta^{n-1}(g)\rangle,$$

   which has dimension $k+n-\ell-1$, by Corollary 1.21.

5. The claim follows considering that by Proposition 7.24 $\mathcal{H}^{\eta}_{k,\theta}(g) = \mathcal{H}^{\eta^{-1}}_{k,\theta^{-1}}(\theta^k(g))$, $\theta^\ell = (\theta^{-1})^{m-\ell}$, and using part 3.

6. The claim follows considering that by Proposition 7.24, $\mathcal{H}^{\eta}_{k,\theta}(g) = \mathcal{H}^{\eta^{-1}}_{k,\theta^{-1}}(\theta^k(g))$, $\theta^\ell = (\theta^{-1})^{m-\ell}$, and using part 4.

7. If $0 \leq \ell \leq k$ or $m-k \leq \ell \leq m-1$, the claim holds by parts 1 and 2. The case $k \leq \ell \leq m-k$ follows from parts 3 and 5.

□

7.3 Applications

7.3.1 Number of Inequivalent Codes

In this section we use the results above in order to determine upper and lower bounds on the number of inequivalent Gabidulin and twisted Gabidulin codes.

In order to do that, for any code C, we need to give an estimate of the number of automorphisms σ for which C is a σ-Gabidulin code. Since $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) \cong (\mathbb{Z}/m\mathbb{Z})$ and the set of generators is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*$, we introduce the following notation. For a code C we define the set

$$A_C := \{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) \mid C \text{ is a } \sigma\text{-Gabidulin code }\}.$$

If we fix a generator θ of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, the set A_C corresponds to the set

$$A_{C,\theta} := \left\{\ell \in (\mathbb{Z}/m\mathbb{Z})^* \mid C \text{ is a } \theta^\ell\text{-Gabidulin code }\right\}.$$

In the rest of this subsection, the use of both the sets $(\mathbb{Z}/m\mathbb{Z})$ and $(\mathbb{Z}/m\mathbb{Z})^*$ is motivated as follows. The notion of θ-Gabidulin codes requires θ to be a generator of the Galois group, while the set $(\mathbb{Z}/m\mathbb{Z})$ will be used for counting reasons in the proofs of Lemma 7.27 and Theorem 7.28. We now state the following auxiliary result.

Lemma 7.27. *Let $3 \leq k \leq n-3$ be integers and θ be a generator of* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. *Let moreover C be a θ-Gabidulin code.*

1. *$A_{C,\theta} \cap \{2, \dots, n-2\} = \emptyset$.*
2. *If $r \in A_{C,\theta}$ for some integer $r \in (\mathbb{Z}/m\mathbb{Z})^*$, then $A_{C,\theta} \cap \{r+3, r+4. \dots, r+n-3\} = \emptyset$.*
3. *If $r \in A_{C,\theta}$ for some integer $r \in (\mathbb{Z}/m\mathbb{Z})^*$, then $|A_{C,\theta} \cap \{r+1, r+2, r+n-2\}| \leq 1$.*
4. *For any $r \in \mathbb{Z}/m\mathbb{Z}$, $|A_{C,\theta} \cap \{r, r+1, \dots, r+n-2\}| \leq 2$.*

Proof. Let $g \in \mathbb{F}_{q^m}^n$ with $\mathrm{rk}_q(g) = n$ be such that $C = \mathcal{G}_{k,\theta}(g)$.

1. Let $\ell \in \{2, \dots, n-2\}$. By parts 1, 3 and 4 of Proposition 7.18, $s_1^{\theta^\ell}(C) \geq k+2$, so C can not be a θ^ℓ-Gabidulin code.

2. Suppose $r \in A_{C,\theta}$. By definition and by Theorem 4.12, $s_1^{\theta^r}(C) = k+1$. Suppose that $s_1^{\theta^{r+i}}(C) = k+1$ for some $i \in \{3, 4, \dots, n-3\}$. Then $\dim(C + \theta^r(C) + \theta^{r+i}(C)) \leq k+2$. In particular, $s_1^{\theta^i}(\theta^r(C)) \leq k+2$, which is not possible for $i \in \{3, 4. \dots, n-3\}$, by Proposition 7.18, since $\theta^r(C)$ is a θ-Gabidulin code.

3. Suppose $r+1, r+n-2 \in A_{C,\theta}$. Then, $\dim(C + \theta^{r+1}(C) + \theta^{r+n-2}(C)) \leq k+2$. This implies that $s_1^{\theta^{n-3}}(\theta^{r+1}(C)) \leq k+2$, which is not possible by part 4 of Proposition 7.18. The same argument shows that $r+2$ and $r+n-2$ can not belong simultaneously to $A_{C,\theta}$. It remains to show that $r+1$ and $r+2$ can not belong to $A_{C,\theta}$ at the same time. Suppose that this instead holds. Therefore, we have $s_1^{\theta^r}(C) = s_1^{\theta^{r+1}}(C) = s_1^{\theta^{r+2}}(C)$. Consider the space $\mathcal{U} := \langle g, \theta(g), \dots, \theta^{k-1}(g), \theta^{r+2}(g), \dots, \theta^{r+k-1}(g) \rangle$. Thus, $C \subseteq \mathcal{U} \subseteq \mathcal{S}_1^{\theta^r}(C) \cap \mathcal{S}_1^{\theta^{r+1}}(C) \cap \mathcal{S}_1^{\theta^{r+2}}(C)$. Then, $\dim(\mathcal{U})$ can only be equal to k or $k+1$.

   If $\dim(\mathcal{U}) = k+1$, then $\mathcal{S}_1^{\theta^r}(C) = \mathcal{S}_1^{\theta^{r+1}}(C) = \mathcal{S}_1^{\theta^{r+2}}(C)$, and $\mathcal{S}_1^{\theta^r}(C) + \mathcal{S}_1^{\theta^{r+1}}(C) + \mathcal{S}_1^{\theta^{r+2}}(C) = C + \mathcal{S}_2^{\theta}(\theta^r(C))$ has dimension $k+1$, which is impossible, since $s_2^\theta(\theta^r(C)) = k+2$.

   If $\dim(\mathcal{U}) = k$, then $\theta^{r+2}(g), \dots, \theta^{r+k-1}(g) \in \langle g, \dots, \theta^{k-1}(g) \rangle$. Hence, we can write $\theta^{r+2}(g) = \sum_{i=0}^{k-1} \lambda_i \theta^i(g)$, for some $\lambda_i \in \mathbb{F}_{q^m}$. Imposing also $\theta^{r+2+i}(g) \in \langle g, \dots, \theta^{k-1}(g) \rangle$, for every $i \in \{0, \dots, k-3\}$, we get that necessarily $\theta^{r+2}(g) \in \langle g, \theta(g), \theta^2(g) \rangle$. However, C is a θ^{r+2}-Gabidulin code, so $s_1^{\theta^{r+2}}(C) = k+1$. This implies $\lambda_2 = 0$ and $\lambda_1 \neq 0$. At the same time, we can write $\theta^r(g) = \mu_0 \theta^{m-2}(g) + \mu_1 \theta^{m-1}(g)$, where $\mu_i = \theta^{-2}(\lambda_i)$ for $i \in \{0, 1\}$. By assumption, C is θ^r-Gabidulin, therefore $s_1^{\theta^r}(C) = k+1$. This implies that necessarily $\mu_0 = 0 = \lambda_0$ and $\mu_1 \neq 0$. Therefore, $\theta^{r+2}(g) = \lambda_1 \theta(g)$. However, this contradicts the fact that C is a θ^{r+1}-Gabidulin code, since in this case we have $s_1^{\theta^{r+1}}(C) = k$.

4. It follows directly from the previous parts.

□

Theorem 7.28. *Let k, n, m be integers with $2 < k < n-2$ and $n \leq m$. Then*

$$|\operatorname{Gab}_q(k,n,m)| \geq \frac{\phi(m)}{\lfloor \frac{2m}{n-1} \rfloor} \prod_{i=1}^{n-1}(q^m - q^i).$$

Proof. First we provide an upper bound on the cardinality of the set $A_{C,\theta}$, where C is a θ-Gabidulin code, using a double counting argument. Consider the number

$$\sum_{r \in \mathbb{Z}/m\mathbb{Z}} |A_{C,\theta} \cap \{r, r+1, \dots, r+n-2\}|.$$

On one hand, by Lemma 7.27, we have that it is upper-bounded by $2m$. On the other hand, every $\ell \in A_{C,\theta}$ is counted exactly $n-1$ times. Therefore we get

$$(n-1)|A_{C,\theta}| = \sum_{r \in \mathbb{Z}/m\mathbb{Z}} |A_{C,\theta} \cap \{r, r+1, \dots, r+n-2\}| \leq 2m,$$

from which we deduce that $|A_{C,\theta}| \leq \lfloor \frac{2m}{n-1} \rfloor$. At this point, combining this upper bound with Corollary 4.7, we get the desired lower bound, since every θ-Gabidulin code C is counted at most $|A_{C,\theta}|$ times. □

Moreover, for $1 \leq k < n \leq m$ we define $N_q(k,n,m)$ as the number of inequivalent $[n,k]_{q^m}$ Gabidulin codes, i.e.

$$N_q(k,n,m) := |\operatorname{Gab}_q(k,n,m)/\sim_v|.$$

Theorem 7.29. *Let $\mathbb{F}_q$ be a finite field of characteristic p and $2 < k < n-2$ be integers.*

1. *If $m = n$, then*
$$N_q(k,m,m) = \frac{\phi(m)}{2}.$$

2. *If $m > n$, then*
$$\frac{(n-1)\phi(m)}{2m^2[\mathbb{F}_q : \mathbb{F}_p]} \prod_{i=2}^{n} \frac{q^{m-i+1}-1}{q^i - 1} \leq N_q(k,m,n) \leq \frac{\phi(m)}{2} \prod_{i=2}^{n} \frac{q^{m-i+1}-1}{q^i-1}.$$

Proof. 1. Let σ_1, σ_2 be two generators of $\operatorname{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, and $g, h \in \mathbb{F}_{q^m}^m$ be two vectors such that $\operatorname{rk}_q(g) = \operatorname{rk}_q(h) = m$. Consider two Gabidulin codes $C = \mathcal{G}_{k,\sigma_1}(g)$ and $C' = \mathcal{G}_{k,\sigma_2}(h)$. First we show that if $\sigma_1 = \sigma_2$ then $C \sim C'$. Since $n = m$ then $\operatorname{supp}_q(g) = \operatorname{supp}_q(h)$. Therefore, there exists $A \in \mathrm{GL}_m(q)$ such that $gA = h$. This implies that $C \cdot A = C'$ and therefore, $C \sim C'$. Now, suppose that $\sigma_1 = \sigma_2^{-1}$. Then, by the previous argument, we can assume $g = h$. Since by Proposition 4.8, $\mathcal{G}_{k,\sigma_2^{-1}}(h) = \mathcal{G}_{k,\sigma_2}(\sigma_2^{1-k}(h))$, we obtain again $C \sim C'$. Finally, if $\sigma_1 \notin \{\sigma_2, \sigma_2^{-1}\}$, then $\sigma_1 = \sigma_2^{\ell}$, with $\ell \notin \{1, -1\}$, and by part 7 of Proposition 7.18, we have $s_1^{\sigma_1}(C') = k+1$ and $s_1^{\sigma_2}(C) \geq k+2$. By Lemma 7.11 we deduce that they cannot be equivalent. Since there are exactly $\phi(m)$ generators for $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, we conclude.

2. By Corollary 4.9, we have that there are at most $\frac{\phi(m)}{2}\prod_{i=1}^{n-1}(q^m-q^i)$ many Gabidulin codes. Moreover, consider the action

$$\begin{array}{rcl} \mathrm{GL}_n(q)\times \mathrm{Gab}_q(k,n,m) & \longrightarrow & \mathrm{Gab}_q(k,n,m) \\ (A,\mathcal{G}_{k,\theta}(g)) & \longmapsto & \mathcal{G}_{k,\theta}(g)\cdot A := \mathcal{G}_{k,\theta}(gA). \end{array} \tag{7.4}$$

We have that, by Theorem 4.6, $\mathcal{G}_{k,\theta}(g)\cdot A=\mathcal{G}_{k,\theta}(g)$, if and only if $gA=\lambda g$, for some $\lambda\in\mathbb{F}_{q^m}^*$. Since $g=(g_1,\dots,,g_n)$ is such that the g_i's are $\mathbb{F}_q$-linearly independent, it easily follows that $gA=\lambda g$ if and only if $A=\lambda I_n$. Therefore, the action defined in (7.4) induces a free action of $\mathrm{GL}_n(q)/\mathbb{F}_q^*$, with the same orbits. Since this action is free, and every orbit is contained in an equivalence class, we have that

$$N_q(k,m,n)\leq |\,\mathrm{Gab}_q(k,n,m)|\frac{|\mathbb{F}_q^*|}{|\,\mathrm{GL}_n(q)|}=\frac{\phi(m)}{2}\prod_{i=2}^{n}\frac{q^{m-i+1}-1}{q^i-1}.$$

We now prove the lower bound. By Theorem 7.28, we have at least $\frac{\phi(m)}{\lfloor\frac{2m}{n-1}\rfloor}\prod_{i=1}^{n-1}(q^m-q^i)$ many distinct Gabidulin codes. Considering again the action in (7.4), we get that the number of orbits under that action, is at least

$$\frac{\phi(m)}{\lfloor\frac{2m}{n-1}\rfloor}\prod_{i=1}^{n-1}\frac{q^{m-i}-1}{q^{i+1}-1}.$$

If we now consider the equivalence classes of Gabidulin codes, it remains to study the action of the subgroup $\mathrm{Aut}(\mathbb{F}_{q^m})$, which has cardinality exactly $m[\mathbb{F}_q:\mathbb{F}_p]$. Therefore, an equivalence class can be union of at most $m[\mathbb{F}_q:\mathbb{F}_p]$ orbits of the action (7.4), which leads to the desired result.

□

The first part of Theorem 7.29 already appeared in [82, Theorem 1], and the generalization is part of [83]. It provides the exact number of inequivalent Gabidulin codes in the case $n=m$. Moreover, for the general case $n<m$, it provides both an upper and a lower bound on this number. It is important to observe that, whenever $(n-1)\phi(m)>2m[\mathbb{F}_q:\mathbb{F}_p]$, the lower bound is better than the one given in Theorem 4.10, due to Schmidt and Zhou [101].

For a prime power q, and two integers k,m we consider the set $X_q(m,k):=\{\alpha\in\mathbb{F}_{q^m}\mid \mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)\neq(-1)^{km}\}$, and the left group action

$$\begin{array}{rcl} \mathrm{Aut}(\mathbb{F}_{q^m})\times X_q(m,k) & \longrightarrow & X_q(m,k) \\ (\tau,\alpha) & \longmapsto & \tau(\alpha). \end{array} \tag{7.5}$$

Observe that the one above is well-defined. Indeed, if $\alpha \in X_q(m,k)$, and $\tau \in \mathrm{Aut}(\mathbb{F}_{q^m})$, then

$$\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\tau(\alpha)) = \prod_{i=0}^{m-1} \theta^i(\tau(\alpha)) = \prod_{i=0}^{m-1} \tau(\theta^i(\alpha)) = \tau(\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)).$$

Since $(-1)^{km}$ belongs to the prime field, and therefore is fixed by any automorphism $\tau \in \mathrm{Aut}(\mathbb{F}_{q^m})$, we have that also $\tau(\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)) \neq (-1)^{km}$. We denote by $\mathcal{X}_q(m,k)$ the cardinality of the set of orbits of this group action. Moreover, we denote by $R_q(k,n,m)$ the number of inequivalent twisted Gabidulin codes, that is

$$R_q(k,n,m) := \left|\mathrm{TGab}_q(k,n,m)/\sim_v\right|.$$

Theorem 7.30. *[82, Theorem 2] Let $\mathbb{F}_q$ be a finite field of characteristic p and $2 < k < n-2$ be integers. If $m = n$, then*

$$R_q(k,m,m) = \mathcal{X}_q(m,k)\frac{\phi(m)}{2}.$$

Proof. The proof is similar to the one of part 1 of Theorem 7.29. Let σ_1, σ_2 be two generators of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, and $g, h \in \mathbb{F}_{q^m}^m$ be two vectors such that $\mathrm{rk}_q(g) = \mathrm{rk}_q(h) = n$, and let $\eta, \eta' \in \mathbb{F}_{q^m}$ with norm not equal to $(-1)^{km}$. Consider two twisted Gabidulin codes $C = \mathcal{H}^{\eta}_{k,\sigma_1}(g)$ and $C' = \mathcal{H}^{\eta'}_{k,\sigma_2}(h)$. Suppose $\sigma_1 \notin \{\sigma_2, \sigma_2^{-1}\}$, then $\sigma_1 = \sigma_2^{\ell}$, with $\ell \notin \{1,-1\}$, and by part 3 of Proposition 7.26, we have $s_1^{\sigma_1}(C') = k+2$ and $s_1^{\sigma_1}(C) \geq k+3$. By Lemma 7.11 we conclude that they cannot be equivalent. Now, recall that $C \sim C'$ if and only if there exist $\tau \in \mathrm{Aut}(\mathbb{F}_{q^m})$ and $A \in \mathrm{GL}_n(q)$ such that $C' = \tau(C)A$. When $C = \mathcal{H}^{\eta}_{k,\sigma_2}(g)$ we get $\tau(C)A = \mathcal{H}^{\tau(\eta)}_{k,\sigma_2}(\tau(g))$. Assume $\eta' = \tau(\eta)$ for some $\tau \in \mathrm{Aut}(\mathbb{F}_{q^m})$. If $\sigma_2 = \sigma_1$ then, $\mathbb{F}_{q^m}^m = \mathrm{supp}_q(\tau(g)) = \mathrm{supp}_q(h)$. This implies that there exists $A \in \mathrm{GL}_m(q)$ such that $\tau(g)A = h$ and $\tau(C)A = C'$. Hence, for every σ_2 generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, and for every representative η in an orbit of the action defined in (7.5), we have exactly one equivalent class of twisted Gabidulin codes. Moreover, observe that $\mathcal{H}^{\eta}_{k,\sigma_2^{-1}}(g) = \mathcal{H}^{\eta^{-1}}_{k,\sigma_2}(\sigma_2^{-k}(h))$, by Proposition 7.24. This shows that C and C' are equivalent if and only if $\sigma_2 = \sigma_1$ and $\eta = \tau(\eta')$ for some $\tau \in \mathrm{Aut}(\mathbb{F}_{q^m})$ or $\sigma_1 = \sigma_2^{-1}$ and $\eta^{-1} = \tau(\eta')$ for some $\tau \in \mathrm{Aut}(\mathbb{F}_{q^m})$. By counting, we get exactly $\frac{\phi(m)}{2}\mathcal{X}_q(m,k)$ inequivalent twisted Gabidulin codes. □

Theorem 7.30 gives the exact number of inequivalent twisted Gabidulin codes in the case $n = m$. For $n < m$, lower and upper bounds similar to the ones given in Theorem 7.29, could be also developed, with analogous techniques. This would require an estimate on the cardinality of the set of generators σ of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ for which a given code is σ-twisted Gabidulin, together with the use of Theorem 7.22.

7.3.2 Characterization Results

In this subsection we study the θ-sequences, in order to derive characterization results of some families of codes. Unfortunately, concerning the sequence $\{s_i^\sigma(C)\}$, we have “asymptotically bad news”. This is explained by the following result.

Proposition 7.31. *[23, Proposition 2] If C is an $[n,k]_{q^m}$ code chosen at random and uniformly among all the possible $[n,k]_{q^m}$ codes, then for any nonnegative integer b and for a positive integer $i<k$, we have*

$$\Pr\{s_i^\theta(C) \leq \min\{n,(i+1)k\} - b\} = \mathcal{O}(q^{-mb}),$$

for $m \to +\infty$.

However, this happens only when m is quite big. In particular, one can expect that codes which have no maximal dimension (usually) have good algebraic structures. Moreover, restricting to consider MRD codes and the case $n=m$ has a different effect. An idea of this different behaviour is explained by the following result due to Payne in 1971. The original result is formulated in a completely different way, since it was determined in the framework of hyperovals and linearized o-polynomials. See [20] for more details.

Theorem 7.32. *[88] Let C be an $[n,2]_{2^n}$ MRD code. Then, there exists θ generator of* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ *such that $s_i^\theta(C) = 2+i$ for every $i \in \{0,\dots,n-2\}$.*

In common language, Theorem 7.32 states that all the $[n,2]_{2^n}$ MRD codes are Gabidulin codes. We state now two conjectures, which represent a generalization of Theorem 7.32.

Conjecture 1. *Let C be an $[n,3]_{2^n}$ MRD code.Then, there exists θ generator of* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, *such that $s_i^\theta(C) = 3+i$ for every $i \in [n-3]$. Equivalently, all the $[n,3]_{2^n}$ MRD codes are Gabidulin codes.*

Conjecture 2. *Let C be an $[n,k]_{2^n}$ MRD code. Then, there exists θ generator of* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, *such that $s_i^\theta(C) = k+i$ for every $i \in [n-k]$. Equivalently, all the $[n,k]_{2^n}$ MRD codes are Gabidulin codes.*

Now we are going to use the sequences for characterizing Gabidulin codes. The following result follows from [43, Lemma 3.5], but we are going to include a proof for completeness, which uses the tools developed in this chapter.

Lemma 7.33. *Let $0<k<n\leq m$ be integers, C be an $[n,k]_{q^m}$ code, and θ be a generator of* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. *If $s_1^\theta(C) = k+1$, then there exists $g \in \mathbb{F}_{q^m}^n$, $0 \leq t \leq k$ such that*

$$C := C_1 \oplus \mathcal{G}_{t,\theta}(g),$$

where C_1 is an $[n,k-t]_{q^m}$ code which has a basis of rank 1 vectors, and $\mathrm{rk}_q(g) > t$.

Proof. Let $U_1 = \{v \in \mathbb{F}_{q^m}^n \mid \mathrm{rk}_q(v) = 1\}$. Then we can write $C = C_1 \oplus C'$, where $C_1 = \langle C \cap U_1 \rangle$. Hence $C' \cap U_1 = \emptyset$. In particular, if $\dim(C_1) = k - t$, then C' is an $[n, t, d]_{q^m}$ code with $d > 1$. Moreover, $C + \theta(C) = C_1 \oplus (C' + \theta(C'))$. Therefore, without loss of generality, we can assume $C_1 = \{0\}$, and the minimum distance of C greater than 1.

We proceed by induction on k. For $k = 1$ it is trivially true. Suppose now that $k \geq 2$ and that the statement is true for $k - 1$; we want to prove the lemma for an $[n, k]_{q^m}$ code C. By hypothesis, $s_1^\theta(C) = k + 1$, then $t_1^\theta(C) = k - 1$, by Proposition 7.17. Consider the code $D := C \cap \theta(C) = \mathcal{T}_1^\theta(C)$. This code has dimension $k - 1$. Moreover, $D \cap U_1 = \emptyset$, and

$$k - 2 \geq t_2^\theta(C) = t_1^\theta(C) - \Lambda_1^\theta(C) \geq t_1^\theta(C) - \Lambda_0^\theta(C) = k - 1.$$

However, observe that $t_1^\theta(D) = t_2^\theta(C)$. Therefore, if $t_2^\theta(C) = k - 1$, then $t_1^\theta(D) = t_0^\theta(D)$, which implies, by part 3 of Proposition 7.15, that D has a basis of elements in $\mathbb{F}_q^n$, or, equivalently, that $D = \langle D \cap U_1 \rangle$. Since $k - 1 > 0$, $D \subseteq C$ and $C \cap U_1 = \emptyset$, which is a contradiction. Hence, we necessarily have that $t_1^\theta(D) = t_2^\theta(C) = k - 2$. Thus, by inductive hypothesis, $D = \mathcal{G}_{k-1}(h)$, for some $h \in \mathbb{F}_{q^m}^n$ with $\mathrm{rk}_q(h) \geq k$. Moreover, $\theta^{-1}(h) \in \theta^{-1}(D) = \theta^{-1}(C) \cap C \subseteq C$. Therefore, $C \supseteq \langle \theta^{-1}(h), h, \ldots, \theta^{k-2}(h) \rangle$. Since $\mathrm{rk}_q(h) \geq k$, by Corollary 1.21 we get $C = \mathcal{G}_{k,\theta}(g)$, where $g := \theta^{-1}(h)$. We only need to show that $\mathrm{rk}_q(g) > k$. Suppose $\mathrm{rk}_q(g) = k$, and let $\{f_1, \ldots, f_k\}$ be a basis for $\mathrm{supp}_q(g)$. Then, there exists $A \in \mathrm{GL}_n(q)$ such that $gA = (f_1, \ldots, f_k, 0, \ldots, 0)$. Moreover, the code $C \cdot A = \mathcal{G}_{k,\theta}(gA) \sim C$ and has the same parameters. It is easy to see that this code has generator matrix $(I_k \mid 0)$, since the last $n - k$ entries of the code $C \cdot A$ are all zeros. This implies that $C \cdot A$ has (a basis of) codewords of rank 1, which yields a contradiction. Hence, $\mathrm{rk}_q(g) > k$ and this concludes the proof. □

Remark 7.34. Observe that in Lemma 7.33, the notation $\mathcal{G}_{k,\theta}(g)$ is used to indicate the code $\{(f(g_1), \ldots, f(g_n)) \mid f \in \mathcal{G}_{k,\theta}\}$, which is not necessarily a θ-Gabidulin code, since $\mathrm{rk}_q(g)$ can be smaller than n. Moreover, we have that $C_1 = \{0\}$ if and only if the minimum distance of C is strictly greater than 1.

From Lemma 7.33 we can derive a new criterion for characterizing a Gabidulin code. In order to put all the criteria together, we state a very general characterization theorem which includes also Theorem 4.12 and Theorem 4.25.

Theorem 7.35 (Characterization of θ-Gabidulin codes)**.** *Let C be an $[n, k, d]_{q^m}$ code with $d > 1$ and let θ be a generator of* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$*. The following are equivalent:*

1. *C is a θ-Gabidulin code.*
2. *C is MRD and $s_1^\theta(C) = k + 1$.*
3. $(s_i^\theta(C))_{i=0}^{n-k} = (k, k + 1, \ldots, n)$.
4. $(\Delta_i^\theta(C))_{i=0}^{n-k} = (1, 1, \ldots, 1, 0)$.

5. $s_1^\theta(C) = k+1$ *and* $s_{n-k}^\theta(C) = n$.

6. $\Delta_0^\theta(C) = \Delta_{n-k-1}^\theta(C) = 1$.

7. $C = \mathrm{rowsp}(I_k \mid X)$, *where:*
   (a) $\mathrm{rk}(\theta(X) - X) = 1$,
   (b) *the q-rank of the first row of* $\theta(X) - X$ *is* $n-k$,
   (c) *the q-rank of the first column of* $\theta(X) - X$ *is* k.

Proof. The equivalence between 1, 2 and 7 follows from Theorems 4.12 and 4.25. It is also clear that 3 implies 5, and 4 implies 6. Moreover, by part 1 of Proposition 7.18, 1 implies 3.

The equivalence between 3 and 4 follows from the definition. Indeed the s_i^θ's and the Δ_i^θ's are related by (7.1)

If $\Delta_{n-k-1}^\theta(C) = \Delta_0^\theta(C) = 1$, by Proposition 7.14, we have $1 = \Delta_0^\theta(C) \geq \ldots \geq \Delta_{n-k-1}^\theta(C) = 1$, hence we have all equalities. Tihs shows the equivalence between 4 and 6.

Moreover, if $s_1^\theta(C) = k+1$, and $s_{n-k}^\theta(C) = n$, then $\Delta_0^\theta(C) = s_1^\theta(C) - k = 1$, and by (7.1), we have

$$n = s_{n-k}^\theta(C) = k + \sum_{i=0}^{n-k-1} \Delta_i^\theta(C) \leq k + \sum_{i=0}^{n-k-1} \Delta_0^\theta(C) = k + (n-k).$$

Therefore, $\Delta_i^\theta(C) = 1$, for every $i = 0, \ldots, n-k-1$, and we get that 5 implies 4.

Now, suppose that 5 holds. Since $s_1^\theta(C) = 1$, then, by Lemma 7.33 and the fact that $d > 1$, we have that $C = \mathcal{G}_{k,\theta}(g)$, where $\mathrm{rk}_q(g) > k$. Moreover, $\mathcal{S}_{n-k}^\theta(C) = \mathcal{G}_{n,\theta}(g)$. By hypothesis, we also have that $n = s_{n-k}^\theta(C) = \dim(\mathcal{G}_{n,\theta}(g))$. However, by Corollary 1.21, $\dim(\mathcal{G}_{n,\theta}(g)) = \mathrm{rk}_q(g)$. Therefore, C is a θ-Gabidulin code. This concludes the proof

□

After this characterization result, we conclude the chapter by proving that Gabidulin's new codes of Definitions 7.7 and 7.9 are actually the classical Gabidulin codes, whenever they are MRD.

Theorem 7.36. *Let* $1 \leq k \leq m$ *be integers and* θ *be a generator of* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. *Let, moreover,* $\eta \in \mathbb{F}_{q^m}$ *with* $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\eta) \neq (-1)^{km}$, *and* $g \in \mathbb{F}_{q^m}^n$ *be such that* $\mathrm{rk}_q(g) = n$.

1. *If* $m - k > k$, *then the code* $C := \mathcal{N}_{k,\theta}^{\eta,I}(g)$ *is a* θ*-Gabidulin code.*

2. *If* $m \leq k$, *then the code* $D := \mathcal{N}_{k,\theta}^{\eta,II}(g)$ *is a* θ*-Gabidulin code.*

Proof.

1. It is immediate to observe that $C = \mathcal{G}_{k,\theta}(h)$, where $h = g + \eta\theta^k(g)$. Then, since by Proposition 7.10 C is MRD, we conclude using part 2 of the characterization result in Theorem 7.35.

2. By Proposition 7.10, we know that D is MRD. Moreover, if we compute $\mathcal{S}_1^\theta(D)$ we get that $\theta(D)$ is generated by

- $\theta^i(g) + \theta^i(\eta)\theta^{k+i}(g)$ for $1 \leq i < m - k$, which are already contained in D,
- $\theta^i(g)$ for $m - k < i \leq k$, which includes a new, linearly independent, vector $\theta^k(g)$, and
- $\theta^{m-k}(g) + \theta^{m-k}(\eta)\theta^m(g) = \theta^{m-k}(g) + \theta^{m-k}(\eta)g$, which is a linear combination of $\theta^{m-k}(g)$ (which is in D), $\theta^k(g)$ (which is in $\theta(D)$), and $g + \theta^k(\eta)\theta^k(g)$ (which is in D).

Hence, their sum, $\mathcal{S}_1^\theta(D)$ has dimension $k + 1$. We conclude using part 2 of the characterization result in Theorem 7.35.

□

Chapter 8

Further Applications

Rank-metric codes can be seen as spaces of matrices or spaces of vectors over an extension field. In both the frameworks described, rank-metric codes have been shown to have many interesting applications. Roth was the first to use them for crisscross error correction in [96]. Then, Silva, Kschischang and Kötter proposed a scheme that uses rank-metric codes for error correction in network coding [58, 111, 109]. After those groundbreaking papers, many researchers, not only from the coding theory community, focused their attention on rank-metric codes. More recently, many other applications have been investigated, such as in distributed storage systems [108], construction and decoding of space-time codes [39, 13, 70], and low-rank matrix recovery [35, 78]. However, one of the most appealing and important research directions is oriented towards code-based cryptography. Indeed, in the last few years, rank-metric codes seem to represent one of the most promising tools in post-quantum cryptography. Since the introduction of the GPT cryptosystem developed by Gabidulin, Paramonov and Tretjakov in [40], that was attacked by Gibson in [41, 42], many researchers tried to repair it and further attacks have been developed [37, 87, 71, 52]. Few variants of code-based cryptosystems based on rank-metric codes are considered safe at the moment [72, 117], and two of them [94, 99] made it for the second round of the NIST Post-Quantum Standardization Cryptography call [85].

In this chapter we will present two applications of rank-metric codes. The first concerns fuzzy authentication, which deals with the problem of authentication using approximate matching under a certain metric of similarity, while still enabling a secure storage of sensible authentication data. The typical, but not the only scenario, where such a system is needed, is in the use of biometric features, like fingerprints, for authentication purposes.

The second application which we focus on is related to partial MDS (PMDS) codes, a special class of locally repairable codes, used for distributed storage system.

8.1 Fuzzy Authentication

The results of this section were published by Neri, Rosenthal and Schipani in [84].

In 1999, Juels and Wattenberg [56] proposed a fuzzy commitment scheme to allow fuzzy authentication with secure storage of biometric data in binary form. In [100], Schipani and Rosenthal revisited the scheme in the setting of an arbitrary finite field by focusing on implementations and security concerns. In [6], Baldi et al. proposed a dual version of the scheme, called fuzzy syndrome hashing, featuring some advantages in terms of security and use of iterative decoding. Moreover, in [34], Fontein et al. presented scenarios involving burst error correction and higher dimensional data.

Here, we are going to describe a new fuzzy commitment scheme using the rank metric. In Subsection 8.1.3, we will describe a few scenarios where this scheme can be applied.

In our authentication model, we wish to consider two vectors $b, b' \in \mathbb{F}_{q^m}^n$ (or, equivalently, their matrix representations $\Gamma(b), \Gamma(b') \in \mathbb{F}_q^{m\times n}$) as belonging to the same person or entity as long as their rank distance is less than a certain predetermined threshold. And, for security concerns, we do not want to store vectors (or matrices) unencrypted.

Suppose now that we have a vector rank-metric code $C \subseteq \mathbb{F}_{q^m}^n$ whose minimum distance is $d = 2t+1$ and assume that there exists an efficient algorithm for decoding up to t errors.

Let $h : \mathbb{F}_q^{m\times n} \to \mathbb{F}_q^{m\times r}$ be a collision resistant hash function, i.e. such that it is not feasible to compute an $u \in h^{-1}(v)$ for any $v \in \mathbb{F}_q^{m\times r}$. Observe that a hash function $h' : \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}^r$ can be defined starting from h, as the diagram

$$\begin{tikzcd}
\mathbb{F}_q^{m\times n} \arrow[r, "h"] \arrow[d, leftrightarrow] & \mathbb{F}_q^{m\times r} \arrow[d, leftrightarrow] \\
\mathbb{F}_{q^m}^n \arrow[r, dotted, "h'"] & \mathbb{F}_{q^m}^r
\end{tikzcd}$$

shows.

As in the standard fuzzy commitment scheme, we select at random a codeword $c_b \in C$ and we store the tuple

$$(l, h(c_b))$$

where $l = b - c_b$.

This scheme is essentially the analogue of the standard fuzzy commitment with the difference that we use rank-metric codes instead of codes in the Hamming metric. Analogously to [100, Theorem 1], one can show the following result.

Theorem 8.1. *If $b \in \mathbb{F}_{q^m}^n$ can be chosen uniformly over the entire ambient space $\mathbb{F}_{q^m}^n$, then computing $b \in \mathbb{F}_{q^m}^n$ from the stored data $(l, h(c_b))$ is computationally equivalent to invert the 'restricted' hash function*

$$h_{|C} : C \longrightarrow \mathbb{F}_{q^m}^r.$$

8.1.1 A Linearized Polynomial Fuzzy Vault Scheme

The polynomial fuzzy vault (PFV) scheme was introduced in [55] and allows fuzzy authentication in the set-difference metric. In [76] the authors proposed a fuzzy vault scheme using codes in another metric, relating the set difference with the subspace distance on the set of Grassmannians. The PFV scheme can also be generalized in a natural way using linearized polynomials and codes endowed with the rank metric as follows.

First, we make the following assumption about the set of features used for authentication, both the set initially used to build the vault and the one submitted later for authentication.

Assumption 1. *Assume that the set of features (A or W in the following) is given by n $\mathbb{F}_q$-linearly independent elements in $\mathbb{F}_{q^n}$, i.e. it is an $\mathbb{F}_q$-basis for $\mathbb{F}_{q^n}$.*

This is usually not a restrictive assumption given the follwing result:

Lemma 8.2. *If the features are chosen with uniform distribution, then Assumption 1 is satisfied with probability*

$$\prod_{i=0}^{n-1} \frac{(q^n - q^i)}{(q^n - i)} \geq \prod_{i=0}^{n-1} (1 - q^{i-n}).$$

Proof. The number of $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$ is $\frac{\prod_{i=0}^{n-1}(q^n-q^i)}{n!}$, while the number of subsets of $\mathbb{F}_{q^n}$ with cardinality n is $\binom{q^n}{n}$. □

Now, let $\ell < n$ be two positive integers and let θ be a generator of $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. Let $(k_0, \ldots, k_{\ell-1}) \in \mathbb{F}_{q^n}^{\ell}$ be the secret key and $\kappa(x) = k_0 x + k_1 x^{\theta} + \ldots + k_{\ell-1} x^{\theta^{\ell-1}} \in \mathcal{L}_n(\mathbb{F}_{q^n})$ be the corresponding θ-polynomial. Consider a set of features $A = \{g_1, \ldots, g_n\} \subseteq \mathbb{F}_{q^n}$ given by n $\mathbb{F}_q$-linearly independent elements. Choose a random map $\lambda : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$ such that $\lambda(x) \neq \kappa(x)$ for all $x \in B$, where $B = \mathbb{F}_{q^n} \setminus A$.

Following the classical PFV scheme, we define the sets

$$\begin{aligned} \mathcal{P}_{\text{auth}} &= \{(x, \kappa(x)) \mid x \in A\}, \\ \mathcal{P}_{\text{chaff}} &= \{(x, \lambda(x)) \mid x \in B\}, \\ \mathcal{V} &= \mathcal{P}_{\text{auth}} \cup \mathcal{P}_{\text{chaff}}. \end{aligned}$$

$\mathcal{P}_{\text{auth}}$ is called *set of authentic points*, $\mathcal{P}_{\text{chaff}}$ is the *set of chaff points*, and $\mathcal{V}$ is called *set of vault points.*

The last ingredients of the fuzzy vault scheme are the code

$$C = \mathcal{G}_{\ell,\theta}(g),$$

where $g = (g_1, \ldots, g_n)$, and an error correction decoding algorithm for C.

For our constructions of the Linearized Polynomial Fuzzy Vault (LPFV), it is convenient to consider a Gabidulin code as a code whose codewords consist of evaluations of a θ-polynomial $f \in \mathcal{L}_{\ell,\theta}$ over any set of n linearly independent elements in $\mathbb{F}_{q^n}$. Concretely, we think of a codeword as a set of pairs $\{(g_i, y_i)\}_{i=1}^{n}$, where $g_i \in \mathbb{F}_{q^n}$, are linearly independent over $\mathbb{F}_q$, and $y_i = f(g_i)$, for a linearized polynomial $f \in \mathcal{L}_{\ell,\theta}$. In this framework, suppose that a witness attempts to gain access to the key, and submits a set of features $W \subset \mathbb{F}_{q^n}$.

Given Assumption 1, if $Z \subseteq \mathcal{V}$ is the subset of vault points (x, y) with $x \in W$, we can consider the $\mathbb{F}_q$-linear map

$$L_Z : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$$

such that $L_Z(x) = y$ for all $(x, y) \in Z$. Now, think of the received word c' as consisting of the set of pairs $\{(g_i, L_Z(g_i))\}_{i=1}^{n}$, for $g_i \in A$. The secret codeword of the LPFV scheme is instead c, given by the set of pairs $\{(g_i, \kappa(g_i))\}_{i=1}^{n}$. With this notation it is easy to see that

$$\mathrm{rk}_q(c - c') = \mathrm{rk}(\kappa - L_Z).$$

The following results relate the rank distance with the set difference, showing that the rank metric can be a good approximation of the set-difference metric. Let $d_\Delta(A, W) := |(A \setminus W) \cup (W \setminus A)|$ denote the set-difference between A and W.

Proposition 8.3. *In the setting of the LPFV scheme, suppose that the values $\lambda(x)$, for $x \in B$ are chosen at random uniformly and independently in $\mathbb{F}_{q^n} \setminus \{\kappa(x)\}$. Then*

1. $2\,\mathrm{rk}_q(c - c') \leq d_\Delta(A, W)$.
2. *Let $0 \leq u \leq n$ be an integer. Then*

$$\Pr\left\{2\,\mathrm{rk}_q(c - c') = d_\Delta(A, W) \mid |A \cap W| = u\right\} = \prod_{i=0}^{n-u-1} \frac{(q^n - q^i)}{(q^n - 1)} = 1 + \mathcal{O}(q^{-u-1}).$$

Proof. 1. Let W be the set of features submitted, and let $u = |A \cap W|$. Then we have $d_\Delta(A, W) = 2n - 2|A \cap W| = 2n - 2u$. Consider now the $\mathbb{F}_q$-linear map $L_Z : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$ such that $L_Z(x) = y$ for $(x, y) \in Z$. The set of first coordinates of Z is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$ and the linear map $\kappa - L_Z$ is 0 on $A \cap W$. Therefore

$$d_R(c, c') = \mathrm{rk}(\kappa - L_Z) \leq n - u = \frac{d_\Delta(A, W)}{2}.$$

2. Since the $\lambda(x)$, for $x \in B$, are chosen at random uniformly and independently in $\mathbb{F}_{q^n} \setminus \{\kappa(x)\}$, then the values $(L_Z - \kappa)(x)$, for $x \in W \setminus (A \cap W)$ are chosen at random uniformly and independently in $\mathbb{F}_{q^n} \setminus \{0\}$. Furthermore, the condition $2\,\mathrm{rk}_q(c - c') = d_\Delta(A, W)$ is equivalent to the condition that the values $(L_z - \kappa)(x)$, for $x \in W \setminus (A \cap W)$ are linearly

independent. Hence,

$$\Pr\left\{2\operatorname{rk}_q(c-c') = d_\Delta(A,W) \mid |A\cap W| = u\right\} = \frac{\left|\left\{A \in \mathbb{F}_q^{n\times(n-u)} \mid \operatorname{rk}(A) = n-u\right\}\right|}{(q^n-1)^{(n-u)}}.$$

□

Theorem 8.4. *Under the same hypothesis of Proposition 8.3, the following statements hold.*

1. *If $d_\Delta(A,W) \le 2\left\lfloor\frac{n-\ell}{2}\right\rfloor$, then the vault recovers the key $\kappa(x)$.*
2. $\Pr\{2\operatorname{rk}_q(c-c') = d_\Delta(A,W)\} = 1+\mathcal{O}(q^{-1})$.

Proof. 1. By Proposition 8.3 we have $2\operatorname{rk}_q(c-c') \le d_\Delta(A,W) \le 2\left\lfloor\frac{n-\ell}{2}\right\rfloor$. Therefore, we are within the error-correction capability and we can correctly obtain the codeword c, and hence the key $\kappa(x)$.

2. We can write $\Pr\{2\operatorname{rk}_q(c-c') = d_\Delta(A,W)\}$ as

$$\begin{aligned}
&\sum_{u=0}^{n}\Pr\left\{2\operatorname{rk}_q(c-c') = d_\Delta(A,W) \mid |A\cap W| = u\right\}\Pr\{|A\cap W| = u\}\\
&= \sum_{u=0}^{n}\left(1+\mathcal{O}(q^{-u-1})\right)\Pr\{|A\cap W| = u\}\\
&= \sum_{u=0}^{n}\left(1+\mathcal{O}(q^{-1})\right)\Pr\{|A\cap W| = u\}\\
&= \left(1+\mathcal{O}(q^{-1})\right)\sum_{u=0}^{n}\Pr\{|A\cap W| = u\}\\
&= 1+\mathcal{O}(q^{-1}),
\end{aligned}$$

where the second equality follows from part 2 of Proposition 8.3.

□

Remark 8.5. Probabilistic results in Proposition 8.3 and Theorem 8.4 do not depend on the probability distribution of the choice of the features. We are only assuming that our construction of the Linearized Polynomial Fuzzy Vault is made by choosing at random uniformly and independently the values $\lambda(x)$ for $x \in B$.

8.1.2 Generalization of the LPFV Scheme

In our construction of the LPFV we considered θ-Gabidulin codes of length n over $\mathbb{F}_{q^n}$. The motivation is that, given a set of features W satisfying Assumption 1, the map $L_Z : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is uniquely determined, and hence also the received word c'.

We can generalize our LPFV considering θ-Gabidulin codes of length n over the field $\mathbb{F}_{q^m}$, where $n < m$, but we need to define the map L_Z in a suitable way.

Before explaining how to construct L_Z, we can observe that an analogue of Lemma 8.2 holds and it can be proved in the same way, but in this case the probability that the set of features is made of linearly independent elements is equal to

$$\prod_{i=0}^{n-1} \frac{(q^m - q^i)}{(q^m - i)} = 1 + \mathcal{O}(q^{-1-m+n}).$$

Now, let $\mathcal{W}$ and $\mathcal{A}$ be the $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^m}$ spanned respectively by W and A. First, we can observe that, in order to build the received word c' as the set $\{(g_i, L_Z(g_i))\}_{i=1}^n$, we only need to define map L_Z on $\mathcal{A}$. We propose the following construction.

We first define the map L_Z on W as $L_Z(x) = y$ for all $(x, y) \in Z$. Then complete W to a basis B of $\mathcal{A} + \mathcal{W}$, by adding the elements g_i in increasing order with respect to the indices i. For those g_i, we set $L_Z(g_i) = \kappa(g_i) + \sigma^i(\alpha)$, where σ is a generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, $\alpha \in \mathbb{F}_{q^m}$ and $\{\sigma^i(\alpha)\}_{i=0}^{m-1}$ is a normal basis of $\mathbb{F}_{q^m}$ as an $\mathbb{F}_q$-vector space.

In this way, our map is uniquely determined on $\mathcal{A} + \mathcal{W}$, and in particular on $\mathcal{A}$. Let again c be the codeword given by the set of pairs $\{(g_i, \kappa(g_i))\}_{i=1}^n$. With this notation it is easy to see that

$$\mathrm{rk}_q(c - c') = \mathrm{rk}(\kappa - L_Z)_{|\mathcal{A}} \leq \mathrm{rk}(\kappa - L_Z).$$

The following results are the analogues of Proposition 8.3 and Theorem 8.4, and they relate the rank distance of c and c' with the set difference of A and W.

Proposition 8.6. *In the setting of the generalized LPFV scheme, suppose that the values $\lambda(x)$, for $x \in B$ are chosen at random uniformly and independently in $\mathbb{F}_{q^m} \setminus \{\kappa(x)\}$.*

1. *Let the subspace distance be $d_S(\mathcal{A}, \mathcal{W}) := \dim_{\mathbb{F}_q}(\mathcal{A}) + \dim_{\mathbb{F}_q}(\mathcal{W}) - 2\dim_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{W})$. Then*

$$d_S(\mathcal{A}, \mathcal{W}) \leq 2\,\mathrm{rk}_q(c - c') \leq d_S(\mathcal{A}, \mathcal{W}) + 2\,\mathrm{rk}(\kappa - L_Z)_{|\mathcal{A}\cap\mathcal{W}} \leq d_\Delta(A, W).$$

2. *Let $0 \leq u \leq v \leq n$ be two integers. Then*

$$\Pr\left\{2\,\mathrm{rk}_q(c - c') = d_\Delta(A, W) \mid |A \cap W| = u, \dim(\mathcal{A} \cap \mathcal{W}) = v\right\} = \prod_{i=n-v}^{n-u-1} \frac{(q^m - q^i)}{q^m - 1}.$$

Proof. 1. Following the construction of the map L_Z, we can write the subspace $\mathcal{A}$ as the direct sum of $\mathcal{A} \cap \mathcal{W}$ and the subspace $\widehat{\mathcal{A}}$, where $\widehat{\mathcal{A}} = \langle g_i \mid i \in I \rangle$ and $I \subset \{1, \ldots, n\}$ with $|I| = n - \dim_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{W})$. Therefore, we can write

$$\mathrm{rk}(\kappa - L_Z)_{|\widehat{\mathcal{A}}} \leq \mathrm{rk}(\kappa - L_Z)_{|\mathcal{A}} \leq \mathrm{rk}(\kappa - L_Z)_{|\widehat{\mathcal{A}}} + \mathrm{rk}(\kappa - L_Z)_{|\mathcal{A}\cap\mathcal{W}}. \tag{8.1}$$

Let $r = \dim_{\mathbb{F}_q}(\widehat{\mathcal{A}})$. By definition of the L_Z, we have

$$\mathrm{rk}(\kappa - L_Z)_{|_{\widehat{\mathcal{A}}}} = \mathrm{rk}(\sigma^{i_1}(\alpha), \dots, \sigma^{i_r}(\alpha)).$$

By construction, $\{\sigma^i(\alpha)\}_{i=0}^{m-1}$ is a normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and hence we can conclude that

$$\mathrm{rk}(\kappa - L_Z)_{|_{\widehat{\mathcal{A}}}} = r = \dim_{\mathbb{F}_q}(\widehat{\mathcal{A}}) = n - \dim_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{W}) = \frac{d_S(\mathcal{A}, \mathcal{W})}{2}.$$

Substituting this equation in (8.1) we obtain the first two inequalities.

For the last inequality, we notice that the map $(\kappa - L_Z)_{|_{\mathcal{A}\cap\mathcal{W}}}$ is 0 on $A \cap W$, and therefore,

$$\mathrm{rk}(\kappa - L_Z)_{|_{\mathcal{A}\cap\mathcal{W}}} \leq \dim_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{W}) - |A \cap W|.$$

Hence we can conclude that

$$d_S(\mathcal{A}, \mathcal{W}) + 2\,\mathrm{rk}(\kappa - L_Z)_{|_{\mathcal{A}\cap\mathcal{W}}} \leq 2n - 2|A \cap W| = d_\Delta(A, W).$$

2. Let $u = |A \cap W|, v = \dim(\mathcal{A} \cap \mathcal{W})$. Then we can write

$$W = \{u_1, \dots, u_{n-v}, w_{n-v+1}, \dots, w_{n-u}, g_{j_1}, \dots, g_{j_u}\},$$

where $u_i \notin \mathcal{A}$ for $i = 1, \dots, n-v$ and $w_i \in \mathcal{A} \setminus A$ for $i = n-v+1, \dots, n-u$. Therefore $2\,\mathrm{rk}(\kappa - L_Z)_{|_{\widehat{\mathcal{A}}}} = 2n - 2v$, and the condition

$$\mathrm{rk}(\kappa - L_Z)_{|_{\mathcal{A}}} = \mathrm{rk}(\kappa - L_Z)_{|_{\widehat{\mathcal{A}}}} + \mathrm{rk}(\kappa - L_Z)_{|_{\mathcal{A}\cap\mathcal{W}}} = n - u$$

is equivalent to the condition

$$\mathrm{rk}(\sigma^{i_1}(\alpha), \dots, \sigma^{i_{n-v}}(\alpha), (\kappa - L_Z)(w_{n-v+1}), \dots, (\kappa - L_Z)(w_{n-u})) = n - u.$$

By hypothesis the values $(L_Z - \kappa)(w_i)$, for $i = n-v+1, \dots, n-u$ are chosen at random uniformly and independently in $\mathbb{F}_{q^m} \setminus \{0\}$, and we can conclude that the probability we are looking for is equal to

$$\frac{\left|\left\{M \in \mathbb{F}_q^{m\times(v-u)} \mid \mathrm{rk}(M \mid X) = n - u\right\}\right|}{(q^m - 1)^{(v-u)}},$$

where X is the matrix representation over $\mathbb{F}_q$ of the vector $(\sigma^{i_1}(\alpha), \dots, \sigma^{i_{n-v}}(\alpha))$. Since

$$\left|\left\{M \in \mathbb{F}_q^{m\times(v-u)} \mid \mathrm{rk}(M \mid X) = n - u\right\}\right| = \prod_{i=n-v}^{n-u-1} (q^m - q^i),$$

this concludes the proof.

□

Theorem 8.7. *Under the same hypothesis of Proposition 8.6, the following statements hold.*

1. *If* $d_\Delta(A, W) \leq 2\left\lfloor \frac{n-\ell}{2} \right\rfloor$, *then the vault recovers the key* $\kappa(x)$.
2. $\Pr\{2\,\mathrm{rk}_q(c - c') = d_\Delta(A, W)\} = 1 + \mathcal{O}(q^{-1-m+n})$.

Proof. 1. The proof is essentially the same as the proof of part 1 of Theorem 8.4, using part 1 of Proposition 8.6.

2. In order to simplify the notation we introduce the events $D_u = \{|A \cap W| = u\}$, $E_v = \left\{\dim_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{W}) = v\right\}$ for $0 \leq u, v \leq n$, and $X = \{2\,\mathrm{rk}_q(c - c') = d_\Delta(A, W)\}$. Then, we have

$$\begin{aligned}
\Pr\{X\} &= \sum_{0 \leq u \leq v \leq n} \Pr\{X \mid D_u \cap E_v\} \Pr\{D_u \cap E_v\} \\
&= \sum_{0 \leq u \leq v \leq n} \left(1 + \mathcal{O}(q^{-1-m-u+n})\right) \Pr\{D_u \cap E_v\} \\
&= \sum_{0 \leq u \leq v \leq n} \left(1 + \mathcal{O}(q^{-1-m+n})\right) \Pr\{D_u \cap E_v\} \\
&= \left(1 + \mathcal{O}(q^{-1-m+n})\right) \sum_{0 \leq u \leq v \leq n} \Pr\{D_u \cap E_v\} \\
&= 1 + \mathcal{O}(q^{-1-m+n}),
\end{aligned}$$

where the second equality follows from part 2 of Proposition 8.6.

□

Remark 8.8. Suppose one wants to use a generalized LPFV scheme with n genuine features, and suppose moreover that a field $\mathbb{F}_q$ and an extension field $\mathbb{F}_{q^m}$, with $m \geq n$, are given. By part 2 of Theorem 8.7 we can see that the bigger is m the better is the approximation of the set difference with the rank distance. On the other hand, increasing m implies an increase of the computational cost of the operations. Then one can choose the best m based on the application and the particular requirements of the context.

8.1.3 Motivations

The schemes presented above can be applied in several scenarios for different purposes. In this subsection we would like to give just a few examples.

One scenario for the fuzzy commitment scheme in the rank metric is the following. Suppose B is the matrix used to create the stored tuple and imagine it as an image. It may happen for some reason that B gets somehow damaged in a way that a few rows (or columns) are erased or anyway not the same as before. One can then authenticate with the new matrix B' as long as not too many rows (or columns) are different. In another situations the matrix B may be slightly changed into B' by having all elements increased by a common error, and again the difference between the two matrices is a matrix of low rank, exactly 1 in this case.

Another scenario involves a multi-factor authentication problem. Suppose that in order to perform authentication one needs a large number of conditions fulfilled, namely imagine a matrix with a large number of columns whereby condition number i is fulfilled whenever column number i equals a predetermined vector v_i. If you want to allow authentication as long as a certain big enough number of conditions are satisfied, then the fuzzy commitment scheme in the rank metric can be used. Indeed having two matrices A and A' that both satisfy a certain condition corresponds to a zero column in the difference $A - A'$ which directly affects the rank distance between the two.

Applications for the linearized polynomial fuzzy vault scheme overlap with those of the standard fuzzy vault, i.e. we are considering authentication based on the set-difference metric. It may be preferable to use the linearized version and decoding in the rank metric for certain choices and combinations of parameters which are usually dependent on the application. Also, the use of linear maps may be preferred for certain implementations.

8.2 Partial-MDS Codes

Partial-MDS (PMDS) codes are a family of locally repairable codes, mainly used for distributed storage. They are defined to be able to correct any pattern of s additional erasures, after a given number of erasures per locality group have occurred. This makes them also *maximally recoverable (MR) codes*, another class of locally repairable codes. Both terms will be properly defined in the next subsection.

It is known that MR codes in general, and PMDS codes in particular, exist for any set of parameters, if the field size is large enough [22]. Moreover, some explicit constructions of PMDS codes are known, mostly (but not always) with a strong restriction on the number of erasures that can be corrected per locality group [10, 11, 12, 21, 44]. In this section we generalize the notion of PMDS codes to allow locality groups of different sizes. We give an algebraic description of such PMDS codes via their generator matrix. Then, we give a general construction of PMDS codes with $s = 1$ global parity, i.e., one additional erasure can be corrected. This construction can be seen as a generalization of the code construction from [21]. Furthermore, we show that all PMDS codes for the given parameters are of this form, i.e., we give a classification of these codes. More specifically, we prove that PMDS codes with $s = 1$ exist, if and only if MDS codes of length one more than the length of the largest locality block exist. This implies a necessary and sufficient condition on the underlying field size for the existence of these codes (assuming that the MDS conjecture is true). For some parameter sets our generalized construction gives rise to PMDS codes with a smaller field size than any other known construction. Finally, we provide a general construction of PMDS codes for arbitrary number s of global parities, which is based on MRD and MDS codes.

The results of this section were published by Horlemann-Trautmann and Neri in [53] and [80].

8.2.1 Preliminaries

In a distributed storage system we store a file $x \in \mathbb{F}_q^k$, encoded as some codeword $c \in \mathbb{F}_q^n$, over several storage nodes. For simplicity, we assume that each node stores one coordinate of c. If some of these nodes fail, we want to be able to recover the lost information with as little "effort" as possible. One of the important parameters in this context is the *locality* of a code for such a distributed storage system, which is the number of nodes one has to contact to repair a lost node. We call the set of nodes one has to contact if a given node fails, the locality group of that node. The topology given by the set of all locality groups is also called a *configuration*.

Definition 8.9. A code is called *maximally recoverable (MR)* for a given configuration, if any erasure pattern that is information theoretically correctable is correctable.

From now on we consider a distributed storage system with m disjoint locality groups, where the i-th group is of size n_i $(i = 1, \dots, m)$ and can correct any r_i erasures. Analogously we can separate the coordinates of the code (of length n) into blocks of length $n_1, n_2, \dots, n_m$ such that $\sum_{i=1}^m n_i = n$ and such that each block represents a locality group. Furthermore, we fix the locality for the whole code to be ℓ.

Remark 8.10. Our setup is a generalization of the commonly studied setup where all locality groups have the same size. Our generalized setup can be useful for the design of codes for distributed storage systems where the various servers have different error/erasure behavior.

We can now define PMDS codes, generalizing the definition of Blaum-Hafner-Hetzler [10] to locality groups of different sizes but with a fixed locality ℓ:

Definition 8.11. Let $\ell, m, r_1, \dots, r_m \in \mathbb{N}$. Define $n := \sum_{i=1}^m (r_i + \ell)$ and let $C \subseteq \mathbb{F}_q^n$ be a linear code of dimension $k < n$ with generator matrix

$$G = (B_1 \mid \cdots \mid B_m) \in \mathbb{F}_q^{k \times n}$$

such that $B_i \in \mathbb{F}_q^{k \times (r_i + \ell)}$. Then C is an $[n, k, \ell; r_1, \dots, r_m]_q$ *partial-MDS (PMDS) code* if

- for $i \in \{1, \dots, m\}$ the row space of B_i is an $[r_i + \ell, \ell]_q$ MDS code, and
- for any simultaneous r_i erasures in the i-th block $(i = 1, \dots, m)$, the remaining code (after puncturing the coordinates of the erasures) is an $[m\ell, k]_q$ MDS code.

The idea of PMDS codes is to be able to correct more erasures than the prescribed r_i erasures per block. In particular, the erasure correction capability of PMDS code is as follows.

Lemma 8.12. *An $[n, k, \ell; r_1, \dots, r_m]_q$ PMDS code can correct any r_i erasures in the i-th block (simultaneously) plus $s := m\ell - k$ additional erasures anywhere in the code.*

Proof. If we puncture the code in the r_i erased coordinates in each block, by definition the remaining code is an MDS code of length $n - \sum_{i=1}^{m} r_i = m\ell$ and dimension k, and so it can correct any set of $s = m\ell - k$ erasures. Furthermore, after correcting the s erasures, we can correct any r_i erasures in the i-th block, because the block represents an $[r_i+\ell, \ell]_q$ MDS code. □

One can easily see that for the above definition to make sense we need $k \geq \ell$, which we will assume for the rest of the section. If we have equality then there exist only trivial PMDS codes, in the sense that they are MDS codes:

Proposition 8.13. *If $k = \ell$, then a code is an $[n, k, k; r_1, \dots, r_m]_q$ PMDS code if and only if it is an $[n, k]_q$ MDS code.*

Proof. Assume the code is $[n, k, k; r_1, \dots, r_m]_q$ PMDS. Let S be a submatrix of the generator matrix $G = (B_1 \mid \cdots \mid B_m)$ after erasing r_i columns per block B_i. Then each block B_i still has k columns, i.e., for S to generate an MDS code all maximal minors (including minors completely inside one block) need to be non-zero. Since we need to check the MDS property for any such S, all maximal minors of G need to be non-zero, i.e., G generates an MDS code.

For the other direction assume that C is an $[n, k]_q$ MDS code. Then any puncturing of at most $n - k = n - \ell$ coordinates gives an MDS code of dimension $k = \ell$. In particular, since $n - k = k(m-1) + \sum_{i=1}^{m} r_i$, the two conditions for the PMDS property are fulfilled. □

We note that Proposition 8.13 also includes the case $m = 1$, since this automatically implies $k = \ell$. Furthermore, the case $k = 1$ is also included, since this implies $\ell = k = 1$.

Remark 8.14. In [10] PMDS codes are studied with respect to RAID architectures, where all blocks have the same size $n_1 = \ell + r_1$, such that a codeword is written in an $m \times n_1$ array and complete columns are erased when a RAID disk fails. Moreover, due to the physical nature of solid state disks, with age s additional erasures may occur anywhere in the codeword.

It was shown in [44, Lemma 4] that, in the case that the locality groups are disjoint and $r_i = 1$ for $i = 1, \dots, m$, the MR property is equivalent to the PMDS property. That MR implies PMDS for configurations with disjoint locality blocks is straightforward. The other direction was proved by showing that any other erasure pattern than the ones with at most one erasure per block plus s extra erasures anywhere cannot be correctable at all. Thus, any $[n, k, \ell; 1, \dots, 1]_q$ PMDS code is also an MR code. We will now generalize this result to variable values of $r_1, \dots, r_m$.

Theorem 8.15. *[53] An $[n, k, \ell; r_1, \dots, r_m]_q$ PMDS code is maximally recoverable. Moreover, for a given configuration with m disjoint locality groups of length $\ell + r_i$ $(i = 1, \dots, m)$ and locality ℓ, a maximally recoverable code is an $[n, k, \ell; r_1, \dots, r_m]_q$ PMDS code.*

Remark 8.16. The conditions of Definition 8.11 are necessary in order to have maximum recoverability of the code. Indeed, suppose that we only require the row space of some B_j to be contained in, but not equal to, an $[r_j + \ell, \ell]_q$ MDS code. Then the row space of B_j has dimension $\leq \ell - 1$. Therefore, also the dimension of the column space of B_j has dimension $\leq \ell - 1$. After puncturing every block B_i in r_i coordinates for $i = 1, \dots, m$, we get a code whose generator matrix has ℓ linearly dependent columns, namely the remaining columns of the block B_j. Since $k \geq \ell$, this implies that the resulting code cannot be MDS, and therefore it is not able to correct every set of $s = m\ell - k$ erasures.

In the following we give a brief overview of known results for (non-trivial) PMDS codes.

Proposition 8.17. *[22] MR codes of length n and dimension k exist for any configuration over any finite field of size $q > \binom{n-1}{k-1}$.*

Since MR codes are PMDS codes for disjoint locality blocks, the above result also implies that PMDS codes exist for any set of parameters if the field size is large enough.

Some specific constructions of PMDS codes, either for small r or small s, are given in [10, 11, 12, 44]. In [10] a construction of PMDS codes with $s = 1$ and equal block length $n_i = n/m$ over $\mathbb{F}_q$ with $q = 2^b \geq \max\{n_i, m\}$ was given.

Another construction for PMDS codes with $s = 1$ and equal block length $n_i = n/m$, requiring field size $q \geq n_i$, was given in [21, Theorem 1]:

Proposition 8.18. *[21] $[n, m\ell - 1, \ell; r, \dots, r]_q$ PMDS codes exist over any finite field of size $q \geq n/m = \ell + r$.*

This construction (as the ones of [10]) is based on Vandermonde matrices and thus it is equivalent to using generalized Reed-Solomon codes as building blocks. In the following, we will give a generalized construction of PMDS codes with $s = 1$, allowing various block lengths and any MDS codes as building blocks. In some cases this generalized construction will allow us to reduce the field size compared to the construction of [21]. Moreover, in contrast to the construction of [21], our construction provides generator matrices in systematic (or standard) form.

Note that a natural lower bound on the field size is given by the condition that every block constitutes an $[r_i + \ell, \ell]_q$ MDS code. To derive a bound from this condition we assume that the MDS conjecture ([103], see also [95, Conjecture 11.16]) is true (it has been proven for many parameter sets):

Conjecture 3 (MDS Conjecture)**.** *[103] An $[n, k]_q$ MDS code with $1 < k < n - 1$ has length $n \leq q + 1$, unless $q = 2^h$ and $k \in \{3, q - 1\}$, in which case $n \leq q + 2$.*

Assuming that the MDS Conjecture is true, it follows that, when $\ell > 1$, an $[n, k, \ell; r_1, \dots, r_m]_q$ PMDS code cannot exist over $\mathbb{F}_q$ if $q < \max_i\{r_i + \ell - 1\}$, except if $(\ell, \max_i\{r_i\}) \in \{(3, 2^h - 1), (2^h - 1, 3)\}$, in which case such a code cannot exist if $q < \max_i\{r_i + \ell - 2\}$. Under this assumption, in Corollary 8.25, we will show that, in the case that $s = 1$, this bound cannot be obtained in general, but that it has to be increased by 1. Furthermore, it can be proved that, for $s > 1$, a lower bound for the field size is given by $\max_i\{r_i + \ell + s - 1\}$ (except for some special parameter sets) [53].

8.2.2 Algebraic Description of PMDS Codes

We will now define a standard form for generator matrices of PMDS codes. This standard form is the main tool for the random construction of PMDS codes.

Theorem 8.19 (PMDS standard form)**.** *Let $m \geq 2$ and $s, \ell, r_1, \dots, r_m \geq 1$ and let C be an $[n, k = m\ell - s, \ell; r_1, \dots, r_m]_q$ PMDS code. Then C has a generator matrix of the form*

$$G = (B_1 \mid \cdots \mid B_m)\,, \tag{8.2}$$

where

- *$B_i = (C_i \mid D_i)$, $C_i \in \mathbb{F}_q^{k\times\ell}$ and $D_i \in \mathbb{F}_q^{k\times r_i}$ for $i = 1, \dots, m$, and*
- *the submatrix $G_C = (C_1 \mid \cdots \mid C_m)$ is of the form*

$$G_C = (I_k \mid A)\,,$$

with A being superregular.

Proof. Let $\widetilde{G}$ be a generator matrix for C as in Definition 8.11, i.e.

$$\widetilde{G} = \left(\widetilde{B}_1 \mid \cdots \mid \widetilde{B}_m\right).$$

Puncturing every block $\widetilde{B}_i$ in the last r_i columns, we get that the submatrix $\widetilde{G}_C$ is the generator matrix of an $[m\ell, k]_q$ MDS code. Operating on the rows of such a submatrix we can transform it to a matrix $G_C = (I_k \mid A)$, with A superregular. More specifically, there exists an invertible matrix $P \in \mathrm{GL}_k(\mathbb{F}_q)$ such that $P\widetilde{G}_C = (I_k \mid A)$, and therefore the matrix $G := P\widetilde{G}$ is a generator matrix of C of the required form. □

We now consider the entries $a_{w,z}$ of A as variables $x_{w,z}$ for $w = 1, \dots, k$ amd $z = 1, \dots, s$. We know that the column space of D_i is inside the column space of C_i, by the parameters of the block MDS codes. This means that every column in D_i is a linear combination of the columns of C_i. If we denote by $D_i^{(j)}$ the j-th column of D_i, then

$$D_i^{(j)} = \sum_{t=1}^{\ell} y_{t,i,j} C_i^{(t)} \tag{8.3}$$

for some $y_{t,i,j}$, which we also consider as variable. In this way we can consider a $k \times n$ generator matrix as a matrix in $\mathbb{F}_q[x_{w,z}, y_{t,i,j}]^{k\times n}$ (where $\mathbb{F}_q[x_{w,z}, y_{t,i,j}]$ denotes the polynomial ring in all $x_{w,z}, y_{t,i,j}$).

Let $R = \sum_{i=1}^{m} r_i$. We denote $\boldsymbol{\alpha} := (\alpha_{w,z})_{w,z} \in \mathbb{F}_q^{sk}$ and $\boldsymbol{\beta} := (\beta_{t,i,j})_{t,i,j} \in \mathbb{F}_q^{\ell R}$. If we replace the variables $x_{w,z}, y_{t,i,j}$ described above in a matrix in PMDS standard form by the values $\alpha_{w,z}, \beta_{t,i,j}$, we denote the corresponding generator matrix by

$$G(\boldsymbol{\alpha}, \boldsymbol{\beta}).$$

Analogously we will denote the variable form by $G(\boldsymbol{x}, \boldsymbol{y})$.

However, a general matrix of this form is not necessarily a generator matrix of a PMDS code for any values $\boldsymbol{\alpha}, \boldsymbol{\beta}$. The following proposition shows what needs to be fulfilled to generate a PMDS code:

Proposition 8.20. *A matrix $G \in \mathbb{F}_q^{k\times n}$ generates an $[n, k = m\ell - s, \ell; r_1, \dots, r_m]_q$ PMDS code if and only if every submatrix in the set*

$$\mathcal{T}_{k,\ell}(G) := \left\{ S \in \mathbb{F}^{k\times k} \mid \begin{array}{c} S \text{ is a submatrix of } G \text{ with} \\ \text{at most } \ell \text{ columns per block } B_i \end{array} \right\}$$

has non-zero determinant.

Proof. This follows from the definition of PMDS, cf. also [53]. □

8.2.3 Classification of PMDS Codes with $s = 1$

In this subsection we state a complete classification of PMDS codes that can correct one additional erasure anywhere in the code, by determining the systematic form of their generator matrix. This characterization is given in [53].

Lemma 8.21. *Let $m \geq 2$ and $\ell, r_1, \dots, r_m \geq 1$ and let C be an $[n, k = m\ell - 1, \ell; r_1, \dots, r_m]_q$ PMDS code. Then C has a generator matrix of the form*

$$G = \left(\begin{array}{cccc|c} B_1 & 0 & \dots & 0 & M_1 \\ 0 & B_2 & \dots & 0 & M_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & B_{m-1} & M_{m-1} \\ \hline 0 & 0 & \dots & 0 & A \end{array} \right) \tag{8.4}$$

where $B_i \in \mathbb{F}_q^{\ell\times(\ell+r_i)}, A \in \mathbb{F}_q^{(\ell-1)\times(\ell+r_m)}, M_i \in \mathbb{F}_q^{\ell\times(\ell+r_m)}$ *are of the form*

$$B_i = \begin{pmatrix} 1 & 0 & \dots & 0 & x_{1,1}^{(i)} & \dots & x_{1,r_i}^{(i)} \\ 0 & 1 & \dots & 0 & x_{2,1}^{(i)} & \dots & x_{2,r_i}^{(i)} \\ \vdots & & \ddots & & \vdots & & \vdots \\ 0 & 0 & \dots & 1 & x_{\ell,1}^{(i)} & \dots & x_{\ell,r_i}^{(i)} \end{pmatrix}, \tag{8.5}$$

$$A = \begin{pmatrix} 1 & 0 & \dots & 0 & \alpha_1^{(m)} & \alpha_1^{(m)}x_{1,1}^{(m)} & \dots & \alpha_1^{(m)}x_{1,r_m}^{(m)} \\ 0 & 1 & \dots & 0 & \alpha_2^{(m)} & \alpha_2^{(m)}x_{2,1}^{(m)} & \dots & \alpha_2^{(m)}x_{2,r_m}^{(m)} \\ \vdots & & \ddots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 & \alpha_{\ell-1}^{(m)} & \alpha_{\ell-1}^{(m)}x_{\ell-1,1}^{(m)} & \dots & \alpha_{\ell-1}^{(m)}x_{\ell-1,r_m}^{(m)} \end{pmatrix},$$

$$M_i = \begin{pmatrix} 0 & 0 & \dots & 0 & \alpha_1^{(i)} & \alpha_1^{(i)}x_{\ell,1}^{(m)} & \dots & \alpha_1^{(i)}x_{\ell,r_m}^{(m)} \\ 0 & 0 & \dots & 0 & \alpha_2^{(i)} & \alpha_2^{(i)}x_{\ell,1}^{(m)} & \dots & \alpha_2^{(i)}x_{\ell,r_m}^{(m)} \\ \vdots & & \ddots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 & \alpha_\ell^{(i)} & \alpha_\ell^{(i)}x_{\ell,1}^{(m)} & \dots & \alpha_\ell^{(i)}x_{\ell,r_m}^{(m)} \end{pmatrix},$$

up to permutation of variables.

Theorem 8.22. *[53] For any* $m \geq 2$ *and* $\ell, r_1, \dots, r_m \geq 1$*, a linear code over* $\mathbb{F}_q$ *of length* $n = m\ell + \sum_{i=1}^m r_i$ *and dimension* $k = m\ell - 1$ *is an* $[n, k, \ell; r_1, \dots, r_m]_q$ *PMDS code if and only if it has a generator matrix of the form*

$$G = \left(\begin{array}{cccc|c} B_1 & 0 & \dots & 0 & M_1 \\ 0 & B_2 & \dots & 0 & M_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & B_{m-1} & M_{m-1} \\ \hline 0 & 0 & \dots & 0 & A \end{array}\right) \tag{8.6}$$

where $B_i \in \mathbb{F}_q^{\ell\times(\ell+r_i)}, A \in \mathbb{F}_q^{(\ell-1)\times(\ell+r_m)}, M_i \in \mathbb{F}_q^{\ell\times(\ell+r_m)}$ *are of the form*

$$B_i = \begin{pmatrix} 1 & 0 & \dots & 0 & x_{1,1}^{(i)} & \dots & x_{1,r_i}^{(i)} \\ 0 & 1 & \dots & 0 & x_{2,1}^{(i)} & \dots & x_{2,r_i}^{(i)} \\ \vdots & & \ddots & & \vdots & & \vdots \\ 0 & 0 & \dots & 1 & x_{\ell,1}^{(i)} & \dots & x_{\ell,r_i}^{(i)} \end{pmatrix},$$

$$A = \begin{pmatrix} 1 & 0 & \dots & 0 & \alpha_1^{(m)} & \alpha_1^{(m)}x_{1,1}^{(m)} & \dots & \alpha_1^{(m)}x_{1,r_m}^{(m)} \\ 0 & 1 & \dots & 0 & \alpha_2^{(m)} & \alpha_2^{(m)}x_{2,1}^{(m)} & \dots & \alpha_2^{(m)}x_{2,r_m}^{(m)} \\ \vdots & & \ddots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 & \alpha_{\ell-1}^{(m)} & \alpha_{\ell-1}^{(m)}x_{\ell-1,1}^{(m)} & \dots & \alpha_{\ell-1}^{(m)}x_{\ell-1,r_m}^{(m)} \end{pmatrix},$$

$$M_i = \begin{pmatrix} 0 & 0 & \dots & 0 & \alpha_1^{(i)} & \alpha_1^{(i)} x_{\ell,1}^{(m)} & \dots & \alpha_1^{(i)} x_{\ell,r_m}^{(m)} \\ 0 & 0 & \dots & 0 & \alpha_2^{(i)} & \alpha_2^{(i)} x_{\ell,1}^{(m)} & \dots & \alpha_2^{(i)} x_{\ell,r_m}^{(m)} \\ \vdots & & \ddots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 & \alpha_\ell^{(i)} & \alpha_\ell^{(i)} x_{\ell,1}^{(m)} & \dots & \alpha_\ell^{(i)} x_{\ell,r_m}^{(m)} \end{pmatrix},$$

such that $\alpha_j^{(i)} \neq 0$ for any i, j, and, for $i = 1, \dots, m-1$, the matrices

$$\widehat{B}_i = \left(\begin{array}{c|c} & \alpha_1^{(i)} \\ & \alpha_2^{(i)} \\ B_i & \vdots \\ & \alpha_\ell^{(i)} \end{array} \right),$$

are generator matrices of $[\ell + r_i + 1, \ell]_q$ MDS codes and

$$\widehat{A} = \begin{pmatrix} 1 & 0 & \dots & 0 & 1 & x_{\ell,1}^{(m)} & \dots & x_{\ell,r_m}^{(m)} \\ 0 & 1 & \dots & 0 & 1 & x_{1,1}^{(m)} & \dots & x_{1,r_m}^{(m)} \\ \vdots & & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 & 1 & x_{\ell-1,1}^{(m)} & \dots & x_{\ell-1,r_m}^{(m)} \end{pmatrix}$$

is a generator matrix of an $[\ell + r_m + 1, \ell]_q$ MDS code.

Several results follow from Theorem 8.22. The first one is a characterization of PMDS codes with one global parity in terms of their parity check matrix.

Theorem 8.23. *[53] For any $m \geq 2$ and $\ell, r_1, \dots, r_m \geq 1$, a linear code over $\mathbb{F}_q$ of length $n = m\ell + \sum_{i=1}^m r_i$ and dimension $k = m\ell - 1$ is an $[n, k, \ell; r_1, \dots, r_m]_q$ PMDS code if and only if it has a parity check matrix of the form*

$$H = \left(\begin{array}{cccc} H_1 & 0 & \dots & 0 \\ 0 & H_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & H_m \\ \hline v_1 & v_2 & \dots & v_m \end{array} \right), \tag{8.7}$$

where $H_i \in \mathbb{F}_q^{r_i \times (\ell + r_i)}$ is a parity check matrix of an $[\ell + r_i, \ell]_q$ MDS code, and $v_i \in \mathbb{F}_q^{1 \times (\ell + r_i)}$ is such that

$$\begin{pmatrix} H_i \\ v_i \end{pmatrix}$$

is a parity check matrix of an $[\ell + r_i, \ell - 1]_q$ MDS code.

The second result that can be deduced from Theorem 8.22 relates the existence of PMDS codes with $s = 1$ to the existence of MDS codes.

Corollary 8.24. *Let $m \geq 2$ and $\ell, r_1, \dots, r_m \geq 1$ be integers, $n = m\ell + \sum_{i=1}^{m} r_i$ and q be a prime power. The following are equivalent:*

1. *There exists an $[n, k = m\ell - 1, \ell; r_1, \dots, r_m]_q$ PMDS code.*
2. *There exists an $[\ell + r_i + 1, \ell]_q$ MDS code, for every $i = 1, \dots, m$.*
3. *There exists an $[\ell + \max\{r_i\} + 1, \ell]_q$ MDS code.*

Proof. The equivalence between 1 and 2 directly follows from Theorem 8.22. Moreover, it is clear that 2 implies 3. The implication from 3 to 2 follows from the fact that puncturing an $[\ell + \max\{r_i\} + 1, \ell]_q$ MDS code in at most $j \leq \max\{r_i\}$ coordinates results in an $[\ell + \max\{r_i\} + 1 - j, \ell]_q$ MDS code. □

Finally, we can state the following result, which shows that one cannot construct PMDS codes with $s = 1$ over smaller fields, if the MDS conjecture is true.

Corollary 8.25. *Assuming that the MDS-conjecture (Conjecture 3) is correct, we have:*

1. *If there exists an $[n, k = m\ell - 1, \ell; r_1, \dots, r_m]_q$ PMDS code such that $\ell \in \{3, 2^h - 1\}$ and $\max_i\{r_i\} + \ell = 2^h + 1$ (for some $h > 1$), then $q \geq 2^h = \max_i\{r_i\} + \ell - 1$.*
2. *If there exists an $[n, k = m\ell - 1, \ell; r_1, \dots, r_m]_q$ PMDS code such that the parameters are not included in case 1. and $\ell > 1$, then $q \geq \max_i\{r_i\} + \ell$.*

Theorem 8.22, or equivalently Theorem 8.23, gives a complete characterization of PMDS codes that can correct $s = 1$ global erasure – on one hand we show how to construct PMDS codes for a given valid parameter set with $s = 1$, and on the other hand we show that every PMDS code that can correct at most $s = 1$ additional erasure has to be of this form essentially. This completes the picture for PMDS codes correcting one global erasure.

8.2.4 General Construction via MRD Codes

Here, we reformulate and generalize the construction given in [19], where the authors use Gabidulin codes in order to build $[n, k, \ell; r, \dots, r]_{q^N}$ PMDS codes. We will show that this construction also works for different r_i, and that Gabidulin codes can be replaced by any vector MRD code.

Fix $n, k, \ell, r_1, \dots, r_m$, and let $\widetilde{G} \in \mathbb{F}_{q^N}^{k \times m\ell}$ be the generator matrix of an $[m\ell, k]_{q^N}$ MRD code. For the existence of an MRD code we need $N \geq m\ell$. Moreover, for every $i = 1, \dots, m$, we consider an $[\ell + r_i, \ell]_q$ MDS code with generator matrix M_i, and define

$$M := \begin{pmatrix} M_1 & 0 & \dots & 0 \\ 0 & M_2 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & M_m \end{pmatrix} \in \mathbb{F}_q^{m\ell \times n}. \tag{8.8}$$

We can now formulate our PMDS construction.

Theorem 8.26. *Let $\widetilde{G} \in \mathbb{F}_{q^N}^{k \times m\ell}$ be the generator matrix of an $[m\ell, k]_{q^N}$ MRD code and let M be the matrix defined in (8.8). Then the matrix $\widetilde{G}M$ is a generator matrix for an $[n, k, \ell; r_1, \dots, r_m]_{q^N}$ PMDS code.*

Proof. Let $G := \widetilde{G}M$ and let $S \in \mathcal{T}_{k,\ell}(G)$ be the submatrix obtained by selecting columns $h_1, \dots, h_{k_j}$ from the j-th block for $j = 1, \dots, m$, where $k_i \leq \ell$ and $k_1 + \ldots + k_m = k$. S is equal to $\widetilde{G}\widetilde{M}$, where

$$\widetilde{M} = \begin{pmatrix} N_1 & 0 & \dots & 0 \\ 0 & N_2 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & N_m \end{pmatrix},$$

and N_j is the $\ell \times k_j$ submatrix of M_j obtained by the respective selected columns. Since M_i generates an $[\ell + r_i, \ell]_q$-MDS code, any ℓ columns of M_i are linearly independent. Thus, $\mathrm{rk}(N_i) = k_i$ and $\mathrm{rk}(\widetilde{M}) = k_1 + \ldots + k_m = k$. By Proposition 3.8 we have that $\det(\widetilde{G}\widetilde{M}) \neq 0$, and we conclude the proof, using Proposition 8.20. □

Example 8.27. Let $q = 5, N = 4$ and α a root of $x^4 + x^3 + x^2 + x + 3$. We use the MRD code over $\mathbb{F}_{5^4}$ from [51, Example 5.8], with generator matrix

$$\widetilde{G} = \begin{pmatrix} 1 & 0 & \alpha & \alpha^2 \\ 0 & 1 & \alpha^2 & 2\alpha \end{pmatrix}$$

and the MDS codes over $\mathbb{F}_5$ with generator matrices

$$M_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \end{pmatrix}.$$

Then the matrix

$$\widetilde{G}\begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix} = \left(\begin{array}{cccc|ccc} 1 & 1 & 1 & 1 & \alpha + \alpha^2 & \alpha + 2\alpha^2 & \alpha + 3\alpha^2 \\ 1 & 2 & 3 & 4 & \alpha^2 + 2\alpha & \alpha^2 + 4\alpha & \alpha^2 + \alpha \end{array}\right)$$

generates an $[7, 2, 2; 2, 1]_{5^4}$-PMDS code. This code can correct two erasures in the first block, one erasure in the second block, plus two erasures anywhere.

Example 8.28. Let $q = 3, N = 6$ and α a root of $x^6 + 2x^4 + x^2 + 2x + 1$. We use the MRD code over $\mathbb{F}_{3^6}$ with generator matrix

$$\widetilde{G} = \begin{pmatrix} \alpha^{669} & \alpha^{253} & \alpha^{593} & \alpha^{244} & \alpha^{354} & \alpha^{227} \\ 1 & \alpha^{3} & \alpha^{6} & \alpha^{9} & \alpha^{12} & \alpha^{15} \\ 1 & \alpha^{9} & \alpha^{18} & \alpha^{27} & \alpha^{36} & \alpha^{45} \end{pmatrix}.$$

This code is a twisted Gabidulin code $\mathcal{H}^{\eta}_{3,\bar{\theta}}(g)$, where $\bar{\theta}$ is the 3-Frobenius automorphism, $g = (1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5)$ and $\eta = \alpha^{699}+2$. Furthermore, we use the MDS codes over $\mathbb{F}_3$ with generator matrices

$$M_1 = M_2 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}, \quad M_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \end{pmatrix}.$$

The matrix obtained by multiplying $\widetilde{G}$ with the diagonal block matrix defined by M_1, M_2 and M_3 is

$$\left(\begin{array}{cccc|cccc|ccc} \alpha^{629} & \alpha^{391} & \alpha^{669} & \alpha^{253} & \alpha^{600} & \alpha^{178} & \alpha^{593} & \alpha^{244} & \alpha^{557} & \alpha^{477} & \alpha^{354} \\ \alpha^{380} & \alpha^{663} & 1 & \alpha^{3} & \alpha^{386} & \alpha^{669} & \alpha^{6} & \alpha^{9} & \alpha^{392} & \alpha^{675} & \alpha^{12} \\ \alpha^{412} & \alpha^{533} & 1 & \alpha^{9} & \alpha^{430} & \alpha^{551} & \alpha^{18} & \alpha^{27} & \alpha^{448} & \alpha^{569} & \alpha^{36} \end{array}\right)$$

and it generates a $[11, 3, 2; 2, 2, 1]_{3^6}$-PMDS code. This code can correct two erasures in the first and in the second block, one erasure in the third block, plus three erasures anywhere.

Corollary 8.29. *Let $m \geq 2$ and $\ell, r_1, \ldots, r_m \geq 1$, $k \geq \ell$ be positive integers. Then, for every prime p and every positive integers $L_1 \geq m\ell$, $L_2 \geq n_0$ there exists an $[n, k, \ell; r_1, \ldots, r_m]_{p^{L_1 L_2}}$ PMDS code, where*

$$n_0 = \min\{j \in \mathbb{N} \mid p^j \geq \ell + r_i - 1, \ \textit{for } i = 1, \ldots, m\}.$$

Proof. An MRD code in $\mathbb{F}_{q^N}^{m\ell}$ exists if $N \geq m\ell$. Suitable MDS codes over $\mathbb{F}_q$ for the matrix in (8.8) exist if q is a prime power with $q \geq \max\{\ell + r_i - 1\}$. The statement follows from Theorem 8.26. □

Bibliography

[1] A. A. Albert. Generalized twisted fields. *Pacific J. Math*, 11(1):1–8, 1961.

[2] J. Antrobus and H. Gluesing-Luerssen. Maximal Ferrers diagram codes: Constructions and genericity considerations. *arXiv preprint arXiv:1804.00624*, 2018.

[3] D. Augot. Generalization of Gabidulin codes over fields of rational functions. In *21st International Symposium on Mathematical Theory of Networks and Systems (MTNS 2014)*, 2014.

[4] D. Augot, P. Loidreau, and G. Robert. Rank metric and Gabidulin codes in characteristic zero. In *2013 IEEE International Symposium on Information Theory*, pages 509–513. IEEE, 2013.

[5] D. Augot, P. Loidreau, and G. Robert. Generalized Gabidulin codes over fields of any characteristic. *Designs, Codes and Cryptography*, 86(8):1807–1848, 2018.

[6] M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani. On fuzzy syndrome hashing with LDPC coding. In *4th International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL)*, pages 1–5. ACM, 2011.

[7] S. Ballet and J. Pieltant. On the tensor rank of multiplication in any extension of $\mathbb{F}_2$. *Journal of Complexity*, 27(2):230–245, 2011.

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

[9] I. Blanco-Chacón, E. Byrne, I. Duursma, and J. Sheekey. Rank metric codes and zeta functions. *Designs, Codes and Cryptography*, 86(8):1767–1792, 2018.

[10] M. Blaum, J. L. Hafner, and S. Hetzler. Partial-MDS codes and their application to RAID type of architectures. *IEEE Transactions on Information Theory*, 59(7):4510–4519, 2013.

[11] M. Blaum, J. S. Plank, M. Schwartz, and E. Yaakobi. Partial MDS (PMDS) and sector-disk (SD) codes that tolerate the erasure of two random sectors. In *2014 IEEE International Symposium on Information Theory*, pages 1792–1796. IEEE, 2014.

[12] M. Blaum, J. S. Plank, M. Schwartz, and E. Yaakobi. Construction of partial MDS and sector-disk codes with two global parity symbols. *IEEE Transactions on Information Theory*, 62(5):2673–2681, 2016.

[13] M. Bossert, E. M. Gabidulin, and P. Lusina. Space-time codes based on Gaussian integers. In *Proceedings IEEE International Symposium on Information Theory,*, page 273. IEEE, 2002.

[14] R. W. Brockett and D. Dobkin. On the optimal evaluation of a set of bilinear forms. *Linear Algebra and Its Applications*, 19(3):207–235, 1978.

[15] P. Bürgisser, M. Clausen, and M. A. Shokrollahi. *Algebraic complexity theory*, volume 315. Springer Science & Business Media, 2013.

[16] E. Byrne, A. Neri, A. Ravagnani, and J. Sheekey. Tensor representation of rank-metric codes. *SIAM Journal on Applied Algebra and Geometry*, accepted for publication, 2019.

[17] E. Byrne and A. Ravagnani. Covering radius of matrix codes endowed with the rank metric. *SIAM Journal on Discrete Mathematics*, 31(2):927–944, 2017.

[18] E. Byrne and A. Ravagnani. Partition-balanced families of codes and asymptotic enumeration in coding theory. *arXiv preprint arXiv:1805.02049*, 2018.

[19] G. Calis and O. O. Koyluoglu. A general construction for PMDS codes. *IEEE Communications Letters*, 21(3):452–455, 2017.

[20] F. Caullery and K.-U. Schmidt. On the classification of hyperovals. *Advances in Mathematics*, 283:195–203, 2015.

[21] J. Chen, K. W. Shum, Q. Yu, and C. W. Sung. Sector-disk codes and partial MDS codes with up to three global parities. In *2015 IEEE International Symposium on Information Theory (ISIT)*, pages 1876–1880. IEEE, 2015.

[22] M. Chen, C. Huang, and J. Li. On the maximally recoverable property for multi-protection group codes. In *2007 IEEE International Symposium on Information Theory*, pages 486–490. IEEE, 2007.

[23] D. Coggia and A. Couvreur. On the security of a Loidreau's rank metric code based encryption scheme. In *WCC 2019-Workshop on Coding Theory and Cryptography*, 2019.

[24] B. Cooperstein. *Advanced linear algebra*. Chapman and Hall/CRC Press, 2015.

[25] A. Cossidente, G. Marino, and F. Pavese. Non-linear maximum rank distance codes. *Designs, Codes and Cryptography*, 79(3):597–609, 2016.

[26] B. Csajbók, G. Marino, O. Polverino, and C. Zanella. A new family of MRD-codes. *Linear Algebra and its Applications*, 548:203–220, 2018.

[27] B. Csajbók, G. Marino, O. Polverino, and Y. Zhou. Maximum rank-distance codes with maximum left and right idealisers. *arXiv preprint arXiv:1807.08774*, 2018.

[28] B. Csajbók, G. Marino, O. Polverino, and F. Zullo. Maximum scattered linear sets and MRD-codes. *Journal of Algebraic Combinatorics*, 46(3-4):517–531, 2017.

[29] J. de la Cruz, M. Kiermaier, A. Wassermann, and W. Willems. Algebraic structures of MRD codes. *Advances in Mathematics of Communications*, 10(3):499–510, 2016.

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

[31] R. A. DeMillo and R. J. Lipton. A probabilistic remark on algebraic program testing. Technical report, 1977.

[32] L. E. Dickson. *Linear Groups: With an Exposition of the Galois Field Theory*, volume 6. BG Teubner, 1901.

[33] A. Dür. The automorphism groups of Reed-Solomon codes. *Journal of Combinatorial Theory, Series A*, 44(1):69–82, 1987.

[34] F. Fontein, K. Marshall, J. Rosenthal, D. Schipani, and A.-L. Trautmann. On burst error correction and storage security of noisy data. In *20th International Symposium on Mathematical Theory of Networks and Systems (MTNS)*, pages 1–7, 2012.

[35] M. A. Forbes and A. Shpilka. On identity testing of tensors, low-rank recovery and compressed sensing. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 163–172. ACM, 2012.

[36] E. M. Gabidulin. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii*, 21(1):3–16, 1985.

[37] E. M. Gabidulin. Attacks and counter-attacks on the GPT public key cryptosystem. *Designs, Codes and Cryptography*, 48(2):171–177, 2008.

[38] E. M. Gabidulin. New rank codes with efficient decoding. In *Engineering and Telecommunication (EnT), 2017 IVth International Conference on*, pages 23–27. IEEE, 2017.

[39] E. M. Gabidulin, M. Bossert, and P. Lusina. Space-time codes based on rank codes. In *2000 IEEE International Symposium on Information Theory (Cat. No. 00CH37060)*, page 284. IEEE, 2000.

[40] E. M. Gabidulin, A. Paramonov, and O. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In *Advances in Cryptology – EUROCRYPT'91*, pages 482–489. Springer, 1991.

[41] K. Gibson. Severely denting the Gabidulin version of the McEliece public key cryptosystem. *Designs, Codes and Cryptography*, 6(1):37–45, 1995.

[42] K. Gibson. The security of the Gabidulin public key cryptosystem. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 212–223. Springer, 1996.

[43] L. Giuzzi and F. Zullo. Identifiers for MRD-codes. *Linear Algebra and its Applications*, 2019.

[44] P. Gopalan, C. Huang, B. Jenkins, and S. Yekhanin. Explicit maximally recoverable codes with locality. *IEEE Transactions on Information Theory*, 60(9):5245–5256, 2014.

[45] E. Gorla. Rank-metric codes. In *A Concise Encyclopedia of Coding Theory*. CRC Press, to appear.

[46] E. Gorla, R. Jurrius, H. H. López, and A. Ravagnani. Rank-metric codes and q-polymatroids. *arXiv preprint arXiv:1803.10844*, 2018.

[47] V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and algebraic-geometric codes. In *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)*, pages 28–37. IEEE, 1998.

[48] R. W. Hamming. Error detecting and error correcting codes. *Bell System technical journal*, 29(2):147–160, 1950.

[49] R. Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 2013.

[50] J. Håstad. Tensor rank is NP-complete. *Journal of Algorithms*, 11(4):644–654, 1990.

[51] A.-L. Horlemann-Trautmann and K. Marshall. New criteria for MRD and Gabidulin codes and some rank-metric code constructions. *Advances in Mathematics of Communications*, 11(3):533–548, 2017.

[52] A.-L. Horlemann-Trautmann, K. Marshall, and J. Rosenthal. Extension of Overbeck's attack for Gabidulin-based cryptosystems. *Designs, Codes and Cryptography*, 86(2):319–340, 2018.

[53] A.-L. Horlemann-Trautmann and A. Neri. A complete classification of partial-MDS (maximally recoverable) codes with one global parity. *Advances in Mathematics of Communications*, 14:69–88, 2020.

[54] L.-K. Hua. A theorem on matrices over a sfield and its applications. *Acta Math. Sinica*, 1(2):109–163, 1951.

[55] A. Juels and M. Sudan. A fuzzy vault scheme. *Des. Codes Cryptography*, 38(2):237–257, 2006.

[56] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In *6th ACM conference on Computer and communications security*, CCS '99, pages 28–36, 1999.

[57] D. E. Knuth. Finite semifields and projective planes. *Journal of Algebra*, 2(2):182–217, 1965.

[58] R. Koetter and F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory*, 54(8):3579–3591, 2008.

[59] R. Koetter and A. Vardy. Algebraic soft-decision decoding of Reed-Solomon codes. *IEEE Transactions on Information Theory*, 49(11):2809–2825, 2003.

[60] J. B. Kruskal. Three-way arrays: rank and uniqueness of trilinear decompositions, with application to arithmetic complexity and statistics. *Linear algebra and its applications*, 18(2):95–138, 1977.

[61] A. Kshevetskiy and E. M. Gabidulin. The new construction of rank codes. In *Proceedings of the International Symposium on Information Theory (ISIT) 2005*, pages 2105–2108, Sept 2005.

[62] T.-Y. Lam and A. Leroy. Vandermonde and Wronskian matrices over division rings. *Journal of Algebra*, 119(2):308–336, 1988.

[63] M. Lavrauw. Finite semifields and nonsingular tensors. *Designs, codes and cryptography*, 68(1-3):205–227, 2013.

[64] M. Lavrauw, A. Pavan, and C. Zanella. On the rank of $3 \times 3 \times 3$-tensors. *Linear and Multilinear Algebra*, 61(5):646–652, 2013.

[65] M. Lavrauw and J. Sheekey. Canonical forms of $2 \times 3 \times 3$ tensors over the real field, algebraically closed fields, and finite fields. *Linear Algebra and its Applications*, 476:133–147, 2015.

[66] S. Lefschetz. *Algebraic geometry*. Courier Corporation, 2012.

[67] D. Lewin and S. Vadhan. Checking polynomial identities over any field: Towards a derandomization? In *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pages 438–447. ACM, 1998.

[68] R. Lidl and H. Niederreiter. *Finite Fields*, volume 20. Cambridge University Press, 1997.

[69] R. A. Liebler. On nonsingular tensors and related projective planes. *Geometriae Dedicata*, 11(4):455–464, 1981.

[70] Y. Liu, M. P. Fitz, and O. Y. Takeshita. A rank criterion for QAM space-time codes. *IEEE Transactions on Information Theory*, 48(12):3062–3079, 2002.

[71] P. Loidreau. Designing a rank metric based McEliece cryptosystem. In *International Workshop on Post-Quantum Cryptography*, pages 142–152. Springer, 2010.

[72] P. Loidreau. An evolution of GPT cryptosystem. In *workshop on Algebraic and Combinatorial Coding Tehroy*, 2016.

[73] G. Lunardon. MRD-codes and linear sets. *Journal of Combinatorial Theory, Series A*, 149:1–20, 2017.

[74] G. Lunardon, R. Trombetti, and Y. Zhou. Generalized twisted Gabidulin codes. *Journal of Combinatorial Theory, Series A*, 159:79–106, 2018.

[75] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*, volume 16. Elsevier, 1977.

[76] K. Marshall, D. Schipani, A.-L. Trautmann, and J. Rosenthal. Subspace fuzzy vault. In *Physical and Data-Link Security Techniques for Future Communication Systems*, pages 163–172. Springer, 2016.

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

[78] S. Müelich, S. Puchinger, and M. Bossert. Low-rank matrix recovery using Gabidulin codes in characteristic zero. *Electronic Notes in Discrete Mathematics*, 57:161–166, 2017.

[79] A. Neri. Systematic encoders for generalized Gabidulin codes and the q-analogue of Cauchy matrices. *arXiv preprint arXiv:1805.06706*, 2018.

[80] A. Neri and A.-L. Horlemann-Trautmann. Random construction of Partial MDS codes. *arXiv preprint arXiv:1801.05848*, 2018.

[81] A. Neri, A.-L. Horlemann-Trautmann, T. Randrianarisoa, and J. Rosenthal. On the genericity of maximum rank distance and Gabidulin codes. *Designs, Codes and Cryptography*, 86(2):341–363, 2018.

[82] A. Neri, S. Puchinger, and A.-L. Horlemann-Trautmann. Invariants and inequivalence of linear rank-metric codes. In *IEEE International Symposium on Information Theory (ISIT)*, pages 2049–2053, 2019.

[83] A. Neri, S. Puchinger, and A.-L. Horlemann-Trautmann. Equivalence and characterizations based on invariants of linear rank-metric codes. In preparation.

[84] A. Neri, J. Rosenthal, and D. Schipani. Fuzzy authentication using rank distance. In *International Worskhop on Communication Security*, pages 97–108. Springer, 2017.

[85] NIST. Post–Quantum Cryptography Standardization. `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography`, 2017.

[86] K. Otal and F. Özbudak. Additive rank metric codes. *IEEE Transactions on Information Theory*, 63(1):164–168, 2017.

[87] R. Overbeck. Structural attacks for public key cryptosystems based on Gabidulin codes. *Journal of Cryptology*, 21(2):280–301, 2008.

[88] S. E. Payne. A complete determination of translation ovoids in finite Desarguian planes. *Atti Accad. Naz. Lincei Rend.*, 51(5):328–331, 1971.

[89] S. Puchinger. *Construction and Decoding of Evaluation Codes in Hamming and Rank Metric*. PhD thesis, Universität Ulm, 2018.

[90] S. Puchinger, J. Rosenkilde né Nielsen, and J. Sheekey. Further generalisations of twisted Gabidulin codes. In *International Workshop on Coding and Cryptography*, 2017.

[91] A. Ravagnani. Generalized weights: An anticode approach. *Journal of Pure and Applied Algebra*, 220(5):1946–1962, 2016.

[92] A. Ravagnani. Rank-metric codes and their duality theory. *Designs, Codes and Cryptography*, 80(1):197–216, 2016.

[93] I. S. Reed and G. Solomon. Polynomial codes over certain finite fields. *Journal of the society for industrial and applied mathematics*, 8(2):300–304, 1960.

[94] ROLLO. Rank-Ouroboros, LAKE and LOCKER. `http://www.pqc-rollo.org/`, 2017.

[95] R. Roth. *Introduction to coding theory*. Cambridge University Press, 2006.

[96] R. M. Roth. Maximum-rank array codes and their application to crisscross error correction. *IEEE Transactions on Information Theory*, 37(2):328 –336, mar 1991.

[97] R. M. Roth and A. Lempel. On MDS codes via Cauchy matrices. *IEEE transactions on information theory*, 35(6):1314–1319, 1989.

[98] R. M. Roth and G. Seroussi. On generator matrices of MDS codes (corresp.). *IEEE Transactions on Information Theory*, 31(6):826–830, 1985.

[99] RQC. Rank Quasi-Cyclic. http://pqc-rqc.org/, 2017.

[100] D. Schipani and J. Rosenthal. Coding solutions for the secure biometric storage problem. In *Information Theory Workshop (ITW), 2010*, pages 1–4, 2010.

[101] K.-U. Schmidt and Y. Zhou. On the number of inequivalent Gabidulin codes. *Designs, Codes and Cryptography*, pages 1–10, 2017.

[102] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, Oct. 1980.

[103] B. Segre. Curve razionali normali e k-archi negli spazi finiti. *Annali di Matematica Pura ed Applicata*, 39(1):357–379, 1955.

[104] G. Seroussi and R. M. Roth. On MDS extensions of generalized Reed-Solomon codes. *IEEE Transactions on Information Theory*, 32(3):349–354, 1986.

[105] C. E. Shannon. A mathematical theory of communication. *Bell system technical journal*, 27(3):379–423, 1948.

[106] J. Sheekey. A new family of linear maximum rank distance codes. *Advances in Mathematics of Communications*, 10(3):475–488, 2016.

[107] J. Sheekey and G. Van de Voorde. Rank-metric codes, linear sets, and their duality. *arXiv preprint arXiv:1806.05929*, 2018.

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

[109] D. Silva and F. R. Kschischang. Security for wiretap networks via rank-metric codes. In *2008 IEEE International Symposium on Information Theory*, pages 176–180. IEEE, 2008.

[110] D. Silva and F. R. Kschischang. Fast encoding and decoding of Gabidulin codes. In *2009 IEEE International Symposium on Information Theory*, pages 2858–2862. IEEE, 2009.

[111] D. Silva, F. R. Kschischang, and R. Koetter. A rank-metric approach to error control in random network coding. *IEEE transactions on information theory*, 54(9):3951–3967, 2008.

[112] R. Singleton. Maximum distance q-nary codes. *IEEE Transactions on Information Theory*, 10(2):116–118, 1964.

[113] N. J. Sloane et al. The on-line encyclopedia of integer sequences, 2003.

[114] R. Trombetti and Y. Zhou. A new family of MRD codes in $\mathbb{F}_q^{2n\times 2n}$ with right and middle nuclei $\mathbb{F}_{q^n}$. *IEEE Transactions on Information Theory*, 65(2):1054–1062, 2019.

[115] J. van Lint. *Introduction to Coding Theory*, volume 86. Springer Science & Business Media, 2012.

[116] A. Wachter-Zeh, V. Afanassiev, and V. Sidorenko. Fast decoding of Gabidulin codes. *Designs, codes and cryptography*, 66(1-3):57–73, 2013.

[117] A. Wachter-Zeh, S. Puchinger, and J. Renner. Repairing the Faure-Loidreau public-key cryptosystem. In *2018 IEEE International Symposium on Information Theory (ISIT)*, pages 2426–2430. IEEE, 2018.

[118] Z. Wan and L. Hua. *Geometry of matrices.* World Scientific, 1996.

[119] B. Wu and Z. Liu. Linearized polynomials over finite fields revisited. *Finite Fields and Their Applications*, 22:79–100, 2013.

[120] R. Zippel. Probabilistic algorithms for sparse polynomials. In *International Symposium on Symbolic and Algebraic Manipulation*, pages 216–226. Springer, 1979.

[121] F. Zullo. *Linear codes and Galois geometries: between two worlds.* PhD thesis, Università degli Studi della Campania "Luigi Vanvitelli", 2019.