

ulm university universität
uulm

Institut für Nachrichtentechnik

Codes in the Sum-Rank Metric and Codes over Rings

DISSERTATION

zur Erlangung des akademischen Grades eines

Doktors der Naturwissenschaften
(Dr. rer. nat.)

der Fakultät für Ingenieurwissenschaften,
Informatik und Psychologie der Universität Ulm

von

Cornelia Ott

geboren in Laupheim

2025

First Reviewer:

Prof. Dr.-Ing. Martin Bossert
Institute of Communications Engineering
Faculty of Engineering, Computer Science and Psychology
Ulm University, Germany

Second Reviewer:

Prof. Dr. Anna-Lena Horlemann
School of Computer Science
University of St. Gallen, Switzerland

Acting Dean:

Prof. Dr. Matthias Tichy
Institute of Software Engineering and Programming Languages
Faculty of Engineering, Computer Science and Psychology
Ulm University, Germany

Date of the Doctoral Examination: July 13, 2026

Acknowledgments

This dissertation comprises most of my work as a research assistant at the Institute of Communications Engineering, Ulm University, Germany, carried out between January 2018 and December 2023. Throughout these years, I had the privilege of being inspired, motivated, and supported by many people who not only contributed to my research but also made this period an enjoyable and enriching experience. To all of them, I would like to extend my heartfelt thanks.

First and foremost, I would like to thank my doctoral supervisor, Martin Bossert, for his outstanding guidance and continuous support throughout my research. I am especially thankful for his generous encouragement of my academic activities, including support for conference participation and the facilitation of my research stays in Rennes. His broad professional network also opened doors to collaborations with other scientists. Martin created a motivating working environment shaped by his enthusiasm for solving new problems, his encouragement to initiate collaborations, and the freedom he gave his doctoral students to explore a wide range of research topics. Equally enriching were his passion for teaching and his ability to reveal connections across disciplines, thereby fostering creative thinking. I also fondly remember the moments we shared outside of research, such as our cycling tour, which reflected his friendly and down-to-earth nature and contributed to a warm and collegial atmosphere. Above all, he was always accessible, took time, and had an open ear for any concerns.

I am also very grateful to Anna-Lena Horlemann who kindly agreed to be my second examiner and for taking the time to prepare an evaluation of my dissertation.

My sincere thanks are further due to Robert Fischer. His support during the final phase of my time at Ulm University enabled me to continue my work at the Institute of Communications Engineering. It was a pleasure to explore the fascinating field of quaternions with him and to benefit from our scientific discussions.

At the beginning of my doctoral studies, I greatly benefited from collaborating with my former colleague Sven Puchinger. His insightful contributions and enthusiastic approach to research made him not only a great co-author but also a valued mentor in this formative phase.

Special appreciation is due to Johannes Pfeiffer, with whom I shared an office during the last phase of my time at Ulm University. The discussions we had, ranging from scientific topics to political and societal issues, were a true enrichment and turned this period into a very enjoyable and valuable experience.

I also wish to acknowledge my colleague Sven Müelich, who supported me especially in the early phase of my PhD, in particular with administrative and organizational matters. I also fondly recall our many interesting and humorous conversations, which made this time a truly pleasant experience.

I am grateful to Sebastian Stern for being not only a great co-author, but also an awesome travel companion and office mate.

My thanks also go to my former colleagues not mentioned yet: Sebastian Bitzer, Zaid Dhannoon, Günther Haas, Rebekka Schulz, Carmen Sippel, Susanne Sparrer, Elena Sterk, Werner Teich and George Yammine for the pleasant and collegial atmosphere we shared.

I would like to express my sincere gratitude to Lia (Hedongliang Liu) for our fruitful collaboration and for the inspiring time we shared during our joint research stays in Rennes. I am also deeply thankful for the time and care she devoted to proofreading parts of this thesis.

My heartfelt thanks also go to Felix Ulmer, for the time he devoted to Lia and me during our research stays in Rennes. I greatly appreciate all I learned from him about codes over rings, and I am equally thankful for the memorable experiences outside of research that he shared with Lia and me, such as our trip to the sea and his guided tour through Rennes. These moments made our stay an unforgettable time.

I also had the privilege of supervising students in their bachelor's and master's theses: Musab Ahmed Eltayeb Ahmed, Yulin Chen, Yvette Groner, and Josip Jelčić. Working with them was both enjoyable and rewarding.

Collaborating with my co-authors Martin Bossert, Robert Fischer, Cong Ling, Hedongliang Liu, Sven Puchinger, Carmen Sippel, Sebastian Stern, Felix Ulmer, and Antonia Wachter-Zeh, was both a privilege and an invaluable experience.

A special thanks goes to Hannes Bartz for his support during the final writing phase, especially for his careful proofreading and for giving me the opportunity to involve my colleagues in proofreading this work. My heartfelt thanks also go to my colleagues Giulia Cavicchioni, Felicitas Hörmann, Thomas Jerkovits, Luana Kurmann, Svenja Lage and Renate Ulla Schwank for their time, dedication, and the many helpful comments that have significantly contributed to the quality of this dissertation.

Finally, my heartfelt thanks go to my family, especially my parents Regina and Josef and my brothers Christian and Matthias, for their constant support, encouragement, and motivation.

Last but not least, I am infinitely grateful to my partner Johannes for his love and support.

Ulm, December 2025 Cornelia Ott

Abstract

This thesis explores error-correcting codes beyond the classical framework of linear codes over finite fields in the Hamming metric. Two different directions are pursued: first, codes defined over finite rings, which enrich the algebraic framework and enable constructions not possible over fields; and second, codes in the sum-rank metric, a distance measure that combines properties of the Hamming metric and rank metric and is increasingly relevant in applications such as multishot network coding, space-time coding, code-based cryptography and distributed storage. Together, these investigations uncover new structural phenomena and establish refined performance bounds for coding theory.

The first part considers cyclic left module codes over finite rings within the framework of skew polynomial rings. By transforming duality conditions from a set of differential equations into a system of multivariate polynomial equations solvable via Gröbner bases, dual-containing codes can be constructed algorithmically. The analysis reveals several special features: the dual of a cyclic module code is not necessarily cyclic, non-trivial endomorphisms and derivations are indispensable for certain constructions, and certain codes arise only in the presence of non-central modulus polynomials. These results extend the theory of codes over rings and might be of interest for the design of quantum error-correcting codes, where dual containment is essential.

The second part focuses on codes in the sum-rank metric. A geometric perspective is employed by analyzing spheres, balls, and their intersections, leading to efficiently computable volume bounds. Building upon this foundation, classical results such as the Gilbert–Varshamov, sphere-packing, and Singleton bounds are generalized to the sum-rank-metric setting for linear codes, and asymptotic variants are derived. It is shown that random linear codes achieve a Gilbert–Varshamov-like bound with high probability. Covering properties are also studied, yielding upper and lower bounds on code sizes for given covering radii. Overall, this part characterizes the trade-offs between redundancy and error-correcting capability and advances the algebraic and geometric understanding of error-correcting codes in the sum-rank-metric setting.

Contents

1. Introduction **1**

2. Preliminaries **5**
2.1. Foundational Terminology 5
2.1.1. Notation 5
2.1.2. Block Codes 6
2.1.3. Algebra 11
2.2. Codes in Various Metrics 13
2.2.1. Codes in the Hamming Metric 13
2.2.2. Codes in the Rank Metric 14
2.2.3. Codes in Sum-Rank Metric 14
2.3. Bounds on the Cardinality of Linear Codes in the Hamming Metric 18

Part I: Codes over Rings **23**

3. Dual-Containing Codes over Finite Commutative Rings **23**
3.1. Introduction 23
3.2. Algebraic Framework for (θ, δ)-Codes 24
3.2.1. Skew Polynomial Rings and Code Constructions 24
3.2.2. Cyclic Left Module (θ, δ)-Codes 27
3.3. Parity-Check Matrix and Generator Matrix of the Euclidean and Hermitian Dual Code 32
3.4. Computing All Dual-Containing (θ, δ)-Codes 36
3.4.1. Polynomial Maps 36
3.4.2. Computations via Gröbner Bases over a subalgebra 39
3.5. Computational Results for $\mathbb{F}_2[v]/(v^2 + v)$ 41
3.6. Computational Results for $\mathbb{F}_2[u]/(u^2)$ 46
3.7. Computational Results for $\mathbb{F}_4$ 48
3.8. Computational Results for the Galois Ring $GR(4, 2)$ 49

Part II: Codes in Sum-Rank Metric **53**

4. Properties of the Sum-Rank Metric **53**
4.1. The Connection Between the Sum-Rank Metric and Elementary Linear Subspaces . . . 53
4.2. Spheres and Balls in the Sum-Rank Metric . . . 57
4.2.1. The Volume of Spheres and Balls in the Sum-Rank Metric . . . 57
4.2.2. Bounds on the Volume of Sum-Rank-Metric Spheres and Balls . . . 59
4.2.3. The Intersection of Two Balls in Sum-Rank Metric . . . 61

5. Properties of Codes in the Sum-Rank Metric **71**
5.1. Bounds on the Cardinality of Codes in the Sum-Rank Metric . . . 72
5.1.1. A Singleton-Like Bound and MSRD Codes . . . 72
5.1.2. A Gilbert–Varshamov-Like Bound . . . 79
5.1.3. Sphere-Packing Bound . . . 83
5.1.4. Numerical Comparison of the Bounds . . . 84
5.2. Covering Properties of Codes in the Sum-Rank Metric . . . 86
5.2.1. Lower Bounds on the Minimum Cardinality of a Code for a Given Covering Radius . . . 90
5.2.2. Upper Bounds on the Minimum Cardinality of a Code for a Given Covering Radius . . . 94
5.2.3. Numerical Comparison of the Upper and Lower Bounds . . . 98

6. Conclusion **101**

A. List of Symbols and Acronyms **105**

Bibliography **109**

1

Introduction

When transmitting data from one location to another or storing data to access it later, errors occur, i.e., the transmitted data differs from the received data. In order to correct these errors, channel codes are used, which add redundancy before the transmission over a communication channel. In [Sha48] Shannon introduced the mathematical theory of information transmission over communication channels. He provided limits on how much redundancy must be added in order to transmit error-free asymptotically. One of the first error-correcting codes was introduced by Hamming in [Ham50] including the introduction of the so-called *Hamming metric*. Building on this early work, an important class of channel codes that has been extensively studied is that of block codes. Such a code $\mathcal{C}$ is generally defined over an alphabet Σ as a subset of Σ^n, where Σ^n denotes the set of all sequences of length n with entries from Σ. The elements of the code $\mathcal{C}$ are called *codewords* and have the same fixed length n. While the alphabet Σ can be any finite set, choosing a more structured alphabet provides additional algebraic properties that are beneficial for both encoding and decoding. In particular, selecting Σ to be a field allows for the definition of linear codes. In practice, Σ is typically taken to be a finite field, since linear codes over finite fields possess a rich algebraic structure and support efficient algorithms for error detection and correction. The distance between two codewords is measured with respect to a given metric. Different metrics are chosen depending on the code alphabet and the type of communication channel, as error patterns vary in different contexts. Therefore, the choice of the metric affects a code's ability to detect and correct errors. Usually the Hamming metric is employed, which is the natural metric for most communication channels. It measures the distance between two codewords by counting the number of positions in which they differ, thereby directly modeling the effect of symbol errors occurring independently at different positions during transmission. The so-called *minimum distance* of a code is then defined as the minimum of all distances between any two different codewords. One aim of channel coding is to construct codes that exhibit a large minimum distance, since this provides good error correcting properties.

This dissertation is divided into two parts. In the first part, we explore codes over finite rings, thereby extending the classical framework where codes are typically defined over finite fields. Working over rings allows for larger flexibility and broader construc-

tions, which can lead to codes with desirable properties not achievable over finite fields. Despite this generalization, we aim at retaining a similar level of algebraic structure. To that end, we focus on ring-linear codes. These codes preserve many of the advantages of linear codes over fields while enabling richer algebraic behavior and new design possibilities. In particular, we investigate codes over finite commutative rings using so-called *skew polynomial rings*. Building upon the framework introduced by Boucher, Geiselmann and Ulmer [BGU07], we study *cyclic left module codes* and analyze their duality and structural properties from an algebraic perspective. This enables the construction and classification of dual-containing and self-dual codes, which are especially relevant for applications in quantum error correction. To demonstrate the practicality of our approach, we give explicit examples over small commutative rings.

In the second part of this dissertation, we shift our focus from using of a more general code alphabet than a finite field, as explored in Part 1, to the consideration of a more general metric than the commonly used Hamming metric. Specifically, we study codes in the *sum-rank metric*, a distance measure that extends the classical Hamming metric by incorporating features of both the Hamming metric and the so-called *rank metric* within a unified framework. This facilitates the analysis of codes that exhibit properties of both metrics and offers insight into how these properties transition and interact in intermediate regimes. As a result, the sum-rank metric is particularly well suited to communication scenarios where neither the Hamming nor the rank metric alone is sufficient. The sum-rank metric is conceptually grounded in the rank metric, which was originally introduced by Hua [Hua45, Hua51] under the name *arithmetic distance*, and later independently adopted in coding theory by Gabidulin [Gab85], Delsarte [Del78], and Roth [Rot91]. The rank metric has since been shown to outperform the Hamming metric in various applications, such as network coding [GPB10, SKK08], space-time coding [GBL00, LGB03, PSBF16], and distributed data storage [SRV12]. For a comprehensive overview of the rank-metric and its applications, see [BHL22]. The sum-rank metric itself was first introduced in [LK05] in the context of space-time code design. Its potential for error control in non-coherent multishot network coding was later demonstrated by Nóbrega and Uchôa-Filho, who proposed a multilevel code construction in [NUF10]. This application area has since become one of the central motivations for studying sum-rank-metric codes. Beyond multishot network coding, sum-rank codes have found applications in distributed data storage [MPK19b], space-time coding [SK20], and are increasingly being explored for their potential in code-based quantum-resistant cryptography [PRR22]. A wide variety of code constructions have been developed within the sum-rank framework including partial unit memory codes constructed from rank-metric codes [WSBZ11], convolutional codes in the rank metric [WZSS15, NPRV17, NPRV], variable block-size constructions [BGLR21] and so-called *maximum sum-rank distance codes* (see [MP18]). In parallel, several decoding algorithms have been proposed for these codes, addressing both general and specific constructions (see [BJPR21, PRR22, HBP22, JBWZ24, HB24]). For a comprehensive overview of codes in the sum-rank metric, we refer to [MPSK22].

This dissertation contributes to the theoretical understanding of the sum-rank metric in two main directions. First, we investigate geometric properties of the sum-rank metric

itself. In particular, we study spheres and balls in the sum-rank space. This geometric perspective is not only of intrinsic interest, but also has direct implications for code design and performance bounds. Second, we examine fundamental properties of codes in the sum-rank metric, focusing on bounds on the cardinality of a code as well as covering properties of codes. These investigations are crucial for assessing the error-correcting capability and practical efficiency of sum-rank codes.

Outline

This dissertation is structured in six chapters, divided into two main parts.

Chapter 2 lays the theoretical groundwork by introducing the algebraic and coding-theoretic concepts used throughout this dissertation. We define the notation, formalize block codes over fields and rings, and explore structural properties such as linearity, duality, and cyclicity. Key concepts, including generator and parity-check matrices, are presented, as well as various representations of codes. Additionally, relevant algebraic foundations such as skew polynomials are introduced, and the Hamming, rank, and sum-rank metric are discussed. The chapter also reviews classical bounds on the cardinality of a code in the Hamming metric, which serve as a basis for later generalizations.

The remaining chapters contain new results. Most of these findings are already published: Hence, we give the corresponding references at the end of each chapter's introduction.

Chapter 3 starts Part I of the dissertation, which investigates linear codes over finite commutative rings. In particular, we study cyclic left module codes defined over skew polynomial rings. A key contribution is an algebraic framework that enables the construction of dual-containing and self-dual codes using Gröbner basis techniques. These results are particularly relevant for the design of quantum error-correcting codes. The chapter includes algorithms for testing duality, explores the role of nontrivial endomorphisms and derivations, and provides explicit code examples over small rings. Specifically, we perform explicit computations over all commutative rings of order four, as well as over the Galois ring $\mathrm{GR}(4, 2)$ of order 16.

Chapter 4 opens Part II, shifting the focus to the sum-rank metric as a generalization of both the Hamming and rank metric. The chapter introduces elementary linear subspaces as a powerful tool for analyzing sum-rank metric structures. We then investigate spheres and balls in the sum-rank metric, and provide both lower and upper bounds on their volume. In addition, we analyze the volume of the intersection of two balls, which plays a key role in the analysis of packing and covering problems. These geometric results are not only of theoretical interest but also provide essential foundations for the study of code performance.

Chapter 5 builds on the geometric insights of the previous chapter and focuses on the properties of codes in the sum-rank metric. Two main aspects are addressed: bounds on the cardinality of codes and their covering properties. Classical results such as the Singleton, Gilbert–Varshamov, and sphere-packing bound are extended to the sum-rank-metric setting. In addition, the chapter examines covering properties, establishing bounds on the cardinality of a sum-rank-metric code for a given covering radius as well as relation-

ships between the sum-rank, rank, and the Hamming metric. These findings contribute to a deeper understanding of code efficiency and error-correcting capability in practical applications.

Chapter 6 concludes the dissertation with a summary of the main contributions and a discussion of potential directions for future research.

2

Preliminaries

This chapter introduces the notation, algebraic concepts, as well as coding theoretic constructs and properties that will be used throughout this thesis. We begin in Section 2.1 by fixing the notational conventions used to describe finite fields, vectors, matrices, and vector spaces. Subsequently, we define the class of block codes with emphasis on those that exhibit linearity over rings and fields, and we explain their structural properties, such as generator and parity-check matrices, dual codes, as well as different code representations. In the latter part of this section, we introduce algebraic concepts that are fundamental to this thesis, including the notion of *skew polynomial rings* which generalize ordinary polynomial rings and provide the essential framework used for studying codes over rings in Part I of this thesis. In Section 2.2 we introduce the Hamming, rank, and sum-rank metric, providing the necessary background for Part II of the thesis, where we work with the sum-rank metric, a generalization of the Hamming and the rank metric. Finally, we conclude in Section 2.3 with classical bounds on the cardinality of linear codes in the Hamming metric, including the Singleton, sphere-packing, and Gilbert–Varshamov bound. We build on these results in Section 5.1, where we explore analogous bounds in the context of the sum-rank metric.

2.1. Foundational Terminology

2.1.1. Notation

We present the notation and concepts that will be utilized throughout this dissertation. A summary of the notation and associated abbreviations can be found in Appendix A. We denote by q a prime power, by m a positive integer, by $\mathbb{F}_q$ a finite field with q elements and by $\mathbb{F}_{q^m}$ its extension field with extension degree m. Vectors and matrices are represented using bold letters, while matrices are typically denoted with capital letters. Square brackets are employed to enclose elements of matrices, vectors, or tuples. Vectors are assumed to be indexed from 0, such as $\boldsymbol{v} = [v_0, ..., v_{n-1}]$ and are typically considered as row vectors. For $r \in \mathbb{N}^*$ we denote by $\langle \boldsymbol{v}_0, \dots, \boldsymbol{v}_{r-1} \rangle_{\mathbb{F}_q}$ the $\mathbb{F}_q$-linear vector space spanned by the vectors $\boldsymbol{v}_0, \dots, \boldsymbol{v}_{r-1}$. Let A be a ring. We denote by $A[X]$ the ring of polynomials in one indeterminate X with coefficients in A. For a polynomial $f \in A[X]$, we write $A[X]/(f)$ for the quotient ring of $A[X]$ by the ideal generated by f,

whose elements are equivalence classes of polynomials modulo f, that is,

$$A[X]/(f) = \{\, p + (f) \mid p \in A[X] \,\}.$$

2.1.2. Block Codes

Coding theory broadly distinguishes between two main types of codes: infinite-length codes and finite-length codes. The latter, commonly known as block codes, were first systematically studied with pioneering contributions by Golay [Gol49] and Hamming [Ham50]. This thesis focuses exclusively on block codes.

In this section, we present only the concepts essential for the developments presented in this work. Readers interested in a comprehensive treatment of error-correcting codes are referred to standard textbooks on coding theory, such as [Bos13], [MS77], and [Rot06].

Traditionally, codes are defined over finite fields, and the distance between codewords is measured using the so-called *Hamming metric*. In this thesis, however, we consider codes defined over more general alphabets and study metrics that extend the classical Hamming metric. Therefore, we begin with a general definition of a block code to establish the necessary foundations.

Definition 2.1 ($[n, M, d]$-Block Code)**.** Let Σ be a set, n a positive integer and let Σ^n be the set of all sequences of length n whose elements come from Σ, that is,

$$\Sigma^n = \{(a_0, a_2, \ldots, a_{n-1}) \mid a_i \in \Sigma \text{ for all } i = 0, \ldots, n-1\}.$$

Let $d \in \mathbb{N}_0$ and $\mathrm{d} : \Sigma^n \times \Sigma^n \to \mathbb{Z}_+$ a metric [1]. We define a *block code* $\mathcal{C}$ of length n, cardinality M and minimum distance d as

$$\mathcal{C} \coloneqq \Big\{ \boldsymbol{c}^{(1)}, \ldots, \boldsymbol{c}^{(M)} \in \Sigma^n \mid \min_{\substack{\boldsymbol{c}^{(i)} \neq \boldsymbol{c}^{(j)} \\ i,j \in \{1,\ldots,M\}}} \{\mathrm{d}(\boldsymbol{c}^{(i)}, \boldsymbol{c}^{(j)})\} = d \Big\}.$$

Its elements $\boldsymbol{c} = [c_0, \ldots, c_{n-1}] \in \mathcal{C}$ are called *codewords* and Σ is called the *code alphabet*.

In this thesis, we denote by $\mathcal{C}$ a block code and by n and d positive integers that correspond to the length and the minimum distance of a code, respectively.

2.1.2.1. Structure of Codes

In this work, we restrict ourselves to codes whose code alphabet Σ has at least a ring structure and whose codewords are elements of a so-called *free module*. A module is a generalization of a vector space in which the scalars are taken from a (unitary) ring rather than a field. While concepts such as scalar multiplication, linear combinations, linear dependence and generating sets extend naturally from vector spaces to modules, the existence of a basis is no longer guaranteed for arbitrary modules. A module is called

[1] i.e., $\mathrm{d}(\boldsymbol{x}, \boldsymbol{y}) \geq 0$, $\mathrm{d}(\boldsymbol{x}, \boldsymbol{y}) = 0 \Leftrightarrow \boldsymbol{x} = \boldsymbol{y}$, $\mathrm{d}(\boldsymbol{x}, \boldsymbol{y}) = \mathrm{d}(\boldsymbol{y}, \boldsymbol{x})$, and $\mathrm{d}(\boldsymbol{x}, \boldsymbol{z}) \leq \mathrm{d}(\boldsymbol{x}, \boldsymbol{y}) + \mathrm{d}(\boldsymbol{y}, \boldsymbol{z})$ for all $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in \Sigma^n$.

free if it possesses a basis, i.e., if it is isomorphic to a direct sum of copies of the ring which we denote by Σ^n for a given code length n. In the following, we initially posit that the free module is not only isomorphic but identical to Σ^n. Later in this section, we will explore alternative representations of codewords, resulting in modules that are isomorphic but not necessarily identical to Σ^n.

(Ring-)Linearity If a code, denoted as $\mathcal{C}$, constitutes a free submodule within a free module over a ring A (e.g., a subspace of a vector space over a field $\mathcal{K}$), then we refer to the code as *ring-linear* or just *linear*, if A is a field. For such codes, we employ the parameters $[n, k, d]$, where n and d correspond, as usual, to the codeword length and the minimum distance, respectively. The parameter k signifies the rank of the code as a submodule of the underlying ring A or rather, the dimension of the code as a subspace of the underlying field $\mathcal{K}$. This motivates the definition of a *ring-linear code*, as a specific case of a block code as outlined in Definition 2.1.

Definition 2.2 ((Ring-)Linear $[n, k, d]$-Code)**.** Let Σ be a ring and let n be a positive integer. A *(ring-)linear code* of *length* n over Σ is a subset $\mathcal{C} \subseteq \Sigma^n$ that forms a free Σ-submodule. If Σ is a field, then $\mathcal{C}$ is simply called a *linear code*, and its elements are Σ-linear combinations of k linearly independent codewords. The *dimension* of the code is the rank of the submodule, denoted $k \coloneqq \mathrm{rk}_\Sigma(\mathcal{C}) \in \mathbb{N}_0$. The cardinality of the code is then $|\mathcal{C}| = |\Sigma|^k$. Let $\mathrm{d} : \Sigma^n \times \Sigma^n \to \mathbb{Z}_+$ be a metric. The *minimum distance* of the code $\mathcal{C}$ is defined as

$$d \coloneqq \min_{\mathbf{c} \neq \mathbf{c}' \in \mathcal{C}} \mathrm{d}(\mathbf{c}, \mathbf{c}') \,.$$

The *rate* of the code is given by $R \coloneqq \frac{k}{n}$.

Cyclic Codes

Definition 2.3 (Cyclic Shift)**.** Let $\boldsymbol{c} = [c_0, c_1, \ldots, c_{n-1}] \in \mathbb{F}_q^n$ be a vector over a finite field $\mathbb{F}_q$. The *cyclic shift* of $\boldsymbol{c}$ by i positions is the vector

$$\sigma_i(\boldsymbol{c}) \coloneqq [c_i, \ldots, c_{n-1}, c_0, c_1, \ldots, c_{i-1}].$$

Definition 2.4 (Cyclic Code)**.** A linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is called a *cyclic code* if it is closed under the cyclic shift operation; that is, for every $\boldsymbol{c} \in \mathcal{C}$, any cyclic shift $\sigma_i(\boldsymbol{c})$ is also in $\mathcal{C}$.

2.1.2.2. Generator Matrix

Let $\mathcal{C} \subseteq \Sigma^n$ be a (ring-)linear $[n, k, d]$-code. Since $\mathcal{C}$ is a free Σ-submodule of rank k, it admits a basis $\mathcal{B} = \{\mathbf{b}_0, \ldots, \mathbf{b}_{k-1}\}$ over Σ. By arranging the basis vectors as the rows

of a matrix, we obtain a *generator matrix* of the code:

$$\boldsymbol{G} \coloneqq \begin{bmatrix} \mathbf{b}_0 \\ \vdots \\ \mathbf{b}_{k-1} \end{bmatrix} \in \Sigma^{k \times n}.$$

Each codeword $\mathbf{c} \in \mathcal{C}$ can be expressed as a linear combination of the basis vectors, which means that every codeword is of the form

$$\mathbf{c} = \mathbf{m} \cdot \boldsymbol{G},$$

where $\mathbf{m} \in \Sigma^k$ is a message vector. The generator matrix thus defines a Σ-linear map

$$\Sigma^k \to \Sigma^n, \quad \mathbf{m} \mapsto \mathbf{m} \cdot \boldsymbol{G},$$

whose image is exactly the code $\mathcal{C}$.

In summary, the generator matrix encodes a message by specifying a basis, and it provides a direct method for mapping message vectors to codewords.

2.1.2.3. Duality of Codes

In coding theory, the concept of duality plays a central role in understanding the structure and properties of codes. Given a linear code over a ring or field, its dual code consists of all vectors orthogonal to the original code under a specified inner product. The two most common notions of duality are based on the Euclidean and Hermitian inner products.

Definition 2.5 (Euclidean Dual)**.** Let A be a commutative ring and $\mathcal{C} \subseteq A^n$ a linear code. The *Euclidean inner product* of two vectors $\boldsymbol{x} = [x_0, \ldots, x_{n-1}]$ and $\boldsymbol{y} = [y_0, \ldots, y_{n-1}]$ in A^n is defined by

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle \coloneqq \sum_{i=0}^{n-1} x_i y_i \,.$$

The *Euclidean dual code* of $\mathcal{C}$ is the set

$$\mathcal{C}^{\perp} \coloneqq \{\boldsymbol{v} \in A^n \mid \langle \boldsymbol{v}, \boldsymbol{c} \rangle = 0 \text{ for all } \boldsymbol{c} \in \mathcal{C}\} \,.$$

We also use the notation $\langle \cdot, \cdot \rangle$ to denote the linear span. The intended meaning will always be clear from the context. When A is equipped with a nontrivial automorphism of order dividing 2, we can generalize this concept using the Hermitian inner product.

Definition 2.6 (Hermitian Inner Product and Dual)**.** Let σ be an automorphism of a ring A such that $\sigma^2 = \mathrm{id}$. The *σ-Hermitian inner product* of vectors $\boldsymbol{x}, \boldsymbol{y} \in A^n$ is defined as

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle_{\sigma} \coloneqq \sum_{i=0}^{n-1} x_i \sigma(y_i).$$

The *σ-Hermitian dual code* of a code $\mathcal{C} \subseteq A^n$ is given by

$$\mathcal{C}^{\perp_\sigma} \coloneqq \{\boldsymbol{v} \in A^n \mid \langle \boldsymbol{v}, \boldsymbol{c} \rangle_\sigma = 0 \text{ for all } \boldsymbol{c} \in \mathcal{C}\}.$$

A code $\mathcal{C}$ is called σ-self-orthogonal if $\mathcal{C} \subseteq \mathcal{C}^{\perp_\sigma}$, and σ-dual-containing if $\mathcal{C} \supseteq \mathcal{C}^{\perp_\sigma}$. If both inclusions hold, i.e., $\mathcal{C} = \mathcal{C}^{\perp_\sigma}$, the code is called σ-self-dual. In other words, self-orthogonal codes are contained in their duals, dual-containing codes contain their duals, and self-dual codes are equal to their duals.

If $\sigma = \mathrm{id}$ is the identity automorphism, the Hermitian inner product reduces to the Euclidean one, and the corresponding dual code coincides with the Euclidean dual. In this case, we typically omit the subscript σ in the notation.

2.1.2.4. Parity-Check Matrix

Let $\mathcal{C} \subseteq \Sigma^n$ be a (ring-)linear code. If the dual code $\mathcal{C}^\perp$ (or more generally, $\mathcal{C}^{\perp_\sigma}$) is a *free* Σ-submodule of Σ^n of rank $n-k$, then it admits a basis consisting of $n-k$ vectors. In this case, we can represent the dual code using a matrix $\boldsymbol{G}^\perp \in \Sigma^{(n-k)\times n}$, whose rows form a basis of the dual code, i.e., a generator matrix of $\mathcal{C}^\perp$.

A *parity-check matrix* is a matrix $\boldsymbol{H} \in \Sigma^{(n-k)\times n}$ that characterizes the code $\mathcal{C}$ via the orthogonality condition

$$\boldsymbol{H} \cdot \mathbf{c}^\top = \mathbf{0} \quad \text{if and only if } \mathbf{c} \in \mathcal{C}.$$

Equivalently, $\mathcal{C}$ can be described as the kernel of the Σ-linear map defined by $\boldsymbol{H}$:

$$\mathcal{C} = \ker(\boldsymbol{H}) = \left\{\mathbf{c} \in \Sigma^n \;\middle|\; \boldsymbol{H} \cdot \mathbf{c}^\top = \mathbf{0}\right\}.$$

If Σ is a field, the existence of such a parity-check matrix is guaranteed. Moreover, every parity-check matrix is a generator matrix of the dual code, i.e., $\boldsymbol{H} = \boldsymbol{G}^\perp$. Over a general ring, however, the existence of a parity-check matrix is not guaranteed. Even if $\mathcal{C}^\perp$ is free and admits a generator matrix $\boldsymbol{G}^\perp$, it does not necessarily hold that $\mathcal{C} = \ker(\boldsymbol{G}^\perp)$.

When the Hermitian inner product is used instead of the Euclidean inner product, the same principle applies.

2.1.2.5. Representation of Codewords

In this thesis, we use different representations of codeswords.

- Representation of codewords as vectors:

  For a code $\mathcal{C}$ with alphabet Σ, a codeword is typically represented as a vector of length n, that is, $\mathbf{c} = [c_0, c_1, \ldots, c_{n-1}] \in \mathcal{C} \subseteq \Sigma^n$.

- Representation of codewords as matrices:

  If the code alphabet Σ is a free module over a ring A of rank $m \geq 1$, such as a vector space $\mathcal{K}^m$ over a field $\mathcal{K}$ of dimension $m \geq 1$, one can also represent the

codewords as matrices. In order to represent for a example a vector $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$ as a matrix $\boldsymbol{V} \in \mathbb{F}_q^{m\times n}$, we define a mapping. Let therefore $\mathcal{B} \coloneqq \{b_0, \dots, b_{m-1}\}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. The fundamental property that every element $\alpha \in \mathbb{F}_{q^m}$ can be expressed as a linear combination $\alpha = \sum_{i=0}^{m-1} \alpha_i b_i$ with $\alpha_i \in \mathbb{F}_q$ for all $i \in \{0, \dots, m-1\}$, enables us to define the following mapping:

$$\mathrm{ext}_{\mathcal{B}} : \mathbb{F}_{q^m}^n \to \mathbb{F}_q^{m\times n},$$

$$\boldsymbol{v} = [v_0, \dots, v_{n-1}] = \left[\sum_{i=0}^{m-1} V_{i,0} b_i, \dots, \sum_{i=0}^{m-1} V_{i,n-1} b_i\right] \mapsto \boldsymbol{V} = \begin{bmatrix} V_{0,0} & \cdots & V_{0,n-1} \\ \vdots & \ddots & \vdots \\ V_{m-1,0} & \cdots & V_{m-1,n-1} \end{bmatrix}.$$

This representation of codewords is particularly useful, for example, when measuring the distances between codewords in the rank and the sum-rank metric. In this context we refer to the rank of a vector $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$ as the rank of its corresponding matrix $\boldsymbol{V} = \mathrm{ext}_{\mathcal{B}}(\boldsymbol{v})$, in other words:

$$\mathrm{rk}_{\mathbb{F}_q}(\boldsymbol{v}) \coloneqq \mathrm{rk}(\mathrm{ext}_{\mathcal{B}}(\boldsymbol{v})) = \mathrm{rk}(\boldsymbol{V})$$

for a given basis $\mathcal{B}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Note, that the rank does not depend on the choice of the basis $\mathcal{B}$.

- Representation of codewords as polynomials:

  In addition to their standard vector representation, codewords are often represented as polynomials. While this representation is commonly associated with evaluation codes, where codewords arise from evaluating polynomials at a prescribed set of points, it is by no means limited to them. In many broader settings, such as cyclic codes, skew polynomial codes, or module codes over rings, codewords are naturally expressed as polynomial objects.

  Let A be a ring, $f \in A[X]$ a polynomial of degree n (commonly $f = X^n - 1$ is used) and let $\mathbf{c} = [c_0, c_1, \dots, c_{n-1}] \in A^n$ be a codeword. We associate $\mathbf{c}$ with the polynomial

  $$c(X) = c_0 + c_1 X + c_2 X^2 + \cdots + c_{n-1} X^{n-1} \in A[X]/(f).$$

  This defines a natural isomorphism between the A-module A^n and the subspace of polynomials in $A[X]$ of degree less than n:

  $$\varphi : A^n \longrightarrow A[X]/(f), \quad \varphi([c_0, \dots, c_{n-1}]) = \sum_{i=0}^{n-1} c_i X^i.$$

  The inverse map simply recovers the vector by extracting the coefficients of the polynomial. This representation is frequently used in coding theory, particularly in the study of cyclic, skew, and module codes.

There exist alternative representations of codewords, which will not be explored within the scope of this thesis.

2.1.2.6. Generator Polynomials and the Ideal Structure of a Code

The polynomial representation of codes allows us to model codes as ideals. This approach is particularly useful when working with cyclic codes, where the generator and parity-check properties can be described using divisibility in polynomial rings.

Classical Case: Codes over Finite Fields A cyclic code over $\mathbb{F}_q$ corresponds to an ideal in the ring $\mathbb{F}_q[X]/(X^n-1)$. Since this ring is a principal ideal ring, any ideal is generated by a single polynomial $g(X)$:

$$\mathcal{C} = \langle g(X) \rangle \subseteq \mathbb{F}_q[X]/(X^n - 1),$$

where $g(X)$ is a monic divisor of $X^n - 1$ and is called the *generator polynomial* of the code. Every codeword in $\mathcal{C}$ is a multiple of $g(X)$:

$$\mathcal{C} = \{a(X)g(X) \mod (X^n - 1) \mid a(X) \in \mathbb{F}_q[X]\}.$$

Codes over Finite Rings When the alphabet is a finite ring A, we can generalize the above by considering $R = A[X]/(X^n - 1)$. A cyclic code is then an ideal in R. If R is a principal ideal ring, then the code is again generated by a single polynomial. However, complications arise due to the presence of zero divisors and the fact that not all submodules are free or principal.

2.1.3. Algebra

This subsection introduces algebraic tools and notations that are fundamental to the results presented in this dissertation. We begin with basic combinatorial quantities used throughout the work. We then recall the definition of generalized q-Krawtchouk polynomials. Finally, we introduce a generalization of classical polynomial rings known as Ore (or skew) polynomial rings.

2.1.3.1. Combinatorial Quantities

The q-ary Gaussian binomial coefficient, also called the q-binomial coefficient represents the number of t-dimensional subspaces of $\mathbb{F}_q^n$ and is given by

$$\begin{bmatrix} n \\ t \end{bmatrix}_q = \begin{cases} \prod_{i=1}^{t} \frac{(1-q^{n-i+1})}{(1-q^i)}, & \text{if } t \leq n \\ 0, & \text{else.} \end{cases} \tag{2.1}$$

The number of $m \times n$ matrices over $\mathbb{F}_q$ of rank t is denoted by $\mathrm{NM}_q(m, n, t)$. The exact number is (see e.g. [MMO04]):

$$\mathrm{NM}_q(m, n, t) = \begin{bmatrix} n \\ t \end{bmatrix}_q \cdot \prod_{i=0}^{t-1} (q^m - q^i). \tag{2.2}$$

Furthermore, we define

$$\gamma_q := \prod_{i=1}^{\infty} (1 - q^{-i})^{-1}. \tag{2.3}$$

Note, that γ_q is monotonically decreasing in q with a limit of 1, and e.g. $\gamma_2 \approx 3.463$, $\gamma_3 \approx 1.785$, and $\gamma_4 \approx 1.452$.

2.1.3.2. Generalized q-Krawtchouk Polynomials

For $q, c \in \mathbb{Q}$, $q > 1, c > \frac{1}{q}$, $n \in \mathbb{N}_0$ and $\delta \in \{0, 1, \ldots, n\}$ the generalized q-Krawtchouk polynomial was defined in [Del76] as

$$\mathfrak{K}_\delta(X, n) := \sum_{j=0}^{\delta} (-1)^{\delta - j} \left(cq^n\right)^j q^{\binom{\delta - j}{2}} \begin{bmatrix} n - j \\ n - \delta \end{bmatrix}_q \begin{bmatrix} n - X \\ j \end{bmatrix}_q .$$

2.1.3.3. Ore Polynomials

Skew polynomial rings were introduced and studied by Øystein Ore in [Ore33]. Subsequently, we give the relevant definitions and notations used throughout this work.

Definition 2.7 (Derivation)**.** Let $A \neq \{0\}$ be a unitary ring, and let $\theta \colon A \to A$ be a ring endomorphism. A map $\delta \colon A \to A$ is called a **θ-derivation** if, for all $a, b \in A$, the following conditions hold:

$$\delta(a + b) = \delta(a) + \delta(b) \quad \text{and} \quad \delta(ab) = \delta(a)b + \theta(a)\delta(b).$$

A θ-derivation δ is said to be an **inner θ-derivation** if there exists an element $\beta \in A$ such that

$$\delta(X) = \beta X - \theta(X)\beta, \quad \text{for all } X \in A.$$

In particular, for $\beta = 0$ we obtain the zero derivation which is denoted by 0.

Throughout this thesis, we will use exponential notation for convenience: $\theta(a) = a^\theta$ and $\delta(a) = a^\delta$.

Definition 2.8. (Skew Polynomial Ring) Let $A \neq \{0\}$ be a unitary ring, $\theta \colon A \to A$ a ring endomorphism, and $\delta \colon A \to A$ a θ-derivation. The **skew polynomial ring** $A[X; \theta, \delta]$ is defined as the set of (left) polynomials

$$A[X; \theta, \delta] := \left\{ \sum_{i=0}^{n} a_i X^i \,\middle|\, a_i \in A,\, n \in \mathbb{N} \right\},$$

with addition given by the usual polynomial addition, and multiplication defined by the rule

$$Xa = a^\theta X + a^\delta, \quad \text{for all } a \in A,$$

extended to $A[X; \theta, \delta]$ by associativity and distributivity.

2.2. Codes in Various Metrics

The concept of distance is fundamental in mathematics, providing a measure of how "far apart" objects are within a given space. In coding theory, different metrics are used for different code alphabets and communication channels to capture different types of errors and are tailored to the structure and behavior of the underlying channel. This is due to the fact, that different channels introduce different error patterns (e.g., random symbol errors, burst errors, linear combinations of signals). The choice of the metric directly impacts the error detection and correction capabilities of a code and is crucial for designing efficient error-correcting codes and ensuring optimal performance. In this context, two fundamental concepts are necessary:

(i) A norm, measuring the weight wt of a vector.

(ii) A metric d, which measures the distance between two vectors.

A metric d on a vector space (or module) is called *translation invariant* if

$$\mathrm{d}(x, y) = \mathrm{d}(x - y, 0) \quad \text{for all } x, y.$$

Equivalently, the distance between two vectors depends only on their difference. If a code $\mathcal{C}$ is linear and the underlying metric is translation invariant, then the minimum weight of the code $\mathcal{C}$ is equal to its minimum distance:

$$\min_{\substack{\boldsymbol{c},\boldsymbol{c}'\in\mathcal{C}\\ \boldsymbol{c}\neq\boldsymbol{c}'}}\{\mathrm{d}(\boldsymbol{c},\boldsymbol{c}')\} = \min_{\substack{\boldsymbol{c},\boldsymbol{c}'\in\mathcal{C}\\ \boldsymbol{c}\neq\boldsymbol{c}'}}\{\mathrm{wt}(\boldsymbol{c}'-\boldsymbol{c})\} \overset{\boldsymbol{c}'=\boldsymbol{c}_0+\boldsymbol{c}}{=} \min_{\substack{\boldsymbol{c},\boldsymbol{c}_0\in\mathcal{C}\\ \boldsymbol{c}_0\neq 0}}\{\mathrm{wt}(\boldsymbol{c}+\boldsymbol{c}_0-\boldsymbol{c})\} = \min_{\substack{\boldsymbol{c}_0\in\mathcal{C}\\ \boldsymbol{c}_0\neq 0}}\{\mathrm{wt}(\boldsymbol{c}_0)\}.$$

In the following we introduce three different metrics that are essential throughout this work: the Hamming metric, the rank metric and the sum-rank metric.

2.2.1. Codes in the Hamming Metric

We use the so-called *Hamming metric* for block codes over finite fields for discrete memoryless channels where errors typically affect individual symbols independently.

Definition 2.9 (Hamming Weight and Distance)**.** Let $\boldsymbol{x} = [x_0, \ldots, x_{n-1}]$ and $\boldsymbol{y} = [y_0, \ldots, y_{n-1}] \in \mathbb{F}_q^n$. The *Hamming weight* is defined as:

$$\mathrm{wt_H} : \mathbb{F}_q^n \to \mathbb{N}_0, \quad \boldsymbol{x} \mapsto |\{i \mid x_i \neq 0, 0 \leq i \leq n-1\}|.$$

The *Hamming distance* between $\boldsymbol{x}$ and $\boldsymbol{y}$ is given by:

$$\mathrm{d_H} : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{N}_0, \quad (\boldsymbol{x}, \boldsymbol{y}) \mapsto |\{i \mid x_i \neq y_i, 0 \leq i \leq n-1\}|.$$

Based on the Hamming weight and Hamming distance introduced in Definition 2.9, we now define block codes with respect to the Hamming metric.

Definition 2.10 (Hamming-Metric Code)**.** A linear $[n, k, d]$ Hamming-metric code $\mathcal{C}$ over $\mathbb{F}_q$ is an $\mathbb{F}_q$-linear subspace $\mathcal{C} \subseteq \mathbb{F}_q^n$ with $\dim_{\mathbb{F}_q}(\mathcal{C}) = k$. Consequently, the code has cardinality $|\mathcal{C}| = q^k$.

The minimum Hamming distance d of $\mathcal{C}$ is defined as

$$d \coloneqq \min_{\boldsymbol{x} \neq \boldsymbol{y} \in \mathcal{C}} \{\mathrm{d_H}(\boldsymbol{x}, \boldsymbol{y})\} = \min_{\boldsymbol{x} \in \mathcal{C} \setminus \{\boldsymbol{0}\}} \{\mathrm{wt_H}(\boldsymbol{x})\}.$$

2.2.2. Codes in the Rank Metric

We employ the *rank metric* in linear spaces over extension fields for channels with structured noise, such as random linear network coding or multiple-input multiple-output (MIMO) systems, where errors affect entire vector spaces rather than individual symbols, making rank-based metrics more appropriate.

Definition 2.11 (Rank Weight and Distance)**.** Let $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$. The *rank weight* of $\boldsymbol{x}$ is defined by

$$\mathrm{wt_R} : \mathbb{F}_{q^m}^n \to \mathbb{N}_0, \quad \boldsymbol{x} \mapsto \dim(\langle x_0, \ldots, x_{n-1} \rangle_{\mathbb{F}_q}) = \mathrm{rk}_{\mathbb{F}_q}\Big(\mathrm{ext}_{\mathcal{B}}(\boldsymbol{x})\Big),$$

for an arbitrary basis $\mathcal{B} = \{\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{m-1}\}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. For two vectors $\boldsymbol{x}, \boldsymbol{x}' \in \mathbb{F}_{q^m}^n$ the *rank distance* is defined by

$$\mathrm{d_R} : \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n \to \mathbb{N}_0, \quad (\boldsymbol{x}, \boldsymbol{x}') \mapsto \mathrm{wt_R}(\boldsymbol{x} - \boldsymbol{x}').$$

Based on the rank weight and rank distance introduced in Definition 2.11, one can consider different classes of rank-metric codes. In the following, we define rank-metric codes that are linear over the extension field $\mathbb{F}_{q^m}$.

Definition 2.12 ($\mathbb{F}_{q^m}$-linear Rank-Metric Code)**.** An $\mathbb{F}_{q^m}$-linear $[n, k, d]$ rank-metric code $\mathcal{C}$ is an $\mathbb{F}_{q^m}$-subspace $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ with $\dim_{\mathbb{F}_{q^m}}(\mathcal{C}) = k$. Consequently, the code has cardinality $|\mathcal{C}| = q^{mk}$.

The minimum rank distance d of $\mathcal{C}$ is defined as

$$d \coloneqq \min_{\boldsymbol{x} \neq \boldsymbol{x}' \in \mathcal{C}} \{\mathrm{d_R}(\boldsymbol{x}, \boldsymbol{x}')\} = \min_{\boldsymbol{x} \in \mathcal{C} \setminus \{\boldsymbol{0}\}} \{\mathrm{wt_R}(\boldsymbol{x})\}.$$

2.2.3. Codes in Sum-Rank Metric

The sum-rank metric is a hybrid metric that is useful for channels where errors exhibit both rank and Hamming-type behavior, such as multi-block transmission in distributed storage and space-time coding. In this dissertation, when discussing sum-rank-metric codes, we primarily consider linear codes over $\mathbb{F}_{q^m}$. In this subsection, we introduce these codes, starting with the definition of the sum-rank weight and distance.

Definition 2.13 (Sum-Rank Weight and Distance)**.** Let ℓ and η be positive integers and $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$. We split the vector $\boldsymbol{x}$ into ℓ equal-sized blocks of length η. Hence,

$\boldsymbol{x} = [\boldsymbol{x}_0|\dots|\boldsymbol{x}_{\ell-1}] \in \mathbb{F}_{q^m}^n$ with $\boldsymbol{x}_i = [x_{i_0}, \dots, x_{i_{\eta-1}}] \in \mathbb{F}_{q^m}^\eta$ for all $i \in \{0, \dots, \ell-1\}$ and we have the relation $\eta \cdot \ell = n$. The *ℓ-sum-rank weight* of $\boldsymbol{x}$ is defined by

$$\mathrm{wt}_{SR,\ell} : \mathbb{F}_{q^m}^n \to \mathbb{N}_0, \quad \boldsymbol{x} \mapsto \sum_{i=0}^{\ell-1} \dim(\langle x_{i_0}, \dots, x_{i_{\eta-1}} \rangle_{\mathbb{F}_q}) = \sum_{i=0}^{\ell-1} \mathrm{rk}_{\mathbb{F}_q}\Big(\mathrm{ext}_{\mathcal{B}}(\boldsymbol{x}_i)\Big),$$

for an arbitrary basis $\mathcal{B} = \{\boldsymbol{b}_0, \dots, \boldsymbol{b}_{m-1}\}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. For two vectors $\boldsymbol{x}, \boldsymbol{x}' \in \mathbb{F}_{q^m}^n$ the *ℓ-sum-rank distance* is defined by

$$\mathrm{d}_{SR,\ell} : \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n \to \mathbb{N}_0, \quad (\boldsymbol{x}, \boldsymbol{x}') \mapsto \mathrm{wt}_{SR,\ell}(\boldsymbol{x} - \boldsymbol{x}').$$

Obviously it holds for $\boldsymbol{x}_i \in \mathbb{F}_{q^m}^\eta$ that $\mathrm{rk}_{\mathbb{F}_q}(\boldsymbol{x}_i) = \dim(\langle x_{i_0}, \dots, x_{i_{\eta-1}} \rangle_{\mathbb{F}_q}) \in \{0, \dots, \mu\}$, with $\mu \coloneqq \min\{m, \eta\}$. When considering an arbitrary subspace $\mathcal{V} \subset \mathbb{F}_{q^m}^n$, the ($\ell$-)sum-rank distance of a vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^n \setminus \mathcal{V}$ to the subspace $\mathcal{V}$ is defined as the (ℓ-)sum-rank distance of $\boldsymbol{x}$ to the closest vector in $\mathcal{V}$, i.e.,

$$\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \mathcal{V}) = \min_{\boldsymbol{v} \in \mathcal{V}} \{\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \boldsymbol{v})\}.$$

There exist more general definitions, allowing for varying block sizes and even different extension degrees of the blocks (see e.g. [BGLR21]). However, in this work, we focus specifically on the definition given in Definition 2.13.

Throughout this dissertation we denote by ℓ the number of blocks of a vector $\boldsymbol{x} = [\boldsymbol{x}_0|\dots|\boldsymbol{x}_{\ell-1}] \in \mathbb{F}_{q^m}^n$, by η the size of each block $\boldsymbol{x}_i$ fulfilling the relation $n = \eta \cdot \ell$ and by μ we denote the minimum of the extension degree m and the blocksize η. To analyze the structure of vectors in the sum-rank metric, we introduce the concept of the sum-rank weight decomposition. This decomposition provides a finer characterization of vectors beyond their total sum-rank weight. The following definition formalizes this concept.

Definition 2.14 (Sum-Rank Weight Decomposition)**.** Let $\boldsymbol{v} = [\boldsymbol{v}_0|\dots|\boldsymbol{v}_{\ell-1}] \in \mathbb{F}_{q^m}^n$ with $\boldsymbol{v}_i \in \mathbb{F}_{q^m}^\eta$. The sum-rank weight decomposition of $\boldsymbol{v}$ is given by the vector

$$[\mathrm{rk}_{\mathbb{F}_q}(\boldsymbol{v}_0), \dots, \mathrm{rk}_{\mathbb{F}_q}(\boldsymbol{v}_{\ell-1})],$$

where $\mathrm{rk}_{\mathbb{F}_q}(\boldsymbol{v}_i) \in \mathbb{N}_0$ is at most μ for all $i \in \{0, \dots, \ell-1\}$.

In the following proposition, we recall the fundamental property that the sum-rank distance defines a metric.

Proposition 2.15 ([MPSK22])**.** *The sum-rank distance constitutes a metric.*

Proof. To demonstrate that the sum-rank distance defined in Definition 2.13 is indeed a metric, we verify that it satisfies the three fundamental axioms of a metric for any $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \mathbb{F}_{q^m}^n$:

(i) Positive Definiteness: $\mathrm{d}_{SR,\ell}(\boldsymbol{a}, \boldsymbol{b}) \geq 0 \quad \wedge \quad \mathrm{d}_{SR,\ell}(\boldsymbol{a}, \boldsymbol{b}) = 0$, if and only if $\boldsymbol{a} = \boldsymbol{b}$.

(ii) Symmetry: $\mathrm{d}_{SR,\ell}(\boldsymbol{a}, \boldsymbol{b}) = \mathrm{d}_{SR,\ell}(\boldsymbol{b}, \boldsymbol{a})$.

(iii) Triangle Inequality: $\mathrm{d}_{SR,\ell}(\boldsymbol{a},\boldsymbol{b}) + \mathrm{d}_{SR,\ell}(\boldsymbol{b},\boldsymbol{c}) \geq \mathrm{d}_{SR,\ell}(\boldsymbol{a},\boldsymbol{c})$.

We split the vectors $\boldsymbol{a}$, $\boldsymbol{b}$ and $\boldsymbol{c}$ into ℓ blocks:

$$\boldsymbol{a} = [\boldsymbol{a}_0|\ldots|\boldsymbol{a}_{\ell-1}], \quad \boldsymbol{b} = [\boldsymbol{b}_0|\ldots|\boldsymbol{b}_{\ell-1}], \quad \boldsymbol{c} = [\boldsymbol{c}_0|\ldots|\boldsymbol{c}_{\ell-1}].$$

Let $\mathcal{B} = \{\beta_1, \ldots, \beta_m\}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Since the rank of a matrix is always non-negative and is zero only if the matrix is the zero matrix, we have:

$$\mathrm{d}_{SR,\ell}(\boldsymbol{a},\boldsymbol{b}) = \mathrm{wt}_{SR,\ell}(\boldsymbol{b}-\boldsymbol{a}) = \sum_{i=0}^{\ell-1} \mathrm{rk}_{\mathbb{F}_q}\Big(\mathrm{ext}_{\mathcal{B}}(\boldsymbol{b}_i - \boldsymbol{a}_i)\Big) \geq 0,$$

where equality is fulfilled if and only if the matrix $\mathrm{ext}_{\mathcal{B}}(\boldsymbol{b}_i - \boldsymbol{a}_i)$ is the zero matrix for each $i \in \{0,\ldots,\ell-1\}$, which implies $\boldsymbol{a} = \boldsymbol{b}$. This establishes property (i). As $\mathrm{ext}_{\mathcal{B}}(\cdot)$ is an $\mathbb{F}_q$-linear mapping and since the rank of a matrix remains unchanged under multiplication by -1, we obtain:

$$\begin{aligned}
\mathrm{d}_{SR,\ell}(\boldsymbol{a},\boldsymbol{b}) = \mathrm{wt}_{SR,\ell}(\boldsymbol{b}-\boldsymbol{a}) &= \sum_{i=0}^{\ell-1} \mathrm{rk}_{\mathbb{F}_q}\Big(\mathrm{ext}_{\mathcal{B}}(\boldsymbol{b}_i - \boldsymbol{a}_i)\Big) = \sum_{i=0}^{\ell-1} \mathrm{rk}_{\mathbb{F}_q}\Big(\mathrm{ext}_{\mathcal{B}}(\boldsymbol{b}_i) - \mathrm{ext}_{\mathcal{B}}(\boldsymbol{a}_i)\Big) \\
&= \sum_{i=0}^{\ell-1} \mathrm{rk}_{\mathbb{F}_q}\Big(\mathrm{ext}_{\mathcal{B}}(\boldsymbol{a}_i) - \mathrm{ext}_{\mathcal{B}}(\boldsymbol{b}_i)\Big) = \sum_{i=0}^{\ell-1} \mathrm{rk}_{\mathbb{F}_q}\Big(\mathrm{ext}_{\mathcal{B}}(\boldsymbol{a}_i - \boldsymbol{b}_i)\Big) = \mathrm{wt}_{SR,\ell}(\boldsymbol{a}-\boldsymbol{b}) \\
&= \mathrm{d}_{SR,\ell}(\boldsymbol{b},\boldsymbol{a}),
\end{aligned}$$

showing (ii). Finally, we verify (iii): Using the well-known property of matrix ranks $\mathrm{rk}(\boldsymbol{A}+\boldsymbol{B}) \leq \mathrm{rk}(\boldsymbol{A}) + \mathrm{rk}(\boldsymbol{B})$, we get:

$$\begin{aligned}
\mathrm{d}_{SR,\ell}(\boldsymbol{a},\boldsymbol{b}) + \mathrm{d}_{SR,\ell}(\boldsymbol{b},\boldsymbol{c}) &= \mathrm{wt}_{SR,\ell}(\boldsymbol{b}-\boldsymbol{a}) + \mathrm{wt}_{SR,\ell}(\boldsymbol{c}-\boldsymbol{b}) \\
&= \sum_{i=0}^{\ell-1} \mathrm{rk}_{\mathbb{F}_q}\Big(\mathrm{ext}_{\mathcal{B}}(\boldsymbol{b}_i) - \mathrm{ext}_{\mathcal{B}}(\boldsymbol{a}_i)\Big) + \sum_{i=0}^{\ell-1} \mathrm{rk}_{\mathbb{F}_q}\Big(\mathrm{ext}_{\mathcal{B}}(\boldsymbol{c}_i) - \mathrm{ext}_{\mathcal{B}}(\boldsymbol{b}_i)\Big) \\
&\geq \sum_{i=0}^{\ell-1} \mathrm{rk}_{\mathbb{F}_q}\Big(\mathrm{ext}_{\mathcal{B}}(\boldsymbol{b}_i) - \mathrm{ext}_{\mathcal{B}}(\boldsymbol{a}_i) + \mathrm{ext}_{\mathcal{B}}(\boldsymbol{c}_i) - \mathrm{ext}_{\mathcal{B}}(\boldsymbol{b}_i)\Big) \\
&= \mathrm{wt}_{SR,\ell}(\boldsymbol{c}-\boldsymbol{a}) = \mathrm{d}_{SR,\ell}(\boldsymbol{a},\boldsymbol{c}).
\end{aligned}$$

□

The sum-rank metric serves as a generalization of both the Hamming metric and the rank metric, unifying their properties within a single framework. The sum-rank metric reduces to the Hamming metric when each block consists of a single symbol, i.e., when $\ell = n$ and $\eta = 1$. In this case, each block $\boldsymbol{x}_i$ contains exactly one element from $\mathbb{F}_{q^m}$, and the rank over $\mathbb{F}_q$ is either 0 (if the symbol is zero) or 1 (if the symbol is non-zero). So, in this setting, the sum-rank weight simply counts the number of non-zero symbols, which is exactly the Hamming weight. The sum-rank metric also generalizes the rank metric when a vector is treated as a single block, i.e., when $\ell = 1$ and $\eta = n$. In this

setting, the sum-rank weight reduces to the rank of the extension of the entire vector as matrix over $\mathbb{F}_q$, which corresponds to its rank weight. For this reason we introduce the following notation.

Notation 2.16. *We denote by* $\mathrm{wt}_{SR,n}(\cdot)$ *and* $\mathrm{d}_{SR,n}(\cdot)$ *the Hamming weight and Hamming distance of a vector and by* $\mathrm{wt}_{SR,1}(\cdot)$ *and* $\mathrm{d}_{SR,1}(\cdot)$ *the rank weight and the rank distance, respectively.*

Thus, the sum-rank weight acts as an intermediate measure between the Hamming weight and the rank weight. The following proposition recalls a well-known relationship between these three weights, showing that the sum-rank weight is always bounded above by the Hamming weight and below by the rank weight.

Proposition 2.17. *Let* $\boldsymbol{x} \in \mathbb{F}_{q^m}$ *then it holds:*

$$\mathrm{wt}_{SR,n}(\boldsymbol{x}) \geq \mathrm{wt}_{SR,\ell}(\boldsymbol{x}) \geq \mathrm{wt}_{SR,1}(\boldsymbol{x}).$$

Proof. We first show that the sum-rank weight of a vector is at most its Hamming weight. This can be seen when considering $\boldsymbol{x} = [\boldsymbol{x}_0|\ldots|\boldsymbol{x}_{\ell-1}] \in \mathbb{F}_{q^m}^n$ with $\mathrm{wt}_{SR,n}(\boldsymbol{x}) = n - t = \eta - t_0 + \ldots + \eta - t_{\ell-1}$ where $\sum_{i=0}^{\ell-1} t_i = t$ and each $\boldsymbol{x}_i$ has t_i zero entries. For the sum-rank weight one gets $\mathrm{wt}_{SR,\ell}(\boldsymbol{x}) = \sum_{i=0}^{\ell-1} \mathrm{rk}_q(\boldsymbol{x}_i) \leq \sum_{i=0}^{\ell-1} \min\{m, \eta - t_i\} \leq \sum_{i=0}^{\ell-1}(\eta - t_i) = n - t = \mathrm{wt}_{SR,n}(\boldsymbol{x})$. Now we prove that the rank weight of a vector is at most its sum-rank weight. We assume w.l.o.g. $n \leq m$. Let $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ be a vector of sum-rank weight $t = t_0 + \ldots + t_{\ell-1}$, i.e., each $\boldsymbol{x}_i$ has t_i $\mathbb{F}_q$-linearly independent columns for $i \in \{0, \ldots \ell - 1\}$, so $\boldsymbol{x}$ has at most t $\mathbb{F}_q$-linearly independent columns in the union of all blocks, which corresponds to the rank weight of $\boldsymbol{x}$. □

A property of many distance metrics is translation invariance, meaning that shifting all vectors by the same amount does not affect the measured distances. This property ensures that the relative positioning of vectors remains consistent under translations. The following proposition establishes that the sum-rank metric possesses this property, showing that the sum-rank distance between two vectors remains unchanged when both are translated by the same vector.

Proposition 2.18. *The sum-rank metric is invariant under the translation of vectors.*

Proof. Let $\boldsymbol{x} = [\boldsymbol{x}_0|\ldots|\boldsymbol{x}_{\ell-1}], \boldsymbol{y} = [\boldsymbol{y}_0|\ldots|\boldsymbol{y}_{\ell-1}], \boldsymbol{z} = [\boldsymbol{z}_0|\ldots|\boldsymbol{z}_{\ell-1}] \in \mathbb{F}_{q^m}^n$. We show that the sum-rank distance between $\boldsymbol{x}$ and $\boldsymbol{y}$ remains unchanged when shifting both vectors by the vector $\boldsymbol{z}$.

$$\mathrm{d}_{SR,\ell}(\boldsymbol{x} + \boldsymbol{z}, \boldsymbol{y} + \boldsymbol{z}) = \mathrm{wt}_{SR,\ell}(\boldsymbol{y} + \boldsymbol{z} - \boldsymbol{x} - \boldsymbol{z}) = \mathrm{wt}_{SR,\ell}(\boldsymbol{y} - \boldsymbol{x}) = \mathrm{d}_{SR,\ell}(\boldsymbol{x}, \boldsymbol{y}).$$

□

We give the definition of a linear sum-rank-metric code, including its dimension, structure, and minimum distance.

Definition 2.19 (Sum-Rank-Metric Code)**.** A linear $[n, k, d]$ sum-rank-metric code $\mathcal{C}$ over $\mathbb{F}_{q^m}$ is an $\mathbb{F}_{q^m}$-vector space $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ with $\dim_{\mathbb{F}_{q^m}}(\mathcal{C}) = k$. Consequently, the code has cardinality $|\mathcal{C}| = q^{mk}$. Each codeword $\boldsymbol{c} = [\boldsymbol{c}_1|\dots|\boldsymbol{c}_\ell] \in \mathcal{C}$ is composed of ℓ blocks $\boldsymbol{c}_i \in \mathbb{F}_{q^m}^\eta$ each of length η. The minimum (ℓ)-sum-rank distance d is defined as

$$d \coloneqq \min_{\boldsymbol{c} \neq \boldsymbol{c}' \in \mathcal{C}} \{\mathrm{d}_{SR,\ell}(\boldsymbol{c}, \boldsymbol{c}')\} = \min_{\boldsymbol{c} \in \mathcal{C}} \{\mathrm{wt}_{SR,\ell}(\boldsymbol{c})\}.$$

2.3. Bounds on the Cardinality of Linear Codes in the Hamming Metric

A central problem in coding theory is determining how many codewords a code can have for a given minimum distance and length. This leads to two fundamental questions: "How many codewords can exist at most?" and "How many codewords must exist at least?" These questions give rise to upper and lower bounds on the cardinality of codes. In this section, we focus on linear codes in the Hamming metric and introduce three classical bounds that address these questions: the Singleton bound (an upper bound), the sphere-packing bound (another upper bound), and the Gilbert–Varshamov bound (a lower bound). We start with the Singleton bound.

Theorem 2.20 (Singleton Bound [Sin64], [Jos58], [Kom53])**.** *Let $\mathcal{C}$ be a linear $[n, k, d]$-code over a finite field $\mathbb{F}_{q^m}$, then it holds:*

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

Codes that achieve the Singleton bound with equality are known as *Maximum Distance Separable* (MDS) codes. These codes are optimal in the sense that they have the largest possible number of codewords for a given length and minimum distance. Beyond the Hamming metric, Singleton-like bounds have also been established for other metrics, such as the rank metric (see [Del78]) and the sum-rank metric (see [MP18]), providing analogous criteria for optimality in these settings.

The sphere-packing bound, first introduced by Hamming in his seminal work on error-correcting codes [Ham50], was originally formulated for binary codes in the Hamming metric and is also known as Hamming Bound. The core idea behind the sphere-packing bound is to visualize codewords as the centers of spheres in the metric space, where each sphere contains all vectors within a certain radius t (where t corresponds to the code's error-correcting capability). To ensure reliable error correction, these spheres must be disjoint, preventing overlap that could lead to decoding errors. The bound is derived by comparing the total number of vectors in the space with the sum of the volumes of these non-overlapping spheres, providing an upper limit on the number of codewords a code can have while still guaranteeing correct error correction. Figure 2.1 visualizes how the volume of these spheres of radius t (shown in red) are determined with respect to the Hamming metric.

Theorem 2.21 (Sphere-Packing Bound [Ham50])**.** *Let $\mathcal{C}$ be a linear $[n, k, d]$-code over a finite field $\mathbb{F}_{q^m}$ and $t \coloneqq \lfloor \frac{d-1}{2} \rfloor$ then it holds:*

$$q^k \cdot \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leq q^n.$$

Codes that achieve the sphere-packing bound with equality are called perfect codes. In these codes, the spheres centered at each codeword exactly partition the entir bounde vector space without any overlaps or gaps, allowing for optimal error correction. Classic examples of perfect codes include Hamming codes and certain Golay codes in the Hamming metric (see [Bos13]). Beyond the Hamming metric, sphere-packing bounds have also been developed for other metrics, such as the rank metric (see [GY06]) and the sum-rank metric (see [BGLR21]). Additionally, the sphere-packing bound can be formulated in a metric-independent manner, providing a generalized framework applicable to various coding scenarios without relying on a specific distance measure.

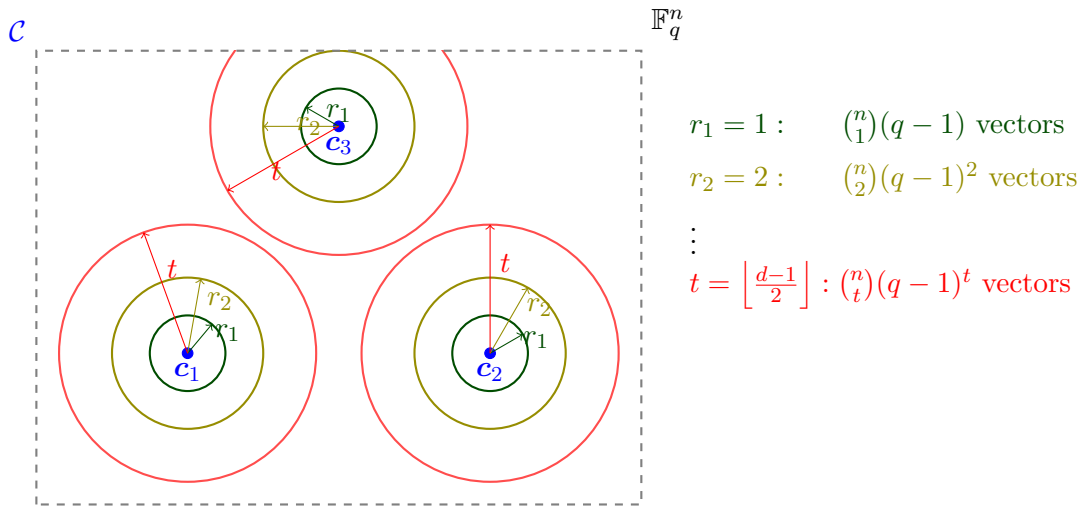


Figure 2.1.: Illustration of How the Volume of Hamming Spheres Is Determined for the Sphere-Packing Bound [Bos13].

The Gilbert–Varshamov bound is a fundamental result in coding theory that provides a lower bound on the maximum size of a code with a given length and minimum distance over a finite field. Introduced independently by Gilbert in 1952 [Gil52] and Varshamov in 1957 [Var57], this bound demonstrates the existence of codes with specific parameters, even if explicit constructions are not always known. As with other classical bounds in coding theory, such as the Singleton bound and the sphere-packing bound, the Gilbert–Varshamov bound admits extensions beyond the Hamming metric. In particular, versions of the Gilbert–Varshamov bound have been established for the rank metric (see [GY06]) and the sum-rank metric (cf. [BGLR21]), providing existential guarantees for codes measured with respect to these distances. Moreover, the underlying

argument admits a metric-independent formulation. There is a slight difference between the bounds proposed by Gilbert and Varshamov. We introduce Gilbert's version which is based on a greedy algorithm approach. It iteratively selects codewords such that each newly chosen codeword maintains a minimum distance from all previously selected codewords. This process continues until no more codewords can be added without violating the minimum distance constraint. The approach guarantees the existence of codes with a certain cardinality, offering a powerful tool for evaluating the achievability of specific code parameters.

Theorem 2.22 (Gilbert–Varshamov Bound [Gil52], [Var57])**.** *Let $\mathbb{F}_{q^m}$ be a finite field and let n, k, d be positive integers such that*

$$\sum_{i=0}^{d-2} \binom{n-1}{d-2} (q-1)^k < q^{n-k},$$

then there exists a linear $[n, k, d]$-code over $\mathbb{F}_{q^m}$.

Part I

Codes over Rings

3

Dual-Containing Codes over Finite Commutative Rings

3.1. Introduction

Error-correcting codes are traditionally centered on constructions over finite fields. However, the use of finite rings as code alphabets can be traced back to the early 1960s. One of the earliest contributions in this direction was made by Assmus and Mattson in [AM63], who studied linear codes over rings. Later, Blake in [Bla72] constructed codes over $\mathbb{Z}_m$ by lifting from cyclic codes over $\mathbb{Z}_{p_i}$, where $m = p_1 \cdot \ldots \cdot p_r$ is a product of distinct primes. The real breakthrough, however, came with the seminal work of Hammons, Kumar, Calderbank, Sloane, and Solé in [HKC94], which demonstrated that many well-known nonlinear binary codes are in fact linear over the ring $\mathbb{Z}_4$, revealing also their duality relationships, and enabling simpler algebraic decoding methods. This discovery fundamentally shifted the perception of ring-linear codes and launched a broad interest in their study. A central foundation of this chapter is the contribution by Boucher, Geiselmann and Ulmer [BGU07], in which the concept of cyclic codes is extended to the non-commutative setting. They define cyclic codes via generator polynomials in skew polynomial rings, which significantly broadens the algebraic framework and forms the basis for our investigation of cyclic left module codes.

In this chapter we study codes over finite commutative rings based on skew polynomials, i.e., the codes are constructed as submodules in $R = A[X; \theta, \delta]$, where A is a commutative Frobenius ring, θ is an endomorphism of A, and δ is a θ-derivation. These rings generalize classical polynomial rings and are a natural setting for constructing codes with rich algebraic structure. We focus on so-called *cyclic left module codes* of the form $\mathcal{C} = Rg/Rf \subset R/Rf$, where g and f are elements of the skew polynomial ring R. Here, cyclicity refers to a ring-theoretic property, namely, that the code is generated by a single element (the generator polynomial g) in the module, not to the notion of cyclicity commonly used in the context of coding theory. To derive a parity-check matrix for such codes, we make the additional assumption that there exists $\hbar \in R$ such that $f = hg = g\hbar$, that is, g is both a left and right divisor of f. Parity-check matrices for these types of codes have been established in [BU09a, Corollary 4] for $A = \mathbb{F}_q$, and in [BD18, BD21] for more general finite commutative Frobenius rings A. While the ap-

proach in [BD18, BD21] relies on pseudo-linear transformations, the method presented here is based solely on the algebraic structure of skew polynomial rings. One of the main challenges in this framework is that the entries of the parity-check matrix involve nested applications of θ and δ acting on the coefficients of g and $\hbar$, leading to expressions that are difficult to analyze. Under the condition that $A = B[a_1, \ldots, a_s]$ is a free B-algebra where B is the smallest unitary subring of A, it follows that both θ and δ restrict to polynomial maps on the subalgebra B. By expressing the unknown coefficients of g and $\hbar$ in terms of a B-basis, the associated conditions for dual containment and parity-check construction can be translated into a system of multivariate polynomial equations over B. This reformulation enables the application of Gröbner basis techniques [AL22],[BCP97] to solve the structural conditions imposed by dual-containing or self-dual code requirements. This is of particular interest in the construction of quantum error-correcting codes, where dual containment is essential. Within the computational complexity constraints of the Gröbner basis, our approach allows us to find all dual-containing codes $\mathcal{C} = Rg/Rf \subset R/Rf$ over A for any given parameters $[n, k]$ and to test various structural properties of such codes:

- We provide an algorithm to determine whether the dual of a given code remains a cyclic left module code, i.e., whether it is generated by a single polynomial $g^{\perp}$. Using this algorithm, we demonstrate that many (Hermitian-) dual-containing codes do not have cyclic duals.

- We highlight the necessity of considering non-trivial endomorphisms and non-zero derivations by showing that certain dual-containing codes cannot be found without them.

- We present examples of codes for which the modulus f is non-central, meaning the factorizations $f = hg$ and $f = g\hbar$ yield distinct polynomials $h \neq \hbar$.

We illustrate our approach with explicit computations over all commutative rings of order four and over the Galois ring $\mathrm{GR}(4, 2)$ of order 16.

This chapter differs slightly in notation from the rest of the thesis due to the technical nature of the constructions. Since we frequently switch between the vector and polynomial representations of a code, we explicitly distinguish between the two. We denote the polynomial representation by $\mathcal{C}$ and the vector representation by C. This contrasts with the rest of the thesis, where the notation $\mathcal{C}$ is used for both representations interchangeably. This chapter is based on the results published in [LOU25].

3.2. Algebraic Framework for (θ, δ)-Codes

3.2.1. Skew Polynomial Rings and Code Constructions

Let $A \neq \{0\}$ be a unitary ring, that is, a ring with a multiplicative identity $1 \in A \setminus \{0\}$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in A$. Throughout this work, we consider only

unitary endomorphisms $\theta\colon A \to A$ that preserve the identity, i.e., $\theta(1) = 1$. The identity endomorphism on A will be denoted by id.

Let $R = A[X; \theta, \delta]$ be the associated skew polynomial ring, where δ is a θ-derivation. In this setting, we consider codes that are cyclic left R-modules, that is, submodules of R/Rf generated by a single polynomial $g \in R$, referred to as the *generator polynomial*.

More precisely, we study codes of the form

$$\mathcal{C} = Rg/Rf \subset R/Rf,$$

where $f = hg$ for some $f, g, h \in R$. To construct such codes, we aim to utilize the well-known relation

$$\deg(hg) = \deg(h) + \deg(g), \tag{3.1}$$

which is fundamental in the analysis of skew polynomial modules. This relation holds whenever the leading coefficient of g is invertible. If this condition is not met, the leading coefficient of g may be a zero divisor in A, potentially causing the product of the leading coefficients of h and g to vanish, thereby invalidating (3.1). One practical way to guarantee that g has an invertible leading coefficient is to choose the modulus polynomial f to be monic and ensure that g is a right divisor of f. Hence, we deliberately choose our setting such that the polynomial f is monic and g is a right divisor of f. Under these assumptions, the degree-additivity property (3.1) is ensured for all $h \in R$.

Left and Right Division in Skew Polynomial Rings

Let A be a (not necessarily division) ring, and let θ be an automorphism of A. Consider the skew polynomial ring $A[X; \theta, \delta]$, and let $g = \sum_{i=0}^{m} g_i X^i \in A[X; \theta, \delta]$ be a skew polynomial with an invertible leading coefficient $g_m \in A$.

In this setting, for any $f = \sum_{i=0}^{n} f_i X^i \in A[X; \theta, \delta]$, we can perform both right and left division by g. In each case, there exists a unique right (respectively left) remainder of degree strictly less than $\deg(g)$. This holds even though A is not a division ring, due to the invertibility of g_m and the structure induced by θ.

To see this, assume $m \leq n$. Let $q(X) \in A[X; \theta, \delta]$ be a skew polynomial of the form

$$q(X) = f_n \theta^{n-m}(g_m^{-1}) X^{n-m} + \sum_{j=0}^{n-m-1} q_j X^j.$$

Subtracting $q(X)g(X)$ from $f(X)$ reduces the degree of f. More precisely, $r(X) :=$

$f(X) - q(X)g(X)$ satisfies:

$$\begin{aligned}
\deg(r) &= \deg\left(f - q \cdot g\right) \\
&= \deg\left(\sum_{i=0}^{n} f_i X^i - \left(f_n \theta^{n-m}(g_m^{-1}) X^{n-m} + \sum_{j=0}^{n-m-1} q_j X^j\right) \cdot \sum_{i=0}^{m} g_i X^i\right) \\
&\leq \max\left\{\deg\left(f_n X^n - f_n \theta^{n-m}(g_m^{-1}) X^{n-m} \cdot \sum_{i=0}^{m} g_i X^i\right), n-1\right\} \\
&= \max\left\{\deg\left(f_n X^n - f_n \theta^{n-m}(g_m^{-1}) X^{n-m} \cdot g_m X^m\right), n-1\right\} \\
&= \max\left\{\deg\left(f_n X^n - f_n \theta^{n-m}(g_m^{-1} g_m) X^n\right), n-1\right\} \\
&= \max\left\{\deg(f_n X^n - f_n X^n), n-1\right\} = n-1.
\end{aligned}$$

Thus, a right division step reduces the degree by at least one. Hence, there is a full right division algorithm with a remainder of degree less than $\deg(g)$.

Similarly, for the left division, let $q \in A[X; \theta, \delta]$ be of the form

$$q(X) = \theta^{-m}(g_m^{-1} f_n) X^{n-m} + \sum_{j=0}^{n-m-1} q_j X^j,$$

and $r(X) \coloneqq f(X) - g(X)q(X)$, then:

$$\begin{aligned}
\deg(r) &= \deg\left(f - g \cdot q\right) \\
&= \deg\left(\sum_{i=0}^{n} f_i X^i - \sum_{j=0}^{m} g_j X^j \left(\theta^{-m}(g_m^{-1} \cdot f_n) X^{n-m} + \sum_{j=0}^{n-m-1} q_j X^j\right)\right) \\
&= \deg\left(\sum_{i=0}^{n} f_i X^i - g_m X^m \theta^{-m}(g_m^{-1} f_n) X^{n-m} - g_m X^m \sum_{j=0}^{n-m-1} q_j X^j \right. \\
&\qquad \left. - \sum_{j=0}^{m-1} g_j X^j \theta^{-m}(g_m^{-1} f_n) X^{n-m} - \sum_{j=0}^{m} g_j X^j \sum_{j=0}^{n-m-1} q_j X^j\right) \\
&\leq \max\left\{\deg\left(\sum_{i=0}^{n} f_i X^i - g_m X^m \theta^{-m}(g_m^{-1} f_n) X^{n-m}\right), n-1\right\} \\
&= \max\left\{\deg\left(f_n X^n - X^m \theta^{-m}(g_m^{-1} g_m f_n) X^{n-m}\right), n-1\right\} \\
&= \max\left\{\deg\left(f_n X^n - f_n X^n\right), n-1\right\} = n-1.
\end{aligned}$$

Thus, the degree also strictly decreases in each left division step. Repeating the process eventually yields a remainder of degree less than $\deg(g)$.

Remark 3.1. *The right division algorithm still works even if θ is only an endomorphism (not necessarily invertible), as long as the leading coefficient of g is invertible. However, for the left division algorithm, θ being an automorphism is necessary, since it requires the inverse θ^{-1}.*

Since we are also interested in codes where θ is an endomorphism that is not an automorphism, we will consistently perform right division throughout this chapter. This approach naturally leads to the construction of left module codes over the skew polynomial ring R.

To see the uniqueness of the remainder, suppose that

$$f = qg + r = \tilde{q}g + \tilde{r}$$

for some $q, \tilde{q} \in R$ and remainders $r, \tilde{r} \in R$ with $\deg(r), \deg(\tilde{r}) < \deg(g) = m$. Subtracting the two expressions yields

$$(q - \tilde{q})g = \tilde{r} - r.$$

Assume for contradiction that $q \neq \tilde{q}$, and let $q - \tilde{q} = c_s X^s + \dots$ with $c_s \neq 0$ and s the highest index (i.e., the degree of the difference). Then the leading term of $(q - \tilde{q})g$ is

$$c_s \theta^s(g_m) X^{s+m},$$

where g_m is the leading coefficient of g. Since θ is a unitary endomorphism, it maps invertible elements to invertible elements, and in particular preserves nonzero elements. Hence, $c_s \theta^s(g_m) \neq 0$, and the leading term of $(q - \tilde{q})g$ is of degree $s + m \geq m$.

On the other hand, the right-hand side $\tilde{r} - r$ has degree strictly less than m by assumption. This leads to a contradiction, so we must have $q = \tilde{q}$ and $r = \tilde{r}$. Therefore, the remainder is unique.

3.2.2. Cyclic Left Module (θ, δ)-Codes

Definition 3.2 (Cyclic Left Module (θ, δ)-Code)**.** Let A be a finite ring, θ an endomorphism of A, and δ a θ-derivation. Let $R = A[X; \theta, \delta]$ denote the corresponding skew polynomial ring. Suppose $f \in R$ is a monic skew polynomial and $g \in R$ is a right divisor of f. A *cyclic left module (θ, δ)-code* (or simply a *(θ, δ)-code*) is defined as

$$\mathcal{C} = Rg/Rf \subset R/Rf$$

in its polynomial representation. The corresponding vector representation is given by

$$C \coloneqq \left\{ \mathbf{c} = [c_0, c_1, \dots, c_{n-1}] \;\middle|\; c_0 + c_1 X + \cdots + c_{n-1} X^{n-1} \in Rg/Rf \right\}.$$

Remark 3.3. *The term* cyclic *in this setting refers to the module-theoretic property that the code $\mathcal{C}$ is a* ***cyclic left R-module****, meaning it is generated by a single element. This is distinct from the classical coding-theoretic notion of cyclicity, which involves invariance under coordinate-wise cyclic shifts.*

However, classical shift-based structures can still be recovered in this framework by choosing specific forms for the modulus polynomial f. Suppose there exists a unit $a \in A$ such that $f = X^n - a$ and g is a right divisor of f. Then the resulting code $\mathcal{C} = Rg/Rf$ is called a ***θ-constacyclic code****, i.e., the code satisfies the shift-invariance condition*

$$[a_0, a_1, \dots, a_{n-2}, a_{n-1}] \in C \;\Rightarrow\; [a \cdot \theta(a_{n-1}), \theta(a_0), \theta(a_1), \dots, \theta(a_{n-2})] \in C.$$

Special cases include:

- *If $a = 1$, then the code is a* θ***-cyclic code.***
- *If $a = -1$, then the code is a* θ***-negacyclic code.***

In the classical setting where $\theta = \mathrm{id}$ and $\delta = 0$, the skew polynomial ring R becomes the usual commutative polynomial ring $A[X]$. In this case:

- $f = X^n - 1$ *yields a* classical cyclic code*,*
- $f = X^n - a$ *gives a* classical constacyclic code*, and*
- $f = X^n + 1$ *corresponds to a* classical negacyclic code*.*

We note that (θ, δ)-codes over finite rings, where θ is an endomorphism and δ is a corresponding θ-derivation, have been investigated in various works, including [BU14, BD18, BD21, SB18].

Proposition 3.4 ([LOU25, Proposition 1])**.** *Let $R = A[X; \theta, \delta]$ be a skew polynomial ring, and let $f \in R$ be a monic polynomial of degree n. Suppose $g \in R$ is a right divisor of f with $\deg(g) = n - k$. Then the cyclic left module (θ, δ)-code $\mathcal{C} = Rg/Rf \subset R/Rf$ satisfies the following properties:*

(i) The left R-module R/Rf is a free left A-module of rank n, with basis $(1, X, \ldots, X^{n-1})$, and is therefore isomorphic to A^n.

(ii) $\mathcal{C} = Rg/Rf$ is a left R-submodule of R/Rf.

(iii) As a subset of $R/Rf \cong A^n$, the code $\mathcal{C}$ is also a free left A-submodule of rank $k = \deg(f) - \deg(g)$. Hence, it defines a ring-linear code of length n and dimension k over the alphabet A.

(iv) If g is both a left and right divisor of f, i.e., $f = hg = g\hbar$ for some $h, \hbar \in R$, then all three polynomials f, g, and h in the factorization $f = hg$ can be chosen to be monic. Moreover, the monic generator polynomial g is unique.

(v) If θ is an automorphism and g is a two-sided divisor of f, i.e., $f = hg = g\hbar$, then all four polynomials f, g, h, and $\hbar$ can be assumed to be monic.

Proof. Since $f \in R$ is monic of degree n, we can perform a right division of any element in R by f, obtaining a unique remainder of degree strictly less than n. Therefore, each element in R/Rf has a unique representative (the remainder of the right division) of the form $\sum_{i=0}^{n-1} a_i X^i$ for $a_i \in A$. R/Rf can be viewed as a free left A-module of rank n, with basis $\{1, X, \ldots, X^{n-1}\}$, i.e., every element in R/Rf is a linear combination of those elements. This shows statement (i).

For $g \in R$ we have $Rf \subset Rg$ if and only if g is a right factor of f and in this case Rg/Rf is a cyclic left R-submodule of R/Rf generated by g. Hence, statement (ii) holds.

As $f = hg$ is monic, the leading coefficient g_{n-k} of $g = \sum_{i=0}^{n-k} g_i X^i$ must be a right divisor of 1, and thus invertible. In particular, this guarantees that the degree-additivity property $\deg(hg) = \deg(h) + \deg(g)$ holds for all $h \in R$ and implies that the elements $X^i g$ (for $i = 0, \ldots, k-1$) are linearly independent over A, and span a free left A-module of rank k in R/Rf. This establishes that the R-module Rg/Rf is a free A-module of rank k with basis $g, Xg, \ldots, X^{k-1}g$, and thus corresponds to a linear code of length n and dimension k over A. This confirms part (iii) of the proposition.

To prove statement (iv), assume $f = hg = g\hbar$ and write

$$g = g_{n-k}X^{n-k} + \cdots + g_0, \qquad h = h_k X^k + \cdots + h_0.$$

Then

$$f = hg = (h_k X^k + \cdots + h_0)(g_{n-k}X^{n-k} + \cdots + g_0).$$

Since f is monic, the leading coefficient of $f = hg$ is $h_k\theta^k(g_{n-k}) = 1$, showing that h_k and $\theta^k(g_{n-k})$ are invertible. We insert the multiplicative identity by multiplying with $g_{n-k} \cdot g_{n-k}^{-1}$ and obtain:

$$f = \underbrace{(h_k X^k + \cdots + h_0) \cdot g_{n-k}}_{\tilde{h}} \cdot \underbrace{g_{n-k}^{-1}(g_{n-k}X^{n-k} + \cdots + g_0)}_{\tilde{g}}.$$

In this representation $\tilde{g}$ is a monic polynomial. Since θ is a unitary endomorphism mapping 1 to 1, the product rule of $A[X; \theta, \delta]$ shows that the leading coefficient of $\tilde{h}\tilde{g}$ is the leading coefficient of $\tilde{h}$. But $f = \tilde{h}\tilde{g}$ is monic, so $\tilde{h}$ must also be monic. The polynomials g and $\tilde{g}$ differ by an invertible factor in A. Using the above equations in both directions, we observe that any product of g with a polynomial of degree at most $k-1$ can equally be expressed as a product of $\tilde{g}$ by a polynomial of degree $\leq k-1$ and vice versa. Therefore, g and $\tilde{g}$ generate the same left module: $Rg = R\tilde{g}$. Thus, the code $Rg/Rf = R\tilde{g}/Rf$, and we can assume without loss of generality that f, g and h are monic. The uniqueness of the monic generator follows from the fact that if $\mathcal{C}$ is a cyclic left module (θ, δ)-code with parameters $[n, k]$ and monic generator polynomial g, then any codeword is of the form $c = m \cdot g$ with $\deg(g) = n - k$, $m \in R$, and $\deg(m) < k$. In particular, the only monic polynomial of degree $n - k$ in $\mathcal{C}$ is $g = 1 \cdot g$. This establishes the validity of part (iv) of the proposition.

Finally, we show that $\hbar = \hbar_k X^k + \cdots + \hbar_0$ is monic if θ is an automorphism. The same reasoning as above applies to $\hbar$ if θ is an automorphism: since $f = g\hbar$ and both f and g are monic, the leading coefficient of f, namely $\theta^{n-k}(\hbar_k)$, must equal 1. As θ^{n-k} is an automorphism and hence preserves invertibility, it follows that $\hbar_k = 1$, and thus $\hbar$ is monic as well. □

Example 3.5 ([LOU25, Example 1])**.** *Let $A = \mathbb{F}_2[u]/(u^2)$. This is a Frobenius chain ring and also a free $\mathbb{F}_2$-algebra with $\mathbb{F}_2$-basis $\{1, u\}$. The only automorphism of A is the identity map $\theta_1 : x \mapsto x$. In addition, there exists a unique non-trivial endomorphism θ_2 defined by $\theta_2(u) = 0$ (recall that $\theta_2(1) = 1$). On both $\mathbb{F}_2$ and the ring A itself, the map θ_2 acts as a polynomial function, specifically, it coincides with the squaring map $\theta_2 : x \mapsto x^2$.*

Any θ-derivation δ is fully determined by its value on u, since $\delta(1) = \delta(0) = 0$. In the Table 3.1 all θ-derivations are listed:

Table 3.1.: All θ-derivations on $A = \mathbb{F}_2[u]/(u^2)$.

	Automorphism	
	$\theta_1 = \mathrm{Id}$	$\theta_2 : \ u \mapsto 0$
$\delta_1 = 0$	$u \mapsto 0$	$u \mapsto 0$
δ_2	$u \mapsto 1$	
δ_3	$u \mapsto u$	$u \mapsto u$
δ_4	$u \mapsto u + 1$	

The inner θ-derivations are highlighted in green. In Theorem 3.4, we showed that for a cyclic left module (θ, δ)-code of the form $Rg/Rf \subset R/Rf$, all three polynomials in the factorization $f = hg$ can be chosen to be monic. However, if θ is not an automorphism, then the factor $\hbar$ in the right factorization $f = g\hbar$ is not necessarily monic. To illustrate this, consider the skew polynomial ring $R = A[X; \theta_2, \delta_3]$, where $\theta_2(u) = 0$ and $\delta_3(u) = u$, and the code Rg/Rf defined by

$$g = X^2 + uX + u + 1, \quad f = X^4 + (u+1)X^3 + X + u + 1.$$

It can be verified that

$$f = hg \quad \textit{with} \quad h = X^2 + (u+1)X + 1,$$

and also

$$f = g\hbar \quad \textit{with either} \quad \hbar = (u+1)X^2 + (u+1)X + u + 1 \quad \textit{or} \quad \hbar = (u+1)X^2 + X + u + 1.$$

In both cases, $\hbar$ is not monic, illustrating that $\hbar$ being monic is not guaranteed when θ is not invertible.

3.2.2.1. Generator Matrix

The encoding of an information vector $[b_0, b_1, \ldots, b_{k-1}] \in A^k$ in a cyclic left module (θ, δ)-code $\mathcal{C} = Rg/Rf \subset R/Rf$ is performed by multiplying the information polynomial $\sum_{i=0}^{k-1} b_i X^i$ from the left with the generator polynomial g. The resulting product $(\sum_{i=0}^{k-1} b_i X^i)g \in Rg/Rf$ corresponds to a codeword in $\mathcal{C}$ and can be represented by its coefficients as a vector in A^n using the basis $\{1, X, \ldots, X^{n-1}\}$. Equivalently, this encoding process can be realized as multiplication with a generator matrix $\boldsymbol{G}$, whose rows are obtained from the coefficients of the left multiples $g, Xg, \ldots, X^{k-1}g$ modulo Rf:

$$\boldsymbol{G} = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & \\ g_0^{\delta} & g_1^{\delta} + g_0^{\theta} & g_2^{\delta} + g_1^{\theta} & \cdots & g_{n-k}^{\theta} & 0 & \cdots \\ \vdots & \ddots & \ddots & \cdots & \ddots & \ddots & \\ g_0^{\delta^{k-1}} & & \cdots & & \cdots & & g_{n-k}^{\theta^{k-1}} \end{bmatrix}.$$

The row polynomials $X^i \cdot g$ are computed using the skew multiplication rule $Xa = a^\theta X + a^\delta$ for all $a \in A$. The code $\mathcal{C}$ is thus completely determined by the triple (g, θ, δ).

Example 3.6 ([LOU25, Example 2]). *Let $R = A[X; \theta, \delta]$, and consider a monic polynomial $f = hg \in R$ of degree 4, where $g = g_1X + g_0$ and $h = \sum_{i=0}^{3} h_i X^i$. Suppose that the leading coefficient satisfies $h_3 g_1 = 1$, ensuring that f is monic. Then the cyclic left module (θ, δ)-code $\mathcal{C} = Rg/Rf \subset R/Rf$ is an $[4, 3]_A$ code.*

A generator matrix for $\mathcal{C}$ is given by:

$$\boldsymbol{G} = \begin{bmatrix} g_0 & g_1 & 0 & 0 \\ g_0^\delta & g_1^\delta + g_0^\theta & g_1^\theta & 0 \\ g_0^{\delta^2} & g_0^{\delta\theta} + g_0^{\theta\delta} + g_1^{\delta^2} & g_0^{\theta^2} + g_1^{\delta\theta} + g_1^{\theta\delta} & g_1^{\theta^2} \end{bmatrix}.$$

When A is a finite field $\mathbb{F}_q$, the endomorphism θ is necessarily of the form $a \mapsto a^{p^m}$, and any θ-derivation δ must be an inner derivation, i.e., of the form $\delta(a) = \beta a - \theta(a)\beta$. In this setting, the entries of the generator matrix can be expressed as polynomials in the coefficients of the generator polynomial g, making explicit and efficient computations possible. Consequently, most known examples of self-dual (θ, δ)-codes are constructed over finite fields.

3.2.2.2. Duality and Cardinality over Frobenius Rings

A fundamental result in coding theory over a finite field $\mathbb{F}_q$ is

$$|C| \cdot |C^\perp| = q^n,$$

which expresses a precise relationship between a linear code and its Euclidean dual. Remarkably, this relationship extends to codes over more general algebraic structures, such as Frobenius rings. The following lemma generalizes this result to (Hermitian) duality over commutative Frobenius rings.

Lemma 3.7 ([SW17, Theorem 4.2]). *Let A be a commutative Frobenius ring and let C be a linear code over A. Then for the (Hermitian) dual code $C^{\perp_\sigma}$, we have*

$$|C| \cdot |C^{\perp_\sigma}| = |A|^n.$$

This holds for Hermitian duals with respect to any involutive automorphism (i.e., $\sigma^2 = \mathrm{id}$), including the case $\sigma = \mathrm{id}$, which recovers the classical Euclidean dual as a special case. It ensures that the product of the sizes of a code and its dual always equals the total number of elements in the ambient module A^n. In particular, this implies that the Hermitian dual $C^{\perp_\sigma}$ is uniquely determined (up to isomorphism) by C. The lemma plays a central role in structural results and duality theory for codes over rings.

While Frobenius rings are not the primary focus of this thesis, we make use of Lemma 3.7 in several key results throughout this chapter. In order to ensure its applicability, we restrict our attention here to codes over commutative Frobenius rings. This restriction is not motivated by an interest in the structural theory of Frobenius

rings themselves, but rather by the need to work in a setting that is as general as possible while still guaranteeing that the duality identity and the results that rely on it, remain valid. For this reason, we will not provide a detailed treatment of Frobenius rings; instead, we refer the reader to the literature (e.g., [SW17]) for background and properties.

3.3. Parity-Check Matrix and Generator Matrix of the Euclidean and Hermitian Dual Code

Parity-check matrices for cyclic left module (θ, δ)-codes have been studied in various algebraic settings. For example, in the case where the base ring is a field $\mathbb{F}_q$ and the derivations are inner, a construction is given in [BU09a, Corollary 4]. Extensions to commutative Frobenius rings are discussed in [BD18, BD21]. Furthermore, in [SB18], parity-check matrices for codes over the non-chain ring $A = (\mathbb{Z}/4\mathbb{Z})[X]/(X^2 - 1)$ are studied, under the assumption that the defining polynomial $f = hg$ is central.

Our approach follows the strategy in [BU09a] and [SB18], focusing on cyclic left R-modules of the form $Rg/Rf \subset R/Rf$, where $R = A[X; \theta, \delta]$ and $f = hg = g\hbar$ and Rg/Rf is an ideal in R/Rf. This assumption, that g is both a right and left divisor of f, is notably weaker than the condition that f is central. See, for instance, the $[6, 4]$ example in Section 3.5.

In the following lemma, we make this construction explicit by describing how codewords in Rg/Rf can be characterized via a linear system, leading to a matrix representation whose left kernel gives the corresponding code. This provides a concrete tool for analyzing and constructing parity-check matrices in the general skew polynomial setting.

Lemma 3.8 (Parity-Check-Like Matrix ([LOU25, Lemma 2]))**.** *Let θ be an endomorphism and δ a θ-derivation of a finite ring A, and let $R = A[X; \theta, \delta]$ be the corresponding skew polynomial ring. Suppose $f \in R$ is monic and has both a right and a left divisor g, so that $f = hg = g\hbar$, and define the cyclic left module code $\mathcal{C} = Rg/Rf \subset R/Rf$. Then a word $\boldsymbol{w} \in A^n$ with polynomial representation $w \in R$ of degree $< n$ corresponds to a codeword in $\mathcal{C}$ if and only if the coset of $w \cdot \hbar = 0$ in R/Rf. In this case, we obtain an $n \times n$ matrix $\boldsymbol{M}$ such that the vector representation of $\mathcal{C}$ is given by*

$$C = \{\mathbf{w} \in A^n \mid \mathbf{w}\boldsymbol{M} = \mathbf{0}\},$$

i.e., $C = \ker_L(\boldsymbol{M})$ is a left kernel of $\boldsymbol{M}$, where the entries of $\boldsymbol{M}$ are images under compositions of θ and δ of the coefficients of $\hbar$ and g. The i-th row of $\boldsymbol{M}$ corresponds to the coefficients of $X^{i-1}\hbar \mod f$, for $i = 1, \ldots, n$.

Proof. Since f is monic, any element in $R/Rf \cong A^n$ has a unique representative $w \in R$ of degree less than n as a remainder of the right division by f. Following [BU09b, Lemma 8], we now show that an element $w \in R$ belongs to $\mathcal{C}$ if and only if (the coset of) $w \cdot \hbar = 0$ in R/Rf. If $w \in \mathcal{C}$, then $w = \tilde{w}g$ for some $\tilde{w} \in R$, and hence $w\hbar = \tilde{w}g\hbar = \tilde{w}(h \cdot g) = \tilde{w}f \equiv 0 \mod f$.

Conversely, if $w \cdot \hbar \equiv 0 \mod f$, then $w \cdot \hbar = \tilde{w}(h \cdot g) = \tilde{w}f = \tilde{w}g\hbar$, so by cancellation (since $\hbar$ is not a zero divisor in R), we conclude $w = \tilde{w}g \in \mathcal{C}$. As f is monic, every word in A^n corresponds uniquely to a coset $w = \sum_{i=0}^{n-1} w_i X^i \in R/Rf$, where $\deg(w) < n$. A coset representative w belongs to the code $\mathcal{C} = Rg/Rf$ if and only if $w \cdot \hbar = 0$ in R/Rf. To check this condition, we compute the product

$$w \cdot \hbar \mod f = \left(\sum_{i=0}^{n-1} w_i X^i \right) \left(\sum_{j=0}^{k} \hbar_j X^j \right) \mod f.$$

Due to the noncommutative multiplication in $R = A[X; \theta, \delta]$, the coefficients $\hbar_j$ are brought to the left, and the result is reduced modulo f using right division. The code C is then described as the set of all coefficient vectors $\mathbf{c} = [c_0, \ldots, c_{n-1}] \in A^n$ for which $w \cdot \hbar \equiv 0 \mod f$. This defines a system of linear equations over A, and hence C can be expressed as the left kernel of a matrix $\boldsymbol{M}$:

$$C = \left\{ \mathbf{c} \in A^n \;\middle|\; \sum_{i=0}^{n-1} c_i M_{i,j} = 0 \text{ for all } j = 0, \ldots, n-1 \right\}.$$

The entries $\boldsymbol{M}_{ij} \in A$ are compositions of images under θ and δ of the coefficients of $\hbar$ and f. Since $f = g\hbar$, the structure of $\boldsymbol{M}$ can be expressed in terms of the coefficients of both $\hbar$ and g. The i-th row of $\boldsymbol{M}$ corresponds to the contribution of the term $c_i X^i \cdot \hbar \mod f$ in the product $w \cdot \hbar = 0 \mod f$. □

The lemma shows that the polynomial $\hbar$ plays the role of a parity-check polynomial: it defines a right multiplication condition that characterizes membership in the code and determines the structure of the associated parity-check matrix.

To make the construction from Lemma 3.8 more concrete, we now consider a small illustrative example with parameters $n = 3$ and $k = 1$. This toy example demonstrates how a cyclic left (θ, δ)-code defined as a quotient $\mathcal{C} = Rg/Rf$ in a skew polynomial ring $R = A[X; \theta, \delta]$ can be translated into a matrix condition. We explicitly compute the matrix $\boldsymbol{M}$ whose left kernel corresponds to the code.

Example 3.9 (A Toy Example for $n = 3$, $k = 1$ (see [LOU25, Example 3]))**.** *Let A be a ring and $R = A[X; \theta, \delta]$ the associated skew polynomial ring. Suppose the polynomial $f \in R$ is monic of degree 3 and factors as $f = g\hbar$, where*

$$g = g_2 X^2 + g_1 X + g_0, \quad \hbar = \hbar_1 X + \hbar_0.$$

According to Lemma 3.8, a word $w = w_0 + w_1 X + w_2 X^2 \in R$ defines a codeword in the cyclic left module code $\mathcal{C} = Rg/Rf \subset R/Rf$ if and only if

$$w \cdot \hbar \equiv 0 \mod f.$$

Expanding the product $w \cdot \hbar$ modulo f gives:

$$\begin{aligned} w \cdot \hbar \mod f = &\left(w_2(\hbar_1^{\theta\delta} + \hbar_1^{\delta\theta} + \hbar_0^{\theta^2} - \hbar_1^{\theta^2} f_2) + w_1 \hbar_1^{\theta}\right) X^2 \\ &+ \left(w_2(\hbar_1^{\delta^2} + \hbar_0^{\theta\delta} + \hbar_0^{\delta\theta} - \hbar_1^{\theta^2} f_1) + w_1(\hbar_1^{\delta} + \hbar_0^{\theta}) + w_0 \hbar_1\right) X \\ &+ \left(w_2(\hbar_0^{\delta^2} - \hbar_1^{\theta^2} f_0) + w_1 \hbar_0^{\delta} + w_0 \hbar_0\right). \end{aligned}$$

This gives rise to a matrix $\boldsymbol{M} \in A^{3\times 3}$ such that $\boldsymbol{w}\cdot\boldsymbol{M} = \boldsymbol{0}$, where $\boldsymbol{w} = [w_0, w_1, w_2] \in A^3$. The matrix $\boldsymbol{M}$ is explicitly:

$$\boldsymbol{M} = \begin{bmatrix} \hbar_0 & \hbar_1 & 0 \\ \hbar_0^{\delta} & (\hbar_1^{\delta} + \hbar_0^{\theta}) & \hbar_1^{\theta} \\ \hbar_0^{\delta^2} - \hbar_1^{\theta^2} f_0 & \hbar_1^{\delta^2} + \hbar_0^{\theta\delta} + \hbar_0^{\delta\theta} - \hbar_1^{\theta^2} f_1 & \hbar_1^{\theta\delta} + \hbar_1^{\delta\theta} + \hbar_0^{\theta^2} - \hbar_1^{\theta^2} f_2 \end{bmatrix}. \tag{3.2}$$

Each entry M_{ij} corresponds to the coefficient of the term $w_i X^j$ in the expansion of $w \cdot \hbar$ mod *f.*

For codes defined over skew polynomial rings, understanding when the dual code is free and how it can be described in terms of the original code is of foundational importance. The following theorem provides a result for duals of cyclic left module (θ, δ)-codes in skew polynomial rings $R = A[X; \theta, \delta]$, where A is a finite commutative Frobenius ring. It shows that under the mild assumption that a monic polynomial $f \in R$ admits both a right and a left divisor g (i.e., $f = hg = g\hbar$), the dual code $C^{\perp}$ of the cyclic code $\mathcal{C} = Rg/Rf \subset R/Rf$ is a free A-submodule of A^n, where $n = \deg(f)$. Moreover, it provides an explicit construction of a parity-check matrix for C, whose rows form a generating set for the dual code $C^{\perp}$. The matrix entries are determined by the coefficients of g and $\hbar$ via compositions of the ring endomorphism θ and the θ-derivation δ.

A similar result appears in [BD18, BD21], where the dual code is studied in the framework of pseudo-linear transformations and matrix-product codes. In contrast, our formulation and proof are based directly on the structure theory of skew polynomial rings. We now formally state the theorem.

Theorem 3.10 (Generator Matrix of the Euclidean Dual (cf. [BD18, SB18] and [LOU25, Theorem 1]))**.** *Let A be a finite commutative Frobenius ring, θ an endomorphism of A, and δ a θ-derivation. Consider the skew polynomial ring $R = A[X; \theta, \delta]$, and let $f \in R$ be a monic polynomial that admits both a right and a left divisor g, i.e., $f = hg = g\hbar$ for some $h, \hbar \in R$. Define the cyclic left module (θ, δ)-code $\mathcal{C} = Rg/Rf \subset R/Rf$, and let $C \subset A^n$ be its vector representation, where $n = \deg(f)$. Then, the dual code $C^{\perp}$ is a free A-module and satisfies the cardinality relation*

$$|C| \cdot |C^{\perp}| = |A|^n.$$

Moreover, there exists a parity-check matrix $\boldsymbol{H} \in A^{(n-k)\times n}$ for C whose rows generate $C^{\perp}$. The entries of $\boldsymbol{H}$ are given by compositions of θ and δ applied to the coefficients of g and $\hbar$.

Proof. Let $\boldsymbol{M}$ be the $n \times n$ matrix from Lemma 3.8 whose left kernel is exactly the code C. Define $\widetilde{C}$ to be the A-submodule generated by the columns of $\boldsymbol{M}$. By construction we have that $\tilde{C} \subset C^{\perp}$. Note that $\boldsymbol{w} \in C$ if and only if $\boldsymbol{w}\boldsymbol{M} = \boldsymbol{0}$, which is equivalent to $\boldsymbol{w}$ being orthogonal to all generators of $\tilde{C}$. Thus, $C = \tilde{C}^{\perp}$. Applying Lemma 3.7, we have $|\tilde{C}^{\perp}| \cdot |\tilde{C}| = |A|^n$, and since $C = \widetilde{C}^{\perp}$ and $|C| = |A|^k$, we also have $|\widetilde{C}| = |A|^{n-k}$. On the other hand, the duality relation $|C^{\perp}| \cdot |C| = |A|^n$ in Lemma 3.7 also implies that $|C^{\perp}| = |A|^{n-k}$. It follows that $\widetilde{C}$ and $C^{\perp}$ are A-modules of the same cardinality and $\widetilde{C} \subseteq C^{\perp}$. Therefore, $\widetilde{C} = C^{\perp}$, showing that the dual code is generated by the columns of $\boldsymbol{M}$.

To identify a generator matrix of $C^{\perp}$, note that Lemma 3.8 shows that for each $i = 1, \ldots, n-k$, the i-th row of $\boldsymbol{M}$ corresponds to the coefficients of $X^{i-1} \cdot \hbar \mod f$ (e.g., the green part in (3.2)). This shows that the right-upper $(n-k) \times (n-k)$ submatrix of $\boldsymbol{M}$ is lower triangular with invertible diagonal elements $\hbar_k, \theta(\hbar_k), \ldots, \theta^{n-k-1}(\hbar_k)$ and the right-most $n-k$ columns of M are therefore linearly independent. Hence, the A-submodule generated by the right-most $n-k$ columns of $\boldsymbol{M}$ contains $|A|^{n-k}$ elements. This shows that $C^{\perp}$ is a free A-module generated by the right-most $n-k$ columns of $\boldsymbol{M}$ which (after transposing) form a parity-check matrix of C (see (3.3) for an example). □

To illustrate Theorem 3.10, we revisit the toy example from Example 3.9. There, we constructed a cyclic left (θ, δ)-code $\mathcal{C} = Rg/Rf \subset R/Rf$ of length $n = 3$ and dimension $k = 1$, along with the associated matrix $\boldsymbol{M}$ derived from the condition $w \cdot \hbar \equiv 0 \mod f$. We now examine the dual code $C^{\perp}$ of C and explicitly determine a parity-check matrix.

Example 3.11 ([LOU25, Example 4])**.** *According to Theorem 3.10, the dual code $C^{\perp}$ of the code C from Example 3.9 is generated by the right-most $n-k = 2$ columns of the matrix $\boldsymbol{M}$ in* (3.2)*. Transposing these columns yields the parity-check matrix $\boldsymbol{H}$ of C:*

$$\boldsymbol{H} = \begin{bmatrix} \hbar_1 & \hbar_1^{\delta} + \hbar_0^{\theta} & \hbar_1^{\delta^2} + \hbar_0^{\theta\delta} + \hbar_0^{\delta\theta} - \hbar_1^{\theta^2} f_1 \\ 0 & \hbar_1^{\theta} & \hbar_1^{\theta\delta} + \hbar_1^{\delta\theta} + \hbar_0^{\theta^2} - \hbar_1^{\theta^2} f_2 \end{bmatrix}. \tag{3.3}$$

In many applications, it is not only of interest to determine the Euclidean dual of a linear code, but also its Hermitian dual with respect to a given involutive automorphism. The following result provides a practical way to obtain a generator matrix for the σ-Hermitian dual code by applying the automorphism σ to the entries of a known generator matrix for the Euclidean dual. This connection simplifies the construction of Hermitian dual codes in the context of cyclic left (θ, δ)-codes over skew polynomial rings.

Theorem 3.12 (Generator Matrix of the Hermitian Dual (see [LOU25, Theorem 2]))**.** *Let σ be an automorphism of order 2 on a finite commutative Frobenius ring A, and let θ be an endomorphism of A and δ a θ-derivation. Define the skew polynomial ring $R = A[X; \theta, \delta]$ and consider a monic polynomial $f \in R$ with both a right and left divisor g such that $f = hg = g\hbar$. Let $\mathcal{C} = Rg/Rf \subset R/Rf$ be the corresponding cyclic left module code, and let C be its vector representation. Suppose $\boldsymbol{H}$ is a generator matrix of the Euclidean dual code $C^{\perp}$. Then, the matrix $\sigma(\boldsymbol{H})$, obtained by applying σ entrywise to $\boldsymbol{H}$, is a generator matrix for the σ-Hermitian dual code $C^{\perp_\sigma}$. The entries of $\sigma(\boldsymbol{H})$*

are given by expressions in images under compositions of θ, δ and σ applied to the coefficients of g and $\hbar$.

Proof. Let $\boldsymbol{G}$ be a generator matrix for the code C, with rows g_s for $s = 1, \ldots, k$, and let $\boldsymbol{G}^{\perp}$ be a generator matrix for the Euclidean dual code $C^{\perp}$, with rows $g_t^{\perp}$ for $t = 1, \ldots, n-k$. By definition of duality, we have

$$\langle g_s, g_t^{\perp} \rangle = \sum_{i=1}^{n} g_{s,i}\, g_{t,i}^{\perp} = 0$$

for all $s \in \{1, \ldots, k\}$ and $t \in \{1, \ldots, n-k\}$. Now consider the σ-Hermitian inner product. Since σ is an automorphism with $\sigma^2 = \mathrm{Id}$, we compute:

$$\langle g_s, \sigma(g_t^{\perp}) \rangle_{\sigma} = \sum_{i=1}^{n} g_{s,i}\, \sigma(\sigma(g_{t,i}^{\perp})) = \sum_{i=1}^{n} g_{s,i}\, g_{t,i}^{\perp} = 0.$$

This shows that each row g_s of $\boldsymbol{G}$ is orthogonal (in the σ-Hermitian sense) to each row of $\sigma(\boldsymbol{G}^{\perp})$. Hence, the code generated by $\sigma(\boldsymbol{G}^{\perp})$ is contained in the σ-Hermitian dual $C^{\perp_\sigma}$. Moreover, since $C^{\perp}$ is a free module of rank $n-k$ and σ is a ring automorphism, the matrix $\sigma(\boldsymbol{G}^{\perp})$ also generates a free A-submodule of rank $n-k$. Therefore, by Lemma 3.7, which ensures that $|C| \cdot |C^{\perp_\sigma}| = |A|^n$, we conclude that $\sigma(\boldsymbol{G}^{\perp})$ generates $C^{\perp_\sigma}$. □

3.4. Computing All Dual-Containing (θ, δ)-Codes

This section presents an algorithmic approach to identify all dual-containing cyclic left module (θ, δ)-codes over skew polynomial rings. While the case of zero derivation ($\delta = 0$) and finite fields ($A = \mathbb{F}_q$) is well-studied (see [BSU08, BU09b, BU11, BD18, BD21]), much less is known when A is an arbitrary Frobenius ring or when $\delta \neq 0$. We show that the dual of a cyclic left module (θ, δ)-code is in general not a cyclic left module (θ, δ)-code and provide a method to compute and characterize them.

3.4.1. Polynomial Maps

Our first step is to handle algebraic expressions involving compositions of θ and δ applied to the coefficients of polynomials $\hbar$ and g (cf. matrix $\boldsymbol{M}$ in (3.2)). To do so, we reformulate these expressions as multivariate polynomials over a subalgebra of A.

Definition 3.13 (Polynomial Map)**.** A *polynomial map* on a ring B is a function $f : B \to B$ of the form $f(x) = \sum_{i=0}^{s} b_i x^i$, with $s \in \mathbb{N}$ and $b_i \in B$.

Lemma 3.14 ([LOU25, Lemma 3])**.** *Let A be a finite ring with endomorphism θ and θ-derivation δ. Suppose $B \subseteq A$ is a subring such that $A = B[a_1, \ldots, a_s]$ is a free B-algebra and θ, δ restrict to polynomial maps over B. Then any system $\mathcal{E}$ of finitely many equations that are polynomial expressions in the images under θ and δ of a finite set of variables $y_1, \ldots, y_m$, can be translated into a system of polynomial equations over B in the ms variables $y_{i,j}$ such that $y_i = \sum_{j=1}^{s} y_{i,j} a_j$.*

Proof. The action of θ and δ on the B-basis $\{a_1, \ldots, a_s\}$ can be expressed as linear combinations with coefficients in B. By expanding each y_i in terms of the a_j and applying θ and δ using these linear rules, we express all derivatives as B-linear combinations whose coefficients are polynomial expressions in the $y_{i,j}$. The action of the maps θ and δ on this basis is given by:

$$\theta(a_i) = \sum_{j=1}^{s} \gamma_{i,j} a_j, \quad \delta(a_i) = \sum_{j=1}^{s} \beta_{i,j} a_j,$$

for some fixed coefficients $\gamma_{i,j}, \beta_{i,j} \in B$.

Now, for any element $y_i \in A$ written as $y_i = \sum_{j=1}^{s} y_{i,j} a_j$, we compute:

$$\begin{aligned} y_i^\theta &= \left(\sum_{j=1}^{s} y_{i,j} a_j \right)^\theta = \sum_{j=1}^{s} y_{i,j}^\theta a_j^\theta = \sum_{j=1}^{s} y_{i,j}^\theta \left(\sum_{k=1}^{s} \gamma_{j,k} a_k \right), \\ y_i^\delta &= \left(\sum_{j=1}^{s} y_{i,j} a_j \right)^\delta = \sum_{j=1}^{s} (y_{i,j} a_j)^\delta = \sum_{j=1}^{s} \left(y_{i,j}^\delta a_j + y_{i,j}^\theta a_j^\delta \right) \\ &= \sum_{j=1}^{s} \left(y_{i,j}^\delta a_j + y_{i,j}^\theta \sum_{k=1}^{s} \beta_{j,k} a_k \right). \end{aligned}$$

Given:

1. The algebra multiplication rules $a_i a_j = \sum_{k=1}^{s} \mu_{i,j,k} a_k$, with known $\mu_{i,j,k} \in B$,
2. The additive and multiplicative properties of θ and δ,
3. That θ and δ restrict to polynomial maps on B, so $y_{i,j}^\theta$ and $y_{i,j}^\delta$ are polynomial expressions in the $y_{i,j}$ over B,

we can recursively convert any system of polynomial equations in variables $y_1, \ldots, y_m \in A$ into a system of polynomial equations in the components $y_{i,j} \in B$, where $1 \leq i \leq m$, $1 \leq j \leq s$. That is, solutions in A^m are transformed into solutions in B^{ms}. □

The following examples illustrate that there exist endomorphisms θ and θ-derivations δ of a ring A that *are not* polynomial maps over A itself, but *are* polynomial maps over a subring $B \subseteq A$. In both examples, we consider finite commutative rings of order 4 with characteristic 2. We analyze the possible automorphisms and endomorphisms, along with their associated derivations, and determine whether they can be expressed as polynomial maps with coefficients in the ambient ring A. The examples demonstrate that in some cases, certain maps fail to be polynomial over A, even though they may behave polynomially over $\mathbb{F}_2$, the minimal subring.

Example 3.15 ([LOU25, Example 5])**.** *Let $A = \mathbb{F}_2[v]/(v^2 + v)$ be the Frobenius ring of order 4. This ring admits two automorphisms, $\theta_1 = \mathrm{id}$ and θ_2 of order 2, as well as two non-trivial endomorphisms, θ_3 and θ_4. A θ-derivation $\delta\colon A \to A$ is completely*

determined by the value $\delta(v)$ (since $\delta(1) = 0$). All possible θ-derivations are shown in Table 3.2, with the inner derivations highlighted in green. In this case, every θ-derivation is inner.

Table 3.2.: All θ-derivations on $A = \mathbb{F}_2[v]/(v^2 + v)$.

	Automorphism		**Endomorphism**	
	$\theta_1 = \mathrm{id}$	$\theta_2(v) = v + 1$	$\theta_3(v) = 0$	$\theta_4(v) = 1$
$\delta_1 = 0$	$v \mapsto 0$	$v \mapsto 0$	$v \mapsto 0$	$v \mapsto 0$
δ_2		$v \mapsto 1$		
δ_3		$v \mapsto v$	$v \mapsto v$	
δ_4		$v \mapsto v + 1$		$v \mapsto v + 1$

We now show that the automorphism θ_2 cannot be expressed as a polynomial map on A. Assume for contradiction that there exist coefficients $\alpha_{i,j} \in \mathbb{F}_2$ such that

$$\theta_2(x) = \sum_{i \geq 0} (\alpha_{i,1} v + \alpha_{i,0}) x^i = \sum_{i \geq 0} \alpha_{i,1} v x^i + \sum_{i \geq 0} \alpha_{i,0} x^i.$$

Since $\theta_2(0) = 0$, we must have $\alpha_{0,0} = 0$. As $\alpha_{i,j} \in \mathbb{F}_2$, $f(v)$ is a sum of positive powers of v. Moreover, because $v^2 = v$ in A, any power of v reduces to either v^1 or v^0. Thus, $f(v)$ is a sum of v, which is either v or 0 in this ring. But $\theta_2(v) = v+1$, which is neither 0 nor v. Therefore, we obtain that θ_2 is not a polynomial map on A.

So, we observe that automorphisms and derivations of a finite Frobenius ring A are not, in general, polynomial maps over the entire ring A. However, they do exhibit polynomial behavior when restricted to the smallest unitary subring of A, as established in the following lemma.

Lemma 3.16 ([LOU25, Lemma 4])**.** *Let A be a finite Frobenius ring. Then any automorphism and any derivation is a polynomial map over the smallest unitary subring $B \subseteq A$.*

Proof. The smallest unitary subring $B \subseteq A$ is the image of the canonical map $\mathbb{Z} \to A$ given by $1 \mapsto 1$. Let p be the characteristic of the entire ring A. Then B is either isomorphic to the finite field $\mathbb{F}_p$ (if p is a prime number) or to the integer modular ring $\mathbb{Z}_p = \mathbb{Z}/(p)$ (if p is a composite number). Any automorphism θ of A must fix the elements of B, meaning $\theta(x) = x$ for all $x \in B$. Likewise, any θ-derivation δ satisfies $\theta(x) = 0$ for all $x \in B$. Thus, both automorphisms and derivations are polynomial maps over B. □

3.4.2. Computations via Gröbner Bases over a subalgebra

In this section we assume that θ and δ are polynomial maps over a subalgebra $B \subseteq A$. This assumption is always satisfied whenever B is the smallest unitary subring of A (see Theorem 3.16) and $A = B[a_1, \ldots, a_s]$ is a free B-algebra. These assumptions allow us to rewrite any expression involving θ and δ over A (in the variables $y_1, \ldots, y_m$) as a polynomial expression over B in the variables $y_{1,1}, \ldots, y_{1,s}, \ldots, y_{m,1}, \ldots, y_{m,s}$ (cf. Theorem 3.14). To solve such systems, we use the classical method of Gröbner bases for commutative multivariate polynomial rings over B, specifically in the ring

$$B[y_{1,1}, \ldots, y_{1,s}, \ldots, y_{m,1}, \ldots, y_{m,s}].$$

Gröbner basis algorithms exist in particular when B is a field or an integer quotient ring (see [AL22], [BCP97]). Since this includes all possible forms of the smallest unitary subring B of the finite unitary ring A (Theorem 3.16), the method is applicable in our setting.

3.4.2.1. An Algorithm to Compute All Dual-Containing (θ, δ)-Codes

We begin by expressing the unknown coefficients of g and $\hbar$ in A as linear combinations of a fixed B-basis of A, using unknown coefficients $x_i \in B$. The expressions in images under compositions of θ and δ of the coefficients of $\hbar$ and g then become polynomial expressions in the variables x_i, with coefficients in B. From these, we construct a parity-check-like matrix $\boldsymbol{M}$ as described in Lemma 3.8, whose entries are also polynomials in the indeterminates x_i. To ensure that g divides $g\hbar$ on the right, we require that the coefficients of the remainder, each a polynomial in the unknown x_i, vanish. Similarly, the condition $C^{\perp} \subset C$ can be enforced by requiring that all entries of

$$\boldsymbol{M}^{\top} \cdot \boldsymbol{M}$$

(which are also polynomials in the x_i) are zero. Together, these conditions define a multivariate polynomial system over B in the unknowns x_i. If a Gröbner basis algorithm exists for the ring B, we can compute all dual-containing cyclic left module (θ, δ)-codes

$$\mathcal{C} = Rg/Rf \subset R/Rf$$

for the fixed parameters $[n, k]$. It is important to note that the property $\mathcal{C}^{\perp} \subset \mathcal{C}$ depends only on the code $\mathcal{C}$, not on the particular choice of f, h, or $\hbar$. In other words, if the inclusion holds for one valid solution of $f, h, \hbar$, it holds for all valid solutions. Thus, it suffices to compute an elimination ideal for the possible polynomials g and retain only those skew polynomials g that can be extended to a solution of the whole system.

Algorithm 1: Computing all *dual-containing* cyclic module (θ, δ)-codes for given $[n, k]$ (see [LOU25, Algorithm 1])

Input: A, θ, δ, a subalgra $B \subset A$ over which $A = B[a_1, \ldots, a_s]$ is free and over which θ, δ are polynomial maps and the Gröbner basis can be computed, code parameters n, k.

Output: A set of solutions $\mathcal{P} = \{g, \hbar, f \mid \mathcal{C} = Rg/Rf \text{ is dual-containing}\}$

$P_1 \leftarrow B\big[g_{i,j},\ \hbar_{u,v} \mid 0 \le i \le n-k-1,\ 0 \le u \le k-1,\ 1 \le j, v \le s\big]$;
`/* multivariate polynomial ring over` B `*/`

$\mathcal{P} \leftarrow \{\}$; `/* Initialize a set to collect` $g, \hbar$ `of self-dual codes */`

foreach $\hbar_k = \sum_{v=1}^{s} \hbar_{k,v} a_v \in \{$*non-invertible element of* $A\}$ **do**

  $\mathsf{LSEs} \leftarrow \{$Constrains such that $g_{i,j}, \hbar_{u,v} \in B\}$; `/*` $g_{i,j}^p = g_{i,j}, \hbar_{u,v}^p = \hbar_{u,v}$ `if` $B = \mathbb{F}_p$ `*/`

  $g \leftarrow \sum_{i=0}^{n-k-1} (\sum_{j=1}^{s} g_{i,j} a_j) X^i + X^{n-k}$; `/*` $g \in P_1[X; \theta, \delta]$ `*/`

  $\hbar \leftarrow \sum_{u=0}^{k-1} (\sum_{v=1}^{s} \hbar_{u,v} a_v) X^i + (\sum_{v=1}^{s} \hbar_{k,v} a_v) X^k$; `/*` $\hbar \in P_1[X; \theta, \delta]$ `*/`

  $f \leftarrow g \cdot \hbar$; `/*` $LC(f)$ `may not be monic but does not contain variable */`

  $h, r \leftarrow$ quotient, remainder of g right dividing f ; `/*` $h, r \in P_1[X; \theta, \delta]$ `*/`

  $\mathsf{LSEs} \xleftarrow{\text{Append}} \{$All coefficients of r are 0 $\}$; `/* implies` $g \mid_r f$ `*/`

  $\boldsymbol{G} \leftarrow$ a generator matrix constructed from g;

  $\boldsymbol{M} \leftarrow$ the matrix constructed from $\hbar$ according to Theorem 3.9;

  $\mathsf{LSEs} \xleftarrow{\text{Append}} \{$All entries in $\boldsymbol{M}^\top \cdot \boldsymbol{M}$ are $0\}$; `/* implies` $C^\perp \subseteq C$ `*/`

  $\mathcal{S} \leftarrow \{$solutions of $g_{0,1}, \ldots, g_{n-k-1,s}, \hbar_{0,1}, \ldots, \hbar_{k-1,s}$ from the Gröbner basis of $\mathsf{LSEs}\}$;

  $\mathcal{P} \xleftarrow{\text{Append}} \{g, \hbar, f \in A[X; \theta, \delta] : \forall$ solution in $\mathcal{S}\}$;

  `/*` $g, \hbar \in A[X; \theta, \delta]$ `are reconstructed by evaluating coefficients of` $g, \hbar \in P_1[X; \theta, \delta]$ `for each solution in` $\mathcal{S}$`;` f `is reconstructed by` $f = g \cdot \hbar$ `*/`

3.4.2.2. Characterization of the Dual $C^{\perp_\sigma}$ of a Cyclic Module (θ, δ)-Code

Let σ denote either the identity automorphism or an automorphism of order 2 on A. According to Theorem 3.12, the generator matrix $\boldsymbol{G}^{\perp_\sigma} = \sigma(\boldsymbol{H})$ has rows corresponding to skew polynomials $p_1, \ldots, p_k$ in R/Rf, which form an A-basis of the dual code $C^{\perp_\sigma}$. This code is free, and its structure raises the following question: is $C^{\perp_\sigma}$ itself a cyclic module code of the form $Rg^{\perp_\sigma}/R\tilde{f} \subset R/R\tilde{f}$ for some monic skew polynomial $g^{\perp_\sigma}$ of degree k? If such a generator polynomial $g^{\perp_\sigma}$ exists, it must be a left divisor of all the polynomials $p_1, \ldots, p_k$.

We now follow the notation introduced in Algorithm 1. To test whether such a cyclic

structure exists, we define a candidate monic polynomial of degree k of the form

$$g^{\perp_\sigma} = \sum_{i=0}^{k-1} \left(\sum_{j=1}^{s} g_{i,j}^{\perp_\sigma} a_j \right) X^i + X^k \in R,$$

where the coefficients $g_{i,j}^{\perp_\sigma}$ are indeterminates in B. Next, we perform a right division of each polynomial $p_1, \ldots, p_{n-k}$ by $g^{\perp_\sigma}$, and set the resulting remainders $r_1, \ldots, r_{n-k}$ equal to zero. The coefficients of the remainders $r_1, \ldots, r_{n-k}$ are polynomials in the indeterminates $g_{i,j}^{\perp_\sigma}$ with coefficients in B (so the polynomials are elements in $B[g_{0,1}^{\perp_\sigma}, \ldots, g_{k-1,s}^{\perp_\sigma}]$). The condition that all remainders vanish yields a multivariate polynomial system over B. This system can be solved using a Gröbner basis algorithm. If the resulting Gröbner basis is $\{1\}$, the system has no solution, and hence $C^{\perp_\sigma}$ is not a cyclic module code in R/Rf for any $f \in R$. Otherwise, the Gröbner basis gives the generator polynomial $g^{\perp_\sigma}$ of degree k for a cyclic module code $C^{\perp_\sigma}$.

3.5. Computational Results for $\mathbb{F}_2[v]/(v^2+v)$

We retain the notation from Example 3.15 and compute dual-containing cyclic left module (θ, δ)-codes over the ring $A = \mathbb{F}_2[v]/(v^2+v)$ using the algorithm described in Section 3.4.2.1. By Lemma 3.16, we may work over the subalgebra $B = \mathbb{F}_2 \subset A$ for these computations. Codes of small length over A have been classified in [Huf05]. Following [DS01], we define the Lee weight of the elements $0, 1, v, v+1$ as $0, 2, 1, 1$ respectively, and the Bachoc weight as $0, 1, 2, 2$ respectively. Table 3.3a and Table 3.4 show the best Euclidean and Hermitian dual-containing codes $\mathcal{C} = Rg/Rf \subset R/Rf$; all possible codes of this kind are identified by the algorithm. An empty set indicates that no dual-containing code $Rg/Rf \subset R/Rf$ exists for the corresponding parameters $[n, k]$. A question mark indicates that such a code does exist, but its minimum distance was not computed. Codes that cannot be found without using non-zero derivations are highlighted in light green; those that require both a non-zero derivation and an endomorphism that is not an automorphism are marked in darker green. Examples include the three distinct weight distributions of the $[6, 4]$ codes shown in Table 3.5. Finally, Table 3.5 and Table 3.6 provide a detailed overview of which Hamming weight enumerators could only be obtained using specific (θ, δ) combinations.

Table 3.3.: Results on dual-containing cyclic module (θ, δ)-code over $\mathbb{F}_2[v]/(v^2+v)$.

(a) Best Hamming, Lee and Bachoc d_H, d_L, d_B distance of dual-containing (θ, δ)-codes over $\mathbb{F}_2[v]/[v^2+v]$

$n \setminus k$	2	3	4	5	6	7	8	9	10	11	12
3	$1,1,2$										
4	$2,2,4$	$2,2,2$									
5		$\emptyset$	$\emptyset$								
6		$2,2,2$	$2,2,2$	$2,2,2$							
7			$3,3,5$	$\emptyset$	$\emptyset$						
8			$4,4,7$	$2,2,4$	$2,2,2$	$2,2,2$					
9				$\emptyset$	$\emptyset$	$\emptyset$	$1,1,2$				
10				$2,2,2$	$2,2,2$	$\emptyset$	$\emptyset$	$2,2,2$			
11					$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$		
12					$4,4,6$	$3,3,4$	$2,2,?$	$2,?,?$	$?,?,?$	$?,?,?$	
13						$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$

(b) Existence of cyclic module structure in the duals $C^\perp$ of dual-containing cyclic (θ, δ)-codes $C = Rg/Rf \subset R/Rf$ over $\mathbb{F}_2[v]/[v^2+v]$, based on the criterion from Section 3.4.2.2.

$n \setminus k$	2	3	4	5	6	7	8	9
3	None							
4	All	Some						
5		/	/					
6		All	Some	Some				
7			All	/	/			
8			All	Some	Some	Some		
9				/	/	/	None	
10				All	Some	/	/	All

(c) Number of dual-containing (θ, δ)-codes and how many of them have a dual that is also a cyclic module (θ, δ)-code. (Only parameter sets marked as "Some" in Table 3.3(b) are included.)

$[n, k]$	# of dual-containing cyclic module codes Rg/Rf for each (θ, δ) # of those whose dual is also cyclic (θ, δ)-code								
	$(\mathrm{Id}; 0)$	$(\theta_2, 0)$	(θ_2, δ_2)	(θ_2, δ_3)	(θ_2, δ_4)	$(\theta_3, 0)$	(θ_3, δ_3)	$(\theta_4, 0)$	(θ_4, δ_4)
$[4, 3]$	1	1	3	1	1	1	2	1	2
	1	1	1	1	1	1	1	1	1
$[6, 4]$	1	1	1	2	2	1	4	1	4
	1	1	1	1	1	1	2	1	2
$[6, 5]$	1	1	1	2	2	1	1	1	1
	1	1	1	1	1	1	1	1	1
$[8, 5]$	1	3	5	1	1	1	8	1	8
	1	3	1	1	1	1	1	1	1
$[8, 6]$	1	3	5	1	1	1	4	1	4
	1	3	3	1	1	1	2	1	2
$[8, 7]$	1	1	3	1	1	1	2	1	2
	1	1	1	1	1	1	1	1	1
$[10, 6]$	1	1	1	1	1	1	16	1	16
	1	1	1	1	1	1	2	1	2

Table 3.4.: Best Hamming, Lee, Bachoc distance of θ_2-Hermitian dual-containing (θ,δ)-codes over $\mathbb{F}_2[v]/(v^2+v)$.

$n \setminus k$	2	3	4	5	6	7	8	9
4	$2,2,4$	$2,2,2$						
5		$2,2,2$	$1,1,2$					
6		$3,3,4$	$2,2,4$	$2,2,2$				
7			$3,3,5$	$1,1,2$	$1,1,2$			
8			$3,3,6$	$2,2,4$	$2,2,2$	$2,2,2$		
9				$1,1,2$	$\emptyset$	$\emptyset$	$\emptyset$	
10				$2,2,2$	$2,2,2$	$\emptyset$	$\emptyset$	$2,2,2$

Table 3.5.: Hamming weight enumerator of dual-containing (θ,δ)-codes over $\mathbb{F}_2[v]/[v^2+v]$.

$[n,k]$	Hamming Weight Enumerator	Constructed with (θ,δ)
[4,2]	$1+6w^2+9w^4$	all combinations (θ,δ) provide such an example
	$1+4w^2+4w^3+7w^4$	$(\theta_2,\delta_2),\ (\theta_3,\delta_3),\ (\theta_4,\delta_4)$
[6,3]	$1+9w^2+27w^4+\ldots$	all combinations (θ,δ) provide such an example
[6,4]	$1+9w^2+24w^3+\ldots$	all combinations (θ,δ) provide such an example
	$1+17w^2+24w^3+\ldots$	$(\theta_2,\delta_3),\ (\theta_2,\delta_3)$
	$1+2w+11w^2+\ldots$	$(\theta_3,\delta_3),\ (\theta_4,\delta_4)$
	$1+13w^2+24w^3+\ldots$	$(\theta_3,\delta_3),\ (\theta_4,\delta_4)$
[8,4]	$1+12w^2+54w^4+\ldots$	all combinations (θ,δ) provide such an example
	$1+28w^4+56w^5+\ldots$	$(\theta_2,0)$
	$1+4w^2+38w^4+\ldots$	$(\theta_2,\delta_2),\ (\theta_3,\delta_3),\ (\theta_4,\delta_4)$

Table 3.6.: Hamming weight enumerator of θ_2-Hermitian dual-containing (θ,δ)-codes over $\mathbb{F}_2[v]/[v^2+v]$.

$[n,k]$	Hamming Weight Enumerator	Constructed with (θ,δ)
[4,2]	$1+6w^2+9w^4$	all combinations (θ,δ) provide such an example
	$1+2w^2+8w^3+5w^4$	$(\theta_2,0)$
[4,3]	$1+18w^2+24w^3+21w^4$	all combinations (θ,δ) provide such an example
	$1+2w+16w^2+22w^3+23w^4$	$(\theta_2,\delta_2),\ (\theta_3,\delta_3),\ (\theta_4,\delta_4)$
	$1+2w+12w^2+30w^3+19w^4$	$(\theta_2,\delta_3),\ (\theta_2,\delta_4)$
[5,3]	$1+8w^2+14w^3+23w^4+18w^5$	$(\theta_2,\delta_3),\ (\theta_2,\delta_4)$
	$1+w+6w^2+14w^3+\ldots$	$(\theta_3,\delta_3),\ (\theta_4,\delta_4)$
[5,4]	$1+3w+22w^2+66w^3+\ldots$	$(\theta_2,\delta_3),\ (\theta_2,\delta_4)$
[6,3]	$1+9w^2+27w^4+\ldots$	all combinations (θ,δ) provide such an example
	$1+8w^3+21w^4+24w^5+10w^6$	$(\theta_3,\delta_3),\ (\theta_4,\delta_4)$

Table 3.7.: $[6, 4]$ dual-containing (θ, δ)-codes over $\mathbb{F}_2[v]/(v^2 + v)$ with Hamming weight enumerator $1 + 13w^2 + 24w^3 + \ldots$.

Index	g	(θ, δ)	**G**
1	$X^2 + X + v + 1$	(θ_3, δ_3)	$\begin{bmatrix} v+1 & 1 & 1 & 0 & 0 & 0 \\ v & 1 & 1 & 1 & 0 & 0 \\ v & 0 & 1 & 1 & 1 & 0 \\ v & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$
2	$X^2 + (v + 1)X + 1$	(θ_3, δ_3)	$\begin{bmatrix} 1 & v+1 & 1 & 0 & 0 & 0 \\ 0 & v+1 & 1 & 1 & 0 & 0 \\ 0 & v & 1 & 1 & 1 & 0 \\ 0 & v & 0 & 1 & 1 & 1 \end{bmatrix}$
3	$X^2 + vX + 1$	(θ_4, δ_4)	$\begin{bmatrix} 1 & v & 1 & 0 & 0 & 0 \\ 0 & v & 1 & 1 & 0 & 0 \\ 0 & v+1 & 1 & 1 & 1 & 0 \\ 0 & v+1 & 0 & 1 & 1 & 1 \end{bmatrix}$
4	$X^2 + X + v$	(θ_4, δ_4)	$\begin{bmatrix} v & 1 & 1 & 0 & 0 & 0 \\ v+1 & 1 & 1 & 1 & 0 & 0 \\ v+1 & 0 & 1 & 1 & 1 & 0 \\ v+1 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$

Beyond the complexity of computing a Gröbner basis, the computational effort in our approach also stems from the fact that, for a fixed polynomial g, there may exist many different factorizations of the form $f = hg = g\hbar$. Despite these variations, all such combinations define the same code, since the generator matrix depends solely on g and the associated ring $A[X, \theta, \delta]$. To illustrate this, we show in more detail the results of the $[6, 4]$ code with Hamming weight enumerator $1 + 13w^2 + 24w^3 + \ldots$. In this case, there are four possible generator polynomials g, listed in Table 3.7. Once g and the ring $A[X, \theta, \delta]$ are fixed, constructing a generator matrix for the code is straightforward. As a specific example, consider the first polynomial in the table:

$$g = X^2 + X + v + 1 \in \left(\mathbb{F}_2[v]/[v^2 + v]\right)[X; \theta_3, \delta_3].$$

For this g, there exist eight distinct *non-central* polynomials f for which there are polynomials h and $\hbar$ such that $f = hg = g\hbar$, that is, g acts as both a left and right divisor of f:

$$
\begin{aligned}
f_1 &= X^6 + vX^4 + vX^3 + vX + v + 1 = (X^4 + X^3 + vX^2 + X + v + 1) \cdot g,\\
f_2 &= X^6 + X^5 + (v+1)X^4 + X^3 + vX + v + 1 = (X^4 + vX^2 + (v+1)X + 1) \cdot g,\\
f_3 &= X^6 + (v+1)X^4 + vX^3 + vX^2 + X + v + 1 = (X^4 + X^3 + (v+1)X^2 + 1) \cdot g,\\
f_4 &= X^6 + X^5 + vX^4 + X^3 + vX^2 + X + v + 1 = (X^4 + (v+1)X^2 + vX + v + 1) \cdot g,\\
f_5 &= X^6 + vX^4 + vX^3 + X^2 + (v+1)X = (X^4 + X^3 + vX^2 + X + v) \cdot g,\\
f_6 &= X^6 + X^5 + (v+1)X^4 + X^3 + X^2 + (v+1)X = (X^4 + vX^2 + (v+1)X) \cdot g,\\
f_7 &= X^6 + (v+1)X^4 + vX^3 + (v+1)X^2 = (X^4 + X^3 + (v+1)X^2) \cdot g,\\
f_8 &= X^6 + X^5 + vX^4 + X^3 + (v+1)X^2 = (X^4 + (v+1)X^2 + vX + v) \cdot g.
\end{aligned}
$$

For each polynomial f_i, there exists a unique polynomial h such that $f_i = hg$. Additionally, there are exactly 16 distinct polynomials $\hbar$ satisfying $f_i = g\hbar$. Among these 16, one of the $\hbar$ is equal to the corresponding h, meaning that g is simultaneously a left and right divisor of f_i. The following are the 15 distinct polynomials $\hbar \neq h$ such that $f_1 = g \cdot \hbar$, where $g = X^2 + X + v + 1$ and $f_1 = (X^4 + X^3 + vX^2 + X + v + 1) \cdot g$:

$$
\begin{aligned}
f_1 &= g \cdot \left(X^4 + (v+1)X^3 + vX^2 + (v+1)X + v + 1\right) = g \cdot \left(X^4 + X^3 + X + v + 1\right)\\
&= g \cdot \left(X^4 + X^3 + (v+1)X + v + 1\right) = g \cdot \left(X^4 + (v+1)X^3 + vX^2 + X + v + 1\right)\\
&= g \cdot \left(X^4 + (v+1)X^3 + X + v + 1\right) = g \cdot \left(X^4 + (v+1)X^3 + vX^2 + (v+1)X + 1\right)\\
&= g \cdot \left(X^4 + X^3 + vX^2 + (v+1)X + 1\right) = g \cdot \left(X^4 + (v+1)X^3 + (v+1)X + 1\right)\\
&= g \cdot \left(X^4 + X^3 + (v+1)X + 1\right) = g \cdot \left(X^4 + (v+1)X^3 + (v+1)X + v + 1\right)\\
&= g \cdot \left(X^4 + (v+1)X^3 + vX^2 + X + 1\right) = g \cdot \left(X^4 + X^3 + vX^2 + X + 1\right)\\
&= g \cdot \left(X^4 + (v+1)X^3 + X + 1\right) = g \cdot \left(X^4 + X^3 + X + 1\right)\\
&= g \cdot \left(X^4 + X^3 + vX^2 + (v+1)X + v + 1\right).
\end{aligned}
$$

We apply the algorithm presented in Subsection 3.4.2.2 to determine for which dual-containing codes $C = Rg/Rf \subset R/Rf$ the dual code $C^\perp$ is itself a cyclic module (θ, δ)-code. An overview of the results is provided in Table 3.3b and Table 3.3c. The following two examples demonstrate that not all dual-containing cyclic module (θ, δ)-codes have a dual that is again a cyclic module code:

- For $[n = 4, k = 3]$, we found three generator polynomials $g \in A[X; \theta_2, \delta_2]$ that yield dual-containing cyclic module codes:

  $$g_1 = X + v + 1, \quad g_2 = X + 1, \quad g_3 = X + v.$$

  Among these, only the dual of $g_2 = X + 1$ is a cyclic module code with

  $$g_2^\perp = X^3 + X^2 + X + 1.$$

- For $[n = 6, k = 4]$, we found four generator polynomials $g \in A[X; \theta_3, \delta_3]$ corresponding to dual-containing cyclic module codes:

$$g_1 = X^2 + (v+1)X + v + 1,$$
$$g_2 = X^2 + X + 1,$$
$$g_3 = X^2 + X + v + 1,$$
$$g_4 = X^2 + (v+1)X + 1.$$

  Only the duals of g_2 and g_4 yield cyclic module codes with

$$g_2^\perp = X^4 + X^3 + X + 1, \quad g_4^\perp = X^4 + (v+1)X^3 + X + v + 1.$$

3.6. Computational Results for $\mathbb{F}_2[u]/(u^2)$

We retain the notation from Example 3.5, where the ring is given by $A = \mathbb{F}_2[u]/(u^2)$. By Lemma 3.16 and Algorithm 1, we can search for dual-containing cyclic left module (θ, δ)-codes $\mathcal{C} = Rg/Rf \subset R/Rf$ using a Gröbner basis approach over the subalgebra $B = \mathbb{F}_2 \subset A$.

Following [DS01], we define the Lee weight of the elements $0, 1, u, u+1$ as $0, 1, 2, 1$, respectively, and the Euclidean weight as $0, 1, 4, 1$.

Table 3.8 provides an overview of the best dual-containing codes $\mathcal{C} = Rg/Rf \subset R/Rf$ (the algorithm found all such codes). In the cells marked in green, the corresponding codes were identified only when using the maps (id, δ_2) and (id, δ_4).

Table 3.8.: Best Hamming, Lee, and Euclidean distances of dual-containing cyclic module (θ, δ)-codes over $\mathbb{F}_2[u]/(u^2)$.

$n \setminus k$	2	3	4	5	6	7	8	9
4	$2,4,4$	$2,2,2$						
5		$\emptyset$	$1,2,2$					
6		$2,4,4$	$2,2,2$	$2,2,2$				
7			$3,3,3$	$\emptyset$	$1,2,2$			
8			$4,4,4$	$2,4,4$	$2,2,2$	$2,2,2$		
9				$\emptyset$	$\emptyset$	$\emptyset$	$1,2,2$	
10				$2,4,6$	$2,4,5$	$\emptyset$	$\emptyset$	$2,2,2$

Table 3.9 summarizes the cases in which the duals $C^\perp$ of the dual-containing cyclic module codes $\mathcal{C} = Rg/Rf \subset R/Rf$, identified via Algorithm 1, are themselves cyclic module (θ, δ)-codes, as discussed in Section 3.4.2.2.

Table 3.10 shows examples in which Hamming weight enumerators could only be found using specific (θ, δ) combinations. In particular the green cells indicate those that can only be obtained using a non-zero derivation.

Table 3.9.: Combinations of (θ, δ) for which the dual $C^\perp$ of a dual-containing cyclic (θ, δ)-codes $C = Rg/Rf \subset R/Rf$ over $\mathbb{F}_2[u]/(u^2)$ has a cyclic module structure, based on the criterion from Section 3.4.2.2.

$n \setminus k$	2	3	4	5	6	7	8	9
4	All	All						
5		/	(Id, δ_2): None (Id, δ_4): All					
6		All	All	All				
7			All	/	All			
8			All	All	All	All		
9				/	/	/	(Id, δ_2): None (Id, δ_4): Some	
10				All	All	/	/	All

Table 3.10.: Hamming weight enumerator of dual-containing (θ, δ)-codes over $\mathbb{F}_2[u]/(u^2)$.

$[n, k]$	Hamming Weight Enumerator	Constructed with (θ, δ)
[4,2]	$1 + 2w^2 + 8w^3 + 5w^4$	$(\mathrm{id}, 0)$, (id, δ_2), (id, δ_3), (θ_2, δ_2)
	$1 + 6w^2 + 9w^4$	all combinations (θ, δ) provide such an example
[8,4]	$1 + 4w^2 + 30w^4 + \ldots$	$(\mathrm{id}, 0)$, (θ_2, δ_2)
	$1 + 4w^2 + 46w^4 + \ldots$	$(\mathrm{id}, 0)$
	$1 + 4w^2 + 16w^3 + \ldots$	$(\mathrm{id}, 0)$
	$1 + 12w^2 + 54w^4 + \ldots$	all combinations (θ, δ) provide such an example
	$1 + 26w^4 + 64w^5 + \ldots$	(id, δ_2)
[8,5]	$1 + 4w^2 + 16w^3 + 94w^4 + \ldots$	$(\mathrm{id}, 0)$, (id, δ_2)
	$1 + 4w^2 + 16w^3 + 110w^4 + \ldots$	$(\mathrm{id}, 0)$
	$1 + 12w^2 + 102w^4 + \ldots$	all combinations (θ, δ) provide such an example
	$1 + 16w^2 + 8w^3 + 114w^4 + \ldots$	(id, δ_2)

3.7. Computational Results for $\mathbb{F}_4$

The finite field $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ with $\alpha^2 = \alpha + 1$ has two automorphisms: the identity $\theta_1 = \mathrm{id}$ and the Frobenius automorphism $\theta_2 : x \mapsto x^2$. The automorphism θ_2 has order 2 and is a polynomial map over both $\mathbb{F}_4$ and its subfield $\mathbb{F}_2$. All θ-derivations in this setting are inner derivations; these are highlighted in green in the list below.

Table 3.11.: All θ-derivations on $A = \mathbb{F}_4$.

	Automorphism	
	$\theta_1 = \mathrm{id}$	$\theta_2(\alpha) = \alpha + 1$
$\delta_1 = 0$	$\alpha \mapsto 0$	$\alpha \mapsto 0$
δ_2		$\alpha \mapsto 1$
δ_3		$\alpha \mapsto \alpha$
δ_4		$\alpha \mapsto \alpha + 1$

As in [DS01] we define the Lee weight of $0, 1, \alpha, \alpha{+}1$ respectively as $0, 2, 1, 1$. According to [LS01] we define the corresponding Euclidean weight respectively as $0, 1, 2, 1$.

Table 3.12 presents the existence and best Hamming, Lee, and Euclidean distances (d_H, d_L, and d_E, respectively) of θ_2-Hermitian dual-containing cyclic module (θ, δ)-codes $\mathcal{C} = Rg/Rf \subset R/Rf$ over $\mathbb{F}_4$. Green-shaded cells indicate codes that can only be obtained using non-zero derivations.

Table 3.12.: Best Hamming, Lee, and Euclidean distances of θ_2-Hermitian dual-containing codes $Rg/Rf \subset R/Rf$ over $\mathbb{F}_4$.

$n \setminus k$	2	3	4	5	6	7	8	9
4	$2,2,2$	$2,2,2$						
5		$3,3,3$	$1,1,1$					
6		$4,4,4$	$2,2,2$	$2,2,2$				
7			$3,3,3$	$\emptyset$	$1,1,1$			
8			$2,2,2$	$2,2,2$	$2,2,2$	$2,2,2$		
9				$\emptyset$	$\emptyset$	$\emptyset$	$1,1,1$	
10				$4,4,4$	$3,3,3$	$2,2,2$	$2,2,2$	$2,2,2$

Table 3.13 illustrates representative Hamming weight distributions of selected codes.

This demonstrates that, in the Hermitian case, non-zero derivations yield codes that do not arise in the $\delta = 0$ setting. In contrast, no new codes were found when restricting to $\delta = 0$.

Table 3.13.: Weight enumerator of θ_2-Hermitian dual-containing cyclic module (θ,δ)-codes over $\mathbb{F}_4$.

$[n,k]$	Hamming Weight Enumerator	Constructed with (θ,δ)
[4,3]	$1+18w^2+24w^3+211w^4$	all combinations (θ,δ) provide such an example
	$1+6w+12w^2+18w^3+27w^4$	(θ_2,δ_2)
[5,4]	$1+9w+30w^2+54w^3+81w^4+81w^5$	(θ_2,δ_2)
[6,5]	$1+45w^2+120w^3+315w^4+360w^5+183w^6$	all combinations (θ,δ) provide such an example
	$1+12w+57w^2+144w^3+243w^4+324w^5+243w^6$	(θ_2,δ_2)
[7,6]	$1+15w+93w^2+315w^3+675w^4+1053w^5+\ldots$	(θ_2,δ_2)
[8,7]	$1+84w^2+336w^3+1470w^4+\ldots$	all combinations (θ,δ) provide such an example
	$1+18w+138w^2+594w^3+1620w^4+\ldots$	(θ_2,δ_2)
[9,8]	$1+21w+192^2+1008w^3+3402w^4+\ldots$	(θ_2,δ_2)
[10,9]	$1+135w^2+720w^3+4410w^4+15120w^5+\ldots$	all combinations (θ,δ) provide such an example
	$1+24w+255w^2+1584w^3+6426w^4+\ldots$	(θ_2,δ_2)

3.8. Computational Results for the Galois Ring $GR(4,2)$

The Galois ring $A=\mathrm{GR}(4,2)=\mathbb{Z}_4[u]=(\mathbb{Z}/4\mathbb{Z})[u]/(u^2+u+1)$ is a Frobenius ring of order 16. This ring admits two automorphisms: the identity $\theta_1=\mathrm{id}$ and a nontrivial automorphism θ_2 defined by $\theta_2(u)=3u+3$. The automorphism θ_2 generates a cyclic group of order 2.

The only id-derivation is the zero derivation. In contrast, all θ_2-derivations are inner derivations, meaning they are of the form

$$\delta(a)=\beta a-\theta_2(a)\beta \quad \text{for some } \beta\in A.$$

The following list shows all θ_2-derivations, one for each $\beta\in A$, expressed by their action on u:

$$\begin{aligned}
&\delta_1(u)=0, && \delta_2(u)=u, && \delta_3(u)=2u, && \delta_4(u)=3u,\\
&\delta_5(u)=1, && \delta_6(u)=u+1, && \delta_7(u)=2u+1, && \delta_8(u)=3u+1,\\
&\delta_9(u)=2, && \delta_{10}(u)=u+2, && \delta_{11}(u)=2u+2, && \delta_{12}(u)=3u+2,\\
&\delta_{13}(u)=3, && \delta_{14}(u)=u+3, && \delta_{15}(u)=2u+3, && \delta_{16}(u)=3u+3.
\end{aligned}$$

We computed all $[4,2]$ self-dual and $[4,3]$ dual-containing cyclic left module (θ,δ)-codes over $A=\mathrm{GR}(4,2)$ as described in Algorithm 1.

For the $[4,2]$ case, each map in Table 3.14 yields 8 distinct generator polynomials g, each of which defines a $[4,2,d_H=3]$ code. While the resulting codes have distinct codebooks (i.e., the sets of codewords differ), they all share the same weight enumerator:

$1+60w^3+195w^4$. For each such g, there are 16 valid choices of f, all of which are central elements. Each set includes at least one f of the form $X^n - a$ for some $a \in \mathbb{Z}_4$.

The $[4, 3]$ dual-containing codes can also be obtained for all (θ, δ) maps. Each map yields four distinct generator polynomials g, and for each g, there are over 1000 corresponding f's. These include at least one central f and at least one of the form $X^n - a$ with $a \in \mathbb{Z}_4$. All resulting codes share the same weight enumerator, as listed in Table 3.14.

Table 3.14.: The best Hamming distance d_H of dual-containing codes $Rg/Rf \subset R/Rf$ over $GR(4, 2)$.

$[n, k]$	Existing code for map (θ_i, δ_j)	Best d_H	Weight Distribution
[3,2]	$(1,1),\ (2,2),\ (2,4),\ (2,6),\ (2,8),$ $(2,10),\ (2,12),\ (2,14),\ (2,16)$	2	$1 + 45w^2 + 210w^3$
[4,2]	$(2,1),\ (2,3),\ (2,9),\ (2,11)$	3	$1 + 60w^3 + 195w^4$
[4,3]	All maps	2	$1 + 90w^2 + 840w^3 + 3165w^4$
[5,3]	$\emptyset$	/	/

Part II

Codes in the Sum-Rank Metric

4

Properties of the Sum-Rank Metric

The sum-rank metric, a generalization of both the Hamming and rank metric, gained prominence, particularly motivated by its application in multi-shot network coding. Initially introduced in 2005 in [LK05, Section III] for defining space-time codes and later in 2010 using multilevel rank-metric code constructions for multishot network coding in [NUF10], the sum-rank metric holds significance in both theoretical and practical contexts. In this chapter, we begin by introducing the concept of so-called *elementary linear subspaces*, providing valuable insights as an analytical tool for sum-rank metric analysis. In the main part of this chapter, the second section, we delve into the geometric properties of spheres and balls in the sum-rank metric. This includes exploring the volumes of sum-rank-metric spheres and balls, along with an analysis of the volume of the intersection of two balls. All notations and concepts used throughout this chapter have been introduced in Chapter 2. Unless explicitly stated otherwise, all vectors are elements in $\mathbb{F}_{q^m}^n$, which can be divided into ℓ blocks, represented as $\boldsymbol{x} = [\boldsymbol{x}_0|\dots|\boldsymbol{x}_{\ell-1}]$. Each block $\boldsymbol{x}_i \in \mathbb{F}_{q^m}^\eta$ has a size of η, so the total vector size is $n = \eta \cdot \ell$. Consequently, when we replace ℓ with 1, we are referring to the rank metric, and when ℓ equals n, we are dealing with the Hamming metric. Additionally, we represent by μ the minimum value of m and η. The findings presented in this chapter have been published in [OPB21], [OLWZ22] and [OLWZ23].

4.1. The Connection Between the Sum-Rank Metric and Elementary Linear Subspaces

In the field of linear algebra it is a commonly acknowledged principle, that one can represent a vector $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$ with rank weight $\mathrm{wt}_{SR,1}(\boldsymbol{v}) \leq r \leq n$ as a product of the form $[a_0, \dots, a_{r-1}] \cdot \boldsymbol{B}$, where a_i belongs to $\mathbb{F}_{q^m}$ for each $i \in \{0, \dots, r-1\}$, and $\boldsymbol{B}$ is an $r \times n$ matrix with a rank of $\mathrm{rk}(\boldsymbol{B}) = r$. This representation leads to the introduction of what are called *"elementary linear subspace"*. This concept is a valuable tool when studying properties of the sum-rank metric and codes in this metric. In the realm of rank-metric codes, the concept of elementary linear subspaces has been extensively explored in prior work such as [GY08b] and [GY08a]. In this subsection, we will provide the definition of an elementary linear subspace, recall some established findings, and also adapt known

results that are employed in the rank metric for the usage in the context of the sum-rank metric. The results presented here will be utilized in Section 4.2 to examine geometrical properties of the sum-rank metric. Furthermore, these results will play a crucial role in Chapter 5, primarily to investigate covering properties of sum-rank-metric codes, but also to explore so-called *Maximum Sum-Rank Distance (MSRD) Codes*.

First we provide the definition of an elementary linear subspace.

Definition 4.1 (Elementary Linear Subspace)**.** Let $\mathcal{V} \subset \mathbb{F}_{q^m}^n$ be a linear subspace of $\mathbb{F}_{q^m}^n$ of dimension k. If there exists a basis $\{\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{k-1}\}$ of $\mathcal{V}$ with $\boldsymbol{b}_i \in \mathbb{F}_q^n$ for each $i \in \{0, \ldots, k-1\}$, then $\mathcal{V}$ is called an *elementary linear subspace* of $\mathbb{F}_{q^m}^n$. We denote the set of all elementary linear subspaces of $\mathbb{F}_{q^m}^n$ with dimension $\dim(\mathcal{V}) = k$ by $\mathcal{E}_k(\mathbb{F}_{q^m}^n)$.

In [GY08a], it was illustrated that each vector in $\mathbb{F}_{q^m}^n$ of rank weight at most k belongs to an elementary linear subspace of dimension k. Furthermore, in [GY08b] it was demonstrated that when a vector has precisely rank weight k, it uniquely corresponds to an elementary linear subspace. We will now recap these results in the following two lemmas.

Lemma 4.2 ([GY08a])**.** *Let $\boldsymbol{v}$ be a vector in $\mathbb{F}_{q^m}^n$ and k a positive integer with $k \leq \min\{m, n\}$. Then the rank weight of $\boldsymbol{v}$ is $\mathrm{wt}_{SR,1}(\boldsymbol{v}) \leq k$ if and only if there exists a $\mathcal{V} \in \mathcal{E}_k(\mathbb{F}_{q^m}^n)$ such that $\boldsymbol{v} \in \mathcal{V}$.*

Lemma 4.3 ([GY08b])**.** *Every vector $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$ with rank weight $\mathrm{wt}_{SR,1}(\boldsymbol{v}) = k$, where k is a positive integer satisfying $k \leq \min\{m, n\}$, belongs to a unique elementary linear subspace $\mathcal{V} \in \mathcal{E}_k(\mathbb{F}_{q^m}^n)$.*

Lemma 4.2 and Lemma 4.3 show the connection between elementary linear subspaces in $\mathbb{F}_{q^m}^n$ and the rank weight of a vector in $\mathbb{F}_{q^m}^n$. We further expand upon this concept in the subsequent corollaries to establish a link between a sequence of elementary linear subspaces in $\mathbb{F}_{q^m}^\eta$ and the sum-rank weight of a vector in $\mathbb{F}_{q^m}^n$, where each block belongs to $\mathbb{F}_{q^m}^\eta$. The following corollary is the sum-rank metric pendant to Lemma 4.2, showing that each vector of sum-rank weight at most k belongs to a Cartesian product $\mathcal{V} = \mathcal{V}_0 \times \ldots \times \mathcal{V}_{\ell-1}$ of subspaces of $\mathbb{F}_{q^m}^\eta$.

Corollary 4.4. *Let $\boldsymbol{v} = [\boldsymbol{v}_0 | \ldots | \boldsymbol{v}_{\ell-1}] \in \mathbb{F}_{q^m}^n$ be a vector comprising ℓ blocks $\boldsymbol{v}_i \in \mathbb{F}_{q^m}^\eta$ with $i \in \{0, \ldots, \ell-1\}$ and k a positive integer fulfilling $k \leq \mu \cdot \ell$. The sum-rank weight of $\boldsymbol{v}$ is $\mathrm{wt}_{SR,\ell}(\boldsymbol{v}) \leq k$ if and only if there are elementary linear subspaces $\mathcal{V}_0, \ldots, \mathcal{V}_{\ell-1}$ of $\mathbb{F}_{q^m}^\eta$ such that $\boldsymbol{v}_i$ belongs to $\mathcal{V}_i$ for each $i \in \{0, \ldots, \ell-1\}$, meaning that the entire vector $\boldsymbol{v} = [\boldsymbol{v}_0 | \ldots | \boldsymbol{v}_{\ell-1}]$ corresponds to the Cartesian product of these subspaces $\mathcal{V} \coloneqq \mathcal{V}_0 \times \ldots \times \mathcal{V}_{\ell-1}$ and the sum of their dimensions satisfies $\sum_{i=0}^{\ell-1} \dim(\mathcal{V}_i) = k$.*

Proof. Let the sum-rank weight of $\boldsymbol{v}$ be $\mathrm{wt}_{SR,\ell}(\boldsymbol{v}) = k' \leq k$. Then the weight decomposition of $\boldsymbol{v}$ satisfies $\sum_{i=0}^{\ell-1} \mathrm{wt}_{SR,1}(\boldsymbol{v}_i) = k'$. We denote by k_i the rank weight of the i-th block, i.e., $\mathrm{wt}_{SR,1}(\boldsymbol{v}_i) = k_i$. By applying Lemma 4.2 we can conclude that there exist elementary linear subspaces $\mathcal{V}_0, \ldots, \mathcal{V}_{\ell-1}$ with $\boldsymbol{v}_i \in \mathcal{V}_i \in \mathcal{E}_{k_i}(\mathbb{F}_{q^m}^\eta)$ for all $i \in \{0, \ldots, \ell-1\}$ such that $\sum_{i=0}^{\ell-1} k_i = k'$. In the case where $k' < k$, we choose one

subspace $\mathcal{V}_j \in \mathcal{E}_{k_j}(\mathbb{F}_{q^m}^{\eta})$ of the subspaces $\mathcal{V}_0, \ldots, \mathcal{V}_{\ell-1}$ arbitrary. It holds now that there is a superspace $\tilde{\mathcal{V}}_j \in \mathcal{E}_{k_j+k-k'}(\mathbb{F}_{q^m}^{\eta})$ of $\mathcal{V}_j$ which implies that $\boldsymbol{v}_j \in \mathcal{V}_j \subset \tilde{\mathcal{V}}_j$. Hence, $\boldsymbol{v} \in \mathcal{V} \coloneqq \mathcal{V}_0 \times \ldots \times \mathcal{V}_{j-1} \times \tilde{\mathcal{V}}_j \times \mathcal{V}_{j+1} \times \ldots \times \mathcal{V}_{\ell-1}$. Finally, it holds that $\sum_{i=0, i\neq j}^{\ell-1} \dim(\mathcal{V}_i) + \dim(\tilde{\mathcal{V}}_j) = k$.

Now we prove the reverse direction. Let therefore be again $\boldsymbol{v} = [\boldsymbol{v}_0|\ldots|\boldsymbol{v}_{\ell-1}]$ a vector in $\in \mathbb{F}_{q^m}^n$. Suppose that there is a Cartesian product of elementary linear subspaces $\mathcal{V} = \mathcal{V}_0 \times \ldots \times \mathcal{V}_{\ell-1}$ with $\mathcal{V}_i \in \mathcal{E}_{k_i}(\mathbb{F}_{q^m}^{\eta})$ for $i \in \{0, \ldots, \ell-1\}$, fulfilling $\sum_{i=0}^{\ell-1} \dim(\mathcal{V}_i) = k$. We denote by k_i the dimension of $\mathcal{V}_i$ for each $i \in \{0, \ldots, \ell-1\}$. With Lemma 4.2 it follows that each block $\boldsymbol{v}_i$ ($i \in \{0, \ldots, \ell-1\}$) has rank weight $\mathrm{wt}_{SR,1}(\boldsymbol{v}_i) \leq k_i$ and hence $\mathrm{wt}_{SR,\ell}(\boldsymbol{v}) = \sum_{i=0}^{\ell-1} \mathrm{wt}_{SR,1}(\boldsymbol{v}_i) \leq \sum_{i=0}^{\ell-1} k_i = k$. □

The following corollary serves as the sum-rank metric counterpart to Lemma 4.3. It demonstrates that a vector with a sum-rank weight precisely equal to k is associated to a uniquely determined Cartesian product of elementary linear subspaces, given a fixed weight decomposition.

Corollary 4.5. *Let $k \leq \mu \cdot \ell$ be a positive integer and and let $\boldsymbol{v} = [\boldsymbol{v}_0|\ldots|\boldsymbol{v}_{\ell-1}] \in \mathbb{F}_{q^m}^n$ be a vector of sum-rank weight k with a fixed sum-rank weight decomposition $\sum_{i=0}^{\ell-1} k_i = k$, where $\mathrm{wt}_{SR,1}(\boldsymbol{v}_i) = k_i$ for each block $i \in \{0, \ldots, \ell-1\}$. Then there exists a unique Cartesian product of elementary linear subspaces $\mathcal{V} \coloneqq \mathcal{V}_0 \times \ldots \times \mathcal{V}_{\ell-1}$ where each $\mathcal{V}_i \in \mathcal{E}_{k_i}(\mathbb{F}_{q^m}^{\eta})$ such that $\boldsymbol{v} \in \mathcal{V}$.*

Proof. For a vector $\boldsymbol{v} = [\boldsymbol{v}_0|\ldots|\boldsymbol{v}_{\ell-1}] \in \mathbb{F}_{q^m}^n$ with $\mathrm{wt}_{SR,1}(\boldsymbol{v}_i) = k_i$, Lemma 4.3 implies that there are uniquely determined subspaces $\mathcal{V}_0, \ldots, \mathcal{V}_{\ell-1}$ of $\mathbb{F}_{q^m}^{\eta}$ such that $\boldsymbol{v}_i \in \mathcal{V}_i \in \mathcal{E}_{k_i}(\mathbb{F}_{q^m}^{\eta})$ for each block $i \in \{0, \ldots, \ell-1\}$. The entire vector $\boldsymbol{v}$ is an element of the Cartesian product $\mathcal{V} \coloneqq \mathcal{V}_0 \times \ldots \times \mathcal{V}_{\ell-1}$. □

In [GY08a], it was demonstrated that for any subspace $\mathcal{V} \in \mathcal{E}_k(\mathbb{F}_{q^m}^n)$, there exists a complement $\bar{\mathcal{V}} \in \mathcal{E}_{n-k}(\mathbb{F}_{q^m}^n)$ such that their direct sum forms the entire space, i.e., $\mathcal{V} \oplus \bar{\mathcal{V}} = \mathbb{F}_{q^m}^n$. In [GY08b], the number of such decompositions was provided. We revisit this in the forthcoming lemma.

Lemma 4.6 ([GY08b])**.** *Let $\mathcal{V}$ be an elementary linear subspace in $\mathcal{E}_k(\mathbb{F}_{q^m}^n)$. For a given subspace $\mathcal{A} \in \mathcal{E}_a(\mathcal{V})$, there exist $q^{a\cdot(k-a)}$ elementary linear subspaces $\mathcal{B} \in \mathcal{E}_{k-a}(\mathcal{V})$, such that $\mathcal{A} \oplus \mathcal{B} = \mathcal{V}$. If we do not fix A, then for each $\mathcal{V} \in \mathcal{E}_k(\mathbb{F}_{q^m}^n)$ there are $q^{a\cdot(k-a)} \cdot \begin{bmatrix} k \\ a \end{bmatrix}_q$ pairs $(\mathcal{A}, \mathcal{B})$ satisfying $\mathcal{A} \oplus \mathcal{B} = \mathcal{V}$.*

We extend the result of the recently introduced lemma to be utilized in the sum-rank metric.

Corollary 4.7. *For given positive integers k and a, satisfying $a \leq k \leq \mu \cdot \ell$ and elementary linear subspaces $\mathcal{V} = \mathcal{V}_0 \times \ldots \times \mathcal{V}_{\ell-1} \in \mathcal{E}_{k_1}(\mathbb{F}_{q^m}^{\eta}) \times \ldots \times \mathcal{E}_{k_\ell}(\mathbb{F}_{q^m}^{\eta}) = \mathcal{E}_k(\mathbb{F}_{q^m}^n)$ with*

fixed partitions $k = \sum_{i=0}^{\ell-1} k_i$ *and* $a = \sum_{i=0}^{\ell-1} a_i$ *satisfying* $a_i \leq k_i$ *for all* $i \in \{0, \ldots, \ell-1\}$ *there exist*

$$\prod_{i=0}^{\ell-1} q^{a_i \cdot (k_i - a_i)} \cdot \begin{bmatrix} k_i \\ a_i \end{bmatrix}_q$$

pairs of Cartesian products $(\mathcal{A}, \mathcal{B}) = (\mathcal{A}_0 \times \ldots \times \mathcal{A}_{\ell-1}, \mathcal{B}_0 \times \ldots \times \mathcal{B}_{\ell-1})$ *such that* $\mathcal{A}_i \oplus \mathcal{B}_i = \mathcal{V}_i$ *for all* $i \in \{0, \ldots, \ell-1\}$.

Proof. This conclusion follows directly from Lemma 4.6. □

In [GY08b], the behavior of the rank weight of a vector upon projection onto both a subspace and its complement was explained. We recapitulate this in the following lemma. To denote the projection of a vector $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$ onto an elementary linear subspace $\mathcal{V}$ of $\mathbb{F}_{q^m}^n$ along its complement $\bar{\mathcal{V}}$, we use the notation $\boldsymbol{v}^{(\mathcal{V})}$. Note that $\boldsymbol{v} = \boldsymbol{v}^{(\mathcal{V})} + \boldsymbol{v}^{(\bar{\mathcal{V}})}$.

Lemma 4.8. *[GY08b] Let* $\mathcal{V}$ *be an elementary linear subspace belonging to* $\mathcal{E}_k(\mathbb{F}_{q^m}^n)$*, let* k *and* a *be positive integers fulfilling* $a \leq k \leq \min\{m, n\}$ *and let* $\boldsymbol{u}$ *be a vector belongig to* $\mathcal{V}$ *with rank weight* $\mathrm{wt}_{SR,1}(\boldsymbol{u}) = k$*. For any pair of subspaces* $(\mathcal{A}, \mathcal{B}) \in \mathcal{E}_a(\mathbb{F}_{q^m}^n) \times \mathcal{E}_{k-a}(\mathbb{F}_{q^m}^n)$ *satisfying* $\mathcal{A} \oplus \mathcal{B} = \mathcal{V}$*, the following holds: the rank weight of the projection of* $\boldsymbol{u}$ *onto* $\mathcal{A}$ *is* $\mathrm{wt}_{SR,1}(\boldsymbol{u}^{(\mathcal{A})}) = a$ *whereas the rank weight of the projection of* $\boldsymbol{u}$ *onto* $\mathcal{B}$ *is* $\mathrm{wt}_{SR,1}(\boldsymbol{u}^{(\mathcal{B})}) = k - a$*. The functions*

$$\phi_{\boldsymbol{u}} : \mathcal{E}_a(\mathbb{F}_{q^m}^n) \times \mathcal{E}_{k-a}(\mathbb{F}_{q^m}^n) \to \mathcal{A}, \quad (\mathcal{A}, \mathcal{B}) \mapsto \boldsymbol{u}^{(\mathcal{A})}$$

$$\psi_{\boldsymbol{u}} : \mathcal{E}_a(\mathbb{F}_{q^m}^n) \times \mathcal{E}_{k-a}(\mathbb{F}_{q^m}^n) \to \mathcal{B}, \quad (\mathcal{A}, \mathcal{B}) \mapsto \boldsymbol{u}^{(\mathcal{B})}$$

are both injective.

In [GY08b] a bijection was established between two elementary linear subspaces with equal dimension, where vector spaces underlie that differ only in the extension degree of the underlying field. We recall this in the following lemma.

Lemma 4.9. *[GY08b] Let* u, n, m *be positive integers with* $u > 1$*. Let* $\alpha_0, \ldots, \alpha_{m-1}$ *be a basis of* $\mathbb{F}_{q^m}$ *over* $\mathbb{F}_q$ *with* $\alpha_0 = 1$ *and let* $\beta_0, \ldots, \beta_{m+u-1}$ *be a basis of* $\mathbb{F}_{q^{m+u}}$ *over* $\mathbb{F}_q$ *with* $\beta_0 = 1$*. Moreover, we define* $\mathcal{B}_m := \langle \beta_0, \ldots, \beta_{m-1} \rangle$*. The mapping*

$$f_u : \mathbb{F}_{q^m} \to \mathcal{B}_m, \quad \alpha_i \mapsto f_u(\alpha_i) = \beta_i \quad \text{for all } i \in \{0, \ldots, m-1\}$$

is linear and bijective. So each element $a = \sum_{i=0}^{m-1} a_i \alpha_i \in \mathbb{F}_{q^m}$ *is mapped to* $f_u(a) = f(\sum_{i=0}^{m-1} a_i \alpha_i) = \sum_{i=0}^{m-1} a_i f_u(\alpha_i) = \sum_{i=0}^{m-1} a_i \beta_i$*. Since* $\alpha_0 = \beta_0 = 1$*, it follows that* $f_u(\mathbb{F}_q) = \mathbb{F}_q$*. We extend* f_u *to* n*-dimensional vectors by just applying it componentwise:*

$$\bar{f}_u : \mathbb{F}_{q^m}^n \to \mathcal{B}_m^n, \quad \boldsymbol{v} = [v_0, \ldots, v_{n-1}] \mapsto \bar{f}_u(\boldsymbol{v}) = [f_u(v_0), \ldots, f_u(v_{n-1})].$$

For a positive integer r *with* $r < n$*, let* $\mathcal{V}$ *be an elementary linear subspace belonging to* $\mathcal{E}_r(\mathbb{F}_{q^m}^n)$*. Then the image* $\bar{f}_u(\mathcal{V})$ *is a subset of an elementary linear subspace of* $\mathbb{F}_{q^{m+u}}^n$ *with dimension* r*. Moreover,* $\bar{f}_u$ *establishes a bijection between* $\mathcal{E}_r(\mathbb{F}_{q^m}^n)$ *and* $\mathcal{E}_r(\mathbb{F}_{q^{m+u}}^n)$*.*

4.2. Spheres and Balls in the Sum-Rank Metric

In this section, we define spheres and balls in the sum-rank metric, along with their respective volumes. We also provide a link to a previously known algorithm that allows us to exactly and efficiently compute these volumes. Furthermore, we present both upper and lower bounds on these volumes that offer more streamlined calculations. The results find application when studying bounds on the cardinalities of sum-rank-metric codes and when investigating the covering properties of sum-rank-metric codes in Chapter 5.

Definition 4.10 (Sum-Rank-Metric Spheres, Balls and their Volume)**.** Let $\delta \in \mathbb{N}_0$ with $\delta \leq \ell \cdot \mu$ and $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$. A sum-rank-metric sphere with radius δ and center $\boldsymbol{x}$ is defined as

$$\mathcal{S}_\ell(\boldsymbol{x}, \delta)_{\mathbb{F}_{q^m}^n} \coloneqq \{\boldsymbol{y} \in \mathbb{F}_{q^m}^n \mid \mathrm{d}_{SR,\ell}(\boldsymbol{x}, \boldsymbol{y}) = \delta\}.$$

Analogously, we define a ball of sum-rank radius δ with center $\boldsymbol{x}$ by

$$\mathcal{B}_\ell(\boldsymbol{x}, \delta)_{\mathbb{F}_{q^m}^n} \coloneqq \bigcup_{i=0}^{\delta} \mathcal{S}_\ell(\boldsymbol{x}, i).$$

Also we define the volume of a sphere and a ball in the sum-rank metric as follows:

$$\mathrm{Vol}_{\mathcal{S}_\ell}(\delta)_{\mathbb{F}_{q^m}^n} \coloneqq |\{\boldsymbol{y} \in \mathbb{F}_{q^m}^n \mid \mathrm{wt}_{SR,\ell}(\boldsymbol{y}) = \delta\}|,$$

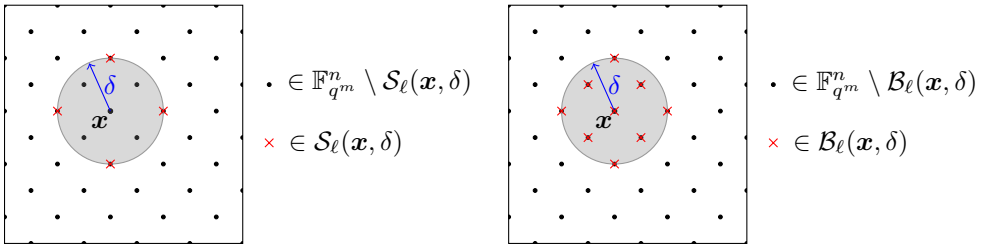
$$\mathrm{Vol}_{\mathcal{B}_\ell}(\delta)_{\mathbb{F}_{q^m}^n} \coloneqq \sum_{i=0}^{\delta} \mathrm{Vol}_{\mathcal{S}_\ell}(i).$$

For improved readability, we will omit the subscript $\mathbb{F}_{q^m}^n$ when referring to spheres, balls and their volumes in $\mathbb{F}_{q^m}^n$ from now on, and we will simply denote the respective sets and cardinalities by $\mathcal{S}_\ell(\boldsymbol{x}, \delta)$, $\mathcal{B}_\ell(\boldsymbol{x}, \delta)$, $\mathrm{Vol}_{\mathcal{S}_\ell}(\delta)$ and $\mathrm{Vol}_{\mathcal{B}_\ell}(\delta)$. If we discuss other vector spaces, we will explicitly specify them in the subscript.

Figure 4.1 illustrates a sum-rank-metric sphere and a sum-rank-metric ball of radius δ, both centered at the point $\mathbf{x}$.

4.2.1. The Volume of Spheres and Balls in the Sum-Rank Metric

Because the sum-rank metric is invariant under the translation of vectors, the sizes represented by $\mathrm{Vol}_{\mathcal{S}_\ell}(\delta)$ and $\mathrm{Vol}_{\mathcal{B}_\ell}(\delta)$ are not influenced by the positions of their centers and therefore $\mathrm{Vol}_{\mathcal{S}_\ell}(\delta)$ and $\mathrm{Vol}_{\mathcal{B}_\ell}(\delta)$ correspond to the volume of any shpere and any ball of radius δ, respectively. In contrast to the extreme cases, Hamming and rank metric, calculating these volumes in general is a complex task. The formula for computing the volume of a sum-rank-metric sphere given in [BGLR21, Definition III.4] consists of a sum whose number of terms can grow super-polynomially in δ, depending on how ℓ and η compare in size. In [PRR22] a dynamic programming algorithm has been provided, enabling an efficient computation of the volume of a sum-rank-metric sphere within a polynomial time frame. In order to give the exact volume of a sum-rank-metric sphere



(a) Sphere with sum-rank radius δ and center $\mathbf{x}$.

(b) Ball with sum-rank radius δ and center $\mathbf{x}$.

Figure 4.1.: Spheres and balls in the sum-rank metric.

and ball, it is crucial to consider, that for a given sum-rank radius δ, there are numerous potential weight decompositions. This is why we need to introduce and investigate the following set of all possible sum-rank weight decompositions:

$$\mathcal{T}_{\delta,\ell,\mu} \coloneqq \left\{ [\delta_0, \ldots, \delta_{\ell-1}] \in \mathbb{N}_0^\ell \mid \sum_{i=0}^{\ell-1} \delta_i = \delta, \delta_i \leq \mu \quad \forall i \in \{0, \ldots, \ell-1\} \right\}, \tag{4.1}$$

which corresponds combinatorially to the set of ordered partitions of the integer δ into ℓ terms each of size at most μ. Its cardinality corresponds to the δ-th coefficient of the generating function

$$p^{(\ell,\mu)}(x) \coloneqq \left(\sum_{i=0}^{\mu} x^i \right)^\ell,$$

i.e.,

$$p_\delta^{(\ell,\mu)} = |\mathcal{T}_{\delta,\ell,\mu}| = \sum_{i=0}^{\left\lfloor \frac{\delta}{\mu+1} \right\rfloor} (-1)^i \binom{\ell}{i} \binom{\delta + \ell - 1 - (\mu+1)i}{\ell - 1}$$

(see also [Rat08] and [PRR22]). In particular, the cardinality of $\mathcal{T}_{\delta,\ell,\mu}$ can be computed efficiently and is upper bounded by

$$|\mathcal{T}_{\delta,\ell,\mu}| \leq \tbinom{\delta+\ell-1}{\ell-1}. \tag{4.2}$$

This upper bound is obtained by using a stars and bars argument (see also [PRR22]). Together with the cardinalities introduced in Chapter 2.1.3 we can now provide the exact volume of a sum-rank-metric sphere and ball:

$$\mathrm{Vol}_{\mathcal{S}_\ell}(\delta) = \sum_{\substack{[\delta_0,\ldots,\delta_{\ell-1}] \\ \in \mathcal{T}_{\delta,\ell,\mu}}} \prod_{i=0}^{\ell-1} \mathrm{NM}_q(\eta, m, \delta_i) \quad \text{and} \tag{4.3}$$

$$\mathrm{Vol}_{\mathcal{B}_\ell}(\delta) = \sum_{j=0}^{\delta} \sum_{\substack{[\delta_0,\ldots,\delta_{\ell-1}] \\ \in \mathcal{T}_{j,\ell,\mu}}} \prod_{i=0}^{\ell-1} \mathrm{NM}_q(\eta, m, \delta_i), \tag{4.4}$$

consisting of all vectors in $\mathbb{F}_{q^m}^n$ of sum-rank weight δ and all vectors of sum-rank weight lower than or equal to δ, respectively. The volume of a sum-rank-metric ball with radius δ can be computed in complexity $\mathcal{O}^{\sim}(\ell^2\delta^3 + \ell\delta^4(m+\eta)\log(q))$, where the $\mathcal{O}$ notation $\mathcal{O}^{\sim}(\cdot)$ neglects logarithmic factors in the input parameters, using the efficient algorithm for computing $\mathrm{Vol}_{\mathcal{S}_\ell}$ in [PRR22]. Even though the complexity is polynomial, the calculation remains time-consuming for large parameters. Therefore, we give bounds on the volume of a sum-rank-metric ball that can be computed faster than the exact volume.

4.2.2. Bounds on the Volume of Sum-Rank-Metric Spheres and Balls

In this section, we provide both a lower and an upper bound on the volume of a sum-rank-metric ball. To establish the lower bound, our initial step is to derive a lower bound on the number of $m \times n$ matrices over $\mathbb{F}_q$ of rank δ. We address this in the following lemma.

Lemma 4.11 ([OPB21, Lemma 1])**.** *The number of all $m \times n$ matrices over $\mathbb{F}_q$ of rank $\delta \leq \min\{m,n\}$ is bounded by*

$$\mathrm{NM}_q(n,m,\delta) \geq q^{(m+n-\delta)\delta}\gamma_q^{-1}.$$

Proof. In [KK08], the following lower bound for the q-binomial coefficient was provided:

$$\begin{bmatrix} n \\ \delta \end{bmatrix}_q \geq q^{(n-\delta)\delta}.$$

By applying this bound to the q-binomial coefficient, we derive the following bound on the number of $m \times n$ matrices over $\mathbb{F}_q$ of rank $\delta \leq \min\{m,n\}$:

$$\begin{aligned}
\mathrm{NM}_q(n,m,\delta) &\geq q^{(n-\delta)\delta}\prod_{i=0}^{\delta-1}(q^m - q^i) = q^{(n+m-\delta)\delta}\prod_{i=0}^{\delta-1}(1-q^{i-m}) \\
&\geq q^{(n+m-\delta)\delta}\prod_{j=1}^{\delta}(1-q^{-j}) \geq q^{(n+m-\delta)\delta}\prod_{j=1}^{\infty}(1-q^{-j}) \\
&\geq q^{(n+m-\delta)\delta}\gamma_q^{-1}.
\end{aligned}$$

□

Using this bound enables us to establish the following lower bound on the volume of a sum-rank-metric sphere $\mathrm{Vol}_{\mathcal{S}_\ell}(\delta)$ and a sum-rank-metric ball $\mathrm{Vol}_{\mathcal{B}_\ell}(\delta)$ which encompasses all vectors in $\mathbb{F}_{q^m}^n$ of sum-rank weight δ and $\leq \delta$, respectively.

Theorem 4.12 ([OPB21, Lemma 2])**.** *For the volumes of a sphere and a ball with a sum-rank radius of δ, the following inequalities apply:*

$$\mathrm{Vol}_{\mathcal{B}_\ell}(\delta) \geq \mathrm{Vol}_{\mathcal{S}_\ell}(\delta) \geq q^{(m+\eta-\frac{\delta}{\ell})\delta-\frac{\ell}{4}} \cdot \gamma_q^{-\ell}.$$

Proof. We have

$$\begin{aligned}\mathrm{Vol}_{\mathcal{S}_\ell}(\delta) &= \sum_{\substack{[\delta_0,\ldots,\delta_{\ell-1}]\\ \in\mathcal{T}_{\delta,\ell,\mu}}} \prod_{i=0}^{\ell-1} \mathrm{NM}_q(\eta,m,\delta_i) \\ &\geq \max_{\substack{[\delta_0,\ldots,\delta_{\ell-1}]\\ \in\mathcal{T}_{\delta,\ell,\mu}}} \left\{ \prod_{i=0}^{\ell-1} q^{(m+\eta-\delta_i)\delta_i} \gamma_q^{-1} \right\} \\ &= q^{(m+\eta)\delta} \cdot q^{-\min_{\substack{[\delta_0,\ldots,\delta_{\ell-1}]\\ \in\mathcal{T}_{\delta,\ell,\mu}}} \left\{ \sum_{i=0}^{\ell-1} \delta_i^2 \right\}} \cdot \gamma_q^{-\ell}.\end{aligned}$$

Given that ℓ is not equal to 0, it is feasible to represent $\delta \in \mathbb{N}_0$ in the form

$$\delta = \delta_* \cdot \ell + r, \quad \text{with } 0 \leq r < \ell.$$

The expression $\sum_{i=0}^{\ell-1} \delta_i^2$ is minimized by the so-called *quasi-equal decomposition*, i.e., $[\delta_0,\ldots,\delta_{\ell-1}]$ with $\delta_{i_1} = \ldots = \delta_{i_r} = \delta_* + 1$ and $\delta_{i_r} = \ldots = \delta_{i_l} = \delta_*$. By employing this weight decomposition, we obtain the minimum

$$\min_{\substack{[\delta_0,\ldots,\delta_{\ell-1}]\\ \in\mathcal{T}_{\delta,\ell,\mu}}} \left\{ \sum_{i=0}^{\ell-1} \delta_i^2 \right\} = r \cdot (\delta_* + 1)^2 + (\ell - r) \cdot \delta_*^2 = \frac{\delta^2 - r^2}{\ell} + r.$$

Since $\max_{r\in\mathbb{N}_{\leq \ell-1}} \{r - \frac{r^2}{\ell}\} \leq \frac{\ell}{4}$, it can be concluded that

$$\min_{\substack{[\delta_0,\ldots,\delta_{\ell-1}]\\ \in\mathcal{T}_{\delta,\ell,\mu}}} \left\{ \sum_{i=0}^{\ell-1} \delta_i^2 \right\} \leq \frac{\delta^2}{\ell} + \frac{\ell}{4}.$$

Consequently,

$$\mathrm{Vol}_{\mathcal{S}_\ell}(\delta) \geq q^{(m+\eta)\delta} \cdot q^{-\frac{\delta^2}{\ell} - \frac{\ell}{4}} \cdot \gamma_q^{-\ell}.$$

The statement follows because the volume of a ball is always larger than or equal to the volume of a sphere with the same radius. □

For the special case that the number of blocks ℓ is a divisor of the radius δ, we can simplify the statement in Theorem 4.12 as follows.

Remark 4.13 ([OPB21, Remark 2])**.** *It is evident from the proof of Theorem 4.12 that when ℓ divides δ, we obtain a simpler bound:*

$$\mathrm{Vol}_{\mathcal{B}_\ell}(\delta) \geq \mathrm{Vol}_{\mathcal{S}_\ell}(\delta) \geq q^{(m+\eta-\frac{\delta}{\ell})\delta} \cdot \gamma_q^{-\ell}.$$

This allows us to omit the term $-\frac{\ell}{4}$ from the exponent of q.

To establish an upper bound for the volume of a sum-rank-metric ball, we leverage the following existing upper bound on the volume of a sum-rank-metric sphere.

Theorem 4.14 ([PRR22])**.** *The volume of a sphere in the sum-rank metric with a radius of δ is upper bounded as follows:*

$$\mathrm{Vol}_{\mathcal{S}_\ell}(\delta) \leq \binom{\ell+\delta-1}{\ell-1}\gamma_q^\ell q^{\delta(m+\eta-\frac{\delta}{\ell})}.$$

This result allows us to readily deduce the following upper bound on the volume of a ball. We make the assumption of $\delta > 1$ to simplify the statement and avoid more technical details.

Theorem 4.15 ([OPB21])**.** *For $\delta > 1$, the volume of a ball in the sum-rank metric with a radius of δ is upper bounded as follows:*

$$\mathrm{Vol}_{\mathcal{B}_\ell}(\delta) \leq \binom{\ell+\delta-1}{\ell-1}\delta\gamma_q^\ell q^{\delta(m+\eta-\frac{\delta}{\ell})}.$$

Proof. Due to

$$\mathrm{Vol}_{\mathcal{B}_\ell}(\delta) = \sum_{i=0}^{\delta}\mathrm{Vol}_{\mathcal{S}_\ell}(i) \leq \delta\mathrm{Vol}_{\mathcal{S}_\ell}(\delta)$$

for $\delta > 1$, we immediatly get the upper bound on $\mathrm{Vol}_{\mathcal{B}_\ell}(t)$ with Theorem 4.14. □

4.2.3. The Intersection of Two Balls in Sum-Rank Metric

We define the volume of the intersection of two balls with sum-rank radii δ, δ' and sum-rank distance τ between their centers.

Definition 4.16 (Intersection of two Balls in Sum-Rank Metric)**.** Let $\delta, \delta', \tau \in \mathbb{N}_0$ with $\delta, \delta' \leq \ell \cdot \mu$, and $\boldsymbol{x}, \boldsymbol{x}' \in \mathbb{F}_{q^m}^n$. We denote the intersection of two sum-rank-metric balls $\mathcal{B}_\ell(\boldsymbol{x}, \delta)$ and $\mathcal{B}_\ell(\boldsymbol{x}', \delta')$ by

$$\mathcal{I}_\ell(\boldsymbol{x}, \delta, \boldsymbol{x}', \delta')_{\mathbb{F}_{q^m}^n} \coloneqq \mathcal{B}_\ell(\boldsymbol{x}, \delta) \cap \mathcal{B}_\ell(\boldsymbol{x}', \delta').$$

Its volume is only dependent on their radii δ, δ' and the distance $\tau = \mathrm{d}_{SR,\ell}(\boldsymbol{x}, \boldsymbol{x}')$ between their respective centers, but not on the position of their centers (cf. Figure 4.2). This volume is determined by counting the number of vectors that exist within this intersection, which can be represented as:

$$\mathrm{Vol}_{\mathcal{I}_\ell}(\delta, \delta', \tau)_{\mathbb{F}_{q^m}^n} \coloneqq |\{\boldsymbol{y} \in \mathbb{F}_{q^m}^n | \mathrm{wt}_{SR,\ell}(\boldsymbol{y}) \leq \delta \wedge \mathrm{d}_{SR,\ell}(\boldsymbol{y}, \boldsymbol{d}) \leq \delta'\}|,$$

where $\boldsymbol{d} \in \mathbb{F}_{q^m}^n$ is arbitrary but fixed with $\mathrm{wt}_{SR,\ell}(\boldsymbol{d}) = \tau$. Obviously if $\tau > \delta + \delta'$, the balls do not intersect, hence $\mathrm{Vol}_{\mathcal{I}_\ell}(\delta, \delta', \tau)_{\mathbb{F}_{q^m}^n} = 0$. In the same manner as we did for the notations of spheres, balls, and their volumes, we will in the following also exclude the subscript $\mathbb{F}_{q^m}^n$ when mentioning the intersection of two balls in $\mathbb{F}_{q^m}^n$. We will instead simply use the notations $\mathcal{I}_\ell(\boldsymbol{x}, \delta, \boldsymbol{x}', \delta')$ and $\mathrm{Vol}_{\mathcal{I}_\ell}(\delta, \delta', \tau)$. If we are discussing vector spaces other than $\mathbb{F}_{q^m}^n$, we will explicitly indicate them with the appropriate subscript.

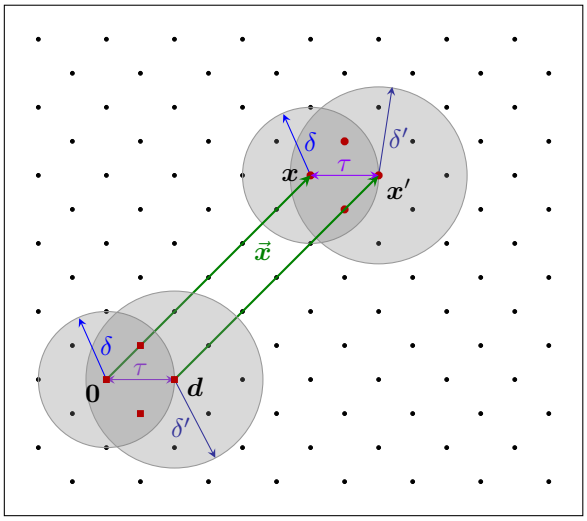


Figure 4.2.: Translation invariance of the intersection of two balls in the sum-rank metric.

The number of vectors in $\mathbb{F}_{q^m}^n$ that are situated within the intersection of two rank-metric balls was given in [GY09] for the case $m \geq n$. Here, we provide this cardinality without the restriction $m \geq n$.

Theorem 4.17 (cf. [GY09])**.** *The volume of the intersection of two rank-metric balls in the vector space $\mathbb{F}_{q^m}^n$ with radii δ, δ' having distance τ between their centers fulfilling $\delta + \delta' \geq \tau$ is given by*

$$\mathrm{Vol}_{\mathcal{I}_1}(\delta,\delta',\tau) = \frac{1}{q^{mn}\mathrm{NM}_q(n,m,\tau)} \sum_{i=0}^{\delta}\sum_{j=0}^{\delta'}\sum_{s=0}^{\kappa} \mathrm{NM}_q(n,m,s)\mathfrak{K}_i(s,\kappa)\mathfrak{K}_j(s,\kappa)\mathfrak{K}_\tau(s,\kappa),$$

with $\iota \coloneqq \max\{m,n\}$, $\kappa \coloneqq \min\{m,n\}$ and

$$\mathfrak{K}_\delta(x,\kappa) \coloneqq \sum_{j=0}^{\delta}(-1)^{\delta-j}q^{j\iota+\binom{\delta-j}{2}} \begin{bmatrix}\kappa-j\\ \kappa-\delta\end{bmatrix}_q \begin{bmatrix}\kappa-x\\ j\end{bmatrix}_q$$

is the generalized q-Krawtchouk polynomial as given in Chapter 2.1.3 with $c = q^{\iota-\kappa}$.

With this cardinality we can now deduce the volume of the intersection of two balls in the sum-rank metric.

Theorem 4.18 ([OLWZ23, Theorem 1])**.** *Let δ, δ', τ be positive integers such that $\delta + \delta' \geq \tau$. The number of vectors $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$ lying in the intersection of two balls with*

sum-rank radii δ and δ' and sum-rank distance τ between their centers is

$$\begin{aligned}&\mathrm{Vol}_{\mathcal{I}_\ell}(\delta,\delta',\tau)\\ &=\sum_{\substack{[\delta_0,\ldots,\delta_{\ell-1}]\\ \in\mathcal{T}_{\delta,\ell,\mu}}}\sum_{\substack{[\delta'_1,\ldots,\delta'_\ell]\\ \in\mathcal{T}_{\delta',\ell,\mu}}}\sum_{\substack{[\tau_1,\ldots,\tau_\ell]\\ \in\mathcal{T}_{\tau,\ell,\mu}}}\prod_{i=0}^{\ell-1}\mathrm{Vol}_{\mathcal{I}_1}(\delta_i,\delta'_i,\tau_i)_{\mathbb{F}_{q^m}^\eta}.\end{aligned}$$

Proof. Let $\mathcal{B}_\ell(\boldsymbol{x},\delta)$ and $\mathcal{B}_\ell(\boldsymbol{x}',\delta')$ be two sum-rank-metric balls with centers

$$\boldsymbol{x}=[\boldsymbol{x}_0|\ldots|\boldsymbol{x}_{\ell-1}],\quad \boldsymbol{x}'=[\boldsymbol{x}'_0|\ldots|\boldsymbol{x}'_{\ell-1}]\in\mathbb{F}_{q^m}^n$$

and sum-rank distance $\mathrm{d}_{SR,\ell}(\boldsymbol{x},\boldsymbol{x}')=\tau$ between their centers. When we fix the partitions of their radii as $\delta=\sum_{i=0}^{\ell-1}\delta_i$ and $\delta'=\sum_{i=0}^{\ell-1}\delta'_i$ as well as the partition of the distance between their centers as $\tau=\sum_{i=0}^{\ell-1}\tau_i$, it holds that for each block $i\in\{0,\ldots,\ell-1\}$ the number of vectors $\boldsymbol{v}_i\in\mathbb{F}_{q^m}^\eta$ having a rank distance of at most δ_i to $\boldsymbol{x}_i$, i.e., $\mathrm{d}_{SR,1}(\boldsymbol{x}_i,\boldsymbol{v}_i)_{\mathbb{F}_{q^m}^\eta}\leq\delta_i$ and also $\mathrm{d}_{SR,1}(\boldsymbol{x}'_i,\boldsymbol{v}_i)_{\mathbb{F}_{q^m}^\eta}\leq\delta'_i$ is given by $\mathrm{Vol}_{\mathcal{I}_1}(\delta_i,\delta'_i,\tau_i)_{\mathbb{F}_{q^m}^\eta}$. Consequently, the number of vectors $\boldsymbol{v}\in\mathbb{F}_{q^m}^n$ having a sum-rank distance of at most δ to $\boldsymbol{x}$ and a sum-rank distance of at most δ' to $\boldsymbol{x}'$ can be determined as $\prod_{i=0}^{\ell-1}\mathrm{Vol}_{\mathcal{I}_1}(\delta_i,\delta'_i,\tau_i)_{\mathbb{F}_{q^m}^\eta}$ for the chosen partitions. For an arbitrary choice of the partitions of the radii δ and δ' and the distance between the centers τ, the claim follows. □

Calculating the volume of the intersection of two sum-rank-metric balls in this general scenario is computationally demanding. However, driven by the motivation of discovering bounds on covering problems in Chapter 5, our objective is to explore more efficient methods for computing this volume. Therefore, we present the volume of the intersection for two specific cases, in which efficient computation is feasible. Similar statements for the rank metric were previously presented in [GY08b]. In the first case, we consider one ball with a radius of δ and another with a radius of 1, separated by a distance of δ between their centers. In order to calculate the volume of the intersection in this instance, we initially need to determine the number of pairs of two vectors having sum-rank weights 1 and δ, respectively, while also satisfying the requirement that the sum of their rank weights equals to the rank weight of their difference. The number of these pairs is established in the following lemma.

Lemma 4.19 ([OLWZ23, Lemma 7])**.** *Let $\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_{q^m}^n$ with $\mathrm{wt}_{SR,1}(\boldsymbol{y})=1$ and $\mathrm{wt}_{SR,1}(\boldsymbol{x})=\delta$. Then there exist*

$$\frac{(q^n-q^\delta)(q^m-q^\delta)}{q-1}$$

pairs of $(\boldsymbol{x},\boldsymbol{y})$ that satisfy $\mathrm{wt}_{SR,1}(\boldsymbol{x})+\mathrm{wt}_{SR,1}(\boldsymbol{y})=\mathrm{wt}_{SR,1}(\boldsymbol{x}-\boldsymbol{y})$.

Proof. Let $\boldsymbol{x},\boldsymbol{y}$ be vectors in $\mathbb{F}_{q^m}^n$ with rank weights $\mathrm{wt}_{SR,1}(\boldsymbol{y})=1$ and $\mathrm{wt}_{SR,1}(\boldsymbol{x})=\delta$, respectively. Let $\mathcal{B}$ be an arbitrary $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$ and $\boldsymbol{X}\coloneqq\mathrm{ext}_{\mathcal{B}}(\boldsymbol{x})\in\mathbb{F}_q^{m\times n}$ the matrix representation of $\boldsymbol{x}\in\mathbb{F}_{q^m}^n$ w.r.t. the basis $\mathcal{B}$. We denote by $\langle\boldsymbol{x}\rangle_{\mathrm{row}}$ the $\mathbb{F}_q$-row space of $\boldsymbol{X}$

and by $\langle \boldsymbol{x} \rangle_{\text{col}}$ its $\mathbb{F}_q$-column space. The equation $\text{wt}_{SR,1}(\boldsymbol{x}) + \text{wt}_{SR,1}(\boldsymbol{y}) = \text{wt}_{SR,1}(\boldsymbol{x}-\boldsymbol{y})$ holds true if and only if $\dim(\langle \boldsymbol{x} \rangle_{\text{row}} \cap \langle \boldsymbol{y} \rangle_{\text{row}}) = \dim(\langle \boldsymbol{x} \rangle_{\text{col}} \cap \langle \boldsymbol{y} \rangle_{\text{col}}) = \{\boldsymbol{0}\}$ whereas this statement is equivalent to $\langle \boldsymbol{y} \rangle_{\text{row}} \not\subset \langle \boldsymbol{x} \rangle_{\text{row}}$ and $\langle \boldsymbol{y} \rangle_{\text{col}} \not\subset \langle \boldsymbol{x} \rangle_{\text{col}}$. The probability that $\langle \boldsymbol{y} \rangle_{\text{row}} \subset \langle \boldsymbol{x} \rangle_{\text{row}}$ under the condition that $\boldsymbol{y}$ has rank 1 is given by

$$\Pr(\langle \boldsymbol{y} \rangle_{\text{row}} \subset \langle \boldsymbol{x} \rangle_{\text{row}} \mid \text{wt}_{SR,1}(\boldsymbol{y}) = 1) = \frac{\begin{bmatrix} \delta \\ 1 \end{bmatrix}_q}{\begin{bmatrix} n \\ 1 \end{bmatrix}_q} = \frac{q^\delta - 1}{q^n - 1}$$

and hence the probability of the complementary event under the same condition is

$$\Pr(\langle \boldsymbol{y} \rangle_{\text{row}} \not\subset \langle \boldsymbol{x} \rangle_{\text{row}} \mid \text{wt}_{SR,1}(\boldsymbol{y}) = 1) = 1 - \frac{q^\delta - 1}{q^n - 1}.$$

An analogous statement can be derived for the corresponding column space:

$$\Pr(\langle \boldsymbol{y} \rangle_{\text{col}} \not\subset \langle \boldsymbol{x} \rangle_{\text{col}} \mid \text{wt}_{SR,1}(\boldsymbol{y}) = 1) = 1 - \frac{q^\delta - 1}{q^m - 1}.$$

Since the number of vectors in $\mathbb{F}_{q^m}^n$ of rank weight 1 is

$$|\{\boldsymbol{y} \in \mathbb{F}_{q^m}^n \mid \text{wt}_{SR,1}(\boldsymbol{y}) = 1\}| = \begin{bmatrix} n \\ 1 \end{bmatrix}_q \cdot (q^m - 1) = \frac{(q^m-1)(q^n-1)}{q-1},$$

we obtain

$$\begin{aligned} &\Pr(\langle \boldsymbol{y} \rangle_{\text{row}} \not\subset \langle \boldsymbol{x} \rangle_{\text{row}} \wedge \langle \boldsymbol{y} \rangle_{\text{col}} \not\subset \langle \boldsymbol{x} \rangle_{\text{col}} \mid \text{wt}_{SR,1}(y) = 1) \cdot |\{\boldsymbol{y} \in \mathbb{F}_{q^m}^n \mid \text{wt}_{SR,1}(\boldsymbol{y}) = 1\}| \\ =&\frac{(q^m-1)(q^n-1)}{q-1} \cdot \Big(1 - \frac{q^\delta - 1}{q^n - 1}\Big) \cdot \Big(1 - \frac{q^\delta - 1}{q^m - 1}\Big) = \frac{(q^n - q^\delta)(q^m - q^\delta)}{q-1}. \end{aligned}$$

□

Now, we can calculate the volume of the intersection of two sum-rank-metric balls. One ball has a radius of δ, and the other has a radius of 1, with a distance of δ between their centers (cf. Figure 4.3).

Theorem 4.20 ([OLWZ23, Theorem 2])**.** *Let $\boldsymbol{x}, \boldsymbol{x}' \in \mathbb{F}_{q^m}^n$ be two vectors with sum-rank distance $\text{d}_{SR,\ell}(\boldsymbol{x}, \boldsymbol{x}') = \delta$. The number of vectors lying in the intersection of two balls, one centered at $\boldsymbol{x}$ with a radius of 1, and the other centered at $\boldsymbol{x}'$ with a radius of δ, is given by*

$$\begin{aligned} \text{Vol}_{\mathcal{I}_\ell}(1, \delta, \delta) =& |\mathcal{B}_\ell(\boldsymbol{x}, 1) \cap \mathcal{B}_\ell(\boldsymbol{x}', \delta)| \\ =& 1 + \frac{(q^m-1)(q^n-1)}{q-1} - \sum_{\substack{\boldsymbol{\delta}=[\delta_0,\ldots,\delta_{\ell-1}] \\ \in \tau_{\delta,\ell,\mu}}} \sum_{i=0}^{\ell-1} \frac{(q^\eta - q^{\delta_i}) \cdot (q^m - q^{\delta_i})}{q-1}. \end{aligned}$$

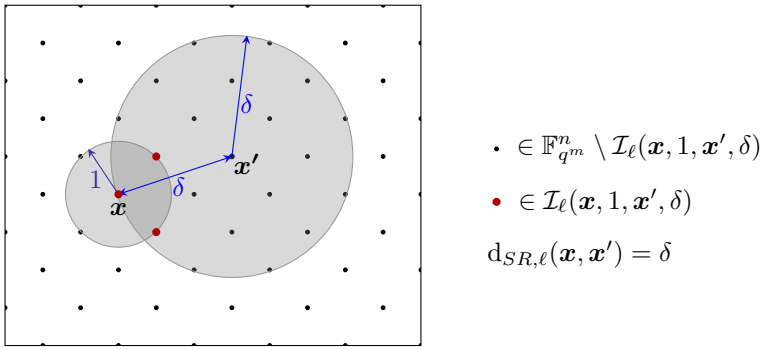


Figure 4.3.: Intersection of two balls in sum-rank metric: special case $\mathrm{Vol}_{\mathcal{I}_\ell}(1, \delta, \delta)$.

Proof. In order to calculate the volume of the intersection of two sum-rank-metric balls with centers $\boldsymbol{x}$ and $\boldsymbol{x}' \in \mathbb{F}_{q^m}^n$ and sum-rank distance $\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \boldsymbol{x}') = \delta$ between their centers, we can assume w.l.o.g. that $\boldsymbol{x} = \boldsymbol{0}$ and $\mathrm{wt}_{SR,\ell}(\boldsymbol{x}') = \delta$. This is because the sum-rank metric remains invariant under the translation of vectors. The set of vectors within the intersection of $\mathcal{B}_\ell(\boldsymbol{x}, 1) \cap \mathcal{B}_\ell(\boldsymbol{x}', \delta)$ consist then of the zero vector as well as all vectors $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$ that lie on the sphere $\mathcal{S}_\ell(\boldsymbol{x}, 1)$ except for those having a sum-rank distance of at least $\delta+1$ from $\boldsymbol{x}'$. However, since for each $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$, the triangle inequality

$$\mathrm{d}_{SR,\ell}(\boldsymbol{v}, \boldsymbol{x}') \leq \mathrm{wt}_{SR,\ell}(\boldsymbol{x}') + \mathrm{wt}_{SR,\ell}(\boldsymbol{v}) = \delta + 1,$$

holds, we only need to subtract the number of vectors having a sum-rank distance of exactly $\delta + 1$ to $\boldsymbol{x}'$. Hence, we have the following:

$$|\mathcal{B}_\ell(\boldsymbol{x}', \delta) \cap \mathcal{B}_\ell(\boldsymbol{x}, 1)| = |\{\boldsymbol{0}\}| + |\mathcal{S}_\ell(\boldsymbol{x}, 1)| - |\{\boldsymbol{v} \in \mathcal{S}_\ell(\boldsymbol{x}, 1) \mid \mathrm{d}_{SR,\ell}(\boldsymbol{v}, \boldsymbol{x}') = \delta + 1\}|.$$

Since a vector's sum-rank weight is 1 if and only if its rank weight is 1, the volume of a sphere with sum-rank radius 1 is given by

$$|\mathcal{S}_\ell(\boldsymbol{x}, 1)| = |\{\boldsymbol{v} \in \mathbb{F}_{q^m}^n \mid \mathrm{wt}_{SR,1}(\boldsymbol{v}) = 1\}| = \frac{(q^m - 1)(q^n - 1)}{q - 1}.$$

To determine the cardinality of the set

$$\mathcal{S}_\ell(\boldsymbol{x}, 1) \setminus \{\boldsymbol{v} \in \mathcal{S}_\ell(\boldsymbol{x}, 1) \mid \mathrm{d}_{SR,\ell}(\boldsymbol{v}, \boldsymbol{x}') = \delta + 1\},$$

we adopt a fixed sum-rank weight decomposition of $\boldsymbol{x}' = [\boldsymbol{x}'_0 | \ldots | \boldsymbol{x}'_{\ell-1}]$, where we designate the rank of each block as $\mathrm{rk}(\boldsymbol{x}'_i) = \delta_i$ for all $i \in \{0, \ldots, \ell - 1\}$ subject to the constraint that $\sum_{i=0}^{\ell-1} \delta_i = \delta$. Consider now a non-zero vector $\boldsymbol{w} \in \mathbb{F}_{q^m}^n$ with a sum-rank weight of $\mathrm{wt}_{SR,\ell}(\boldsymbol{w}) = 1$. This means that there is exactly one block with a rank weight of 1, and the rank weight of all other blocks is 0. Suppose that the i-th block of $\boldsymbol{w}$ is the non-zero block, then it holds, that the sum-rank distance between $\boldsymbol{w}$ and $\boldsymbol{x}'$ is $\mathrm{d}_{SR,\ell}(\boldsymbol{w}, \boldsymbol{x}') = \delta+1$ if and only if the rank distance in the i-th block of the corresponding vectors is $\mathrm{d}_{SR,1}(\boldsymbol{w}_i, \boldsymbol{x}'_i) = \delta_i + 1$. Our goal now is to determine the number of vectors

$\boldsymbol{w}_i$ in $\mathbb{F}_{q^m}^{\eta}$ that have a rank distance of $\delta_i + 1$ from the vector $\boldsymbol{x'}_i$, which itself has a rank weight of δ_i. According to Lemma 4.19, there are $\frac{(q^\eta - q^{\delta_i}) \cdot (q^m - q^{\delta_i})}{q-1}$ such vectors. This amount of vectors we have for each possible non-zero block $i \in \{0, \dots, \ell - 1\}$. Consequently, the total number of such vectors $\boldsymbol{w}$ in the intersection, given a specific partition of δ, is the summation

$$\sum_{i=0}^{\ell-1} \frac{(q^\eta - q^{\delta_i}) \cdot (q^m - q^{\delta_i})}{q-1}.$$

Adding up this quantity for each feasible partition of δ concludes our argument. □

Up to this point, we have utilized the set of ordered partitions $\mathcal{T}_{\delta,\ell,\mu}$ for our previous calculations, where δ is partitioned into ℓ terms, and each term is upper-bounded by μ. In the upcoming analysis, it is necessary to work with a distinct set of ordered partitions, where each term has its own specific upper bound. We introduce this set in the following: for two positive integers ℓ and δ and a vetor $\boldsymbol{\mu} = [\mu_0, \dots, \mu_{\ell-1}]$ whose entries are also positive integers, the set of all partitions of δ into ℓ terms $\delta_0, \dots, \delta_{\ell-1}$, where each term δ_i is upper-bounded by μ_i, is denoted by

$$\mathcal{T}_{\delta,\ell,\boldsymbol{\mu}} \coloneqq \left\{ [\delta_0, \dots, \delta_{\ell-1}] \in \mathbb{N}_0^\ell \mid \sum_{i=0}^{\ell-1} \delta_i = \delta, \delta_i \leq \mu_i \quad \forall i \in \{0, \dots, \ell-1\} \right\}. \tag{4.5}$$

Now, let us explore another specific scenario regarding the intersection of two sum-rank-metric balls. In this case, one ball has a sum-rank radius of γ, while the other ball has a sum-rank radius of $\delta - \gamma$. The distance between the centers of the two balls is δ (as illustrated in Figure 4.4). The illustration is based on a Euclidean geometric intuition and therefore gives the impression that the two balls intersect in only a single point. However, this is merely a schematic visualization. In the sum-rank metric, the intersection in fact contains multiple points. A similar phenomenon already occurs in the rank metric (cf. [GY08b]).

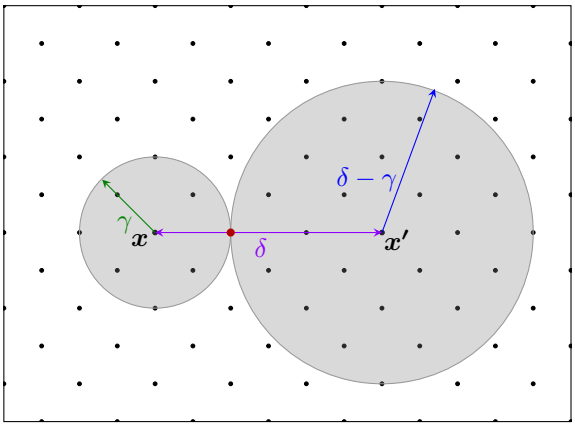


Figure 4.4.: Intersection of two balls in sum-rank metric: special case $\mathrm{Vol}_{\mathcal{I}_\ell}(\gamma, \delta - \gamma, \delta)$.

Theorem 4.21 ([OLWZ23, Theorem 3])**.** *Let $\boldsymbol{x}$ and $\boldsymbol{x}'$ be two vectors in $\mathbb{F}_{q^m}^n$ with a sum-rank distance of $\mathrm{d}_{SR,\ell}(\boldsymbol{x},\boldsymbol{x}') = \delta$. The number of vectors residing in the intersection of two balls, one centered at $\boldsymbol{x}$ with a sum-rank radius of γ, and the other centered at $\boldsymbol{x}'$ with a sum-rank radius of $\delta-\gamma$, is as follows:*

$$\begin{aligned}\mathrm{Vol}_{\mathcal{I}_\ell}(\gamma,\delta-\gamma,\delta) &= |\mathcal{B}_\ell(\boldsymbol{x},\gamma)\cap\mathcal{B}_\ell(\boldsymbol{x}',\delta-\gamma)| \\ &= \sum_{\substack{\boldsymbol{\delta}=[\delta_0,\ldots,\delta_{\ell-1}]\\ \in\tau_{\delta,\ell,\mu}}} \sum_{\substack{\boldsymbol{\gamma}=[\gamma_0,\ldots,\gamma_{\ell-1}]\\ \in\tau_{\gamma,\ell,\boldsymbol{\delta}}}} \prod_{i=0}^{\ell-1} q^{\gamma_i\cdot(\delta_i-\gamma_i)}\cdot \begin{bmatrix}\delta_i\\ \gamma_i\end{bmatrix}_q\end{aligned}$$

for $0\le\gamma\le\delta$, where $\tau_{\delta,\ell,\mu}$ and $\tau_{\gamma,\ell,\boldsymbol{\delta}}$ are defined as in equation (4.1) and (4.5), respectively.

Proof. Let $\boldsymbol{x},\boldsymbol{x}'\in\mathbb{F}_{q^m}^n$ be two vectors with a sum-rank distance of $\mathrm{d}_{SR,\ell}(\boldsymbol{x},\boldsymbol{x}')=\delta$. Due to the translational invariance of the sum-rank metric, we again assume w.l.o.g. that $\boldsymbol{x}=\boldsymbol{0}$ and the sum-rank weight of $\boldsymbol{x}'$ is $\mathrm{wt}_{SR,\ell}(\boldsymbol{x}')=\delta$. We fix the weight decomposition of $\boldsymbol{x}'$ as follows: $\mathrm{wt}_{SR,\ell}(\boldsymbol{x}')=\delta=\sum_{i=0}^{\ell-1}\delta_i$. By utilizing Corollary 4.5, we can conclude that there exists a unique Cartesian product of elementary linear subspaces $\mathcal{V}\coloneqq\mathcal{V}_0\times\ldots\times\mathcal{V}_{\ell-1}$ with $\mathcal{V}_i\in\mathcal{E}_{\delta_i}(\mathbb{F}_{q^m}^\eta)$ such that $\boldsymbol{x}'\in\mathcal{V}$. We also fix a partition of $\gamma=\sum_{i=0}^{\ell-1}\gamma_i$. Our first objective is to demonstrate that all vectors $\boldsymbol{v}\in\mathcal{B}_\ell(\boldsymbol{0},\gamma)\cap\mathcal{B}_\ell(\boldsymbol{x}',\delta-\gamma)$ are contained within the Cartesian product $\mathcal{V}=\mathcal{V}_0\times\ldots\times\mathcal{V}_{\ell-1}$. For each of these subspaces $\mathcal{V}_i$ there exists a unique complement $\mathcal{W}_i\in\mathcal{E}_{\eta-\delta_i}(\mathbb{F}_{q^m}^\eta)$ such that $\mathcal{V}_i\oplus\mathcal{W}_i=\mathbb{F}_{q^m}^\eta$. We denote by $\mathcal{W}$ the Cartesian product $\mathcal{W}_0\times\ldots\times\mathcal{W}_{\ell-1}$. Now, consider a vector $\boldsymbol{v}\in\mathbb{F}_{q^m}^n$ in the intersection $\mathcal{B}_\ell(\boldsymbol{0},\gamma)\cap\mathcal{B}_\ell(\boldsymbol{x}',\delta-\gamma)$. We can express each block $\boldsymbol{v}_i$ as the sum $\boldsymbol{v}_i=\boldsymbol{v}_i^{(\mathcal{V}_i)}+\boldsymbol{v}_i^{(\mathcal{W}_i)}$, where $\boldsymbol{v}_i^{(\mathcal{V}_i)}$ represents the projection of $\boldsymbol{v}_i$ onto $\mathcal{V}_i$ along $\mathcal{W}_i$, and $\mathbf{v}_i^{(\mathcal{W}_i)}$ is the projection onto $\mathcal{W}_i$, for all $i\in\{0,\ldots,\ell-1\}$. Since the entire vector $\boldsymbol{v}$ simultaneously belongs to both $\mathcal{B}_\ell(\boldsymbol{0},\gamma)$ and $\mathcal{B}_\ell(\boldsymbol{x}',\delta-\gamma)$, the following relations hold:

$$\mathrm{wt}_{SR,\ell}(\boldsymbol{v}^{(\mathcal{V})})\le\mathrm{wt}_{SR,\ell}(\boldsymbol{v})\le\gamma, \tag{4.6}$$

$$\mathrm{wt}_{SR,\ell}((\boldsymbol{x}'-\boldsymbol{v})^{(\mathcal{V})})\le\mathrm{wt}_{SR,\ell}(\boldsymbol{x}'-\boldsymbol{v})\le\delta-\gamma. \tag{4.7}$$

Since the projection is a linear mapping and considering that $\boldsymbol{x}'$ belongs to the subspace $\mathcal{V}$, we can exploit the property that $\boldsymbol{v}^{(\mathcal{V})}+(\boldsymbol{x}'-\boldsymbol{v})^{(\mathcal{V})}=(\boldsymbol{v}+(\boldsymbol{x}'-\boldsymbol{v}))^{(\mathcal{V})}=\boldsymbol{x}'^{(\mathcal{V})}=\boldsymbol{x}'$. Consequently, we derive the following inequalities:

$$\begin{aligned}\mathrm{wt}_{SR,\ell}(\boldsymbol{x}') &= \mathrm{wt}_{SR,\ell}(\boldsymbol{v}^{(\mathcal{V})}+(\boldsymbol{x}'-\boldsymbol{v})^{(\mathcal{V})}) && (4.8)\\ &\le \mathrm{wt}_{SR,\ell}(\boldsymbol{v}^{(\mathcal{V})})+\mathrm{wt}_{SR,\ell}((\boldsymbol{x}'-\boldsymbol{v})^{(\mathcal{V})}) && (4.9)\\ &\le \gamma+\delta-\gamma=\delta. && (4.10)\end{aligned}$$

However, since $\mathrm{wt}_{SR,\ell}(\boldsymbol{x}')=\delta$, we observe equality in both (4.9) and (4.10). In conjunction with the previously established inequalities in (4.6) and (4.7), we deduce the following equalities:

$$\mathrm{wt}_{SR,\ell}(\boldsymbol{v}^{(\mathcal{V})}) = \mathrm{wt}_{SR,\ell}(\boldsymbol{v})=\gamma, \tag{4.11}$$

$$\mathrm{wt}_{SR,\ell}((\boldsymbol{x}'-\boldsymbol{v})^{(\mathcal{V})}) = \mathrm{wt}_{SR,\ell}(\boldsymbol{x}'-\boldsymbol{v})=\delta-\gamma. \tag{4.12}$$

The equality in (4.11) leads to the expression:

$$\gamma = \sum_{i=0}^{\ell-1} \mathrm{wt}_{SR,1}(\boldsymbol{v}_i^{(\mathcal{V}_i)}) = \sum_{i=0}^{\ell-1} \mathrm{wt}_{SR,1}(\boldsymbol{v}_i) = \sum_{i=0}^{\ell-1} \mathrm{wt}_{SR,1}(\boldsymbol{v}_i^{(\mathcal{V}_i)} + \boldsymbol{v}_i^{(\mathcal{W}_i)}) \ . \tag{4.13}$$

Since $\boldsymbol{v}_i^{(\mathcal{V}_i)}$ and $\boldsymbol{v}_i^{(\mathcal{W}_i)}$ must be linearly independent (due to $\mathcal{V}_i \oplus \mathcal{W}_i = \mathbb{F}_{q^m}^{\eta}$), it follows that $\mathrm{wt}_{SR,1}(\boldsymbol{v}_i^{(\mathcal{V}_i)}) \leq \mathrm{wt}_{SR,1}(\boldsymbol{v}_i^{(\mathcal{V}_i)} + \boldsymbol{v}_i^{(\mathcal{W}_i)}) = \mathrm{wt}_{SR,1}(\boldsymbol{v}_i)$ for all $i \in \{0, \ldots, \ell-1\}$. This, combined with equation (4.13), implies:

$$\mathrm{wt}_{SR,1}(\boldsymbol{v}_i^{(\mathcal{V}_i)}) = \mathrm{wt}_{SR,1}(\boldsymbol{v}_i), \ \forall i \in \{0, \ldots, \ell-1\}. \tag{4.14}$$

In a similar fashion, we derive, based on the equation (4.12), that

$$\mathrm{wt}_{SR,1}((\boldsymbol{x'}_i - \boldsymbol{v}_i)^{(\mathcal{V}_i)}) = \mathrm{wt}_{SR,1}(\boldsymbol{x'}_i - \boldsymbol{v}_i), \ \forall i \in \{0, \ldots, \ell-1\}. \tag{4.15}$$

Equation (4.14) implies that

$$\langle \boldsymbol{v}_i^{(\mathcal{W}_i)} \rangle_{\mathbb{F}_{q^m}} \subset \langle \boldsymbol{v}_i^{(\mathcal{V}_i)} \rangle_{\mathbb{F}_{q^m}}, \forall i \in \{0, \ldots, \ell-1\}. \tag{4.16}$$

Similarly, utilizing Equation (4.15), we can deduce:

$$\langle (\boldsymbol{x'}_i - \boldsymbol{v}_i)^{(\mathcal{W}_i)} \rangle_{\mathbb{F}_{q^m}} \subset \langle (\boldsymbol{x'}_i - \boldsymbol{v}_i)^{(\mathcal{V}_i)} \rangle_{\mathbb{F}_{q^m}} \ , \ \forall i \in \{0, \ldots, \ell-1\}. \tag{4.17}$$

As a consequence of the equality in (4.9), we can infer that the vectors within the span $\langle \boldsymbol{v}^{(\mathcal{V})} \rangle_{\mathbb{F}_{q^m}}$ are linearly independent of those in $\langle (\boldsymbol{x'} - \boldsymbol{v})^{(\mathcal{V})} \rangle_{\mathbb{F}_{q^m}} = \{\boldsymbol{0}\}$. Hence, these two subspaces only intersect at the zero vector. This observation holds true for each block, as expressed in the following equation:

$$\langle \boldsymbol{v}_i^{(\mathcal{V}_i)} \rangle_{\mathbb{F}_{q^m}} \cap \langle (\boldsymbol{x'}_i - \boldsymbol{v}_i)^{(\mathcal{V}_i)} \rangle_{\mathbb{F}_{q^m}} = \{\boldsymbol{0}\} \ , \ \forall i \in \{0, \ldots, \ell-1\}. \tag{4.18}$$

Utilizing the relationships (4.16), (4.17), and (4.18), we derive:

$$\langle \boldsymbol{v}_i^{(\mathcal{W}_i)} \rangle_{\mathbb{F}_{q^m}} \cap \langle (\boldsymbol{x'}_i - \boldsymbol{v}_i)^{(\mathcal{W}_i)} \rangle_{\mathbb{F}_{q^m}} = \{\boldsymbol{0}\}, \ \forall i \in \{0, \ldots, \ell-1\}.$$

Combined with $\boldsymbol{x'}_i^{(\mathcal{W}_i)} + (\boldsymbol{v}_i - \boldsymbol{x'}_i)^{(\mathcal{W}_i)} = \boldsymbol{0}$ for all $i \in \{0, \ldots, \ell-1\}$ it follows that $\boldsymbol{v}_i^{(\mathcal{W}_i)} = (\boldsymbol{x'}_i - \boldsymbol{v}_i)^{(\mathcal{W}_i)} = \boldsymbol{0}$ and, consequently, $\boldsymbol{v}_i \in \mathcal{V}_i$ for all $i \in \{0, \ldots, \ell-1\}$. This implies $\boldsymbol{v} \in \mathcal{V}$.

Now, we demonstrate that for each $i \in \{0, \ldots, \ell-1\}$, the vector $\boldsymbol{v}_i$ must be a projection of $\boldsymbol{x'}_i$ onto a specific elementary linear subspace $\mathcal{A}_i$ within $\mathcal{V}_i$. If $\boldsymbol{v}_i \in \mathcal{V}_i$ satisfies $\mathrm{wt}_{SR,1}(\boldsymbol{v}_i) = \gamma_i$ and $\mathrm{wt}_{SR,1}(\boldsymbol{x'}_i - \boldsymbol{v}_i) = \delta_i - \gamma_i$ for all $i \in \{0, \ldots, \ell-1\}$ then each $\boldsymbol{v}_i$ belongs to some elementary linear subspace $\mathcal{A}_i$ of $\mathcal{V}_i$ and each $\boldsymbol{x'}_i - \boldsymbol{v}_i$ belongs to a corresponding elementary linear subspace $\mathcal{B}_i$ of $\mathcal{V}_i$ such that $\mathcal{A}_i \oplus \mathcal{B}_i = \mathcal{V}_i$ for all $i \in \{0, \ldots, \ell-1\}$. Consequently, $\boldsymbol{v}_i = \boldsymbol{x'}_i^{(\mathcal{A}_i)}$ and $\boldsymbol{x'}_i - \boldsymbol{v}_i = \boldsymbol{x'}_i^{(\mathcal{B}_i)}$ for all $i \in \{0, \ldots, \ell-1\}$.

Conversely, Lemma 4.8 implies, that for any $\mathcal{A}_i \in \mathcal{E}_{\gamma_i}(\mathbb{F}_{q^m}^{\eta})$ and any $\mathcal{B}_i \in \mathcal{E}_{\delta_i - \gamma_i}(\mathbb{F}_{q^m}^{\eta})$ such that $\mathcal{A}_i \oplus \mathcal{B}_i = \mathcal{V}_i$, the vector $\boldsymbol{x'}_i^{(\mathcal{A}_i)}$ has rank weight γ_i and rank distance $\delta_i - \gamma_i$

from $\boldsymbol{x'}_i$ and Lemma 4.8 also implies that all these vectors $\boldsymbol{x'}_i^{(\mathcal{A}_i)}$ are distinct. Thus, for each block, there are as many vectors $\boldsymbol{x'}_i$ as ordered pairs $(\mathcal{A}, \mathcal{B})$ for a fixed partition of δ and γ. According to Lemma 4.6, there are $q^{\gamma_i \cdot (\delta_i - \gamma_i)} \cdot \begin{bmatrix} \delta_i \\ \gamma_i \end{bmatrix}_q$ such ordered pairs for each block. Consequently, by applying Corollary 4.7, we can deduce that there are $\prod_{i=0}^{\ell-1} q^{\gamma_i \cdot (\delta_i - \gamma_i)} \cdot \begin{bmatrix} \delta_i \\ \gamma_i \end{bmatrix}_q$ vectors $\boldsymbol{v} = [\boldsymbol{v}_0 | \dots | \boldsymbol{v}_{\ell-1}]$ such that each block $\boldsymbol{v}_i$ represents a projection of $\boldsymbol{x'}_i$ onto an elementary linear subspace $\mathcal{A}_i$ of $\mathcal{V}_i$ for a fixed partition of δ and γ. Taking into account that $\gamma_i \leq \delta_i$ for each block $i \in \{0, \dots, \ell - 1\}$, we obtain in conclusion:

$$|\mathcal{B}_\ell(\boldsymbol{x}, \gamma) \cap \mathcal{B}_\ell(\boldsymbol{x'}, \delta - \gamma)| = \sum_{\substack{\boldsymbol{\delta} = [\delta_0, \dots, \delta_{\ell-1}] \\ \in \tau_{\delta, \ell, \mu}}} \sum_{\substack{\boldsymbol{\gamma} = [\gamma_0, \dots, \gamma_{\ell-1}] \\ \in \tau_{\gamma, \ell, \boldsymbol{\delta}}}} \prod_{i=0}^{\ell-1} q^{\gamma_i \cdot (\delta_i - \gamma_i)} \cdot \begin{bmatrix} \delta_i \\ \gamma_i \end{bmatrix}_q .$$

□

5

Properties of Codes in the Sum-Rank Metric

This chapter explores properties of codes with respect to the sum-rank metric over finite fields. Sum-rank-metric codes gained prominence due to their applicability in areas such as multishot network coding [MPK19a], [NUF10], space-time coding [SK20], and local repair in distributed storage systems [MPK19b]. A comprehensive summary of codes in the sum-rank metric can be found in [MPSK22]. The two main properties we focus on are bounds on the code cardinality and the covering properties of codes in the sum-rank metric. These topics are crucial for understanding the efficiency and performance of such codes, particularly in practical applications where optimizing the size and decoding capability of codes is essential.

In the first section, we explore various bounds on the cardinality of sum-rank-metric codes. Specifically, we revisit classic bounds such as the Singleton bound, the Gilbert–Varshamov (GV) bound, and the sphere-packing (SP) bound, while extending them to the sum-rank-metric setting. In the second section, we turn to the covering properties of codes, investigating the minimum number of balls required to cover a vector space and the related concept of the covering radius. This geometric property has significant implications for error correction in coding theory, and our treatment of it builds upon foundational work in both the rank and Hamming metric. Together, these two sections offer both theoretical insights and practical bounds that underlie code design and analysis in modern applications of coding theory.

Throughout this chapter, all notations and fundamental principles employed have been previously outlined in Chapter 2. Additionally, certain results build upon those introduced in Chapter 4. Unless explicitly stated otherwise, vectors belong to $\mathbb{F}_{q^m}^n$ and are splitted into ℓ blocks denoted as $\boldsymbol{x} = [\boldsymbol{x}_0|\dots|\boldsymbol{x}_{\ell-1}]$. The size of each block $\boldsymbol{x}_i \in \mathbb{F}_{q^m}^\eta$ is η, resulting in a total vector size of $n = \eta \cdot \ell$. Consequently, the subscript ℓ denotes the number of blocks. When we substitute ℓ with 1, we specifically refer to the rank metric, whereas setting ℓ equal to n corresponds to the Hamming metric. Moreover, we denote by μ the minimum of m and η, and by ν their maximum. The results presented in this chapter have been partially published in [OPB21] and [OLWZ22].

5.1. Bounds on the Cardinality of Codes in the Sum-Rank Metric

In this section, we explore three different bounds on the cardinality of sum-rank-metric codes: the Singleton bound, the Gilbert–Varshamov (GV) bound, and the sphere-packing (SP) bound. These bounds are already established in the literature (see [MPK19b] and [BGLR21]). In [BGLR21], the authors introduced a sphere-packing and a GV-like bound for sum-rank-metric codes, along with presenting asymptotic versions applicable to bounded block sizes and an increasing number of blocks. The finite parameter bounds rely on the sum-rank-metric ball size, which is super-polynomial to compute using the provided formula. In this section, we revisit variations of the sphere-packing and GV-like bound for linear codes and establish a connection to an algorithm for computing sum-rank-metric sphere sizes [PRR22]. This algorithm enables the computation of these bounds in polynomial time. By incorporating lower and upper bounds on the sum-rank-metric ball size, we derive simplified bounds, facilitating faster computation compared to exact calculations. These simplified bounds also yield asymptotic variants of these two bounds, extending the results in [BGLR21] to cover cases with a growing block size. Moreover, it is well known that random linear codes achieve the GV bound in the Hamming metric and a GV-like bound in the rank metric with high probability [Loi08]. We extend this observation to the sum-rank metric, demonstrating that codes achieving nearly the sum-rank GV-like bound are the generic case. Regarding the Singleton bound, we articulate various criteria for a code to meet this bound with equality. Analogous to the concept of maximum distance separable (MDS) codes in the Hamming metric and maximum rank distance codes in the rank metric, codes meeting these criteria are termed *maximum sum-rank distance codes (MSRD Codes)*. An example of a code class fulfilling this, is the class of the so-called *linearized Reed–Solomon (LRS) codes*, as introduced in [MP18, Theorem 4]. Their code parameters are limited by $\ell < q$ and $\eta \leq m$. MSRD codes that deviate from these constraints are thus of particular interest. In this section, we establish three lower bounds on the probability that a random linear code is an MSRD code. These bounds smoothly interpolate between the established bounds in the Hamming and rank metric, illustrating that MSRD codes become generic as the extension degree of the underlying field grows.

5.1.1. A Singleton-Like Bound and MSRD Codes

In [MPK19b], two Singleton-like bounds for the sum-rank metric were introduced. The tightness of these bounds depends on the relationship between m and η, determining which of the two bounds is more restrictive. We will rephrase the statement to present a unified bound dependent on the maximum of m and η .

Theorem 5.1 ([MPK19b, Corollary 4, 5])**.** *For a linear $[n, k, d]$ ℓ-sum-rank-metric code $\mathcal{C} \in \mathbb{F}_{q^m}^n$ with $\nu = \max\{m, \eta\}$, the following inequality holds:*

$$d \leq \frac{nm}{\nu} - \frac{km}{\nu} + 1.$$

As previously mentioned, codes that attain equality in this bound are referred to as *maximum sum-rank distance (MSRD)* codes. In order to derive lower bounds on a random linear code to be MSRD, we commence with a characterization of a code being MSRD (Lemma 5.2) and introduce the notation of the following sets of block matrices given positive integers n, η, ℓ and t, such that $n = \eta \cdot \ell$ and $t \leq n$:

$$\mathcal{A}_{\ell,t} \coloneqq \left\{ \boldsymbol{A} = \bigoplus_{i=0}^{\ell-1} \boldsymbol{A}_i \in \mathbb{F}_q^{t\times n} \mid \boldsymbol{A}_i \in \mathbb{F}_q^{t_i\times \eta}, \mathrm{rk}(\boldsymbol{A}_i) = t_i, \sum_{i=0}^{\ell-1} t_i = t \right\}$$

$$\mathcal{U}_{\ell,t} \coloneqq \left\{ \boldsymbol{U} = \bigoplus_{i=0}^{\ell-1} \boldsymbol{U}_i \in \mathcal{A}_{\ell,t} \mid \boldsymbol{U}_i \text{ upper triangular matrix for all } i \in \{0,\dots,\ell-1\} \right\}.$$

The lemma below establishes necessary and sufficient conditions for a code to be MSRD. The equivalence between (i) and (ii) has previously been investigated in a similar form in [MPK19b, AMPN20, PRR22]. We use this, as well as the equivalence between (i) and (iii) for deriving the two bounds on the probability of a random code to be MSRD. Additionally, the equivalence between (i) and (iv) provides a criterion in terms of elementary linear subspaces, which we will use when studying covering properties in Section 5.2. A similar result for the rank metric was presented in [GY08b, Lemma 9]. However, in our case, instead of considering a single elementary linear subspace of $\mathbb{F}_{q^m}^n$ we consider for the sum-rank metric the Cartesian product of ℓ elementary linear subspaces of $\mathbb{F}_{q^m}^\eta$. Notably, in contrast to [GY08b] we impose no restrictions on the relationship between n and m.

Lemma 5.2 ([OPB21, Lemma 3], [OLWZ22, Lemma 6])**.** *Consider a linear $[n,k,d]$ ℓ-sum-rank-metric code $\mathcal{C}$ over $\mathbb{F}_{q^m}$ with parity check matrix $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ and generator matrix $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k\times n}$. Then the following statements are equivalent:*

(i) $\mathcal{C}$ *is MSRD,*

(ii) $\mathrm{rk}_{\mathbb{F}_{q^m}}(\boldsymbol{A}\boldsymbol{G}^\top) = k \quad \forall \boldsymbol{A} \in \mathcal{A}_{\ell,k}$,

(iii) $\mathrm{rk}_{\mathbb{F}_{q^m}}(\boldsymbol{U}\boldsymbol{G}^\top) = k \quad \forall \boldsymbol{U} \in \mathcal{U}_{\ell,k}$,

(iv) $\left(\mathcal{V}_0 \times \ldots \times \mathcal{V}_{\ell-1}\right) \oplus \mathcal{C} = \mathbb{F}_{q^m}^n$ *for each sequence $(\mathcal{V}_i)_{1\leq i\leq \ell}$ fulfilling that each $\mathcal{V}_i$ is an elementary linear subspace of $\mathbb{F}_{q^m}^\eta$ and $\sum_{i=0}^{\ell-1} \dim(\mathcal{V}_i) = \frac{nm}{\nu} - \frac{km}{\nu}$.*

Proof. The equivalence between (i) and (ii) is a direct consequence of prior work in [MPK19b, AMPN20, PRR22].

We now demonstrate the equivalence between (ii) and (iii). As $\mathcal{U}_{\ell,k} \subset \mathcal{A}_{\ell,k}$, it follows that (ii) is sufficient for (iii). Hence, our task is to establish the necessity of (ii) for (iii). In order to do so, we assume, that the rank $\mathrm{rk}_{\mathbb{F}_{q^m}}(\boldsymbol{U}\boldsymbol{G}^\top) = k$ for each matrix $\boldsymbol{U} \in \mathcal{U}_{\ell,k}$. Let now $\boldsymbol{A} = \bigoplus_{i=0}^{\ell-1} \boldsymbol{A}_i$ be a blockmatrix belonging to the set $\mathcal{A}_{\ell,k}$. Then each block $\boldsymbol{A}_i$ is a matrix in $\mathbb{F}_q^{k_i\times\eta}$ with a rank of $\mathrm{rk}(\boldsymbol{A}_i) = k_i$ for all $i \in \{0,\dots,\ell-1\}$.

The sum of all these ranks is $\sum_{i=0}^{\ell-1} k_i = k$. For each block $\boldsymbol{A}_i$ let $\boldsymbol{U}_i$ be its reduced row echolon form, then there exists a regular matrix $\boldsymbol{X}_i \in \mathbb{F}_q^{k_i \times k_i}$ such that $\boldsymbol{A}_i = \boldsymbol{X}_i \boldsymbol{U}_i$ for all $i \in \{0, \ldots, \ell-1\}$. We introduce the definitions $\boldsymbol{X} \coloneqq \bigoplus_{i=0}^{\ell-1} \boldsymbol{X}_i$ and $\boldsymbol{U} \coloneqq \bigoplus_{i=0}^{\ell-1} \boldsymbol{U}_i$. Consequently, $\boldsymbol{X}$ is a regular matrix, $\boldsymbol{U}$ belongs to $\mathcal{U}_{\ell,k}$, and $\boldsymbol{A} = \boldsymbol{X}\boldsymbol{U}$. Since $\boldsymbol{X}$ has full rank, it follows that

$$\mathrm{rk}_{\mathbb{F}_{q^m}}(\boldsymbol{A}\boldsymbol{G}^\top) = \mathrm{rk}_{\mathbb{F}_{q^m}}(\boldsymbol{X}\boldsymbol{U}\boldsymbol{G}^\top) = \mathrm{rk}_{\mathbb{F}_{q^m}}(\boldsymbol{U}\boldsymbol{G}^\top) = k.$$

Now, we establish the equivalence between (i) and (iv). We begin with the sufficiency: (i)⇒(iv). Let $\mathcal{C}$ be an MSRD code. Following Theorem 5.1 it holds that $d = \frac{nm}{\nu} - \frac{km}{\nu} + 1$. Moreover, consider a sequence $(\mathcal{V}_i)_{0 \le i \le \ell-1}$ of elementary linear subspaces of $\mathbb{F}_{q^m}^\eta$ such that $\sum_{i=0}^{\ell-1} \dim(\mathcal{V}_i) = \frac{nm}{\nu} - \frac{km}{\nu}$. Then it holds that each vector in the Cartesian product $\mathcal{V}_0 \times \ldots \times \mathcal{V}_{\ell-1}$ has a sum-rank weight of at most $\frac{nm}{\nu} - \frac{km}{\nu}$. Thus, no codeword, except the zero codeword, is part of this Cartesian product; in other words,

$$(\mathcal{V}_0 \times \ldots \times \mathcal{V}_{\ell-1}) \cap \mathcal{C} = \{0\}.$$

Consequently, the direct sum of the Cartesian product with the code spans the entire space:

$$(\mathcal{V}_0 \times \ldots \times \mathcal{V}_{\ell-1}) \oplus \mathcal{C} = \mathbb{F}_{q^m}^n.$$

Conversely, to demonstrate the necessity (i)⇐(iv), consider a sequence $(\mathcal{V}_i)_{1 \le i \le \ell}$ of elementary linear subspaces of $\mathbb{F}_{q^m}^\eta$ such that the sum of their dimensions equals

$$\sum_{i=0}^{\ell-1} \dim(\mathcal{V}_i) = \frac{nm}{\nu} - \frac{km}{\nu}$$

and the direct sum of the Cartesian product with the code is $\left(\mathcal{V}_0 \times \ldots \times \mathcal{V}_{\ell-1}\right) \oplus \mathcal{C} = \mathbb{F}_{q^m}^n$. Hence, it it can be deduced that $\left(\mathcal{V}_0 \times \ldots \times \mathcal{V}_{\ell-1}\right) \cap \mathcal{C} = \{0\}$, indicating that $\mathcal{C}$ exclusively consists of vectors with sum-rank weight at least $\frac{nm}{\nu} - \frac{km}{\nu} + 1$. □

In the subsequent two lemmas, we derive upper bounds on the cardinalities of the sets $\mathcal{A}_{\ell,t}$ and $\mathcal{U}_{\ell,t}$.

Lemma 5.3 ([OPB21, Lemma 4])**.** *For positive integers n, η, ℓ and t, with $n = \eta \cdot \ell$ and $t \le n$, the cardinality of the set $\mathcal{A}_{\ell,t}$ and its upper bound is*

$$|\mathcal{A}_{\ell,t}| = \sum_{t \in \mathcal{T}_{t,\ell,\mu}} \prod_{j=0}^{t_i-1} (q^\eta - q^j) \le \binom{t+\ell-1}{\ell-1} q^{\eta t}.$$

Proof. According to Equation (2.2) the number of matrices $\boldsymbol{A}_i \in \mathbb{F}_q^{\eta \times t_i}$ of rank t_i is given by

$$\mathrm{NM}_q(\eta, t_i, t_i) = \prod_{j=0}^{t_i-1} (q^\eta - q^j) \le q^{\eta t_i}$$

for each $i \in \{0, \dots, \ell-1\}$, since the q-ary Gaussian binomial coefficient $\begin{bmatrix} t_i \\ t_i \end{bmatrix}_q = 1$. Thus, it follows, that for a fixed weight decomposition $t = \sum_{i=0}^{\ell-1} t_i$ with the restriction, $0 \leq t_i \leq \eta$ the number of matrices $\boldsymbol{A} = \boldsymbol{A}_0 \oplus \boldsymbol{A}_1 \oplus \ldots \oplus \boldsymbol{A}_{\ell-1} \in \mathbb{F}_q^{n \times t}$ with $\boldsymbol{A}_i \in \mathbb{F}_q^{\eta \times t_i}$ and $\mathrm{rk}(\boldsymbol{A}_i) = t_i$ is

$$\prod_{i=0}^{\ell-1} \prod_{j=0}^{t_i-1} (q^\eta - q^j) \leq q^{\eta \sum_{i=0}^{\ell-1} t_i} = q^{\eta t}.$$

Utilizing the number of ordered partitions $\mathcal{T}_{t,\ell,\mu}$ (see equation 4.1) and its upper bound (see inequality 4.2) we obtain

$$|\mathcal{A}_{\ell,t}| = \sum_{t \in \mathcal{T}_{t,\ell,\mu}} \prod_{i=0}^{\ell-1} \prod_{j=0}^{t_i-1} (q^\eta - q^j) \leq \binom{t+\ell-1}{\ell-1} q^{\eta t}.$$

□

Lemma 5.4 ([OPB21, Lemma 5])**.** *Let n, η, ℓ and t be positive integers, fulfilling $n = \eta \cdot \ell$ and $t \leq n$, then the cardinality of the set $\mathcal{U}_{\ell,t}$ and its upper bound is given by*

$$|\mathcal{U}_{\ell,t}| = \sum_{t \in \mathcal{T}_{t,\ell,\mu}} \prod_{i=0}^{\ell-1} \begin{bmatrix} \eta \\ t_i \end{bmatrix}_q \leq \binom{t+\ell-1}{\ell-1} q^{t(\eta - \frac{t}{\ell})} \cdot \gamma_q^\ell.$$

Proof. The number of upper triangular matrices $\boldsymbol{U}_i \in \mathbb{F}_q^{t_i \times \eta}$ of rank t_i corresponds to the number of t_i-dimensional subspaces of $\mathbb{F}_q^\eta$ and is therefore equal to the q-ary Gaussian binomial coefficient $\begin{bmatrix} \eta \\ t_i \end{bmatrix}_q$ (cf. Equation (2.1)). Utilizing the same arguments as in the proof of Lemma 5.3 we deduce $|\mathcal{U}_{\ell,t}| = \sum_{t \in \mathcal{T}_{t,\ell,\mu}} \prod_{i=0}^{\ell-1} \begin{bmatrix} \eta \\ t_i \end{bmatrix}_q$. By applying the upper bound on the q-ary Gaussian binomial coefficient

$$\begin{bmatrix} \eta \\ t_i \end{bmatrix}_q < \gamma_q \cdot q^{t_i(\eta - t_i)}$$

(see [KK08], [Ber80]), where γ_q is given in equation 2.3, we obtain

$$\begin{aligned} |\mathcal{U}_{\ell,t}| &< \sum_{t \in \mathcal{T}_{t,\ell,\mu}} \gamma_q^\ell q^{\sum_{i=0}^{\ell-1} t_i \eta - t_i^2} \\ &\leq |\mathcal{T}_{t,\ell,\mu}| \cdot \gamma_q^\ell q^{t\eta} \cdot \max_{\boldsymbol{t} \in \mathcal{T}_{t,\ell,\mu}} q^{-\sum_{i=0}^{\ell-1} t_i^2}. \end{aligned}$$

It was derived in [PRR22, Proof of Theorem 5] through the application of Jensen's inequality, that the choice $t_i = \frac{t}{\ell}$ leads to the upper bound $\max_{\boldsymbol{t} \in \mathcal{T}_{t,\ell,\mu}} -\left\{ \sum_{i=0}^{\ell-1} t_i^2 \right\} \leq -\frac{t^2}{\ell}$. As a result, we obtain the following upper bound on the cardinality of $\mathcal{U}_{\ell,t}$:

$$|\mathcal{U}_{\ell,t}| < |\mathcal{T}_{t,\ell,\mu}| \cdot \gamma_q^\ell q^{t\eta - \frac{t^2}{\ell}}.$$

By applying the upper bound on the cardinality of $\mathcal{T}_{t,\ell,\mu}$ (see (4.2)), the claim follows. □

Subsequently, we establish two lower bounds on the probability that a random linear code is an MSRD code. These bounds are adaptations of those provided in [NHTRR18] for the rank metric to the sum-rank metric. Similar to their approach, we employ the Schwartz–Zippel Lemma along with a counting argument on matrices. The distinction from their proof lies in the fact that these matrices possess a special block structure, resulting in bounds that smoothly interpolate between the Hamming-metric and the rank-metric cases. Notably, unlike the two bounds in [NHTRR18], each of our two bounds is advantageous in different parameter ranges. This is due to the nature of the bounds on the number of these matrices. The bounds converge to 1 for fixed n, k, ℓ and $m \to \infty$. This means that for large enough extension degree m, most linear codes are MSRD.

We recall the Schwartz–Zippel Lemma, which asserts that, for a multivariate non-zero polynomial $f \in \mathbb{F}_{q^m}[x_0, \dots, x_{r-1}]$ and for $v_0, \dots, v_{r-1}$ selected independently and uniformly at random from a subset $\mathcal{F}$ of $\mathbb{F}_{q^m}$ the following probability bound holds:

$$\Pr(f(v_0, \dots, v_{r-1}) = 0) \leq \frac{\deg(f)}{|\mathcal{F}|}.$$

Theorem 5.5 ([OPB21, Theorem 9])**.** *Let $\boldsymbol{G} = [\boldsymbol{I}_k \mid \boldsymbol{X}] \in \mathbb{F}_{q^m}^{k \times n}$ be a systematic generator matrix, where the entries of $\boldsymbol{X}$ are independently and uniformly chosen from $\mathbb{F}_{q^m}$. Denote by $\mathcal{C}$ the row space of $\boldsymbol{G}$ and by p the probability, that $\mathcal{C}$ is an MSRD code (w.r.t. ℓ). Then, it holds*

$$p \geq 1 - k\tbinom{k+\ell-1}{\ell-1} q^{\eta k - m}.$$

Proof. Lemma 5.2 establishes that $\mathcal{C}$ is MSRD if and only if $\mathrm{rk}_{\mathbb{F}_{q^m}}(\boldsymbol{G} \cdot \boldsymbol{A}) = k$ for all $\boldsymbol{A} \in \mathcal{A}_{\ell,k}$. Conversely, $\mathcal{C}$ is not MSRD if and only if there exists a matrix $\boldsymbol{A} \in \mathcal{A}_{\ell,k}$ such that $\det(\boldsymbol{G} \cdot \boldsymbol{A}) = 0$. Considering the entries of $\boldsymbol{X}$ as variables $x_0, \dots, x_{k(n-k)-1}$, the product $\boldsymbol{G} \cdot \boldsymbol{A}$ can be expressed as

$$\boldsymbol{G} \cdot \boldsymbol{A} = [\boldsymbol{I}_k | \boldsymbol{X}] \cdot \boldsymbol{A} = \Big(a_{ij} + \sum_{r=k}^{n-1} x_{ir-k} a_{rj}\Big)_{ij}$$

where each variable $x_0, \dots, x_{k(n-k)-1}$ appears in at most one row. Thus, the determinant of this product, denoted as $f_{\boldsymbol{A}} \coloneqq \det([\boldsymbol{I}_k | \boldsymbol{X}] \cdot \boldsymbol{A}) \in \mathbb{F}_q[x_0, \dots, x_{k(n-k)-1}]$, is a multivariate polynomial of degree at most k for each $\boldsymbol{A} \in \mathcal{A}_{\ell,k}$.

Utilizing the notation

$$f(x_0, \dots x_{k(n-k)-1}) \coloneqq \prod_{\boldsymbol{A} \in \mathcal{A}_{\ell,k}} f_{\boldsymbol{A}}(x_0, \dots x_{k(n-k)-1})$$

we can express the probability, that $\mathcal{C}$ is not MSRD as $\Pr(f(x_0, \dots x_{k(n-k)-1}) = 0)$.

As f is not the zero polynomial and the variables $x_0, \dots x_{k(n-k)-1}$ are independently and uniformly distributed, we can apply the Schwartz–Zippel Lemma and deduce

$$\Pr(f(x_0, \dots x_{k(n-k)-1}) = 0) \leq \frac{\deg f}{|\mathbb{F}_{q^m}|} = \frac{k|\mathcal{A}_{\ell,k}|}{q^m}. \tag{5.1}$$

Lemma 5.3 implies that

$$|\mathcal{A}_{\ell,k}| \leq \begin{bmatrix} k+\ell-1 \\ \ell-1 \end{bmatrix} q^{\eta k},$$

and we obtain together with inequality (5.1), that

$$\Pr(\mathcal{C} \text{ is not MSRD}) \leq \frac{k\begin{bmatrix} k+\ell-1 \\ \ell-1 \end{bmatrix} q^{\eta k}}{q^m}.$$

The counter probability provides the claim. □

The set of matrices $\mathcal{U}_{\ell,t}$ is a subset of $\mathcal{A}_{\ell,t}$, i.e., the number of matrices in $\mathcal{U}_{\ell,t}$ is less than or equal to those in $\mathcal{A}_{\ell,t}$. This observation prompts the formulation of the following bound, leveraging the criterion established in Lemma 5.2 (iii) alongside the insight from Lemma 5.4.

Theorem 5.6 ([OPB21, Theorem 10])**.** *Consider $\boldsymbol{G} = [\boldsymbol{I}_k \mid \boldsymbol{X}] \in \mathbb{F}_{q^m}^{k\times n}$ as a systematic generator matrix, where the entries of the random matrix $\boldsymbol{X}$ are independently and uniformly chosen from $\mathbb{F}_{q^m}$. The row space of $\boldsymbol{G}$ forms a linear ℓ-sum-rank-metric code over $\mathbb{F}_{q^m}$, denoted as $\mathcal{C}$. The probability p that $\mathcal{C}$ is MSRD is subject to the lower bound*

$$p \geq 1 - k\begin{bmatrix} k+\ell-1 \\ \ell-1 \end{bmatrix} q^{k(\eta-\frac{k}{\ell})-\frac{\ell}{4}-m} \cdot \gamma_q^{\ell}.$$

Proof. Following the same arguments as in the proof of Theorem 5.5 we use Lemma 5.2 (iii) and obtain by just replacing $\mathcal{A}_{\ell,k}$ by $\mathcal{U}_{\ell,k}$

$$\Pr(\mathcal{C} \text{ is not MSRD}) \leq \frac{k|\mathcal{U}_{\ell,k}|}{q^m}. \tag{5.2}$$

Applying Lemma 5.4 to inequality (5.2) yields

$$\Pr(\mathcal{C} \text{ is not MSRD}) \leq k\begin{bmatrix} k+\ell-1 \\ \ell-1 \end{bmatrix} q^{k(\eta-\frac{k}{\ell})-\frac{\ell}{4}} \cdot \gamma_q^{\ell} q^{-m}.$$

Consequently, the counter probability substantiates the claim. □

In [BR20, Corollary 5.4], both lower and upper bounds for the density of MRD codes in the set of all linear rank-metric codes are provided. In the following theorem we extend this result to the sum-rank metric.

Theorem 5.7 ([OPB21, Theorem 11])**.** *The probability of a linear code with length n and dimension k to be MSRD, denoted by p, is bounded from below and above as follows:*

$$\begin{aligned}
&1-\begin{bmatrix} n \\ k \end{bmatrix}_{q^m}^{-1} \sum_{h=0}^{n-k} \begin{bmatrix} n-k \\ h \end{bmatrix}_{q^m} \sum_{s=h}^{n-k} \begin{bmatrix} n-k-h \\ s-h \end{bmatrix}_{q^m} \begin{bmatrix} n-s \\ n-k \end{bmatrix}_{q^m} (-1)^{s-h} q^{m\binom{s-h}{2}} \\
\geq & p \\
\geq & 1-\frac{q^{mk}-1}{(q^m-1)(q^{mn}-1)}\left((n-k)\begin{pmatrix} \ell+n-k-1 \\ \ell-1 \end{pmatrix}\gamma_q^{\ell} q^{(n-k)(m+\eta-\frac{n-k}{\ell})}-1\right).
\end{aligned}$$

Proof. Consider $\mathcal{F}$ as the set encompassing all linear codes for a specified length n and dimension k. Let $\mathcal{F}'$ be a subset of $\mathcal{F}$ comprising all those codes with a minimum distance less than d. Using the subscripts n, ℓ and 1 we denote the corresponding sets for the differenet metrics: Hamming, sum-rank and rank metric, respectively. In [BR20, Corollary 5.2], it was demonstrated that the set of all Maximum Distance Separable (MDS) codes is dense among the set of all Hamming-metric codes over $\mathbb{F}_q$ of fixed length and dimension. This was achieved by providing upper and lower bounds on $\frac{|\mathcal{F}'_n|}{|\mathcal{F}_n|}$. Here, we focus on their lower bound:

$$\begin{bmatrix} n \\ k \end{bmatrix}_{q}^{-1} \sum_{h=0}^{d-1} \begin{bmatrix} d-1 \\ h \end{bmatrix}_{q} \sum_{s=h}^{d-1} \begin{bmatrix} d-1-h \\ s-h \end{bmatrix}_{q} \begin{bmatrix} n-s \\ n-k \end{bmatrix}_{q} (-1)^{s-h} q^{m\binom{s-h}{2}} \leq \frac{|\mathcal{F}'_n|}{|\mathcal{F}_n|}. \tag{5.3}$$

Since the $\mathbb{F}_q$-sum-rank weight of a vector over $\mathbb{F}_{q^m}$ is at most its Hamming weight, we obtain using inequality 5.3 its sum-rank version:

$$\begin{bmatrix} n \\ k \end{bmatrix}_{q^m}^{-1} \sum_{h=0}^{d-1} \begin{bmatrix} d-1 \\ h \end{bmatrix}_{q^m} \sum_{s=h}^{d-1} \begin{bmatrix} d-1-h \\ s-h \end{bmatrix}_{q^m} \begin{bmatrix} n-s \\ n-k \end{bmatrix}_{q^m} (-1)^{s-h} q^{m\binom{s-h}{2}} \leq \frac{|\mathcal{F}'_\ell|}{|\mathcal{F}_\ell|}. \tag{5.4}$$

In [BR20, Threorem 5.1], a metric-independent upper bound on $\frac{|\mathcal{F}'|}{|\mathcal{F}|}$ for codes over $\mathbb{F}_q$ was presented:

$$\frac{|\mathcal{F}'|}{|\mathcal{F}|} \leq \frac{q^k-1}{(q-1)(q^n-1)}\Big(\mathrm{Vol}_{\boldsymbol{B}}(d-1)-1\Big).$$

This can be specified to sum-rank-metric codes over $\mathbb{F}_{q^m}$ as follows:

$$\frac{|\mathcal{F}'_\ell|}{|\mathcal{F}_\ell|} \leq \frac{q^{mk}-1}{(q^m-1)(q^{mn}-1)}\Big(\mathrm{Vol}_{\boldsymbol{B}_\ell}(d-1)-1\Big). \tag{5.5}$$

Inequality (5.4) together with inequality (5.5) states that the set of all MSRD codes is dense among the set of all sum-rank-metric codes over $\mathbb{F}_{q^m}$ of fixed length and dimension. Let now $\mathcal{C}$ be a random code. To determine the probability for a code to be MSRD, we simply plug in $d = n-k+1$ into these inequalities, such that $\mathcal{F}'_\ell$ is the set of all non-MSRD codes and we also incorporate the upper bound on $\mathrm{Vol}_{\mathcal{B}_\ell}(d)$ given in

Theorem 4.15. This results in the following bounds on the probability of $\mathcal{C}$ not being MSRD:

$$\begin{aligned}
&\begin{bmatrix} n \\ k \end{bmatrix}_{q^m}^{-1} \sum_{h=0}^{n-k} \begin{bmatrix} n-k \\ h \end{bmatrix}_{q^m} \sum_{s=h}^{n-k} \begin{bmatrix} n-k-h \\ s-h \end{bmatrix}_{q^m} \begin{bmatrix} n-s \\ n-k \end{bmatrix}_{q^m} (-1)^{s-h} q^{m\binom{s-h}{2}} \\
\leq &\Pr(\mathcal{C} \text{ is not MSRD}) \\
\leq &\frac{q^{mk}-1}{(q^m-1)(q^{mn}-1)} \left((n-k) \binom{\ell+n-k-1}{\ell-1} \gamma_q^\ell q^{(n-k)(m+\eta-\frac{n-k}{\ell})} - 1 \right).
\end{aligned}$$

The counter probability shows the claim. □

The bounds presented in Theorems 5.5 and 5.6 converge to 1 as $m \to \infty$ for fixed values of n, k and ℓ. In other words, for sufficiently large extension degrees m, the majority of linear codes exhibit MSRD properties. Figure 5.1 illustrates the minimal values of the extension degree m required for a non-zero probability of a code being MSRD. This exploration considers varying numbers of blocks ℓ while keeping n, k, and q constant. These minimal values $m_{\min}$ form a smooth interpolation between the established extreme cases: $\ell = 1$ and $\ell = n$. The corresponding counter probabilities of the two bounds differ by the factor $\zeta \coloneqq q^{-\frac{k^2}{\ell}-\frac{\ell}{4}}\gamma_q^\ell$. Hence, the relation of ζ to 1 determines, which of the two bounds is tighter. This can be observed in Figure 5.1. For smaller values of ℓ, Theorem 5.6 yields a tighter bound, while for larger values of ℓ, Theorem 5.5 provides the better bound. Consequently, both bounds exhibit advantages within specific ranges of ℓ. This differs from the situation described in [NHTRR18], where the bound in [NHTRR18, Theorem 26] is an improvement over the outcome established in [NHTRR18, Theorem 21]. Nevertheless, the bound introduced in Theorem 5.6 outperforms the one outlined in Theorem 5.7.

5.1.2. A Gilbert–Varshamov-Like Bound

We commence with a recall of a GV-like bound for linear codes in the sum-rank metric.

Theorem 5.8 (cf. GV-like Bound [BGLR21])**.** *Let $\mathbb{F}_{q^m}$ be a finite field, n, k, d, μ, ℓ, η be positive integers fulfilling $n = \eta \cdot \ell \geq k$, $\mu = \min\{m, \eta\}$ and $d \leq \mu\ell$. If the inequality*

$$q^{m(k-1)} \cdot \mathrm{Vol}_{\mathcal{B}_\ell}(d-1) < q^{mn},$$

hold, then there exists a linear code of length n, dimension k, and minimum ℓ-sum-rank distance at least d.

Remark 5.9. *The computational complexity for calculating the bound in Theorem 5.8 is $\mathcal{O}^{\sim}\left(\ell^2 d^3 + \ell d^4 (m+\eta)\log(q)\right)$. This efficiency is achieved through the utilization of the efficient algorithm for computing $\mathrm{Vol}_{\mathcal{S}_\ell}$ outlined in [PRR22].*

While it is feasible to compute the GV-like bound exactly within polynomial time, for large parameters the calculation still becomes time-consuming. This motivates the derivation of the subsequent simplified GV-like bound.

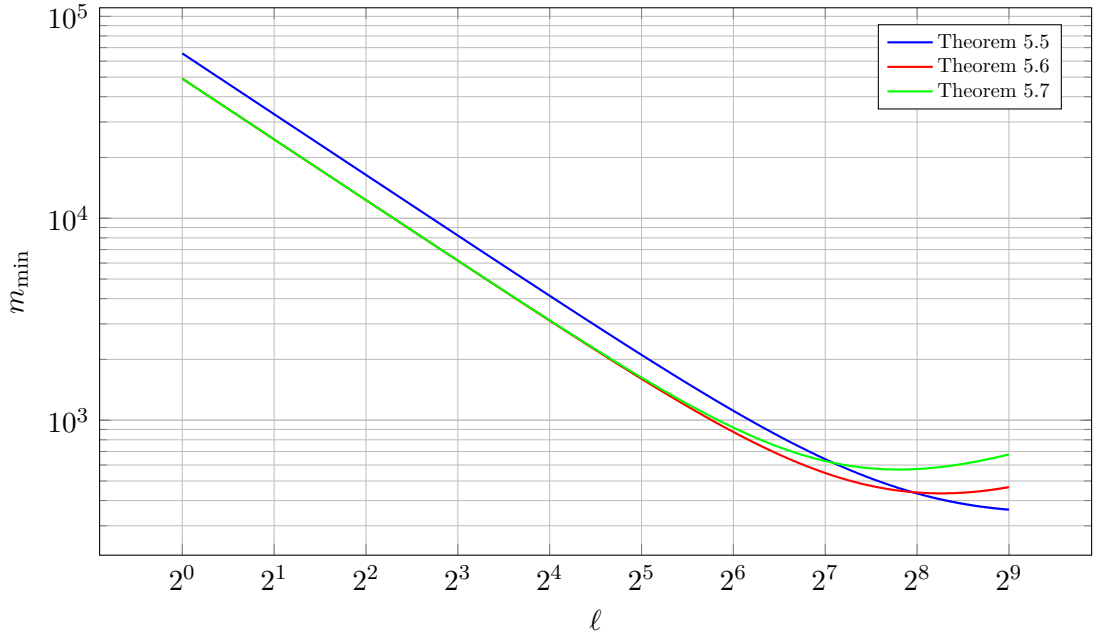


Figure 5.1.: Comparison of Theorem 5.5, Theorem 5.6 and Theorem 5.7 for $n = 2^{10}$, $k = 2^8$ and $q = 4$. Adapted from [OPB21]. © 2021 IEEE.

Theorem 5.10 (Simplified GV-Like Bound [OPB21, Theorem 6])**.** *For a finite field $\mathbb{F}_{q^m}$ and positive integers n, k, d, ℓ, η, $\mu \coloneqq \min\{m, \eta\}$ that satisfy $n = \eta \cdot \ell \geq k$ and $d \leq \mu\ell$, it holds that if the following inequality*

$$q^{m(k-1)} \cdot (d-1) \begin{pmatrix} \ell + d - 2 \\ \ell - 1 \end{pmatrix} \gamma_q^{\ell} q^{(d-1)(m+\eta-\frac{d-1}{\ell})} < q^{mn},$$

is fulfilled, then there exists a linear code of length n, dimension k, and minimum ℓ-sum-rank distance at least d.

Proof. By substituting the upper bound on the volume of a sum-rank-metric ball given in Theorem 4.15 into the GV-like bound given in Theorem 5.8, the assertion follows. □

The simplified GV-like bound leads to the following asymptotic version of the GV-like bound.

Theorem 5.11 (Asymptotic GV-Like Bound [OPB21, Theorem 7])**.** *For a finite field $\mathbb{F}_{q^m}$ and positive integers $n, k = \mathcal{R} \cdot n, d, \ell, \eta, \mu \coloneqq \min\{m, \eta\}$ satisfying $n = \eta \cdot \ell \geq k$ and $d \leq \mu\ell$ with $\delta \coloneqq \frac{d}{n}$ and $2 < d \leq \mu\ell$, the existence of a linear ℓ-sum-rank-metric code with rate $\mathcal{R}$ and relative minimum sum-rank distance at least δ is guaranteed if the*

following inequality is met:

$$\begin{aligned}\mathcal{R} \leq & \delta^2 \frac{\eta}{m} - \delta\Big(1 + \frac{\eta}{m} + \frac{2\eta}{nm}\Big) + 1 + \frac{1}{n} + \frac{\eta}{nm} + \frac{\eta}{n^2 m} \\ & - \frac{\sum_{i=1}^{\delta n - 1} \log_q\left(1 + \frac{\ell-1}{i}\right) + \log_q(\delta n - 1)}{mn} - \frac{\log_q(\gamma_q)}{\eta m},\end{aligned}$$

with γ_q as given in equation (2.3). For a constant ξ with $m = \eta\xi \to \infty$ and $m \in \omega(\log_q(\ell))$, the rate $\mathcal{R}$ behaves asymptotically as follows:

$$\mathcal{R} \sim \delta^2 \frac{1}{\xi} - \delta\Big(1 + \frac{1}{\xi}\Big) + 1.$$

Proof. The simplified GV-like bound provided in Theorem 5.10 leads to a slightly different statement: if the following inequality

$$q^{mk}(d-1)\binom{\ell + d - 2}{\ell - 1}\gamma_q^{\ell} q^{(d-1)(m+\eta-\frac{d-1}{\ell})} \leq q^{mn} \tag{5.6}$$

holds, then there exists a linear $[n, k, d]$ ℓ-sum-rank-metric code $\mathcal{C}$. We can rewrite inequality (5.6) as follows

$$\begin{aligned}\frac{k}{n} \leq & \Big(\frac{d}{n}\Big)^2 \frac{\eta}{m} - \frac{d}{n}\Big(1 + \frac{\eta}{m} + \frac{2\eta}{nm}\Big) + 1 + \frac{1}{n} + \frac{\eta}{nm} + \frac{\eta}{n^2 m} \\ & - \frac{\log_q\left((d-1)\cdot\binom{\ell+d-2}{\ell-1}\right)}{mn} - \frac{\log_q(\gamma_q)}{\eta m}.\end{aligned}$$

Upon substituting $\delta \coloneqq \frac{d}{n}$, we obtain the highest possible rate $\mathcal{R}_* \geq \mathcal{R}$:

$$\begin{aligned}& \delta^2 \frac{\eta}{m} - \delta\Big(1 + \frac{\eta}{m} + \frac{2\eta}{nm}\Big) + 1 + \frac{1}{n} + \frac{\eta}{nm} + \frac{\eta}{n^2 m} \\ & - \frac{\sum_{i=1}^{\delta n - 1} \log_q\left(1 + \frac{\ell-1}{i}\right) + \log_q(\delta n - 1)}{mn} - \frac{\log_q(\gamma_q)}{\eta m} \\ =: & \mathcal{R}_*.\end{aligned}$$

Considering a constant ξ, we explore the limit of $\mathcal{R}_*$ as $m = \eta\xi \to \infty$ under the condition that m grows faster than $\log_q(\ell)$. This can be expressed as follows:

$$\lim_{\substack{m=\eta\xi\to\infty \\ m\in\omega(\log_q(\ell))}} \mathcal{R}_* = \delta^2 \frac{1}{\xi} - \delta\Big(1 + \frac{1}{\xi}\Big) + 1.$$

□

We now apply the established result to the sum-rank metric, affirming that codes nearly achieving the GV-like bound represent the generic case.

Theorem 5.12 ([OPB21, Theorem 8]). *Let q, m, n, d be positive integers, $\epsilon \in \Big(0, 1 - \log_q\left(\mathrm{Vol}_{\mathcal{B}_\ell}(d-1)^{\frac{1}{mn}}\right) - n^{-1}\Big]$ and $k \coloneqq n(1 - \log_q(\mathrm{Vol}_{\mathcal{B}_\ell}(d-1)^{\frac{1}{mn}}) - \epsilon)$. If $\mathcal{C}$ is chosen uniformly at random from the set of linear codes of length n and dimension k over $\mathbb{F}_{q^m}$, then the probability that $\mathcal{C}$ has a minimum sum-rank distance of at least d is at least $1 - e^{-\Omega(mn)}$.*

Proof. Rather than picking a code randomly with a specific dimension k, we have a different approach: We choose a matrix $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ by filling its entries independently uniformly at random. Its row space is the random code $\mathcal{C}$. Let A denote the event occurring when the matrix $\boldsymbol{G}$ achieves the maximum possible rank k. Additionally, let B represent the event where the minimum sum-rank distance of the code is at least d. The probability we are interested in is $\Pr(B \mid A)$, which signifies the likelihood that event B happens given that event A has occurred. In essence, we are interested in the probability that our code, constructed with the specified matrix and satisfying the maximum rank condition (event A), also possesses a minimum sum-rank distance of at least d (event B). Initially, we examine the complementary probability of A, denoted as $\neg A$. This entails considering the scenario where event A does not occur. For $\neg A$ the following upper bound is applicable:

$$\Pr(\neg A) = \sum_{\boldsymbol{x} \in \mathbb{F}_{q^m}^k \setminus \{\boldsymbol{0}\}} \Pr(\boldsymbol{x} \cdot \boldsymbol{G} = \boldsymbol{0}) = \sum_{\boldsymbol{x} \in \mathbb{F}_{q^m}^k \setminus \{\boldsymbol{0}\}} \frac{1}{q^{mn}} = (q^{mk} - 1) \cdot \frac{1}{q^{mn}} < e^{-\Omega(mn)}.$$

Hence, we deduce a lower bound for the event A, which is given by:

$$\Pr(A) \geq 1 - e^{-\Omega(mn)}. \tag{5.7}$$

We also provide an upper bound for the probability $\Pr(B)$. Given an information vector $\boldsymbol{i} \in \mathbb{F}_{q^m}^k$, let $E_{\boldsymbol{i}}$ be the event that the sum-rank weight of the product $\boldsymbol{i} \cdot \boldsymbol{G}$ is bounded as follows: $0 < \mathrm{wt}_{SR,\ell}(\boldsymbol{i} \cdot \boldsymbol{G}) < d$. Applying the union bound, we obtain:

$$\Pr(\neg B) = \Pr\Big(\bigcup_{\boldsymbol{i} \in \mathbb{F}_{q^m}^k} E_{\boldsymbol{i}}\Big) \leq \sum_{\boldsymbol{i} \in \mathbb{F}_{q^m}^k} \Pr(E_{\boldsymbol{i}}). \tag{5.8}$$

For $\boldsymbol{i} = \boldsymbol{0}$, it holds that $\Pr(E_{\boldsymbol{i}}) = 0$ and for $\boldsymbol{i} \neq 0$, we obtain

$$\Pr(E_{\boldsymbol{i}}) = \sum_{\boldsymbol{c} \in \mathbb{F}_{q^m}^n : \mathrm{wt}_{SR,\ell}(\boldsymbol{c}) \leq d-1} \Pr(\boldsymbol{i} \cdot \boldsymbol{G} = \boldsymbol{c}) = \sum_{\boldsymbol{c} \in \mathbb{F}_{q^m}^n : \mathrm{wt}_{SR,\ell}(\boldsymbol{c}) \leq d-1} \frac{1}{q^{mn}} = \frac{\mathrm{Vol}_{\mathcal{B}_\ell}(d-1)}{q^{m \cdot n}}. \tag{5.9}$$

Upon merging the inequalities (5.8) and (5.9), we obtain the following lower bound on the event B:

$$\Pr(B) \geq 1 - \frac{q^{mk} \cdot \mathrm{Vol}_{\mathcal{B}_\ell}(d-1)}{q^{mn}} \geq 1 - q^{-mn\epsilon} \tag{5.10}$$

for the given choice of $k = n(1 - \log_q(\mathrm{Vol}_{\mathcal{B}_\ell}(d-1)^{\frac{1}{mn}}) - \epsilon)$ and $\epsilon \in \left(0, 1 - \log_q\left(\mathrm{Vol}_{\mathcal{B}_\ell}(d-1)^{\frac{1}{mn}}\right) - n^{-1}\right]$. Finally, since $\Pr(B \mid A) \geq \Pr(B \cap A)$ by combining the lower bound on the event A (see inequality (5.7)) and the event B (cf. (5.10)) it holds that

$$\Pr(B \mid A) \geq \Pr(B \cap A) = \Pr(A) \cdot \Pr(B) \geq 1 - e^{-\Omega(mn)},$$

which proves the claim. □

5.1.3. Sphere-Packing Bound

We begin by revisiting the sphere-packing (SP) bound for linear codes in the sum-rank metric.

Theorem 5.13 (Sphere-Packing Bound [BGLR21])**.** *Let $\mathcal{C}$ be a linear $[n, k, d]$ sum-rank-metric code, then the following inequality holds*

$$q^{mk} \cdot \mathrm{Vol}_{\mathcal{B}_\ell}\Big(\Big\lfloor \frac{d-1}{2} \Big\rfloor\Big) \leq q^{mn}.$$

Similar to the GV-like bound, the SP bound can be exactly computed within polynomial time, as indicated in Remark 5.9. Nevertheless, the calculation becomes time-consuming when dealing with large parameters. This motivates the subsequent simplified SP bound, for which we rely on an lower bound on $\mathrm{Vol}_{\mathcal{B}_\ell}(\cdot)$, which was derived in Lemma 4.12.

Theorem 5.14 (Simplified SP Bound [OPB21, Theorem 4])**.** *A linear $[n, k, d]$ sum-rank-metric code $\mathcal{C}$ satisfies the following inequality*

$$q^{mk} \cdot q^{(m+\eta-\frac{1}{\ell}\lfloor\frac{d-1}{2}\rfloor)\lfloor\frac{d-1}{2}\rfloor-\frac{\ell}{4}} \cdot \gamma_q^{-\ell} \leq q^{mn}.$$

Proof. By substituting the lower bound for the volume of a sum-rank-metric ball, as provided in Theorem 4.12 into the SP bound outlined in Theorem 5.13, the conclusion can be derived. □

The simplified SP bound gives rise to the following asymptotic variations of the bound in two scenarios: one with a bounded block size and increasing numbers of blocks, as discussed in [BGLR21], and another with a growing block size, for which no asymptotic bounds have been established thus far.

Theorem 5.15 (Asymptotic SP Bound [OPB21, Theorem 5])**.** *Consider a linear $[n, k, d]$ sum-rank-metric code denoted as $\mathcal{C}$, where $\delta \coloneqq \frac{d}{n}$ represents the relative minimum distance. The code rate, $\mathcal{R} = \frac{k}{n}$, is subject to an upper bound given by*

$$\begin{aligned}\mathcal{R} < \delta^2 \frac{\eta}{4m} - \delta\Big(\frac{1}{2} + \frac{\eta}{m}\Big(\frac{1}{2} + \frac{1}{n}\Big)\Big) + \frac{1}{n}\Big(1 + \frac{\eta}{m} + \frac{\eta}{nm}\Big) \\ + \frac{1}{\eta m}\Big(\frac{1}{4} + \log_q(\gamma_q)\Big) + 1 =: \mathcal{R}^*(\delta),\end{aligned}$$

with γ_q as given in equation 2.3. Assume a fixed positive value ξ. In this context, we provide the limits defined by the following two scenarios.

(i) When $m = \eta\xi \to \infty$ the code rate $\mathcal{R}$ approaches

$$\mathcal{R} \sim \delta^2 \frac{1}{4\xi} - \frac{\delta}{2}\Big(1 + \frac{1}{\xi}\Big) + 1.$$

(ii) As $\ell \to \infty$, the code rate $\mathcal{R}$ exhibits the asymptotic behavior

$$\mathcal{R} \sim \delta^2 \frac{\eta}{4m} - \frac{\delta}{2}\Big(1 + \frac{\eta}{m}\Big) \quad + \frac{1}{\eta m}\Big(\frac{1}{4} + \log_q(\gamma_q)\Big) + 1.$$

Proof. By transforming the simplified SP bound, as outlined in Theorem 5.14 with $t \coloneqq \lfloor \frac{d-1}{2} \rfloor$ we arrive at the following inequality:

$$\frac{k}{n} \leq 1 - \frac{\Big(m + \eta - \frac{t}{\ell}\Big)t - \ell\Big(\frac{1}{4} + \log_q(\gamma_q)\Big)}{mn}.$$

As t is equal to $\lfloor \frac{d-1}{2} \rfloor \geq \frac{d-2}{2} = \frac{1}{2}\delta n - 1$ for $\delta = \frac{d}{n}$, the inequality remains valid when substituting t with $\frac{1}{2}\delta n - 1$. Consequently, this results in

$$\begin{aligned}\frac{k}{n} \leq & \delta^2 \frac{\eta}{4m} - \delta\Big(\frac{1}{2} + \frac{\eta}{m}\Big(\frac{1}{2} + \frac{1}{n}\Big)\Big) + \frac{1}{n}\Big(1 + \frac{\eta}{m} + \frac{\eta}{nm}\Big) \\ & + \frac{1}{\eta m}\Big(\frac{1}{4} + \log_q(\gamma_q)\Big) + 1 =: \mathcal{R}^*(\delta).\end{aligned}$$

Let ξ be a constant. We explore the following limit scenarios:

(i) As m approaches infinity such that $m = \eta\xi$, the limit of $\mathcal{R}^*(\delta)$ converges to an expression defined by

$$\lim_{m=\eta\xi\to\infty} \mathcal{R}^*(\delta) = \delta^2 \frac{1}{4\xi} - \frac{\delta}{2}\Big(1 + \frac{1}{\xi}\Big) + 1.$$

(ii) When ℓ tends to infinity, the limit of $\mathcal{R}^*(\delta)$ is characterized by:

$$\lim_{\ell\to\infty} \mathcal{R}^*(\delta) = \delta^2 \frac{\eta}{4m} - \frac{\delta}{2}\Big(1 + \frac{\eta}{m}\Big) + \frac{1}{\eta m}\Big(\frac{1}{4} + \log_q(\gamma_q)\Big) + 1.$$

□

5.1.4. Numerical Comparison of the Bounds

We evaluate our simplified and asymptotic bounds by comparing them to precise bounds under two distinct parameter regimes and asymptotic settings:

- *Bounded Block Size*: In this scenario, we maintain a constant extension degree m and block size η, allowing the number of blocks ℓ to approach infinity. It aligns with existing asymptotic bounds, as detailed in [BGLR21].

- *Growing Block Size*: Here, we allow all parameters η, m, and ℓ to grow simultaneously towards infinity in a proportional manner. For finite parameter plots, we select constants close to 1 for the ratios $\frac{\ell}{\eta}$ and $\frac{\eta}{m}$.

In contrast to the approach in [BGLR21], our analysis extends to larger parameters (e.g., $n = 2^{11}$ and beyond). This expanded scope is facilitated by employing efficient algorithms for calculating the sum-rank ball size, as introduced in [PRR22].

5.1.4.1. Bounded Block Size

In Figure 5.2, we conduct a comparative analysis, juxtaposing our simplified bounds (refer to Lemma 4.12 and Theorem 5.10) with their corresponding exact counterparts (detailed in Theorem 5.13 and Theorem 5.8). Additionally, for the SP bound, we include a comparison with the asymptotic bound presented in Theorem 5.15 (ii). Furthermore, we assess our SP and GV-like bounds against the asymptotic induced Hamming bound, as well as the asymptotic SP and sphere-covering bounds, as outlined in [BGLR21, Theorem 4.4 and Corollary 4.10]. In this specific parameter regime, our simplified bounds exhibit a larger deviation from the exact bounds in comparison to the case with growing block size. This discrepancy arises because the bounds on $\mathrm{Vol}_{\mathcal{B}_\ell}(t)$ are more effective when $\ell \approx \eta$. Remarkably, for $n = 2^{11}$, the simplified, exact, and asymptotic bounds are nearly indistinguishable. Starting from $\delta \geq 0.2$, the asymptotic SP bound closely approximates the exact bound, surpassing the induced Hamming bound for this parameter setting. It is noteworthy that the asymptotic SP and sphere-covering bounds from [BGLR21, Corollary 4.10] closely align with the exact SP and GV-like bounds for $n = 2^{11}$, respectively.

5.1.4.2. Growing Block Size

In Figure 5.3, we present a comparison of asymptotic bounds as per Theorem 5.15 (i) and Theorem 5.11 with their respective exact counterparts (refer to Theorem 5.13 and Theorem 5.8). We also include a comparison with the simplified bounds (as outlined in Lemma 4.12 and Theorem 5.10) for two distinct parameter sets ℓ, m, η, and n. In this particular asymptotic scenario, it becomes apparent that as η and ℓ grow, the gap between the simplified and exact bounds diminishes. Notably, for $n = 2^{10}$, there exists no significant difference between the simplified and the exact bounds. Moreover, in the context of finite n, these bounds almost coincide with the asymptotic bounds. However, in comparison to the Singleton-like bound, the SP bound provides a looser bound for $\delta > 0.1$.

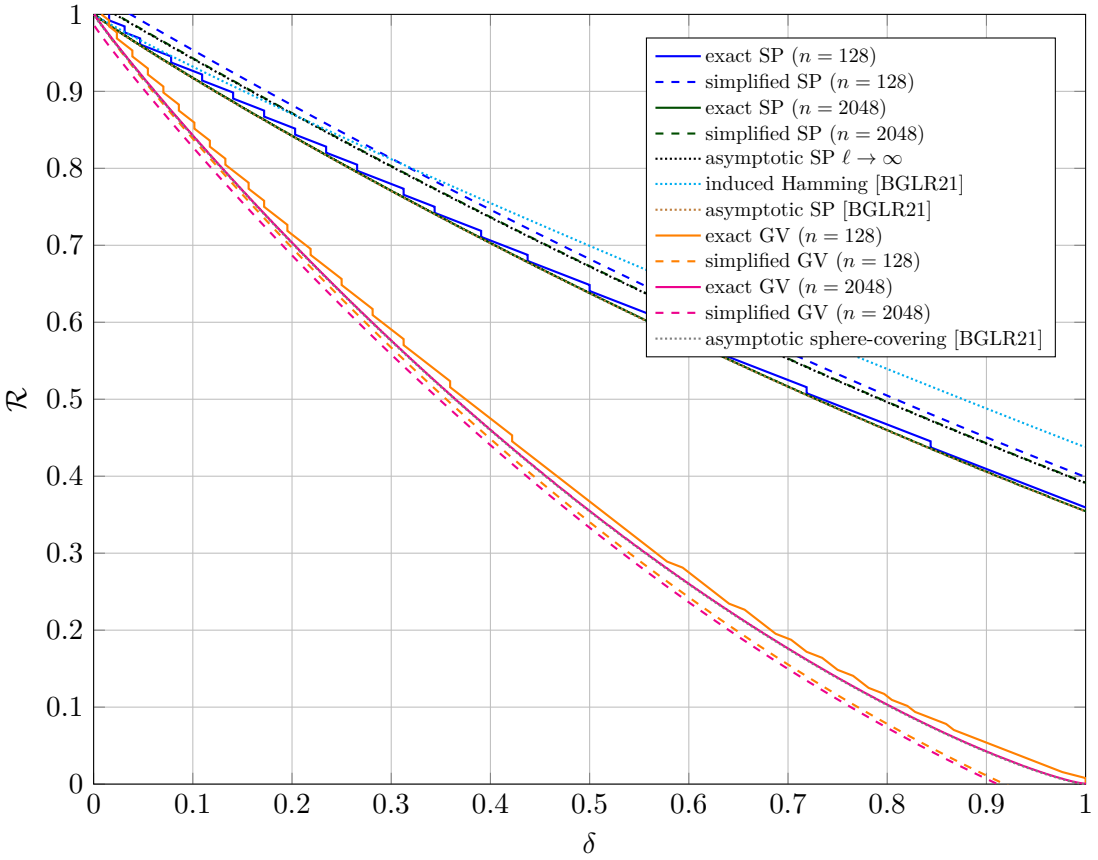


Figure 5.2.: Comparison of different bounds for fixed value $q = 2$, $\eta = 8$ and $m = 16$ for different values of n ($\ell = \frac{n}{\eta}$). Adapted from [OPB21]. © 2021 IEEE.

5.2. Covering Properties of Codes in the Sum-Rank Metric

In this section we explore the covering properties of codes in the sum-rank metric. The so-called *covering problem* addresses the following question: "Given a vector space, what is the minimum number of balls of a certain sum-rank radius that cover this space entirely?" Or in turn, for a given vector space and a specified number of balls: "What is the minimum sum-rank radius, such that these balls cover the space entrirely?" This radius is called: *the covering radius*.
Within the realm of coding theory, the centers of these balls correspond to codewords. Therefore, the covering radius serves as a fundamental geometric parameter for a code and acts as an indicator of code performance. Specifically, the covering radius of a code is associated with the maximum weight of a correctable error. While this aspect has been extensively investigated for the Hamming metric (see, for example, [BGP14], [CHLL97], [CKMS85]), covering properties in the rank metric have been explored in [GY08b] and [GY09]. In this section, we commence by presenting foundational concepts related to the

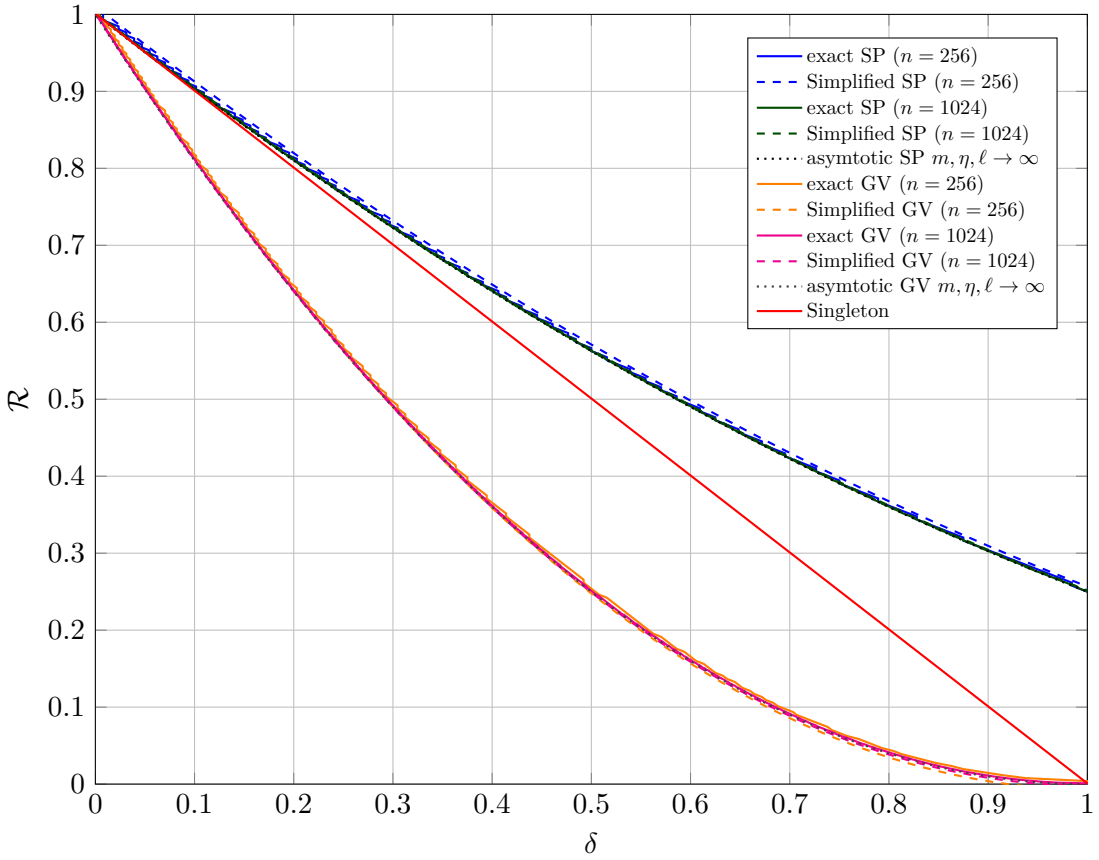


Figure 5.3.: Comparison of different bounds for fixed value of $q = 16$ and different values of n with $\eta = \ell = m$. Adapted from [OPB21]. © 2021 IEEE.

covering properties of codes in the sum-rank metric. We show the relationships among covering radii in the rank, sum-rank, and Hamming metric. Additionally, we investigate the connections between the minimum cardinality of a code and a given covering radius in these three metrics. Building upon the insights from [GY08b], we establish lower and upper bounds on the minimum cardinality of a code for a given covering radius.

Definition 5.16 (Covering Radius)**.** Let $\mathcal{C}$ be a linear $[n, k, d]$ ℓ-sum-rank-metric code over $\mathbb{F}_{q^m}$. The *covering radius* of $\mathcal{C}$, denoted as $\rho_{SR,\ell}$, is the smallest integer ensuring that any vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ exhibits a sum-rank distance of at most $\rho_{SR,\ell}$ to some codeword $\boldsymbol{c} \in \mathcal{C}$. To put it differently, $\rho_{SR,\ell}$ signifies the maximal sum-rank distance from any vector to its nearest codeword. This is mathematically expressed as

$$\rho_{SR,\ell} = \max_{\boldsymbol{x} \in \mathbb{F}_{q^m}^n} \{\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \mathcal{C})\}.$$

The subscript ℓ indicates the number of blocks. Hence, the notions $\rho_{SR,1}$ and $\rho_{SR,n}$ are utilized to refer to the covering radius in the rank and in the Hamming metric,

respectively. Similarly, we use ρ to denote the covering radius for an arbitrary metric, defined as $\rho = \max_{\boldsymbol{x}\in\mathbb{F}_{q^m}^n} \mathrm{d}(\boldsymbol{x}, \mathcal{C})$.

For a pair of codes $\mathcal{C}$ and $\mathcal{C}'$ such that $\mathcal{C} \subset \mathcal{C}' \subset \mathbb{F}_{q^m}^n$, it is established that their covering radii, denoted as ρ and ρ' respectively, satisfy $\rho \geq \rho'$ irrespective of the metric used. Moreover, it can be demonstrated that ρ is inherently larger than or equal to the minimum distance d' of $\mathcal{C}'$. To illustrate this, consider the choice of a vector $\boldsymbol{x} \in \mathcal{C}' \setminus \mathcal{C}$. This selection implies that for every $\boldsymbol{c} \in \mathcal{C}'$, the distance $\mathrm{d}(\boldsymbol{x}, \boldsymbol{c})$ is larger than or equal to d', and this holds true for every $\boldsymbol{c} \in \mathcal{C}$ as well. Consequently, $\min_{\boldsymbol{c}\in\mathcal{C}} \mathrm{d}(\boldsymbol{x}, \boldsymbol{c}) \geq d'$, which translates to $\mathrm{d}(\boldsymbol{x}, \mathcal{C}) \geq d'$. This leads to the conclusion that $\rho = \max_{\boldsymbol{x}\in\mathbb{F}_{q^m}^n} \mathrm{d}(\boldsymbol{x}, \mathcal{C}) \geq d'$. This observation lays the groundwork for the concept of *maximal codes*.

Definition 5.17 (Maximal Codes)**.** A linear $[n, k, d]$ code $\mathcal{C}$ is called *maximal* if there is no linear $[n, k', d]$ code $\mathcal{C}'$ with the same length n and minimum distance d, but with a larger dimension $k' > k$, such that $\mathcal{C} \subsetneq \mathcal{C}'$.

It is a known fact that the covering radius of a maximal code is smaller than its minimum distance (see, e.g., [GY08b]). This observation stems from the fact that for a maximal $[n, k, d]$ code $\mathcal{C}$, there is no element $\boldsymbol{x} \in \mathbb{F}_{q^m}^n \setminus \mathcal{C}$ such that $\mathrm{d}(\boldsymbol{x}, \mathcal{C}) \geq d$. Indeed, if such an element existed, one could construct a code $\mathcal{C}' = \langle \mathcal{C} \cup \{\boldsymbol{x}\} \rangle \supsetneq \mathcal{C}$ with $d(\mathcal{C}') = d$, contradicting the assumption that $\mathcal{C}$ is maximal.

It is important to note that maximal codes and perfect codes are distinct concepts. For a *perfect code*, the *packing radius* (that is, $\lfloor (d-1)/2 \rfloor$) equals the covering radius ρ, meaning that the spheres of radius $\lfloor (d-1)/2 \rfloor$ around the codewords exactly partition the entire space $\mathbb{F}_{q^m}^n$. A maximal code needs not be perfect. Consider, for example, a binary repetition code $\mathcal{C}$ in the Hamming-metric case ($\ell = n$) of even length n, i.e., $\mathcal{C} \subset \mathbb{F}_2^n$ is an $[n, 1, n]$ code. The covering radius of this code is $\rho = \frac{n}{2}$, whereas the packing radius is $\lfloor \frac{n-1}{2} \rfloor = \frac{n}{2} - 1$. Hence, the code is not perfect. However, $\mathcal{C}$ is maximal, since an $[n, 2, n]$ code $\mathcal{C}'$ cannot exist: every nonzero codeword of a binary code with minimum distance n must have weight n. Over $\mathbb{F}_2$, there is only one vector of weight n, namely the all-one vector. Thus, it is impossible to have two linearly independent nonzero codewords of weight n, in particular none with covering radius $\rho = \frac{n}{2}$.

Notation 5.18. *For a given vector space $\mathbb{F}_{q^m}^n$ and a specified integer ρ, we denote the minimum cardinality of a code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ with sum-rank covering radius ρ as $\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho)$. This value can be expressed as follows: Let*

$$\mathcal{A}_\ell \coloneqq \left\{ \mathcal{C} \subset \mathbb{F}_{q^m}^n : \bigcup_{\boldsymbol{c}\in\mathcal{C}} \mathcal{B}_\ell(\boldsymbol{c}, \rho) \supset \mathbb{F}_{q^m}^n \right\}.$$

Then,

$$\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho) = \min_{\mathcal{C}\in\mathcal{A}} \{|\mathcal{C}|\}.$$

Similarly to the covering radius we again use the subscript ℓ to indicate the number of blocks. Hence, for a given covering radius ρ and a vector space $\mathbb{F}_{q^m}^n$ we denote by $\mathcal{K}_{SR,1}(\mathbb{F}_{q^m}^n, \rho)$ and $\mathcal{K}_{SR,n}(\mathbb{F}_{q^m}^n, \rho)$ the minimum cardinality of a code in rank and in Hamming metric, respectively.

With this groundwork, we now formulate the sphere-covering problem for the sum-rank metric.

Problem 5.19. *Determine the minimum number of sum-rank balls, denoted as $\mathcal{B}_\ell(\boldsymbol{x}, \rho)$ with radius ρ for all $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$, required to completely cover the vector space $\mathbb{F}_{q^m}^n$. This problem is analogous to finding the minimum cardinality $\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho)$ of a code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ such that it possesses a sum-rank covering radius of ρ.*

The covering problem is visualized in Figure 5.4.

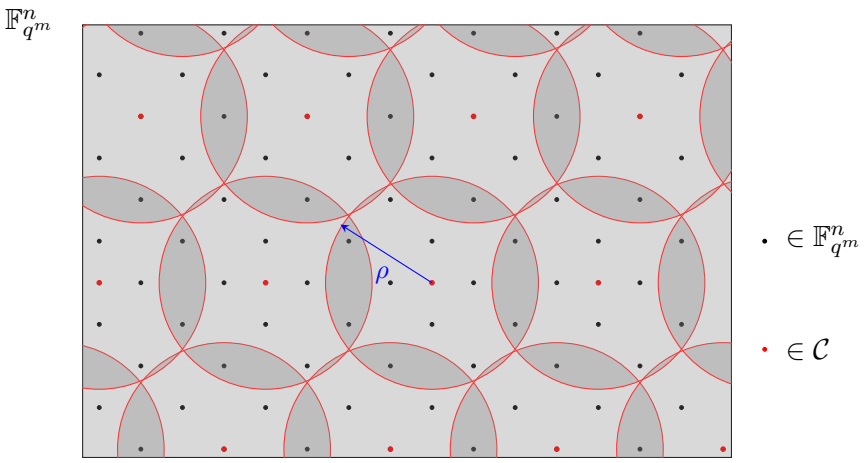


Figure 5.4.: Covering problem in the sum-rank metric.

For the covering radius there exist two extreme cases:

(i) $\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, 0) = q^{mn}$

(ii) $\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \mu\ell) = 1.$

Case (i) holds because when $\rho_{SR,\ell} = 0$, it implies $\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \mathcal{C}) = 0$ for all $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$, and consequently, $\boldsymbol{x} \in \mathcal{C}$. Therefore, $\mathcal{C} = \mathbb{F}_{q^m}^n$. For Case (ii), consider $\rho_{SR,\ell} = \max_{\boldsymbol{x} \in \mathbb{F}_{q^m}^n} \{\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \mathcal{C})\} = \mu \cdot \ell$. This implies the existence of an $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ such that $\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \mathcal{C}) = \mu \cdot \ell$. This condition is already satisfied by choosing $\mathcal{C} = \{(0, \ldots, 0)\}$. To explore non-trivial cases, we assume $0 < \rho_{SR,\ell} < \mu \cdot \ell$. For a fixed code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$, the relationship between covering radii in the rank and Hamming metric is well-established. In the following, we categorize the covering radii in the sum-rank metric within this established relation.

Lemma 5.20 ([OLWZ22, Lemma 1])**.** *For a code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$, the corresponding covering radii $\rho_{SR,1}$, $\rho_{SR,\ell}$, and $\rho_{SR,n}$ in the rank, sum-rank, and Hamming metrics, respectively, satisfy the inequality*

$$\rho_{SR,1} \leq \rho_{SR,\ell} \leq \rho_{SR,n}.$$

Proof. Given a fixed vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$, the relation of the weights in the different metrics:

$$\mathrm{wt}_{SR,1}(\boldsymbol{x}) \leq \mathrm{wt}_{SR,\ell}(\boldsymbol{x}) \leq \mathrm{wt}_{SR,n}(\boldsymbol{x}),$$

as introduced in Section 2.2.3 implies the following relation for the distance of the fixed vector $\boldsymbol{x}$ to the code $\mathcal{C}$:

$$\mathrm{d}_{SR,1}(\boldsymbol{x}, \mathcal{C}) \leq \mathrm{d}_{SR,\ell}(\boldsymbol{x}, \mathcal{C}) \leq \mathrm{d}_{SR,n}(\boldsymbol{x}, \mathcal{C}).$$

Consequently,

$$\max_{\boldsymbol{x} \in \mathbb{F}_{q^m}^n} \{\mathrm{d}_{SR,1}(\boldsymbol{x}, \mathcal{C})\} \leq \max_{\boldsymbol{x} \in \mathbb{F}_{q^m}^n} \{\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \mathcal{C})\} \leq \max_{\boldsymbol{x} \in \mathbb{F}_{q^m}^n} \{\mathrm{d}_{SR,n}(\boldsymbol{x}, \mathcal{C})\}.$$

□

In the following theorem, we establish the relationship between the minimum cardinality of a code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ in the rank, sum-rank, and Hamming metric for a fixed covering radius ρ.

Theorem 5.21 ([OLWZ22, Theorem 2])**.** *Let ρ be a positive integer satisfying $0 < \rho < \mu \cdot \ell$. Then the following relations hold for the minimum cardinality of a code in the rank, sum-rank and Hamming metric:*

$$\mathcal{K}_{SR,1}(\mathbb{F}_{q^m}^n, \rho) \leq \mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho) \leq \mathcal{K}_{SR,n}(\mathbb{F}_{q^m}^n, \rho).$$

Proof. We define the set of codes with sum-rank covering radius ρ as

$$\mathcal{A}_{SR,\ell} \coloneqq \{\mathcal{C} \subset \mathbb{F}_{q^m}^n \mid \bigcup_{\boldsymbol{c} \in \mathcal{C}} \mathcal{B}_\ell(\boldsymbol{c}, \rho) \supset \mathbb{F}_{q^m}^n\}.$$

Since $\mathrm{wt}_{SR,1}(\boldsymbol{x}) \leq \mathrm{wt}_{SR,\ell}(\boldsymbol{x}) \leq \mathrm{wt}_{SR,n}(\boldsymbol{x})$ for a fixed vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$, it follows that

$$\bigcup_{\boldsymbol{c} \in \mathcal{C}} \mathcal{B}_1(\boldsymbol{c}, \rho) \supset \bigcup_{\boldsymbol{c} \in \mathcal{C}} \mathcal{B}_\ell(\boldsymbol{c}, \rho) \supset \bigcup_{\boldsymbol{c} \in \mathcal{C}} \mathcal{B}_n(\boldsymbol{c}, \rho),$$

establishing the relationship $\mathcal{A}_{SR,1} \supset \mathcal{A}_{SR,\ell} \supset \mathcal{A}_{SR,n}$. With

$$\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho) = \min_{\mathcal{C} \in \mathcal{A}_{SR,\ell}} \{|\mathcal{C}|\},$$

the statement follows. □

5.2.1. Lower Bounds on the Minimum Cardinality of a Code for a Given Covering Radius

For the rank metric, [GY08b, Proposition 6] established both a lower and an upper bound on the minimum cardinality of a code with a specified covering radius. Referred to as the *sphere-covering bound*, the lower bound is now mirrored in the sphere-covering bound analog for the sum-rank metric, which we present in the subsequent theorem.

Theorem 5.22 (Sphere-Covering Bound [OLWZ22, Theorem 3])**.** *The minimum cardinality of a code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ with a sum-rank covering radius $0 < \rho < \mu \cdot \ell$ is bounded by the inequality*

$$\frac{q^{mn}}{\mathrm{Vol}_{\mathcal{B}_\ell}(\rho)} \leq \mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho).$$

Proof. Should it be feasible to cover the entire space $\mathbb{F}_{q^m}^n$ with non-overlapping balls of radius ρ, then $\frac{q^{mn}}{\mathrm{Vol}_{\mathcal{B}_\ell}(\rho)} = \mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho)$. However, this circumstance is only achievable for perfect sum-rank-metric codes. In contrast to the rank metric, where no nontrivial perfect codes exist, the sum-rank metric allows for such codes. This is due to the presence of nontrivial perfect codes in the Hamming metric, which are encompassed in the sum-rank metric when considering the number of blocks $\ell = n$. If there is any overlap among the balls, then $\frac{q^{mn}}{\mathrm{Vol}_{\mathcal{B}_\ell}(\rho)} < \mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho)$. □

To exactly compute the bound, it is necessary to determine the exact volume of a ball for a given sum-rank radius, as introduced in equation (4.4). It is worth noting that this calculation can be performed with a complexity of $\mathcal{O}^{\sim}(\ell^2\delta^3 + \ell\delta^4(m+\eta)\log(q))$ using the efficient algorithm for computing $\mathrm{Vol}_{\mathcal{S}_\ell}$ as outlined in [PRR22]. Nevertheless, despite the polynomial complexity, computing it for large parameters remains time-consuming. This motivates the formulation of the following simplified version of the sphere-covering bound.

Theorem 5.23 (Simplified Sphere-Covering Bound [OLWZ22, Theorem 4])**.** *The minimum cardinality of a code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ with a sum-rank covering radius ρ satisfying $0 < \rho < \mu \cdot \ell$ is lower bounded as follows:*

$$\frac{q^{mn-\rho(m+\eta-\frac{\rho}{\ell})}}{\rho \cdot \binom{\ell+\rho-1}{\ell-1}\gamma_q^\ell} \leq \mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho).$$

Proof. By substituting the upper bound on $\mathrm{Vol}_{\mathcal{B}_\ell}(\rho)$, as provided in Theorem 4.15 into Theorem 5.22, the assertion follows. □

For the rank metric, it was demonstrated in [GY09, Proposition 7] that a code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ with a covering radius $0 < \rho < n < m$ comprises at least three codewords. We extend this finding to the sum-rank metric. In contrast to [GY09], there is no constraint on the relationship between n and m.

Theorem 5.24 ([OLWZ22, Theorem 5])**.** *Each sum-rank-metric code with covering radius ρ fulfilling $0 < \rho < \mu \cdot \ell$ consists of at least three codewords: $\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho) \geq 3$.*

Proof. We show the claim by contradiction. Therefore, we assume the existence of a code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ of length n with cardinality $|\mathcal{C}| = 2$ and covering radius ρ satisfying $\rho < \mu \cdot \ell$. W.l.o.g., we suppose $\mathcal{C} = \{\mathbf{0}, \boldsymbol{c}\}$. To obtain the smallest possible covering radius ρ, we select $\boldsymbol{c}$ with a sum-rank weight of $\mu\ell$ such that the cardinality of the union of balls with radius ρ around the two codewords $|\mathcal{B}_\ell(\mathbf{0}, \rho) \cup \mathcal{B}_\ell(\boldsymbol{c}, \rho)|$ is maximized. The code $\mathcal{C}' \coloneqq \langle \boldsymbol{c} \rangle$ forms a linear $[n, 1, \mu\ell]$ sum-rank-metric code. Consequently, any vector

$\boldsymbol{x} \in \mathcal{C}' \setminus \mathcal{C}$ has a sum-rank distance of $\mu\ell$ to $\mathcal{C}$, implying $\rho = \mu\ell$. This contradicts the assumption $\rho < \mu \cdot \ell$. It is important to note that opting for a smaller sum-rank weight for $\boldsymbol{c}$ cannot yield a smaller covering radius. □

In the subsequent theorem, we present a nontrivial lower bound on the minimum cardinality of a code with a specified covering radius. This bound serves as the sum-rank-metric analogue to the one derived in [GY08b]. A notable characteristic of this bound is that the right-hand side constitutes a monotonically increasing function in k, where $0 \leq k \leq \lfloor \log_{q^m}(\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho)) \rfloor$. This property allows for iterative utilization of the bound. We commence with $k = \lfloor \log_{q^m}(\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho)) \rfloor$, for which the bound is most stringent. However, since the exact value of $\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho)$ is generally unknown, we employ a previously established lower bound to determine the initial value of k, such as the simplified sphere-covering bound in Theorem 5.23. In each iteration (i-th), we employ the bound derived in the previous iteration $i-1$ to compute a new value of k which results in a new bound. We conclude the process when the value of k no longer improves upon application of the bound.

Theorem 5.25 ([OLWZ22, Theorem 6])**.** *Let ρ be a positive integer satisfying $0 < \rho < \mu \cdot \ell$. Then the minimum cardinality $\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho)$ of a code over $\mathbb{F}_{q^m}^n$ with covering radius ρ, is lower bounded as follows:*

$$\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho) \geq \frac{q^{mn} - q^{km}\mathrm{Vol}_{\mathcal{I}_\ell}(\rho, \rho, \frac{nm}{\nu} - \frac{km}{\nu}) + \sum_{\substack{k'=\max\{1,\\ \lceil n + \frac{\nu}{m}(1-2\rho)\rceil\}}}^{k} (q^{k'm} - q^{(k'-1)m})\mathrm{Vol}_{\mathcal{I}_\ell}(\rho, \rho, \frac{nm}{\nu} - \frac{k'm}{\nu} + 1)}{\mathrm{Vol}_{\mathcal{B}_\ell}(\rho) - \mathrm{Vol}_{\mathcal{I}_\ell}(\rho, \rho, \frac{nm}{\nu} - \frac{km}{\nu})},$$

for each positive integer k, fulfilling $k \leq \lfloor \log_{q^m}(\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho)) \rfloor$.

Proof. We define $k_{\max} \coloneqq \lfloor \log_{q^m}(\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho)) \rfloor$ and $K \coloneqq q^{mk_{\max}}$. Then, there exists a code with cardinality K and covering radius ρ, denoted by $\mathcal{C} \coloneqq \{\boldsymbol{c}_0, \ldots, \boldsymbol{c}_{K-1}\} \subset \mathbb{F}_{q^m}^n$. Additionally, for each j with $0 \leq j \leq K-1$ we define a subcode $\mathcal{C}_j \coloneqq \{\boldsymbol{c}_0, \ldots, \boldsymbol{c}_j\} \subset \mathcal{C}$ where the labeling of its codewords is chosen such that the distance of the codeword $\boldsymbol{c}_j$ to the code $\mathcal{C}_{j-1}$ is decreasing for $j > 0$, i.e.,

$$\mathrm{d}_{SR,\ell}(\boldsymbol{c}_1, \mathcal{C}_0) \geq \mathrm{d}_{SR,\ell}(\boldsymbol{c}_2, \mathcal{C}_1) \geq \ldots \geq \mathrm{d}_{SR,\ell}(\boldsymbol{c}_{K-1}, \mathcal{C}_{K-2}).$$

We denote by $\mathrm{d_j}$ the minimum distance of the subcode $\mathcal{C}_j$. Hence, $\mathrm{d}_{SR,\ell}(\boldsymbol{c}_j, \mathcal{C}_{j-1}) = \min_{1 \leq i \leq j}\{\mathrm{d}_{SR,\ell}(\boldsymbol{c}_i, \mathcal{C}_{i-1})\}$ corresponds to the minimum distance $\mathrm{d_j}$ of $\mathcal{C}_j$ for every j with $0 < j < K-1$. Let k' be a positive integer fulfilling $1 \leq k' \leq k_{\max}$ and let j and be chosen such that $q^{m(k'-1)} \leq j \leq q^{mk'}$, then the Singleton bound for the sum-rank metric (Theorem 5.1) provides

$$\mathrm{d_j} = \mathrm{d}_{SR,\ell}(\boldsymbol{c}_j, \mathcal{C}_{j-1}) \leq \frac{nm}{\nu} - \frac{k'm}{\nu} + 1.$$

Thus, the number of vectors covered by a ball of radius ρ around $\boldsymbol{c}_j$ that are not covered by the union of balls of radius ρ around the codewords in $\mathcal{C}_{j-1}$ is upper bounded as follows:

$$|\mathcal{B}_\ell(\boldsymbol{c}_j,\rho) \setminus \bigcup_{\boldsymbol{c}\in\mathcal{C}_{j-1}} \mathcal{B}_\ell(\boldsymbol{c},\rho)| \leq \mathrm{Vol}_{\mathcal{B}_\ell}(\rho) - \mathrm{Vol}_{\mathcal{I}_\ell}(\rho,\rho,\frac{nm}{\nu}-\frac{k'm}{\nu}+1). \tag{5.11}$$

As the covering radius of the whole code $\mathcal{C}$ is ρ, the set of vectors that are covered by the union of balls of radius ρ around the codewords in $\mathcal{C}$ is the entire space $\mathbb{F}_{q^m}^n$. Therefore, for $1 \leq k \leq k_{\max}$ it holds that

$$\begin{aligned} q^{mn} = \Big|\bigcup_{\boldsymbol{c}\in\mathcal{C}} \mathcal{B}_\ell(\boldsymbol{c},\rho)\Big| \leq \Big|\mathcal{B}_\ell(\boldsymbol{c}_0,\rho)\Big| \\ + \sum_{k'=1}^{k} \Big|\{\boldsymbol{c}\in\mathcal{C}_{q^{mk'}} \setminus \mathcal{C}_{q^{m(k'-1)}}\}\Big| \cdot \Big|\mathcal{B}_\ell(\boldsymbol{c}_{q^{mk'}},\rho) \setminus \bigcup_{\boldsymbol{c}\in\mathcal{C}_{q^{m(k'-1)}}} \mathcal{B}_\ell(\boldsymbol{c},\rho)\Big| \\ + \Big|\{\boldsymbol{c}\in\mathcal{C} \setminus \mathcal{C}_{q^{mk}}\}\Big| \cdot \Big|\mathcal{B}_\ell(\boldsymbol{c}_{K-1},\rho) \setminus \bigcup_{\boldsymbol{c}\in\mathcal{C}_{q^{mk}}} \mathcal{B}_\ell(\boldsymbol{c},\rho)\Big|. \end{aligned}$$

Combining this with inequality (5.11) leads to

$$\begin{aligned} q^{mn} \leq & \mathrm{Vol}_{\mathcal{B}_\ell}(\rho) + \sum_{k'=1}^{k} (q^{k'm} - q^{(k'-1)m}) \cdot \Big(\mathrm{Vol}_{\mathcal{B}_\ell}(\rho) - \mathrm{Vol}_{\mathcal{I}_\ell}(\rho,\rho,\frac{nm}{\nu}-\frac{km}{\nu}+1)\Big) \\ & + (K - q^{km})\Big(\mathrm{Vol}_{\mathcal{B}_\ell}(\rho) - \mathrm{Vol}_{\mathcal{I}_\ell}(\rho,\rho,\frac{nm}{\nu}-\frac{km}{\nu})\Big). \end{aligned}$$

Transforming this inequality yields

$$\begin{aligned} & K\left(\mathrm{Vol}_{\mathcal{B}_\ell}(\rho) - \mathrm{Vol}_{\mathcal{I}_\ell}(\rho,\rho,\frac{nm}{\nu}-\frac{km}{\nu})\right) \\ & \geq q^{mn} - \mathrm{Vol}_{\mathcal{I}_\ell}\Big(\rho,\rho,\frac{nm}{\nu}-\frac{km}{\nu}\Big)q^{km} - \mathrm{Vol}_{\mathcal{B}_\ell}(\rho)\left(\sum_{k'=1}^{k}\Big(q^{k'm}-q^{(k'-1)m}\Big) - q^{km} + 1\right) \\ & + \sum_{k'=1}^{k}\Big(q^{k'm}-q^{(k'-1)m}\Big)\left(\mathrm{Vol}_{\mathcal{I}_\ell}\Big(\rho,\rho,\frac{nm}{\nu}-\frac{k'm}{\nu}+1\Big)\right). \end{aligned}$$

If $\frac{m}{\nu}k' < \frac{nm}{\nu} + 1 - 2\rho$, then $\mathrm{Vol}_{\mathcal{I}_\ell}(\rho,\rho,\frac{nm}{\nu}-\frac{k'm}{\nu}+1) = 0$ which leads to

$$\begin{aligned} & K\Big(\mathrm{Vol}_{\mathcal{B}_\ell}(\rho) - \mathrm{Vol}_{\mathcal{I}_\ell}\Big(\rho,\rho\frac{nm}{\nu}-\frac{km}{\nu}\Big)\Big) \\ & \geq q^{mn} - \mathrm{Vol}_{\mathcal{I}_\ell}\Big(\rho,\rho,\frac{nm}{\nu}-\frac{km}{\nu}\Big)q^{km} - \mathrm{Vol}_{\mathcal{B}_\ell}(\rho)\Big(q^{km}-1-q^{km}+1\Big) \\ & + \sum_{\substack{k'=\max\{1,\\ \lceil n+\frac{\nu}{m}(1-2\rho)\rceil\}}}^{k} \Big(q^{k'm}-q^{(k'-1)m}\Big)\cdot\mathrm{Vol}_{\mathcal{I}_\ell}\Big(\rho,\rho,\frac{nm}{\nu}-\frac{k'm}{\nu}+1\Big) \end{aligned}$$

This concludes the proof. □

To derive an explicit lower bound from Theorem 5.25, we need to calculate the volume of the intersection of two balls in the sum-rank metric exactly. This calculation is required either in general or at least for the specific cases considered in Theorem 5.25. For deriving a closed-form expression for these special cases, Theorems 4.20 and 4.21 provide a starting point. The general formula for calculating the volume is given in Theorem 4.18. However, using this formula involves exponential complexity. Therefore, it would be beneficial to develop a polynomial-time algorithm for this calculation, similar to what exists for the volume of a single ball in the sum-rank metric (cf. [PRR22]). Another approach to derive a closed-form expression for Theorem 5.25 is to establish bounds on the volume of the intersection of the two balls. However, it would be necessary to determine both an upper bound and a lower bound for this volume. These considerations need to be addressed in future research.

5.2.2. Upper Bounds on the Minimum Cardinality of a Code for a Given Covering Radius

For the rank metric, an upper bound on the minimum cardinality of a code with given covering radius was derived in [GY08b, Proposition 6]. In what follows, we extend this bound to the sum-rank metric. Unlike [GY08b], we impose no restrictions on the relation between m and n.

Theorem 5.26 ([OLWZ22, Theorem 7])**.** *The minimum cardinality of a code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ with sum-rank covering radius ρ, where $0 < \rho < \mu \cdot \ell$ is upper bounded as follows:*

$$\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho) \leq q^{m(n-\rho)}.$$

Proof. Let $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ be a sum-rank-metric code and let $\boldsymbol{G} = (\boldsymbol{I}|\boldsymbol{A})$ be its systematic generator matrix. For each vector $\boldsymbol{x} = [x_0, \ldots, x_{n-1}] \in \mathbb{F}_{q^m}^n$ there exists a codeword $\boldsymbol{c}$, such that the first k positions coincide with the first k positions of $\boldsymbol{x}$, i.e., $\boldsymbol{c} = [x_0, \ldots, x_{k-1}, c_k, \ldots, c_{n-1}] \in \mathcal{C}$. Consequently, the sum-rank distance between $\boldsymbol{c}$ and $\boldsymbol{x}$ is upper bounded by

$$\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \boldsymbol{c}) = \mathrm{wt}_{SR,\ell}([0, \ldots, 0, c_k, \ldots, c_{n-1}] \leq \mathrm{wt}_{SR,n}[0, \ldots, 0, c_k, \ldots, c_{n-1}] \leq n - k.$$

Therefore, for each vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ it holds that $\min_{\boldsymbol{c}\in\mathcal{C}}\{\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \boldsymbol{c})\} \leq n - k$ and hence $\rho = \max_{\boldsymbol{x}\in\mathbb{F}_{q^m}^n}\{\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \mathcal{C})\} \leq n - k$. Since $\rho \leq n - k$ we obatin $k \leq n - \rho$, which leads to the upper bound

$$\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho) \leq |\mathcal{C}| = q^{mk} \leq q^{m(n-\rho)}.$$

□

To establish a non-trivial upper bound on the covering problem, we need the following result which allows us to construct a code with a specified covering radius using an MSRD code over a smaller field maintaining the same covering radius ρ, code length n and

dimension k. This approach was introduced for the rank metric in [GY08b, Proposition 10]. In contrast to [GY08b] we do not impose any restriction on the relation between m and n, however we do require a stricter condition on the covering radius ρ.

Lemma 5.27 ([OLWZ22, Theorem 8])**.** *Let $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ be a sum-rank-metric code with parameters $[n, n-\rho, \rho+1]$, i.e., $\mathcal{C}$ is MSRD and let ρ be its covering radius. Additionally, let $\bar{f}_u$ be a function defined as in Lemma 4.9, where u is a positive integer such that $0 \leq u \cdot \ell \leq \rho$. Then $\bar{f}_u(\mathcal{C})$ is an $[n, n-\rho]$ ℓ-sum-rank-metric code over $\mathbb{F}_{q^{m+u}}$ with covering radius ρ.*

Proof. As the mapping $\bar{f}_u : \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^{m+u}}^n$ is linear and bijective, applying $\bar{f}_u$ to the code $\mathcal{C}$ results in a linear code $\bar{f}_u(\mathcal{C}) \subset \mathbb{F}_{q^{m+u}}^n$, where the length n and dimension $n-\rho$ are unchanged.

We prove now that the covering radius of $\bar{f}_u(\mathcal{C})$ is ρ. Let $\mathcal{B}_m$ be as in Lemma 4.9 and let $\mathcal{A}$ be a subspace of $\mathbb{F}_q^{m+u}$ over $\mathbb{F}_q$ of dimension u, such that $\mathcal{A} \oplus \mathcal{B}_m = \mathbb{F}_q^{m+u}$. Hence, any vector $\boldsymbol{u} = [\boldsymbol{u}_0 | \ldots | \boldsymbol{u}_{\ell-1}] \in \mathbb{F}_{q^{m+u}}^n$ can be expressed as a sum

$$\boldsymbol{u} = \boldsymbol{a} + \boldsymbol{b} = [\boldsymbol{a}_0 + \boldsymbol{b}_0 | \ldots | \boldsymbol{a}_{\ell-1} + \boldsymbol{b}_{\ell-1}] \tag{5.12}$$

with $\boldsymbol{a}_i \in \mathcal{A}^\eta, \boldsymbol{a} \in \mathcal{A}^n, \boldsymbol{b}_i \in \mathcal{B}^\eta$ and $\boldsymbol{b} \in \mathcal{B}^n$. Since the $\mathbb{F}_q$-dimension of $\mathcal{A}$ is u, the sum-rank weight of $\boldsymbol{a}$ is upper bounded by

$$\mathrm{wt}_{SR,\ell}(\boldsymbol{a}) = \sum_{i=0}^{\ell-1} \mathrm{wt}_{SR,1}(\boldsymbol{a}_i) \leq \ell \cdot u.$$

According to Lemma 4.3 each $\boldsymbol{a}_i$ belongs to a unique elementary linear subspace $\mathcal{W}_i \in \mathcal{E}_u(\mathbb{F}_{q^{m+u}}^\eta)$ for every $i \in \{0, \ldots, \ell-1\}$. Furthermore, the Cartesian product of these elementary linear subspaces $\mathcal{W} \coloneqq \mathcal{W}_0 \times \ldots \times \mathcal{W}_{\ell-1}$ is also uniquely determined and $\mathcal{W} \in \mathcal{E}_\rho(\mathbb{F}_{q^{m+u}}^n)$. As $\mathcal{C}$ is an MSRD code, Lemma 5.2 indicates, that for each sequence $(\mathcal{V}_i)_{0 \leq i \leq \ell-1}$ of elementary linear subspaces of $\mathbb{F}_{q^m}^\eta$ maintaining that $\sum_{i=0}^{\ell-1} \dim(\mathcal{V}_i) = \frac{nm}{\nu} - \frac{km}{\nu}$, the direct sum of their Cartesian product with the code $\mathcal{C}$ is the entire space. In other words: let $\mathcal{M}$ be the set

$$\mathcal{M}_\mathcal{C} \coloneqq \left\{ \mathcal{V}_0 \times \ldots \times \mathcal{V}_{\ell-1} | \mathcal{V}_i \in \mathcal{E}_\eta(\mathbb{F}_{q^m}^\eta) \wedge \sum_{i=0}^{\ell-1} \dim(\mathcal{V}_i) = \frac{nm}{\nu} - \frac{km}{\nu} \right\},$$

where μ, η, k and ℓ are determined by the code $\mathcal{C}$, then

$$\mathcal{V} \oplus \mathcal{C} = \mathbb{F}_{q^m}^n \text{ for all } \mathcal{V} \in \mathcal{M}_\mathcal{C}. \tag{5.13}$$

As $k = n - \rho$ and $\frac{m}{\nu} \leq 1$, we obtain $\frac{m}{\nu}(n-k) \leq \rho$. Consequently, $\sum_{i=0}^{\ell-1} \dim(\mathcal{V}_i) = \frac{nm}{\nu} - \frac{km}{\nu} \leq \rho$, implying that $\mathcal{M}_\mathcal{C} \subset \mathcal{E}_\rho(\mathbb{F}_{q^m}^n)$. By Lemma 4.9, we can write $\boldsymbol{b}$ in equation (5.12) as $\boldsymbol{b} = \bar{f}_u(\boldsymbol{u})$. Together with equation 5.13 and the linearity of $\bar{f}_u$ we obtain that $\boldsymbol{b}$ can be expressed as

$$\boldsymbol{b} = \bar{f}_u(\boldsymbol{u}) = \bar{f}_u(\boldsymbol{c} + \boldsymbol{e}) = \bar{f}_u(\boldsymbol{c}) + \bar{f}_u(\boldsymbol{e})$$

where $\boldsymbol{c} \in \mathcal{C}$ and $\boldsymbol{e} = [\boldsymbol{e}_1|\dots|\boldsymbol{e}_\ell] \in \mathcal{V} \in \mathcal{M}_\mathcal{C} \subset \mathcal{E}_\rho(\mathbb{F}_{q^m}^n)$ such that $\bar{f}_u(\mathcal{V}) \subset \mathcal{W} \in \mathcal{E}_\rho(\mathbb{F}_{q^{m+u}}^n)$. Hence, $\bar{f}_u(\boldsymbol{e}) \in \mathcal{W}$ and consequently, $\bar{f}_u(\boldsymbol{e}) + \boldsymbol{a} \in \mathcal{W}$. Therefore,

$$\boldsymbol{u} = \boldsymbol{a} + \boldsymbol{b} = \boldsymbol{a} + \bar{f}_u(\boldsymbol{c}) + \bar{f}_u(\boldsymbol{e})$$

with $\mathrm{wt}_{SR,\ell}(\boldsymbol{a} + \bar{f}_u(\boldsymbol{e})) = \sum_{i=0}^{\ell-1} \mathrm{wt}_{SR,1}(\boldsymbol{a}_i + \bar{f}_u(\boldsymbol{e}_i)) \leq \rho$. Thus, the sum-rank distance of $\boldsymbol{u}$ to $\bar{f}_u(\boldsymbol{c})$ is upper bounded by

$$\mathrm{d}_{SR,\ell}(\boldsymbol{u}, \bar{f}_u(\boldsymbol{c})) = \mathrm{wt}_{SR,\ell}(\boldsymbol{a} + \bar{f}_u(\boldsymbol{e})) \leq \rho.$$

So, the distance of $\boldsymbol{u}$ to the image of the code $\mathcal{C}$ under $\bar{f}_u$ is also upper bounded by ρ, i.e., $\mathrm{d}_{SR,\ell}(\boldsymbol{u}, \bar{f}_u(\mathcal{C})) \leq \rho$, leading to

$$\max_{\boldsymbol{u} \in \mathbb{F}_{q^{m+u}}^n} \mathrm{d}_{SR,\ell}(\boldsymbol{u}, \bar{f}_u(\mathcal{C})) \leq \rho.$$

This shows that the covering radius of $\bar{f}_u(\mathcal{C})$ is smaller than or equal to ρ.

Since $\mathcal{C}$ has covering radius ρ, there exists a vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ such that $\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \mathcal{C}) = \rho$. Using that $\bar{f}_u$ is rank-preserving and linear, we obtain that $\bar{f}_u$ is even sum-rank preserving. Thus, for this vector $\boldsymbol{x}$ it follows that

$$\begin{aligned}\rho = \mathrm{d}_{SR,\ell}(\boldsymbol{x}, \mathcal{C}) &= \min_{\boldsymbol{c} \in \mathcal{C}} \{\mathrm{wt}_{SR,\ell}(\boldsymbol{c} - \boldsymbol{x})\} = \min_{\boldsymbol{c} \in \mathcal{C}} \{\mathrm{wt}_{SR,\ell}(\bar{f}_u(\boldsymbol{c} - \boldsymbol{x}))\} \\ &= \min_{\boldsymbol{c} \in \mathcal{C}} \{\mathrm{wt}_{SR,\ell}(\bar{f}_u(\boldsymbol{c}) - \bar{f}_u(\boldsymbol{x}))\} = \mathrm{d}_{SR,\ell}(\bar{f}_u(\boldsymbol{x}), \bar{f}_u(\mathcal{C})),\end{aligned}$$

which indicates that there is a vector with a sum-rank distance of ρ to $\bar{f}_u(\mathcal{C})$. Therefore, the covering radius of $\bar{f}_u(\mathcal{C})$ is exactly ρ. □

Using the result from Lemma 5.27, we can now establish a non-trivial upper bound on the minimum cardinality of a code with a given covering radius. A similar result was derived for the rank metric case in [GY08b]. Unlike their result, our bound does not impose any restrictions on the relationship between m and n.

Theorem 5.28 ([OLWZ22, Theorem 9])**.** *For an ℓ-sum-rank-metric code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ with sum-rank covering radius ρ, where $0 < \rho < \mu \cdot \ell$, the minimum cardinality of the code is upper bounded by*

$$\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho) \leq q^{(m - \lfloor \frac{\rho}{\ell} \rfloor) \cdot (n - \rho)}.$$

Proof. Let m, n, ℓ be positive integers such that ℓ is a divisor of n. Furthermore let μ be the minimum $\min\{m, \eta\}$, $\nu \coloneqq m - \lfloor \frac{\rho}{\ell} \rfloor$ and ρ a positive integer such that $\rho < \mu \cdot \ell$. With Lemma 5.27 it follows, that there exists a linear ℓ-sum-rank-metric code $\mathcal{C}$ over $\mathbb{F}_{q^\nu}^n$ of length n, dimension $n - \rho$ and covering radius ρ with minimum distance $\rho + 1$, i.e., $\mathcal{C}$ is an MSRD code. Given a basis $\alpha_0, \dots, \alpha_{\nu-1}$ of $\mathbb{F}_{q^\nu}$ and a basis $\beta_0, \dots, \beta_{m-1}$ of $\mathbb{F}_{q^m}$ with $\alpha_0 = \beta_0 = 1$ and $\mathcal{B}_\nu \coloneqq \langle \beta_0, \dots, \beta_{\nu-1} \rangle$, we define the following sum-rank-preserving mapping, similar to the one defined in Lemma 4.9, with $u \coloneqq \lfloor \frac{\rho}{\ell} \rfloor$:

$$f_u : \mathbb{F}_{q^\nu} \to \mathcal{B}_\nu, \quad \alpha_i \mapsto f_u(\alpha_i) = \beta_i \quad \text{for all } i \in \{0, \dots, \nu - 1\}.$$

Hence, each element $a = \sum_{i=0}^{\nu-1} a_i\alpha_i \in \mathbb{F}_{q^\nu}$, with $a_i \in \mathbb{F}_q$, is mapped to

$$f_u(a) = f_u\Big(\sum_{i=0}^{\nu-1} a_i\alpha_i\Big) = \sum_{i=0}^{\nu-1} a_i f_u(\alpha_i) = \sum_{i=0}^{\nu-1} a_i\beta_i.$$

The extension of f_u to n-dimensional vectors is given by just applying it componentwise:

$$\bar{f}_u : \mathbb{F}_{q^\nu}^n \to \mathcal{B}_\nu^n, \quad \boldsymbol{v} = [v_0, \ldots, v_{n-1}] \mapsto \bar{f}_u(\boldsymbol{v}) = [\bar{f}_u(v_0), \ldots, \bar{f}_u(v_{n-1})].$$

Since $u \cdot \ell \leq \rho$ we can apply Lemma 5.27 which tells us, that the image $\bar{f}_u(\mathcal{C}) \subset \mathbb{F}_{q^m}^n$ is an $[n, n-\rho]$ code with covering radius ρ. Now, we consider the cardinality of $\bar{f}_u(\mathcal{C})$. As $\bar{f}_u$ is a bijective mapping, we have that

$$|\bar{f}_u(\mathcal{C})| = |\mathcal{C}|.$$

The dimension of $\mathcal{C}$ over $\mathbb{F}_{q^\nu}$ is $n-\rho$. Hence,

$$|\mathcal{C}| = q^{\nu(n-\rho)} = q^{(m-\lfloor\frac{\rho}{\ell}\rfloor)\cdot(n-\rho)}.$$

As the minimum cardinality of a code in $\mathbb{F}_{q^m}^n$ with covering radius ρ is upper bounded by the cardinality of $\bar{f}_u(\mathcal{C})$, we obtain

$$\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho) \leq |\bar{f}_u(\mathcal{C})| = |\mathcal{C}| = q^{(m-\lfloor\frac{\rho}{\ell}\rfloor)\cdot(n-\rho)}.$$

□

In the context of finding bounds on the minimum cardinality of a code for a given vector space and covering radius, it is useful to establish relationships between the minimum cardinalities of codes with different lengths and covering radii. Such relationships can provide insights into how the code parameters scale and how larger codes can be constructed from smaller ones while maintaining or enhancing their error-correction capabilities. The following proposition addresses this problem by establishing a relationship between the minimum cardinality of a code of length n and covering radius ρ, a code of length n' and covering radius ρ' and a code of combined length $n+n'$ and covering radius $\rho+\rho'$. This proposition shows that the minimum cardinality of the combined code is upper bounded by the product of the minimum cardinalities of the individual codes.

Proposition 5.29 ([OLWZ22, Lemma 7])**.** *Let n, n', ρ, ρ', ℓ and m be nonnegative integers with $m > 0$ where ℓ divides both n and n'. Then the minimum cardinality of a code in $\mathbb{F}_{q^m}^{n+n'}$ with covering radius $\rho+\rho'$ is upper bounded by the product of the minimum cardinalities of codes in $\mathbb{F}_{q^m}^n$ with covering radius ρ and $\mathbb{F}_{q^m}^{n'}$ with covering radius ρ':*

$$\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^{n+n'}, \rho+\rho') \leq \mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho) \cdot \mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^{n'}, \rho').$$

Proof. Let $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_{q^m}^n$ and $\boldsymbol{x}', \boldsymbol{y}' \in \mathbb{F}_{q^m}^{n'}$. The concatenated vectors $(\boldsymbol{x}|\boldsymbol{x}')$ and $(\boldsymbol{y}|\boldsymbol{y}')$ belong to $\mathbb{F}_{q^m}^{n+n'}$. Then the sum-rank distance between these concatenated vectors satisfies the following inequality:

$$\mathrm{d}_{SR,\ell}((\boldsymbol{x}|\boldsymbol{x}'),(\boldsymbol{y}|\boldsymbol{y}')) \leq \mathrm{d}_{SR,\ell}(\boldsymbol{x},\boldsymbol{y}) + \mathrm{d}_{SR,\ell}(\boldsymbol{x}',\boldsymbol{y}'). \tag{5.14}$$

Now, consider codes $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ and $\mathcal{C}' \subset \mathbb{F}_{q^m}^{n'}$ with covering radii ρ and ρ', respectively. Then for any vector $(\boldsymbol{v}|\boldsymbol{v}') \in \mathbb{F}_{q^m}^{n+n'}$ there exist codewords $(\boldsymbol{c}|\boldsymbol{c}') \in \mathcal{C} \oplus \mathcal{C}'$ with $\boldsymbol{c} \in \mathcal{C}$ and $\boldsymbol{c}' \in \mathcal{C}'$ such that $\mathrm{d}_{SR,\ell}(\boldsymbol{c},\boldsymbol{v}) \leq \rho$ and $\mathrm{d}_{SR,\ell}(\boldsymbol{c}',\boldsymbol{v}') \leq \rho'$. By applying inequality (5.14) we obtain

$$\mathrm{d}_{SR,\ell}((\boldsymbol{c}|\boldsymbol{c}'),(\boldsymbol{v}|\boldsymbol{v}')) \leq \rho + \rho'.$$

Since for any two linear subspaces $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ and $\mathcal{C}' \subset \mathbb{F}_{q^m}^{n'}$ it holds for their cardinality that

$$|\mathcal{C}| \cdot |\mathcal{C}'| = |\mathcal{C} \oplus \mathcal{C}'|,$$

the claim follows. □

5.2.3. Numerical Comparison of the Upper and Lower Bounds

To conclude this section, we provide a detailed numerical interpretation of the covering bounds given in Section 5.2.1 and Section 5.2.2. In order to compute these bounds, we rely on the formulas for the volume of sum-rank balls given in Section 4.2.1 and on bounds on this volume given in Section 4.2.2. A major limitation in earlier work was the inability to evaluate the bound from Theorem 5.25 involving the intersection of two balls, since no general method to compute such intersection volumes was available. This gap has recently been addressed in [OLWZ23] (see Section 4.2.3), which provides the required intersection formulas. With this tool at hand, we are now able to compare our bounds including the one that depends on ball intersections. However, this computation is currently feasible only for small parameter choices due to its complexity. Figure 5.5 plots the minimum rate of sum-rank-metric codes as a function of their relative covering radius $\frac{\rho}{n}$, using the parameter setting $q = 2$ and $m = \eta = \ell = 32$. As the covering radius ρ increases (and consequently the relative covering radius $\frac{\rho}{n}$), fewer codewords are required to fully cover the ambient space with spheres of radius ρ. Thus, the minimum achievable rate decreases with increasing covering radius.

Behavior of the Lower Bounds

The red curve corresponds to the lower bound (Sphere-Covering Bound) established in Theorem 5.22, which provides a fundamental limit on the minimum number of codewords needed to ensure full coverage. Its simplified version from Theorem 5.23 is computationally easier to evaluate and is visualized by the orange curve. The difference between the two lower bounds is minimal across the whole range, with the simplified bound closely approximating the exact bound, though the red curve remains slightly tighter accross most of the range.

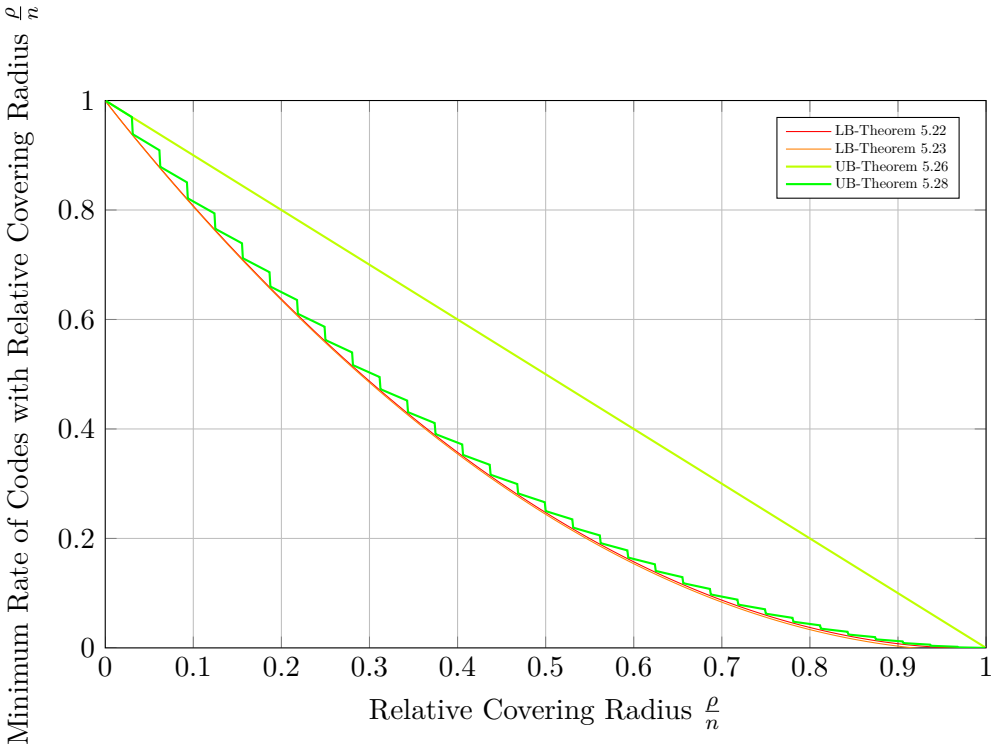


Figure 5.5.: Covering Bounds with $q = 2$, $m = 32$, $\eta = 32$, $\ell = 32$.

Behavior of the Upper Bounds

Two upper bounds are used to cap the achievable rate from above. The non-trivial upper bound (Theorem 5.28), shown as the green staircase curve, incorporates a floor function that leads to its stepped shape. This bound is more refined than the trivial upper bound and provides a sharper rate estimate across the range. In contrast, the lime green straight line represents the trivial upper bound from Theorem 5.26. This bound decreases linearly with $\frac{\rho}{n}$ and serves as a pessimistic but simple estimate. While easy to compute, it significantly overestimates the code rate for a given covering radius, especially in the mid-range of $\frac{\rho}{n}$ compared to the tighter bound provided by Theorem 5.28. Nevertheless, its inclusion is valuable as a worst-case upper limit and as a theoretical reference despite not accounting for dependencies on the number of blocks ℓ.

Tightness and Practical Implications

Most notably, the gap between the green upper bound and the red and orange lower bounds remains small across the full range of relative covering radii. This close alignment indicates that the bounds are tight and that practical code constructions can potentially achieve rates close to the theoretical limits.

6

Conclusion

This thesis has explored structural and performance-related aspects of error-correcting codes beyond the classical setting of codes over finite fields in the Hamming metric, with a particular emphasis on codes over rings and on codes in the sum-rank metric. The presented results broaden the theoretical foundations of coding theory while also being of practical relevance in the design of efficient and robust codes.

In Chapter 3, we have investigated dual-containing codes over finite commutative Frobenius rings within the framework of skew polynomial rings. We constructed cyclic left module codes of the form $\mathcal{C} = Rg/Rf \subset R/Rf$ with $f = hg = g\hbar$. A key step in our approach was to derive conditions for dual containment and parity-check construction by reducing the structural constraints which are differential equations on the generator g and its cofactor $\hbar$ to systems of multivariate polynomial equations over a smaller subring B. This reformulation enabled the application of Gröbner basis methods, allowing us to algorithmically identify all dual-containing codes with prescribed parameters and to test their structural properties. Our results demonstrate several important phenomena. First, the dual of a cyclic left module code is not necessarily a cyclic left module code, a fact confirmed by an explicit algorithmic test. Second, non-trivial endomorphisms and derivations play an essential role, as certain dual-containing codes can only be obtained in their presence. Third, we illustrate the interest of non-central modulus polynomials f, i.e., the factorizations $f = hg$ and $f = g\hbar$ yield distinct cofactors. As an example, we give a generating polynomial g of a $[6, 4]$ dual-containing code for which all eight degree-6 polynomials $f = hg = g\hbar$ are non-central. Beyond their intrinsic structural interest, these results have practical significance for the construction of quantum error-correcting codes, where dual containment is a fundamental requirement. The Gröbner basis approach provides a tool for exploring dual-containing codes over finite rings, though it remains computationally constrained by the complexity of Gröbner basis computations. Nevertheless, by applying the method to small commutative rings of order four and to the Galois ring $\mathrm{GR}(4, 2)$, we were able to produce explicit examples that illustrate the diversity and potential of such codes. A natural direction for future work is to accelerate the Gröbner basis approach so that it can handle significantly larger parameters. This would not only broaden the range of practically computable examples but also enable the discovery of new families of dual-containing codes and may reveal new structural properties and phenomena that remain hidden at small parameter sizes.

In Chapter 4, we introduced the concept of elementary linear subspaces, adapting and extending established results from the rank metric to the sum-rank metric. This framework serves as an effective analytical tool for investigating structural properties of the metric. Building on these foundations, we examined the geometry of spheres and balls in the sum-rank metric, analyzing their volumes and establishing tight upper and lower bounds that enable more efficient computation. Motivated by the study of covering properties of sum-rank-metric codes, we further analyzed the volume of the intersection of two balls with radii δ and δ' whose centers are separated by a sum-rank distance δ. We derived a general expression for this volume, identified two special cases in which it can be computed efficiently and derived closed-form formulas for these scenarios. A promising direction for future research is the development of fast computable upper and lower bounds for the volume of this intersection in general, which would further advance the study of covering properties and related coding-theoretic questions. Another natural direction of investigation for the future is the derivation of an efficient algorithm, similar to the one for computing ball sizes in [PRR22], for evaluating the volume of ball intersections.

In Chapter 5, we investigated fundamental properties of codes in the sum-rank metric, focusing on their cardinality bounds and covering properties. Building upon the geometric foundations established in Chapter 4, we revisited sum-rank analogues of classical cardinality bounds such as the sphere-packing (SP) and Gilbert–Varshamov (GV) bound for linear codes. A central aspect of this analysis was the connection to an algorithm for computing sum-rank sphere sizes introduced in [PRR22], which makes the evaluation of these bounds feasible in polynomial time. Since the exact computation of ball sizes can be prohibitively expensive, we further developed simplified bounds by incorporating lower and upper estimates of the sum-rank ball volume. These approximations not only allow for faster computation but also lead to asymptotic variants of these bounds. In contrast to earlier work such as [BGLR21], which primarily addressed the case of bounded block sizes, our results cover scenarios with growing block sizes and thus broaden the scope of asymptotic analysis. Moreover, we established that random linear codes achieving the GV-like bound in the sum-rank metric, much like in the Hamming and rank metric, are the generic case. Finally, we examined the Singleton bound in the sum-rank metric setting, identifying structural criteria for codes to achieve it with equality. Codes satisfying these conditions, termed maximum sum-rank distance (MSRD) codes, generalize MDS and MRD codes. Linearized Reed–Solomon (LRS) codes provide a prominent example, though their parameters are restricted by $\ell < q$ and $\eta \leq m$. To highlight the abundance of MSRD codes, we derived probabilistic lower bounds showing that, as the extension degree of the underlying field grows, random linear codes achieve the MSRD property with high probability. In addition to cardinality bounds, we also analyzed covering properties of codes in the sum-rank metric. The covering problem, which asks for the minimum number of metric balls of a fixed radius required to cover the entire ambient space, is fundamental to evaluating the efficiency of codes in both theory and applications. We established relationships between the covering radius in the sum-rank, Hamming, and rank metrics. Building on this, we provided lower and upper bounds on

the minimum code size required for a given covering radius. The trivial upper bound offers a simple worst-case estimate, while the refined non-trivial bound incorporates block structure and provides a much sharper characterization. On the other side, our lower bounds guarantee that any code covering the space must have at least a certain size, thereby constraining the achievable trade-offs between redundancy and error-correcting capability. Importantly, our results show that the gap between the best known lower and upper bounds remains small across a wide parameter range, highlighting the tightness of our bounds. Hence, efficient code constructions can in practice operate close to these theoretical limits. From an applied perspective, the covering radius serves as a measure of the worst-case error correctable by a code. The investigations of cardinality bounds and covering properties contribute to a more comprehensive picture of the fundamental trade-offs between low redundancy and strong error-correcting capability in sum-rank-metric codes. Beyond their theoretical significance, these insights have practical relevance for the design of codes in the sum-rank metric, and pave the way for the study of explicit constructions and decoding algorithms that achieve or approximate these bounds. One promising avenue for future research is the construction of explicit families of codes in the sum-rank metric that approach the established cardinality and covering bounds while allowing for efficient decoding algorithms. Another important direction lies in the refinement of covering results, in particular through the derivation of asymptotic bounds.

A

List of Symbols and Acronyms

Algebraic Notations

$\mathbb{N}_0$	Set of all positive integers including 0
$\mathbb{N}^*$	Set of all positive integers except 0
$\mathbb{F}_q$	Finite field with q elements (q prime power)
$\mathbb{F}_{q^m}$	Finite extension field with q^m elements (q prime power, m $\in \mathbb{N}$)
$\mathbb{Z}_m$	Ring of integers modulo m
$\mathrm{ext}_{\mathcal{B}}(\cdot)$	Mapping $\mathbb{F}_{q^m}^n \to \mathbb{F}_q^{m\times n}$ w.r.t. the $\mathbb{F}_q$-basis $\mathcal{B}$ of $\mathbb{F}_{q^m}$
$A[X]$	Ring of polynomials in one indeterminate X with coefficients in A
$A[X]/(f)$	Quotient ring of $A[X]$ modulo the ideal generated by $f \in A[X]$
$R = A[X;\theta,\delta]$	Skew polynomial ring over A with indeterminate X, endomorphism θ and derivation δ
$\langle \boldsymbol{x} \rangle_{\mathrm{row}}$	Row space of $\boldsymbol{X} \coloneqq \mathrm{ext}_{\mathcal{B}}(\boldsymbol{x})$ with a basis $\mathcal{B}$
$\langle \boldsymbol{x} \rangle_{\mathrm{col}}$	Column space of $\boldsymbol{X} \coloneqq \mathrm{ext}_{\mathcal{B}}(\boldsymbol{x})$ with a basis $\mathcal{B}$
$\mathrm{NM}_q(n,m,t)$	Number of $m \times n$ matrices over $\mathbb{F}_q$ of rank t
$\begin{bmatrix} n \\ t \end{bmatrix}_q$	q-binomial coefficient
γ_q	$\prod_{i=1}^{\infty}(1-q^{-i})^{-1}$
$\mathfrak{K}_\delta(x,n)$	Generalized q-Krawtchouk polynomial
$\mathcal{E}_k(\mathbb{F}_{q^m}^n)$	Set of all elementary linear subspaces of $\mathbb{F}_{q^m}^n$ of dimension k
$\boldsymbol{v}^{(\mathcal{V})}$	The projection of $\boldsymbol{v} \in \mathcal{W}$ on $\mathcal{V} \subset \mathcal{W}$ along $\bar{\mathcal{V}}$, where $\mathcal{V} \oplus \bar{\mathcal{V}} = \mathcal{W}$
$\mathcal{A}_{\ell,t}$	Set of block matrices given $n,\eta,\ell,t \in \mathbb{N}$ with $t \le n = \eta \cdot \ell$: $\left\{ \boldsymbol{A} = \bigoplus_{i=1}^{\ell} \boldsymbol{A}_i \in \mathbb{F}_q^{t\times n} \mid \boldsymbol{A}_i \in \mathbb{F}_q^{t_i\times\eta}, \mathrm{rk}(\boldsymbol{A}_i) = t_i, \sum_{i=0}^{\ell} t_i = t \right\}$
$\mathcal{U}_{\ell,t}$	Set of block matrices given $n,\eta,\ell,t \in \mathbb{N}$ with $t \le n = \eta \cdot \ell$: $\left\{ \boldsymbol{U} = \bigoplus_{i=1}^{\ell} \boldsymbol{U}_i \in \mathcal{A}_{\ell,t} \mid \boldsymbol{U}_i \text{ upper triangular matrix} \right\}$
$\ker_L(\cdot)$	Left kernel
$\ker_R(\cdot)$	Right kernel

Codes

$\mathcal{C}$	Code
n	Code length
k	Dimension of a linear code
d	Minimum distance (w.r.t.) a given metric
R	Code rate $\frac{k}{n}$
$[n,k,d]$-code $\mathcal{C}$	(Ring-)linear code $\mathcal{C}$ of length n, dimension k, and minimum distance d
$\mathcal{C}^{\perp}$	Euclidean dual code
$\mathcal{C}^{\perp_\sigma}$	σ-Hermitian dual code
$\mathrm{d}(\cdot)$	Metric (or distance) on a given set
$\mathrm{wt}(\cdot)$	Norm (or weight) which maps each vector of a given vector space to a postive integer

Sum-Rank Metric (Codes)

Most of the following notations depend on the number of blocks, represented as ℓ. When we substitute ℓ with 1, we are referring to the rank metric, and when ℓ equals n, we are dealing with the Hamming metric. Also, the majority of the notations are contingent on the associated vector space, denoted by the subscript $\mathcal{W}$. If there is no subscript, we are dealing with $\mathcal{W} = \mathbb{F}_{q^m}^n$ by default.

ℓ	Number of blocks of a vector $\boldsymbol{x} = [\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{\ell-1}] \in \mathbb{F}_{q^m}^n$
η	Size of a block $\boldsymbol{x}_i$ of a vector $\boldsymbol{x} = [\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{\ell-1}] \in \mathbb{F}_{q^m}^n$
μ	$\min\{m, \eta\}$
ν	$\max\{m, \eta\}$
$\mathrm{d}_{SR,\ell}(\cdot)$	Sum-rank metric (or distance) with ℓ blocks
$\mathrm{wt}_{SR,\ell}(\cdot)$	Sum-rank norm (or sum-rank weight) with ℓ blocks
$\rho_{SR,\ell}$	Covering radius of a sum-rank-metric code with ℓ blocks
$\mathcal{K}_{SR,\ell}(\mathcal{V}, \rho)$	Minimum cardinality of a code over $\mathcal{V}$ in the sum-rank metric with covering radius ρ
$\mathcal{T}_{t,\ell,\mu}$	Set of ordered partitions of t into ℓ terms of size $\leq \mu$
$\mathcal{T}_{t,\ell,\boldsymbol{\mu}}$	Set of ordered partitions of t into ℓ terms $t_i \leq \mu_i$ $\forall i \in \{0, \ldots, \ell-1\}$
$\mathcal{S}_\ell(\boldsymbol{x}, \delta)_{\mathcal{W}}$	Sum-rank-metric sphere in $\mathcal{W}$ of radius δ and center $\boldsymbol{x}$
$\mathcal{B}_\ell(\boldsymbol{x}, \delta)_{\mathcal{W}}$	Sum-rank-metric ball in $\mathcal{W}$ of radius δ and center $\boldsymbol{x}$
$\mathrm{Vol}_{\mathcal{S}_\ell}(\delta)_{\mathcal{W}}$	Volume of a sum-rank-metric sphere in $\mathcal{W}$ of radius δ
$\mathrm{Vol}_{\mathcal{B}_\ell}(\delta)_{\mathcal{W}}$	Volume of a sum-rank-metric ball in $\mathcal{W}$ of radius δ
$\mathcal{I}_\ell(\boldsymbol{x}_1, \delta_1, \boldsymbol{x}_2, \delta_2)_{\mathcal{W}}$	Intersection of two sum-rank-metric balls $\mathcal{B}_\ell(\boldsymbol{x}_1, \delta_1) \cap \mathcal{B}_\ell(\boldsymbol{x}_2, \delta_2)$ in $\mathcal{W}$
$\mathrm{Vol}_{\mathcal{I}_\ell}(\delta_1, \delta_2, \tau)_{\mathcal{W}}$	Volume of the intersection of two sum-rank-metric balls in $\mathcal{W}$ of radii δ_1, δ_2 with distance τ between their respective centers

Further Notations

$\Pr(\cdot)$	Probability measure which maps each element of a given σ-algebra into the interval $[0, 1]$
$f \in \omega(g)$	f grows faster than g
$f \in \Omega(g)$	f grows at least as fast as g
$f \in \mathcal{O}(g)$	f is asymptotically upper bounded by g
$f \in \mathcal{O}^{\sim}(g)$	As $\mathcal{O}(g)$, but ignoring logarithmic factors in the input parameter

Acronyms

GRS	**G**eneralized **R**eed–**S**olomon
MDS	**M**aximum **D**istance **S**eparable
MRD	**M**aximum **R**ank **D**istance
MSRD	**M**aximum **S**um-**R**ank **D**istance
SP	**S**phere **P**acking
GV	**G**ilbert–**V**arshamov
LRS	**L**inearized **R**eed–**S**olomon

Bibliography

References

[AM63] EF Assmus Jr and Harold F Mattson. Error-Correcting Codes: An Axiomatic Approach. *Information and Control*, 6(4):315–330, 1963.

[AL22] William W Adams and Philippe Loustaunau. *An Introduction to Gröbner bases*, volume 3. American Mathematical Society, 2022.

[AMPN20] Paulo Almeida, Umberto Martínez-Peñas, and Diego Napp. Systematic Maximum Sum Rank Codes. *Finite Fields and Their Applications*, 65:101677, 2020.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma Algebra System I: The User Language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997.

[BD18] Mhammed Boulagouaz and Abdulaziz Deajim. Characterizations and properties of principal (f, σ, δ)-codes over rings. *arXiv preprint arXiv:1809.10409*, 2018.

[BD21] Mhammed Boulagouaz and Abdulaziz Deajim. Matrix-Product Codes over Commutative Rings and Constructions Arising from (σ,δ)-Codes. *Journal of Mathematics*, 2021:1–10, 2021.

[Ber80] Elwyn R Berlekamp. The Technology of Error-Correcting Codes. *Proceedings of the IEEE*, 68(5):564–593, 1980.

[BGLR21] Eimear Byrne, Heide Gluesing-Luerssen, and Alberto Ravagnani. Fundamental Properties of Sum-Rank-Metric Codes. *IEEE Transactions on Information Theory*, 67(10):6456–6475, 2021.

[BGP14] Daniele Bartoli, Massimo Giulietti, and Irene Platoni. On the Covering Radius of MDS Codes. *IEEE Transactions on Information Theory*, 61(2):801–811, 2014.

[BGU07] Delphine Boucher, Willi Geiselmann, and Félix Ulmer. Skew-Cyclic Codes. *Applicable Algebra in Engineering, Communication and Computing*, 18:379–389, 2007.

[BHL22] Hannes Bartz, Lukas Holzbaur, Hedongliang Liu, Sven Puchinger, Julian Renner, Antonia Wachter-Zeh. Rank-Metric Codes and Their Applications. *Foundations and Trends® in Communications and Information Theory*, 19(3):390–546, 2022.

[BJPR21] Hannes Bartz, Thomas Jerkovits, Sven Puchinger, and Johan Rosenkilde. Fast Decoding of Codes in the Rank, Subspace, and Sum-Rank Metric. *IEEE Transactions on Information Theory*, 67(8):5026–5050, 2021.

[Bla72] Ian F Blake. Codes over Certain Rings. *Information and Control*, 20(4):396–404, 1972.

[Bos13] Martin Bossert. *Kanalcodierung*. Oldenbourg Wissenschaftsverlag Verlag, 2013.

[BR20] Eimear Byrne and Alberto Ravagnani. Partition-Balanced Families of Codes and Asymptotic Enumeration in Coding Theory. *Journal of Combinatorial Theory, Series A*, 171:105169, 2020.

[BSU08] Delphine Boucher, Patrick Solé, and Felix Ulmer. Skew Constacyclic Codes over Galois Rings. *Advances in Mathematics of Communications*, 2(3):273–292, 2008.

[BU09a] Delphine Boucher and Felix Ulmer. Codes as Modules over Skew Polynomial Rings. In *Cryptography and Coding: 12th IMA International Conference, Cryptography and Coding, Cirencester, UK, December 15-17, 2009. Proceedings 12*, pages 38–55. Springer, 2009.

[BU09b] Delphine Boucher and Felix Ulmer. Coding with Skew Polynomial Rings. *Journal of Symbolic Computation*, 44(12):1644–1656, 2009.

[BU11] Delphine Boucher and Felix Ulmer. A Note on the Dual Codes of Module Skew Codes. In *IMA International Conference on Cryptography and Coding*, pages 230–243. Springer, 2011.

[BU14] Delphine Boucher and Felix Ulmer. Linear Codes Using Skew Polynomials with Automorphisms and Derivations. *Designs, Codes and Cryptography*, 70:405–431, 2014.

[CHLL97] Gérard Cohen, Iiro Honkala, Simon Litsyn, and Antoine Lobstein. *Covering Codes*, volume 54. Elsevier, 1997.

[CKMS85] Gérard Cohen, Mark Karpovsky, H Mattson, and James Schatz. Covering Radius—Survey and Recent Results. *IEEE Transactions on Information Theory*, 31(3):328–343, 1985.

[Del76] Philippe Delsarte. Properties and Applications of the Recurrence $F(i+1, k+1, n+1) = q^{k+1}F(i, k+1, n) - q^kF(i, k, n)$. *SIAM Journal on Applied Mathematics*, 31(2):262–270, 1976.

[Del78] Philippe Delsarte. Bilinear Forms over a Finite Field with Applications to Coding Theory. *Journal of Combinatorial Theory, Series A*, 25(3):226–241, 1978.

[DS01] Steven T Dougherty and Keisuke Shiromoto. Maximum Distance Codes over Rings of Order 4. *IEEE Transactions on Information Theory*, 47(1):400–404, 2001.

[Gab85] Ernst M Gabidulin. Theory of Codes with Maximum Rank Distance. *Problems of Information Transmission*, 21(1):3–16, 1985.

[GBL00] Ernst M Gabidulin, Martin Bossert, and Paul Lusina. Space-Time Codes Based on Rank Codes. In *2000 IEEE International Symposium on Information Theory (Cat. No. 00CH37060)*, page 284. IEEE, 2000.

[Gil52] E. N. Gilbert. A Comparison of Signalling Alphabets. *The Bell System Technical Journal*, 31(3):504–522, 1952.

[Gol49] Marcel JE Golay. Notes on Digital Coding. *Proc. IEEE*, 37:657, 1949.

[GPB10] Ernst M Gabidulin, Nina I Pilipchuk, and Martin Bossert. Decoding of Random Network Codes. *Problems of Information Transmission*, 46(4):300–320, 2010.

[GY06] Maximilien Gadouleau and Zhiyuan Yan. Genp1-1: Properties of Codes with the Rank Metric. In *IEEE Globecom 2006*, pages 1–5. IEEE, 2006.

[GY08a] Maximilien Gadouleau and Zhiyuan Yan. On the Decoder Error Probability of Bounded Rank-Distance Decoders for Maximum Rank Distance Codes. *IEEE Transactions on Information Theory*, 54(7):3202–3206, 2008.

[GY08b] Maximilien Gadouleau and Zhiyuan Yan. Packing and Covering Properties of Rank Metric Codes. *IEEE Transactions on Information Theory*, 54(9):3873–3883, 2008.

[GY09] Maximilien Gadouleau and Zhiyuan Yan. Bounds on Covering Codes with the Rank Metric. *IEEE Communications Letters*, 13(9):691–693, 2009.

[Ham50] Richard W Hamming. Error Detecting and Error Correcting Codes. *Bell Labs Technical Journal*, 29(2):147–160, 1950.

[HB24] Felicitas Hörmann and Hannes Bartz. Interpolation-Based Decoding of Folded Variants of Linearized and Skew Reed–Solomon Codes. *Designs, Codes and Cryptography*, 92(3):553–586, 2024.

[HBP22] Felicitas Hörmann, Hannes Bartz, and Sven Puchinger. Error-erasure Decoding of Linearized Reed-Solomon Codes in the Sum-Rank Metric. In *2022 IEEE International Symposium on Information Theory (ISIT)*, pages 7–12. IEEE, 2022.

[HKC94] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Solé. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and Related Codes. *IEEE Transactions on Information Theory*, 40(2):301–319, 1994.

[Hua45] Loo-Keng Hua. Geometries of Matrices. I. Generalizations of von Staudt's Theorem. *Transactions of the American Mathematical Society*, 57(3):441–481, 1945.

[Hua51] Loo-Keng Hua. A Theorem on Matrices over a Field and its Applications. *Acta Mathematica Sinica*, 1(2):109–163, 1951.

[Huf05] W Cary Huffman. On the Classification and Enumeration of Self-Dual Codes. *Finite Fields and Their Applications*, 11(3):451–490, 2005.

[JBWZ24] Thomas Jerkovits, Hannes Bartz, and Antonia Wachter-Zeh. Support-Guessing Decoding Algorithms in the Sum-Rank Metric. *arXiv preprint arXiv:2410.15806*, 2024.

[Jos58] Durga Datt Joshi. A Note on Upper Bounds for Minimum Distance Codes. *Information and Control*, 1(3):289–295, 1958.

[KK08] Ralf Koetter and Frank R Kschischang. Coding for Errors and Erasures in Random Network Coding. *IEEE Transactions on Information theory*, 54(8):3579–3591, 2008.

[Kom53] Yasuo Komamiya. Application of Logical Mathematics to Information Theory. *Proc. 3rd Japan. Nat. Cong. Appl. Math*, 437(3), 1953.

[LGB03] Paul Lusina, Ernst Gabidulin, and Martin Bossert. Maximum Rank Distance Codes as Space-Time Codes. *IEEE Transactions on Information Theory*, 49(10):2757–2760, 2003.

[LK05] Hsiao-feng Lu and P Vijay Kumar. A Unified Construction of Space-Time Codes with Optimal Rate-Diversity Tradeoff. *IEEE Transactions on Information Theory*, 51(5):1709–1730, 2005.

[Loi08] Pierre Loidreau. Properties of Codes in Rank Metric. In *11th International Workshop on Algebraic and Combinatorial Coding Theory*, pages 192–198, 2008.

[LS01] San Ling and Patrick Solé. Type II Codes over $\mathbb{F}_4 + u\mathbb{F}_4$. *European Journal of Combinatorics*, 22(7):983–997, 2001.

[MMO04] Theresa Migler, Kent E Morrison, and Mitchell Ogle. Weight and Rank of Matrices over Finite Fields. *arXiv preprint math/0403314*, 2004.

[MP18] Umberto Martínez-Peñas. Skew and Linearized Reed–Solomon Codes and Maximum Sum-Rank Distance Codes over any Division Ring. *Journal of Algebra*, 504:587–612, 2018.

[MPK19a] Umberto Martínez-Peñas and Frank R Kschischang. Reliable and Secure Multishot Network Coding Using Linearized Reed-Solomon Codes. *IEEE Transactions on Information Theory*, 2019.

[MPK19b] Umberto Martínez-Peñas and Frank R Kschischang. Universal and Dynamic Locally Repairable Codes with Maximal Recoverability via Sum-Rank Codes. *IEEE Transactions on Information Theory*, 2019.

[MPSK22] Umberto Martínez-Peñas, Mohannad Shehadeh, Frank R Kschischang Codes in the Sum-Rank Metric: Fundamentals and Applications. *Foundations and Trends® in Communications and Information Theory*, 19(5):814–1031, 2022.

[MS77] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The Theory of Error Correcting Codes*. Elsevier, 1977.

[NHTRR18] Alessandro Neri, Anna-Lena Horlemann-Trautmann, Tovohery Randrianarisoa, and Joachim Rosenthal. On the Genericity of Maximum Rank Distance and Gabidulin Codes. *Designs, Codes and Cryptography*, 86(2):341–363, 2018.

[NPRV] Diego Napp, Raquel Pinto, Joachim Rosenthal, and Paolo Vettori. Faster Decoding of Rank Metric Convolutional Codes, 2018

[NPRV17] Diego Napp, Raquel Pinto, Joachim Rosenthal, and Paolo Vettori. MRD Rank Metric Convolutional Codes. In *2017 IEEE International Symposium on Information Theory (ISIT)*, pages 2766–2770. IEEE, 2017.

[NUF10] Roberto W. Nóbrega and Bartolomeu F. Uchôa-Filho. Multishot Codes for Network Coding Using Rank-Metric Codes. In *2010 Third IEEE International Workshop on Wireless Network Coding*, pages 1–6, 2010. doi:10.1109/WINC.2010.5507933.

[Ore33] Oystein Ore. Theory of Non-Commutative Polynomials. *Annals of mathematics*, pages 480–508, 1933.

[PRR22] Sven Puchinger, Julian Renner, and Johan Rosenkilde. Generic Decoding in the Sum-Rank Metric. *IEEE Transactions on Information Theory*, 68(8):5075–5097, 2022.

[PSBF16] Sven Puchinger, Sebastian Stern, Martin Bossert, and Robert FH Fischer. Space-Time Codes Based on Rank-Metric Codes and Their Decoding. In *2016 International Symposium on Wireless Communication Systems (ISWCS)*, pages 125–130. IEEE, 2016.

[Rat08] Joel Ratsaby. Estimate of the Number of Restricted Integer-Partitions. *Applicable Analysis and Discrete Mathematics*, pages 222–233, 2008.

[RB19] Alberto Ravagnani and Eimear Byrne. On the Sparsity of MRD Codes. In *11th International Workshop on Coding and Cryptography-WCC 2019*.

[Rot91] Ron M Roth. Maximum-Rank Array Codes and Their Application to Crisscross Error Correction. *IEEE Transactions on Information Theory*, 37(2):328–336, 1991.

[Rot06] Ron M. Roth. *Introduction to Coding Theory*. Cambridge University Press, 2006.

[SB18] Amit Sharma and Maheshanand Bhaintwal. A Class of Skew-Cyclic Codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ with Derivation. *Advances in Mathematics of Communications*, 12(4), 2018.

[Sha48] Claude Elwood Shannon. A Mathematical Theory of Communication. *Bell System Technical Journal*, 27(3):379–423, 1948.

[Sin64] Richard Singleton. Maximum Distance q-nary Codes. *IEEE Transactions on Information Theory*, 10(2):116–118, 1964.

[SK20] Mohannad Shehadeh and Frank R Kschischang. Rate-Diversity Optimal Multiblock Space-Time Codes via Sum-Rank Codes. In *2020 IEEE International Symposium on Information Theory (ISIT)*, pages 3055–3060. IEEE, 2020.

[SKK08] Danilo Silva, Frank R Kschischang, and Ralf Koetter. A Rank-Metric Approach to Error Control in Random Network Coding. *IEEE Transactions on Information Theory*, 54(9):3951–3967, 2008.

[SRV12] Natalia Silberstein, Ankit Singh Rawat, and Sriram 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.

[SW17] Steve Szabo and Jay A Wood. Properties of Dual Codes Defined by Nondegenerate Forms. *Journal of Algebra Combinatorics Discrete Structures and Applications*, pages 105–113, 2017.

[Var57] Rom Rubenovich Varshamov. Estimate of the Number of Signals in Error Correcting Codes. *Docklady Akad. Nauk, SSSR*, 117:739–741, 1957.

[WSBZ11] Antonia Wachter, Vladimir R Sidorenko, Martin Bossert, and Victor V Zyablov. On (partial) Unit Memory Codes Based on Gabidulin codes. *Problems of Information Transmission*, 47(2):117–129, 2011.

[WZSS15] Antonia Wachter-Zeh, Markus Stinner, and Vladimir Sidorenko. Convolutional Codes in Rank Metric with Application to Random Network coding. *IEEE Transactions on Information Theory*, 61(6):3199–3213, 2015.

Publications Containing Parts of this Thesis

[LOU25] Hedongliang Liu, Cornelia Ott, and Felix Ulmer. A Gröbner Approach to Dual-Containing Cyclic Left Module (θ, δ)-codes over Finite Commutative Frobenius Rings. *Advances in Mathematics of Communications*, vol. 19, no. 6, pp. 1723–1741, 2025.

[OLWZ22] Cornelia Ott, Hedongliang Liu, and Antonia Wachter-Zeh. Covering properties of sum-rank metric codes. In *2022 58th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1–7. IEEE, 2022.

[OLWZ23] Cornelia Ott, Hedongliang Liu, and Antonia Wachter-Zeh. Geometrical Properties of Balls in Sum-Rank Metric. In *WSA & SCC 2023; 26th International ITG Workshop on Smart Antennas and 13th Conference on Systems, Communications, and Coding*, pages 1–6. VDE, 2023.

[OPB21] Cornelia Ott, Sven Puchinger, and Martin Bossert. Bounds and genericity of sum-rank-metric codes. In *2021 XVII International Symposium" Problems of Redundancy in Information and Control Systems"(REDUNDANCY)*, pages 119–124. IEEE, 2021.

Other Publications by the Author of this Thesis

[SLOF25] Sebastian Stern, Cong Ling, Cornelia Ott, and Robert FH Fischer. Quaternionic minkowski reduction and its application in dual-polarized mimo systems. In *2025 14th International ITG Conference on Systems, Communications and Coding (SCC)*, pages 1–6. IEEE, 2025.

[SOPB19] Carmen Sippel, Cornelia Ott, Sven Puchinger, and Martin Bossert. Reed–Solomon Codes over Fields of Characteristic Zero. In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 1537–1541. IEEE, 2019.