# Codes in the Sum-Rank Metric: Fundamentals and Applications

**Other titles in Foundations and Trends® in Communications and Information Theory**

*Cache Optimization Models and Algorithms*
Georgios Paschos, George Iosifidis and Giuseppe Caire
ISBN: 978-1-68083-702-5

*Lattice-Reduction-Aided and Integer-Forcing Equalization: Structures, Criteria, Factorization, and Coding*
Robert F. H. Fischer, Sebastian Stern and Johannes B. Huber
ISBN: 978-1-68083-644-8

*Group Testing: An Information Theory Perspective*
Matthew Aldridge, Oliver Johnson and Jonathan Scarlett
ISBN: 978-1-68083-596-0

*Sparse Regression Codes*
Ramji Venkataramanan, Sekhar Tatikonda and Andrew Barron
ISBN: 978-1-68083-580-9

# Codes in the Sum-Rank Metric: Fundamentals and Applications

**Umberto Martínez-Peñas**
University of Valladolid
Spain
umberto.martinez@uva.es

**Mohannad Shehadeh**
University of Toronto
Canada
mshehadeh@ece.utoronto.ca

**Frank R. Kschischang**
University of Toronto
Canada
frank@ece.utoronto.ca

now
the essence of knowledge
Boston — Delft

# Foundations and Trends® in Communications and Information Theory

*Published, sold and distributed by:*
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

*Outside North America:*
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

U. Martínez-Peñas *et al.*. *Codes in the Sum-Rank Metric: Fundamentals and Applications*. Foundations and Trends® in Communications and Information Theory, vol. 19, no. 5, pp. 813–1030, 2022.

ISBN: 978-1-63828-031-6

**Foundations and Trends® in Communications and Information Theory**
Volume 19, Issue 5, 2022

# Editorial Board

# Editorial Scope

## Topics

Foundations and Trends® in Communications and Information Theory publishes survey and tutorial articles in the following topics:

- Coded modulation
- Coding theory and practice
- Communication complexity
- Communication system design
- Cryptology and data security
- Data compression
- Data networks
- Demodulation and Equalization
- Denoising
- Detection and estimation
- Information theory and statistics
- Information theory and computer science
- Joint source/channel coding
- Modulation and signal design
- Multiuser detection
- Multiuser information theory
- Optical communication channels
- Pattern recognition and learning
- Quantization
- Quantum information processing
- Rate-distortion theory
- Shannon theory
- Signal processing for communications
- Source coding
- Storage and recording codes
- Speech and Image Compression
- Wireless Communications

## Information for Librarians

Foundations and Trends® in Communications and Information Theory, 2022, Volume 19, 4 issues. ISSN paper version 1567-2190. ISSN online version 1567-2328 . Also available as a combined paper and online subscription.

# Contents

# Codes in the Sum-Rank Metric: Fundamentals and Applications

Umberto Martínez-Peñas[1], Mohannad Shehadeh[2] and Frank R. Kschischang[2]

[1] *University of Valladolid, Spain; umberto.martinez@uva.es*
[2] *University of Toronto, Canada; mshehadeh@ece.utoronto.ca; frank@ece.utoronto.ca*

ABSTRACT

Codes in the sum-rank metric have attracted significant attention for their applications in distributed storage systems, multishot network coding, streaming over erasure channels, and multi-antenna wireless communication. This monograph provides a tutorial introduction to the theory and applications of sum-rank metric codes over finite fields. At the heart of the monograph is the construction of linearized Reed–Solomon codes, a general construction of maximum sum-rank distance (MSRD) codes with polynomial field sizes. Linearized Reed–Solomon codes specialize to classical Reed–Solomon and Gabidulin code constructions in the Hamming and rank metrics, respectively, and they admit an efficient Welch–Berlekamp decoding algorithm. Applications of these codes in distributed storage systems, network coding, and multi-antenna communication are developed. Other families of codes in the sum-rank metric, including convolutional codes and subfield subcodes are described, and recent results in the general theory of codes in the sum-rank metric are surveyed.

Umberto Martínez-Peñas, Mohannad Shehadeh and Frank R. Kschischang (2022), "Codes in the Sum-Rank Metric: Fundamentals and Applications", Foundations and Trends® in Communications and Information Theory: Vol. 19, No. 5, pp 813–1030. DOI: 10.1561/0100000120.

# 1

# Introduction to the Sum-Rank Metric and MSRD Codes

This first section provides an overview of this monograph followed by a careful introduction to the *sum-rank metric* and *maximum sum-rank distance* (MSRD) codes. We will focus on their definitions and main properties, deferring an actual construction to Section 2. However, before delving into any of this, we will preface with an *informal* introduction which aims to immediately answer the basic questions of what codes in the sum-rank metric are and why they are of both practical and theoretical interest.

### Why the Sum-Rank Metric?

The *sum-rank metric* arises in problems of communication over multiplicative-additive matrix channels involving the action of a *block diagonal* matrix. In particular, consider the scenario where Alice communicates with Bob by transmitting a matrix $X \in F^{n\times m}$ where $F$ is some field. Bob then receives $Y \in F^{s\times m}$ given by

$$\begin{aligned} Y &= AX + Z \\ &= \mathrm{Diag}(A_1, A_2, \ldots, A_\ell)X + Z \end{aligned} \tag{1.1}$$

where $Z \in F^{s\times m}$ and $A = \mathrm{Diag}(A_1, A_2, \ldots, A_\ell) \in F^{s\times n}$ is a block diagonal matrix with $A_1 \in F^{s_1\times n_1}, A_2 \in F^{s_2\times n_2}, \ldots, A_\ell \in F^{s_\ell\times n_\ell}$ (in which case we must have $s_1+s_2+\cdots+s_\ell = s$ and $n_1+n_2+\cdots+n_\ell = n$). It is convenient to partition $X$ into $X_1 \in F^{n_1\times m}, X_2 \in F^{n_2\times m}, \ldots, X_\ell \in F^{n_\ell\times m}$ and appropriately partition $Y$ and $Z$ so that (1.1) becomes

$$\begin{aligned}\begin{pmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_\ell \end{pmatrix} &= \begin{pmatrix} A_1 & 0 & \ldots & 0 \\ 0 & A_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & A_\ell \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_\ell \end{pmatrix} + \begin{pmatrix} Z_1 \\ Z_2 \\ \vdots \\ Z_\ell \end{pmatrix} \\ &= \begin{pmatrix} A_1X_1 \\ A_2X_2 \\ \vdots \\ A_\ell X_\ell \end{pmatrix} + \begin{pmatrix} Z_1 \\ Z_2 \\ \vdots \\ Z_\ell \end{pmatrix},\end{aligned} \tag{1.2}$$

which lends itself to the interpretation of being $\ell$ transmissions across a varying multiplicative-additive matrix channel. The classic coding-theoretic task is then to construct the largest possible code $\mathcal{C} \subseteq F^{n\times m}$ for Alice to signal with, while allowing Bob to reliably recover $X \in \mathcal{C}$ from a distorted observation $Y$.

We now make the first of three crucial points. This first point is that the communication scenario described by (1.1) occurs in a variety of disparate applications covered in Sections 3, 4, and 5 of this monograph:

- Section 3 considers applications to erasure coding for distributed storage. The problem of constructing information-theoretically optimal locally repairable codes can be cast as the problem of constructing a code for communication across the channel described by (1.1) with $F$ being a finite field, $A$ being a rank-deficient block diagonal matrix, and $Z$ being the zero matrix (see Proposition 3.3 or Theorem 3.4). In this application, a rank-deficient block diagonal $A$ represents the composition of local codes with erasures.
- Section 4 considers applications to network coding. Here, the problem of adversarial multishot network coding is similarly formulated as (1.1) with $F$ a finite field and $A$ a rank-deficient and block diagonal matrix. However, this time, $Z_1, Z_2, \ldots, Z_\ell$ are potentially nonzero but are of bounded rank (see Section 4.1). In

this application, the rank deficiency of $A$ represents packet losses in the network and the rank-constrained $Z_1, Z_2, \ldots, Z_\ell$ represent the action of an adversary injecting a limited number of packets into the network.

- Section 5 considers applications to multi-antenna wireless communication. The problem of communicating across a multiple-input multiple-output block-fading channel can be formulated as (1.1) with $F$ being the field of complex numbers and $A_1, A_2, \ldots, A_\ell$ and $Z$ being *random* complex Gaussian matrices.

Note that depending on the conventions of the application area, we may consider in this monograph alternative but equivalent descriptions of (1.1) or (1.2) such as transposed formulations involving right instead of left matrix multiplications. In fact, the main parts of this section will consider the transposed situation with right matrix multiplications.

We come now to the second crucial point. In all three of these applications, including the markedly different third application involving randomness and the complex field, the problem of constructing a good code $\mathcal{C} \subseteq \mathbb{F}^{n\times m}$, i.e., one which facilitates reliable recovery of $X$ from $Y$ in some sense, reduces to the problem of constructing $\mathcal{C}$ so that the minimum *sum-rank* distance is large. In particular, for any codeword pair $X, X' \in \mathcal{C}$ with $X \neq X'$, we require that the quantity

$$\mathrm{Rk}(X_1 - X_1') + \mathrm{Rk}(X_2 - X_2') + \cdots + \mathrm{Rk}(X_\ell - X_\ell'), \tag{1.3}$$

where $\mathrm{Rk}(\cdot)$ denotes the matrix rank, is large. The quantity (1.3) is termed the *sum-rank* distance between $X$ and $X'$ and will soon be shown to be a *metric* in the mathematical sense (see Proposition 1.1). Thus, we have that the sum-rank metric (1.3) arises when considering communication across channels of the form (1.1) or (1.2) whether adversarial or probabilistic and whether over finite fields or the field of complex numbers.

Apart from its role in applications, the sum-rank metric (1.3) can be seen as a generalization of the *Hamming* and *rank* metrics. The *Hamming metric* has played a major role in coding theory since Hamming's seminal work [62]. The alternative metric called the *rank metric* was later introduced independently in [41], [46], [152]. This metric has

gained considerable attention in the past decades since codes with large minimum rank distance can correct error and erasure patterns, such as those appearing in matrix-multiplicative channels [88], uncorrectable by traditional codes. See [57] for a nice survey of rank-metric codes.

For a long time, results in the rank metric were called *q-analogues* of similar results in the Hamming metric [18], [47], [56], [79]. The *sum-rank metric* (1.3) was explicitly introduced more recently in the network coding literature [136] but was used implicitly much earlier in the space–time coding literature [42], [102] (see Section 5.1 for details). As observed in [116, Ex. 36 & 37], the sum-rank metric recovers the Hamming metric and the rank metric as two extremal particular cases. This will be seen soon in Propositions 1.4 and 1.5 but the impatient reader can consider taking $m = n_1 = n_2 = \cdots = n_\ell = 1$ in which case (1.3) simply becomes the Hamming distance between $X \in F^{\ell \times 1}$ and $X' \in F^{\ell \times 1}$. On the other hand, if $\ell = 1$, then (1.3) becomes the rank of the difference between $X \in F^{n \times m}$ and $X' \in F^{n \times m}$ which is precisely the rank distance. In this sense, the sum-rank metric interpolates between the Hamming and rank metrics.

The sum-rank metric is not, however, simply a theoretical framework to provide common generalizations of results for the Hamming and rank metrics. In problem domains described in Sections 3, 4, and 5, block codes with *maximum sum-rank distance* (MSRD) arise as natural solutions. Interestingly, such codes can always be constructed as *maximum rank distance* (MRD) block codes [41], [46], [152], as will be seen soon (see Proposition 1.8 and the ensuing discussion), every MRD code is also an MSRD code. However, the alphabet size required for such MRD solutions is exponential in the code length (see 1.34), making MRD codes computationally impractical except for small parameter regimes. Additionally, the parameters of MRD codes impose further disadvantages such as constrained codeword dimensions in matrix representation which translates to long delay in space–time coding with multiple fading blocks (see Section 5).

This brings us to the third and final crucial point of this preface. The theory of sum-rank metric codes becomes interesting precisely because of the existence of MSRD block codes with sub-exponential alphabet size that overcome the disadvantages of these MRD solutions. In other

words, while the strength of the MRD property is sufficient to solve the various coding problems considered here, the introduction of non-MRD MSRD codes makes it unnecessary to pay the cost (in alphabet size) of MRD codes. We will treat a particular family of such MSRD codes called *linearized Reed–Solomon codes* in Section 2.

This monograph ends with Section 6 which considers other codes in the sum-rank metric besides the linearized Reed–Solomon codes introduced in Section 2 and applied in Sections 3, 4, and 5. These include alternative constructions and analogues to BCH codes and to convolutional codes.

**Notation:** Throughout the text, $\mathbb{N}$, $\mathbb{Z}^{>0}$, $\mathbb{Z}$, $\mathbb{R}^{\geq 0}$, $\mathbb{R}$, and $\mathbb{C}$ denote, respectively, the natural numbers (including 0), the positive integers, the integers, the nonnegative real numbers, the real numbers, and the complex numbers. A finite field with $q$ elements is denoted as $\mathbb{F}_q$. The finite field $\mathbb{F}_4$, which is often used to provide examples in the first two sections, is written concretely as

$$\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}, \text{ where } \bar{\omega} = \omega^2 = 1 + \omega. \tag{1.4}$$

For positive integers $m$ and $n$, the $n$-fold Cartesian product of a set $A$ with itself is denoted as $A^n$, and the set of matrices with $m$ rows and $n$ columns having entries from $A$ is denoted as $A^{m\times n}$. The transpose of a matrix $M \in A^{m\times n}$ is the matrix $M^{\intercal} \in A^{n\times m}$. The set $\{1, 2, \ldots, n\}$ will be denoted as $[n]$. The cardinality (the number of elements) of a finite set $A$ is denoted as $|A|$. For $x \in \mathbb{R}$, the function $\max(x, 0)$ is denoted as $(x)^+$. Further notation will be introduced as needed.

## 1.1 The Sum-Rank Metric

This initial section introduces the *sum-rank metric*. We present its definition on tuples of matrices and on vectors over an extended finite field, and we prove that it is indeed a distance function. In this monograph, we will use the words *metric* and *distance* interchangeably. For a definition, see Proposition 1.1 below.

As its name would suggest, the simplest way to define the sum-rank metric is by sums of ranks. To this end, we fix a finite field $\mathbb{F}_q$, where $q$

is a power of a prime number, often a power of 2. The ambient space for the sum-rank metric is the Cartesian-product set

$$\mathbb{F}_q^{m_1\times n_1} \times \mathbb{F}_q^{m_2\times n_2} \times \cdots \times \mathbb{F}_q^{m_\ell\times n_\ell}, \tag{1.5}$$

for positive integers $\ell$, $m_1, m_2, \ldots, m_\ell$, $n_1, n_2, \ldots, n_\ell$. The set in (1.5) therefore is the set of tuples of length $\ell$ containing an $m_i \times n_i$ matrix with entries in $\mathbb{F}_q$ at the $i$th position.

**Example 1.1.** Consider $q = 2$, $\ell = 2$, $m_1 = m_2 = 2$, $n_1 = 2$ and $n_2 = 3$. An element in the set in (1.5) for these parameters could be

$$C = (C_1, C_2) = \left( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \right).$$

The set of all such tuples is $\mathbb{F}_2^{2\times 2} \times \mathbb{F}_2^{2\times 3}$.

Observe that the set in (1.5) is a vector space over the finite field $\mathbb{F}_q$ under componentwise addition of tuples of matrices in $\mathbb{F}_q^{m_1\times n_1} \times \mathbb{F}_q^{m_2\times n_2} \times \cdots \times \mathbb{F}_q^{m_\ell\times n_\ell}$ and multiplication by arbitrary scalars in $\mathbb{F}_q$.

The sum-rank metric can be defined using *sum-rank weights*, in the same way that the Hamming metric can be defined using Hamming weights. The first explicit formal definition of this metric was given in [136] under the name *extended distance*.

**Definition 1.1 (Sum-rank metric).** The sum-rank weight is the function

$$\mathrm{wt}_{SR} : \mathbb{F}_q^{m_1\times n_1} \times \mathbb{F}_q^{m_2\times n_2} \times \cdots \times \mathbb{F}_q^{m_\ell\times n_\ell} \longrightarrow \mathbb{N}$$

given by

$$\begin{aligned} \mathrm{wt}_{SR}(C_1, C_2, \ldots, C_\ell) &= \mathrm{Rk}(C_1) + \mathrm{Rk}(C_2) + \cdots + \mathrm{Rk}(C_\ell) \\ &= \sum_{i=1}^{\ell} \mathrm{Rk}(C_i), \end{aligned}$$

where $\mathrm{Rk}(\cdot)$ returns the rank of its argument as a matrix over $\mathbb{F}_q$ and where $C_i \in \mathbb{F}_q^{m_i\times n_i}$, for $i \in [\ell]$. With such weights at hand, we may define the sum-rank metric as the function

$$\mathrm{d}_{SR} : \left(\mathbb{F}_q^{m_1\times n_1} \times \mathbb{F}_q^{m_2\times n_2} \times \cdots \times \mathbb{F}_q^{m_\ell\times n_\ell}\right)^2 \longrightarrow \mathbb{N}$$

given by

$$\mathrm{d}_{SR}(C, D) = \mathrm{wt}_{SR}(C - D),$$

for arbitrary $C, D \in \mathbb{F}_q^{m_1 \times n_1} \times \mathbb{F}_q^{m_2 \times n_2} \times \cdots \times \mathbb{F}_q^{m_\ell \times n_\ell}$.

**Example 1.2.** For the ordered pair $C = (C_1, C_2)$ of matrices in Example 1.1, we have

$$\mathrm{wt}_{SR}(C) = \mathrm{Rk}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \mathrm{Rk}\begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = 2 + 1 = 3.$$

Consider another ordered pair of matrices

$$D = (D_1, D_2) = \left(\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}\right)$$

having parameters commensurate with those of $C$. The sum-rank distance between $C$ and $D$ is

$$\mathrm{d}_{SR}(C, D) = \mathrm{Rk}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \mathrm{Rk}\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix} = 1 + 1 = 2.$$

The following proposition shows that the sum-rank metric is indeed a metric (or distance).

**Proposition 1.1.** The sum-rank metric $\mathrm{d}_{SR}$ is a metric in the set $\mathbb{F}_q^{m_1 \times n_1} \times \mathbb{F}_q^{m_2 \times n_2} \times \cdots \times \mathbb{F}_q^{m_\ell \times n_\ell}$. In other words, it satisfies the following properties, for all $C, D, E \in \mathbb{F}_q^{m_1 \times n_1} \times \mathbb{F}_q^{m_2 \times n_2} \times \cdots \times \mathbb{F}_q^{m_\ell \times n_\ell}$:

1. $\mathrm{d}_{SR}(C, D) \geq 0$, and $\mathrm{d}_{SR}(C, D) = 0$ if, and only if, $C = D$.
2. $\mathrm{d}_{SR}(C, D) = \mathrm{d}_{SR}(D, C)$.
3. $\mathrm{d}_{SR}(C, D) \leq \mathrm{d}_{SR}(C, E) + \mathrm{d}_{SR}(E, D)$.

Proposition 1.1 above follows from the fact that $\mathrm{wt}_{SR}$ is a weight. In other words, $\mathrm{wt}_{SR}$ satisfies the following properties (left to the reader to prove) for all $C, D \in \mathbb{F}_q^{m_1 \times n_1} \times \mathbb{F}_q^{m_2 \times n_2} \times \cdots \times \mathbb{F}_q^{m_\ell \times n_\ell}$:

1. $\mathrm{wt}_{SR}(C) \geq 0$, and $\mathrm{wt}_{SR}(C) = 0$ if, and only if, $C = 0$.
2. $\mathrm{wt}_{SR}(\lambda C) = \mathrm{wt}_{SR}(C)$, for all $\lambda \in \mathbb{F}_q \setminus \{0\}$.
3. $\mathrm{wt}_{SR}(C + D) \leq \mathrm{wt}_{SR}(C) + \mathrm{wt}_{SR}(D)$.

Notice that the last inequality follows from the sub-additivity of matrix rank.

A code suitable for the sum-rank metric is just a nonempty subset of the set in (1.5), and it is often called a *sum-rank code*. We may define its *minimum sum-rank distance* in the same way as with any other metric.

**Definition 1.2.** Given a code $\mathcal{C} \subseteq \mathbb{F}_q^{m_1 \times n_1} \times \mathbb{F}_q^{m_2 \times n_2} \times \cdots \times \mathbb{F}_q^{m_\ell \times n_\ell}$, we define its minimum sum-rank distance as

$$\mathrm{d}_{SR}(\mathcal{C}) = \min\{\mathrm{d}_{SR}(C, D) \mid C, D \in \mathcal{C}, C \neq D\}.$$

As for any other distance, the minimum sum-rank distance measures the sum-rank weight of additive errors that the code may correct. In other words, $\mathrm{d}_{SR}(\mathcal{C}) \geq d$ if, and only if, $\mathcal{C}$ has a decoder that can uniquely correct any additive error $E$ such that $2t + 1 \leq d$, where $t = \mathrm{wt}_{SR}(E)$. A similar statement holds for erasures. We will come back to error (and erasure) correction in Section 2.7, when we describe a Welch–Berlekamp decoder for linearized Reed–Solomon codes in the sum-rank metric. Sum-rank error correction will be of importance in Section 4.

Since the ambient space (1.5) is a vector space over $\mathbb{F}_q$, we may consider linear codes as $\mathbb{F}_q$-linear subspaces. For such codes, the minimum sum-rank distance coincides with the minimum sum-rank weight.

**Proposition 1.2.** If $\mathcal{C} \subseteq \mathbb{F}_q^{m_1 \times n_1} \times \mathbb{F}_q^{m_2 \times n_2} \times \cdots \times \mathbb{F}_q^{m_\ell \times n_\ell}$ is a linear code (over $\mathbb{F}_q$), then

$$\mathrm{d}_{SR}(\mathcal{C}) = \min\{\mathrm{wt}_{SR}(C) \mid C \in \mathcal{C}, C \neq 0\},$$

where 0 denotes the tuple formed by placing a zero matrix in each coordinate.

**Example 1.3.** Let $q = 2$, $\ell = 2$, $m_1 = m_2 = 2$, $n_1 = 2$ and $n_2 = 3$, as in Example 1.1. Consider the $\mathbb{F}_2$-linear subspace

$$\mathcal{C} = \langle C, D \rangle_{\mathbb{F}_2} \subseteq \mathbb{F}_2^{2\times 2} \times \mathbb{F}_2^{2\times 3},$$

spanned by $\{C, D\}$ where $C, D \in \mathbb{F}_2^{2\times 2} \times \mathbb{F}_2^{2\times 3}$ are as in Example 1.2. Since $\mathbb{F}_2 = \{0, 1\}$, we deduce that $\mathcal{C} = \{0, C, D, C+D\}$. Since $\mathrm{wt}_{SR}(C) = \mathrm{wt}_{SR}(D) = 3$ and $\mathrm{wt}_{SR}(C + D) = 2$, we conclude that

$$\mathrm{d}_{SR}(\mathcal{C}) = 2.$$

We turn now to a different representation of the sum-rank metric. We will consider the case where the matrices at different positions of the tuple all have $m$ rows, i.e., the case where

$$m = m_1 = m_2 = \ldots = m_\ell. \tag{1.6}$$

In this particular case, as we will elaborate upon below, we can represent tuples of matrices from the set (1.5) simply as vectors in the vector space

$$\mathbb{F}_{q^m}^n = \mathbb{F}_{q^m}^{n_1+n_2+\cdots+n_\ell}, \tag{1.7}$$

where $\mathbb{F}_{q^m}^n = \mathbb{F}_{q^m}^{1\times n}$ (the set of row vectors of length $n$ with entries in the finite field $\mathbb{F}_{q^m}$), and

$$n = n_1 + n_2 + \cdots + n_\ell. \tag{1.8}$$

In other words, each column of each matrix in the tuple is viewed as an element of the finite field $\mathbb{F}_{q^m}$. We refer to any $\ell$-tuple $\mathbf{n} = (n_1, n_2, \ldots, n_\ell)$, where $n_1, \ldots, n_\ell$ are positive integers summing to $n$, as a *length-$n$ sum-rank partition of order $\ell$*, or simply a *length partition*. Unless otherwise stated, for the remainder of this monograph we will assume that (1.6) and (1.8) hold.

In order to see tuples of matrices as vectors in $\mathbb{F}_{q^m}^n$, we need the so-called *matrix representation map*. As its name suggests, it represents an $n_i$-tuple in $\mathbb{F}_{q^m}^{n_i}$ as a matrix in $\mathbb{F}_q^{m\times n_i}$. Recall that $\mathbb{F}_{q^m}$ can be seen as an $m$-dimensional vector space over its subfield $\mathbb{F}_q$. If $\{\alpha_1, \ldots, \alpha_m\}$ is any basis for this vector space, then each element $c_1 \in \mathbb{F}_{q^m}$ can be written as $c_1 = c_{1,1}\alpha_1 + c_{2,1}\alpha_2 + \cdots + c_{m,1}\alpha_m$ for unique scalars $c_{1,1}, c_{2,1}, \ldots, c_{m,1} \in \mathbb{F}_q$. If the basis is ordered as $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m)$ then $c_1$ can be associated with a unique column vector $(c_{1,1}, \ldots, c_{m,1})^\intercal$ of coordinates. The matrix representation map extends this representation to $r$-tuples in the obvious way.

**Definition 1.3.** Fix an ordered basis $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_m) \in \mathbb{F}_{q^m}^m$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. For each positive integer $r$, define the matrix representation map $M_{\boldsymbol{\alpha}}^r : \mathbb{F}_{q^m}^r \longrightarrow \mathbb{F}_q^{m\times r}$ which takes $\mathbf{c} = (c_1, \ldots, c_r)$ to

$$M_{\boldsymbol{\alpha}}^r(\mathbf{c}) = \begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,r} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,r} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m,1} & c_{m,2} & \cdots & c_{m,r} \end{pmatrix} \in \mathbb{F}_q^{m\times r}, \tag{1.9}$$

where $c_{i,j} \in \mathbb{F}_q$, for $i \in [m]$ and $j \in [r]$ and where $\boldsymbol{\alpha} M_{\boldsymbol{\alpha}}^r(\mathbf{c}) = \sum_{i=1}^m \alpha_i (c_{i,1}, c_{i,2}, \ldots, c_{i,r}) = \mathbf{c}$.

Evidently the $j$th column of $M_{\boldsymbol{\alpha}}^r(c_1, \ldots, c_r)$ is the vector of coordinates of $c_j$ with respect to the ordered basis $\boldsymbol{\alpha}$. It is also important to observe that $M_{\boldsymbol{\alpha}}^r$ is an isomorphism of vector spaces over $\mathbb{F}_q$, that is, it is bijective and $\mathbb{F}_q$-linear.

**Example 1.4.** Consider the finite field $\mathbb{F}_q = \mathbb{F}_4$ as defined in (1.4). Then we may consider $m = 3$ and construct $\mathbb{F}_{q^m} = \mathbb{F}_{4^3}$ using the polynomial $1 + x + x^3$, which is irreducible over $\mathbb{F}_4$. An ordered basis of $\mathbb{F}_{4^3}$ over $\mathbb{F}_4$ is $\boldsymbol{\alpha} = (1, \alpha, \alpha^2)$, where $\alpha \in \mathbb{F}_{4^3}$ is such that $\alpha^3 = \alpha + 1$. Take now as an example the vector

$$\mathbf{c} = (\omega + \alpha, 1 + \bar{\omega}\alpha^2) \in \mathbb{F}_{4^3}^2.$$

Then its matrix representation is

$$M_{\boldsymbol{\alpha}}^2(\mathbf{c}) = \begin{pmatrix} \omega & 1 \\ 1 & 0 \\ 0 & \bar{\omega} \end{pmatrix} \in \mathbb{F}_4^{3\times 2},$$

and of course $\boldsymbol{\alpha} M_{\boldsymbol{\alpha}}^2(\mathbf{c}) = \mathbf{c}$.

Given a length partition $\mathbf{n} = (n_1, \ldots, n_\ell)$, the next step is to subdivide a vector in $\mathbb{F}_{q^m}^n$ into vectors in $\mathbb{F}_{q^m}^{n_i}$, for $i \in [\ell]$, and apply the matrix representation map to each of the shorter vectors.

**Definition 1.4.** Let $\mathbf{n} = (n_1, \ldots, n_\ell)$ be a length-$n$ sum-rank partition of order $\ell$. Subdivide any given vector $\mathbf{c}$ in $\mathbb{F}_{q^m}^n$ as

$$\mathbf{c} = \left(\mathbf{c}^{(1)}, \mathbf{c}^{(2)}, \ldots, \mathbf{c}^{(\ell)}\right) \in \mathbb{F}_{q^m}^n, \tag{1.10}$$

where $\mathbf{c}^{(i)} \in \mathbb{F}_{q^m}^{n_i}$, for $i \in [\ell]$. For any ordered basis $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^m$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, we may define the *total matrix representation map*

$$M_{\boldsymbol{\alpha}}^{\mathbf{n}} : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^{m\times n_1} \times \mathbb{F}_q^{m\times n_2} \times \cdots \times \mathbb{F}_q^{m\times n_\ell}$$

by

$$M_{\boldsymbol{\alpha}}^{\mathbf{n}}(\mathbf{c}) = \left(M_{\boldsymbol{\alpha}}^{n_1}\left(\mathbf{c}^{(1)}\right), M_{\boldsymbol{\alpha}}^{n_2}\left(\mathbf{c}^{(2)}\right), \ldots, M_{\boldsymbol{\alpha}}^{n_\ell}\left(\mathbf{c}^{(\ell)}\right)\right), \tag{1.11}$$

where $\mathbf{c} \in \mathbb{F}_{q^m}^n$ is subdivided as in (1.10).

For vectors $\mathbf{c}, \mathbf{d} \in \mathbb{F}_{q^m}^n$, we define sum-rank weights and distances via $M_{\boldsymbol{\alpha}}^{\mathbf{n}}$ as

$$\begin{aligned} \mathrm{wt}_{SR}(\mathbf{c}) &= \mathrm{wt}_{SR}\left(M_{\boldsymbol{\alpha}}^{\mathbf{n}}(\mathbf{c})\right), \text{ and} \\ \mathrm{d}_{SR}(\mathbf{c},\mathbf{d}) &= \mathrm{d}_{SR}\left(M_{\boldsymbol{\alpha}}^{\mathbf{n}}(\mathbf{c}), M_{\boldsymbol{\alpha}}^{\mathbf{n}}(\mathbf{d})\right) = \mathrm{wt}_{SR}(\mathbf{c}-\mathbf{d}). \end{aligned} \tag{1.12}$$

For a (linear or nonlinear) code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, we define its minimum sum-rank distance via the total matrix representation map, as

$$\begin{aligned} \mathrm{d}_{SR}(\mathcal{C}) &= \mathrm{d}_{SR}\left(M_{\boldsymbol{\alpha}}^{\mathbf{n}}(\mathcal{C})\right) \\ &= \min\{\mathrm{d}_{SR}(\mathbf{c},\mathbf{d}) \mid \mathbf{c},\mathbf{d} \in \mathcal{C}, \mathbf{c} \neq \mathbf{d}\} \\ &\overset{*}{=} \min\{\mathrm{wt}_{SR}(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}, \mathbf{c} \neq 0\}, \end{aligned} \tag{1.13}$$

where (*) holds if $\mathcal{C}$ is a linear code.

Now that we may see codes as subsets of $\mathbb{F}_{q^m}^n$, we will say that a code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is linear if it is $\mathbb{F}_{q^m}$-linear.

Although for simplicity we do not write it explicitly, it is important to note that the sum-rank weight and metric defined on $\mathbb{F}_{q^m}^n$ depend on the subfield $\mathbb{F}_q$ and the length partition $(n_1, \ldots, n_\ell)$, i.e., they depend on the pair $(q, \mathbf{n})$. However, the sum-rank weight and metric do *not* depend on the choice of ordered basis $\boldsymbol{\alpha}$, as shown in the following proposition.

**Proposition 1.3.** Given two ordered bases $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{F}_{q^m}^m$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, the equality

$$\mathrm{wt}_{SR}\left(M_{\boldsymbol{\alpha}}^{\mathbf{n}}(\mathbf{c})\right) = \mathrm{wt}_{SR}\left(M_{\boldsymbol{\beta}}^{\mathbf{n}}(\mathbf{c})\right),$$

holds for all $\mathbf{c} \in \mathbb{F}_{q^m}^n$.

*Proof.* We only need to prove that, for each $i \in [\ell]$, we have that

$$\mathrm{Rk}\left(M_{\boldsymbol{\alpha}}^{n_i}(\mathbf{d})\right) = \mathrm{Rk}\left(M_{\boldsymbol{\beta}}^{n_i}(\mathbf{d})\right), \tag{1.14}$$

for all $\mathbf{d} \in \mathbb{F}_{q^m}^{n_i}$. We know from linear algebra that there exists an invertible matrix $A \in \mathbb{F}_q^{m\times m}$ such that $\boldsymbol{\beta} = \boldsymbol{\alpha}A$. Since $\mathbf{d} = \boldsymbol{\alpha}M_{\boldsymbol{\alpha}}^{n_i}(\mathbf{d}) = \boldsymbol{\alpha}AM_{\boldsymbol{\beta}}^{n_i}(\mathbf{d})$ holds for every $\mathbf{d} \in \mathbb{F}_{q^m}^{n_i}$, we must have that

$$M_{\boldsymbol{\alpha}}^{n_i}(\mathbf{d}) = A \cdot M_{\boldsymbol{\beta}}^{n_i}(\mathbf{d}).$$

Since multiplying by an invertible matrix does not change rank, we conclude that (1.14) holds. □

Since the matrix representation map $M_{\boldsymbol{\alpha}}^{n_i}$ is a vector space isomorphism, for $i \in [\ell]$, the total matrix representation map $M_{\boldsymbol{\alpha}}^{\mathbf{n}}$ is a vector space isomorphism too (over $\mathbb{F}_q$). For this reason, for nonlinear or $\mathbb{F}_q$-linear codes, we may work with either $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ or its matrix form $\mathcal{C}' = M_{\boldsymbol{\alpha}}^{\mathbf{n}}(\mathcal{C}) \subseteq \mathbb{F}_q^{m\times n_1} \times \mathbb{F}_q^{m\times n_2} \times \cdots \times \mathbb{F}_q^{m\times n_\ell}$. It is important to take into account that, if $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is a linear code (over $\mathbb{F}_{q^m}$), then $M_{\boldsymbol{\alpha}}^{\mathbf{n}}(\mathcal{C})$ is only $\mathbb{F}_q$-linear ($\mathbb{F}_{q^m}$-linearity is lost).

Unless otherwise stated, we will work with linear codes in $\mathbb{F}_{q^m}^n$, meaning $\mathbb{F}_{q^m}$-linear, and with assumptions as in (1.6) and (1.8).

As the last results of the section, we show that the sum-rank metric recovers both the rank metric [41], [46], [152] and the Hamming metric [62] as particular cases.

**Proposition 1.4.** If $\ell = 1$, then the sum-rank weight $\mathrm{wt}_{SR}$ and metric $\mathrm{d}_{SR}$ become the rank weight and metric, respectively, and the ambient space (1.5) becomes the space of matrices $\mathbb{F}_q^{m\times n}$.

**Proposition 1.5.** If $m = m_1 = m_2 = \ldots = m_\ell = 1$ and $n_1 = n_2 = \ldots = n_\ell = 1$, then for the ordered basis $\boldsymbol{\alpha} = (1) \in \mathbb{F}_{q^1}^1$, we may think of the matrix representation map as the identity map

$$M_{\boldsymbol{\alpha}}^{\mathbf{n}} \equiv \mathrm{Id} : \mathbb{F}_q^\ell \longrightarrow \left(\mathbb{F}_q^{1\times 1}\right)^\ell,$$

and the sum-rank weight $\mathrm{wt}_{SR}$ and metric $\mathrm{d}_{SR}$ in this setting become the Hamming weight and metric, defined respectively as

$$\begin{aligned} \mathrm{wt}_H(c_1, c_2, \ldots, c_\ell) &= |\{i \in [n] \mid c_i \neq 0\}|, \text{ and} \\ \mathrm{d}_H(\mathbf{c}, \mathbf{d}) &= \mathrm{wt}_H(\mathbf{c} - \mathbf{d}), \end{aligned} \tag{1.15}$$

for all $c_1, c_2, \ldots, c_\ell \in \mathbb{F}_q$ and all $\mathbf{c}, \mathbf{d} \in \mathbb{F}_q^\ell$.

*Proof.* This follows from the observation that when a scalar $c \in \mathbb{F}_q$ is regarded as a $1 \times 1$ matrix, i.e., $c \in \mathbb{F}_q^{1\times 1}$, we have

$$\mathrm{Rk}(c) = \begin{cases} 1, & \text{if } c \neq 0; \\ 0, & \text{if } c = 0. \end{cases} \tag{1.16}$$

□

Proposition 1.5 also holds when $m > 1$. To see this, recall the extended definition (1.12) of sum-rank weights and distances for vectors over extension fields and note that (1.16) also holds for all $c \in \mathbb{F}_q^{m\times 1}$.

We will illustrate the points made above with an extension to the sum-rank metric of the classical repetition code.

**Example 1.5 (The sum-rank repetition code).** The traditional repetition code is the linear code generated by the vector $(1, 1, \ldots, 1)$ of arbitrary length $n$. It is a "good" code for the Hamming metric (it is MDS, that is, maximum distance separable) since the Hamming weight of the vector $(1, 1, \ldots, 1)$ equals its length $n$. However, its sum-rank weight is smaller than $n$ in general. To remedy this, fix an ordered basis $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and take a length-$n$ sum-rank partition $\mathbf{n} = (n_1, \ldots, n_\ell)$ of order $\ell$ with $n_i \leq m$ for all $i \in [\ell]$. We may then define the *sum-rank repetition code* as the one-dimensional linear code

$$\mathcal{C} = \left\langle \left( \boldsymbol{\alpha}^{(n_1)}, \boldsymbol{\alpha}^{(n_2)}, \ldots, \boldsymbol{\alpha}^{(n_\ell)} \right) \right\rangle_{\mathbb{F}_{q^m}} \subseteq \mathbb{F}_{q^m}^n,$$

where $\langle \cdot \rangle_{\mathbb{F}_{q^m}}$ denotes $\mathbb{F}_{q^m}$-linear span and

$$\boldsymbol{\alpha}^{(n_i)} = (\alpha_1, \alpha_2, \ldots, \alpha_{n_i}) \in \mathbb{F}_{q^m}^{n_i},$$

for $i \in [\ell]$. Observe that

$$M_{\boldsymbol{\alpha}}^{\mathbf{n}} \left( \boldsymbol{\alpha}^{(n_1)}, \boldsymbol{\alpha}^{(n_2)}, \ldots, \boldsymbol{\alpha}^{(n_\ell)} \right) = \left( I_m^{n_1}, I_m^{n_2}, \ldots, I_m^{n_\ell} \right),$$

where $I_m^{n_i} \in \mathbb{F}_q^{m\times n_i}$ denotes the first $n_i$ columns of the $m \times m$ identity matrix for $i \in [\ell]$. Therefore, we have that

$$\mathrm{wt}_{SR} \left( \boldsymbol{\alpha}^{(n_1)}, \boldsymbol{\alpha}^{(n_2)}, \ldots, \boldsymbol{\alpha}^{(n_\ell)} \right) = \sum_{i=1}^{\ell} \mathrm{Rk} \left( I_m^{n_i} \right) = \sum_{i=1}^{\ell} n_i = n.$$

By Proposition 1.6 below, we have that $\mathrm{d}_{SR}(\mathcal{C}) = \mathrm{d}_{SR}\left(M_{\boldsymbol{\alpha}}^{\mathbf{n}}(\mathcal{C})\right) = n$, as in the classical Hamming-metric repetition code. Finally, note that, since $M_{\boldsymbol{\alpha}}^{\mathbf{n}}\left(\boldsymbol{\alpha}^{(n_1)}, \boldsymbol{\alpha}^{(n_2)}, \ldots, \boldsymbol{\alpha}^{(n_\ell)}\right) = (I_m^{n_1}, I_m^{n_2}, \ldots, I_m^{n_\ell})$, then in the Hamming-metric case ($m = n_1 = n_2 = \ldots = n_\ell = 1$), we have that $M_{\boldsymbol{\alpha}}^{\mathbf{n}}\left(\boldsymbol{\alpha}^{(n_1)}, \boldsymbol{\alpha}^{(n_2)}, \ldots, \boldsymbol{\alpha}^{(n_\ell)}\right) = (1, 1, \ldots, 1)$, $n = \ell$ times. Hence we recover the classical repetition code as a particular case, which motivates this definition of the sum-rank repetition code.

## 1.2 Linear Isometries for the Sum-Rank Metric

In this section, we describe the linear maps (over $\mathbb{F}_{q^m}$) that preserve sum-rank weights, i.e., the *linear isometries* for the sum-rank metric.

Our interest in this concept is that it enables us to connect sum-rank weights and Hamming weights (see Theorem 1.2, Corollary 1.3 and (1.20) below). We will also use this connection in Section 1.4 to define maximum sum-rank distance (MSRD) codes in terms of MDS codes (see Theorem 1.4 and Definition 1.7 below). Such a characterization will also be of interest in some applications (see Section 3), where we want codes which are MDS after being multiplied on the right by any invertible block-diagonal matrix.

We start with the following basic definition.

**Definition 1.5.** We say that a map $\phi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$ is a linear sum-rank isometry if it is linear (over $\mathbb{F}_{q^m}$), bijective, and

$$\mathrm{wt}_{SR}\left(\phi(\mathbf{c})\right) = \mathrm{wt}_{SR}(\mathbf{c}),$$

for all $\mathbf{c} \in \mathbb{F}_{q^m}^n$.

Although defined as being weight-preserving, if $\phi$ is a linear sum-rank isometry, then it preserves distances also, i.e., it really *is* an isometry. This follows since for any pair of vectors $\mathbf{c}, \mathbf{d} \in \mathbb{F}_{q^m}^n$, we have

$$\begin{aligned} \mathrm{d}_{SR}(\phi(\mathbf{c}), \phi(\mathbf{d})) &= \mathrm{wt}_{SR}(\phi(\mathbf{c}) - \phi(\mathbf{d})) \\ &\overset{(a)}{=} \mathrm{wt}_{SR}(\phi(\mathbf{c} - \mathbf{d})) \\ &\overset{(b)}{=} \mathrm{wt}_{SR}(\mathbf{c} - \mathbf{d}) = \mathrm{d}_{SR}(\mathbf{c}, \mathbf{d}), \end{aligned}$$

where (a) follows from the linearity of $\phi$ and (b) follows from the fact that $\phi$ is weight-preserving.

In fact there is some redundancy in the definition, since as is the case for any metric, a linear map preserving distances is necessarily injective ($\mathrm{d}_{SR}(\mathbf{c}, \mathbf{d}) = 0$ if, and only if, $\mathbf{c} = \mathbf{d}$). Since the domains and codomains in Definition 1.5 are vector spaces of equal dimension, a linear injective map is also bijective. In other words, we may remove the condition of being bijective from Definition 1.5 above. We have kept it as a reminder for the reader.

As is the case with any other metric, we may say that two linear codes $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_{q^m}^n$ are *equivalent* for the sum-rank metric if there exists a linear sum-rank isometry $\phi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$ such that $\phi(\mathcal{C}_1) = \mathcal{C}_2$. Since $\phi$ is a linear sum-rank isometry, additive errors and their sum-rank weights are preserved, and the sum-rank error correction capability of $\mathcal{C}_1$ and $\mathcal{C}_2$ is the same. Furthermore, since $\phi$ is linear and bijective, then $\mathcal{C}_1$ and $\mathcal{C}_2$ are isomorphic as vector spaces and have the same dimension.

We start with the following basic result, which is also useful on its own (see, e.g., Example 1.5 above).

**Proposition 1.6.** For any $\mathbf{c} \in \mathbb{F}_{q^m}^n$ and any $\beta \in \mathbb{F}_{q^m} \setminus \{0\}$,

$$\mathrm{wt}_{SR}(\beta\mathbf{c}) = \mathrm{wt}_{SR}(\mathbf{c}).$$

*Proof.* Since $\beta \neq 0$, the reader may verify that the vector

$$\beta\boldsymbol{\alpha} = (\beta\alpha_1, \beta\alpha_2, \ldots, \beta\alpha_m) \in \mathbb{F}_{q^m}^m$$

is an ordered basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, for any ordered basis $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^m$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. It now follows from the definition of the total matrix representation map (Definition 1.11) that

$$M_{\beta\boldsymbol{\alpha}}^{\mathbf{n}}(\beta\mathbf{c}) = M_{\boldsymbol{\alpha}}^{\mathbf{n}}(\mathbf{c}),$$

for all $\mathbf{c} \in \mathbb{F}_{q^m}^n$, and the result follows by Proposition 1.3. □

We now give a different family of linear sum-rank isometries.

**Proposition 1.7.** Given $\mathbf{c} \in \mathbb{F}_{q^m}^n$, invertible matrices $A_i \in \mathbb{F}_q^{n_i \times n_i}$, for $i \in [\ell]$, and setting

$$A = \mathrm{Diag}(A_1, A_2, \ldots, A_\ell) = \begin{pmatrix} A_1 & 0 & \ldots & 0 \\ 0 & A_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & A_\ell \end{pmatrix} \in \mathbb{F}_q^{n \times n}, \quad (1.17)$$

we have, for the length partition $\mathbf{n} = (n_1, \ldots, n_\ell)$, that

$$\mathrm{wt}_{SR}(\mathbf{c}A) = \mathrm{wt}_{SR}(\mathbf{c}).$$

*Proof.* Consider $C = M_{\boldsymbol{\alpha}}^{\mathbf{n}}(\mathbf{c}) = (C_1, C_2, \ldots, C_\ell)$, where

$$C_i = M_{\boldsymbol{\alpha}}^{n_i}\left(\mathbf{c}^{(i)}\right) \in \mathbb{F}_q^{m \times n_i},$$

for $i \in [\ell]$, and where $\mathbf{c}$ is subdivided as in (1.10).

Fix invertible matrices $A_i \in \mathbb{F}_q^{n_i \times n_i}$, for $i \in [\ell]$. Fix one such index $i$. The reader may verify that

$$C_i A_i = M_{\boldsymbol{\alpha}}^{n_i}\left(\mathbf{c}^{(i)}\right) A_i = M_{\boldsymbol{\alpha}}^{n_i}\left(\mathbf{c}^{(i)} A_i\right). \quad (1.18)$$

In other words, writing $A = \mathrm{Diag}(A_1, A_2, \ldots, A_\ell)$, we have that

$$M_{\boldsymbol{\alpha}}^{\mathbf{n}}(\mathbf{c}A) = (C_1 A_1, C_2 A_2, \ldots, C_\ell A_\ell).$$

Since $A_i \in \mathbb{F}_q^{m \times n_i}$ is invertible, we have

$$\mathrm{Rk}(C_i) = \mathrm{Rk}(C_i A_i).$$

Therefore, we conclude that

$$\mathrm{wt}_{SR}(\mathbf{c}A) = \sum_{i=1}^{\ell} \mathrm{Rk}(C_i A_i) = \sum_{i=1}^{\ell} \mathrm{Rk}(C_i) = \mathrm{wt}_{SR}(\mathbf{c}),$$

and we are done. □

In fact, combining the linear isometries from Propositions 1.6 and 1.7, together with possibly some permutations of coordinates, we obtain all linear sum-rank isometries. The following result was obtained in [119, Th. 2]. We omit the proof for brevity.

**Theorem 1.1.** A map $\phi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$ is a linear isometry if, and only if, there exist scalars $\beta_1, \beta_2, \ldots, \beta_\ell \in \mathbb{F}_{q^m} \setminus \{0\}$, invertible matrices $A_i \in \mathbb{F}_q^{n_i \times n_i}$, for $i \in [\ell]$, and a permutation $\sigma : [\ell] \longrightarrow [\ell]$ satisfying that $\sigma(i) \neq j$ if $n_i \neq n_j$, and such that

$$\phi(\mathbf{c}) = \left(\beta_1 \mathbf{c}^{(\sigma(1))} A_1, \beta_2 \mathbf{c}^{(\sigma(2))} A_2, \ldots, \beta_\ell \mathbf{c}^{(\sigma(\ell))} A_\ell\right),$$

for all $\mathbf{c} \in \mathbb{F}_{q^m}^n$, subdivided as in (1.10).

Note that Theorem 1.1 recovers, as particular cases, the classical expressions of linear isometries for the Hamming and rank metrics.

Finally, the main result of this section is to describe sum-rank weights as a function of Hamming weights and the linear sum-rank isometries from Proposition 1.7. This result was obtained in [124, Th. 1].

**Theorem 1.2.** Given $\mathbf{c} \in \mathbb{F}_{q^m}^n$ and defining the Hamming weight and metric in $\mathbb{F}_{q^m}^n$ as in Proposition 1.5 ($\mathrm{wt}_H(\mathbf{c})$ is the number of nonzero entries over $\mathbb{F}_{q^m}$ of $\mathbf{c} \in \mathbb{F}_{q^m}^n$), the sum-rank weight of $\mathbf{c}$ satisfies

$$\begin{aligned}\mathrm{wt}_{SR}(\mathbf{c}) = \min\{\mathrm{wt}_H(\mathbf{c}A) \mid & A = \mathrm{Diag}(A_1, A_2, \ldots, A_\ell) \in \mathbb{F}_q^{n \times n}, \\ & A_i \in \mathbb{F}_q^{n_i \times n_i} \text{ invertible}, 1 \leq i \leq \ell\}.\end{aligned} \tag{1.19}$$

*Proof.* We will start by proving the inequality $\leq$ in (1.19). Since the number of nonzero columns is an upper bound on the rank of a matrix, we deduce that $\mathrm{wt}_{SR}(\mathbf{d}) \leq \mathrm{wt}_H(\mathbf{d})$, for all $\mathbf{d} \in \mathbb{F}_{q^m}^n$. Combined with Proposition 1.7, we conclude that

$$\mathrm{wt}_{SR}(\mathbf{c}) = \mathrm{wt}_{SR}(\mathbf{c}A) \leq \mathrm{wt}_H(\mathbf{c}A).$$

Next, we prove the opposite inequality $\geq$ in (1.19). As in the proof of Proposition 1.7, consider $C = M_{\boldsymbol{\alpha}}^{\mathbf{n}}(\mathbf{c}) = (C_1, C_2, \ldots, C_\ell)$, where

$$C_i = M_{\boldsymbol{\alpha}}^{n_i}\left(\mathbf{c}^{(i)}\right) \in \mathbb{F}_q^{m \times n_i},$$

for $i \in [\ell]$, and where $\mathbf{c}$ is subdivided as in (1.10). Fix an index $i \in [\ell]$. There exists an invertible matrix $A_i \in \mathbb{F}_q^{n_i \times n_i}$ such that

$$C_i A_i = D_i, \quad \text{and} \quad \mathrm{wt}_H(D_i) = \mathrm{Rk}(C_i).$$

For instance, if we apply Gauss–Jordan elimination column-wise on $C_i$, then $D_i$ is the resulting matrix and $A_i$ is the matrix encoding the column transformations. Setting $A = \mathrm{Diag}(A_1, A_2, \ldots, A_\ell)$, we conclude that

$$\mathrm{wt}_H(\mathbf{c}A) = \sum_{i=1}^{\ell} \mathrm{wt}_H(C_i A_i) = \sum_{i=1}^{\ell} \mathrm{wt}_H(D_i) = \sum_{i=1}^{\ell} \mathrm{Rk}(C_i) = \mathrm{wt}_{SR}(\mathbf{c}),$$

where we have used (1.18), and we are done. □

In fact, since coordinate-wise multiplications by nonzero scalars and permutations of coordinates are also linear isometries for the Hamming metric, then by Theorem 1.1, (1.19) can be rewritten as

$$\mathrm{wt}_{SR}(\mathbf{c}) = \min\{\mathrm{wt}_H(\phi(\mathbf{c})) \mid \phi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n \text{ is a linear sum-rank isometry}\}. \tag{1.20}$$

Theorem 1.2 yields the following corollary on minimum distances. We will use this fact to connect maximum sum-rank distance (MSRD) codes and MDS codes (see Theorem 1.4 and Definition 1.7).

**Corollary 1.3.** The minimum sum-rank distance of a (linear or nonlinear) code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ satisfies

$$\mathrm{d}_{SR}(\mathcal{C}) = \min\{\mathrm{d}_H(\mathcal{C}A) \mid A = \mathrm{Diag}(A_1, A_2, \ldots, A_\ell) \in \mathbb{F}_q^{n\times n}, A_i \in \mathbb{F}_q^{n_i \times n_i} \text{ invertible }, 1 \le i \le \ell\}, \tag{1.21}$$

where $\mathrm{d}_H(\mathcal{C}A)$ denotes the minimum Hamming distance of the code

$$\mathcal{C}A = \{\mathbf{c}A \mid \mathbf{c} \in \mathcal{C}\} \subseteq \mathbb{F}_{q^m}^n. \tag{1.22}$$

**Example 1.6.** Consider the classical repetition code $\mathcal{C} = \langle(1, 1, \ldots, 1)\rangle_{\mathbb{F}_{q^m}} \subseteq \mathbb{F}_{q^m}^n$, for an arbitrary length partition $\mathbf{n} = (n_1, \ldots, n_\ell)$. If we assume that $m = 1$ and we choose the length partition $\mathbf{n} = (1, 1, \ldots, 1)$, then the sum-rank metric recovers the Hamming metric (Proposition 1.5), and Theorem 1.2 says that

$$\mathrm{d}_H(\mathcal{C}A) = n,$$

if $A = \mathrm{Diag}(a_1, a_2, \ldots, a_n) \in \mathbb{F}_q^{n\times n}$, for all $a_1, a_2, \ldots, a_n \in \mathbb{F}_q \setminus \{0\}$. This is the case because invertible diagonal matrices constitute Hamming

isometries, that is, they preserve Hamming distances. However, if $n$ is even and we choose the length partition $\mathbf{n} = (2, 2, \ldots, 2)$ of order $n/2$, then we may choose the invertible matrices

$$A_i = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \in \mathbb{F}_q^{2\times 2},$$

for $i \in [n/2]$. Setting $A = \mathrm{Diag}(A_1, A_2, \ldots, A_{n/2}) \in \mathbb{F}_q^{n\times n}$, we have that

$$(1, 1, 1, 1 \ldots, 1, 1) \cdot A = (1, 0, 1, 0, \ldots, 1, 0).$$

Hence in this case, we have that

$$\mathrm{d}_H(\mathcal{C}A) = \frac{n}{2} < n = \mathrm{d}_H(\mathcal{C}).$$

For this length partition, the "correct" sum-rank repetition code would be $\mathcal{D} = \langle(\alpha_1, \alpha_2, \alpha_1, \alpha_2, \ldots, \alpha_1, \alpha_2)\rangle_{\mathbb{F}_{q^2}} \subseteq \mathbb{F}_{q^2}^n$, where $m = 2$, and $\alpha_1, \alpha_2 \in \mathbb{F}_{q^2}$ are linearly independent over $\mathbb{F}_q$ (Example 1.5).

## 1.3 The Singleton Bound for the Sum-Rank Metric

In this section, we will provide two Singleton bounds on the size of a code, given its minimum sum-rank distance, or vice versa. Other general upper bounds and existential bounds are explored in [20], [141]. As in the classical case of codes considered with the Hamming metric, the minimum distance and the code size are competing parameters, each of which we would like to be as large as possible.

Taking $A$ as the $n \times n$ identity matrix in (1.21), we have that

$$\mathrm{d}_{SR}(\mathcal{C}) \leq \mathrm{d}_H(\mathcal{C}), \tag{1.23}$$

for all (linear or nonlinear) codes $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$. The inequality (1.23) implies that any upper bound on the minimum Hamming distance of a code is also an upper bound on its minimum sum-rank distance. However, (1.21) is stronger (as it states that equality holds for some matrix $A$), and implies the following form of the Singleton bound, obtained in [124].

**Theorem 1.4 (First Singleton bound).** Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a (linear or nonlinear) code. Then

$$|\mathcal{C}| \leq q^{m(n-\mathrm{d}_{SR}(\mathcal{C})+1)}, \tag{1.24}$$

where equality holds if, and only if,

$$|\mathcal{C}A| = q^{m(n-\mathrm{d}_H(\mathcal{C}A)+1)} \tag{1.25}$$

for all $A = \mathrm{Diag}(A_1, A_2, \ldots, A_\ell) \in \mathbb{F}_q^{n\times n}$, such that $A_i \in \mathbb{F}_q^{n_i\times n_i}$ is invertible, for all $i \in [\ell]$.

If $\mathcal{C}$ is a linear code, then (1.24) and (1.25) can be rewritten as

$$\mathrm{d}_{SR}(\mathcal{C}) \leq n - \dim(\mathcal{C}) + 1, \tag{1.26}$$

where equality holds if, and only if,

$$\mathrm{d}_H(\mathcal{C}A) = n - \dim(\mathcal{C}A) + 1, \tag{1.27}$$

for all $A = \mathrm{Diag}(A_1, A_2, \ldots, A_\ell) \in \mathbb{F}_q^{n\times n}$, such that $A_i \in \mathbb{F}_q^{n_i\times n_i}$ is invertible, for $i \in [\ell]$.

We may obtain an alternative Singleton bound by transposing matrices in the ambient space $\mathbb{F}_q^{m\times n_1} \times \mathbb{F}_q^{m\times n_2} \times \cdots \times \mathbb{F}_q^{m\times n_\ell}$. We give a formal definition as follows.

**Definition 1.6.** Assume that a length-$(N\ell)$ sum-rank partition $\mathbf{n}$ of order $\ell$ is given as $\mathbf{n} = (N, N, \ldots, N)$. Given a (linear or nonlinear) code $\mathcal{C} \subseteq \left(\mathbb{F}_q^{m\times N}\right)^\ell$, we define its transposed code as

$$\mathcal{C}^\intercal = \left\{(C_1^\intercal, C_2^\intercal, \ldots, C_\ell^\intercal) \mid (C_1, C_2, \ldots, C_\ell) \in \mathcal{C}\right\},$$

where $C^\intercal \in \mathbb{F}_q^{N\times m}$. Fix an ordered basis $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m)$ for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and an ordered basis $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_N)$ for $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$. For a code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n = \mathbb{F}_{q^m}^{\ell N}$, we define its transposed code with length-$(m\ell)$ sum-rank partition $\mathbf{m}$ of order $\ell$ given as $\mathbf{m} = (m, m, \ldots, m)$ via

$$\mathcal{C}^\intercal = \left(M_{\boldsymbol{\beta}}^{\mathbf{m}}\right)^{-1} \left(M_{\boldsymbol{\alpha}}^{\mathbf{n}}(\mathcal{C})^\intercal\right) \subseteq \mathbb{F}_{q^N}^{\ell m}.$$

We are now ready to give a second Singleton bound. Observe that this bound works when the matrix sizes are the same at different positions. This result was obtained in [124].

**Theorem 1.5 (Second Singleton bound).** Let $\mathbf{n} = (N, N, \ldots, N)$ be a length-$(\ell N)$ sum-rank partition of order $\ell$ and let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a (linear or nonlinear) code. Then

$$|\mathcal{C}| \leq q^{N(\ell m - \mathrm{d}_{SR}(\mathcal{C})+1)}. \tag{1.28}$$

If $\mathcal{C}$ is linear, then (1.28) can be rewritten as

$$\mathrm{d}_{SR}(\mathcal{C}) \leq \frac{N}{m}\left(\ell m - \dim(\mathcal{C}) + 1\right). \tag{1.29}$$

*Proof.* The inequality (1.28) follows from (1.24), applied on the transposed code $\mathcal{C}^\intercal \subseteq \mathbb{F}_{q^N}^{\ell m}$, and combined with the following equalities:

$$|\mathcal{C}^\intercal| = |\mathcal{C}| \quad \text{and} \quad \mathrm{d}_{SR}\left(\mathcal{C}^\intercal\right) = \mathrm{d}_{SR}(\mathcal{C}). \tag{1.30}$$

□

Although there exist codes attaining this bound (the transposed code of any code attaining the bound (1.24)), we will only use it to obtain a bound on the parameters of codes attaining the first bound (1.24). See Proposition 1.8 below.

## 1.4 Maximum Sum-Rank Distance (MSRD) Codes

Among different possible bounds on the code size given the minimum sum-rank distance, the first Singleton bound (1.24) plays an important role in some applications (for instance, in distributed storage, as we will see in Section 3). This is due to the fact that, by Theorem 1.4, a code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ meets the bound (1.24) for the sum-rank metric if, and only if, the code $\mathcal{C}A \subseteq \mathbb{F}_{q^m}^n$ meets the classical Singleton bound for its minimum Hamming distance (i.e., $\mathcal{C}A$ is an MDS code), for any invertible block-diagonal matrix $A$ as in (1.17).

Due to this result, in this monograph we define maximum sum-rank distance (MSRD) codes as those meeting the first Singleton bound.

**Definition 1.7 (MSRD codes).** We say that a (linear or nonlinear) code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is a *maximum sum-rank distance* code, or MSRD code for short, if one of the following equivalent conditions holds:

1. Equality holds in (1.24), i.e.,
$$|\mathcal{C}| = q^{m(n-\mathrm{d}_{SR}(\mathcal{C})+1)}. \tag{1.31}$$
2. $\mathcal{C}A \subseteq \mathbb{F}_{q^m}^n$ is MDS, for all $A = \mathrm{Diag}(A_1, A_2, \ldots, A_\ell) \in \mathbb{F}_q^{n\times n}$, such that $A_i \in \mathbb{F}_q^{n_i \times n_i}$ is invertible, for all $i \in [\ell]$.

3. (If $\mathcal{C}$ is linear)
$$\mathrm{d}_{SR}(\mathcal{C}) = n - \dim(\mathcal{C}) + 1. \tag{1.32}$$

**Example 1.7.** The sum-rank repetition code is an MSRD code. Let the notation be as in Example 1.5. We know from that example that $\mathrm{d}_{SR}(\mathcal{C}) = n$ and $\dim(\mathcal{C}) = 1$. Hence (1.32) holds. Now, for all invertible matrices $A_i \in \mathbb{F}_q^{n_i \times n_i}$, for $i \in [\ell]$, if we set $A = \mathrm{Diag}(A_1, A_2, \ldots, A_\ell)$, then $\mathcal{C}A$ is also a sum-rank repetition code, hence $\mathrm{d}_H(\mathcal{C}A) = n$ and $\dim(\mathcal{C}A) = 1$, thus $\mathcal{C}A$ is MDS.

Observe that, when $\ell = 1$ and $m \geq N = n_1$, the families of MSRD codes and maximum rank distance (MRD) codes in $\mathbb{F}_{q^m}^N$ coincide. Analogously, when $m = n_1 = n_2 = \ldots = n_\ell = 1$, the families of MSRD codes and MDS codes in $\mathbb{F}_q^\ell$ coincide.

Note that, when $N = n_1 = n_2 = \ldots = n_\ell$, one may obtain a code attaining the second Singleton bound (1.28) from any MSRD code as in Definition 1.7, simply by considering its transposed code (Definition 1.6). However, if the original code is $\mathbb{F}_{q^m}$-linear, then we may only guarantee that the transposed code is $\mathbb{F}_q$-linear.

We devote the remainder of this section to non-existence results for (linear or nonlinear) MSRD codes. Such results will be given in the form of bounds on the parameters $m$, $\ell$, $n_1, n_2, \ldots, n_\ell$, and $q$.

The next result follows from the second Singleton bound (Theorem 1.5) and was obtained in [124].

**Proposition 1.8.** Assume that $\mathbf{n} = (N, N, \ldots, N)$ is a length- $(\ell N)$ sum-rank partition of order $\ell$. If there exists a (linear or nonlinear) MSRD code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^N$ with $\mathrm{d}_{SR}(\mathcal{C}) > 1$ over $\mathbb{F}_q$, then $m \geq N$.

*Proof.* Assume that $\mathcal{C} \subseteq \mathbb{F}_{q^m}^N$ is a code with $d = \mathrm{d}_{SR}(\mathcal{C})$. If $m < N$ and $d > 1$, then by Theorem 1.5, we have that
$$\begin{aligned} |\mathcal{C}| &\leq q^{N(\ell m - d + 1)} \\ &= q^{\ell m N - (d-1)N} \\ &< q^{\ell m N - (d-1)m} \\ &= q^{m(n-d+1)}, \end{aligned}$$
and the code $\mathcal{C}$ cannot satisfy (1.31), hence it cannot be MSRD. □

In the previous proposition, we assumed that $N = n_1 = n_2 = \ldots = n_\ell$. Using puncturing (see Definition 1.9 and Corollary 1.9 below), we may prove that, if there exists a (linear or nonlinear) MSRD code $\mathcal{C} \subsetneq \mathbb{F}_{q^m}^n$ with $\mathrm{d}_{SR}(\mathcal{C}) > 1$ over $\mathbb{F}_q$, for arbitrary $n_1, n_2, \ldots, n_\ell$, then

$$m \geq \min\{n_1, n_2, \ldots, n_\ell\}. \tag{1.33}$$

In fact, linearized Reed–Solomon codes, described in Section 2, are MSRD and exist as long as $m \geq \max\{n_1, n_2, \ldots, n_\ell\}$ and $q > \ell$.

It is important to observe that any MRD code in $\mathbb{F}_{q^m}^n$ (i.e., an MSRD code for the length-$n$ sum-rank partition of order 1) is MSRD for a length-$n$ sum-rank partition of any order $\ell \leq n$. However, by Proposition 1.8 above for $\ell = 1$, MRD codes always require that

$$m \geq n = n_1 + n_2 + \cdots + n_\ell. \tag{1.34}$$

In particular, their symbol alphabet sizes $|\mathbb{F}_{q^m}| \geq q^n$ are exponential in the code length $n$, which is impractical except for small values of $n$. In Section 2, we will describe *linearized Reed–Solomon codes* [116], which are the first known family of MSRD codes with sub-exponential field sizes, and the only known MSRD codes accepting parameters such that $m = \max\{n_1, n_2, \ldots, n_\ell\}$. Further linear MSRD codes with sub-exponential symbol alphabet sizes (smaller than those of linearized Reed–Solomon codes in many cases) appeared recently in [120] (see Section 6.1).

Recently in [20], the following bounds for the existence of MSRD codes were provided. While Proposition 1.8 bounds $m$ in terms of $N$, the following are bounds on $\ell$ that take $q$ into account. They follow from combining the Singleton bound with the projective sphere-packing bound, but we omit the proof for brevity.

**Proposition 1.9.** Let $\mathbf{n} = (N, N, \ldots, N)$ be a length-$(\ell N)$ sum-rank partition of order $\ell$ and suppose that $m \geq N$. Assume that there exists a (linear or nonlinear) MSRD code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n = \mathbb{F}_{q^m}^{\ell N}$ with $d = \mathrm{d}_{SR}(\mathcal{C}) \geq 3$. Then

$$\ell \leq \left\lfloor \frac{d-3}{N} \right\rfloor + \left\lfloor \frac{q^N - q^{N\left\lfloor \frac{d-3}{N} \right\rfloor + N - d + 3} + (q-1)q^m}{q^N - 1} \right\rfloor. \tag{1.35}$$

From (1.35) we deduce the following bounds. First, we have that

$$\ell \leq \left\lfloor \frac{d-3}{N} \right\rfloor + \left\lfloor (q-1) \cdot \frac{q^m}{q^N - 1} \right\rfloor + 1. \tag{1.36}$$

For the case $d = 3$ and arbitrary $m$ and $N$ (with $m \geq N$), we have that

$$\ell \leq \left\lfloor (q-1) \cdot \frac{q^m + 1}{q^N - 1} \right\rfloor, \tag{1.37}$$

and if, furthermore, $N$ divides $m$, and $N \geq 2$, then

$$\ell \leq (q-1) \cdot \frac{q^m - 1}{q^N - 1}. \tag{1.38}$$

Finally, for the case $m = N$ and arbitrary $d$, we have the bound

$$\ell \leq \left\lfloor \frac{d-3}{N} \right\rfloor + q + 1. \tag{1.39}$$

Observe that the bounds above can be rewritten as lower bounds on the field size $q^m$. For instance, (1.36) can be rewritten as

$$q^m \geq \frac{q^N - 1}{q - 1} \cdot \left( \ell - \left\lfloor \frac{d-3}{N} \right\rfloor - 1 \right). \tag{1.40}$$

As in (1.33), we may deduce, via puncturing, non-existence bounds as above in the case of an arbitrary length partition $\mathbf{n} = (n_1, n_2, \ldots, n_\ell)$ of order $\ell$, replacing $N$ by $\min\{n_1, n_2, \ldots, n_\ell\}$.

As we will show in Example 1.8, there exist codes with minimum sum-rank distance $d = 2$, for $\ell$ unbounded and for any fixed $q$, $m$ and $N$. Hence the assumption $d \geq 3$ in Proposition 1.9 cannot be lifted.

Linearized Reed–Solomon codes (Section 2) are the only known general MSRD codes with $m = N$. They require that $\ell \leq q - 1$, where equality may be attained. Hence there is an additive gap of

$$\left\lfloor \frac{d-3}{N} \right\rfloor + 2$$

between the value of $\ell$ that they may attain and the bound (1.39). When $d \leq N + 2$, such an additive gap is reduced to 2, as the bound (1.39) becomes $\ell \leq q + 1$ in that case.

Finally, we note that the bound (1.38) is sharp, and it was attained by the linear MSRD codes introduced in [120], which we study in Section 6.1. It is still an open problem to find if the other bounds from Proposition 1.9 are sharp.

## 1.5 Generator Matrices of MSRD Codes

In this section, we provide characterizations of generator and parity-check matrices of linear MSRD codes in $\mathbb{F}_{q^m}^n$. These characterizations are of interest for some applications (see Section 3). They can also be used to prove that linear codes are MSRD with high probability over large fields [141]. We assume that a length partition $\mathbf{n} = (n_1, \ldots, n_\ell)$ of order $\ell$ is given.

**Theorem 1.6.** Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a $k$-dimensional linear code with generator and parity-check matrices $G \in \mathbb{F}_{q^m}^{k\times n}$ and $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$, respectively. Then the following conditions are equivalent:

1. $\mathcal{C}$ is an MSRD code.
2. Every square $k \times k$ submatrix of $GA \in \mathbb{F}_{q^m}^{k\times n}$ is invertible, for all invertible matrices $A_i \in \mathbb{F}_q^{n_i\times n_i}$, for $i \in [\ell]$, setting $A = \mathrm{Diag}(A_1, A_2, \ldots, A_\ell)$.
3. Every square $(n-k) \times (n-k)$ submatrix of $HA \in \mathbb{F}_{q^m}^{(n-k)\times n}$ is invertible, for all invertible matrices $A_i \in \mathbb{F}_q^{n_i\times n_i}$, for $i \in [\ell]$, setting $A = \mathrm{Diag}(A_1, A_2, \ldots, A_\ell)$.

*Proof.* Let $A_i \in \mathbb{F}_q^{n_i\times n_i}$ be invertible matrices, for $i \in [\ell]$, and set $A = \mathrm{Diag}(A_1, A_2, \ldots, A_\ell)$. Then $GA \in \mathbb{F}_{q^m}^{k\times n}$ and $H\,(A^\intercal)^{-1} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ are generator and parity-check matrices, respectively, of the linear code $\mathcal{C}A \subseteq \mathbb{F}_{q^m}^n$. By Definition 1.7, $\mathcal{C}$ is MSRD if, and only if, $\mathcal{C}A$ is MDS for all such block-diagonal invertible matrices. Therefore, the result follows from the fact that a linear code is MDS if, and only if, every square $k \times k$ submatrix of one of its generator matrices is invertible, and similarly for parity-check matrices. □

The previous theorem implies that any $k$ coordinates in $[n]$ form an information set of a $k$-dimensional linear MSRD code, as is the case for linear MDS codes. In particular, we may choose any $k$ coordinates to form a systematic generator matrix of a linear MSRD code.

We conclude with a characterization of systematic generator matrices of linear MSRD codes. For this purpose, we need to revisit the definition of superregular matrices. See also [153] and [110, Ch. 11, Th. 8].

**Definition 1.8.** For arbitrary positive integers $r$ and $s$, we say that a matrix $M \in \mathbb{F}_{q^m}^{r\times s}$ is *superregular* if all square submatrices of $M$ (of any size up to $\min\{r, s\}$) are invertible.

We have the following characterization of systematic generator matrices of linear MSRD codes in terms of superregular matrices. This result was given in [4].

**Theorem 1.7.** Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a $k$-dimensional linear code with generator matrix $G \in \mathbb{F}_{q^m}^{k\times n}$. Consider a dimension partition $k = k_1 + k_2 + \cdots + k_\ell$, where $0 \leq k_i \leq n_i$, for $i \in [\ell]$, and assume that

$$G = (J_1, P_1, J_2, P_2, \ldots, J_\ell, P_\ell) \in \mathbb{F}_{q^m}^{k\times n},$$

for matrices $J_i \in \mathbb{F}_{q^m}^{k\times k_i}$ and $P_i \in \mathbb{F}_{q^m}^{k\times(n_i-k_i)}$, such that

$$I_k = (J_1, J_2, \ldots, J_\ell) \in \mathbb{F}_{q^m}^{k\times k}$$

is the $k \times k$ identity matrix. Let $P = (P_1, P_2, \ldots, P_\ell) \in \mathbb{F}_{q^m}^{k\times(n-k)}$. Then $\mathcal{C}$ is MSRD if, and only if, the matrix

$$BPA + C \in \mathbb{F}_{q^m}^{k\times(n-k)}$$

is superregular, for all matrices $C_i \in \mathbb{F}_q^{k_i\times(n_i-k_i)}$ and for all invertible matrices $B_i \in \mathbb{F}_q^{k_i\times k_i}$ and $A_i \in \mathbb{F}_q^{(n_i-k_i)\times(n_i-k_i)}$, for $i \in [\ell]$, and where we set

$$\begin{aligned} A &= \mathrm{Diag}(A_1, A_2, \ldots, A_\ell) \in \mathbb{F}_q^{(n-k)\times(n-k)}, \\ B &= \mathrm{Diag}(B_1, B_2, \ldots, B_\ell) \in \mathbb{F}_q^{k\times k}, \\ C &= \mathrm{Diag}(C_1, C_2, \ldots, C_\ell) \in \mathbb{F}_q^{k\times(n-k)}. \end{aligned} \tag{1.41}$$

Here, it may happen that $k_i = 0$ or $n_i - k_i = 0$, for some $i \in [\ell]$. If for instance $k_i = 0$, then in the $i$th block we add $n_i - k_i > 0$ zero columns but we add no rows to form $C$. To form $B$, nothing is added in this case in the $i$th block. Similarly if $n_i - k_i = 0$ (then $k_i > 0$).

*Proof.* Let $A \in \mathbb{F}_q^{(n-k)\times(n-k)}$, $B \in \mathbb{F}_q^{k\times k}$, and $C \in \mathbb{F}_q^{k\times(n-k)}$ be as in (1.41), where $A$ and $B$ are invertible. Define the invertible matrix

$$D_i = \begin{pmatrix} B_i^{-1} & B_i^{-1}C_i \\ 0 & A_i \end{pmatrix} \in \mathbb{F}_q^{n_i\times n_i},$$

for $i \in [\ell]$, and set $D = \mathrm{Diag}(D_1, D_2, \ldots, D_\ell) \in \mathbb{F}_q^{n\times n}$. Then

$$BGD = (J_1, Q_1, J_2, Q_2, \ldots, J_\ell, Q_\ell) \in \mathbb{F}_{q^m}^{k\times n},$$

where $Q_i \in \mathbb{F}_{q^m}^{k\times(n_i-k_i)}$, for $i \in [\ell]$, and

$$(Q_1, Q_2, \ldots, Q_\ell) = BPA + C \in \mathbb{F}_{q^m}^{(n-k)\times n}.$$

Finally, we have that $BGD \in \mathbb{F}_{q^m}^{k\times n}$ is a systematic generator matrix of the $k$-dimensional linear code $\mathcal{C}D \subseteq \mathbb{F}_{q^m}^n$.

Now, if $\mathcal{C}$ is MSRD, then by Definition 1.7, $\mathcal{C}D$ is MDS, and therefore, $BPA + C \in \mathbb{F}_{q^m}^{(n-k)\times n}$ is superregular [110, Ch. 11, Th. 8].

Conversely, if $BPA + C \in \mathbb{F}_{q^m}^{(n-k)\times n}$ is superregular, then we have that $\mathcal{C}D$ is MDS [110, Ch. 11, Th. 8]. Since any invertible matrix in $\mathbb{F}_q^{n_i\times n_i}$ is a product of matrices of the form of $D_i$, we deduce that $\mathcal{C}$ is MSRD by Definition 1.7. □

Observe that, in the classical Hamming-metric case, Theorem 1.7 recovers the well known characterization of systematic generator matrices of MDS codes.

Assume that $\mathbf{n} = (1, 1, \ldots, 1)$ and that $m = 1$. For each $i \in [\ell]$, since $n_i = 1$ and $0 \leq k_i \leq 1$, then either $k_i = 0$ or $n_i - k_i = 0$. This means that $C = 0$ necessarily and $B \in \mathbb{F}_q^{k\times k}$ and $A \in \mathbb{F}_q^{(n-k)\times(n-k)}$ are invertible diagonal matrices. Now, $BPA + C = BPA$ is superregular if, and only if, $P$ is superregular, since $A$ and $B$ are invertible diagonal matrices. Hence in this case, Theorem 1.7 says that $\mathcal{C}$ is MDS if, and only if, $P$ is superregular.

In the rank-metric case, Theorem 1.7 recovers the characterization of systematic generator matrices of MRD codes obtained in [132].

## 1.6 Constructing New Codes from Old Codes

In this section, we will explore constructions of new codes from old ones. We will investigate dual codes, punctured codes, shortened codes, and subfield subcodes.

Define the dual code of a linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ as usual:

$$\mathcal{C}^\perp = \left\{ \mathbf{d} \in \mathbb{F}_{q^m}^n \mid \mathbf{c}\mathbf{d}^\intercal = 0, \text{ for all } \mathbf{c} \in \mathcal{C} \right\}. \tag{1.42}$$

The next theorem follows immediately from Theorem 1.6.

**Theorem 1.8.** A linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is MSRD with respect to a given length partition and subfield $\mathbb{F}_q$ if, and only if, so is its dual $\mathcal{C}^\perp \subseteq \mathbb{F}_{q^m}^n$.

We illustrate Theorem 1.8 with the sum-rank repetition code from Example 1.5.

**Example 1.8 (The sum-rank single-parity-check code).** Let the notation and assumptions be as in Example 1.5. Using the language of generator and parity-check matrices, we know that the sum-rank repetition code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ has the generator matrix

$$G = \left(\boldsymbol{\alpha}^{(n_1)}, \boldsymbol{\alpha}^{(n_2)}, \ldots, \boldsymbol{\alpha}^{(n_\ell)}\right) \in \mathbb{F}_{q^m}^{1\times n}.$$

The reader may verify that a parity-check matrix of $\mathcal{C}$, that is, a generator matrix of its dual $\mathcal{C}^\perp \subseteq \mathbb{F}_{q^m}^n$, is

$$H = \begin{pmatrix} I_{n_1} & 0 & \ldots & 0 & 0 & \alpha_{n_\ell}^{-1}(\boldsymbol{\alpha}^{(n_1)})^\intercal \\ 0 & I_{n_2} & \ldots & 0 & 0 & \alpha_{n_\ell}^{-1}(\boldsymbol{\alpha}^{(n_2)})^\intercal \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & I_{n_{(\ell-1)}} & 0 & \alpha_{n_\ell}^{-1}(\boldsymbol{\alpha}^{(n_{\ell-1})})^\intercal \\ 0 & 0 & \cdots & 0 & I_{(n_\ell)-1} & \alpha_{n_\ell}^{-1}(\boldsymbol{\alpha}^{((n_\ell)-1)})^\intercal \end{pmatrix},$$

where $I_{n_i}$ is the $n_i \times n_i$ identity matrix. It can be verified directly that $\mathrm{d}_{SR}\left(\mathcal{C}^\perp\right) = 2$. Since $\dim\left(\mathcal{C}^\perp\right) = n-1$, we deduce that $\mathcal{C}^\perp$ is also an MSRD code.

We now explore puncturing and shortening. One may consider conceptually more general definitions of puncturing and shortening in the context of the sum-rank metric [20], [118]. For simplicity, in this monograph we restrict ourselves to classical puncturing and shortening.

**Definition 1.9.** Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a linear code, and let $I = \{i_1, i_2, \ldots, i_t\}$, where $t > 0$ and $1 \leq i_1 < i_2 < \ldots < i_t \leq n$. We define the linear codes

$$\mathcal{C}_I = \{(c_{i_1}, c_{i_2}, \ldots, c_{i_t}) \mid (c_1, c_2, \ldots, c_n) \in \mathcal{C}\} \subseteq \mathbb{F}_{q^m}^t, \text{ and}$$
$$\mathcal{C}^I = \{(c_{i_1}, c_{i_2}, \ldots, c_{i_t}) \mid (c_1, c_2, \ldots, c_n) \in \mathcal{C}, \text{ and } c_i = 0 \text{ if } i \notin I\} \subseteq \mathbb{F}_{q^m}^t,$$

called, respectively, the restricted code and shortened code of $\mathcal{C}$ on the coordinates in $I$. We also say that $\mathcal{C}_I$ is the punctured code of $\mathcal{C}$ in the coordinates in $J = [n] \setminus I$.

Punctured and shortened codes behave similarly with respect to the sum-rank metric and the Hamming metric, as shown in the following proposition. However, one needs to be careful about length partitions.

**Proposition 1.10.** Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a linear code with $d = \mathrm{d}_{SR}(\mathcal{C})$. Let $I \subseteq [n]$ be a subset such that $|I| > n - d \geq 0$ (thus $|I| \geq \dim(\mathcal{C})$ by the Singleton bound). Then the following hold:

1. $\dim(\mathcal{C}_I) = \dim(\mathcal{C})$ and $\mathrm{d}_{SR}(\mathcal{C}_I) \geq d - (n - |I|)$, and
2. $\dim\left(\mathcal{C}^I\right) \geq \dim(\mathcal{C}) - (n - |I|)$ and $\mathrm{d}_{SR}\left(\mathcal{C}^I\right) \geq d$,

for the length-$|I|$ sum-rank partition $(|I_1|, |I_2|, \ldots, |I_\ell|)$, where $I_i$ is the set $I$ restricted to the $i$th block of $n_i$ coordinates, for $i \in [\ell]$, and omitting positions where $|I_i| = 0$.

*Proof.* First, the statements on dimensions are general classical results using the minimum Hamming distance of $\mathcal{C}$, and hold because, by (1.23),

$$\mathrm{d}_H(\mathcal{C}) \geq d > n - |I|.$$

The statements on minimum sum-rank distances in items 1 and 2 need a proof but it is similar to the case of the Hamming metric. We show this for item 1. For $\mathbf{c} \in \mathcal{C}$, denote by $\mathbf{c}_I \in \mathcal{C}_I$ the restriction of $\mathbf{c}$ to the coordinates in $I$. Set

$$M_{\boldsymbol{\alpha}}^{\mathbf{n}}(\mathbf{c}) = (C_1, C_2, \ldots, C_\ell) \in \mathbb{F}_q^{m \times n_1} \times \mathbb{F}_q^{m \times n_2} \times \cdots \times \mathbb{F}_q^{m \times n_\ell},$$

where $C_i \in \mathbb{F}_q^{m \times n_i}$, for $i \in [\ell]$. The restricted codeword $\mathbf{c}_I \in \mathcal{C}_I$ corresponds to the $\ell$-tuple of matrices $(C_{1I_1}, C_{2I_2}, \ldots, C_{\ell I_\ell})$, where $C_{iI_i} \in \mathbb{F}_q^{m \times |I_i|}$ is the restriction of the matrix $C_i$ to the columns in $I_i$, for $i \in [\ell]$. Since deleting $n_i - |I_i|$ columns from $C_i$ may only reduce its rank by $n_i - |I_i|$, for $i \in [\ell]$, we deduce that

$$\mathrm{wt}_{SR}(\mathbf{c}_I) \geq \mathrm{wt}_{SR}(\mathbf{c}) - \left(\sum_{i=1}^{\ell} (n_i - |I_i|)\right) = \mathrm{wt}_{SR}(\mathbf{c}) - (n - |I|),$$

and we are done. □

The following result on puncturing and shortening linear MSRD codes follows immediately.

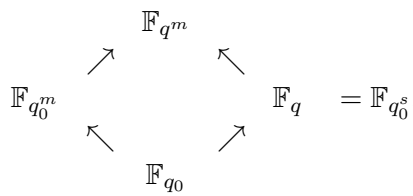
**Corollary 1.9.** Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a $k$-dimensional linear MSRD code. Let $I \subseteq [n]$ be a subset such that $|I| \geq k$, which in this case is equivalent to $|I| > n - d$. Then $\mathcal{C}_I$ and $\mathcal{C}^I$ are linear MSRD codes in $\mathbb{F}_{q^m}^{|I|}$, for the length partition $(|I_1|, |I_2|, \ldots, |I_\ell|)$, omitting zero positions, where $I_i$ is the set $I$ restricted to the $i$th block of $n_i$ coordinates, for $i \in [\ell]$. We also have

1. $\dim(\mathcal{C}_I) = \dim(\mathcal{C})$ and $\mathrm{d}_{SR}(\mathcal{C}_I) = \mathrm{d}_{SR}(\mathcal{C}) - (n - |I|)$, and
2. $\dim\left(\mathcal{C}^I\right) = \dim(\mathcal{C}) - (n - |I|)$ and $\mathrm{d}_{SR}\left(\mathcal{C}^I\right) = \mathrm{d}_{SR}(\mathcal{C})$.

We conclude this section by discussing subfield subcodes as in [124]. To this end, we will consider a subfield $\mathbb{F}_{q_0} \subseteq \mathbb{F}_q$, which is equivalent to considering $q = q_0^s$, for some positive integer $s$. Therefore, we have two finite-field extensions

$$\mathbb{F}_{q_0} \subseteq \mathbb{F}_{q_0^m} \quad \text{and} \quad \mathbb{F}_q \subseteq \mathbb{F}_{q^m}, \quad \text{where } q = q_0^s \text{ and } s \geq 1.$$

To relate these four fields, the following directed graph might be helpful, where $K \longrightarrow L$ means that $K$ is a subfield of $L$:




If we take an ordered basis $\boldsymbol{\alpha}_0 \in \mathbb{F}_{q_0^m}^m$ of $\mathbb{F}_{q_0^m}$ over $\mathbb{F}_{q_0}$, then we may consider the total matrix representation map (Definition 1.4)

$$M_{\boldsymbol{\alpha}_0}^{\mathbf{n}} : \mathbb{F}_{q_0^m}^n \longrightarrow \mathbb{F}_{q_0}^{m \times n_1} \times \mathbb{F}_{q_0}^{m \times n_2} \times \cdots \times \mathbb{F}_{q_0}^{m \times n_\ell}. \tag{1.43}$$

Using $M_{\boldsymbol{\alpha}_0}^{\mathbf{n}}$, the sum-rank metric in $\mathbb{F}_{q_0^m}^n$ coincides with that in $\mathbb{F}_{q_0}^{m \times n_1} \times \mathbb{F}_{q_0}^{m \times n_2} \times \cdots \times \mathbb{F}_{q_0}^{m \times n_\ell}$. This motivates the following definition.

**Definition 1.10.** Given a (linear or nonlinear) code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, we define its subfield subcode over $\mathbb{F}_{q_0^m}$ as the code

$$\mathcal{C}|_{q_0^m} = \mathcal{C} \cap \mathbb{F}_{q_0^m}^n.$$

The following bound on the minimum sum-rank distance of subfield subcodes was given in [124].

**Proposition 1.11.** For any (linear or nonlinear) code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, we have

$$\mathrm{d}_{SR}\left(\mathcal{C}|_{q_0^m}\right) \geq \mathrm{d}_{SR}(\mathcal{C}),$$

where the minimum sum-rank distance $\mathrm{d}_{SR}\left(\mathcal{C}|_{q_0^m}\right)$ is considered via the map $M_{\boldsymbol{\alpha}_0}^{\mathbf{n}}$ as in (1.43).

*Proof.* This follows directly from Theorem 1.2, by noting that an invertible matrix in $\mathbb{F}_{q_0}^{n_i \times n_i}$ is also an invertible matrix in $\mathbb{F}_q^{n_i \times n_i}$, for $i \in [\ell]$. □

For linear codes, we have the following bound on dimensions given by Delsarte [40], which holds regardless of the metric.

**Proposition 1.12.** Given a linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, the subfield subcode $\mathcal{C}|_{q_0^m} \subseteq \mathbb{F}_{q_0^m}^n$ is $\mathbb{F}_{q_0^m}$-linear, and if $q = q_0^s$, then

$$\dim_{\mathbb{F}_{q_0^m}}\left(\mathcal{C}|_{q_0^m}\right) \geq n - s\left(n - \dim_{\mathbb{F}_{q^m}}(\mathcal{C})\right).$$

In Section 6.2, we will describe sum-rank BCH codes [114], which are subfield subcodes of certain linearized Reed–Solomon codes (Section 2), and for which we may give tighter bounds on the dimension than Delsarte's bound (Proposition 1.12).

# Index