ALGEBRAIC CODES FOR RANDOM LINEAR NETWORK CODING

by

Maximilien Gadouleau

A Dissertation

Presented to the Graduate Committee

of Lehigh University

in Candidacy for the Degree of

Doctor of Philosophy

in

Computer Engineering

Lehigh University

April, 2009

This dissertation is accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

Date

Dissertation Advisor: Zhiyuan Yan, PhD
Assistant Professor, ECE
Lehigh University

Accepted Date

Tiffany Li, PhD
Associate Professor, ECE
Lehigh University

Meghanad Wagh, PhD
Associate Professor, ECE
Lehigh University

Bruce Dodson, PhD
Associate Professor, Mathematics
Lehigh University

Mario Blaum, PhD
Lecturer, Electrical Engineering
Santa Clara University

Acknowledgments

I would like to thank my Jennifer, to whom this dissertation is dedicated.

I also wish to thank my advisor Professor Zhiyuan Yan. I truly enjoyed working with such a researcher and hope our collaboration will remain as fruitful in the future.

I would like to thank the members of my doctoral committee for their time and interesting comments.

Finally, I would like to thank my friends and family for their support.

Contents

List of Tables

List of Figures

Abstract

This dissertation is devoted to the study of algebraic codes proposed for error control in random linear network coding, namely rank metric codes, subspace codes, and constant-dimension codes (CDCs). Rank metric codes have further applications in data storage, cryptography, and space-time coding.

Chapter 2 investigates the properties of rank metric codes through a geometric approach. We study the fundamental problems of sphere packing and sphere covering in the rank metric, and our results provide guidelines on the design of rank metric codes.

In Chapter 3, we derive the MacWilliams identity and related identities for rank metric codes which parallel the binomial and power moment identities derived for codes with the Hamming metric. These identities are fundamental relationships between linear rank metric codes and their dual.

In Chapter 4, we introduce a new approach to studying CDCs. We show that optimal CDCs correspond to optimal constant-rank codes over sufficiently large extension fields, hence the problem of determining the cardinality of an optimal CDC can be solved by studying constant-rank codes instead. Constant-rank codes are also a useful tool to investigate the decoder error probability (DEP) of rank metric codes. We thus show that the maximum DEP of rank metric codes used

over an equal row or an equal column space channel decreases exponentially with t^2, where t is the error correction capability of the code.

In Chapter 5, we investigate the packing and covering properties of CDCs and subspace codes. We first construct a new class of CDCs and investigate the covering properties of CDCs. We then prove that optimal packing CDCs are nearly optimal packing subspace codes for both metrics. However, optimal covering CDCs can be used to construct asymptotically optimal covering subspace codes only for the injection metric. We finally determine the DEP of any lifting of a rank metric code over a symmetric operator channel.

Chapter 1

Introduction

Network coding [1,2] is a novel, elegant, and efficient approach to transmitting data across a communication network. Suppose a source node sends a set of packets, grouped into what are referred to as generations, to several destination nodes. Using traditional routing, the intermediate nodes only store and forward the packets towards their destinations with no data processing. On the other hand, network coding allows the intermediate nodes to combine the different packets of the same generation. Using network coding can achieve the highest possible throughput given the network topology, which in general is greater than the one achievable solely by routing [2]. Since only linear combinations of packets over a large enough field are needed to achieve this throughput [3], we consider linear network coding only. Fixing the linear combinations at each node and for each set of source and destination nodes requires the knowledge of the entire network topology and result in a highly rigid network code. Random linear network coding [4–6] was proposed to tackle these difficulties. In random linear network coding, the linear combinations of the packets operated at each node are chosen at random and independently of

the network topology. With the help of little overhead (in order to keep track of the linear combinations undergone by the generation of packets), random linear network coding achieves the maximum throughput with high probability.

While random linear network coding has proved to be a powerful tool for disseminating information in networks, it is highly susceptible to errors caused by various sources such as noise, malicious or malfunctioning nodes, or insufficient min-cut. If received packets are linearly combined at random to deduce the transmitted message, even a single error in one erroneous packet could render the entire transmission useless. Thus, error control for random linear network coding is critical and has received growing attention recently. Error control schemes proposed for random linear network coding assume two types of transmission models: some (see, for example, [7, 8]) depend on and take advantage of the underlying network topology or the particular linear network coding operations performed at various network nodes; others [9, 10] assume that the transmitter and receiver have no knowledge of such channel transfer characteristics. The contrast is similar to that between coherent and noncoherent communication systems.

Viewing a generation of packets as a matrix whose rows are the packets, we can determine a channel model for random linear network coding. Suppose an intermediate node receives some packets, gathered into an input matrix. The node then performs linear combinations on the rows of the input matrix and transmits the obtained output matrix. Although the output matrix is not necessarily equal to the input matrix, they both have the same row space. Therefore, random linear network coding can be viewed as transmitting a subspace of a vector space over a finite field [9]. The errors occurring on the network can hence be viewed as modifications of the transmitted subspace. Two types of modifications are considered: the first

type, referred to as an erasure, is the loss of a dimension; the second type, referred to as an error, is the injection of another dimension to the subspace. The transmission of packets using random linear network coding can hence be modeled as transmitting a subspace over an *operator channel* [9] which performs errors and erasures on the input subspace. Error correction in noncoherent random linear network coding can thus be treated as a coding problem where codewords are linear subspaces and codes are subsets of the projective space of a vector space over a finite field. Such codes are referred to as subspace codes. The metric used to characterize the errors occurring on the network is the so-called subspace metric [9], or in the case of adversarial channels, the injection metric [11]. Both these metrics can be defined in terms of the numbers of errors and erasures required to obtain one subspace from another.

Similar to codes defined over complex Grassmannians for noncoherent multiple-antenna channels, codes defined in Grassmannians associated with the vector space play a significant role in error control for noncoherent random linear network coding; such codes are also referred to as constant-dimension codes (CDCs) [9]. CDCs have several interesting properties. First, the minimum subspace distance of a CDC is equal to twice its minimum injection distance [11], and hence CDCs can be used with either metric. Second, the decoding procedure is simplified, as a fixed number of linearly independent packets are required to perform the decoding. Third, a class of nearly optimal CDCs is given in [10] by lifting rank metric codes.

A rank metric code [12–14] can be viewed as a set of matrices over a finite field where the distance between two codewords, referred to as the rank distance, is the rank of their difference. The theory of rank metric codes shares many similarities with the theory of Hamming metric codes [12, 15]. In particular, a Singleton bound and a class of Reed-Solomon like codes achieving this bound, referred to as Gabidulin

codes, are given independently in [12–14]. A matrix can be lifted into a subspace of fixed dimension [10], and hence a rank metric code can be lifted into a CDC. Since the injection and the subspace distances between two lifted matrices are related to their rank distance, the minimum distances of the lifting of a rank metric code are related to that of the original rank metric code. Thus error control in random linear network coding using CDCs can be turned into a rank metric problem [10]. In particular, liftings of Gabidulin codes are optimal CDC up to a scalar [9], and decoding the errors occurring on the operator channel can be achieved using a generalized rank distance decoder for Gabidulin codes [10].

This dissertation is devoted to the study of codes used for error control in random linear network coding, namely rank metric codes, subspace codes, and CDCs. The rest of the dissertation is organized as follows.

Chapter 2 investigates properties of codes with the rank metric. First, we determine the maximum cardinality of a rank metric code with a given minimum distance and derive its asymptotic behavior. Then, we derive some fundamental combinatorial and geometric properties of the rank metric. Using these properties, we study sphere covering properties of rank metric codes. We derive asymptotically tight lower and upper bounds on the minimum cardinality of a code with a given rank covering radius. We also design classes of covering codes optimal up to a scalar. We finally study the covering properties of linear rank metric codes, and we determine the covering radius of generalized Gabidulin codes.

The MacWilliams identity, which relates the weight distribution of a code to that of its dual code, is useful in determining the weight distribution of codes. In Chapter 3, we derive the MacWilliams identity for linear codes with the rank metric,

and our identity has a different form than that by Delsarte. Using our MacWilliams identity, we also derive related identities for rank metric codes, which parallel the binomial and power moment identities derived for codes with the Hamming metric.

CDCs have recently received attention due to their significance to error control in noncoherent random linear network coding. What the maximal cardinality of any constant-dimension code with finite dimension and minimum distance is and how to construct optimal CDCs that achieve the maximal cardinality both remain open research problems. In Chapter 4, we introduce a new approach to solving these two problems. We first introduce constant-rank codes and establish a connection between constant-rank codes and CDCs. Via this connection, we show that optimal CDCs correspond to optimal constant-rank codes over sufficiently large extension fields. As such, the two aforementioned problems are equivalent to determining the maximum cardinality of constant-rank codes and to constructing optimal constant-rank codes, respectively. To this end, we derive bounds on the maximum cardinality of a constant-rank code with a given minimum rank distance, propose explicit constructions of optimal or asymptotically optimal constant-rank codes, and establish asymptotic bounds on the maximum rate of a constant-rank code. We finally study the decoder error probability (DEP) of rank metric codes using a bounded rank distance decoder. We derive asymptotically tight upper bounds on the DEP of rank metric codes used over an equal row or an equal column space channel, and we determine the exact DEP of maximum rank distance codes used over an equal row space channel.

Subspace codes, and in particular CDCs, have been proposed for two types of error control in random linear network coding. They can either correct errors and erasures inherent to random linear network coding operations by using the subspace

metric, or they can correct errors and erasures due to an adversary injecting packets on the network by using the injection metric. In Chapter 5, we first construct a new class of CDCs, referred to as augmented KK codes, whose cardinalities are greater than previously proposed CDCs in most cases and propose a low-complexity decoding algorithm for these codes. We also investigate the covering properties of CDCs. We first derive bounds on the minimum cardinality of a CDC with a given covering radius and then determine the asymptotic behavior of this quantity. Moreover, we show that liftings of rank metric codes have the highest possible covering radius, and construct good covering CDCs by permuting liftings of rank metric codes. We then study the packing and covering properties of subspace codes using either metric. We first determine some fundamental geometric properties of the projective space. Using these results, we derive bounds on the cardinalities of packing and covering subspace codes, and we determine the asymptotic rate of optimal packing and optimal covering subspace codes for both metrics. We thus show that optimal packing CDCs are optimal packing subspace codes up to a scalar for both metrics if and only if their dimension is half of their length. Hence, CDCs can be used for correcting errors inherent to the network or caused by an adversary with only a limited rate loss. However, we show that optimal covering CDCs can be used to construct asymptotically optimal covering subspace codes only for the injection metric. These results do not only show the difference between the two metrics, but they also illustrate the significance of CDCs. Using geometric properties of the projective space, we finally derive asymptotically tight upper bounds on the DEP of any CDC obtained by lifting a rank metric code using either a bounded subspace distance or a bounded injection distance decoder.

Chapter 2

Properties of Rank Metric Codes

2.1 Introduction

Although the rank has long been known to be a metric (see, for example, [16]), the rank metric was first considered for error control codes by Delsarte [12]. The potential applications of rank metric codes to wireless communications [17, 18], public-key cryptosystems [19], and storage equipments [14, 20] have motivated a steady stream of works [13, 14, 20–30] that focus on their properties. The majority of previous works focus on rank distance properties, code construction, and efficient decoding of rank metric codes, and the seminal works in [12–14] have made significant contribution to these topics. Independently in [12–14], a Singleton bound (up to some variations) on the minimum rank distance of codes was established, and a class of codes achieving the bound with equality was constructed. We refer to this class of codes as Gabidulin codes henceforth. In [12, 13], analytical expressions to compute the weight distribution of linear codes achieving the Singleton bound with equality

were also derived. In [20], it was shown that Gabidulin codes are optimal for correcting crisscross errors (referred to as lattice-pattern errors in [20]). In [14], it was shown that Gabidulin codes are also optimal in the sense of a Singleton bound in crisscross weight, a metric considered in [14, 22, 31] for crisscross errors. Decoding algorithms were introduced for Gabidulin codes in [13, 14, 32, 33].

Both packing and covering properties are significant for error control codes, and packing and covering radii are basic geometric parameters of a code, important in several respects [34]. For instance, the covering radius can be viewed as a measure of performance: if the code is used for error correction, then the covering radius is the maximum weight of a correctable error vector [35]; if the code is used for data compression, then the covering radius is a measure of the maximum distortion [35]. The Hamming packing and covering radii of error control codes have been extensively studied (see, for example, [36,37]), whereas the rank packing and covering radii have received relatively little attention. It was shown that nontrivial perfect rank metric codes do not exist in [21, 27, 38]. In [23], a sphere covering bound for rank metric codes was introduced. Generalizing the concept of rank covering radius, the multi-covering radii of codes with the rank metric were defined in [39]. Bounds on the volume of balls with rank radii were also derived [30].

In this chapter, we investigate packing and covering properties of rank metric codes. The main contributions of this chapter are:

- In Section 2.3, we investigate the packing properties of rank metric codes and also derive the asymptotic maximum code rate for a code with given relative minimum rank distance.

- In Section 2.4, we first derive some instrumental combinatorial properties.

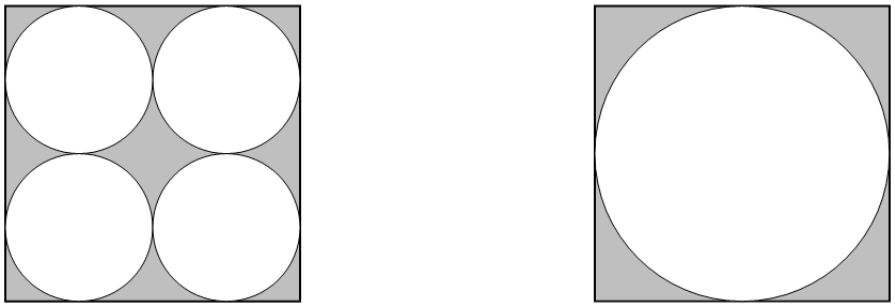

Figure 2.1: Sphere packing.

We then introduce the concept of elementary linear subspace (ELS) which is the counterpart in the rank metric of a subset of coordinates. We finally investigate properties of balls with rank radii. In particular, we derive both upper and lower bounds on the volume of balls with given rank radii, and our bounds are tighter than their respective counterparts in [30]. These technical results are used later in our investigation of properties of rank metric codes.

- In Section 2.5, we first derive both upper and lower bounds on the minimal cardinality of a code with given length and rank covering radius. Our new bounds are tighter than the bounds introduced in [23]. We also establish additional sphere covering properties for linear rank metric codes, and prove that some classes of rank metric codes have maximal covering radius. Finally, we establish the asymptotic minimum code rate for a code with given relative covering radius.

The sphere packing problem we consider is as follows: given a finite field GF(q^m), length n, and radius r, what is the maximum number of non-intersecting balls with radius r that can be packed into GF(q^m)^n? This problem is illustrated in

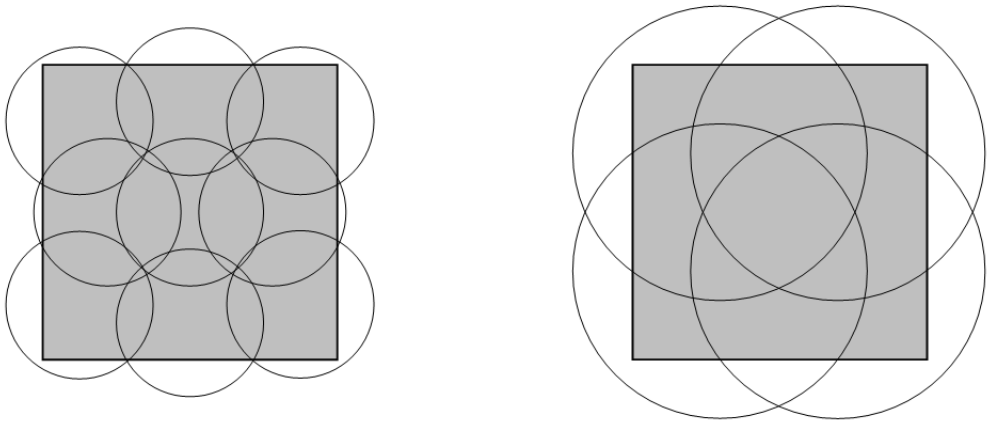

Figure 2.2: Sphere covering.

Figure 2.1 for different sphere radii, where the space is represented as a grey square, and the non-intersecting spheres as white circles. The sphere packing problem is equivalent to finding the maximum cardinality of a code over $\mathrm{GF}(q^m)$ with length n and minimum distance $d \geq 2r + 1$: the spheres of radius r centered at the codewords of such a code do not intersect one another. Furthermore, when these non-intersecting spheres centered at all codewords cover the *whole* space, the code is called a perfect code.

The covering radius ρ of a code $\mathcal{C}$ with length n over $\mathrm{GF}(q^m)$ is defined to be the smallest integer ρ such that all vectors in the space $\mathrm{GF}(q^m)^n$ are within distance ρ of some codeword in $\mathcal{C}$ [37]. It is the maximal distance from any vector in $\mathrm{GF}(q^m)^n$ to the code $\mathcal{C}$. That is, $\rho = \max_{\mathbf{x} \in \mathrm{GF}(q^m)^n} \{d(\mathbf{x}, \mathcal{C})\}$. Also, if $\mathcal{C} \subset \mathcal{C}'$, then the covering radius of $\mathcal{C}$ is no less than the minimum distance of $\mathcal{C}'$. Finally, a code $\mathcal{C}$ with length n and minimum distance d is called a maximal code if there does not exist any code $\mathcal{C}'$ with the same length and minimum distance such that $\mathcal{C} \subset \mathcal{C}'$. A maximal code has covering radius $\rho \leq d - 1$. The sphere covering problem for the rank metric

can be stated as follows: given an extension field GF(q^m), length n, and radius ρ, we want to determine the minimum number of balls of rank radius ρ which cover GF(q^m)^n entirely. It is illustrated in Figure 2.2 for different sphere radii, where the space (pictured as a grey square) is entirely covered by spheres (depicted as white circles). The sphere covering problem is equivalent to finding the minimum cardinality of a code over GF(q^m) with length n and rank covering radius ρ.

2.2 The rank metric

Consider an n-dimensional vector $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}) \in \mathrm{GF}(q^m)^n$. The field GF($q^m$) may be viewed as an m-dimensional vector space over GF(q). The rank weight of $\mathbf{x}$, denoted as $\mathrm{rk}(\mathbf{x})$, is defined to be the *maximum* number of coordinates in $\mathbf{x}$ that are linearly independent over GF(q) [13]. Note that all ranks are with respect to GF(q) unless otherwise specified. The coordinates of $\mathbf{x}$ thus span a linear subspace of GF(q^m), denoted as $S(\mathbf{x})$ or $S(x_0, x_1, \ldots, x_{n-1})$, with dimension equal to $\mathrm{rk}(\mathbf{x})$. For any basis B_m of GF(q^m) over GF(q), each coordinate of $\mathbf{x}$ can be expanded to an m-dimensional column vector over GF(q) with respect to B_m. The rank weight of $\mathbf{x}$ is hence the rank of the $m \times n$ matrix over GF(q) obtained by expanding all the coordinates of $\mathbf{x}$.

Since the rank weight can be defined from either a matrix perspective or a vector viewpoint, both the matrix form [12, 14] and the vector form [13] for rank metric codes have been considered in the literature and shall be considered throughout this dissertation. In this chapter, we shall mostly use the vector form.

For all $\mathbf{x}, \mathbf{y} \in \mathrm{GF}(q^m)^n$, it is easily verified that $d_{\mathrm{R}}(\mathbf{x}, \mathbf{y}) \stackrel{\mathrm{def}}{=} \mathrm{rk}(\mathbf{x} - \mathbf{y})$ is a metric over GF(q^m)^n [13], referred to as the *rank metric* henceforth. The *minimum rank*

distance of a code $\mathcal{C}$, denoted as $d_{\mathrm{R}}(\mathcal{C})$, is simply the minimum rank distance over all possible pairs of distinct codewords. When there is no ambiguity about $\mathcal{C}$, we denote the minimum rank distance as d_{R}. A code with a minimum rank distance d_{R} can correct all errors with rank up to $t = \lfloor (d_{\mathrm{R}} - 1)/2 \rfloor$.

Combining the bounds in [13] and [40] and generalizing slightly to account for nonlinear codes, we can show that the cardinality K of a code $\mathcal{C}$ over $\mathrm{GF}(q^m)$ with length n and minimum rank distance d_{R} satisfies $K \leq \min\left\{q^{m(n-d_{\mathrm{R}}+1)}, q^{n(m-d_{\mathrm{R}}+1)}\right\}$. We refer to this bound as the Singleton bound for codes with the rank metric, and refer to codes that attain the Singleton bound as maximum rank distance (MRD) codes. We refer to MRD codes over $\mathrm{GF}(q^m)$ with length $n \leq m$ and with length $n > m$ as Class-I and Class-II MRD codes respectively. For any given parameter set n, m, and d_{R}, explicit construction for linear or nonlinear MRD codes exists. For $n \leq m$ and $d_{\mathrm{R}} \leq n$, generalized Gabidulin codes [26] constitute a *subclass* of linear Class-I MRD codes. For $n > m$ and $d_{\mathrm{R}} \leq m$, a Class-II MRD code can be constructed by transposing a generalized Gabidulin code of length m and minimum rank distance d_{R} over $\mathrm{GF}(q^n)$, although this code is not necessarily linear over $\mathrm{GF}(q^m)$. When $n = lm$ ($l \geq 2$), linear Class-II MRD codes of length n and minimum distance d_{R} can be constructed by a cartesian product $\mathcal{G}^l \stackrel{\mathrm{def}}{=} \mathcal{G} \times \ldots \times \mathcal{G}$ of an (m, k) linear Class-I MRD code $\mathcal{G}$ [40]. For all q, $1 \leq d \leq r \leq n \leq m$, the number of codewords of rank r in an $(n, n-d+1, d)$ linear MRD code over $\mathrm{GF}(q^m)$ is given by [13]

$$M(q, m, n, d, r) \stackrel{\mathrm{def}}{=} \begin{bmatrix} n \\ r \end{bmatrix} \sum_{j=d}^{r} (-1)^{r-j} \begin{bmatrix} r \\ j \end{bmatrix} q^{(r-j)(r-j-1)/2} \left(q^{m(j-d+1)} - 1\right). \tag{2.1}$$

The vector space $\mathrm{GF}(q)^{m \times n}$ endowed with the rank metric constitutes a metric association scheme [12]. Its *valencies* [41] are given by $N_{\mathrm{R}}(q, m, n, u) = \begin{bmatrix} n \\ u \end{bmatrix} \alpha(m, u)$,

where $\alpha(m,0)=1$ and $\alpha(m,u)=\prod_{i=0}^{u-1}(q^m-q^i)$ for $u\geq 1$ and $\begin{bmatrix} n \\ u \end{bmatrix}=\frac{\alpha(n,u)}{\alpha(u,u)}$ is the Gaussian polynomial [42]. They represent the number of vectors at rank distance u from any vector in $\mathrm{GF}(q^m)^n$. The *intersection numbers* $J_{\mathrm{R}}(q,m,n,u,s,d)$ for rank metric codes are the volumes of the intersection of two balls with rank radii u and s and distance between their centers d and are critical to association schemes. They have the following basic properties [43]:

$$N_{\mathrm{R}}(q,m,n,d)J_{\mathrm{R}}(q,m,n,u,s,d) = N_{\mathrm{R}}(q,m,n,u)J_{\mathrm{R}}(q,m,n,d,s,u) \quad (2.2)$$

$$\sum_{u=0}^{n} J_{\mathrm{R}}(q,m,n,u,s,d) = N_{\mathrm{R}}(q,m,n,s). \quad (2.3)$$

2.3 Packing properties of rank metric codes

It can be shown that the cardinality K of a code $\mathcal{C}$ over $\mathrm{GF}(q^m)$ with length n and minimum rank distance d satisfies $K\leq \min\left\{q^{m(n-d+1)},q^{n(m-d+1)}\right\}$. We refer to this bound as the Singleton bound for codes with the rank metric, and refer to codes that attain the Singleton bound as maximum rank distance (MRD) codes. We remark that special cases of this more general Singleton bound were proposed in [13,14,40].

For any given parameter set n, m, and d, explicit construction for linear or nonlinear MRD codes exists. For $n\leq m$ and $d\leq n$, generalized Gabidulin codes [26] can be constructed. For $n>m$ and $d\leq m$, an MRD code can be constructed by transposing a generalized Gabidulin code of length m and minimum rank distance d over $\mathrm{GF}(q^n)$, although this code is not necessarily linear over $\mathrm{GF}(q^m)$. When $n=lm$ $(l\geq 2)$, linear MRD codes of length n and minimum distance d can be constructed by a cartesian product $\mathcal{G}^l$ of an (m,k) generalized Gabidulin code $\mathcal{G}$. Although maximum distance separable codes, which attain the Singleton bound for the Hamming metric, exist only for limited block length over any given field, MRD

codes can be constructed for any block length n and minimum rank distance d over arbitrary fields $\mathrm{GF}(q^m)$. This has significant impact on the packing properties of rank metric codes as explained below.

For the Hamming metric, although nontrivial perfect codes do exist, the optimal solution to the sphere packing problem is not known for all the parameter sets [36]. In contrast, for rank metric codes, although nontrivial perfect rank metric codes do not exist [21, 38], MRD codes provide an optimal solution to the sphere packing problem for any set of parameters. For given n, m, and r, let us denote the maximum cardinality among rank metric codes over $\mathrm{GF}(q^m)$ with length n and minimum distance $d = 2r + 1$ as $A_{\mathrm{R}}(q, m, n, d)$. Thus, for $d > \min\{n, m\}$, $A_{\mathrm{R}}(q, m, n, d) = 1$ and for $d \leq \min\{n, m\}$, $A_{\mathrm{R}}(q, m, n, d) = \min\left\{q^{m(n-d+1)}, q^{n(m-d+1)}\right\}$. Note that the maximal cardinality is achieved by MRD codes for all parameter sets. Hence, MRD codes admit the optimal solutions to the sphere packing problem for rank metric codes.

The performance of Hamming metric codes of large block length can be studied in terms of asymptotic bounds on the relative minimum distance in the limit of infinite block length. Next, we derive the asymptotic form of $A_{\mathrm{R}}(q, m, n, d)$ when both block length and minimum rank distance go to infinity. However, this cannot be achieved for finite m since the minimum rank distance is no greater than m. Thus, we consider the case where $\lim_{n\to\infty} \frac{n}{m} = \nu$, where ν is a constant.

Define $\delta \stackrel{\text{def}}{=} \lim_{n\to\infty} \frac{d}{n}$ and $a_{\mathrm{R}}(\nu, \delta) \stackrel{\text{def}}{=} \lim_{n\to\infty} \sup\left[\log_{q^{mn}} A_{\mathrm{R}}(q, m, n, \lfloor \delta n \rfloor)\right]$, where $a_{\mathrm{R}}(\nu, \delta)$ represents the maximum possible code rate of a code which has relative minimum distance δ as its length goes to infinity. We can thus determine the maximum possible code rate $a_{\mathrm{R}}(\nu, \delta)$ of a code.

Proposition 2.1. *For $0 \leq \delta \leq \min\{1, \nu^{-1}\}$, the existence of MRD codes for all*

parameter sets implies that $a_{\mathrm{R}}(\nu,\delta) = \min\{1-\delta, 1-\nu\delta\}$.

2.4 Technical results

2.4.1 Combinatorial results

In this section, we derive some combinatorial properties which will be very instrumental throughout this dissertation.

Lemma 2.2. *For* $0 \le u \le m$, $K_q q^{mu} < \alpha(m,u) \le q^{mu}$, *where* $K_q = \prod_{j=1}^{\infty}(1-q^{-j})$. *Also, for* $0 \le u \le m-1$, $\alpha(m,u) > \frac{q}{q-1}K_q q^{mu}$. *Finally, for* $0 \le u \le \lfloor m/2 \rfloor$, $\alpha(m,u) \ge \frac{q^2-1}{q^2}q^{mu}$.

Proof. The upper bound is trivial. We now prove the lower bounds. We have $\alpha(m,u) = q^{mu}\prod_{i=0}^{u-1}(1-q^{i-m}) > q^{mu}K_q$. The second lower bound follows from $\alpha(m,m-1) = \frac{q}{q-1}q^{-m}\alpha(m,m)$.

The third lower bound clearly holds for $m=0$ and $m=1$. Let us assume $m \ge 2$ henceforth and denote $\frac{q^{mu}}{\alpha(m,u)}$ as $D(m,u)$. It can be easily verified that $D(m,u)$ is an increasing function of u. Thus, it suffices to show that $D(m,\lfloor m/2 \rfloor) \le \frac{q^2}{q^2-1}$ for $m \ge 2$. First, if m is odd, $m = 2p+1$, it can be easily shown that $D(2p+1,p) < D(2p,p)$. Hence, we need to consider only the case where $m = 2p$, with $p \ge 1$. Let us further show that $D(2p,p)$ is a monotonically decreasing function of p since

$$\begin{aligned} D(2p+2,p+1) &= \frac{q^{2p+2}}{q^{2p+2}-1}\cdot\frac{q^{2p+2}}{q^{2p+2}-q}\cdot\frac{q^{2p+2}-q^{p+1}}{q^{2p+2}}D(2p,p) \\ &= \frac{q^{2p+1}(q^{2p+2}-q^{p+1})}{(q^{2p+1}-1)(q^{2p+2}-1)}D(2p,p). \end{aligned}$$

The maximum of $D(2p,p)$ is hence given by $D(2,1) = \frac{q^2}{q^2-1}$. □

It is worth noting that K_q above represents the fraction of invertible $m \times m$ matrices over GF(q) as m approaches infinity, and that K_q increases with q.

Corollary 2.3. *For $0 \leq t \leq n$, we have $\begin{bmatrix} n \\ t \end{bmatrix} < K_q^{-1} q^{t(n-t)}$.*

Proof. By definition, $\begin{bmatrix} n \\ t \end{bmatrix} = \alpha(n,t)/\alpha(t,t)$. Since $\alpha(n,t) \leq q^{nt}$ and by Lemma 2.2, $\alpha(t,t) > K_q q^{t^2}$, we obtain $\begin{bmatrix} n \\ t \end{bmatrix} < K_q^{-1} q^{t(n-t)}$. □

2.4.2 Elementary linear subspaces

It is a well-known fact in linear algebra (see, for example, [13]) that a vector $\mathbf{x}$ of rank $\mathrm{rk}(\mathbf{x}) \leq u$ can be represented as $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}) = (e_0, e_1, \ldots, e_{u-1})\mathbf{A}$, where $e_j \in \mathrm{GF}(q^m)$ for $j = 0, 1, \ldots, u-1$ and $\mathbf{A}$ is a $u \times n$ matrix over GF(q) of full rank u. The concept of elementary linear subspace can be introduced as a consequence of this representation. However, due to its usefulness in our approach we define the concept formally and study its properties below from a different perspective.

Definition 2.4 (Elementary linear subspace)**.** *A linear subspace V of $\mathrm{GF}(q^m)^n$ is said to be elementary if it has a basis B consisting of row vectors in $\mathrm{GF}(q)^n$. B is called an elementary basis of V. For $0 \leq v \leq n$, we define $E_v(q,m,n)$ as the set of all ELSs with dimension v in $\mathrm{GF}(q^m)^n$.*

In order to simplify notations, we denote $E_v(q,n) = E_v(q,1,n)$. By definition, a linear subspace V with dimension v is an ELS if and only if it is the row span of a $v \times n$ matrix $\mathbf{B}$ over GF(q) with full rank. Thus there exists a bijection between $E_v(q,m,n)$ and $E_v(q,n)$, and $|E_v(q,m,n)| = \begin{bmatrix} n \\ v \end{bmatrix}$. Also, it can be easily shown that a linear subspace V of $\mathrm{GF}(q^m)^n$ is an ELS if and only if there exists a basis consisting of vectors of rank 1 for V.

Next, we show that the properties of ELSs are similar to those of sets of coordinates.

Proposition 2.5. *For all $V \in E_v(q,m,n)$ there exists $\bar{V} \in E_{n-v}(q,m,n)$ such that $V \oplus \bar{V} = \mathrm{GF}(q^m)^n$, where $V \oplus \bar{V}$ denotes the direct sum of V and $\bar{V}$.*

Proof. Clearly, the ELS $\bar{V}$ having elementary basis $\bar{B}$ such that $B \cup \bar{B}$ is a basis of $\mathrm{GF}(q)^n$ satisfies $V \oplus \bar{V} = \mathrm{GF}(q^m)^n$. □

We say that $\bar{V}$ is an *elementary complement* of V. Even though an elementary complement always exists, we remark that it may not be unique.

The diameter of a code for the Hamming metric is defined in [36] as the maximum Hamming distance between two codewords. Similarly, we can define the rank diameter of a linear subspace.

Definition 2.6. *The rank diameter of a linear subspace L of $\mathrm{GF}(q^m)^n$ is defined to be the maximum rank among the vectors in L, i.e., $\delta(L) \stackrel{def}{=} \max_{\mathbf{x}\in L}\{\mathrm{rk}(\mathbf{x})\}$.*

Proposition 2.7. *For all $V \in E_v(q,m,n)$, $\delta(V) \leq v$. Furthermore, if $v \leq m$, then $\delta(V) = v$.*

Proof. Any vector $\mathbf{x} \in V$ can be expressed as the sum of at most v vectors of rank 1, hence its rank is upper bounded by v. Thus, $\delta(V) \leq v$ by Definition 2.6. If $v \leq m$, we show that there exists a vector in V with rank v. Let $B = \{\mathbf{b}_i\}_{i=0}^{v-1}$ be an elementary basis of V, and consider $\mathbf{y} = \sum_{i=0}^{v-1} \alpha_i \mathbf{b}_i$, where $\{\alpha_i\}_{i=0}^{m-1}$ is a basis of $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$. If we expand the coordinates of $\mathbf{y}$ with respect to the basis $\{\alpha_i\}_{i=0}^{m-1}$, we obtain $\mathbf{Y} = \left(\mathbf{b}_0^T, \ldots, \mathbf{b}_{v-1}^T, \mathbf{0}^T, \ldots, \mathbf{0}^T\right)^T$. Since the row vectors $\mathbf{b}_0, \mathbf{b}_1, \cdots, \mathbf{b}_{v-1}$ are linearly independent over $\mathrm{GF}(q)$, $\mathbf{Y}$ has rank v and $\mathrm{rk}(\mathbf{y}) = v$. □

Lemma 2.8. *Any vector* $\mathbf{x} \in \mathrm{GF}(q^m)^n$ *has rank* r *if and only if it belongs to a unique ELS* $V \in E_r(q, m, n)$.

Proof. The necessity is obvious. We now prove the sufficiency. We can express $\mathbf{x}$ as $\mathbf{x} = \sum_{i=0}^{r-1} a_i \mathbf{v}_i$, where $\mathbf{v}_i \in \mathrm{GF}(q)^n$ for all i. Let V be the ELS of $\mathrm{GF}(q^m)^n$ spanned by $\mathbf{v}_i$'s, then $\dim(V) = r$ and $\mathbf{x} \in V$. We now prove the uniqueness of V. Suppose $\mathbf{x}$ also belongs to W, where $W \in E_r(q, m, n)$ has an elementary basis $\{\mathbf{w}_j\}_{j=0}^{r-1}$, where $\mathbf{w}_j \in \mathrm{GF}(q)^n$ for all j. Therefore, $\mathbf{x} = \sum_{i=0}^{r-1} a_i \mathbf{v}_i = \sum_{j=0}^{r-1} b_j \mathbf{w}_j$, where $a_i, b_j \in \mathrm{GF}(q^m)$ for $0 \leq i, j \leq r-1$. By definition, we have $S(\mathbf{x}) = S(a_0, \ldots, a_{r-1}) = S(b_0, \ldots, b_{r-1})$, therefore b_j's can be expressed as linear combinations of a_i's, i.e., $b_j = \sum_{i=0}^{r-1} c_{j,i} a_i$ where $c_{j,i} \in \mathrm{GF}(q)$. Hence $\mathbf{x} = \sum_{i=0}^{r-1} a_i \mathbf{u}_i$, where $\mathbf{u}_i = \sum_{j=0}^{r-1} c_{j,i} \mathbf{w}_j$ for $0 \leq i \leq r-1$ form an elementary basis of W. Considering the matrix obtained by expanding the coordinates of $\mathbf{x}$ with respect to the basis $\{a_i\}_{i=0}^{m-1}$, we obtain $\mathbf{v}_i = \mathbf{u}_i$, and hence $V = W$. □

Lemma 2.8 shows that an ELS is analogous to a subset of coordinates since a vector $\mathbf{x}$ with Hamming weight r belongs to a unique subset of r coordinates, often referred to as the support of $\mathbf{x}$.

Let L be a linear subspace of $\mathrm{GF}(q^m)^n$ and let $\bar{L}$ be complementary to L, i.e., $L \oplus \bar{L} = \mathrm{GF}(q^m)^n$. We denote the projection of $\mathbf{x}$ on L along $\bar{L}$ as $\mathbf{x}_L$ [44]. Remark that $\mathbf{x} = \mathbf{x}_L + \mathbf{x}_{\bar{L}}$. Note that for any given linear subspace L, its complementary linear subspace $\bar{L}$ is not unique. Thus, $\mathbf{x}_L$ depends on both L and $\bar{L}$, and is well-defined only when both L and $\bar{L}$ are given. All the projections are with respect to a pair of fixed linear subspaces complementary to each other.

The decomposition over a pair of complementary ELSs induces a mapping from $\mathrm{GF}(q^m)^n$ to $\mathrm{GF}(q^m)^v$.

Definition 2.9. *Let $V \in E_v(q, m, n)$ be the row span of $\mathbf{B}$ with an elementary complement $\bar{V}$. For any $\mathbf{x} \in \mathrm{GF}(q^m)^n$, we define $r_V(\mathbf{x}) = (r_0, \ldots, r_{v-1}) \in \mathrm{GF}(q^m)^v$ to be $r_V(\mathbf{x}) = \mathbf{x}_V \mathbf{B}^{-R}$, where $\mathbf{B}^{-R}$ is the right inverse of $\mathbf{B}$.*

We remark that the r_V function is linear and since $\mathbf{B}^{-R}$ has full rank, we have $\mathrm{rk}(r_V(\mathbf{x})) = \mathrm{rk}(\mathbf{x}_V)$ for all $\mathbf{x}$.

Definition 2.10. *For $V \in E_v(q, m, n)$ the row span of $\mathbf{B}$, let $\bar{V}$ be an elementary complement of V which is the row span of $\bar{\mathbf{B}}$. For any $\mathbf{x} \in \mathrm{GF}(q^m)^n$, we define $s_{V,\bar{V}}(\mathbf{x}) = (r_V(\mathbf{x}), r_{\bar{V}}(\mathbf{x})) \in \mathrm{GF}(q^m)^n$.*

Lemma 2.11. *For all $\mathbf{x} \in \mathrm{GF}(q^m)^n$, $\mathrm{rk}(s_{V,\bar{V}}(\mathbf{x})) = \mathrm{rk}(\mathbf{x})$.*

Proof. Note that $\mathbf{x} = s_{V,\bar{V}}(\mathbf{x})\hat{\mathbf{B}}$ where $\hat{\mathbf{B}} = (\mathbf{B}^T|\bar{\mathbf{B}}^T)^T$ is an $n \times n$ matrix over $\mathrm{GF}(q)$ with full rank. Therefore $\mathrm{rk}(s_{V,\bar{V}}(\mathbf{x})) = \mathrm{rk}(\mathbf{x})$. □

Corollary 2.12. *For all $\mathbf{x} \in \mathrm{GF}(q^m)^n$ and two complementary ELSs V and $\bar{V}$, $0 \leq \mathrm{rk}(\mathbf{x}_V) \leq \mathrm{rk}(\mathbf{x})$ and $\mathrm{rk}(\mathbf{x}) \leq \mathrm{rk}(\mathbf{x}_V) + \mathrm{rk}(\mathbf{x}_{\bar{V}})$.*

It can be easily shown that the second inequality in Corollary 2.12 can be strict in some cases. For example, consider $\mathbf{x} = (1, 1) \in \mathrm{GF}(q^2)^2$. For appropriate ELSs V and $\bar{V}$, $\mathbf{x}_V = (1, 0)$ and $\mathbf{x}_{\bar{V}} = (0, 1)$. Clearly, $\mathrm{rk}(\mathbf{x}) < \mathrm{rk}(\mathbf{x}_V) + \mathrm{rk}(\mathbf{x}_{\bar{V}})$. However, when V and $\bar{V}$ are two complementary sets of coordinates, the Hamming weight of any vector $\mathbf{x} \in \mathrm{GF}(q^m)^n$ is the sum of the Hamming weights of the projections of $\mathbf{x}$ on V and $\bar{V}$. Therefore, Corollary 2.12 illustrates the difference between ELSs and sets of coordinates.

In Proposition 2.5, it was shown that an ELS always has a complementary elementary linear subspace. The following lemma enumerates such complementary ELSs.

Lemma 2.13. *Suppose $V \in E_v(q, m, n)$ and $A \subseteq V$ is an ELS with dimension a, then there are $q^{a(v-a)}$ ELSs B such that $A \oplus B = V$. Furthermore, there are $q^{a(v-a)} \begin{bmatrix} v \\ a \end{bmatrix}$ such ordered pairs (A, B).*

Proof. First, remark that $\dim(B) = v - a$. The total number of sets of $v - a$ linearly independent vectors over $\mathrm{GF}(q)$ in $V \backslash A$ is given by $N = (q^v - q^a)(q^v - q^{a+1}) \cdots (q^v - q^{v-1}) = q^{a(v-a)} \alpha(v - a, v - a)$. Note that each set of linearly independent vectors over $\mathrm{GF}(q)$ constitutes an elementary basis set. Thus, the number of possible B is given by N divided by $\alpha(v - a, v - a)$, the number of elementary basis sets for each B. Therefore, once A is fixed, there are $q^{a(v-a)}$ choices for B. Since the number of a-dimensional subspaces A in V is $\begin{bmatrix} v \\ a \end{bmatrix}$, the total number of ordered pairs (A, B) is hence $q^{a(v-a)} \begin{bmatrix} v \\ a \end{bmatrix}$. □

Puncturing a vector with full Hamming weight results in another vector with full Hamming weight. Lemma 2.14 below shows that the situation for vectors with full rank is similar.

Lemma 2.14. *Suppose $V \in E_v(q, m, n)$ and $\mathbf{u} \in V$ has rank v, then $\mathrm{rk}(\mathbf{u}_A) = a$ and $\mathrm{rk}(\mathbf{u}_B) = v - a$ for any $A \in E_a(q, m, n)$ and $B \in E_{v-a}(q, m, n)$ such that $A \oplus B = V$.*

Proof. First, $\mathbf{u}_A \in A$ and hence $\mathrm{rk}(\mathbf{u}_A) \leq a$ by [29, Proposition 2]; similarly, $\mathrm{rk}(\mathbf{u}_B) \leq v - a$. Now suppose $\mathrm{rk}(\mathbf{u}_A) < a$ or $\mathrm{rk}(\mathbf{u}_B) < v - a$, then $v = \mathrm{rk}(\mathbf{u}) \leq \mathrm{rk}(\mathbf{u}_A) + \mathrm{rk}(\mathbf{u}_B) < a + v - a = v$. □

The projection $\mathbf{u}_A$ of a vector $\mathbf{u}$ on an ELS A depends on both A and its complement B. The following lemma further clarifies the relation: changing B always modifies $\mathbf{u}_A$, provided that $\mathbf{u}$ has full rank.

Lemma 2.15. *Suppose $V \in E_v(q,m,n)$ and $\mathbf{u} \in V$ has rank v. For any $A \in E_a(q,m,n)$ and $B \in E_{v-a}(q,m,n)$ such that $A \oplus B = V$, define the functions $f_{\mathbf{u}}(A,B) = \mathbf{u}_A$ and $g_{\mathbf{u}}(A,B) = \mathbf{u}_B$. Then both $f_{\mathbf{u}}$ and $g_{\mathbf{u}}$ are injective.*

Proof. Consider another pair (A', B') with dimensions a and $v-a$ respectively. Suppose $A' \neq A$, then $\mathbf{u}_{A'} \neq \mathbf{u}_A$. Otherwise $\mathbf{u}_A$ belongs to two distinct ELSs with dimension a, which contradicts Lemma 2.8. Hence $\mathbf{u}_{A'} \neq \mathbf{u}_A$ and $\mathbf{u}_{B'} = \mathbf{u} - \mathbf{u}_{A'} \neq \mathbf{u} - \mathbf{u}_A = \mathbf{u}_B$. The argument is similar if $B' \neq B$. □

We now extend the definition of the restriction to linear codes.

Definition 2.16. *For $V \in E_v(q,m,n)$ with elementary basis B and its elementary complement $\bar{V}$, $C_V = \{r_V(\mathbf{c}) | \mathbf{c} \in C\}$ is called the restriction of C to V.*

It is well known that a punctured MDS code is an MDS code [36]. We now show that the restriction of an MRD code to an ELS is also MRD.

Lemma 2.17. *Let C be an $(n, k, n-k+1)$ linear MRD code over $\mathrm{GF}(q^m)$. For all ELS V with dimension v ($k \leq v \leq n$), C_V is an MRD code with length v, cardinality q^{mk}, and minimum rank distance $d_{\mathrm{R}} = v - k + 1$ over $\mathrm{GF}(q^m)$.*

Proof. For $\mathbf{c} \neq \mathbf{d} \in C$, consider $\mathbf{x} = \mathbf{c} - \mathbf{d}$. By the property of r_V function, we have $\mathrm{rk}(r_V(\mathbf{c}) - r_V(\mathbf{d})) = \mathrm{rk}(r_V(\mathbf{c}-\mathbf{d})) = \mathrm{rk}(\mathbf{x}_V) \geq \mathrm{rk}(\mathbf{x}) - \mathrm{rk}(\mathbf{x}_{\bar{V}}) \geq n-k+1-(n-v) = v-k+1$. Therefore, C_V is a code over $\mathrm{GF}(q^m)$ with length v, cardinality q^{mk}, and minimum rank distance $\geq v-k+1$. The Singleton bound on C_V completes the proof. □

2.4.3 Properties of balls with rank radii

We refer to all vectors in $\mathrm{GF}(q^m)^n$ within rank distance r of $\mathbf{x} \in \mathrm{GF}(q^m)^n$ as a ball of rank radius r centered at $\mathbf{x}$, and denote it as $B_r(\mathbf{x})$. Its volume, which does not depend on $\mathbf{x}$, is denoted as $V_{\mathrm{R}}(q,m,n,r) = \sum_{u=0}^{r} N_{\mathrm{R}}(q,m,n,u)$. When there is no ambiguity about the vector space, we denote $V_{\mathrm{R}}(q,m,n,r)$ as $V_{\mathrm{R}}(r)$.

Lemma 2.18. *For* $0 \leq r \leq \min\{n,m\}$, $q^{r(m+n-r)} \leq V_{\mathrm{R}}(q,m,n,r) < K_q^{-1} q^{r(m+n-r)}$, *where* $K_q \stackrel{def}{=} \prod_{j=1}^{\infty}(1-q^{-j})$.

Proof. From Lemma 2.8, every vector $\mathbf{x}$ in the ball belongs to some ELS V with dimension t. Since $|V| = q^{mt}$ and $|E_t(q,m,n)| = \begin{bmatrix} n \\ t \end{bmatrix}$, it follows that $V_{\mathrm{R}}(t) \leq \begin{bmatrix} n \\ t \end{bmatrix} q^{mt}$. By Corollary 2.3, we have $\begin{bmatrix} n \\ t \end{bmatrix} < K_q^{-1} q^{t(n-t)}$, and hence $V_{\mathrm{R}}(t) < K_q^{-1} q^{t(m+n-t)}$.

We now prove the lower bound by constructing $q^{r(m+n-r)}$ vectors $\mathbf{z} \in \mathrm{GF}(q^m)^n$ of rank at most r. Let $\mathbf{x} \in \mathrm{GF}(q^m)^r$ let a subspace T of $\mathrm{GF}(q^m)$ such that $\dim(T) = r$ and $S(\mathbf{x}) \subseteq T$. We consider the vectors $\mathbf{y} \in \mathrm{GF}(q^m)^{n-r}$ such that $S(\mathbf{y}) \subseteq T$. There are q^{mr} choices for $\mathbf{x}$ and, for a given $\mathbf{x}$, $q^{r(n-r)}$ choices for $\mathbf{y}$. Thus the total number of vectors $\mathbf{z} = (\mathbf{x}, \mathbf{y}) \in \mathrm{GF}(q^m)^n$ is $q^{r(m+n-r)}$, and since $S(\mathbf{z}) \subseteq T$, we have $\mathrm{rk}(\mathbf{z}) \leq r$. □

We remark that both bounds in Lemma 2.18 are tighter than their respective counterparts in [30, Proposition 1]. More importantly, the two bounds in Lemma 2.18 differ only by a factor of K_q, and thus they not only provide a good approximation of $V_{\mathrm{R}}(q,m,n,r)$, but also accurately describe the asymptotic behavior of $V_{\mathrm{R}}(q,m,n,r)$. This will enable us to determine the asymptotic behavior of the solution to sphere covering problem in Section 2.5.7.

The diameter of a set is defined to be the maximum distance between any pair of elements in the set [36, p. 172]. For a binary vector space $\mathrm{GF}(2)^n$ and a given

diameter $2r < n$, Kleitman [45] proved that balls with Hamming radius r maximize the cardinality of a set with a given diameter. However, when the underlying field for the vector space is not GF(2), the result is not necessarily valid [37, p. 40]. We show below that balls with rank radii do not maximize the cardinality of a set with a given diameter.

Proposition 2.19. *For $2 \leq 2r \leq n \leq m$, any $S \in E_{2r}(q, m, n)$ has diameter $2r$ and cardinality $|S| > V_{\mathrm{R}}(q, m, n, r)$.*

Proof. Any $S \in E_{2r}(q, m, n)$ has diameter $2r$ and cardinality q^{2mr}. For $r = 1$, we have $V_{\mathrm{R}}(q, m, n, 1) = 1 + \frac{(q^n-1)(q^m-1)}{(q-1)} < q^{2m}$. For $r \geq 2$, we have $V_{\mathrm{R}}(q, m, n, r) < K_q^{-1} q^{r(n+m)-r^2}$ by Lemma 2.18. Since $r^2 > 2 > -\log_q K_q$, we obtain $V_{\mathrm{R}}(q, m, n, r) < q^{r(n+m)} \leq |S|$. □

The intersection of balls with Hamming radii has been studied in [37, Chapter 2], and below we investigate the intersection of balls with rank radii.

Lemma 2.20. *If $0 \leq r, s \leq n$ and $\mathbf{c}_1, \mathbf{c}_2 \in \mathrm{GF}(q^m)^n$, then $|B_r(\mathbf{c}_1) \cap B_s(\mathbf{c}_2)|$ depends on $\mathbf{c}_1$ and $\mathbf{c}_2$ only through $d_{\mathrm{R}}(\mathbf{c}_1, \mathbf{c}_2)$.*

Proof. This follows from the fact that matrices in $\mathrm{GF}(q)^{m \times n}$ together with the rank metric form an association scheme [12, 15]. □

Lemma 2.21. *We have*

$$J_{\mathrm{R}}(u, s, w) = \frac{1}{q^{mn} N_{\mathrm{R}}(w)} \sum_{i=0}^{n} N_{\mathrm{R}}(i) P_u(i) P_s(i) P_w(i), \tag{2.4}$$

where $K_j(i)$ is a q-Krawtchouk polynomial [46]:

$$P_j(i) = \sum_{l=0}^{j} (-1)^{j-l} q^{lm + \binom{j-l}{2}} \begin{bmatrix} n-l \\ n-j \end{bmatrix} \begin{bmatrix} n-i \\ l \end{bmatrix}.$$

Proof. This directly follows [41, Chapter II, Theorem 3.6]. □

Although (2.4) is a direct application of the theory of association schemes, we present it formally since it is a fundamental geometric property of the rank metric which will be instrumental in our later derivations. We also denote the intersection of two **balls** with radii u and s and distance between their centers w as $I(u, s, w)$. Since

$$I(u, s, w) = \sum_{i=0}^{u} \sum_{j=0}^{s} J_{\mathrm{R}}(i, j, w), \tag{2.5}$$

(2.4) also leads to an analytical expression for $I(u, s, w)$. In order to simplify notations, we denote $I(\rho, \rho, d)$ as $I(\rho, d)$.

Proposition 2.22. *If* $0 \leq r, s \leq n$, $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}'_1, \mathbf{c}'_2 \in \mathrm{GF}(q^m)^n$ *and* $d_{\mathrm{R}}(\mathbf{c}_1, \mathbf{c}_2) > d_{\mathrm{R}}(\mathbf{c}'_1, \mathbf{c}'_2)$, *then* $|B_r(\mathbf{c}_1) \cap B_s(\mathbf{c}_2)| \leq |B_r(\mathbf{c}'_1) \cap B_s(\mathbf{c}'_2)|$.

Proof. It suffices to prove the claim when $d_{\mathrm{R}}(\mathbf{c}_1, \mathbf{c}_2) = d_{\mathrm{R}}(\mathbf{c}'_1, \mathbf{c}'_2) + 1 = e + 1$. By Lemma 2.20, we can assume without loss of generality that $\mathbf{c}_1 = \mathbf{c}'_1 = \mathbf{0}$, $\mathbf{c}'_2 = (0, c_1, \ldots, c_e, 0, \ldots, 0)$ and $\mathbf{c}_2 = (c_0, c_1, \ldots, c_e, 0, \ldots, 0)$, where $c_0, \ldots, c_e \in \mathrm{GF}(q^m)$ are linearly independent.

We will show that an injective mapping ϕ from $B_r(\mathbf{c}_1) \cap B_s(\mathbf{c}_2)$ to $B_r(\mathbf{c}'_1) \cap B_s(\mathbf{c}'_2)$ can be constructed. We consider vectors $\mathbf{z} = (z_0, z_1, \ldots, z_{n-1}) \in B_r(\mathbf{c}_1) \cap B_s(\mathbf{c}_2)$. We thus have $\mathrm{rk}(\mathbf{z}) \leq r$ and $\mathrm{rk}(\mathbf{u}) \leq s$, where $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1}) = \mathbf{z} - \mathbf{c}_2 = (z_0 - c_0, z_1 - c_1, \ldots, z_{n-1})$. We also define $\bar{\mathbf{z}} = (z_1, \ldots, z_{n-1})$ and $\bar{\mathbf{u}} = (u_1, \ldots, u_{n-1})$. We consider three cases for the mapping ϕ, depending on $\bar{\mathbf{z}}$ and $\bar{\mathbf{u}}$.

- Case I: $\mathrm{rk}(\bar{\mathbf{u}}) \leq s - 1$. In this case, $\phi(\mathbf{z}) \stackrel{\mathrm{def}}{=} \mathbf{z}$. We remark that $\mathrm{rk}(\mathbf{z} - \mathbf{c}'_2) \leq \mathrm{rk}(\bar{\mathbf{u}}) + 1 \leq s$ and hence $\phi(\mathbf{z}) \in B_r(\mathbf{c}'_1) \cap B_s(\mathbf{c}'_2)$.

- Case II: $\mathrm{rk}(\bar{\mathbf{u}}) = s$ and $\mathrm{rk}(\bar{\mathbf{z}}) \leq r-1$. In this case, $\phi(\mathbf{z}) \stackrel{\text{def}}{=} (z_0 - c_0, z_1, \ldots, z_{n-1})$. We have $\mathrm{rk}(\phi(\mathbf{z})) \leq \mathrm{rk}(\bar{\mathbf{z}}) + 1 \leq r$ and $\mathrm{rk}\,(\phi(\mathbf{z}) - \mathbf{c}_2') = \mathrm{rk}\,(\mathbf{z} - \mathbf{c}_2) \leq s$, and hence $\phi(\mathbf{z}) \in B_r(\mathbf{c}_1') \cap B_s(\mathbf{c}_2')$.

- Case III: $\mathrm{rk}(\bar{\mathbf{u}}) = s$ and $\mathrm{rk}(\bar{\mathbf{z}}) = r$. Since $\mathrm{rk}(\mathbf{u}) = s$, we have $z_0 - c_0 \in S(\bar{\mathbf{u}})$. Similarly, since $\mathrm{rk}(\mathbf{z}) = r$, we have $z_0 \in S(\bar{\mathbf{z}})$. Denote $\dim(S(\bar{\mathbf{u}}, \bar{\mathbf{z}}))$ as d ($d \geq s$). For $d > s$, let $\alpha_0, \ldots, \alpha_{d-1}$ be a basis of $S(\bar{\mathbf{u}}, \bar{\mathbf{z}})$ such that $\alpha_0, \ldots, \alpha_{s-1} \in S(\bar{\mathbf{u}})$ and $\alpha_s, \ldots, \alpha_{d-1} \in S(\bar{\mathbf{z}})$. This basis is fixed for all vectors $\mathbf{z}$ having the same $\bar{\mathbf{z}}$, i.e., it is fixed for all values of z_0. Note that $c_0 \in S(\bar{\mathbf{u}}, \bar{\mathbf{z}})$, and may therefore be uniquely expressed as $c_0 = c_u + c_z$, where $c_u \in S(\alpha_0, \ldots, \alpha_{s-1}) = S(\bar{\mathbf{u}})$ and $c_z \in S(\alpha_s, \ldots, \alpha_{d-1}) \subseteq S(\bar{\mathbf{z}})$. If $d = s$, then $c_z = 0 \in S(\bar{\mathbf{z}})$. In this case, $\phi(\mathbf{z}) \stackrel{\text{def}}{=} (z_0 - c_z, z_1, \ldots, z_{n-1})$. Remark that $z_0 - c_z \in S(\bar{\mathbf{z}})$ and hence $\mathrm{rk}(\phi(\mathbf{z})) = r$. Also, $z_0 - c_z = z_0 - c_0 + c_u \in S(\bar{\mathbf{u}})$ and hence $\mathrm{rk}(\phi(\mathbf{z}) - \mathbf{c}_2') = s$. Therefore $\phi(\mathbf{z}) \in B_r(\mathbf{c}_1') \cap B_s(\mathbf{c}_2')$.

It can be easily verified that ϕ is injective, hence $|B_r(\mathbf{c}_1) \cap B_s(\mathbf{c}_2)| \leq |B_r(\mathbf{c}_1') \cap B_s(\mathbf{c}_2')|$. □

Corollary 2.23. *If* $0 \leq r, s \leq n$, $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_1', \mathbf{c}_2' \in \mathrm{GF}(q^m)^n$ *and* $d_{\mathrm{R}}(\mathbf{c}_1, \mathbf{c}_2) \geq d_{\mathrm{R}}(\mathbf{c}_1', \mathbf{c}_2')$, *then* $|B_r(\mathbf{c}_1) \cup B_s(\mathbf{c}_2)| \geq |B_r(\mathbf{c}_1') \cup B_s(\mathbf{c}_2')|$.

Proof. The result follows from $|B_r(\mathbf{c}_1) \cup B_s(\mathbf{c}_2)| = V_{\mathrm{R}}(r) + V_{\mathrm{R}}(s) - |B_r(\mathbf{c}_1) \cap B_s(\mathbf{c}_2)|$. □

We now quantify the volume of the intersection of two balls with rank radii for some special cases, which will be used in Section 2.5.2.

Proposition 2.24. *If* $\mathbf{c}_1, \mathbf{c}_2 \in \mathrm{GF}(q^m)^n$ *and* $d_{\mathrm{R}}(\mathbf{c}_1, \mathbf{c}_2) = r$, *then* $|B_r(\mathbf{c}_1) \cap B_1(\mathbf{c}_2)| = 1 + (q^m - q^r)\begin{bmatrix} r \\ 1 \end{bmatrix} + (q^r - 1)\begin{bmatrix} n \\ 1 \end{bmatrix}$.

Proof. By Lemma 2.20, we assume without loss of generality that $\mathbf{c}_2 = \mathbf{0}$ and $\mathrm{rk}(\mathbf{c}_1) = r$. By Lemma 2.8, the vector $\mathbf{c}_1$ belongs to a unique ELS $V \in E_r(q, m, n)$. First of all, it is easy to check that $\mathbf{y} = \mathbf{0} \in B_r(\mathbf{c}_1) \cap B_1(\mathbf{0})$. We now consider a nonzero vector $\mathbf{y} \in B_1(\mathbf{0})$ with rank 1. We have $d_{\mathrm{R}}(\mathbf{y}, \mathbf{c}_1) = r+1$ if and only if $\mathbf{y} \notin V$ and $S(\mathbf{y}) \nsubseteq S(\mathbf{c}_1)$. There are $\frac{(q^n-q^r)(q^m-q^r)}{q-1}$ such vectors. Thus, $|B_r(\mathbf{c}_1) \cap B_1(\mathbf{c}_2)| = 1 + N_{\mathrm{R}}(q, m, n, 1) - \frac{(q^n-q^r)(q^m-q^r)}{q-1} = 1 + (q^m - q^r)\begin{bmatrix} r \\ 1 \end{bmatrix} + (q^r - 1)\begin{bmatrix} n \\ 1 \end{bmatrix}$. □

Proposition 2.25. *If* $\mathbf{c}_1, \mathbf{c}_2 \in \mathrm{GF}(q^m)^n$ *and* $d_{\mathrm{R}}(\mathbf{c}_1, \mathbf{c}_2) = r$, *then* $|B_s(\mathbf{c}_1) \cap B_{r-s}(\mathbf{c}_2)| = q^{s(r-s)}\begin{bmatrix} r \\ s \end{bmatrix}$ *for* $0 \le s \le r$.

Proof. By Lemma 2.20, we can assume that $\mathbf{c}_1 = \mathbf{0}$, and hence $\mathrm{rk}(\mathbf{c}_2) = r$. By Lemma 2.8, $\mathbf{c}_2$ belongs to a unique ELS $V \in E_r(q, m, n)$. We first prove that all vectors $\mathbf{y} \in B_s(\mathbf{0}) \cap B_{r-s}(\mathbf{c}_2)$ are in V. Let $\mathbf{y} = \mathbf{y}_V + \mathbf{y}_W$, where $W \in E_{n-r}(q, m, n)$ such that $V \oplus W = \mathrm{GF}(q^m)^n$. We have $\mathbf{y}_V + (\mathbf{c}_2 - \mathbf{y})_V = \mathbf{c}_2$, with $\mathrm{rk}(\mathbf{y}_V) \le \mathrm{rk}(\mathbf{y}) \le s$ and $\mathrm{rk}((\mathbf{c}_2 - \mathbf{y})_V) \le \mathrm{rk}(\mathbf{c}_2 - \mathbf{y}) \le r - s$. Therefore, $\mathrm{rk}(\mathbf{y}_V) = \mathrm{rk}(\mathbf{y}) = s$, $\mathrm{rk}((\mathbf{c}_2 - \mathbf{y})_V) = \mathrm{rk}(\mathbf{c}_2 - \mathbf{y}) = r - s$, and $S(\mathbf{y}_V) \cap S((\mathbf{c}_2 - \mathbf{y})_V) = \{0\}$. Since $\mathrm{rk}(\mathbf{y}_V) = \mathrm{rk}(\mathbf{y})$, we have $S(\mathbf{y}_W) \subseteq S(\mathbf{y}_V)$; and similarly $S((\mathbf{c}_2 - \mathbf{y})_W) \subseteq S((\mathbf{c}_2 - \mathbf{y})_V)$. Altogether, we obtain $S(\mathbf{y}_W) \cap S((\mathbf{c}_2 - \mathbf{y})_W) = \{0\}$. However, $\mathbf{y}_W + (\mathbf{c}_2 - \mathbf{y})_W = \mathbf{0}$, and hence $\mathbf{y}_W = (\mathbf{c}_2 - \mathbf{y})_W = \mathbf{0}$. Therefore, $\mathbf{y} \in V$.

We now prove that $\mathbf{y}$ is necessarily the projection of $\mathbf{c}_2$ onto some ELS A of V. If $\mathbf{y} \in V$ satisfies $\mathrm{rk}(\mathbf{y}) = s$ and $\mathrm{rk}(\mathbf{c}_2 - \mathbf{y}) = r - s$, then $\mathbf{y}$ belongs to some ELS A and $\mathbf{c}_2 - \mathbf{y} \in B$ such that $A \oplus B = V$. We hence have $\mathbf{y} = \mathbf{c}_{2,A}$ and $\mathbf{c}_2 - \mathbf{y} = \mathbf{c}_{2,B}$.

On the other hand, for any $A \in E_s(q, m, n)$ and $B \in E_{r-s}(q, m, n)$ such that $A \oplus B = V$, $\mathbf{c}_{2,A}$ is a vector of rank s with distance $r - s$ from $\mathbf{c}_2$ by Lemma 2.14. By Lemma 2.15, all the $\mathbf{c}_{2,A}$ vectors are distinct. There are thus as many vectors $\mathbf{y}$ as ordered pairs (A, B). By Lemma 2.13, there are $q^{s(r-s)}\begin{bmatrix} r \\ s \end{bmatrix}$ such pairs, and hence $q^{s(r-s)}\begin{bmatrix} r \\ s \end{bmatrix}$ vectors $\mathbf{y}$. □

The problem of the intersection of three balls with rank radii is more complicated since the volume of the intersection of three balls with rank radii is not completely determined by the pairwise distances between the centers. We give a simple example to illustrate this point: consider $\mathrm{GF}(2^2)^3$ and the vectors $\mathbf{c}_1 = \mathbf{c}'_1 = (0,0,0)$, $\mathbf{c}_2 = \mathbf{c}'_2 = (1,\alpha,0)$, $\mathbf{c}_3 = (\alpha,0,1)$, and $\mathbf{c}'_3 = (\alpha,\alpha+1,0)$, where α is a primitive element of the field. It can be verified that $d_{\mathrm{R}}(\mathbf{c}_1,\mathbf{c}_2) = d_{\mathrm{R}}(\mathbf{c}_2,\mathbf{c}_3) = d_{\mathrm{R}}(\mathbf{c}_3,\mathbf{c}_1) = 2$ and $d_{\mathrm{R}}(\mathbf{c}'_1,\mathbf{c}'_2) = d_{\mathrm{R}}(\mathbf{c}'_2,\mathbf{c}'_3) = d_{\mathrm{R}}(\mathbf{c}'_3,\mathbf{c}'_1) = 2$. However, $B_1(\mathbf{c}_1) \cap B_1(\mathbf{c}_2) \cap B_1(\mathbf{c}_3) = \{(\alpha+1,0,0)\}$, whereas $B_1(\mathbf{c}'_1) \cap B_1(\mathbf{c}'_2) \cap B_1(\mathbf{c}'_3) = \{(1,0,0),(0,\alpha+1,0),(\alpha,\alpha,0)\}$. We remark that this is similar to the problem of the intersection of three balls with Hamming radii discussed in [37, p. 58], provided that the underlying field is not $\mathrm{GF}(2)$.

We also derive a bound on the volume of the union of any K balls with radius ρ, which will be instrumental in Section 2.5.

Lemma 2.26. *The volume of the union of* any *K balls with rank radius ρ is at most*

$$\begin{aligned} B_{\mathrm{R}}(K,\rho) &= V_{\mathrm{R}}(\rho) + \sum_{a=1}^{l} (q^{am} - q^{(a-1)m})[V_{\mathrm{R}}(\rho) - I(\rho, n-a+1)] \\ &\quad + (K - q^{lm})[V_{\mathrm{R}}(\rho) - I(\rho, n-l)], \end{aligned}$$

where $l = \lfloor \log_{q^m} K \rfloor$.

Proof. Let $\{\mathbf{v}_i\}_{i=0}^{K-1}$ denote the centers of K balls with rank radius ρ and let $\mathcal{V}_j = \{\mathbf{v}_i\}_{i=0}^{j-1}$ for $1 \le j \le K$. The centers are labeled such that $d_{\mathrm{R}}(\mathbf{v}_j, \mathcal{V}_j)$ is non-increasing for $j > 0$. For $1 \le a \le l$ and $q^{m(a-1)} \le j < q^{ma}$, we have $d_{\mathrm{R}}(\mathbf{v}_j, \mathcal{V}_j) = d_{\mathrm{R}}(\mathcal{V}_{j+1}) \le n - a + 1$ by the Singleton bound. The center $\mathbf{v}_j$ hence covers at most $V_{\mathrm{R}}(\rho) - I(\rho, n-a+1)$ vectors that are not previously covered by $\mathcal{V}_j$. □

2.5 Covering properties of rank metric codes

2.5.1 The sphere covering problem

We denote the *minimum* cardinality of a code of length n and rank covering radius ρ as $K_{\mathrm{R}}(q, m, n, \rho)$. We remark that if $\mathcal{C}$ is a code over $\mathrm{GF}(q^m)$ with length n and covering radius ρ, then its transpose code $\mathcal{C}^T$ is a code over $\mathrm{GF}(q^n)$ with length m and the same covering radius. Therefore, $K_{\mathrm{R}}(q, m, n, \rho) = K_{\mathrm{R}}(q, n, m, \rho)$, and without loss of generality we shall assume $n \leq m$ henceforth in this section. Also note that $K_{\mathrm{R}}(q, m, n, 0) = q^{mn}$ and $K_{\mathrm{R}}(q, m, n, n) = 1$ for all m and n. Hence we assume $0 < \rho < n$ throughout this section. Two bounds on $K_{\mathrm{R}}(q, m, n, \rho)$ can be easily derived.

Proposition 2.27. *For* $0 < \rho < n \leq m$, $\frac{q^{mn}}{V_{\mathrm{R}}(\rho)} < K_{\mathrm{R}}(q, m, n, \rho) \leq q^{m(n-\rho)}$.

Proof. The lower bound is a straightforward generalization of the bound given in [23]. Note that the only codes with cardinality $\frac{q^{mn}}{V_{\mathrm{R}}(\rho)}$ are perfect codes. However, there are no nontrivial perfect codes for the rank metric [38]. Therefore, $K_{\mathrm{R}}(q, m, n, \rho) > \frac{q^{mn}}{V_{\mathrm{R}}(\rho)}$.

Let $\mathcal{C}$ be an (n, k) linear code over $\mathrm{GF}(q^m)$ and without loss of generality assume $(\mathbf{I}_k \,|\, \mathbf{R})$ is its generator matrix. For any $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}) \in \mathrm{GF}(q^m)^n$, there exists $\mathbf{c} = (x_0, x_1, \ldots, x_{k-1}, c_k, \ldots, c_{n-1}) \in \mathcal{C}$ such that $\mathrm{rk}(\mathbf{c} - \mathbf{x}) \leq n - k$ and hence the covering radius ρ of $\mathcal{C}$ satisfies $\rho \leq n - k$. That is, $|\mathcal{C}| \leq q^{m(n-\rho)}$. By definition, $K_{\mathrm{R}}(q, m, n, \rho) \leq |\mathcal{C}|$, which leads to the upper bound. □

We refer to the lower bound in Proposition 2.27 as the sphere covering bound.

For a code over $\mathrm{GF}(q^m)$ with length n and covering radius $0 < \rho < n$, we have $K_{\mathrm{R}}(q, m, n, \rho) \leq K_{\mathrm{H}}(q, m, n, \rho)$, where $K_{\mathrm{H}}(q, m, n, \rho)$ is the minimum cardinality of a

(linear or nonlinear) code over $\mathrm{GF}(q^m)$ with length n and Hamming covering radius ρ. This holds because any code with Hamming covering radius ρ has rank covering radius $\leq \rho$. Since $K_{\mathrm{H}}(q, m, n, \rho) \leq q^{m(n-\rho)}$ [37], this provides a tighter bound than the one given in Proposition 2.27.

Proposition 2.28. *For* $0 < \rho < n \leq m$, $K_{\mathrm{R}}(q, m, n, \rho) \geq 3$.

Proof. Suppose there exists a code $\mathcal{C}$ of cardinality 2 and length n over $\mathrm{GF}(q^m)$ with covering radius $\rho < n$. Without loss of generality, we assume $\mathcal{C} = \{\mathbf{0}, \mathbf{c}\}$. Since $|B_\rho(\mathbf{0}) \cup B_\rho(\mathbf{c})|$ is a non-decreasing function of $\mathrm{rk}(\mathbf{c})$ by Corollary 2.23, we assume $\mathrm{rk}(\mathbf{c}) = n$. The code $\mathcal{G} = \langle \mathbf{c} \rangle$ is hence an $(n, 1, n)$ linear MRD code over $\mathrm{GF}(q^m)$. Therefore, any codeword in $\mathcal{G} \backslash \mathcal{C}$ is at distance n from $\mathcal{C}$. Thus $\rho = n$, which contradicts our assumption. □

Lemma 2.29. $K_{\mathrm{R}}(q, m, n+n', \rho+\rho') \leq K_{\mathrm{R}}(q, m, n, \rho) K_{\mathrm{R}}(q, m, n', \rho')$ *for all* $m > 0$ *and nonnegative* n, n', ρ, *and* ρ'. *In particular,* $K_{\mathrm{R}}(q, m, n+1, \rho+1) \leq K_{\mathrm{R}}(q, m, n, \rho)$ *and* $K_{\mathrm{R}}(q, m, n+1, \rho) \leq q^m K_{\mathrm{R}}(q, m, n, \rho)$.

Proof. For all $\mathbf{x}, \mathbf{y} \in \mathrm{GF}(q^m)^n$ and $\mathbf{x}', \mathbf{y}' \in \mathrm{GF}(q^m)^{n'}$, we have $d_{\mathrm{R}}((\mathbf{x}, \mathbf{x}'), (\mathbf{y}, \mathbf{y}')) \leq d_{\mathrm{R}}(\mathbf{x}, \mathbf{y}) + d_{\mathrm{R}}(\mathbf{y}, \mathbf{y}')$. Therefore, for any $\mathcal{C} \in \mathrm{GF}(q^m)^n$, $\mathcal{C}' \in \mathrm{GF}(q^m)^{n'}$, we have $\rho(\mathcal{C} \oplus \mathcal{C}') \leq \rho(\mathcal{C}) + \rho(\mathcal{C}')$ and the first claim follows. In particular, $(n', \rho') = (1, 1)$ and $(n', \rho') = (1, 0)$ yield the other two claims respectively. □

2.5.2 Lower bounds for the sphere covering problem

We now derive nontrivial lower bounds on $K_{\mathrm{R}}(q, m, n, \rho)$.

Proposition 2.30. *For* $0 < \rho < n \leq m$ *and* $0 \leq l \leq \lfloor \log_{q^m} K_{\mathrm{R}}(q,m,n,\rho) \rfloor$,

$$K_{\mathrm{R}}(q,m,n,\rho) \geq \frac{1}{V_{\mathrm{R}}(\rho) - I(\rho, n-l)} \Bigg[q^{mn} - q^{lm} I(\rho, n-l) + \sum_{a=\max\{1, n-2\rho+1\}}^{l} (q^{am} - q^{(a-1)m}) I(\rho, n-a+1) \Bigg]. \quad (2.6)$$

Proof. Let $\mathcal{C} = \{\mathbf{c}_i\}_{i=0}^{K-1}$ be any code of length n and covering radius ρ over $\mathrm{GF}(q^m)$. By definition, $\mathcal{C}$ covers all q^{mn} vectors in $\mathrm{GF}(q^m)^n$; however, by Lemma 2.26, it cannot cover more than $B_{\mathrm{R}}(|\mathcal{C}|, \rho)$ vectors. Therefore, $|\mathcal{C}| \geq \min\{K : B_{\mathrm{R}}(K, \rho) \geq q^{mn}\}$, which yields (2.6). □

Note that the RHS of (2.6) is a non-decreasing function of l, thus the bound is tightest when $l = \lfloor \log_{q^m} K_{\mathrm{R}}(q,m,n,\rho) \rfloor$. Although $K_{\mathrm{R}}(q,m,n,\rho)$ is unknown in general, this bound can be used iteratively: we start with any lower bound on $K_{\mathrm{R}}(q,m,n,\rho)$, and using the largest l the RHS of (2.6) results in a new lower bound on $K_{\mathrm{R}}(q,m,n,\rho)$; we repeat this until (2.6) does not offer any improvement on the value of $\lfloor \log_{q^m} K_{\mathrm{R}}(q,m,n,\rho) \rfloor$. The initial condition could be either any *other* lower bound on $K_{\mathrm{R}}(q,m,n,\rho)$, or $l = 0$ (which actually is a refinement of the lower bound in Proposition 2.27).

Corollary 2.31. *For* $0 < \rho < n \leq m$, $K_{\mathrm{R}}(q,m,n,\rho) \geq \frac{q^{mn} - I(\rho,n)}{V_{\mathrm{R}}(\rho) - I(\rho,n)}$.

Proof. This is a special case of Proposition 2.30 for $l = 0$. □

Corollary 2.32. *For all* m, n, *and* $0 < \rho \leq \lfloor n/2 \rfloor$,

$$K_{\mathrm{R}}(q,m,n,\rho) \geq \frac{q^{mn} - q^{m(n-2\rho)+\rho^2} \begin{bmatrix} 2\rho \\ \rho \end{bmatrix}}{V_{\mathrm{R}}(\rho) - q^{\rho^2} \begin{bmatrix} 2\rho \\ \rho \end{bmatrix}}.$$

Proof. Since the balls of rank radius ρ around the codewords of an $(n, n-2\rho, 2\rho+1)$ MRD code do not intersect, $q^{mn} \geq V_{\mathrm{R}}(q,m,n,\rho) q^{m(n-2\rho)}$. By the sphere covering

bound, we obtain $K_{\mathrm{R}}(q,m,n,\rho) \geq q^{m(n-2\rho)}$ and hence $\log_{q^m} K_{\mathrm{R}}(q,m,n,\rho) \geq n-2\rho$. Use Proposition 2.30 for $l = n-2\rho \geq 0$, and $I(\rho,2\rho) = q^{\rho^2}\begin{bmatrix}2\rho\\ \rho\end{bmatrix}$ by Proposition 2.25. □

The bound in Corollary 2.32 can be viewed as the counterpart in the rank metric of the bound in [47, Theorem 1].

Van Wee [48, 49] derived several bounds on codes with Hamming covering radii based on the excess of a code, which is determined by the number of codewords covering the same vectors. Although the concepts in [48, 49] were developed for the Hamming metric, they are in fact independent of the underlying metric and we adapt them to the rank metric. For all $V \subseteq \mathrm{GF}(q^m)^n$ and a code $\mathcal{C}$ with covering radius ρ, the excess on V by $\mathcal{C}$ is defined to be $E_{\mathcal{C}}(V) \stackrel{\text{def}}{=} \sum_{\mathbf{c}\in\mathcal{C}} |B_\rho(\mathbf{c}) \cap V| - |V|$. If $\{W_i\}$ is a family of disjoint subsets of $\mathrm{GF}(q^m)^n$, then $E_{\mathcal{C}}\left(\bigcup_i W_i\right) = \sum_i E_{\mathcal{C}}(W_i)$. We define $\mathcal{Z} \stackrel{\text{def}}{=} \{\mathbf{z} \in \mathrm{GF}(q^m)^n | E_{\mathcal{C}}(\{\mathbf{z}\}) > 0\}$, i.e., $\mathcal{Z}$ is the set of vectors covered by at least two codewords in $\mathcal{C}$. Note that $\mathbf{z} \in \mathcal{Z}$ if and only if $|B_\rho(\mathbf{z}) \cap \mathcal{C}| \geq 2$. It can be shown that $|\mathcal{Z}| \leq E_{\mathcal{C}}(\mathcal{Z}) = E_{\mathcal{C}}(\mathrm{GF}(q^m)^n) = |\mathcal{C}|V_{\mathrm{R}}(q,m,n,\rho) - q^{mn}$.

Before deriving the second nontrivial lower bound, we need the following adaptation of [49, Lemma 8]. Let $\mathcal{C}$ be a code with length n and rank covering radius ρ over $\mathrm{GF}(q^m)$. We define $\mathcal{A} \stackrel{\text{def}}{=} \{\mathbf{x} \in \mathrm{GF}(q^m)^n | d_{\mathrm{R}}(\mathbf{x},\mathcal{C}) = \rho\}$.

Lemma 2.33. *For $\mathbf{x} \in \mathcal{A}\backslash\mathcal{Z}$ and $0 < \rho < n$, we have that $E_{\mathcal{C}}(B_1(\mathbf{x})) \geq \epsilon$, where*

$$\epsilon \stackrel{def}{=} \left\lceil \frac{(q^m - q^\rho)(\begin{bmatrix}n\\1\end{bmatrix} - \begin{bmatrix}\rho\\1\end{bmatrix})}{q^\rho \begin{bmatrix}\rho+1\\1\end{bmatrix}} \right\rceil q^\rho \begin{bmatrix}\rho+1\\1\end{bmatrix} + (q^m - q^\rho)\left(\begin{bmatrix}\rho\\1\end{bmatrix} - \begin{bmatrix}n\\1\end{bmatrix}\right).$$

Proof. Since $\mathbf{x} \notin \mathcal{Z}$, there is a unique $\mathbf{c}_0 \in \mathcal{C}$ such that $d_{\mathrm{R}}(\mathbf{x},\mathbf{c_0}) = \rho$. By Proposition 2.24 we have $|B_\rho(\mathbf{c_0}) \cap B_1(\mathbf{x})| = 1 + (q^m - q^\rho)\begin{bmatrix}\rho\\1\end{bmatrix} + (q^\rho - 1)\begin{bmatrix}n\\1\end{bmatrix}$. For any codeword $\mathbf{c}_1 \in \mathcal{C}$ satisfying $d_{\mathrm{R}}(\mathbf{x},\mathbf{c}_1) = \rho + 1$, by Proposition 2.25 we have

$|B_\rho(\mathbf{c}_1) \cap B_1(\mathbf{x})| = q^\rho \begin{bmatrix} \rho+1 \\ 1 \end{bmatrix}$. Finally, for all other codewords $\mathbf{c}_2 \in \mathcal{C}$ at distance $> \rho+1$ from $\mathbf{x}$, we have $|B_\rho(\mathbf{c}_2) \cap B_1(\mathbf{x})| = 0$. Denoting $N \stackrel{\text{def}}{=} |\{\mathbf{c}_1 \in \mathcal{C} | d_{\mathrm{R}}(\mathbf{x}, \mathbf{c}_1) = \rho + 1\}|$, we obtain

$$\begin{aligned} E_{\mathcal{C}}(B_1(\mathbf{x})) &= \sum_{\mathbf{c} \in \mathcal{C}} |B_\rho(\mathbf{c}) \cap B_1(\mathbf{x})| - |B_1(\mathbf{x})| \\ &= (q^m - q^\rho) \begin{bmatrix} \rho \\ 1 \end{bmatrix} + N q^\rho \begin{bmatrix} \rho+1 \\ 1 \end{bmatrix} - \begin{bmatrix} n \\ 1 \end{bmatrix} (q^m - q^\rho) \\ &\equiv (q^m - q^\rho) \left(\begin{bmatrix} \rho \\ 1 \end{bmatrix} - \begin{bmatrix} n \\ 1 \end{bmatrix} \right) \mod \left(q^\rho \begin{bmatrix} \rho+1 \\ 1 \end{bmatrix} \right). \end{aligned}$$

The proof is completed by realizing that $(q^m - q^\rho) \left(\begin{bmatrix} \rho \\ 1 \end{bmatrix} - \begin{bmatrix} n \\ 1 \end{bmatrix} \right) < 0$, while $E_{\mathcal{C}}(B_1(\mathbf{x}))$ is a non-negative integer. □

For $\rho = n - 1$, Lemma 2.33 is improved to:

Corollary 2.34. *For $\mathbf{x} \in \mathcal{A} \backslash \mathcal{Z}$ and $\rho = n - 1$, $E_{\mathcal{C}}(B_1(\mathbf{x})) = \phi$, where $\phi \stackrel{def}{=} q^{n-1} \begin{bmatrix} n \\ 1 \end{bmatrix} |\mathcal{C}| - q^{n-1} \left(q^m + \begin{bmatrix} n-1 \\ 1 \end{bmatrix} \right)$.*

Proof. The proof calls the same arguments as the proof above, with $N = |\mathcal{C}| - 1$ for $\rho = n - 1$. □

Proposition 2.35. *If $\epsilon > 0$, then $K_{\mathrm{R}}(q, m, n, \rho) \geq \frac{q^{mn}}{V_{\mathrm{R}}(\rho) - \frac{\epsilon}{\delta} N_{\mathrm{R}}(q,m,n,\rho)}$, where $\delta \stackrel{def}{=} V_{\mathrm{R}}(1) - q^{\rho-1} \begin{bmatrix} \rho \\ 1 \end{bmatrix} - 1 + 2\epsilon$.*

The proof of Proposition 2.35, provided in Appendix 7.1.1, uses the approach in the proof of [49, Theorem 6] and is based on the concept of excess. The lower bounds in Propositions 2.30 and 2.35, when applicable, are at least as tight as the sphere covering bound. For $\rho = n-1$, Proposition 2.35 is refined into the following.

Corollary 2.36. *Let us denote the coefficients $q^{n-1} \begin{bmatrix} n \\ 1 \end{bmatrix}$ and $q^{n-1} \left(q^m + \begin{bmatrix} n-1 \\ 1 \end{bmatrix} \right)$ as α and β, respectively. $K_{\mathrm{R}}(q, m, n, n-1)$ satisfies $aK_{\mathrm{R}}(q, m, n, n-1)^2 - bK_{\mathrm{R}}(q, m, n, n-$*

$1)+c \geq 0$, *where* $a \stackrel{def}{=} \alpha[V_{\mathrm{R}}(n-1)+V_{\mathrm{R}}(n-2)]$, $b \stackrel{def}{=} V_{\mathrm{R}}(n-1)\big\{q^{n-2}\begin{bmatrix} n-1 \\ 1 \end{bmatrix} - V_{\mathrm{R}}(1)+\beta+1\big\}+2\alpha q^{mn}+\beta V_{\mathrm{R}}(n-2)$, *and* $c \stackrel{def}{=} q^{mn}\{2\beta+1+q^{n-2}\begin{bmatrix} n-1 \\ 1 \end{bmatrix} - V_{\mathrm{R}}(1)\}$.

The proof of Corollary 2.36 is given in Appendix 7.1.2.

We now derive a lower bound on $K_{\mathrm{R}}(q,m,n,\rho)$ based on the linear inequalities satisfied by covering codes.

Proposition 2.37. *For* $0 \leq \delta \leq \rho$, *let* $T_\delta = \min \sum_{i=0}^{n} A_i(\delta)$, *where the minimum is taken over all integer sequences* $\{A_i(\delta)\}$ *which satisfy* $A_i(\delta)=0$ *for* $0 \leq i \leq \delta-1$, $A_\delta(\delta) \geq 1$, $0 \leq A_i(\delta) \leq N_{\mathrm{R}}(i)$ *for* $\delta+1 \leq i \leq n$, *and* $\sum_{i=0}^{n} A_i(\delta) \sum_{s=0}^{\rho} J_{\mathrm{R}}(r,s,i) \geq N_{\mathrm{R}}(r)$ *for* $0 \leq r \leq n$. *Then* $K_{\mathrm{R}}(q^m,n,\rho) \geq \max_{0\leq\delta\leq\rho} T_\delta$.

Proof. Let $\mathcal{C}$ be a code with covering radius ρ. For any $\mathbf{u} \in \mathrm{GF}(q^m)^n$ at distance $0 \leq \delta \leq \rho$ from $\mathcal{C}$, let $A_i(\delta)$ denote the number of codewords at distance i from $\mathbf{u}$. Then $\sum_{i=0}^{n} A_i(\delta) = |\mathcal{C}|$ and we easily obtain $A_i(\delta)=0$ for $0 \leq i \leq \delta-1$, $A_\delta(\delta) \geq 1$, and $0 \leq A_i(\delta) \leq N_{\mathrm{R}}(i)$ for $\delta+1 \leq i \leq n$. Also, for $0 \leq r \leq n$, all the vectors at distance r from $\mathbf{u}$ are covered, hence $\sum_{i=0}^{n} A_i(\delta) \sum_{s=0}^{\rho} J_{\mathrm{R}}(r,s,i) \geq N_{\mathrm{R}}(r)$. □

We note that the notation $A_i(\delta)$ is used above since the constraints on the sequence depend on δ. Since T_δ is the solution of an integer linear programming, it is computationally infeasible to determine T_δ for very large parameter values.

2.5.3 Upper bounds for the sphere covering problem

From the perspective of covering, the following lemma gives a characterization of MRD codes in terms of ELSs.

Lemma 2.38. *Let* $\mathcal{C}$ *be an* (n,k) *linear code over* $\mathrm{GF}(q^m)$ *(*$n \leq m$*).* $\mathcal{C}$ *is an MRD code if and only if* $\mathcal{C} \oplus V = \mathrm{GF}(q^m)^n$ *for all* $V \in E_{n-k}(q,m,n)$.

Proof. Suppose $\mathcal{C}$ is an $(n, k, n-k+1)$ linear MRD code. It is clear that $\mathcal{C} \cap V = \{\mathbf{0}\}$ and hence $\mathcal{C} \oplus V = \mathrm{GF}(q^m)^n$ for all $V \in E_{n-k}(q, m, n)$. Conversely, suppose $\mathcal{C} \oplus V = \mathrm{GF}(q^m)^n$ for all $V \in E_{n-k}(q, m, n)$. Then $\mathcal{C}$ does not contain any nonzero codeword of weight $\leq n-k$, and hence its minimum distance is $n-k+1$. □

For $1 \leq u \leq \rho$, let $\alpha_0 = 1, \alpha_1, \ldots, \alpha_{m+u-1} \in \mathrm{GF}(q^{m+u})$ be a basis set of $\mathrm{GF}(q^{m+u})$ over $\mathrm{GF}(q)$, and let $\beta_0 = 1, \beta_1, \ldots, \beta_{m-1}$ be a basis of $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$. We define the *linear* mapping f between two vector spaces $\mathrm{GF}(q^m)$ and $S_m \stackrel{\text{def}}{=} S(\alpha_0, \alpha_1, \ldots, \alpha_{m-1})$ given by $f(\beta_i) = \alpha_i$ for $0 \leq i \leq m-1$. We remark that $\alpha_0 = \beta_0 = 1$ implies that f maps $\mathrm{GF}(q)$ to itself. This can be generalized to n-dimensional vectors, by applying f componentwise. We thus define $\bar{f} : \mathrm{GF}(q^m)^n \to \mathrm{GF}(q^{m+u})^n$ such that for any $\mathbf{v} = (v_0, \ldots, v_{n-1})$, $\bar{f}(\mathbf{v}) = (f(v_0), \ldots, f(v_{n-1}))$. Note that $\bar{f}$ depends on u, but we omit this dependence for simplicity of notation. This function $\bar{f}$ is a linear bijection from $\mathrm{GF}(q^m)^n$ to its image S_m^n, and hence $\bar{f}$ preserves the rank. $\bar{f}$ also introduces a connection between ELSs as shown below.

Lemma 2.39. *For $u \geq 1$, $r \leq n$, and any $V \in E_r(q, m, n)$, $\bar{f}(V) \subset W$, where $W \in E_r(q, m+u, n)$. Furthermore, $\bar{f}$ induces a bijection between $E_r(q, m, n)$ and $E_r(q, m+u, n)$.*

Proof. Let $B = \{\mathbf{b}_i\}$ be an elementary basis of $V \in E_r(q, m, n)$. Then, $\mathbf{b}_i \in \mathrm{GF}(q)^n$ and $\mathbf{b}_i = \bar{f}(\mathbf{b}_i)$. Thus, $\{\bar{f}(\mathbf{b}_i)\}$ form an elementary basis, and hence $\bar{f}(V) \subset W$, where $W \in E_r(q, m+u, n)$ with $\{\bar{f}(\mathbf{b}_i)\}$ as a basis. It is easy to verify that $\bar{f}$ induces a bijection between $E_r(q, m, n)$ and $E_r(q, m+u, n)$. □

Proposition 2.40. *Let $\mathcal{C}$ be an $(n, n-\rho, \rho+1)$ MRD code over $\mathrm{GF}(q^m)$ $(n \leq m)$ with covering radius ρ. For $0 \leq u \leq \rho$, the code $\bar{f}(\mathcal{C})$, where $\bar{f}$ is as defined above, is a code of length n over $\mathrm{GF}(q^{m+u})$ with cardinality $q^{m(n-\rho)}$ and covering radius ρ.*

Proof. The other parameters for the code are obvious, and it suffices to establish the covering radius. Let T_u be a subspace of $\mathrm{GF}(q^{m+u})$ with dimension u such that $S_m \oplus T_u = \mathrm{GF}(q^{m+u})$. Any $\mathbf{u} \in \mathrm{GF}(q^{m+u})^n$ can be expressed as $\mathbf{u} = \mathbf{v} + \mathbf{w}$, where $\mathbf{v} \in S_m^n$ and $\mathbf{w} \in T_u^n$. Hence $\mathrm{rk}(\mathbf{w}) \leq u$, and $\mathbf{w} \in W$ for some $W \in E_\rho(q, m+u, n)$ by Lemma 2.8. By Lemmas 2.38 and 2.39, we can express $\mathbf{v}$ as $\mathbf{v} = \bar{f}(\mathbf{c} + \mathbf{e}) = \bar{f}(\mathbf{c}) + \bar{f}(\mathbf{e})$, where $\mathbf{c} \in \mathcal{C}$ and $\mathbf{e} \in V$, such that $\bar{f}(V) \subset W$. Eventually, we have $\mathbf{u} = \bar{f}(\mathbf{c}) + \bar{f}(\mathbf{e}) + \mathbf{w}$, where $\bar{f}(\mathbf{e}) + \mathbf{w} \in W$, and thus $d(\mathbf{u}, \bar{f}(\mathbf{c})) \leq \rho$. Thus $\bar{f}(\mathcal{C})$ has covering radius $\leq \rho$. Finally, it is easy to verify that the covering radius of $\bar{f}(\mathcal{C})$ is exactly ρ. □

Corollary 2.41. *For $0 < \rho < n \leq m$, $K_{\mathrm{R}}(q, m, n, \rho) \leq q^{\max\{m-\rho, n\}(n-\rho)}$.*

Proof. We can construct an $(n, n-\rho)$ linear MRD code $\mathcal{C}$ over $\mathrm{GF}(q^\mu)$ with covering radius ρ, where $\mu = \max\{m-\rho, n\}$. By Proposition 2.40, $\hat{f}(\mathcal{C}) \subset \mathrm{GF}(q^m)^n$, where $\hat{f}$ is a rank-preserving mapping from $\mathrm{GF}(q^\mu)^n$ to a subset of $\mathrm{GF}(q^m)^n$ similar to $\bar{f}$ above, has covering radius $\leq \rho$. Thus, $K_{\mathrm{R}}(q, m, n, \rho) \leq |\hat{f}(\mathcal{C})| = |\mathcal{C}| = q^{\mu(n-\rho)}$. □

We use the properties of $K_{\mathrm{R}}(q, m, n, \rho)$ in Lemma 2.29 in order to obtain a tighter upper bound when $\rho > m - n$.

Proposition 2.42. *Given fixed m, n, and ρ, for any $0 < l \leq n$ and (n_i, ρ_i) for $0 \leq i \leq l-1$ so that $0 < n_i \leq n$, $0 \leq \rho_i \leq n_i$, and $n_i + \rho_i \leq m$ for all i, and $\sum_{i=0}^{l-1} n_i = n$ and $\sum_{i=0}^{l-1} \rho_i = \rho$, we have*

$$K_{\mathrm{R}}(q, m, n, \rho) \leq \min_{\{(n_i, \rho_i):\, 0 \leq i \leq l-1\}} \left\{ q^{m(n-\rho) - \sum_i \rho_i (n_i - \rho_i)} \right\}. \tag{2.7}$$

Proof. By Lemma 2.29, we have $K_{\mathrm{R}}(q, m, n, \rho) \leq \prod_i K_{\mathrm{R}}(q, m, n_i, \rho_i)$ for all possible sequences $\{\rho_i\}$ and $\{n_i\}$. For all i, we have $K_{\mathrm{R}}(q, m, n_i, \rho_i) \leq q^{(m-\rho_i)(n-\rho_i)}$ by Corollary 2.41, and hence $K_{\mathrm{R}}(q, m, n, \rho) \leq q^{\sum_i (m-\rho_i)(n_i-\rho_i)} = q^{m(n-\rho) - \sum_i \rho_i (n_i - \rho_i)}$. □

It is clear that the upper bound in (2.7) is tighter than the upper bound in Proposition 2.27. It can also be shown that it is tighter than the bound in Corollary 2.41.

The following upper bound is an adaptation of [37, Theorem 12.1.2].

Proposition 2.43. *For* $0 < \rho < n \leq m$, $K_{\mathrm{R}}(q,m,n,\rho) \leq \frac{1}{1-\log_{q^{mn}}(q^{mn}-V_{\mathrm{R}}(\rho))} + 1$.

Our proof, given in Appendix 7.1.3, adopts the approach used to prove [37, Theorem 12.1.2]. Refining [37, Theorem 12.2.1] for the rank metric, we obtain the following upper bound.

Proposition 2.44. *For* $0 < \rho < n \leq m$ *and* $a \stackrel{def}{=} \min\{n, 2\rho\}$,

$$K_{\mathrm{R}}(q,m,n,\rho) \leq k_{V_{\mathrm{R}}(\rho)} \left(\frac{1}{\min\{s,j\}} - \frac{1}{V_{\mathrm{R}}(\rho)} \right) + \frac{q^{mn}}{V_{\mathrm{R}}(\rho)} H_{\min\{s,j\}},$$

where $k_{V_{\mathrm{R}}(\rho)} = q^{mn} - V_{\mathrm{R}}(\rho) q^{m(n-a)}$, $s = V_{\mathrm{R}}(\rho) - \sum_{i=a-\rho}^{\rho} q^{i(a-i)} \begin{bmatrix} a \\ i \end{bmatrix}$, $j = \lceil V_{\mathrm{R}}(\rho) - V_{\mathrm{R}}(\rho)^2 q^{-ma} \rceil$, *and* $H_k \stackrel{def}{=} \sum_{i=1}^{k} \frac{1}{i}$ *is the* k*-th harmonic number.*

Proof. We denote the vectors of $\mathrm{GF}(q^m)^n$ as $\mathbf{v}_i$ for $i = 0, 1, \ldots, q^{mn} - 1$ and we consider a $q^{mn} \times q^{mn}$ square matrix $\mathbf{A}$ defined as $a_{i,j} = 1$ if $d_{\mathrm{R}}(\mathbf{v}_i, \mathbf{v}_j) \leq \rho$ and $a_{i,j} = 0$ otherwise. Note that each row and each column of $\mathbf{A}$ has exactly $V_{\mathrm{R}}(\rho)$ ones. We present an algorithm that selects K columns of $\mathbf{A}$ with no all-zero rows. These columns thus represent a code with cardinality K and covering radius ρ.

Set $\mathbf{A}_{V_{\mathrm{R}}(\rho)} = \mathbf{A}$ and $k_{V_{\mathrm{R}}(\rho)+1} = q^{mn}$. For $i = V_{\mathrm{R}}(\rho), V_{\mathrm{R}}(\rho) - 1, \ldots, 1$, repeat the following step: First, select from $\mathbf{A}_i$ a maximal set of K_i columns of weight i with pairwise disjoint supports; Then, remove these columns and all the $iK_i = k_{i+1} - k_i$ rows incident to one of them, and denote the remaining $k_i \times (q^{mn} - K_{V_{\mathrm{R}}(\rho)} - \cdots - K_i)$ matrix as $\mathbf{A}_{i-1}$. The set of all $K = K_{V_{\mathrm{R}}(\rho)} + \cdots + K_1$ selected columns hence contains no all-zero rows and forms a covering code.

For $2\rho \leq n$, we can select an $(n, n-2\rho, 2\rho+1)$ linear MRD code $\mathcal{C}$ for the first step. Since an MRD code is maximal, its codewords correspond to a maximal set of columns with disjoint supports. If $2\rho > n$, $\mathcal{C}$ is chosen to be a single codeword, and $K_{V_{\mathrm{R}}(\rho)} = 1$. Thus $K_{V_{\mathrm{R}}(\rho)} = q^{m(n-a)}$ and $k_{V_{\mathrm{R}}(\rho)} = q^{mn} - V_{\mathrm{R}}(\rho)q^{m(n-a)}$, where $a = \min\{n, 2\rho\}$.

We now establish two upper bounds on k_i for $1 \leq i \leq V_{\mathrm{R}}(\rho)$. First, it is obvious that $k_i \leq k_{V_{\mathrm{R}}(\rho)}$. Also, every row of $\mathbf{A}_{i-1}$ contains exactly $V_{\mathrm{R}}(\rho)$ ones; on the other hand, every column of $\mathbf{A}_{i-1}$ contains at most $i-1$ ones. Hence for $1 \leq i \leq V_{\mathrm{R}}(\rho)$, $V_{\mathrm{R}}(\rho)k_i \leq (i-1)(q^{mn} - K_{V_{\mathrm{R}}(\rho)} - \cdots - K_i) \leq (i-1)q^{mn}$, and thus

$$k_i \leq (i-1)\frac{q^{mn}}{V_{\mathrm{R}}(\rho)}. \tag{2.8}$$

Clearly $k_1 = 0$ by (2.8). We have $k_{V_{\mathrm{R}}(\rho)} \leq (i-1)\frac{q^{mn}}{V_{\mathrm{R}}(\rho)}$ if $i - 1 \geq j \stackrel{\text{def}}{=} \left\lceil \frac{V_{\mathrm{R}}(\rho)k_{V_{\mathrm{R}}(\rho)}}{q^{mn}} \right\rceil$.

We now establish an upper bound on $K = \sum_{i=1}^{V_{\mathrm{R}}(\rho)} K_i$. For any vector $\mathbf{x} \in \mathrm{GF}(q^m)^n$, we have $d_{\mathrm{R}}(\mathbf{x}, \mathcal{C}) \leq 2\rho$. This is trivial for $2\rho > n$, while for $2\rho \leq n$ this is because MRD codes are maximal codes. For $2\rho \leq n$, at least $q^{\rho^2}\begin{bmatrix} 2\rho \\ \rho \end{bmatrix}$ vectors in $B_\rho(\mathbf{x})$ are already covered by $\mathcal{C}$ by Proposition 2.25. For $2\rho > n$, it can be shown that at least $\sum_{i=n-\rho}^{\rho} q^{i(n-i)}\begin{bmatrix} n \\ i \end{bmatrix}$ vectors in $B_\rho(\mathbf{x})$ are already covered by $\mathcal{C}$. It follows that after the first step, the column weight is at most $s \stackrel{\text{def}}{=} V_{\mathrm{R}}(\rho) - \sum_{i=a-\rho}^{\rho} q^{i(a-i)}\begin{bmatrix} a \\ i \end{bmatrix}$. Since $s \geq \max\{1 \leq i < V_{\mathrm{R}}(\rho) : K_i > 0\}$, $K = K_{V_{\mathrm{R}}(\rho)} + \sum_{i=1}^{s} K_i = K_{V_{\mathrm{R}}(\rho)} + \frac{k_{V_{\mathrm{R}}(\rho)}}{s} + \sum_{i=2}^{s} \frac{k_i}{i(i-1)}$. Using the two upper bounds on k_i above, we obtain $K \leq k_{V_{\mathrm{R}}(\rho)}\left(\frac{1}{\min\{s,j\}} - \frac{1}{V_{\mathrm{R}}(\rho)}\right) + \frac{q^{mn}}{V_{\mathrm{R}}(\rho)}H_{\min\{s,j\}}$. □

Since [37, Theorem 12.1.2] is referred to as the Johnson-Stein-Lovász Theorem, we refer to the algorithm described in the proof of Proposition 2.44 as the Johnson-Stein-Lovász (JSL) algorithm. The upper bound in Proposition 2.44 can be loosened into the following.

Corollary 2.45. *For* $0 < \rho < n \leq m$, $K_{\mathrm{R}}(q,m,n,\rho) \leq \frac{q^{mn}}{V_{\mathrm{R}}(\rho)}\Big(\ln V_{\mathrm{R}}(\rho) + \gamma + \frac{1}{2V_{\mathrm{R}}(\rho)+1/3}\Big)$, *where* γ *is the Euler-Mascheroni constant [50].*

Proof. Using (2.8), we obtain $K = \sum_{i=1}^{V_{\mathrm{R}}(\rho)} \frac{k_{i+1}-k_i}{i} \leq \frac{q^{mn}}{V_{\mathrm{R}}(\rho)} + \sum_{i=2}^{V_{\mathrm{R}}(\rho)} \frac{k_i}{i(i-1)} \leq \frac{q^{mn}}{V_{\mathrm{R}}(\rho)} H_{V_{\mathrm{R}}(\rho)}$. The proof is concluded by $H_{V_{\mathrm{R}}(\rho)} < \ln V_{\mathrm{R}}(\rho) + \gamma + \frac{1}{2V_{\mathrm{R}}(\rho)+1/3}$ [50]. □

We now refine the upper bound in Proposition 2.44 by providing a nontrivial refinement of the greedy algorithm in [51].

Lemma 2.46. *Let* $\mathcal{C}$ *be a code which covers at least* $q^{mn} - u$ *vectors in* $\mathrm{GF}(q^m)^n$ *with radius* ρ. *Then for any* $k \geq |\mathcal{C}|$, *there exists a code with cardinality* k *which covers at least* $q^{mn} - u_k$ *vectors, where* $u_{|\mathcal{C}|} = u$ *and for* $k \geq |\mathcal{C}|$

$$u_{k+1} = u_k - \left\lceil \frac{u_k V_{\mathrm{R}}(\rho)}{\min\{q^{mn} - k, B_{\mathrm{R}}(u_k, \rho)\}} \right\rceil.$$

Thus $K_{\mathrm{R}}(q,m,n,\rho) \leq \min\{k : u_k = 0\}$.

Proof. The proof is by induction on k. By hypothesis, $\mathcal{C}$ is a code with cardinality $|\mathcal{C}|$ which leaves $u_{|\mathcal{C}|}$ vectors uncovered. Suppose there exists a code with cardinality k which leaves $t_k \leq u_k$ vectors uncovered, and denote the set of uncovered vectors as T_k. Let G be a graph where the vertex set is $\mathrm{GF}(q^m)^n$ and two vertices are adjacent if and only if their rank distance is at most ρ. Let $\mathbf{A}$ be the adjacency matrix of G and $\mathbf{A}_k$ be the t_k columns of $\mathbf{A}$ corresponding to T_k. There are $t_k V_{\mathrm{R}}(\rho)$ ones in $\mathbf{A}_k$, distributed across $|N(T_k)|$ rows, where $N(T_k)$ is the neighborhood of T_k. By construction, $N(T_k)$ does not contain any codeword, hence $|N(T_k)| \leq q^{mn} - k$. Also, by Lemma 2.26, $|N(T_k)| \leq B_{\mathrm{R}}(t_k, \rho) \leq B_{\mathrm{R}}(u_k, \rho)$. Thus $|N(T_k)| \leq \min\{q^{mn} - k, B_{\mathrm{R}}(u_k, \rho)\}$ and there exists a row with at least $\left\lceil \frac{t_k V_{\mathrm{R}}(\rho)}{\min\{q^{mn}-k, B_{\mathrm{R}}(u_k,\rho)\}} \right\rceil$ ones in $\mathbf{A}_k$. Adding the vector corresponding to this row to the code, we obtain a code with

cardinality $k+1$ which leaves at most $t_k - \left\lceil \frac{t_k V_{\mathrm{R}}(\rho)}{\min\{q^{mn}-k, B_{\mathrm{R}}(u_k,\rho)\}} \right\rceil \leq u_{k+1}$ vectors uncovered. □

The upper bound in Lemma 2.46 is nontrivial since the sequence $\{u_k\}$ is monotonically decreasing until it reaches 0 for $k \leq q^{mn}$. Since the sequence $\{u_k\}$ depends on $\mathcal{C}$ only through the number of vectors covered by $\mathcal{C}$, to obtain a tighter bound on $K_{\mathrm{R}}(q,m,n,\rho)$ based on Lemma 2.46, it is necessary to find a code $\mathcal{C}$ which leaves a smaller number of vectors uncovered. We consider two choices for $\mathcal{C}$ below. Since any codeword can cover at most $V_{\mathrm{R}}(\rho)$ vectors uncovered by the other codewords, we have $u \geq q^{mn} - V_{\mathrm{R}}(\rho)|\mathcal{C}|$. In the first choice, we consider the largest code $\mathcal{C}_0$ that achieves $u = q^{mn} - V_{\mathrm{R}}(\rho)|\mathcal{C}_0|$, which is an $(n, n-a, a+1)$ linear MRD code with $a = \min\{n, 2\rho\}$.

An alternative choice would be to select a supercode of $\mathcal{C}_0$, that is, an MRD code with a larger dimension. Since there may be intersection between balls of radius ρ around codewords, we now derive a lower bound on the number of vectors covered by only one codeword in an MRD code.

Lemma 2.47. *Let the vectors $\mathbf{c}_j \in \mathrm{GF}(q^m)^n$ be sorted such that $\{\mathbf{c}_j\}_{j=0}^{q^{m(n-l+1)}-1}$ is an $(n, n-l+1, l)$ MRD code for $1 \leq l \leq n$. For all $1 \leq k \leq q^{mn}-1$, we denote $\{\mathbf{c}_j\}_{j=0}^{k-1}$ as $\mathcal{C}_k$ and its minimum rank distance is given by $d_k = n - \lceil \log_{q^m}(k+1) \rceil + 1$. Then for $d_k \geq 2\rho+1$, $\mathbf{c}_k$ covers $V_{\mathrm{R}}(\rho)$ vectors not covered by $\mathcal{C}_k$. For $d_k \leq 2\rho$, $\mathbf{c}_k$ covers at least $V_{\mathrm{R}}(\rho) - \sum_{l=d_k}^{a} \mu_l I(\rho,l)$ vectors not covered by $\mathcal{C}_k$, where $a = \min\{n, 2\rho\}$, $\mu_{d_k} = \min\{M(d_k,d_k), k\}$, and $\mu_l = \min\left\{M(d_k,l), k - \sum_{j=d_k}^{l-1} \mu_j\right\}$ for $l > d_k$.*

Proof. The case $d_k \geq 2\rho+1$ is straightforward. We assume $d_k \leq 2\rho$ henceforth. We denote the number of codewords in $\mathcal{C}_k$ at distance l $(0 \leq l \leq n)$ from $\mathbf{c}_k$ as $M_l^{(k)}$. Since a codeword in $\mathcal{C}_k$ at distance l from $\mathbf{c}_k$ covers exactly $I(\rho,l)$ vectors

also covered by $\mathbf{c}_k$, $\mathbf{c}_k$ covers at least $V_{\mathrm{R}}(\rho) - \sum_{l=d_k}^{a} M_l^{(k)} I(\rho, l)$ vectors that are not covered by $\mathcal{C}_k$. Since the value of $M_l^{(k)}$ is unknown, we give a lower bound on the quantity above. Since $I(\rho, l)$ is a non-increasing function of l, the sequence $\{\mu_l\}$ as defined above minimizes the value of $V_{\mathrm{R}}(\rho) - \sum_{l=d_k}^{a} M_l^{(k)} I(\rho, l)$ under the constraints $0 \leq M_l^{(k)} \leq M(d_k, l)$ and $\sum_{l=d_k}^{n} M_l^{(k)} = k$. Thus, $\mathbf{c}_k$ covers at least $V_{\mathrm{R}}(\rho) - \sum_{l=d_k}^{a} \mu_l I(\rho, l)$ vectors not covered by $\mathcal{C}_k$. □

Proposition 2.48. *Let $a = \min\{n, 2\rho\}$, $K_0 = q^{m(n-a)}$, and $u_{K_0} = q^{mn} - q^{m(n-a)} V_{\mathrm{R}}(\rho)$. Consider two sequences $\{h_k\}$ and $\{u'_k\}$, both of which are upper bounds on the number of vectors yet to be covered by a code of cardinality k, given by $h_{K_0} = u'_{K_0} = u_{K_0}$ and for $k \geq K_0$*

$$\begin{aligned} h_{k+1} &= h_k - \lambda_{k+1}, \\ u'_{k+1} &= \min\left\{ h_{k+1}, u'_k - \left\lceil \frac{u'_k V_{\mathrm{R}}(\rho)}{\min\{q^{mn} - k, B_{\mathrm{R}}(u'_k, \rho)\}} \right\rceil \right\}. \end{aligned}$$

Then, $K_{\mathrm{R}}(q, m, n, \rho) \leq \min\{k : u'_k = 0\}$.

Proof. Let $\mathcal{C}_0$ be an $(n, n-a, a+1)$ MRD code over $\mathrm{GF}(q^m)$. $\mathcal{C}_0$ has cardinality K_0 and covers $q^{m(n-a)} V_{\mathrm{R}}(\rho) = q^{mn} - u_{K_0}$ vectors in $\mathrm{GF}(q^m)^n$. By Lemma 2.47, adding $k - K_0$ codewords of an MRD code which properly contains $\mathcal{C}_0$ leads to a code with cardinality k which covers at least $q^{mn} - h_k$ vectors. On the other hand, u'_k is the upper bound on the number of vectors yet to be covered by a code of cardinality k that is obtained recursively either by applying the greedy approach in the proof of Lemma 2.46 or by adding more codewords based on the MRD codes as described in the proof of Lemma 2.47. The recursion of u'_k follows from this construction. Since this recursion is constructive, there exists a code with cardinality k which leaves at most u'_k vectors uncovered, and hence $K_{\mathrm{R}}(q, m, n, \rho) \leq \min\{k : u'_k = 0\}$. □

We now construct a new class of covering codes with the rank metric. We assume all the vectors in $\mathrm{GF}(q^m)^n$ are expanded with respect to a given basis of $\mathrm{GF}(q^m)$ to $m \times n$ matrices over $\mathrm{GF}(q)$. First, for any positive integer k, we denote $S_k \stackrel{\text{def}}{=} \{0, 1, \ldots, k-1\}$. For $\mathbf{V} \in \mathrm{GF}(q)^{m\times n}$, $I \subseteq S_m$, and $J \subseteq S_n$, we denote $\mathbf{V}(I, J) = (v_{i,j})_{i\in I, j\in J}$, where the indexes are all sorted increasingly. Consider the code $\mathcal{C}$ which consists of all matrices $\mathbf{C} \in \mathrm{GF}(q)^{m\times n}$ with $\mathbf{C}(S_\rho, S_n) = \mathbf{0}$ and with at most $n - \rho$ nonzero columns.

Proposition 2.49. *$\mathcal{C}$ has covering radius ρ and $K_{\mathrm{R}}(q, m, n, \rho) \leq \sum_{i=0}^{n-\rho} \binom{n}{i} (q^{m-\rho} - 1)^i$.*

Proof. First, the cardinality of $\mathcal{C}$ is given by the number of vectors in $\mathrm{GF}(q^{m-\rho})^n$ with Hamming weight at most $n - \rho$. It remains to prove that $\mathcal{C}$ has rank covering radius ρ. Suppose $\mathbf{V} \in \mathrm{GF}(q)^{m\times n}$ has $\mathrm{rk}(\mathbf{V}(S_\rho, S_n)) = r$ $(0 \leq r \leq \rho)$, then there exist $I \subseteq S_\rho$ and $J \subseteq S_n$ such that $|I| = |J| = \mathrm{rk}(\mathbf{V}(I, J)) = \mathrm{rk}(\mathbf{V}(S_m, J)) = \mathrm{rk}(\mathbf{V}(I, S_n)) = r$. For $\rho \leq i \leq m-1$, let $\mathbf{l}_i = \mathbf{V}(\{i\}, J)\mathbf{V}(I, J)^{-1} \in \mathrm{GF}(q)^{1\times r}$. Define $\mathbf{U}(S_\rho, S_n) = \mathbf{V}(S_\rho, S_n)$ and $\mathbf{U}(\{i\}, S_n) = \mathbf{l}_i\mathbf{V}(I, S_n)$ for all $\rho \leq i \leq m-1$. All the rows of $\mathbf{U}$ are in the row span of $\mathbf{V}(I, S_n)$, therefore $\mathrm{rk}(\mathbf{U}) = r$. Also, $\mathbf{U}(\{i\}, J) = \mathbf{l}_i\mathbf{V}(I, J) = \mathbf{V}(\{i\}, J)$ for $\rho \leq i \leq m-1$ and hence $\mathbf{U}(S_m, J) = \mathbf{V}(S_m, J)$. Thus there exists $\mathbf{U} \in \mathrm{GF}(q)^{m\times n}$ such that $\mathrm{rk}(\mathbf{U}) = r$, $\mathbf{U}(S_\rho, S_n) = \mathbf{V}(S_\rho, S_n)$, and $\mathbf{U}(S_m, J) = \mathbf{V}(S_m, J)$. We also construct $\mathbf{U}' \in \mathrm{GF}(q)^{m\times n}$ by setting $\mathbf{U}'(S_m, J') = \mathbf{V}(S_m, J')$ and $\mathbf{U}'(S_m, S_n \backslash J') = \mathbf{U}(S_m, S_n \backslash J')$, where $|J'| = \rho - r$ and $J \cap J' = \emptyset$. For $\mathbf{C} = \mathbf{V} - \mathbf{U}'$, $\mathbf{C}(S_\rho, S_n) = \mathbf{0}$ and $\mathbf{C}(S_m, J \cup J') = \mathbf{0}$. Therefore, $\mathbf{C} \in \mathcal{C}$ and $d_{\mathrm{R}}(\mathbf{V}, \mathbf{C}) = \mathrm{rk}(\mathbf{U}') \leq \mathrm{rk}(\mathbf{U}) + |J'| = \rho$. □

In order to illustrate the construction in Proposition 2.49, we construct a code over $\mathrm{GF}(2^3)^3$ with covering radius 2 and cardinality 4. Expanding the codewords

according to a basis of $\mathrm{GF}(2^3)$ over $\mathrm{GF}(2)$, the code is given by

$$\mathcal{C} = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}. \tag{2.9}$$

It can be shown using brute force verification that $K_{\mathrm{R}}(2,3,3,2) \geq 4$, and hence $\mathcal{C}$ is an optimal rank metric covering code.

We give an example below of how to determine a codeword $\mathbf{C} \in \mathcal{C}$ at distance at most ρ from a given matrix $\mathbf{V}$. Let $\mathbf{V} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$, then using the notations introduced in the proof of Proposition 2.49, we obtain $\mathbf{U}' = \mathbf{U} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ and hence $\mathbf{C} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

2.5.4 Covering properties of linear rank metric codes

Proposition 2.27 yields bounds on the dimension of a linear code with a given rank covering radius.

Proposition 2.50. *An (n,k) linear code over $\mathrm{GF}(q^m)$ with rank covering radius ρ satisfies $n - \rho - \frac{\rho(n-\rho) - \log_q K_q}{m} < k \leq n - \rho$.*

Proof. The upper bound was proved as part of the proof of Proposition 2.27. We now prove the lower bound. By the sphere covering bound, we have $q^{mk} > \frac{q^{mn}}{V_{\mathrm{R}}(\rho)}$.

However, by Lemma 2.18 we have $V_{\mathrm{R}}(\rho) < q^{\rho(m+n-\rho)-\log_q K_q}$ and hence $q^{mk} > q^{mn-\rho(m+n-\rho)+\log_q K_q}$. □

We do not adapt the bounds in Propositions 2.30 and 2.35 as their advantage over the lower bound in Proposition 2.50 is not significant. Next, we show that the dimension of a linear code with a given rank covering radius can be determined under some conditions.

Proposition 2.51. *Let $\mathcal{C}$ be an (n,k) linear code over $\mathrm{GF}(q^m)$ $(n \leq m)$ with rank covering radius ρ. Then $k = n - \rho$ if $\rho \in \{0, 1, n-1, n\}$ or $\rho(n-\rho) \leq m + \log_q K_q$, or if $\mathcal{C}$ is a generalized Gabidulin code or an ELS.*

Proof. The cases $\rho \in \{0, n-1, n\}$ are straightforward. In all other cases, since $k \leq n - \rho$ by Proposition 2.50, it suffices to prove that $k \geq n - \rho$. First, suppose $\rho = 1$, then k satisfies $q^{mk} > \frac{q^{mn}}{V_{\mathrm{R}}(1)}$ by the sphere covering bound. However, $V_{\mathrm{R}}(1) < q^{m+n} \leq q^{2m}$, and hence $k > n-2$. Second, if $\rho(n-\rho) \leq m + \log_q K_q$, then $0 < \frac{1}{m}\left(\rho(n-\rho) - \log_q K_q\right) \leq 1$ and $k \geq n - \rho$ by Proposition 2.50. Third, if $\mathcal{C}$ is an $(n, k, n-k+1)$ generalized Gabidulin code with $k < n$, then there exists an $(n, k+1, n-k)$ generalized Gabidulin code $\mathcal{C}'$ such that $\mathcal{C} \subset \mathcal{C}'$. We have $\rho \geq d_{\mathrm{R}}(\mathcal{C}') = n - k$, as noted in Section 2.5.1, and hence $k \geq n - \rho$. The case $k = n$ is straightforward. Finally, if $\mathcal{C}$ is an ELS of dimension k, then for all $\mathbf{x}$ with rank n and for any $\mathbf{c} \in \mathcal{C}$, $d_{\mathrm{R}}(\mathbf{x}, \mathbf{c}) \geq \mathrm{rk}(\mathbf{x}) - \mathrm{rk}(\mathbf{c}) \geq n - k$. □

A similar argument can be used to bound the covering radius of the cartesian products of generalized Gabidulin codes.

Corollary 2.52. *Let $\mathcal{G}$ be an (n, k, d_{R}) generalized Gabidulin code $(n \leq m)$, and let $\mathcal{G}^l$ be the code obtained by l cartesian products of $\mathcal{G}$ for $l \geq 1$. Then the rank covering radius of $\mathcal{G}^l$ satisfies $\rho(\mathcal{G}^l) \geq d_{\mathrm{R}} - 1$.*

Note that when $n = m$, $\mathcal{G}^l$ is a maximal code, and hence Corollary 2.52 can be further strengthened.

Corollary 2.53. *Let $\mathcal{G}$ be an (m, k, d_{R}) generalized Gabidulin code over $\mathrm{GF}(q^m)$, and let $\mathcal{G}^l$ be the code obtained by l cartesian products of $\mathcal{G}$. Then $\rho(\mathcal{G}^l) = d_{\mathrm{R}} - 1$.*

2.5.5 Numerical methods

In addition to the above bounds, we use several different numerical methods to obtain tighter upper bounds for relatively small values of m, n, and ρ. First, the JSL algorithm described in the proof of Proposition 2.44 is implemented for small parameter values. Second, local search algorithms [37] similar to the ones available for Hamming metric codes are somewhat less complex than the JSL algorithm. Although the complexity for large parameter values is prohibitive, it is feasible. Third, we construct linear codes with good covering properties, because linear codes have lower complexity.

We can verify if a covering radius is achievable by a given code size by brute force verification, thereby establishing lower bounds on $K_{\mathrm{R}}(q, m, n, \rho)$. Obviously, this is practical for only small parameter values.

2.5.6 Tables

In Table 2.1, we provide bounds on $K_{\mathrm{R}}(q, m, n, \rho)$, for $2 \leq m \leq 7$, $2 \leq n \leq m$, and $1 \leq \rho \leq 6$. Obviously, $K_{\mathrm{R}}(q, m, n, \rho) = 1$ when $\rho = n$. For other sets of parameters, the tightest lower and upper bounds on $K_{\mathrm{R}}(q, m, n, \rho)$ are given, and letters associated with the numbers are used to indicate the tightest bound. The lower case letters a–f correspond to the lower bounds in Propositions 2.28 and 2.30,

m	n	$\rho = 1$	$\rho = 2$	$\rho = 3$
2	2	d 3 E	1	
3	2	d 4 A	1	
	3	d 11-16 E	g 4 B	1
4	2	d 7-8 A	1	
	3	d 40-64 A	c 4-7 E	1
	4	e 293-722 E	d 10-48 F	a 3-5 D
5	2	d 12-16 A	1	
	3	d 154-256 A	c 6-8 A	1
	4	d 2267-4096 A	d 33-256 B	c 4-8 B
	5	d 34894-2^{17} B	d 233-2773 C	f 10-32 G
6	2	d 23-32 A	1	
	3	d 601-1024 A	c 11-16 A	1
	4	d 17822-2^{15} A	c 124-256 A	c 6-16 B
	5	d 550395-2^{20} A	d 1770-2^{14} B	e 31-256 B
	6	e 17318410-2^{26} B	e 27065-401784 C	e 214-4092 C
7	2	d 44-64 A	1	
	3	d 2372-4096 A	c 20-32 A	1
	4	d 141231-2^{18} A	e 484-1024 A	b 10-16 A
	5	d 8735289-2^{24} A	d 13835-2^{15} A	b 112-1024 B
	6	d 549829402-2^{30} A	e 42229-2^{22} B	b 1585-2^{15} B
	7	d 34901004402-2^{37} B	e 13205450-233549482 C	b 23979-573590 C

m	n	$\rho = 4$	$\rho = 5$	$\rho = 6$
5	5	a 3-6 D	1	
6	5	b 4-16 B	1	
	6	e 9-154 D	a 3-7 D	1
7	5	b 6-16 B	1	
	6	e 29-708 C	b 4-16 B	1
	7	e 203-5686 C	f 9-211 D	a 3-8 D

Table 2.1: Bounds on $K_{\mathrm{R}}(q, m, n, \rho)$, for $2 \leq m \leq 7$, $2 \leq n \leq m$, and $1 \leq \rho \leq 6$.

Corollaries 2.31 and 2.32, and Propositions 2.35 and 2.37 respectively. The lower case letter g corresponds to lower bounds obtained by brute force verification. The upper case letters A–D denote the upper bounds in Corollary 2.41 and Propositions 2.42, 2.48, and 2.49 respectively. The upper case letters E–G correspond to upper bounds obtained by the JSL algorithm, local search algorithm, and explicit linear constructions respectively.

In Table 2.2, we provide bounds on the minimum dimension k for $q = 2$, $4 \leq m \leq 8$, $4 \leq n \leq m$, and $2 \leq \rho \leq 6$. The unmarked entries correspond to Proposition 2.51. The lower case letters a and b correspond to the lower bound in Proposition 2.50 and the adaptation of Corollary 2.32 to linear codes respectively. The lower case letter c corresponds to lower bounds obtained by brute force verification for linear codes. The upper case letter A corresponds to the upper bound in Proposition 2.50. The upper case letter B corresponds to upper bounds obtained by explicit linear constructions.

In Appendix 7.1.4, we present the codes, obtained by the numerical methods in Section 2.5.5, that achieve the tightest upper bounds in Tables 2.1 and 2.2.

2.5.7 Asymptotic covering properties

Table 2.1 provides solutions to the sphere covering problem for only small values of m, n, and ρ. Next, we study the asymptotic covering properties when both block length and minimum rank distance go to infinity. As in Section 2.3, we consider the case where $\lim_{n\to\infty} \frac{n}{m} = \nu$, where ν is a constant. In other words, these asymptotic covering properties provide insights on the covering properties of long rank metric codes over large fields.

The asymptotic form of the bounds in Lemma 2.18 are given in the lemma below.

m	n	$\rho = 2$	$\rho = 3$	$\rho = 4$	$\rho = 5$	$\rho = 6$
4	4	b 2 A	1	0		
5	4	c 2 A	1	0		
	5	a 2-3 A	a 1 B	1	0	
6	4	2	1	0		
	5	a 2-3 A	a 1-2 A	1	0	
	6	a 3-4 A	a 2-3 A	a 1-2 A	1	0
7	4	2	1	0		
	5	a 2-3 A	a 1-2 A	1	0	
	6	a 3-4 A	a 2-3 A	a 1-2 A	1	0
	7	a 4-5 A	a 3-4 A	a 2-3 A	a 1-2 A	1
8	4	2	1	0		
	5	3	2	1	0	
	6	a 3-4 A	a 2-3 A	a 1-2 A	1	0
	7	a 4-5 A	a 3-4 A	a 2-3 A	a 1-2 A	1
	8	a 5-6 A	a 3-5 A	a 2-4 A	a 1-3 A	a 1-2 A

Table 2.2: Bounds on k for $q = 2$, $4 \leq m \leq 8$, $4 \leq n \leq m$, and $2 \leq \rho \leq 6$.

Lemma 2.54. *For* $0 \leq \delta \leq \min\{1, \nu^{-1}\}$, $\lim_{n\to\infty} \left[\log_{q^{mn}} V_{\mathrm{R}}(q, m, n, \lfloor \delta n \rfloor)\right] = \delta(1 + \nu - \nu\delta)$.

Proof. By Lemma 2.18, we have $q^{d(m+n-d)} \leq V_{\mathrm{R}}(d) < K_q^{-1} q^{d(m+n-d)}$. Taking the logarithm, this becomes $\delta(1 + \nu - \nu\delta) \leq \log_{q^{mn}} V_{\mathrm{R}}(\lfloor \delta n \rfloor) < \delta(1 + \nu - \nu\delta) - \frac{\log_q K_q}{mn}$. The proof is concluded by taking the limit when n tends to infinity. □

Define $r \stackrel{\text{def}}{=} \frac{\rho}{n}$ and $k(r) = \lim_{n\to\infty} \inf \left[\log_{q^{mn}} K_{\mathrm{R}}(q, m, n, \rho)\right]$. The bounds in Proposition 2.27 and Corollary 2.45 together solve the asymptotic sphere covering problem.

Theorem 2.55. *For all* ν *and* r, $k(r) = (1 - r)(1 - \nu r)$.

Proof. By Lemma 2.54 the sphere covering bound asymptotically becomes $k(r) \geq (1 - r)(1 - \nu r)$. Also, by Corollary 2.45, $K_{\mathrm{R}}(q, m, n, \rho) \leq \frac{q^{mn}}{V_{\mathrm{R}}(\rho)} \left[1 + \ln V_{\mathrm{R}}(\rho)\right] \leq$

$\frac{q^{mn}}{V_{\mathrm{R}}(\rho)}\left[1+mn\ln q\right]$ and hence $\log_{q^{mn}} K_{\mathrm{R}}(q,m,n,\rho) \leq \log_{q^{mn}} \frac{q^{mn}}{V_{\mathrm{R}}(\rho)} + O((mn)^{-1}\ln mn)$. By Lemma 2.54, this asymptotically becomes $k(r) \leq (1-r)(1-\nu r)$. Note that although we assume $n \leq m$ above for convenience, both bounds in Proposition 2.27 and Corollary 2.45 hold for any values of m and n. □

Chapter 3

MacWilliams Identity for the Rank Metric

3.1 Introduction

The MacWilliams identity for codes with the Hamming metric [36], which relates the Hamming weight distribution of a code to the weight distribution of its dual code, is useful in determining the Hamming weight distribution of codes. This is because if the dual code has a small number of codewords or equivalence classes of codewords under some known permutation group, its weight distribution can be obtained by exhaustive examination. It also leads to other identities for the weight distribution such as the Pless identities [36, 52].

In [12], the counterpart of the MacWilliams identity, which relates the rank distance enumerator of a code to that of its dual code, was established using association schemes. However, Delsarte's work lacks an expression of the rank weight enumerator of the dual code as a functional transformation of the enumerator of the

code. In [53, 54], Grant and Varanasi defined a *different* rank weight enumerator and established a functional transformation between the rank weight enumerator of a code and that of its dual code.

In this chapter we show that, similar to the MacWilliams identity for the Hamming metric, the rank weight distribution of any linear code can be expressed as a functional transformation of that of its dual code. It is remarkable that our MacWilliams identity for the rank metric has a similar form to that for the Hamming metric. Similarly, an intermediate result of our proof is that the rank weight enumerator of the dual of any vector depends on only the rank weight of the vector and is related to the rank weight enumerator of a maximum rank distance (MRD) code. We also derive additional identities that relate moments of the rank weight distribution of a linear code to those of its dual code.

Our work differs from those in [12, 53, 54] in several aspects:

- We consider a rank weight enumerator different from that in [53, 54], and solve the original problem of determining the functional transformation of rank weight enumerators between dual codes as defined by Delsarte.

- Our proof, based on character theory, does not require the use of association schemes as in [12] or combinatorial arguments as in [53, 54].

- In [12], the MacWilliams identity is given between the rank distance enumerator sequences of two dual array codes using the q-Krawtchouk polynomials. Our identity is equivalent to that in [12] for linear rank metric codes, although our identity is expressed using different parameters which are shown to be the q-Krawtchouk polynomials as well. We also present this identity in the form of a functional transformation (cf. Theorem 3.17). In such a form, the

MacWilliams identities for both the rank and the Hamming metrics are similar to each other.

- The functional transformation form allows us to derive further identities (cf. Section 3.4) between the rank weight distribution of linear dual codes. We would like to stress that the identities between the moments of the rank distribution proved here are novel and were not considered in the aforementioned papers.

We remark that both the matrix form [12, 14] and the vector form [13] for rank metric codes have been considered in the literature. Following [13], in this chapter the vector form over $\mathrm{GF}(q^m)$ is used for rank metric codes although their rank weight is defined by their corresponding codematrices over $\mathrm{GF}(q)$ [13]. The vector form is chosen in this chapter since our results and their derivations for rank metric codes can be readily related to their counterparts for Hamming metric codes.

The rest of the chapter is organized as follows. Section 3.2 reviews some necessary background. In Section 3.3, we establish the MacWilliams identity for the rank metric. We study the moments of the rank distributions of linear codes in Section 3.4.

3.2 Preliminaries

For all $\mathbf{v} \in \mathrm{GF}(q^m)^n$ with rank weight r, the rank weight function of $\mathbf{v}$ is defined as $f_{\mathrm{R}}(\mathbf{v}) = y^r x^{n-r}$. Let $\mathcal{C}$ be a code of length n over $\mathrm{GF}(q^m)$. Suppose there are A_i codewords in $\mathcal{C}$ with rank weight i $(0 \leq i \leq n)$. Then the rank weight enumerator

of $\mathcal{C}$, denoted as $W_{\mathcal{C}}^{\mathrm{R}}(x,y)$, is defined to be

$$W_{\mathcal{C}}^{\mathrm{R}}(x,y) \stackrel{\mathrm{def}}{=} \sum_{\mathbf{v}\in\mathcal{C}} f_{\mathrm{R}}(\mathbf{v}) = \sum_{i=0}^{n} A_i y^i x^{n-i}.$$

Definition 3.1 ([36]). *Let $\mathbb{C}$ be the field of complex numbers. Let $a \in \mathrm{GF}(q^m)$ and let $\{1, \alpha_1, \ldots, \alpha_{m-1}\}$ be a basis set of $\mathrm{GF}(q^m)$. We thus have $a = a_0 + a_1\alpha_1 + \ldots + a_{m-1}\alpha_{m-1}$, where $a_i \in \mathrm{GF}(q)$ for $0 \le i \le m-1$. Finally, letting $\zeta \in \mathbb{C}$ be a primitive q-th root of unity, $\chi(a) \stackrel{def}{=} \zeta^{a_0}$ maps $\mathrm{GF}(q^m)$ to $\mathbb{C}$.*

Definition 3.2 (Hadamard transform [36]). *For a mapping f from $\mathrm{GF}(q^m)^n$ to $\mathbb{C}$, the* Hadamard transform *of f, denoted as $\hat{f}$, is defined to be*

$$\hat{f}(\mathbf{v}) \stackrel{def}{=} \sum_{\mathbf{u}\in\mathrm{GF}(q^m)^n} \chi(\mathbf{u}\cdot\mathbf{v}) f(\mathbf{u}), \tag{3.1}$$

where $\mathbf{u}\cdot\mathbf{v}$ denotes the inner product of $\mathbf{u}$ and $\mathbf{v}$.

In order to simplify notations, we shall occasionally denote the vector space $\mathrm{GF}(q^m)^n$ as F. We denote the number of vectors of rank u ($0 \le u \le \min\{m,n\}$) in $\mathrm{GF}(q^m)^n$ as $N_{\mathrm{R}}(q,m,n,u)$. We also define $\beta(m,0) \stackrel{\mathrm{def}}{=} 1$ and $\beta(m,u) \stackrel{\mathrm{def}}{=} \prod_{i=0}^{u-1} \begin{bmatrix} m-i \\ 1 \end{bmatrix}$ for $u \ge 1$. These terms are closely related to Gaussian polynomials: $\beta(m,u) = \begin{bmatrix} m \\ u \end{bmatrix} \beta(u,u)$ and $\beta(m+u, m+u) = \begin{bmatrix} m+u \\ u \end{bmatrix} \beta(m,m)\beta(u,u)$. Finally, $\sigma_i \stackrel{\mathrm{def}}{=} \frac{i(i-1)}{2}$ for $i \ge 0$.

3.3 MacWilliams identity for the rank metric

3.3.1 q-product, q-transform, and q-derivative

In order to express the MacWilliams identity in polynomial form as well as to derive other identities, we introduce several operations on homogeneous polynomials.

Let $a(x,y;m) = \sum_{i=0}^{r} a_i(m)y^i x^{r-i}$ and $b(x,y;m) = \sum_{j=0}^{s} b_j(m)y^j x^{s-j}$ be two homogeneous polynomials in x and y of degrees r and s respectively with coefficients $a_i(m)$ and $b_j(m)$ respectively. $a_i(m)$ and $b_j(m)$ for $i,j \geq 0$ in turn are real functions of m, and are assumed to be zero unless otherwise specified.

Definition 3.3 (q-product)**.** *The* q-product *of* $a(x,y;m)$ *and* $b(x,y;m)$ *is defined to be the homogeneous polynomial of degree* $(r+s)$ $c(x,y;m) \stackrel{def}{=} a(x,y;m) * b(x,y;m) = \sum_{u=0}^{r+s} c_u(m)y^u x^{r+s-u}$*, with* $c_u(m) = \sum_{i=0}^{u} q^{is} a_i(m) b_{u-i}(m-i)$*.*

We shall denote the q*-product by* $*$ *henceforth. For* $n \geq 0$ *the* n*-th* q*-power of* $a(x,y;m)$ *is defined recursively:* $a(x,y;m)^{[0]} = 1$ *and* $a(x,y;m)^{[n]} = a(x,y;m)^{[n-1]} * a(x,y;m)$ *for* $n \geq 1$*.*

We provide some examples to illustrate the concept. It is easy to verify that $x * y = yx$, $y * x = qyx$, $yx * x = qyx^2$, and $yx * (q^m - 1)y = (q^m - q)y^2 x$. Note that $x * y \neq y * x$. It is easy to verify that the q-product is neither commutative nor distributive in general. However, it is commutative and distributive in some special cases as described below.

Lemma 3.4. *Suppose* $a(x,y;m) = a$ *is a constant independent from* m*. Then* $a(x,y;m) * b(x,y;m) = b(x,y;m) * a(x,y;m) = ab(x,y;m)$*. Also, if* $\deg[c(x,y;m)] = \deg[a(x,y;m)]$*, then* $[a(x,y;m) + c(x,y;m)] * b(x,y;m) = a(x,y;m) * b(x,y;m) + c(x,y;m) * b(x,y;m)$*, and* $b(x,y;m) * [a(x,y;m) + c(x,y;m)] = b(x,y;m) * a(x,y;m) + b(x,y;m) * c(x,y;m)$*.*

The homogeneous polynomials $a_l(x,y;m) \stackrel{\text{def}}{=} [x + (q^m - 1)y]^{[l]}$ and $b_l(x,y;m) \stackrel{\text{def}}{=} (x-y)^{[l]}$ are very important to our derivations below. The following lemma provides the analytical expressions of $a_l(x,y;m)$ and $b_l(x,y;m)$.

Lemma 3.5. *For $l \geq 0$, we have $y^{[l]} = q^{\sigma_l} y^l$ and $x^{[l]} = x^l$. Furthermore,*

$$a_l(x, y; m) = \sum_{u=0}^{l} \begin{bmatrix} l \\ u \end{bmatrix} \alpha(m, u) y^u x^{l-u},$$

$$b_l(x, y; m) = \sum_{u=0}^{l} \begin{bmatrix} l \\ u \end{bmatrix} (-1)^u q^{\sigma_u} y^u x^{l-u}.$$

Note that $a_l(x, y; m)$ is the rank weight enumerator of $\mathrm{GF}(q^m)^l$. The proof of Lemma 3.5, which goes by induction on l, is easy and hence omitted.

Definition 3.6. *We define the* q-transform *of $a(x, y; m) = \sum_{i=0}^{r} a_i(m) y^i x^{r-i}$ as the homogeneous polynomial $\bar{a}(x, y; m) = \sum_{i=0}^{r} a_i(m) y^{[i]} * x^{[r-i]}$.*

Definition 3.7 (q-derivative [55])**.** *For $q \geq 2$, the q-derivative at $x \neq 0$ of a real-valued function $f(x)$ is defined as*

$$f^{(1)}(x) \stackrel{def}{=} \frac{f(qx) - f(x)}{(q-1)x}.$$

For any real number a, $[f(x) + ag(x)]^{(1)} = f^{(1)}(x) + ag^{(1)}(x)$ for $x \neq 0$. For $\nu \geq 0$, we shall denote the ν-th q-derivative (with respect to x) of $f(x, y)$ as $f^{(\nu)}(x, y)$. The 0-th q-derivative of $f(x, y)$ is defined to be $f(x, y)$ itself.

Lemma 3.8. *For $0 \leq \nu \leq l$, $(x^l)^{(\nu)} = \beta(l, \nu) x^{l-\nu}$. The ν-th q-derivative of $f(x, y) = \sum_{i=0}^{r} f_i y^i x^{r-i}$ is given by $f^{(\nu)}(x, y) = \sum_{i=0}^{r-\nu} f_i \beta(i, \nu) y^i x^{r-i-\nu}$. Also,*

$$\begin{aligned} a_l^{(\nu)}(x, y; m) &= \beta(l, \nu) a_{l-\nu}(x, y; m) \\ b_l^{(\nu)}(x, y; m) &= \beta(l, \nu) b_{l-\nu}(x, y; m). \end{aligned}$$

The proof of Lemma 3.8, which goes by induction on ν, is easy and hence omitted.

Lemma 3.9 (Leibniz rule for the q-derivative)**.** *For two homogeneous polynomials $f(x, y)$ and $g(x, y)$ with degrees r and s respectively, the ν-th ($\nu \geq 0$) q-derivative of*

their q-product is given by

$$[f(x,y) * g(x,y)]^{(\nu)} = \sum_{l=0}^{\nu} \begin{bmatrix} \nu \\ l \end{bmatrix} q^{(\nu-l)(r-l)} f^{(l)}(x,y) * g^{(\nu-l)}(x,y). \tag{3.2}$$

The proof of Lemma 3.9 is given in Appendix 7.2.1.

The q^{-1}-derivative is similar to the q-derivative.

Definition 3.10 (q^{-1}-derivative)**.** *For $q \geq 2$, the q^{-1}-derivative at $y \neq 0$ of a real-valued function $g(y)$ is defined as*

$$g^{\{1\}}(y) \stackrel{def}{=} \frac{g(q^{-1}y) - g(y)}{(q^{-1}-1)y}.$$

For any real number a, $[f(y)+ag(y)]^{\{1\}} = f^{\{1\}}(y)+ag^{\{1\}}(y)$ for $y \neq 0$. For $\nu \geq 0$, we shall denote the ν-th q^{-1}-derivative (with respect to y) of $g(x,y)$ as $g^{\{\nu\}}(x,y)$. The 0-th q^{-1}-derivative of $g(x,y)$ is defined to be $g(x,y)$ itself.

Lemma 3.11. *For $0 \leq \nu \leq l$, the ν-th q^{-1}-derivative of y^l is $(y^l)^{\{\nu\}} = q^{\nu(1-n)+\sigma_\nu}$ $\beta(l,\nu)y^{l-\nu}$. Also,*

$$\begin{aligned} a_l^{\{\nu\}}(x,y;m) &= \beta(l,\nu)q^{-\sigma_\nu}\alpha(m,\nu)a_{l-\nu}(x,y;m-\nu) \\ b_l^{\{\nu\}}(x,y;m) &= (-1)^\nu \beta(l,\nu) b_{l-\nu}(x,y;m). \end{aligned}$$

The proof of Lemma 3.11 is similar to that of Lemma 3.8 and is hence omitted.

Lemma 3.12 (Leibniz rule for the q^{-1}-derivative)**.** *For two homogeneous polynomials $f(x,y;m)$ and $g(x,y;m)$ with degrees r and s respectively, the ν-th ($\nu \geq 0$) q^{-1}-derivative of their q-product is given by*

$$[f(x,y;m) * g(x,y;m)]^{\{\nu\}} = \sum_{l=0}^{\nu} \begin{bmatrix} \nu \\ l \end{bmatrix} q^{l(s-\nu+l)} f^{\{l\}}(x,y;m) * g^{\{\nu-l\}}(x,y;m-l).$$

The proof of Lemma 3.12 is given in Appendix 7.2.2.

3.3.2 The dual of a vector

As an important step toward our main result, we derive the rank weight enumerator of $\langle \mathbf{v} \rangle^{\perp}$, where $\mathbf{v} \in \mathrm{GF}(q^m)^n$ is an arbitrary vector and $\langle \mathbf{v} \rangle \stackrel{\text{def}}{=} \{a\mathbf{v} : a \in \mathrm{GF}(q^m)\}$. Note that $\langle \mathbf{v} \rangle$ can be viewed as an $(n, 1)$ linear code over $\mathrm{GF}(q^m)$ with a generator matrix $\mathbf{v}$. It is remarkable that the rank weight enumerator of $\langle \mathbf{v} \rangle^{\perp}$ depends on only the rank of $\mathbf{v}$.

Berger [24] has determined that linear isometries for the rank distance are given by the scalar multiplication by a non-zero element of $\mathrm{GF}(q^m)$, and multiplication on the right by an nonsingular matrix $\mathbf{B} \in \mathrm{GF}(q)^{n \times n}$. We say that two codes $\mathcal{C}$ and $\mathcal{C}'$ are rank-equivalent if there exists a linear isometry f for the rank distance such that $f(\mathcal{C}) = \mathcal{C}'$.

Lemma 3.13. *Suppose* $\mathbf{v}$ *has rank* $r \geq 1$. *Then* $\mathcal{L} = \langle \mathbf{v} \rangle^{\perp}$ *is rank-equivalent to* $\mathcal{C} \times \mathrm{GF}(q^m)^{n-r}$, *where* $\mathcal{C}$ *is an* $(r, r-1, 2)$ *MRD code and* $\times$ *denotes cartesian product.*

Proof. We can express $\mathbf{v}$ as $\mathbf{v} = \bar{\mathbf{v}}\mathbf{B}$, where $\bar{\mathbf{v}} = (v_0, \ldots, v_{r-1}, 0 \ldots, 0)$ has rank r, and $\mathbf{B} \in \mathrm{GF}(q)^{n \times n}$ has full rank. Remark that $\bar{\mathbf{v}}$ is the parity-check of $\mathcal{C} \times \mathrm{GF}(q^m)^{n-r}$, where $\mathcal{C} = \langle (v_0, \ldots, v_{r-1}) \rangle^{\perp}$ is an $(r, r-1, 2)$ MRD code. It can be easily checked that $\mathbf{u} \in \mathcal{L}$ if and only if $\bar{\mathbf{u}} \stackrel{\text{def}}{=} \mathbf{u}\mathbf{B}^T \in \langle \bar{\mathbf{v}} \rangle^{\perp}$. Therefore, $\langle \bar{\mathbf{v}} \rangle^{\perp} = \mathcal{L}\mathbf{B}^T$, and hence $\mathcal{L}$ is rank-equivalent to $\langle \bar{\mathbf{v}} \rangle^{\perp} = \mathcal{C} \times \mathrm{GF}(q^m)^{n-r}$. □

We hence derive the rank weight enumerator of an $(r, r-1, 2)$ MRD code. Note that the rank weight distribution of linear Class-I MRD codes has been derived in [12, 13]. However, we shall not use the result in [12, 13], and instead derive the rank weight enumerator of an $(r, r-1, 2)$ MRD code directly.

Proposition 3.14. *Suppose* $\mathbf{v}_r \in \mathrm{GF}(q^m)^r$ *has rank* r *(*$0 \le r \le m$*). The rank weight enumerator of* $\mathcal{L}_r = \langle \mathbf{v} \rangle^\perp$ *depends on only* r *and is given by*

$$W^R_{\mathcal{L}_r}(x,y) = q^{-m}\left\{ [x + (q^m-1)y]^{[r]} + (q^m-1)(x-y)^{[r]} \right\}.$$

Proof. We first prove that the number of vectors with rank r in $\mathcal{L}_r$, denoted as $A_{r,r}$, depends only on r and is given by

$$A_{r,r} = q^{-m}[\alpha(m,r) + (q^m-1)(-1)^r q^{\sigma_r}] \tag{3.3}$$

by induction on r ($r \ge 1$). Eq. (3.3) clearly holds for $r = 1$. Suppose (3.3) holds for $r = \bar{r} - 1$.

We consider all the vectors $\mathbf{u} = (u_0, \ldots, u_{\bar{r}-1}) \in \mathcal{L}_{\bar{r}}$ such that the first $\bar{r}-1$ coordinates of $\mathbf{u}$ are linearly independent. Remark that $u_{\bar{r}-1} = -v_{\bar{r}-1}^{-1} \sum_{i=0}^{\bar{r}-2} u_i v_i$ is completely determined by $u_0, \ldots, u_{\bar{r}-2}$. Thus there are $N_{\mathrm{R}}(q,m,\bar{r}-1,\bar{r}-1) = \alpha(m,\bar{r}-1)$ such vectors $\mathbf{u}$. Among these vectors, we will enumerate the vectors $\mathbf{t}$ whose last coordinate is a linear combination of the first $\bar{r}-1$ coordinates, i.e., $\mathbf{t} = (t_0, \ldots, t_{\bar{r}-2}, \sum_{i=0}^{\bar{r}-2} a_i t_i) \in \mathcal{L}_{\bar{r}}$ where $a_i \in \mathrm{GF}(q)$ for $0 \le i \le \bar{r}-2$.

Remark that $\mathbf{t} \in \mathcal{L}_{\bar{r}}$ if and only if $(t_0, \ldots, t_{\bar{r}-2}) \cdot (v_0 + a_0 v_{\bar{r}-1}, \ldots, v_{\bar{r}-2} + a_{\bar{r}-2} v_{\bar{r}-1}) = 0$. It is easy to check that $\mathbf{v}(\mathbf{a}) = (v_0 + a_0 v_{\bar{r}-1}, \ldots, v_{\bar{r}-2} + a_{\bar{r}-2} v_{\bar{r}-1})$ has rank $\bar{r}-1$. Therefore, if $a_0, \ldots, a_{\bar{r}-2}$ are fixed, then there are $A_{\bar{r}-1,\bar{r}-1}$ such vectors $\mathbf{t}$. Also, suppose $\sum_{i=0}^{\bar{r}-2} t_i v_i + v_{\bar{r}-1} \sum_{i=0}^{\bar{r}-2} b_i t_i = 0$. Hence $\sum_{i=0}^{\bar{r}-2} (a_i - b_i) t_i = 0$, which implies $\mathbf{a} = \mathbf{b}$ since t_i's are linearly independent. That is, $\langle \mathbf{v}(\mathbf{a}) \rangle^\perp \cap \langle \mathbf{v}(\mathbf{b}) \rangle^\perp = \{\mathbf{0}\}$ if $\mathbf{a} \ne \mathbf{b}$. We conclude that there are $q^{\bar{r}-1} A_{\bar{r}-1,\bar{r}-1}$ vectors $\mathbf{t}$. Therefore, $A_{\bar{r},\bar{r}} = \alpha(m,\bar{r}-1) - q^{\bar{r}-1} A_{\bar{r}-1,\bar{r}-1} = q^{-m}[\alpha(m,\bar{r}) + (q^m-1)(-1)^{\bar{r}} q^{\sigma_{\bar{r}}}]$.

Denote the number of vectors with rank p in $\mathcal{L}_r$ as $A_{r,p}$. We have $A_{r,p} = \begin{bmatrix} r \\ p \end{bmatrix} A_{p,p}$ [13], and hence $A_{r,p} = \begin{bmatrix} r \\ p \end{bmatrix} q^{-m}[\alpha(m,p) + (q^m-1)(-1)^p q^{\sigma_p}]$. Thus, $W^{\mathrm{R}}_{\mathcal{L}_r}(x,y) = \sum_{p=0}^{r} A_{r,p} x^{r-p} y^p = q^{-m}\left\{ [x + (q^m-1)y]^{[r]} + (q^m-1)(x-y)^{[r]} \right\}$. □

We comment that Proposition 3.14 in fact provides the rank weight distribution of any $(r, r-1, 2)$ MRD code.

Lemma 3.15. *Let $\mathcal{C}_0 \subseteq \mathrm{GF}(q^m)^r$ be a linear code with rank weight enumerator $W^R_{\mathcal{C}_0}(x,y)$, and for $s \geq 0$, let $W^R_{\mathcal{C}_s}(x,y)$ be the rank weight enumerator of $\mathcal{C}_s \stackrel{def}{=} \mathcal{C}_0 \times \mathrm{GF}(q^m)^s$. Then $W^R_{\mathcal{C}_s}(x,y)$ is given by $W^R_{\mathcal{C}_s}(x,y) = W^R_{\mathcal{C}_0}(x,y) * [x + (q^m-1)y]^{[s]}$.*

Proof. For $s \geq 0$, denote $W^{\mathrm{R}}_{\mathcal{C}_s}(x,y) = \sum_{u=0}^{r+s} B_{s,u} y^u x^{r+s-u}$. We will prove that

$$B_{s,u} = \sum_{i=0}^{u} q^{is} B_{0,i} \begin{bmatrix} s \\ u-i \end{bmatrix} \alpha(m-i, u-i) \tag{3.4}$$

by induction on s. Eq. (3.4) clearly holds for $s = 0$. Now assume (3.4) holds for $s = \bar{s} - 1$. For any $\mathbf{x}_{\bar{s}} = (x_0, \ldots, x_{r+\bar{s}-1}) \in \mathcal{C}_{\bar{s}}$, we define $\mathbf{x}_{\bar{s}-1} = (x_0, \ldots, x_{r+\bar{s}-2}) \in \mathcal{C}_{\bar{s}-1}$. Then $\mathrm{rk}(\mathbf{x}_{\bar{s}}) = u$ if and only if either $\mathrm{rk}(\mathbf{x}_{\bar{s}-1}) = u$ and $x_{r+\bar{s}-1} \in S(\mathbf{x}_{\bar{s}-1})$ or $\mathrm{rk}(\mathbf{x}_{\bar{s}-1}) = u-1$ and $x_{r+\bar{s}-1} \notin S(\mathbf{x}_{\bar{s}-1})$. This implies $B_{\bar{s},u} = q^u B_{\bar{s}-1,u} + (q^m - q^{u-1}) B_{\bar{s}-1,u-1} = \sum_{i=0}^{u} q^{i\bar{s}} B_{0,i} \begin{bmatrix} \bar{s} \\ u-i \end{bmatrix} \alpha(m-i, u-i)$. □

Combining Lemma 3.13, Proposition 3.14, and Lemma 3.15, the rank weight enumerator of $\langle \mathbf{v} \rangle^{\perp}$ can be determined at last.

Proposition 3.16. *For $\mathbf{v} \in \mathrm{GF}(q^m)^n$ with rank $r \geq 0$, the rank weight enumerator of $\mathcal{L} = \langle \mathbf{v} \rangle^{\perp}$ depends on only r, and is given by*

$$W^R_{\mathcal{L}}(x,y) = q^{-m} \left\{ [x + (q^m-1)y]^{[n]} + (q^m-1)(x-y)^{[r]} * [x + (q^m-1)y]^{[n-r]} \right\}.$$

3.3.3 MacWilliams identity for the rank metric

Using the results in Section 3.3.2, we now derive the MacWilliams identity for rank metric codes. Let $\mathcal{C}$ be an (n,k) linear code over $\mathrm{GF}(q^m)$, and let $W^{\mathrm{R}}_{\mathcal{C}}(x,y) = \sum_{i=0}^{n} A_i y^i x^{n-i}$ be its rank weight enumerator and $W^{\mathrm{R}}_{\mathcal{C}^{\perp}}(x,y) = \sum_{j=0}^{n} B_j y^j x^{n-j}$ be the rank weight enumerator of its dual code $\mathcal{C}^{\perp}$.

Theorem 3.17. *For any (n,k) linear code $\mathcal{C}$ and its dual code $\mathcal{C}^\perp$ over $\mathrm{GF}(q^m)$,*

$$W^R_{\mathcal{C}^\perp}(x,y) = \frac{1}{|\mathcal{C}|}\bar{W}^R_{\mathcal{C}}\left(x+(q^m-1)y, x-y\right), \tag{3.5}$$

where $\bar{W}^R_{\mathcal{C}}$ is the q-transform of $W^R_{\mathcal{C}}$. Equivalently,

$$\sum_{j=0}^{n} B_j y^j x^{n-j} = q^{-mk}\sum_{i=0}^{n} A_i (x-y)^{[i]} * [x+(q^m-1)y]^{[n-i]}. \tag{3.6}$$

Proof. We have $\mathrm{rk}(\lambda\mathbf{u}) = \mathrm{rk}(\mathbf{u})$ for all $\lambda \in \mathrm{GF}(q^m)^*$ and all $\mathbf{u} \in \mathrm{GF}(q^m)^n$. We want to determine $\hat{f}_{\mathrm{R}}(\mathbf{v})$ for all $\mathbf{v} \in \mathrm{GF}(q^m)^n$. By Definition 3.2, we can split the summation in (3.1) into two parts:

$$\hat{f}_{\mathrm{R}}(\mathbf{v}) = \sum_{\mathbf{u}\in\mathcal{L}} \chi(\mathbf{u}\cdot\mathbf{v}) f_{\mathrm{R}}(\mathbf{u}) + \sum_{\mathbf{u}\in F\backslash\mathcal{L}} \chi(\mathbf{u}\cdot\mathbf{v}) f_{\mathrm{R}}(\mathbf{u}),$$

where $\mathcal{L} = \langle\mathbf{v}\rangle^\perp$. If $\mathbf{u} \in \mathcal{L}$, then $\chi(\mathbf{u}\cdot\mathbf{v}) = 1$ by Definition 3.1, and the first summation is equal to $W^{\mathrm{R}}_{\mathcal{L}}(x,y)$. For the second summation, we divide vectors into groups of the form $\{\lambda\mathbf{u}_1\}$, where $\lambda \in \mathrm{GF}(q^m)^*$ and $\mathbf{u}_1\cdot\mathbf{v} = 1$. We remark that for $\mathbf{u} \in F\backslash\mathcal{L}$ (see [36, Chapter 5, Lemma 9])

$$\sum_{\lambda\in\mathrm{GF}(q^m)^*} \chi(\lambda\mathbf{u}_1\cdot\mathbf{v}) f_{\mathrm{R}}(\lambda\mathbf{u}_1) = f_{\mathrm{R}}(\mathbf{u}_1) \sum_{\lambda\in\mathrm{GF}(q^m)^*} \chi(\lambda) = -f_{\mathrm{R}}(\mathbf{u}_1).$$

Hence the second summation is equal to $-\frac{1}{q^m-1}W^{\mathrm{R}}_{F\backslash\mathcal{L}}(x,y)$. This leads to $\hat{f}_{\mathrm{R}}(\mathbf{v}) = \frac{1}{q^m-1}[q^m W^{\mathrm{R}}_{\mathcal{L}}(x,y) - W^{\mathrm{R}}_F(x,y)]$. Using $W^{\mathrm{R}}_F(x,y) = [x+(q^m-1)y]^{[n]}$ and Proposition 3.16, we obtain $\hat{f}_{\mathrm{R}}(\mathbf{v}) = (x-y)^{[r]} * [x+(q^m-1)y]^{[n-r]}$, where $r = \mathrm{rk}(\mathbf{v})$.

By [36, Chapter 5, Lemma 11], any mapping f from F to $\mathbb{C}$ satisfies $\sum_{\mathbf{v}\in\mathcal{C}^\perp} f(\mathbf{v}) = \frac{1}{|\mathcal{C}|}\sum_{\mathbf{v}\in\mathcal{C}} \hat{f}(\mathbf{v})$. Applying this result to $f_{\mathrm{R}}(\mathbf{v})$ and using Definition 3.6, we obtain (3.5) and (3.6). □

Also, B_j's can be explicitly expressed in terms of A_i's.

Corollary 3.18. *We have*

$$B_j = \frac{1}{|\mathcal{C}|} \sum_{i=0}^{n} A_i P_j(i; m, n), \tag{3.7}$$

where

$$P_j(i; m, n) \stackrel{def}{=} \sum_{l=0}^{j} \begin{bmatrix} i \\ l \end{bmatrix} \begin{bmatrix} n-i \\ j-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(m-l, j-l). \tag{3.8}$$

Proof. We have $(x-y)^{[i]} * (x+(q^m-1)y)^{[n-i]} = \sum_{j=0}^{n} P_j(i; m, n) y^j x^{n-j}$. The result follows Theorem 3.17. □

In order to illustrate the result in Corollary 3.18, we introduce a $(5, 2, 4)$ MRD code $\mathcal{G}$ over GF(2^5). It can be shown that its rank weight distribution is given by $A_i = 1, 0, 0, 0, 961, 62$, for $i = 0, 1, \ldots, 5$, and according to Corollary 3.18, the rank weight distribution of its dual code is $B_j = 1, 0, 0, 4805, 17298, 10664$ for $j = 0, 1, \ldots, 5$.

Note that although the analytical expression in (3.7) is similar to that in [12, (3.14)], $P_j(i; m, n)$ in (3.8) are different from $P_j(i)$ in [12, (A10)] and their alternative forms in [46]. We can show that

Proposition 3.19. *$P_j(x; m, n)$ in (3.8) are the q-Krawtchouk polynomials.*

The proof is given in Appendix 7.2.3. Proposition 3.19 shows that $P_j(x; m, n)$ in (3.8) are an alternative form for $P_j(i)$ in [12, (A10)], and hence our results in Corollary 3.18 are equivalent to those in [12, Theorem 3.3]. Also, it was pointed out in [46] that $\frac{P_j(x;m,n)}{P_j(0;m,n)}$ is actually a basic hypergeometric function.

3.4 Moments of the rank distribution

The moments of the Hamming weight distribution of linear codes have been widely studied [36, 52]. However, the moments of the rank distribution of linear codes have

received little attention. While the identities in the Hamming metric are based on classical combinatorial functions, such as the binomial coefficient, the identities in the rank metric are based on q-analogues, i.e. nontrivial extensions, of these functions. Thus, we not only determine the counterparts in the rank metric of the Hamming metric identities, but we also introduce a wider variety of moments and derive further equalities relating either a moment of a code and that of its dual or different moments of the same code.

3.4.1 Binomial moments of the rank distribution

In this section, we investigate the relationship between moments of the rank distribution of a linear code and those of its dual code. Our results parallel those in [36, p. 131].

Proposition 3.20. *For* $0 \leq \nu \leq n$,

$$\sum_{i=0}^{n-\nu} \begin{bmatrix} n-i \\ \nu \end{bmatrix} A_i = q^{m(k-\nu)} \sum_{j=0}^{\nu} \begin{bmatrix} n-j \\ n-\nu \end{bmatrix} B_j. \tag{3.9}$$

Proof. First, applying Theorem 3.17 to $\mathcal{C}^{\perp}$, we obtain

$$\sum_{i=0}^{n} A_i y^i x^{n-i} = q^{m(k-n)} \sum_{j=0}^{n} B_j b_j(x,y;m) * a_{n-j}(x,y;m). \tag{3.10}$$

Next, we apply the q-derivative with respect to x to (3.10) ν times. By Lemma 3.8 the left hand side (LHS) becomes $\sum_{i=0}^{n-\nu} \beta(n-i,\nu) A_i y^i x^{n-i-\nu}$, while the RHS reduces to $q^{m(k-n)} \sum_{j=0}^{n} B_j \psi_j(x,y)$ by Lemma 3.9, where

$$\begin{aligned} \psi_j(x,y) &\stackrel{\text{def}}{=} [b_j(x,y;m) * a_{n-j}(x,y;m)]^{(\nu)} \\ &= \sum_{l=0}^{\nu} \begin{bmatrix} \nu \\ l \end{bmatrix} q^{(\nu-l)(j-l)} b_j^{(l)}(x,y) * a_{n-j}^{(\nu-l)}(x,y;m). \end{aligned}$$

By Lemma 3.8, $b_j^{(l)}(x,y;m) = \beta(j,l)(x-y)^{[j-l]}$ and $a_{n-j}^{(\nu-l)}(x,y;m) = \beta(n-j,\nu-l)a_{n-j-\nu+l}(x,y;m)$. It can be verified that for any homogeneous polynomial $b(x,y;m)$ and for any $s \geq 0$, $(b*a_s)(1,1;m) = q^{ms}b(1,1;m)$. Also, for $x=y=1$, $b_j^{(l)}(1,1;m) = \beta(j,j)\delta_{j,l}$. We hence have $\psi_j(1,1) = 0$ for $j > \nu$, and $\psi_j(1,1) = \begin{bmatrix}\nu\\ j\end{bmatrix}\beta(j,j)\beta(n-j,\nu-j)q^{m(n-\nu)}$ for $j \leq \nu$. Since $\beta(n-j,\nu-j) = \begin{bmatrix}n-j\\ \nu-j\end{bmatrix}\beta(\nu-j,\nu-j)$ and $\beta(\nu,\nu) = \begin{bmatrix}\nu\\ j\end{bmatrix}\beta(j,j)\beta(\nu-j,\nu-j)$, $\psi_j(1,1) = \begin{bmatrix}n-j\\ \nu-j\end{bmatrix}\beta(\nu,\nu)q^{m(n-\nu)}$. Applying $x=y=1$ to the LHS and rearranging both sides using $\beta(n-i,\nu) = \begin{bmatrix}n-i\\ \nu\end{bmatrix}\beta(\nu,\nu)$, we obtain (3.9). □

For example, for the code $\mathcal{G}$ introduced above, both sides of (3.9) are given by $1024, 992, 155, 155, 31, 1$ for $\nu = 0, 1, \ldots, 5$.

Proposition 3.20 can be simplified if ν is less than the minimum distance of the dual code.

Corollary 3.21. *Let d'_{R} be the minimum rank distance of $\mathcal{C}^{\perp}$. If $0 \leq \nu < d'_{\mathrm{R}}$, then*

$$\sum_{i=0}^{n-\nu} \begin{bmatrix} n-i \\ \nu \end{bmatrix} A_i = q^{m(k-\nu)} \begin{bmatrix} n \\ \nu \end{bmatrix}. \tag{3.11}$$

Proof. We have $B_0 = 1$ and $B_1 = \ldots = B_\nu = 0$. □

For the code $\mathcal{G}$, we have $d'_{\mathrm{R}} = 3$ and both sides of (3.11) are given by $1024, 992, 155$ for $\nu = 0, 1, 2$.

Using the q^{-1}-derivative, we obtain another identity.

Proposition 3.22. *For $0 \leq \nu \leq n$,*

$$\sum_{i=\nu}^{n} \begin{bmatrix} i \\ \nu \end{bmatrix} q^{\nu(n-i)} A_i = q^{m(k-\nu)} \sum_{j=0}^{\nu} \begin{bmatrix} n-j \\ n-\nu \end{bmatrix} (-1)^j q^{\sigma_j} \alpha(m-j,\nu-j) q^{j(\nu-j)} B_j. \tag{3.12}$$

The proof of Proposition 3.22 is similar to that of Proposition 3.20, and is given in Appendix 7.2.4.

For the code $\mathcal{G}$, both sides of (3.12) are given by $1024, 30752, 144150, 124930,$ 17298, 62 for $\nu = 0, 1, \ldots, 5$.

Following [36], we refer to the LHS of (3.9) and (3.12) as binomial moments of the rank distribution of $\mathcal{C}$. Similarly, when either ν is less than the minimum distance d'_{R} of the dual code, or ν is greater than the diameter (maximum distance between any two codewords) δ'_{R} of the dual code, Proposition 3.22 can be simplified.

Corollary 3.23. *If* $0 \leq \nu < d'_{\mathrm{R}}$, *then*

$$\sum_{i=\nu}^{n} \begin{bmatrix} i \\ \nu \end{bmatrix} q^{\nu(n-i)} A_i = q^{m(k-\nu)} \begin{bmatrix} n \\ \nu \end{bmatrix} \alpha(m, \nu). \tag{3.13}$$

For $\delta'_{R} < \nu \leq n$,

$$\sum_{i=0}^{\nu} \begin{bmatrix} n-i \\ n-\nu \end{bmatrix} (-1)^i q^{\sigma_i} \alpha(m-i, \nu-i) q^{i(\nu-i)} A_i = 0. \tag{3.14}$$

Proof. Apply Proposition 3.22 to $\mathcal{C}$, and use $B_1 = \ldots = B_\nu = 0$ to prove (3.13). Apply Proposition 3.22 to $\mathcal{C}^\perp$, and use $B_\nu = \ldots = B_n = 0$ to prove (3.14). □

For the code $\mathcal{G}$, both sides of (3.13) are given by $1024, 30752, 144150$ for $\nu = 0, 1, 2$. We remark that for $\mathcal{G}$, $\delta'_{\mathrm{R}} = n$, and (3.14) cannot be applied.

3.4.2 Pless identities for the rank distribution

In this section, we consider the analogues of the Pless identities [36, 52], in terms of Stirling numbers. The q-Stirling numbers of the second kind $S_q(\nu, l)$ are defined [56] to be

$$S_q(\nu, l) \stackrel{\text{def}}{=} \frac{q^{-\sigma_l}}{\beta(l, l)} \sum_{i=0}^{l} (-1)^i q^{\sigma_i} \begin{bmatrix} l \\ i \end{bmatrix} \begin{bmatrix} l-i \\ 1 \end{bmatrix}^{\nu},$$

and they satisfy

$$\begin{bmatrix} m \\ 1 \end{bmatrix}^{\nu} = \sum_{l=0}^{\nu} q^{\sigma_l} S_q(\nu, l)\beta(m, l). \tag{3.15}$$

The following proposition can be viewed as a q-analogue of the Pless identity with respect to x [52, P_2].

Proposition 3.24. *For* $0 \leq \nu \leq n$,

$$q^{-mk} \sum_{i=0}^{n} \begin{bmatrix} n-i \\ 1 \end{bmatrix}^{\nu} A_i = \sum_{j=0}^{\nu} B_j \sum_{l=0}^{\nu} \begin{bmatrix} n-j \\ n-l \end{bmatrix} \beta(l, l) S_q(\nu, l) q^{-ml+\sigma_l}. \tag{3.16}$$

Proof. We have

$$\begin{aligned} \sum_{i=0}^{n} \begin{bmatrix} n-i \\ 1 \end{bmatrix}^{\nu} A_i &= \sum_{i=0}^{n} A_i \sum_{l=0}^{\nu} q^{\sigma_l} S_q(\nu, l) \begin{bmatrix} n-i \\ l \end{bmatrix} \beta(l, l) && (3.17) \\ &= \sum_{l=0}^{\nu} q^{\sigma_l} \beta(l, l) S_q(\nu, l) \sum_{i=0}^{n} \begin{bmatrix} n-i \\ l \end{bmatrix} A_i \\ &= \sum_{l=0}^{\nu} q^{\sigma_l} \beta(l, l) S_q(\nu, l) q^{m(k-l)} \sum_{j=0}^{l} \begin{bmatrix} n-j \\ n-l \end{bmatrix} B_j && (3.18) \\ &= q^{mk} \sum_{j=0}^{\nu} B_j \sum_{l=0}^{\nu} \begin{bmatrix} n-j \\ n-l \end{bmatrix} q^{\sigma_l} \beta(l, l) S_q(\nu, l) q^{-ml}, \end{aligned}$$

where (3.17) follows (3.15) and (3.18) is due to Proposition 3.20. □

For the code $\mathcal{G}$, both sides of (3.16), once multiplied by $q^{mk} = 2^{10}$, are given by $1024, 992, 1922, 30752, 924482, 28630112$ for $\nu = 0, 1, \ldots, 5$.

Proposition 3.24 can be simplified when ν is less than the minimum distance of the dual code.

Corollary 3.25. *For* $0 \leq \nu < d'_{\mathrm{R}}$,

$$\begin{aligned} q^{-mk} \sum_{i=0}^{n} \begin{bmatrix} n-i \\ 1 \end{bmatrix}^{\nu} A_i &= \sum_{l=0}^{\nu} \beta(n, l) S_q(\nu, l) q^{-ml+\sigma_l} && (3.19) \\ &= q^{-mn} \sum_{i=0}^{n} \begin{bmatrix} n-i \\ 1 \end{bmatrix}^{\nu} \begin{bmatrix} n \\ i \end{bmatrix} \alpha(m, i). && (3.20) \end{aligned}$$

Proof. Since $B_0 = 1$ and $B_1 = \cdots = B_\nu = 0$, (3.16) directly leads to (3.19). Since the right hand side of (3.19) is transparent to the code, without loss of generality we choose $\mathcal{C} = \mathrm{GF}(q^m)^n$ and (3.20) follows naturally. □

Unfortunately, a q-analogue of the Pless identity with respect to y [52, P$_1$] cannot be obtained due to the presence of the $q^{\nu(n-i)}$ term in the LHS of (3.12). Instead, we derive its q^{-1}-analogue. We denote $p \stackrel{\text{def}}{=} q^{-1}$ and define the functions $\alpha_p(m,u)$, $\begin{bmatrix} n \\ u \end{bmatrix}_p$, $\beta_p(m,u)$ similarly to the functions introduced in Section 3.2, only replacing q by p. It is easy to relate these q^{-1}-functions to their counterparts: $\alpha(m,u) = p^{-mu-\sigma_u}(-1)^u \alpha_p(m,u)$, $\begin{bmatrix} n \\ u \end{bmatrix} = p^{-u(n-u)} \begin{bmatrix} n \\ u \end{bmatrix}_p$, and $\beta(m,u) = p^{-u(m-u)-\sigma_u}\beta_p(m,u)$.

Proposition 3.26. *For* $0 \le \nu \le n$,

$$p^{mk} \sum_{i=0}^{n} \begin{bmatrix} i \\ 1 \end{bmatrix}_p^{\nu} A_i = \sum_{j=0}^{\nu} B_j p^{j(m+n-j)} \sum_{l=j}^{\nu} \beta_p(l,l) S_p(\nu,l) (-1)^l \begin{bmatrix} n-j \\ n-l \end{bmatrix}_p \alpha_p(m-j, l-j).$$

For the code $\mathcal{G}$, both sides of the identity in Proposition 3.26 are given by $1, 1.8770, 3.5266, 6.6266, 12.4524, 23.4016$ for $\nu = 0, 1, \ldots, 5$.

The proof of Proposition 3.26 is given in Appendix 7.2.5.

Corollary 3.27. *For* $0 \le \nu < d'_{\mathrm{R}}$,

$$p^{mk} \sum_{i=0}^{n} \begin{bmatrix} i \\ 1 \end{bmatrix}_p^{\nu} A_i = \sum_{l=0}^{\nu} \beta_p(n,l) S_p(\nu,l) \alpha_p(m,l) (-1)^l.$$

Proof. Note that $B_0 = 1$ and $B_1 = \ldots = B_\nu = 0$. □

3.4.3 Further results on the rank distribution

For nonnegative integers λ, μ, and ν, and a linear code $\mathcal{C}$ with rank weight distribution $\{A_i\}$ we define

$$T_{\lambda,\mu,\nu}(\mathcal{C}) \stackrel{\text{def}}{=} q^{-mk} \sum_{i=0}^{n} \begin{bmatrix} i \\ \lambda \end{bmatrix}^{\mu} q^{\nu(n-i)} A_i,$$

whose properties are studied below. We refer to

$$T_{0,0,\nu}(\mathcal{C}) \stackrel{\text{def}}{=} q^{-mk} \sum_{i=0}^{n} q^{\nu(n-i)} A_i \tag{3.21}$$

as the *ν-th q-moment* of the rank distribution of $\mathcal{C}$. We remark that for any code $\mathcal{C}$, the 0-th order q-moment of its rank distribution is equal to 1. We first relate $T_{\lambda,1,\nu}(\mathcal{C})$ and $T_{1,\mu,\nu}(\mathcal{C})$ to $T_{0,0,\nu}(\mathcal{C})$.

Lemma 3.28. *For nonnegative integers λ, μ, and ν we have*

$$T_{\lambda,1,\nu}(\mathcal{C}) = \frac{1}{\alpha(\lambda,\lambda)} \sum_{l=0}^{\lambda} \begin{bmatrix} \lambda \\ l \end{bmatrix} (-1)^l q^{\sigma_l} q^{n(\lambda-l)} T_{0,0,\nu-\lambda+l}(\mathcal{C}) \tag{3.22}$$

$$T_{1,\mu,\nu}(\mathcal{C}) = (1-q)^{-\mu} \sum_{a=0}^{\mu} \binom{\mu}{a} (-1)^a q^{an} T_{0,0,\nu-a}(\mathcal{C}). \tag{3.23}$$

The proof of Lemma 3.28 is given in Appendix 7.2.6. We now consider the case where ν is less than the minimum distance of the dual code.

Proposition 3.29. *For $0 \leq \nu < d'_{\mathrm{R}}$,*

$$T_{0,0,\nu}(\mathcal{C}) = \sum_{j=0}^{\nu} \begin{bmatrix} \nu \\ j \end{bmatrix} \alpha(n,j) q^{-mj} \tag{3.24}$$

$$= q^{-mn} \sum_{i=0}^{n} \begin{bmatrix} n \\ i \end{bmatrix} \alpha(m,i) q^{\nu(n-i)} \tag{3.25}$$

$$= q^{-m\nu} \sum_{l=0}^{\nu} \begin{bmatrix} \nu \\ l \end{bmatrix} \alpha(m,l) q^{n(\nu-l)}. \tag{3.26}$$

The proof of Proposition 3.29 is given in Appendix 7.2.7.

For the code $\mathcal{G}$, $T_{0,0,\nu}(\mathcal{G})$ and the RHS of (3.24)-(3.26), once multiplied by $q^{mk} = 2^{10}$, are given by $1024, 2016, 4930$ for $\nu = 0, 1, 2$.

Proposition 3.29 hence shows that the ν-th q-moment of the rank distribution of a code is transparent to the code when $\nu < d'_{\mathrm{R}}$. As a corollary, we show that $T_{\lambda,1,\nu}(\mathcal{C})$ and $T_{1,\mu,\nu}(\mathcal{C})$ are also transparent to the code when $0 \leq \lambda, \mu \leq \nu < d'_{\mathrm{R}}$.

Corollary 3.30. *For* $0 \leq \lambda, \mu \leq \nu < d'_{\mathrm{R}}$,

$$T_{\lambda,1,\nu}(\mathcal{C}) = q^{-mn} \begin{bmatrix} n \\ \lambda \end{bmatrix} \sum_{i=\lambda}^{n} \begin{bmatrix} n-\lambda \\ i-\lambda \end{bmatrix} q^{\nu(n-i)} \alpha(m,i) \tag{3.27}$$

$$T_{1,\mu,\nu}(\mathcal{C}) = q^{-mn} \sum_{i=0}^{n} \begin{bmatrix} i \\ 1 \end{bmatrix}^{\mu} q^{\nu(n-i)} \begin{bmatrix} n \\ i \end{bmatrix} \alpha(m,i). \tag{3.28}$$

Proof. By Lemma 3.28 and Proposition 3.29, $T_{\lambda,1,\nu}(\mathcal{C})$ and $T_{1,\mu,\nu}(\mathcal{C})$ are transparent to the code. Thus, without loss of generality we assume $\mathcal{C} = \mathrm{GF}(q^m)^n$ and (3.27) and (3.28) follow. □

For the code $\mathcal{G}$, the values of $T_{\lambda,\mu,\nu}(\mathcal{G})$ and their respective counterparts in (3.27) and (3.28), once multiplied by 2^{10}, are given by $T_{0,1,1}(\mathcal{G}) = T_{1,0,1}(\mathcal{G}) = 2016$, $T_{1,1,1}(\mathcal{G}) = 30752$, $T_{0,1,2}(\mathcal{G}) = T_{1,0,2}(\mathcal{G}) = 4930$, $T_{1,1,2}(\mathcal{G}) = 59582$, $T_{2,1,2}(\mathcal{G}) = 144150$, $T_{1,2,2}(\mathcal{G}) = 924482$.

3.4.4 Rank weight distribution of MRD codes

The rank weight distribution of linear Class-I MRD codes was given in [12, 13]. Based on our results in Section 3.4.1, we provide an alternative derivation of the rank distribution of linear Class-I MRD codes, which can also be used to determine the rank weight distribution of Class-II MRD codes.

Proposition 3.31 (Rank distribution of linear Class-I MRD codes)**.** *Let* $\mathcal{C}$ *be an* (n, k, d_{R}) *linear Class-I MRD code over* $\mathrm{GF}(q^m)$ $(n \leq m)$*, and let* $W^R_{\mathcal{C}}(x, y) = \sum_{i=0}^{n} A_i y^i x^{n-i}$ *be its rank weight enumerator. We then have* $A_0 = 1$ *and for* $0 \leq i \leq n - d_{\mathrm{R}}$,

$$A_{d_{\mathrm{R}}+i} = \begin{bmatrix} n \\ d_{\mathrm{R}}+i \end{bmatrix} \sum_{j=0}^{i} (-1)^{i-j} q^{\sigma_{i-j}} \begin{bmatrix} d_{\mathrm{R}}+i \\ d_{\mathrm{R}}+j \end{bmatrix} \left(q^{m(j+1)} - 1\right).$$

Proof. It can be shown that for two sequences of real numbers $\{a_j\}_{j=0}^{l}$ and $\{b_i\}_{i=0}^{l}$ such that $a_j = \sum_{i=0}^{j} \begin{bmatrix} l-i \\ l-j \end{bmatrix} b_i$ for $0 \leq j \leq l$, we have $b_i = \sum_{j=0}^{i} (-1)^{i-j} q^{\sigma_{i-j}} \begin{bmatrix} l-j \\ l-i \end{bmatrix} a_j$ for $0 \leq i \leq l$.

By Corollary 3.21, we have $\sum_{i=0}^{j} \begin{bmatrix} n-d_{\mathrm{R}}-i \\ n-d_{\mathrm{R}}-j \end{bmatrix} A_{d_{\mathrm{R}}+i} = \begin{bmatrix} n \\ n-d_{\mathrm{R}}-j \end{bmatrix} \left(q^{m(j+1)} - 1\right)$ for $0 \leq j \leq n - d_{\mathrm{R}}$. Applying the result above to $l = n - d_{\mathrm{R}}$, $a_j = \begin{bmatrix} n \\ n-d_{\mathrm{R}}-j \end{bmatrix} \left(q^{m(j+1)} - 1\right)$, and $b_i = A_{d_{\mathrm{R}}+i}$, we obtain $A_{d_{\mathrm{R}}+i} = \sum_{j=0}^{i} (-1)^{i-j} q^{\sigma_{i-j}} \begin{bmatrix} n \\ d_{\mathrm{R}}+i \end{bmatrix} \begin{bmatrix} d_{\mathrm{R}}+i \\ d_{\mathrm{R}}+j \end{bmatrix} \left(q^{m(j+1)} - 1\right)$. □

We remark that the above rank distribution is consistent with that derived in [12, 13]. Since Class-II MRD codes can be constructed by transposing linear Class-I MRD codes and the transposition operation preserves the rank weight, the weight distributions Class-II MRD codes can be obtained accordingly.

Chapter 4

Constant-Rank Codes

4.1 Introduction

Error control for noncoherent random linear network coding was first considered in [9][1]. Motivated by the property that random linear network coding is vector-space preserving, an operator channel that captures the essence of the noncoherent transmission model was defined in [9]. Similar to codes defined in complex Grassmannians for noncoherent multiple-antenna channels, codes defined in Grassmannians over a finite field [58,59] and used with the subspace distance (cf. [9, (3)]) play a significant role in error control for noncoherent random linear network coding; Under the subspace distance, the weight of a subspace is simply its dimension; thus, we refer to these codes as constant-dimension codes (CDCs) henceforth. The standard advocated approach to random linear network coding (see, e.g., [60]) involves transmission of packet headers used to record the particular linear combination of the components of the message present in each received packet. From coding theoretic

[1] A related work [57] considers security issues in noncoherent random linear network coding.

perspective, the set of subspaces generated by the standard approach may be viewed as a **suboptimal** CDC with minimum subspace distance 2 in the Grassmannian, because the Grassmannian contains more spaces with minimum subspace distance 2 than those obtained by the standard approach [9]. Hence, studying random linear network coding from coding theoretic perspective results in better error control schemes.

General studies of subspace metric codes (also referred to as codes in projective space or projective geometry) started only recently (see, for example, [61, 62]). On the other hand, there is a steady stream of works that focuses on codes in the Grassmannian. For example, Delsarte [58] proved that the Grassmannian endowed with the subspace distance forms an association scheme, and derived its parameters. The nonexistence of perfect codes in the Grassmannian was proved in [59, 63]. In [64], it was shown that Steiner structures yield diameter-perfect codes in the Grassmannian; properties and constructions of these structures were studied in [65]; in [66], it was shown that Steiner structures result in optimal CDCs. Related work on certain intersecting families and on byte-correcting codes can be found in [67] and [68], respectively. An application of codes in the Grassmanian to linear authentication schemes was considered in [69]. In [9], a Singleton bound for CDCs and a family of codes that are **nearly** Singleton-bound achieving are proposed, and a recursive construction of CDCs which outperform the codes in [9] was given in [70]. Despite the **asymptotic optimality** of the Singleton bound and the codes proposed in [9], both are not optimal in finite cases: upper bounds tighter than the Singleton bound exist and can be achieved in some special cases [66]. It is yet to be determined the **maximal cardinality** of a CDC with **finite** dimension and minimum distance, and it is not clear how to construct the optimal code (or codes) that achieves the

maximal cardinality.

In this chapter, we introduce a novel approach to solving the two aforementioned problems. Namely, we aim to solve these problems via rank metric codes, in particular, constant-rank codes (CRCs), which are the counterparts in rank metric codes of constant Hamming weight codes. There are several reasons for our approach. First, it is difficult to answer the two questions based on CDCs directly since the projective space lacks a natural group structure [10]. Second, the rank metric is similar to the Hamming metric and hence familiar results from the Hamming space can be readily adapted. Furthermore, there are extensive works on rank metric codes in the literature. Finally, the rank metric has been shown relevant to error control for both noncoherent [10] and coherent [11] random linear network coding.

Based on our approach, this chapter makes two main contributions. Our first main contribution is that we establish a connection between CRCs and CDCs. Via this connection, we show that optimal CDCs correspond to optimal CRCs over sufficiently large extension fields. This connection converts the aforementioned open research problems about CDCs into research problems about CRCs, thereby allowing us to use rich results in rank metric codes to tackle such problems. Since constant-rank codes have received little attention in the literature, our second main contribution is our investigation of the properties of CRCs. In particular, we derive upper and lower bounds on the maximum cardinality of a CRC, propose explicit constructions of optimal or asymptotically optimal CRCs, and establish asymptotic bounds on the maximum rate of CRCs.

In a communication channel using an error-correcting code, if more errors occur than can be corrected by the code, then either the decoder returns a failure or it decodes the message into a wrong codeword. The latter case, referred to as a

decoder error, is often more detrimental than a failure, and hence the decoder error probability (DEP) hence is a crucial parameter for code design. This holds especially for random linear network coding, where a codeword consists of several packets. Since liftings of Gabidulin codes are nearly optimal CDCs [9] and a generalized rank metric decoder aimed at correcting the errors occurring on the network is proposed in [10], error control in random linear network coding using CDCs can be turned into a rank metric problem [10], and the errors occurring in the network result into additive rank errors.

We now introduce and motivate our choice of additive rank error models and their significance to error correction in random linear network coding. We consider the case of an adversary who injects linearly independent packets maliciously on the network using two strategies. In the first strategy, the adversary injects a number of packets chosen at random with equal probabilities. The packets undergo linear combinations through the network, and result into an additive error whose rank depends on the number of packets injected. Hence our first error model assumes that all additive errors with the same rank are equiprobable. The second and more general strategy assumes the adversary has some knowledge on and takes advantage of the data transmitted or the protocol used. Hence the adversary may choose to inject some packets which corrupt the messages more efficiently than others [11]. Due to the vector-space preserving property of linear network coding, the row space of the erroneous packets remains unchanged through the linear combinations operated at different nodes. Hence, the additive error can take any value provided its row space is fixed. This leads to our second model of additive rank errors, where all errors with the same row space are equiprobable. Finally, because of the properties of the rank metric, we also consider channels where errors with the same column

space are equiprobable.

The second contribution of this chapter is the investigation of the DEP of rank metric codes using a bounded rank distance decoder in Section 4.5. We derive asymptotically tight upper bounds on the DEP of rank metric codes used over an equal row or an equal column space channel. We also determine the exact DEP of MRD codes used over an equal row space channel.

Our work in this chapter differs from the error performance analysis of rank metric codes in [22] in several aspects, and is an extension of our previous work [29]. The error performance analysis in [22] was aimed at crisscross errors and as such, assumes different channel models and considers decoder errors and decoder failures together. Our previous work [29] derived upper bounds on bounded distance decoders for Gabidulin codes over the rank symmetric channel, and our results in this chapter are more general in terms of both the channel model and underlying codes.

Our results may also be seen as a nontrivial extension of the error performance of Hamming metric codes and maximum distance separable (MDS) codes in particular in [71–73]. In [71], an upper bound on the DEP of bounded Hamming distance decoders for Reed-Solomon codes (in fact, of any linear MDS code) was derived for a channel where all errors with the same Hamming weight are equiprobable. This work was refined in [72], where the exact DEP of linear MDS codes was determined over the same channel. In [73], the results in [71] were extended to more general channels and to any linear code. More precisely, [73] introduces error-value symmetric channels, where all errors with the same support are equiprobable, thus taking bursty channels into account. While our previous work in [29] parallels the work in [71], our analytical expression of the DEP of bounded distance decoders for MRD

codes over the rank symmetric channel parallels the work in [72]. However, our approach to derive our results for MRD codes is significantly different from the one used in [72]. The equal row (or column) space channel we considered can also be viewed as counterparts of the error-value symmetric channels in [73], and hence our results for arbitrary rank metric codes over the equal row (or column) space channel parallel the results in [73].

The rest of the chapter is organized as follows. Section 4.2 reviews some necessary background. In Section 4.3, we determine the connection between optimal CRCs and optimal CDCs. In Section 4.4, we study the maximum cardinality of CRCs, and we present our results on the asymptotic behavior of the maximum rate of a CRC. We finally study the DEP of rank metric codes using a bounded rank distance decoder in Section 4.5.

4.2 Subspace codes and CDCs

We refer to the set of all subspaces of $\mathrm{GF}(q)^n$ with dimension r as the Grassmannian of dimension r and denote it as $E_r(q,n)$ where $|E_r(q,n)| = \begin{bmatrix} n \\ r \end{bmatrix}$; we refer to $E(q,n) = \bigcup_{r=0}^{n} E_r(q,n)$ as the projective space. We remark that these notations are consistant with the ones introduced in Chapter 2 for ELSs. For $U, V \in E(q,n)$, both the *subspace metric* [9, (3)] $d_{\mathrm{S}}(U,V) \stackrel{\mathrm{def}}{=} \dim(U+V) - \dim(U \cap V)$ and *injection metric* [11, Def. 1]

$$\begin{aligned} d_{\mathrm{I}}(U,V) &\stackrel{\mathrm{def}}{=} \frac{1}{2} d_{\mathrm{S}}(U,V) + \frac{1}{2} |\dim(U) - \dim(V)| && (4.1) \\ &= \max\{\dim(U), \dim(V)\} - \dim(U \cap V) && (4.2) \\ &= \dim(U+V) - \min\{\dim(U), \dim(V)\} && (4.3) \end{aligned}$$

are metrics over $E(q,n)$. For all $U, V \in E(q,n)$,

$$\frac{1}{2}d_{\mathrm{S}}(U,V) \leq d_{\mathrm{I}}(U,V) \leq d_{\mathrm{S}}(U,V), \tag{4.4}$$

and $d_{\mathrm{I}}(U,V) = \frac{1}{2}d_{\mathrm{S}}(U,V)$ if and only if $\dim(U) = \dim(V)$, and $d_{\mathrm{I}}(U,V) = d_{\mathrm{S}}(U,V)$ if and only if $U \subseteq V$ or $V \subseteq U$. A *subspace code* is a nonempty subset of $E(q,n)$. The minimum subspace (respectively, injection) distance of a subspace code, is the minimum distance over all pairs of distinct codewords.

The Grassmannian $E_r(q,n)$ endowed with both the subspace metric and the injection metric forms an association scheme [9, 58]. Since $d_{\mathrm{S}}(U,V) = 2d_{\mathrm{I}}(U,V)$ for all $U, V \in E_r(q,n)$ and the injection distance provides a more natural distance spectrum, i.e., $0 \leq d_{\mathrm{I}}(U,V) \leq r$ for all $U, V \in E_r(q,n)$, we only consider the injection metric for the Grassmannian and CDCs. We denote the number of subspaces in $E_r(q,n)$ at distance d from a given subspace as $N_{\mathrm{C}}(d) = q^{d^2}\begin{bmatrix} r \\ d \end{bmatrix}\begin{bmatrix} n-r \\ d \end{bmatrix}$ [9], and a ball in $E_r(q,n)$ of radius t around a subspace U and its volume as $B_t(U)$ and $V_{\mathrm{C}}(t) = \sum_{d=0}^{t} N_{\mathrm{C}}(d)$, respectively.

A subset of $E_r(q,n)$ is called a constant-dimension code (CDC). A CDC is thus a subspace code whose codewords have the same dimension. We denote the **maximum** cardinality of a CDC in $E_r(q,n)$ with minimum distance d as $A_{\mathrm{C}}(q,n,r,d)$. Constructions of CDCs and bounds on $A_{\mathrm{C}}(q,n,r,d)$ have been given in [9, 62, 66, 70, 74]. In particular, $A_{\mathrm{C}}(q,n,r,1) = \begin{bmatrix} n \\ r \end{bmatrix}$ and it is shown [66, 70] for $r \leq \left\lfloor \frac{n}{2} \right\rfloor$ and $2 \leq d \leq r$,

$$\frac{q^{n(r-d+1)} - q^{(r+l)(r-d+1)}}{q^{r(r-d+1)} - 1} \leq A_{\mathrm{C}}(q,n,r,d) \leq \frac{\begin{bmatrix} n \\ r-d+1 \end{bmatrix}}{\begin{bmatrix} r \\ r-d+1 \end{bmatrix}}, \tag{4.5}$$

where $l \equiv n \mod r$. We denote the LHS of (4.5) as $L(q,n,r,d)$ and we refer to the class of codes with cardinality $L(q,n,r,d)$ introduced in [70] as Skachek codes.

CDCs are related to rank metric codes through the lifting operation [10]. The row space and the column space of a matrix $\mathbf{C}$ are denoted as $R(\mathbf{C})$ and $C(\mathbf{C})$, respectively. The lifting of $\mathbf{C} \in \mathrm{GF}(q)^{r\times(n-r)}$ is defined as $I(\mathbf{C}) = R(\mathbf{I}_r|\mathbf{C}) \in E_r(q,n)$. For all $\mathbf{C},\mathbf{D} \in \mathrm{GF}(q)^{r\times(n-r)}$, we have $d_{\mathrm{I}}(I(\mathbf{C}),I(\mathbf{D})) = d_{\mathrm{R}}(\mathbf{C},\mathbf{D})$ [10]. A KK code in $E_r(q,n)$ with minimum injection distance d is the lifting $I(\mathcal{C}) \subseteq E_r(q,n)$ of an MRD code $\mathcal{C} \subseteq \mathrm{GF}(q)^{r\times(n-r)}$ with minimum rank distance d. An efficient bounded subspace distance decoding algorithm for KK codes was also given in [9].

4.3 Connection between constant-dimension codes and constant-rank codes

In this section, we first establish some connections between the rank metric and the injection metric. We then define constant-rank codes and we show how optimal constant-rank codes can be used to construct optimal CDCs.

Let us denote the row span and the column span of $\mathbf{X} \in \mathrm{GF}(q)^{m\times n}$ over $\mathrm{GF}(q)$ as $R(\mathbf{X})$ and $C(\mathbf{X})$, respectively. The notations introduced above are naturally extended to codes as follows: for $\mathcal{C} \subseteq \mathrm{GF}(q)^{m\times n}$, $C(\mathcal{C}) \stackrel{\mathrm{def}}{=} \{C(\mathbf{C}) : \mathbf{C} \in \mathcal{C}\}$ and $R(\mathcal{C}) \stackrel{\mathrm{def}}{=} \{R(\mathbf{C}) : \mathbf{C} \in \mathcal{C}\}$.

Lemma 4.1. *For $U \in E_r(q,m)$, $V \in E_r(q,n)$, and $\mathbf{X} \in \mathrm{GF}(q)^{m\times n}$ with rank r, $C(\mathbf{X}) = U$ and $R(\mathbf{X}) = V$ if and only if $\mathbf{X} = \mathbf{G}^T\mathbf{H}$, where $\mathbf{G} \in \mathrm{GF}(q)^{r\times m}$ is a generator matrix of U and $\mathbf{H} \in \mathrm{GF}(q)^{r\times n}$ is a generator matrix of V.*

The proof of Lemma 4.1 is straightforward and hence omitted. We remark that $\mathbf{X} = \mathbf{G}^T\mathbf{H}$ is referred to as a rank factorization [75]. We now derive a relation between the rank distance between two matrices and the injection distances between

their respective row and column spans.

Theorem 4.2. *For all* $\mathbf{X}, \mathbf{Y} \in \mathrm{GF}(q)^{m\times n}$,

$$\begin{aligned}
&d_{\mathrm{I}}(R(\mathbf{X}), R(\mathbf{Y})) + d_{\mathrm{I}}(C(\mathbf{X}), C(\mathbf{Y})) - |\mathrm{rk}(\mathbf{X}) - \mathrm{rk}(\mathbf{Y})| \\
&\leq d_{\mathrm{R}}(\mathbf{X}, \mathbf{Y}) \\
&\leq \min\{d_{\mathrm{I}}(R(\mathbf{X}), R(\mathbf{Y})), d_{\mathrm{I}}(C(\mathbf{X}), C(\mathbf{Y}))\} + \min\{\mathrm{rk}(\mathbf{X}), \mathrm{rk}(\mathbf{Y})\}.
\end{aligned}$$

Proof. By Lemma 4.1, we have $\mathbf{X} = \mathbf{C}^T\mathbf{R}$ and $\mathbf{Y} = \mathbf{D}^T\mathbf{S}$, where $\mathbf{C} \in \mathrm{GF}(q)^{\mathrm{rk}(\mathbf{X})\times m}$, $\mathbf{R} \in \mathrm{GF}(q)^{\mathrm{rk}(\mathbf{X})\times n}$, $\mathbf{D} \in \mathrm{GF}(q)^{\mathrm{rk}(\mathbf{Y})\times m}$, $\mathbf{S} \in \mathrm{GF}(q)^{\mathrm{rk}(\mathbf{Y})\times n}$ are generator matrices of $C(\mathbf{X})$, $R(\mathbf{X})$, $C(\mathbf{Y})$, and $R(\mathbf{Y})$, respectively.

Hence $\mathbf{X} - \mathbf{Y} = (\mathbf{C}^T| - \mathbf{D}^T)(\mathbf{R}^T|\mathbf{S}^T)^T$. By [76, 0.4.5 (c)], we have

$$\mathrm{rk}(\mathbf{C}^T|\mathbf{D}^T)+\mathrm{rk}(\mathbf{R}^T|\mathbf{S}^T)-\mathrm{rk}(\mathbf{X})-\mathrm{rk}(\mathbf{Y}) \leq \mathrm{rk}(\mathbf{X}-\mathbf{Y}) \leq \min\{\mathrm{rk}(\mathbf{C}^T|\mathbf{D}^T), \mathrm{rk}(\mathbf{R}^T|\mathbf{S}^T)\}.$$

Since $\mathrm{rk}(\mathbf{C}^T|\mathbf{D}^T) = d_{\mathrm{I}}(C(\mathbf{X}), C(\mathbf{Y}))+\min\{\mathrm{rk}(\mathbf{X}), \mathrm{rk}(\mathbf{Y})\}$ and similarly $\mathrm{rk}(\mathbf{R}^T|\mathbf{S}^T) = d_{\mathrm{I}}(R(\mathbf{X}), R(\mathbf{Y})) + \min\{\mathrm{rk}(\mathbf{X}), \mathrm{rk}(\mathbf{Y})\}$, we obtain the claim. □

A *constant-rank code* (CRC) of constant-rank r in $\mathrm{GF}(q)^{m\times n}$ is a nonempty subset of $\mathrm{GF}(q)^{m\times n}$ such that all elements have rank r. Proposition 4.3 below shows how a CRC leads to two CDCs with their minimum injection distance related to the minimum rank distance of the CRC.

Proposition 4.3. *Let* $\mathcal{C}$ *be a CRC of constant-rank* r *and minimum distance* d_{R} *in* $\mathrm{GF}(q)^{m\times n}$. *Then* $R(\mathcal{C}) \subseteq E_r(q, n)$ *and* $C(\mathcal{C}) \subseteq E_r(q, m)$ *have minimum distances at least* $d_{\mathrm{R}} - r$.

The proof of Proposition 4.3 follows Theorem 4.2 and is hence omitted. When the minimum rank distance of a CRC is no less than its constant-rank, Proposition 4.4 below shows how the CRC leads to two CDCs with the **same cardinality**, and the relations between their distances can be further strengthened.

Proposition 4.4. *If $\mathcal{C}$ is a CRC of constant-rank r and minimum distance $d + r$ $(2 \leq d \leq r)$ in $\mathrm{GF}(q)^{m\times n}$, then $R(\mathcal{C}) \subseteq E_r(q,n)$ and $C(\mathcal{C}) \subseteq E_r(q,m)$ have cardinality $|\mathcal{C}|$ and their minimum distances satisfy $d_{\mathrm{I}}(C(\mathcal{C})) + d_{\mathrm{I}}(R(\mathcal{C})) \leq d + r \leq \min\{d_{\mathrm{I}}(C(\mathcal{C})), d_{\mathrm{I}}(R(\mathcal{C}))\} + r$.*

Proof. Let $\mathbf{X}$ and $\mathbf{Y}$ be any two distinct codewords in $\mathcal{C}$. By Theorem 4.2, we have $d_{\mathrm{I}}(R(\mathbf{X}), R(\mathbf{Y})) \geq d_{\mathrm{R}}(\mathbf{X}, \mathbf{Y}) - r \geq d > 0$, and hence $d_{\mathrm{I}}(R(\mathcal{C})) \geq d$ and $|R(\mathcal{C})| = |\mathcal{C}|$. Similarly, $d_{\mathrm{I}}(C(\mathbf{X}), C(\mathbf{Y})) \geq d > 0$, and thus $d_{\mathrm{I}}(C(\mathcal{C})) \geq d$ and $|C(\mathcal{C})| = |\mathcal{C}|$. Furthermore, if $d_{\mathrm{R}}(\mathbf{X}, \mathbf{Y}) = d + r$, then by Theorem 4.2, $d + r \geq d_{\mathrm{I}}(C(\mathbf{X}), C(\mathbf{Y})) + d_{\mathrm{I}}(R(\mathbf{X}), R(\mathbf{Y})) \geq d_{\mathrm{I}}(C(\mathcal{C})) + d_{\mathrm{I}}(R(\mathcal{C}))$. □

Using Lemma 4.1, we can construct CRCs in $\mathrm{GF}(q)^{m\times n}$ from a pair of CDCs in $E(q,n)$ and $E(q,m)$, respectively.

Proposition 4.5. *Let $\mathcal{M}$ be a CDC in $E_r(q,m)$ and $\mathcal{N}$ be a CDC in $E_r(q,n)$ such that $|\mathcal{M}| = |\mathcal{N}|$. Then there exists a CRC $\mathcal{C} \subseteq \mathrm{GF}(q)^{m\times n}$ with constant-rank r and cardinality $|\mathcal{M}|$ satisfying $C(\mathcal{C}) = \mathcal{M}$ and $R(\mathcal{C}) = \mathcal{N}$. Furthermore, its minimum distance d_{R} satisfies $d_{\mathrm{I}}(\mathcal{N}) + d_{\mathrm{I}}(\mathcal{M}) \leq d_{\mathrm{R}} \leq \min\{d_{\mathrm{I}}(\mathcal{N}), d_{\mathrm{I}}(\mathcal{M})\} + r$.*

Proof. Denote the generator matrices of the component subspaces of $\mathcal{M}$ and $\mathcal{N}$ as $\mathbf{G}_i$ and $\mathbf{H}_i$, respectively and define the code $\mathcal{C}$ formed by the codewords $\mathbf{X}_i = \mathbf{G}_i^T\mathbf{H}_i$ for $0 \leq i \leq |\mathcal{M}| - 1$. Then $C(\mathcal{C}) = \mathcal{M}$ and $R(\mathcal{C}) = \mathcal{N}$ by Lemma 4.1 and the lower bound on d_{R} follows Theorem 4.2. Let $\mathbf{X}_i$ and $\mathbf{X}_j$ be distinct codewords in $\mathcal{C}$ such that $d_{\mathrm{I}}(C(\mathbf{X}_i), C(\mathbf{X}_j)) = d_{\mathrm{I}}(\mathcal{M})$. By Theorem 4.2, we obtain $d_{\mathrm{R}} \leq d_{\mathrm{R}}(\mathbf{X}_i, \mathbf{X}_j) \leq d_{\mathrm{I}}(\mathcal{M}) + r$. Similarly, we also obtain $d_{\mathrm{R}} \leq d_{\mathrm{I}}(\mathcal{N}) + r$. □

We denote the maximum cardinality of a CRC in $\mathrm{GF}(q)^{m\times n}$ with constant-rank r and minimum distance d as $A_{\mathrm{R}}(q,m,n,d,r)$. If $\mathcal{C}$ is a CRC in $\mathrm{GF}(q)^{m\times n}$ with

constant-rank r, then its transpose code $\mathcal{C}^T$ forms a CRC in $\mathrm{GF}(q)^{n\times m}$ with the same constant-rank, minimum distance, and cardinality. Therefore $A_{\mathrm{R}}(q,m,n,d,r) = A_{\mathrm{R}}(q,n,m,d,r)$, and henceforth in this chapter we assume $n \leq m$ without loss of generality. We further observe that $A_{\mathrm{R}}(q,m,n,d,r)$ is a non-decreasing function of m and n, and a non-increasing function of d, and that $A_{\mathrm{C}}(q,n,r,d)$ is a non-decreasing function of n and a non-increasing function of d.

Proposition 4.6. *For all q, $2 \leq d \leq r \leq n \leq m$, and any $0 \leq p \leq r$,*

$$\min\{A_{\mathrm{C}}(q,n,r,d+p), A_{\mathrm{C}}(q,m,r,r-p)\} \leq A_{\mathrm{R}}(q,m,n,d+r,r) \leq A_{\mathrm{C}}(q,n,r,d). \tag{4.6}$$

Proof. Using the monotone properties of $A_{\mathrm{R}}(q,m,n,d_{\mathrm{R}},r)$ and $A_{\mathrm{C}}(q,n,r,d)$ above, the upper bound follows Proposition 4.4, while the lower bound follows Proposition 4.5 for $d_{\mathrm{I}}(\mathcal{M}) = r-p$ and $d_{\mathrm{I}}(\mathcal{N}) = d+p$. □

We remark that the lower bound in (4.6) is trivial for $d+p > \min\{r, n-r\}$ or $r-p > \min\{r, m-r\}$. Therefore, the lower bound in (4.6) is nontrivial when $\max\{0, 2r-m\} \leq p \leq \min\{r-d, n-r-d\}$.

Combining the bounds in (4.6), we obtain that the cardinalities of optimal CRCs over sufficiently large fields are equal to the cardinalities of CDCs with related distances. Furthermore, we show that optimal CDCs can be constructed from such optimal CRCs.

Theorem 4.7. *For all q, $2r \leq n \leq m$, and $1 \leq d \leq r$, $A_{\mathrm{R}}(q,m,n,d+r,r) = A_{\mathrm{C}}(q,n,r,d)$ if either $d = r$ or $m \geq m_0$, where $m_0 = (n-r)(r-d+1)+r+1$. Furthermore, if $\mathcal{C}$ is an optimal CRC in $\mathrm{GF}(q)^{m\times n}$ with constant-rank r and minimum distance $d+r$ for $m \geq m_0$ or $d = r$, then $R(\mathcal{C})$ is an optimal CDC in $E_r(q,n)$ with minimum distance d.*

Proof. First, the case where $d = r$ directly follows (4.6) for $p = 0$. Second, if $d < r$ and $m \geq m_0$, by (4.5) we obtain $A_{\mathrm{C}}(q, m, r, r) \geq q^{m-r} \geq q^{m_0-r}$. Also, by [29, Lemma 1], we obtain $q^{r(r-d+1)-1} < \alpha(r, r-d+1) \leq q^{r(r-d+1)}$ for all $2 \leq d < r$, and hence (4.5) yields $A_{\mathrm{C}}(q, n, r, d) < q^{(n-r)(r-d+1)+1} = q^{m_0-r} \leq A_{\mathrm{C}}(q, m, r, r)$. Thus, when $p = 0$, the lower bound in (4.6) simplifies to $A_{\mathrm{R}}(q, m, n, d+r, r) \geq A_{\mathrm{C}}(q, n, r, d)$. Combining with the upper bound in (4.6), we obtain $A_{\mathrm{R}}(q, m, n, d + r, r) = A_{\mathrm{C}}(q, n, r, d)$.

The second claim immediately follows Proposition 4.4. □

Theorem 4.7 implies that to determine $A_{\mathrm{C}}(q, n, r, d)$ and to construct optimal CDCs, it is sufficient to determine $A_{\mathrm{R}}(q, m, n, d + r, r)$ and to construct optimal CRCs over an extension field sufficiently large. We observe that this implies that $A_{\mathrm{R}}(q, m, n, d+r, r)$ remains constant for all $m \geq m_0$. When $d = r$, $A_{\mathrm{R}}(q, m, n, 2r, r)$ remains constant for $m \geq n$. When $d = 1$, $m_0 = (n-r+1)r+1$, but $A_{\mathrm{R}}(q, m, n, r+1, r)$ remains constant for $m \geq n$, and this is shown in Section 4.4.2.

4.4 Constant-rank codes

Having proved that optimal CRCs over sufficiently large extension fields lead to optimal CDCs, in this section we investigate the properties of CRCs.

4.4.1 Bounds

We now derive bounds on the maximum cardinality of CRCs. We first remark that the bounds on $A_{\mathrm{R}}(q, m, n, d, r)$ derived in Section 4.3 can be used in this section. Also, since $A_{\mathrm{R}}(q, m, n, 1, r) = N_{\mathrm{R}}(q, m, n, r)$ and $A_{\mathrm{R}}(q, m, n, d, r) = 1$ for $d > 2r$, we shall assume $2 \leq d \leq 2r$ henceforth.

We first derive the counterparts of the Gilbert and the Hamming bounds for CRCs in terms of intersections of spheres with rank radii.

Proposition 4.8. *For all* q, $1 \leq r, d \leq n \leq m$, *and* $t \stackrel{def}{=} \lfloor \frac{d-1}{2} \rfloor$,

$$\frac{N_{\mathrm{R}}(q,m,n,r)}{\sum_{i=0}^{d-1} J_{\mathrm{R}}(q,m,n,i,r,r)} \leq A_{\mathrm{R}}(q,m,n,d,r) \leq \min_{1 \leq s \leq n} \left\{ \frac{N_{\mathrm{R}}(q,m,n,s)}{\sum_{i=0}^{t} J_{\mathrm{R}}(q,m,n,i,s,r)} \right\}.$$

Proof. The proof of the lower bound is straightforward and hence omitted. Let $\mathcal{C} = \{\mathbf{c}_k\}_{k=0}^{K-1}$ be a CRC with constant-rank r and minimum distance d in $\mathrm{GF}(q)^{m \times n}$. For all $0 \leq k \leq K-1$ and $0 \leq s \leq n-1$, if we denote the set of matrices in $\mathrm{GF}(q)^{m \times n}$ with rank s and distance $\leq t$ from $\mathbf{c}_k$ as $R_{k,s}$, then $|R_{k,s}| = \sum_{i=0}^{t} J_{\mathrm{R}}(i,s,r)$ for all k. Clearly $R_{k,s} \cap R_{l,s} = \emptyset$ for all $k \neq l$, and hence $N_{\mathrm{R}}(s) \geq |\bigcup_{k=0}^{K-1} R_{k,s}| = K|R_{k,s}|$, which yields the upper bound. □

We now derive upper bounds on $A_{\mathrm{R}}(q,m,n,d,r)$. We begin by proving the counterpart in rank metric codes of a well-known bound on constant-weight codes proved by Johnson in [77].

Proposition 4.9. *For all* q, $1 \leq r, d < n \leq m$, $A_{\mathrm{R}}(q,m,n,d,r) \leq \frac{q^n-1}{q^{n-r}-1} A_{\mathrm{R}}(q,m,n-1,d,r)$.

Proof. Note that the row span of any matrix $\mathbf{X} \in \mathrm{GF}(q)^{m \times n}$ with rank r is a subspace of $\begin{bmatrix} n-r \\ 1 \end{bmatrix}$ subspaces in $E_{n-1}(q,n)$.

Let $\mathcal{C}$ be an optimal CRC in $\mathrm{GF}(q)^{m \times n}$ with constant-rank r and minimum distance d. For all $\mathbf{C} \in \mathcal{C}$ and all $V \in E_{n-1}(q,n)$, we define $f(V,\mathbf{C}) = 1$ if $R(\mathbf{C}) \subseteq V$ and $f(V,\mathbf{C}) = 0$ otherwise. For all $\mathbf{C}$, $\sum_{V \in E_{n-1}(q,n)} f(V,\mathbf{C}) = \begin{bmatrix} n-r \\ 1 \end{bmatrix}$, and for all V,

$\sum_{\mathbf{C}\in\mathcal{C}} f(V,\mathbf{C}) = |\{\mathbf{C}\in C : R(\mathbf{C})\subseteq V\}|$. Summing over all possible pairs, we obtain

$$\begin{aligned}\sum_{V\in E_{n-1}(q,n)}\sum_{\mathbf{C}\in\mathcal{C}} f(V,\mathbf{C}) &= \sum_{V\in E_{n-1}(q,n)} |\{\mathbf{C}\in C : R(\mathbf{C})\subseteq V\}| \\ \sum_{\mathbf{C}\in\mathcal{C}}\sum_{V\in E_{n-1}(q,n)} f(V,\mathbf{C}) &= \begin{bmatrix} n-r \\ 1 \end{bmatrix} A_{\mathrm{R}}(q,m,n,d,r).\end{aligned}$$

Hence there exists $U\in E_{n-1}(q,n)$ which satisfies $|\{\mathbf{C}\in C : R(\mathbf{C})\subseteq U\}| \geq \frac{\begin{bmatrix} n-r \\ 1 \end{bmatrix}}{\begin{bmatrix} n \\ 1 \end{bmatrix}} A_{\mathrm{R}}(q,m,n,d,r)$. All the codewords $\mathbf{C}_i$ with $R(\mathbf{C}_i)\subseteq U$ can be expressed as $\mathbf{C}_i = \mathbf{G}_i^T\mathbf{H}_i\mathbf{U}$, where $\mathbf{H}_i\in \mathrm{GF}(q)^{r\times(n-1)}$ and $\mathbf{U}\in\mathrm{GF}(q)^{(n-1)\times n}$ is a generator matrix of U. Therefore, the code $\{\mathbf{G}_i^T\mathbf{H}_i\}$ forms a CRC in $\mathrm{GF}(q)^{m\times n-1}$ with constant-rank r, minimum distance d, and cardinality $|\{\mathbf{C}\in C : R(\mathbf{C})\subseteq U\}|$, and hence $\frac{q^{n-r}-1}{q^n-1}A_{\mathrm{R}}(q,m,n,d,r) \leq |\{\mathbf{C}\in C : R(\mathbf{C})\subseteq U\}| \leq A_{\mathrm{R}}(q,m,n-1,d,r)$. □

The Singleton bound for rank metric codes yields upper bounds on $A_{\mathrm{R}}(q,m,n,d,r)$. For any $I\subseteq\{0,1,\ldots,n\}$, let $A_{\mathrm{R}}(q,m,n,d,I)$ denote the maximum cardinality of a code in $\mathrm{GF}(q)^{m\times n}$ with minimum rank distance d such that all codewords have ranks belonging to I. Then $A_{\mathrm{R}}(q,m,n,d,r)\leq q^{m(n-d+1)} - A_{\mathrm{R}}(q,m,n,d,P_r)$, where $P_r \stackrel{\text{def}}{=} \{i : 0\leq i\leq n, |i-r|\geq d\}$. We now determine the counterpart of the Singleton bound for CRCs.

Proposition 4.10. *For all* $0\leq i\leq \min\{d-1,r\}$, $J_i \stackrel{def}{=} \{r-i, r-i+1,\ldots,\min\{n-i,r\}\}$. *Then*

$$A_{\mathrm{R}}(q,m,n,d,r) \leq A_{\mathrm{R}}(q,m,n-i,d-i,J_i). \tag{4.7}$$

Proof. Let $\mathcal{C}$ be an optimal CRC in $\mathrm{GF}(q)^{m\times n}$ with constant-rank r and minimum distance d, and consider the code $\mathcal{C}_i$ obtained by puncturing i coordinates of the codewords in $\mathcal{C}$. Since $i\leq r$, the codewords of $\mathcal{C}_i$ all have ranks between $r-i$ and $\min\{n-i,r\}$. Also, since $i<d$, any two codewords have distinct puncturings, and

we obtain $|\mathcal{C}_i| = |\mathcal{C}|$ and $d_{\mathrm{R}}(\mathcal{C}_i) \geq d - i$. Hence $A_{\mathrm{R}}(q, m, n, d, r) = |\mathcal{C}| = |\mathcal{C}_i| \leq A_{\mathrm{R}}(q, m, n - i, d - i, J_i)$. □

We now combine the counterparts of the Johnson bound in Proposition 4.9 and of the Singleton bound in Proposition 4.10 in order to obtain an upper bound on $A_{\mathrm{R}}(q, m, n, d, r)$ for $d \leq r$.

Proposition 4.11. *For all q, $1 \leq d \leq r \leq n \leq m$, $A_{\mathrm{R}}(q, m, n, d, r) \leq \begin{bmatrix} n \\ r \end{bmatrix} \alpha(m, r - d + 1)$.*

Proof. Applying Proposition 4.9 $n-r$ times successively, we obtain $A_{\mathrm{R}}(q, m, n, d, r) \leq \begin{bmatrix} n \\ r \end{bmatrix} A_{\mathrm{R}}(q, m, r, d, r)$. For $n = r$ and $i = d - 1$, $J_i = \{r - d + 1\}$ and hence (4.7) yields $A_{\mathrm{R}}(q, m, r, d, r) \leq A_{\mathrm{R}}(q, m, r - d + 1, 1, r - d + 1) = N_{\mathrm{R}}(q, m, r - d + 1, r - d + 1) = \alpha(m, r - d + 1)$. Thus $A_{\mathrm{R}}(q, m, n, d, r) \leq \begin{bmatrix} n \\ r \end{bmatrix} \alpha(m, r - d + 1)$. □

We now derive the counterpart in rank metric codes of the Bassalygo-Elias bound [78]. We also tighten the bound when $d > r + 1$.

Proposition 4.12. *For $\max\{r, d\} \leq k \leq n$, $0 \leq s \leq k$, $k \leq l \leq m$, and any code $\mathcal{C} \subseteq \mathrm{GF}(q)^{l \times k}$ with minimum rank distance d and rank distribution $A_i \stackrel{def}{=} |\{\mathbf{C} \in \mathcal{C} : \mathrm{rk}(\mathbf{C}) = i\}|$,*

$$A_{\mathrm{R}}(q, m, n, d, r) \geq \max_{s, \{A_i\}, k, l} \frac{\sum_{i=0}^{n} A_i J_{\mathrm{R}}(q, l, k, s, r, i)}{N_{\mathrm{R}}(q, l, k, s)}. \tag{4.8}$$

Furthermore, if $r + 1 < d \leq 2r$, then

$$A_{\mathrm{R}}(q, m, n, d, r) \geq \max_{s, \{A_i\}, k, l} \frac{\sum_{i=0}^{n} A_i J_{\mathrm{R}}(q, l, k, s, r, i)}{N_{\mathrm{R}}(q, l, k, s) - \sum_{i=0}^{n} A_i \sum_{t=0}^{d-r-1} J_{\mathrm{R}}(q, l, k, s, t, i)}. \tag{4.9}$$

The proof of Proposition 4.12 is given in Appendix 7.3.1.

Although the RHS of (4.8) and (4.9) can be maximized over $\{A_i\}$, it is difficult to do so since $\{A_i\}$ is not available for most rank metric codes with the exception

of linear MRD codes. Thus, we derive a bound using the rank weight distribution of linear MRD codes.

Corollary 4.13. *For all q, $1 \leq r, d \leq n \leq m$, $A_{\mathrm{R}}(q,m,n,d,r) \geq N_{\mathrm{R}}(q,m,n,r)\, q^{m(-d+1)}$.*

Proof. Applying (4.8) to an $(n, n-d+1, d)$ MRD code over $\mathrm{GF}(q^m)$, we obtain $N_{\mathrm{R}}(q,m,n,s)A_{\mathrm{R}}(q,m,n,d,r) \geq \sum_{i=0}^{n} M(q,m,n,d,i)J_{\mathrm{R}}(q,m,n,s,r,i)$. Summing for all $0 \leq s \leq n$, we obtain $A_{\mathrm{R}}(q,m,n,d,r) \geq N_{\mathrm{R}}(q,m,n,r)q^{m(-d+1)}$ since $\sum_{s=0}^{n} J_{\mathrm{R}}(s,r,i) = N_{\mathrm{R}}(q,m,n,r)$. □

The RHS of (4.8) and (4.9) decrease rapidly with increasing d, rendering the bounds trivial for d approaching $2r$.

We investigate below the tightness of the bound in Corollary 4.13.

Proposition 4.14. *For all q, $2 \leq d \leq r \leq n \leq m$, we define $C(q,m,n,d,r) \stackrel{def}{=} A_{\mathrm{R}}(q,m,n,d,r)/[N_{\mathrm{R}}(q,m,n,r)q^{m(-d+1)}]$. Then $C(q,m,n,d,r) \leq \frac{q^2}{q^2-1}$ for $r+d-1 \leq m$ and $C(q,m,n,d,r) < \frac{q-1}{q}K_q^{-1}$ otherwise.*

Proof. By Proposition 4.11, $C(q,m,n,d,r) \leq q^{m(d-1)}\alpha(m,r-d+1)/\alpha(m,r) = q^{(m-r+d-1)(d-1)}/\alpha(m-r+d-1,d-1)$. Since $\alpha(n,l) > \frac{q}{q-1}K_q q^{nl}$ for all $1 \leq l \leq n-1$ [29, Lemma 1], we obtain $C(q,m,n,d,r) < \frac{q-1}{q}K_q^{-1}$. Finally, $\alpha(n,l) \geq \frac{q^2-1}{q^2}q^{nl}$ for $l \leq n-l$ [29, Lemma 1] yields $C(q,m,n,d,r) \leq \frac{q^2}{q^2-1}$ for $r+d-1 \leq m$. □

The bound in Corollary 4.13 is hence tight up to a scalar when $d \leq r$. However, these bounds are not constructive. Below we derive constructive bounds on $A_{\mathrm{R}}(q,m,n,d,r)$.

4.4.2 Constructions of CRCs

We now give explicit constructions of good CRCs when $d \leq r$, which in turn yield asymptotically tight lower bounds on $A_{\mathrm{R}}(q, m, n, d, r)$. We assume the matrices in $\mathrm{GF}(q)^{m\times n}$ are mapped into vectors in $\mathrm{GF}(q^m)^n$ according to a fixed basis B_m of $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$.

Proposition 4.15. *For all q, $2 \leq d \leq r \leq n \leq m$,*

$$A_{\mathrm{R}}(q, m, n, d, r) \geq M(q, m, n, d, r) > \begin{bmatrix} n \\ r \end{bmatrix} q^{m(r-d)}.$$

Proof. The codewords of rank r in an $(n, n-d+1, d)$ linear MRD code over $\mathrm{GF}(q^m)$ form an (n, d, r) CRC. Thus, $A_{\mathrm{R}}(q, m, n, d, r) \geq M(q, m, n, d, r)$.

We now prove the lower bound on $M(q, m, n, d, r)$. First, for $d = r$ we have $M(q, m, n, r, r) = \begin{bmatrix} n \\ r \end{bmatrix}(q^m-1) > \begin{bmatrix} n \\ r \end{bmatrix}$. Second, suppose $d < r$. By (2.1), $M(q, m, n, d, r)$ can be expressed as $M(q, m, n, d, r) = \begin{bmatrix} n \\ r \end{bmatrix} \sum_{j=d}^{r}(-1)^{r-j}\mu_j$, where $\mu_j = q^{(r-j)(r-j-1)/2} \begin{bmatrix} r \\ j \end{bmatrix}(q^{m(j-d+1)}-1)$. It can be easily shown that $\mu_j > \mu_{j-1}$ for $d+1 \leq j \leq r$, and hence $M(q, m, n, d, r) \geq \begin{bmatrix} n \\ r \end{bmatrix}(\mu_r - \mu_{r-1})$. Therefore, $M(q, m, n, d, r) \geq \begin{bmatrix} n \\ r \end{bmatrix}[(q^{m(r-d+1)} - 1) - \begin{bmatrix} r \\ 1 \end{bmatrix}(q^{m(r-d)} - 1)] > \begin{bmatrix} n \\ r \end{bmatrix} q^{m(r-d)}$. □

Corollary 4.16. *For all q, $1 \leq r \leq n \leq m$, $A_{\mathrm{R}}(q, m, n, r, r) = \begin{bmatrix} n \\ r \end{bmatrix}(q^m - 1)$.*

Proof. By Proposition 4.11, $A_{\mathrm{R}}(q, m, n, r, r) \leq \begin{bmatrix} n \\ r \end{bmatrix}(q^m-1)$, and by Proposition 4.15, $A_{\mathrm{R}}(q, m, n, r, r) \geq M(q, m, n, r, r) = \begin{bmatrix} n \\ r \end{bmatrix}(q^m - 1)$. □

By Corollary 4.16, the codewords of rank r in an $(n, n-r+1, r)$ linear MRD code are optimal. We investigate below the tightness of the constructive lower bound in Proposition 4.15.

Proposition 4.17. *For all q, $1 \leq d < r \leq n \leq m$, we define $B(q,m,n,d,r) \stackrel{def}{=} A_{\mathrm{R}}(q,m,n,d,r)/M(q,m,n,d,r)$. Then for $m \geq 3$,*

$$\begin{aligned}
B(2,m,m,m-1,m) &\leq 2^{m-1}-1 && (4.10)\\
B(q,m,m,m-1,m) &< \frac{q-1}{q-2} \text{ if } q>2 && (4.11)\\
B(q,m,m,m-2,m) &< \frac{(q^2-1)(q-1)}{(q^2-1)(q-2)+1} && (4.12)\\
B(q,m,m,d,m) &< \frac{(q^3-1)(q^2-1)(q-1)}{(q^3-1)(q^2-1)(q-2)+q^3-2} \text{ if } d<m-2 && (4.13)\\
B(q,m,n,d,r) &< \frac{q}{q-1} \quad \textit{for } r<m. && (4.14)
\end{aligned}$$

The proof of Proposition 4.17 is given in Appendix 7.3.2.

Proposition 4.17 shows that for all but one cases, the codewords of rank r in an $(n, n-d+1, d)$ MRD code form a code whose cardinality is close to that of an optimal CRC up to a scalar which tends to 1 for large q.

We now construct CRCs for $d > r$ using generalized Gabidulin codes [26]. Let $\mathbf{g} \in \mathrm{GF}(q^m)^n$ have rank n, and for $0 \leq i \leq m-1$, denote the vector in $\mathrm{GF}(q^m)^n$ obtained by elevating each coordinate of $\mathbf{g}$ to the q^{ai}-th power as $\mathbf{g}^{[i]}$, where a and m are coprime. Let $\mathcal{C}$ be the $(n, n-d+1, d)$ generalized Gabidulin code over $\mathrm{GF}(q^m)$ generated by $\left(\mathbf{g}^{[0]^T}, \mathbf{g}^{[1]^T}, \ldots, \mathbf{g}^{[n-d]^T}\right)^T$, and $\mathcal{C}'$ be the $(n, d-r, n-d+r+1)$ generalized Gabidulin code generated by $\left(\mathbf{g}^{[n-d+1]^T}, \mathbf{g}^{[n-d+2]^T}, \ldots, \mathbf{g}^{[n-r]^T}\right)^T$. We consider the coset $\mathcal{C}+\mathbf{c}'$, where $\mathbf{c}' \in \mathcal{C}'$, and we denote the number of codewords of rank r in $\mathcal{C}+\mathbf{c}'$ as $\sigma_r(\mathbf{c}')$.

Lemma 4.18. *For all $d > r$, there exists $\mathbf{c}' \in \mathcal{C}'$ such that $\sigma_r(\mathbf{c}') \geq \begin{bmatrix} n \\ r \end{bmatrix} q^{m(r-d+1)}$.*

Proof. Any codeword $\mathbf{c}' \in \mathcal{C}'$ can be expressed as $\mathbf{c}' = c_{n-d+1}\mathbf{g}^{[n-d+1]} + c_{n-d+2}\mathbf{g}^{[n-d+2]} + \ldots + c_{n-r}\mathbf{g}^{[n-r]}$, where $c_i \in \mathrm{GF}(q^m)$ for $n-d+1 \leq i \leq n-r$. If $c_{n-r} = 0$, then

$(\mathcal{C}+\mathbf{c}') \subset \mathcal{D}$, where $\mathcal{D}$ is the $(n, n-r, r+1)$ generalized Gabidulin code generated by $\left(\mathbf{g}^{[0]^T}, \mathbf{g}^{[1]^T}, \ldots, \mathbf{g}^{[n-r-1]^T}\right)^T$. Therefore $\sigma_r(\mathbf{c}') = 0$ if $c_{n-r} = 0$.

Denote the number of codewords of rank r in $\mathcal{C} \oplus \mathcal{C}'$ as τ_r. Since $\bigcup_{\mathbf{c}' \in \mathcal{C}'} (\mathcal{C}+\mathbf{c}') = \mathcal{C} \oplus \mathcal{C}'$, we have $\tau_r = \sum_{\mathbf{c}' \in \mathcal{C}'} \sigma_r(\mathbf{c}')$. Also, $\mathcal{C} \oplus \mathcal{C}'$ forms an $(n, n-r+1, r)$ MRD code, and hence $\tau_r = M(q, m, n, r, r) = \begin{bmatrix} n \\ r \end{bmatrix}(q^m - 1)$. Suppose that for all $\mathbf{c}' \in \mathcal{C}'$, $\sigma_r(\mathbf{c}') < \begin{bmatrix} n \\ r \end{bmatrix} q^{m(r-d+1)}$. Then $\tau_r = \sum_{\mathbf{c}' : c_{n-r} \neq 0} \sigma_r(\mathbf{c}') < \begin{bmatrix} n \\ r \end{bmatrix}(q^m - 1)$, which contradicts $\tau_r = \begin{bmatrix} n \\ r \end{bmatrix}(q^m - 1)$. □

Although Lemma 4.18 proves the existence of a vector $\mathbf{c}'$ for which the translate $\mathcal{C} + \mathbf{c}'$ has high cardinality, it does not indicate how to choose $\mathbf{c}'$. For $d = r + 1$, it can be shown that all $\mathbf{c}' \in \mathcal{C}'$ satisfy the bound, and that they all lead to optimal codes.

Corollary 4.19. *If $d = r + 1$, then $\sigma_r(\mathbf{c}') = \begin{bmatrix} n \\ r \end{bmatrix}$ for all $\mathbf{c}' \in \mathcal{C}'$.*

Proof. First, by Proposition 4.6, $\sigma_r(\mathbf{c}') \leq A_{\mathrm{R}}(q, m, n, r+1, r) \leq A_{\mathrm{C}}(q, n, r, 1) = \begin{bmatrix} n \\ r \end{bmatrix}$ for all $\mathbf{c}' \in \mathcal{C}'$. Suppose there exists $\mathbf{c}'$ such that $\sigma_r(\mathbf{c}') < \begin{bmatrix} n \\ r \end{bmatrix}$. Then $\tau_r < \begin{bmatrix} n \\ r \end{bmatrix}(q^m - 1)$, which contradicts $\tau_r = \begin{bmatrix} n \\ r \end{bmatrix}(q^m - 1)$. □

Proposition 4.20. *For all q, $1 \leq r < d \leq n \leq m$, $A_{\mathrm{R}}(q, m, n, d, r) \geq \begin{bmatrix} n \\ r \end{bmatrix} q^{n(r-d+1)}$, and a class of codes that satisfy this bound can be constructed from Lemma 4.18.*

Proof. The codewords of rank r in a code considered in Lemma 4.18 form a CRC in $\mathrm{GF}(q)^{m \times n}$ with constant-rank r, minimum distance d, and cardinality $\geq \begin{bmatrix} n \\ r \end{bmatrix} q^{m(r-d+1)}$. Therefore, $A_{\mathrm{R}}(q, m, n, d, r) \geq \begin{bmatrix} n \\ r \end{bmatrix} q^{m(r-d+1)}$. The proof is concluded by noting that $A_{\mathrm{R}}(q, m, n, d, r) \geq A_{\mathrm{R}}(q, n, n, d, r) \geq \begin{bmatrix} n \\ r \end{bmatrix} q^{n(r-d+1)}$. □

Corollary 4.21. *For all q, $1 \leq r < n \leq m$, $A_{\mathrm{R}}(q, m, n, r+1, r) = \begin{bmatrix} n \\ r \end{bmatrix} = A_{\mathrm{C}}(q, n, r, 1)$.*

Proof. Combine Proposition 4.6 and Proposition 4.20. □

We note that $\begin{bmatrix} n \\ r \end{bmatrix}$ is independent of m. We also remark that the lower bound in Proposition 4.20 is also trivial for d approaching $2r$. Since the proof is only partly constructive, computer search can be used to help find better results for small parameter values.

4.4.3 Asymptotic results

We study the asymptotic behavior of CRCs using the following set of normalized parameters: $\nu = \frac{n}{m}$, $\rho = \frac{r}{m}$, and $\delta = \frac{d}{m}$. By definition, $0 \leq \rho, \delta \leq \nu$, and since we assume $n \leq m$, $\nu \leq 1$. We consider the asymptotic rate defined as $a_{\mathrm{R}}(\nu, \delta, \rho) \stackrel{\text{def}}{=} \lim_{m\to\infty} \sup \left[\log_{q^{m^2}} A_{\mathrm{R}}(q, m, n, d, r)\right]$. We now investigate how $A_{\mathrm{R}}(q, m, n, d, r)$ behaves as the parameters tend to infinity. Without loss of generality, we only consider the case where $0 \leq \delta \leq \min\{\nu, 2\rho\}$, since $a_{\mathrm{R}}(\nu, \delta, \rho) = 0$ for $\delta > 2\rho$.

Proposition 4.22. *For $0 \leq \delta \leq \rho$, $a_{\mathrm{R}}(\nu, \delta, \rho) = \rho(1 + \nu - \rho) - \delta$. For $\rho \leq \delta$, we have to distinguish three cases. First, for $2\rho \leq \nu$,*

$$\max\left\{\frac{(1-\rho)(\nu-\rho)}{1+\nu-2\rho}(2\rho-\delta), \rho(2\nu-\rho)-\nu\delta\right\} \leq a_{\mathrm{R}}(\nu,\delta,\rho) \leq (\nu-\rho)(2\rho-\delta). \tag{4.15}$$

Second, for $\nu \leq 2\rho \leq 1$,

$$\max\left\{\rho(1-\rho)(\nu-\delta), \rho(2\nu-\rho)-\nu\delta\right\} \leq a_{\mathrm{R}}(\nu,\delta,\rho) \leq \rho(\nu-\delta). \tag{4.16}$$

Third, for $2\rho \geq 1$,

$$\max\left\{\frac{\rho}{2}(1+\nu-2\rho-\delta), \rho(2\nu-\rho)-\nu\delta, 0\right\} \leq a_{\mathrm{R}}(\nu,\delta,\rho) \leq \rho(\nu-\delta). \tag{4.17}$$

The proof of Proposition 4.22 is given in Appendix 7.3.3.

Proposition 4.17 indicates that the codewords of a given rank in a linear MRD code form asymptotically optimal CRCs. In particular, Proposition 4.22 shows that the set of codewords with rank n in an $(n, n-d+1, d)$ linear MRD code constitutes a CRC of rank n and asymptotic rate of $\nu - \delta$, which is equal to the asymptotic rate of an optimal rank metric code [27].

We can split the range of δ into two regions: when $\delta \leq \rho$, the asymptotic rate of CRCs is determined due to the construction of good CRCs when $d \leq r$; when $\delta \geq \rho$, we only have bounds on the asymptotic rate of CRCs. Also, the lower bounds based on the connection between CDCs and CRCs (the first lower bound in the LHS of (4.15), (4.16), and (4.17)) are tighter for $2\rho \leq \nu$ and on the other hand become trivial for ρ approaching 1.

4.5 Decoder error probability of rank metric codes

4.5.1 Decoder error probability of rank metric codes used over a rank symmetric channel

We now study the DEP of a rank metric code in $\mathrm{GF}(q)^{m\times n}$ with minimum rank distance d using a bounded rank distance decoder over a rank symmetric channel, defined below.

Definition 4.23. *A channel on* $\mathrm{GF}(q)^{m\times n}$ *is* rank symmetric *if the inputs and the outputs are matrices in* $\mathrm{GF}(q)^{m\times n}$ *and if all the outputs at the same rank distance from the input are equiprobable.*

Since using a code $\mathcal{C} \subseteq \mathrm{GF}(q)^{m\times n}$ over a rank symmetric channel on $\mathrm{GF}(q)^{m\times n}$

is equivalent to using its transpose code $\mathcal{C}^T = \{\mathbf{C}^T : \mathbf{C} \in \mathcal{C}\}$ over a rank symmetric channel on $\mathrm{GF}(q)^{n\times m}$, we assume $n \leq m$ without loss of generality.

Given a matrix $\mathbf{M} \in \mathrm{GF}(q)^{m\times n}$ as input, a bounded distance decoder for a code $\mathcal{C}$ either produces the codeword in $\mathcal{C}$ at distance at most $t = \lfloor \frac{d-1}{2} \rfloor$ from $\mathbf{M}$ if such a codeword exists, or returns a failure otherwise. The *decoder error probability* (DEP) is the probability that the decoder produces a codeword different to the one that was sent. The output of the bounded rank distance decoder depends on $u = d_{\mathrm{R}}(\mathbf{M}, \mathbf{C})$, where $\mathbf{C} \in \mathcal{C}$ is the sent codeword. The decoder returns $\mathbf{C}$ if and only if $u \leq t$, and returns a failure for $t < u < d - t$. The DEP for $u \geq d - t$ depends on the rank distance distribution $A_w(\mathbf{C})$ of the code.

Proposition 4.24. *Assuming a codeword $\mathbf{C} \in \mathcal{C}$, a code in $\mathrm{GF}(q)^{m\times n}$ with minimum rank distance d, is sent over a rank symmetric channel and the channel output is distance u from $\mathbf{C}$, the DEP of a bounded rank distance decoder satisfies*

$$\begin{aligned} P_{\mathrm{R}}(\mathbf{C}, u) &= \frac{1}{N_{\mathrm{R}}(u)} \sum_{w=d}^{n} A_w(\mathbf{C}) \sum_{s=0}^{t} J_{\mathrm{R}}(u, s, w) && (4.18)\\ &\leq \frac{1}{N_{\mathrm{R}}(u)} \sum_{w=d}^{n} \begin{bmatrix} n \\ w \end{bmatrix} \alpha(m, w-d+1) \sum_{s=0}^{t} J_{\mathrm{R}}(u, s, w) && (4.19)\\ &< K_q^{-2} q^{-t(m-n+t)}. && (4.20) \end{aligned}$$

Proof. We have $P_{\mathrm{R}}(\mathbf{C}, u) = \frac{D(\mathbf{C},u)}{N_{\mathrm{R}}(u)}$, where $D(\mathbf{C}, u)$ is the number of decodable matrices at distance u from $\mathbf{C}$. The set of decodable matrices is the disjoint union of balls with radius t around the codewords. For any codeword $\mathbf{D}$ at distance w from $\mathbf{C}$, there exist exactly $J_{\mathrm{R}}(u, s, w)$ matrices $\mathbf{M}$ such that $d_{\mathrm{R}}(\mathbf{D}, \mathbf{M}) = s$ and $d_{\mathrm{R}}(\mathbf{C}, \mathbf{M}) = u$. Summing for all s and all $\mathbf{D}$, we obtain (4.18).

Also, since $\{\mathbf{D} - \mathbf{C} : \mathbf{D} \in \mathcal{C}, d_{\mathrm{R}}(\mathbf{D}, \mathbf{C}) = w\}$ is a CRC with minimum distance at least d and constant-rank w, we have $A_w(\mathbf{C}) \leq A_{\mathrm{R}}(q, m, n, d, w) \leq \begin{bmatrix} n \\ w \end{bmatrix} \alpha(m, w-d+1)$

by Proposition 4.11, which leads to (4.19). We have

$$\begin{bmatrix} n \\ w \end{bmatrix} \alpha(m, w-d+1) = \begin{bmatrix} n \\ w \end{bmatrix} \alpha(m,w) \frac{q^{-(d-1)(w-d+1)}}{\alpha(m-w+d-1, d-1)} < K_q^{-1} q^{-m(d-1)} N_{\mathrm{R}}(w), \tag{4.21}$$

and hence

$$\begin{aligned} P_{\mathrm{R}}(\mathbf{C}, u) &< \frac{1}{N_{\mathrm{R}}(u)} K_q^{-1} q^{-m(d-1)} \sum_{s=0}^{t} \sum_{w=d}^{n} N_{\mathrm{R}}(w) J_{\mathrm{R}}(u,s,w) \\ &= K_q^{-1} q^{-m(d-1)} \sum_{s=0}^{t} \sum_{w=d}^{n} J_{\mathrm{R}}(w,s,u) \qquad (4.22) \\ &\leq K_q^{-1} q^{-m(d-1)} V_{\mathrm{R}}(t), \qquad (4.23) \end{aligned}$$

where (4.22) and (4.23) follow (2.2) and (2.3), respectively. Using Lemma 2.18, we obtain (4.20). □

It is remarkable that the upper bound on the DEP in (4.20) does not depend on $\mathbf{C}$ and u for **any rank metric code**. In fact, applying (4.20) to linear MRD codes leads to [29, Proposition 6]. This general result on the error performance of rank metric codes parallel that for Hamming metric codes [73].

We now show that MRD codes have the **greatest** DEP among all rank metric codes up to a scalar in nontrivial cases. Let us denote the DEP of an MRD code in $\mathrm{GF}(q)^{m\times n}$ with minimum rank distance d as $P_{\mathrm{R,MRD}}(u)$.

Corollary 4.25. *Let $\mathcal{C}$ be any rank metric code in $\mathrm{GF}(q)^{m\times n}$ $(n \leq m)$ with minimum rank distance d and let $\mathbf{C} \in \mathcal{C}$. Then if $q > 2$, $n < m$, or $d \neq m-1$, $P_{\mathrm{R}}(\mathbf{C}, u) < H_q P_{\mathrm{R,MRD}}(u)$, where $H_2 = 3.5$ and $H_q = \frac{q-1}{q-2}$ for $q > 2$.*

Proof. By [79], we have $H_q M(q,m,n,d,r) > A_{\mathrm{R}}(q,m,n,d,r)$ for $n \geq r \geq d$, as long as $q > 2$, $n < m$, or $d \neq m-1$. Hence

$$H_q P_{\mathrm{R,MRD}}(u) > \frac{1}{N_{\mathrm{R}}(u)} \sum_{w=d}^{n} A_{\mathrm{R}}(q,m,n,d,w) \sum_{s=0}^{t} J_{\mathrm{R}}(u,s,w) \geq P_{\mathrm{R}}(\mathbf{C}, u).$$

□

In many applications, the probability that the received matrix is at distance u from the sent codeword decreases rapidly with u, and hence the overall DEP can be approximated by $P_{\mathrm{R}}(\mathbf{C}, d-t)$. We consider this special case next.

Proposition 4.26. *Assume a codeword $\mathbf{C} \in \mathcal{C}$, a code in $\mathrm{GF}(q)^{m\times n}$ with minimum rank distance d, is sent over a rank symmetric channel and the channel output is distance $u = d - t$ from $\mathbf{C}$, the DEP of a bounded rank distance decoder is given by*

$$P_{\mathrm{R}}(\mathbf{C}, d-t) = q^{t(d-t)} \frac{\begin{bmatrix} d \\ t \end{bmatrix}}{\begin{bmatrix} n \\ d-t \end{bmatrix} \alpha(m, d-t)} A_d(\mathbf{C}). \tag{4.24}$$

In particular, the DEP of an MRD code satisfies $P_{\mathrm{R,MRD}}(d-t) > K_q q^{-t(m+n-t)}$ when $d = 2t+1$.

Proof. First, (4.18) yields $P_{\mathrm{R}}(\mathbf{C}, d-t) = \frac{J_{\mathrm{R}}(d-t,t,d)}{N_{\mathrm{R}}(d-t)} A_d(\mathbf{C})$, which gives (4.24). For an MRD code, we have $A_d(\mathbf{C}) = M(q,m,n,d,d) = \begin{bmatrix} n \\ d \end{bmatrix}(q^m - 1)$. Using the bounds on the Gaussian polynomial in Corollary 2.3, we obtain $P_{\mathrm{R,MRD}}(d-t) > K_q q^{-t(m-n+t)}$ when $d = 2t+1$. □

When $u = d-t$, Proposition 4.26 above not only provides the DEP for any code, but also shows that the upper bound on the DEP for MRD codes in (4.20) is **tight** up to a scalar.

4.5.2 Generalization to equal row and equal column space channels

We now consider channels where the errors with the same row (or column) space are equiprobable.

Definition 4.27. *A channel on* $\mathrm{GF}(q)^{m\times n}$ *is equal row (column) space if the error is additive and the error patterns with the same row (column) space are equiprobable.*

Equal row and column space channels are interesting in several respects. First, rank symmetric channels are both equal row and equal column space channels, hence the following results will be generalizations of those in Section 4.5.1. Also, considering these more general channels does not dramatically affect the tightness of the bounds. Finally, it is remarkable that these channels may also be used to model other applications of rank metric codes. Rank metric codes can be used for the correction of two-dimension errors [14, 20] (i.e., errors confined to a certain number of rows and columns) in storage equipments. Hence, our model encompasses the case of two-dimensional errors, where some rows or columns are more likely to be in error than others.

Note that using a code $\mathcal{C}$ over an equal row space channel on $\mathrm{GF}(q)^{m\times n}$ is equivalent to using its transpose code over a column space channel on $\mathrm{GF}(q)^{n\times m}$. We study equal row space channels first. In this case, it is clear that the DEP depends not only on the rank u of the error, but also on its row space $U \in E_u(q,n)$. We hence derive a bound on $P_{\mathrm{R}}(\mathbf{C}, U)$ for all codes, and we also obtain the exact value of $P_{\mathrm{R}}(U)$ for linear MRD codes when $n \leq m$, thus generalizing the results in Proposition 4.24 for equal row space channels.

Proposition 4.28. *Assuming a codeword* $\mathbf{C} \in \mathcal{C}$*, a code in* $\mathrm{GF}(q)^{m\times n}$ *with minimum rank distance* d*, is sent over an equal row space channel and the channel error has row space* $U \in E_u(q,n)$*, the DEP of a bounded rank distance decoder satisfies*

$$P_{\mathrm{R}}(\mathbf{C}, U) \leq \frac{1}{N_{\mathrm{R}}(u)} \sum_{w=d}^{n} \begin{bmatrix} n \\ w \end{bmatrix} \alpha(m, w-d+1) \sum_{s=0}^{t} J_{\mathrm{R}}(u, s, w). \tag{4.25}$$

Furthermore, if $n \leq m$ and $\mathcal{C}$ is a linear MRD code, then the DEP is given by

$$P_{\mathrm{R,MRD}}(U) = \frac{1}{N_{\mathrm{R}}(u)} \sum_{w=d}^{n} M(q, m, n, d, w) \sum_{s=0}^{t} J_{\mathrm{R}}(u, s, w). \tag{4.26}$$

The proof of Proposition 4.28 is given in Appendix 7.3.4. A similar upper bound can be obtained for an equal column space channel.

Proposition 4.29. *Assuming a codeword $\mathbf{C} \in \mathcal{C}$, a code in $\mathrm{GF}(q)^{m \times n}$ with minimum rank distance d, is sent over an equal column space channel and the channel error has column space $U \in E_u(q, m)$, the DEP of a bounded rank distance decoder satisfies*

$$P_{\mathrm{R}}(\mathbf{C}, U) \leq \frac{1}{N_{\mathrm{R}}(u)} \sum_{w=d}^{n} \begin{bmatrix} m \\ w \end{bmatrix} \alpha(n, w - d + 1) \sum_{s=0}^{t} J_{\mathrm{R}}(u, s, w). \tag{4.27}$$

Furthermore, if $n \geq m$ and $\mathcal{C}$ is the transpose code of a linear MRD code, then the DEP is given by

$$P_{\mathrm{R,MRD}}(U) = \frac{1}{N_{\mathrm{R}}(u)} \sum_{w=d}^{m} M(q, n, m, d, w) \sum_{s=0}^{t} J_{\mathrm{R}}(u, s, w). \tag{4.28}$$

The proof of Proposition 4.29 is similar to that of Proposition 4.28 and is hence omitted.

Chapter 5

On Constant-Dimension Codes and Subspace Codes

5.1 Introduction

Due to its vector-space preserving property, random linear network coding [4, 6] can be interpreted as transmitting subspaces over an operator channel [9]. Error control for random linear network coding can hence be modeled as a coding theory problem, where codewords are subspaces and the distance is either the subspace distance [9] or, on adversarial channels, the injection metric [11]. Codes in the projective space, referred to as subspace codes henceforth, and in particular codes in the Grassmannian, referred to as constant-dimension codes (CDCs) henceforth, were proposed for that effect. Using CDCs is advantageous for two main reasons. First, the decoding protocol is simplified, as the receiver only needs a given number of dimensions to perform the decoding. Also, CDCs are related to rank metric codes [12–14] through the lifting operation [10]. In particular, liftings of Gabidulin

codes [9] are asymptotically optimal CDCs and have a polynomial-time bounded subspace distance decoding algorithm [9]. However, although designing a bounded injection distance decoder for a CDC is straightforward, no efficient algorithm is known so far. Although CDCs seem more practical, they cannot offer the same rate as general subspace codes. Comparing the performance of CDCs to that of general subspace codes is hence crucial for code design.

Construction of CDCs has received growing attention in the literature recently. In [9], a Singleton bound for CDCs and a family of codes were proposed, which are nearly Singleton-bound-achieving and referred to as KK codes henceforth. A recursive construction of CDCs was proposed in [70], and we call these codes Skachek codes; Skachek codes have larger cardinalities than KK codes in some scenarios, and reduce to KK codes otherwise. Further constructions for small parameter values were given in [74] and the Johnson bound for CDCs was derived in [66]. Despite these previous works, the maximum cardinality of a CDC with a given minimum distance and how to construct optimal CDCs remain open problems.

Although the packing properties of CDCs were investigated in [9], the covering properties of CDCs have received little attention in the literature. Covering properties are significant for error control codes, and the covering radius is a basic geometric parameter of a code [37]. For instance, the covering radius can be viewed as a measure of performance: if the minimum distance decoding is used, then the covering radius is the maximum weight of a correctable error vector [35]; if the code is used for data compression, then the covering radius is a measure of the maximum distortion [35]. The covering radius is also crucial for code design: if the covering radius is no less than the minimum distance, then there exists a supercode with same minimum distance and higher cardinality.

This chapter has three main contributions. The first contribution is a study of the packing and covering properties of CDCs. First, we introduce a new class of CDCs, referred to as augmented KK codes, based on KK codes. The cardinalities of our augmented KK codes are no less than those for KK and Skachek codes. Furthermore, we propose an efficient decoding algorithm for our augmented KK codes using the bounded subspace distance decoding algorithm in [9]. Our decoding algorithm decodes more errors than a bounded subspace distance decoder. Second, we investigate the covering properties of CDCs. We first derive some key geometric results for Grassmannians. Using these results, we derive upper and lower bounds on the minimum cardinality of a CDC with a given covering radius. Since these bounds are asymptotically tight, we also determine the asymptotic behavior of the minimum cardinality of a CDC with a given covering radius. Although liftings of rank metric codes can be used to construct packing CDCs that are optimal up to a scalar, we show that all liftings of rank metric codes have the greatest covering radius possible and hence they are not optimal packing CDCs. We finally construct good covering CDCs by permuting liftings of rank metric codes.

The second contribution is a study of the properties of subspace codes using either the subspace or the injection metric. We investigate the packing and covering properties of subspace codes. We first determine some fundamental geometric properties of the projective space. Using these results, we derive bounds on the cardinalities of packing subspace codes, and we determine the asymptotic rate of optimal packing subspace codes for both metrics. We thus show that optimal packing CDCs are optimal packing subspace codes up to a scalar for both metrics if and only if their dimension is half of their length. Hence, CDCs can be used for correcting errors inherent to the network or caused by an adversary with only a limited rate

loss. We also study the covering properties of subspace codes. We determine the asymptotic behavior of optimal covering codes in both metrics. We thus show that optimal covering CDCs can be used to construct asymptotically optimal covering subspace codes only for the injection metric. These results not only indicate the significance of CDCs, but also illustrate the similarities and differences between the two metrics.

The third contribution is the study of the DEP of constant-dimension codes using a bounded subspace distance or a bounded injection distance decoder over a symmetric operator channel. We first determine some fundamental geometric properties of the subspace and the injection metrics. Using these properties, we derive asymptotically tight upper bounds on the DEP of any constant-dimension code obtained by lifting a rank metric code using either a bounded subspace distance or a bounded injection distance decoder.

The rest of the chapter is organized as follows. In Section 5.2, we present our augmented KK codes and a decoding algorithm for these codes. In Section 5.3, we investigate the covering properties of CDCs. In Section 5.4, we investigate the packing and covering properties of subspace codes using the subspace metric. In Section 5.5, we study the packing and covering properties of subspace codes using the injection metric. Section 5.6 investigates the DEP of CDCs.

5.2 Construction of CDCs

In this section, we construct a new class of CDCs which contain KK codes as proper subsets. Thus we call them augmented KK codes. We will show that the cardinalities of our augmented KK codes are always greater than those of KK codes, and

that in most cases the cardinalities of our augmented KK code are greater than those of Skachek codes. Furthermore, we propose a low-complexity decoder for our augmented KK codes based on the bounded subspace distance decoder in [9]. Since dual CDCs preserve the distance, we assume $r \leq \frac{n}{2}$ without loss of generality.

5.2.1 Augmented KK codes

Our augmented KK code is so named because it has a layered structure and the first layer is simply a KK code. We denote a KK code in $E_r(q,n)$ with minimum injection distance d ($d \leq r$ by definition) and cardinality $q^{(n-r)(r-d+1)}$ as $\mathcal{E}^0$. For $1 \leq k \leq \left\lfloor \frac{r}{d} \right\rfloor$, we first define two MRD codes $\mathcal{C}^k$ and $\mathcal{D}^k$, and then construct $\mathcal{E}^k$ based on $\mathcal{C}^k$ and $\mathcal{D}^k$. $\mathcal{C}^k$ is an MRD code in $\mathrm{GF}(q)^{(r-kd)\times kd}$ with minimum distance d for $k \leq \left\lfloor \frac{r}{d} \right\rfloor - 1$ ($\left\lfloor \frac{n-r}{d} \right\rfloor \geq \left\lfloor \frac{r}{d} \right\rfloor$) and $\mathcal{C}^{\left\lfloor \frac{r}{d} \right\rfloor} = \{\mathbf{0}\} \subseteq \mathrm{GF}(q)^{\left(r-\left\lfloor \frac{r}{d} \right\rfloor d\right)\times \left\lfloor \frac{r}{d} \right\rfloor d}$; $\mathcal{D}^k$ is an MRD code in $\mathrm{GF}(q)^{r\times(n-r-kd)}$ with minimum distance d for $k \leq \left\lfloor \frac{n-r}{d} \right\rfloor - 1$ and $\mathcal{D}^{\left\lfloor \frac{n-r}{d} \right\rfloor} = \{\mathbf{0}\} \subseteq \mathrm{GF}(q)^{r\times\left(n-r-\left\lfloor \frac{n-r}{d} \right\rfloor d\right)}$. For $1 \leq k < \left\lfloor \frac{r}{d} \right\rfloor$, the block lengths of $\mathcal{C}^k$ and $\mathcal{D}^k$ are at least d, and hence existence of MRD codes with the parameters mentioned above is trivial. For $1 \leq k \leq \left\lfloor \frac{r}{d} \right\rfloor$, $I(\mathcal{C}^k)$ and $I(\mathcal{D}^k)$ are either trivial codes or KK codes with minimum injection distance d in $E_{r-kd}(q,r)$ and $E_r(q,n-kd)$, respectively. For $1 \leq k \leq \left\lfloor \frac{r}{d} \right\rfloor$, $\mathbf{C}_i^k \in \mathcal{C}^k$, and $\mathbf{D}_j^k \in \mathcal{D}^k$, we define $E_{i,j}^k \in E_r(q,n)$ as the row space of $\left(\begin{array}{c|c|c} \mathbf{I}_{r-kd} & \mathbf{C}_i^k & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} & \mathbf{I}_{kd} \end{array}\right) \mathbf{D}_j^k$ and $\mathcal{E}^k = \{E_{i,j}^k\}_{i,j=0}^{|\mathcal{C}^k|-1,|\mathcal{D}^k|-1}$. Our augmented KK code is simply $\mathcal{E} = \bigcup_{k=0}^{\left\lfloor \frac{r}{d} \right\rfloor} \mathcal{E}^k$. In order to determine its minimum distance, we first establish two technical results. First, for any two matrices $\mathbf{A} \in \mathrm{GF}(q)^{a\times n}$, $\mathbf{B} \in \mathrm{GF}(q)^{b\times n}$, we

can easily show that

$$d_{\mathrm{S}}(R(\mathbf{A}), R(\mathbf{B})) = 2\mathrm{rk}(\mathbf{A}^T|\mathbf{B}^T) - \mathrm{rk}(\mathbf{A}) - \mathrm{rk}(\mathbf{B}) \geq |\mathrm{rk}(\mathbf{A}) - \mathrm{rk}(\mathbf{B})|, \quad (5.1)$$

$$d_{\mathrm{I}}(R(\mathbf{A}), R(\mathbf{B})) = \mathrm{rk}(\mathbf{A}^T|\mathbf{B}^T) - \min\{\mathrm{rk}(\mathbf{A}), \mathrm{rk}(\mathbf{B})\} \geq |\mathrm{rk}(\mathbf{A}) - \mathrm{rk}(\mathbf{B})|. \quad (5.2)$$

Second, we show that truncating the generator matrices of two subspaces in $E(q, n)$ can only reduce the (subspace or injection) distance between them.

Lemma 5.1. *Suppose* $0 \leq n_1 \leq n$. *Let* $\mathbf{A} = (\mathbf{A}_1|\mathbf{A}_2) \in \mathrm{GF}(q)^{a\times n}$, $\mathbf{B} = (\mathbf{B}_1|\mathbf{B}_2) \in \mathrm{GF}(q)^{b\times n}$, *where* $\mathbf{A}_1 \in \mathrm{GF}(q)^{a\times n_1}$ *and* $\mathbf{B}_1 \in \mathrm{GF}(q)^{b\times n_1}$. *Then for* $i = 1$ *and* 2, $d_{\mathrm{S}}(R(\mathbf{A}_i), R(\mathbf{B}_i)) \leq d_{\mathrm{S}}(R(\mathbf{A}), R(\mathbf{B}))$ *and* $d_{\mathrm{I}}(R(\mathbf{A}_i), R(\mathbf{B}_i)) \leq d_{\mathrm{I}}(R(\mathbf{A}), R(\mathbf{B}))$.

Proof. It suffices to prove it for $i = 1$ and $n_1 = n - 1$. We need to distinguish two cases, depending on $\mathrm{rk}(\mathbf{A}_1^T|\mathbf{B}_1^T)$. First, if $\mathrm{rk}(\mathbf{A}_1^T|\mathbf{B}_1^T) = \mathrm{rk}(\mathbf{A}^T|\mathbf{B}^T)$, then it is easily shown that $\mathrm{rk}(\mathbf{A}_1) = \mathrm{rk}(\mathbf{A})$ and $\mathrm{rk}(\mathbf{B}_1) = \mathrm{rk}(\mathbf{B})$, and hence $d_{\mathrm{S}}(R(\mathbf{A}_1), R(\mathbf{B}_1)) = d_{\mathrm{S}}(R(\mathbf{A}), R(\mathbf{B}))$ and $d_{\mathrm{I}}(R(\mathbf{A}_1), R(\mathbf{B}_1)) = d_{\mathrm{I}}(R(\mathbf{A}), R(\mathbf{B}))$ by (5.1) and (5.2), respectively. Second, if $\mathrm{rk}(\mathbf{A}_1^T|\mathbf{B}_1^T) = \mathrm{rk}(\mathbf{A}^T|\mathbf{B}^T) - 1$, then $d_{\mathrm{S}}(R(\mathbf{A}_1), R(\mathbf{B}_1)) = 2\mathrm{rk}(\mathbf{A}^T|\mathbf{B}^T) - 2 - \mathrm{rk}(\mathbf{A}_1) - \mathrm{rk}(\mathbf{B}_1) \leq d_{\mathrm{S}}(R(\mathbf{A}), R(\mathbf{B}))$ by (5.1) and $d_{\mathrm{I}}(R(\mathbf{A}_1), R(\mathbf{B}_1)) = \mathrm{rk}(\mathbf{A}^T|\mathbf{B}^T) - 1 - \min\{\mathrm{rk}(\mathbf{A}_1), \mathrm{rk}(\mathbf{B}_1)\} \leq d_{\mathrm{I}}(R(\mathbf{A}), R(\mathbf{B}))$ by (5.2). □

Proposition 5.2. $\mathcal{E}$ *has minimum injection distance* d.

Proof. We show that any two codewords $E_{i,j}^k, E_{a,b}^c \in \mathcal{E}$ are at injection distance at least d using Lemma 5.1. When $c \neq k$, let us assume $c < k$ without loss of generality, and then $d_{\mathrm{I}}(E_{i,j}^k, E_{a,b}^c) \geq d_{\mathrm{I}}(R(\mathbf{I}_{r-kd}|\mathbf{0}), R(\mathbf{I}_{r-cd})) = (k-c)d \geq d$. When $c = k$ and $a \neq i$, then $d_{\mathrm{I}}(E_{i,j}^k, E_{a,b}^k) \geq d_{\mathrm{I}}(I(\mathbf{C}_i^k), I(\mathbf{C}_a^k)) \geq d$. When $c = k$, $a = i$, and $b \neq j$, then $d_{\mathrm{I}}(E_{i,j}^k, E_{i,b}^k) \geq d_{\mathrm{I}}(I(\mathbf{D}_j^k), I(\mathbf{D}_b^k)) \geq d$. □

Let us first determine the cardinality of our augmented KK codes. By construction, $\mathcal{E}$ has cardinality $|\mathcal{E}| = q^{(n-r)(r-d+1)} + \sum_{k=1}^{\lfloor \frac{r}{d} \rfloor} |\mathcal{C}^k||\mathcal{D}^k|$, where $|\mathcal{C}^{\lfloor \frac{r}{d} \rfloor}| = 1$ and

$|\mathcal{C}^k| = \min\{q^{(r-kd)(kd-d+1)}, q^{kd(r-kd-d+1)}\}$ for $1 \leq k \leq \left\lfloor \frac{r}{d} \right\rfloor - 1$ and $|\mathcal{D}^{\left\lfloor \frac{n-r}{d} \right\rfloor}| = 1$ and $|\mathcal{D}^k| = \min\{q^{r(n-r-kd-d+1)}, q^{(n-r-kd)(r-d+1)}\}$ for $1 \leq k \leq \left\lfloor \frac{n-r}{d} \right\rfloor - 1$.

Let us compare the cardinality of our augmented KK codes to those of KK and Skachek codes. Note that all three codes are CDCs with minimum injection distance d in $E_r(q,n)$. First, it is easily shown that our augmented KK codes properly contain KK codes for all parameter values. This is a clear distinction from Skachek codes with cardinality $L(q,n,r,d)$, which by (4.5) reduce to KK codes for $3r > n$. In order to compare our codes to Skachek codes when $3r \leq n$, we first remark that (4.5) and Corollary 2.3 lead to $L(q,n,r,d) - q^{(n-r)(r-d+1)} < K_q^{-1} q^{(n-2r)(r-d+1)}$. Also, we have $|\mathcal{E}| \geq q^{(n-r)(r-d+1)} + |\mathcal{C}^1||\mathcal{D}^1| \geq q^{(n-r)(r-d+1)} + q^{(n-r-d)(r-d+1)}$. Hence $|\mathcal{E}| - q^{(n-r)(r-d+1)} > K_q q^{(r-d)(r-d+1)}(L(q,n,r,d) - q^{(n-r)(r-d+1)})$, and our augmented KK codes have a greater cardinality than Skachek codes when $d < r$. We emphasize that for CDCs of dimension r, their minimum injection distance d satisfies $d \leq r$. A Skachek code is constructed in multiple steps, and in the i-th step ($i \geq 1$), subspaces that correspond to a KK code in $E_r(q, n-ir)$ are added to the code. When $d = r$, $\mathcal{E}$ is actually the code obtained after the first step.

As an illustration of the improvement obtained by using augmented KK codes, the cardinalities of KK codes, Skachek codes, and augmented KK codes are displayed in Table 5.2.1 for $q = 2$, $n = 10$, and $2 \leq r \leq 5$. For the parameters considered in Table 5.2.1, augmented KK codes have the greatest cardinality for all but one case, when $d = r = 2$.

5.2.2 Decoding of augmented KK codes

Let $\mathbf{A} = (\mathbf{A}_0|\mathbf{A}_3) \in \mathrm{GF}(q)^{a\times n}$ be the received matrix, where $\mathbf{A}_0 \in \mathrm{GF}(q)^{a\times r}$ and $\mathbf{A}_3 \in \mathrm{GF}(q)^{a\times(n-r)}$. We propose a decoding algorithm that either produces the

r	d	KK	Skachek	Augmented KK
2	2	256	340	320
3	2	16384	16640	17408
	3	128	144	144
4	2	262144	262144	278544
	3	4096	4096	4112
	4	64	64	65
5	2	1048576	1048576	1056769
	3	32768	32768	32769
	4	1024	1024	1025
	5	32	32	33

Table 5.1: Cardinalities of KK codes, Skachek codes, and augmented KK codes in $E_r(2, 10)$ for $2 \leq r \leq 5$.

unique codeword in $\mathcal{E}$ closest to $R(\mathbf{A})$ in the subspace metric or returns a failure. Suppose the minimum subspace distance of our augmented KK codes is denoted as $2d$, a bounded distance decoder would find the codeword that is closest to $R(\mathbf{A})$ up to subspace distance $d-1$. Our decoding algorithm always returns the correct codeword if it is at subspace distance at most $d-1$ from the received subspace, thus correcting more errors than a bounded subspace distance decoder.

Given the layered structure of $\mathcal{E}$, our decoding algorithm for $\mathcal{E}$ is based on a decoding algorithm for $\mathcal{E}^k$, shown below in Algorithm 5.3, for any k. We denote the codewords in $\mathcal{E}^0$ as $E^0_{0,j}$ for $0 \leq j \leq |\mathcal{E}^0| - 1$.

Algorithm 5.3. EBDD$(k, \mathbf{A})$.

Input: k *and* $\mathbf{A} = (\mathbf{A}_1|\mathbf{A}_2|\mathbf{A}_3) \in \mathrm{GF}(q)^{a\times n}$, $\mathbf{A}_1 \in \mathrm{GF}(q)^{a\times(r-kd)}$, $\mathbf{A}_2 \in \mathrm{GF}(q)^{a\times kd}$, $\mathbf{A}_3 \in \mathrm{GF}(q)^{a\times(n-r)}$.

Output: $(E^k_{i,j}, d_k, f_k)$.

5.3.1 If $k = 0$, *use the decoder for* $\mathcal{E}^0$ *to obtain* $E^0_{0,j}$, *calculate* $d_k = d_{\mathrm{S}}(R(\mathbf{A}), E^0_{0,j})$,

and return $(E^0_{0,j}, d_k, 0)$. *If the decoder returns a failure, return* $(I(\mathbf{0}), d, 0)$.

5.3.2 Use the decoder of $I(\mathcal{C}^k)$ *on* $(\mathbf{A}_1|\mathbf{A}_2)$ *to obtain* $\mathbf{C}^k_i$. *If the decoder returns a failure, set* $\mathbf{C}^k_i = \mathbf{0}$, $\mathbf{D}^k_j = \mathbf{0}$ *and return* $(E^k_{i,j}, d, 0)$.

5.3.3 Use the decoder of $I(\mathcal{D}^k)$ *on* $(\mathbf{A}_1|\mathbf{A}_3)$ *to obtain* $\mathbf{D}^k_j$. *If the decoder returns a failure, set* $\mathbf{D}^k_j = \mathbf{0}$ *and return* $(E^k_{i,j}, d, 0)$.

5.3.4 Calculate $d_k = d_{\mathrm{S}}(R(\mathbf{A}), E^k_{i,j})$ *and*

$$f_k = 2d - \max\{d_{\mathrm{S}}(R(\mathbf{A}_1|\mathbf{A}_2), I(\mathbf{C}^k_i)), d_{\mathrm{S}}(R(\mathbf{A}_1|\mathbf{A}_3), I(\mathbf{D}^k_j))\}$$

and return $(E^k_{i,j}, d_k, f_k)$.

Algorithm 5.3 is based on the bounded distance decoder proposed in [9]. When $k = 0$, $\mathcal{E}^0$ is simply a KK code, and the algorithm in [9] is used directly; when $k \geq 1$, given the structure of $\mathcal{E}^k$, two decoding attempts are made based on $(\mathbf{A}_1|\mathbf{A}_2)$ and $(\mathbf{A}_1|\mathbf{A}_3)$, and both are based on the decoding algorithm in [9].

We remark that Algorithm 5.3 always return $(E^k_{i,j}, d_k, f_k)$. If a unique nearest codeword in $\mathcal{E}^k$ at distance no more than $d-1$ from $R(\mathbf{A})$ exists, then by Lemma 5.1 Steps 5.3.2 and 5.3.3 succeed and Algorithm 5.3 returns the unique nearest codeword in $E^k_{i,j}$. However, when such unique codeword in $\mathcal{E}^k$ at distance no more than $d-1$ does not exist, the return value f_k can be used to find the unique nearest codeword because f_k is a lower bound on the distance from the received subspace to any other codeword in $\mathcal{E}^k$. Also, when $f_k = 0$, Algorithm 5.5 below always returns a failure. Thus, we call Algorithm 5.3 an enhanced bounded distance decoder.

Lemma 5.4. *Suppose the output of* EBDD$(k, \mathbf{A})$ *is* $(E^k_{i,j}, d_k, f_k)$, *then* $d_{\mathrm{S}}(R(\mathbf{A}), E^k_{u,v}) \geq f_k$ *for any* $E^k_{u,v} \in \mathcal{E}^k$ *provided* $(u, v) \neq (i, j)$.

Proof. The case $f_k = 0$ is trivial, and it suffices to consider $f_k = \min\{2d - d_{\mathrm{S}}(R(\mathbf{A}_1|\mathbf{A}_2), I(\mathbf{C}_i^k)), 2d - d_{\mathrm{S}}(R(\mathbf{A}_1|\mathbf{A}_3), I(\mathbf{D}_j^k))\}$. When $u \neq i$, Lemma 5.1 yields

$$\begin{aligned} d_{\mathrm{S}}(R(\mathbf{A}), E_{u,v}^k) &\geq d_{\mathrm{S}}(R(\mathbf{A}_1|\mathbf{A}_2), I(\mathbf{C}_u^k)) \\ &\geq d_{\mathrm{S}}(I(\mathbf{C}_i^k), I(\mathbf{C}_u^k)) - d_{\mathrm{S}}(R(\mathbf{A}_1|\mathbf{A}_2), I(\mathbf{C}_i^k)) \\ &\geq 2d - d_{\mathrm{S}}(R(\mathbf{A}_1|\mathbf{A}_2), I(\mathbf{C}_i^k)) \geq f_k. \end{aligned}$$

Similarly, when $v \neq j$, we obtain $d_{\mathrm{S}}(R(\mathbf{A}), E_{u,v}^k) \geq 2d - d_{\mathrm{S}}(R(\mathbf{A}_1|\mathbf{A}_3), I(\mathbf{D}_j^k)) \geq f_k$. □

The algorithm for $\mathcal{E}$ thus follows.

Algorithm 5.5. *Decoder for $\mathcal{E}$.*

Input: $\mathbf{A} = (\mathbf{A}_0|\mathbf{A}_3) \in \mathrm{GF}(q)^{a\times n}$, $\mathbf{A}_0 \in \mathrm{GF}(q)^{a\times r}$, $\mathbf{A}_3 \in \mathrm{GF}(q)^{a\times(n-r)}$.

Output: Either a failure or the unique nearest codeword in $\mathcal{E}$ from $R(\mathbf{A})$.

5.5.1 If $\mathrm{rk}(\mathbf{A}) < r - d + 1$, *return a failure.*

5.5.2 Calculate $r - \mathrm{rk}(\mathbf{A}_0) = ld + m$ *where* $0 \leq l \leq \left\lfloor \frac{r}{d} \right\rfloor$ *and* $0 \leq m < d$.

5.5.3 Call $\mathrm{EBDD}(l, \mathbf{A})$ *to obtain* $(E_{i,j}^l, d_l, f_l)$. *If* $d_l \leq d - 1$, *return* $E_{i,j}^l$.

5.5.4 If $m = 0$, *return a failure. Otherwise, call* $\mathrm{EBDD}(l{+}1, \mathbf{A})$ *to obtain* $(E_{s,t}^{l+1}, d_{l+1}, f_{l+1})$. *If* $d_{l+1} \leq d - 1$, *return* $E_{s,t}^{l+1}$.

5.5.5 If $d_l < \min\{d + m, f_l, d_{l+1}, f_{l+1}, 2d - m\}$, *return* $E_{i,j}^l$. *If* $d_{l+1} < \min\{d + m, d_l, f_l, f_{l+1}, 2d - m\}$, *return* $E_{s,t}^{l+1}$.

5.5.6 Return a failure.

Proposition 5.6. *If the received subspace is at subspace distance at most $d-1$ from a codeword in $\mathcal{E}$, then Algorithm 5.5 returns this codeword. Otherwise, Algorithm 5.5 returns either a failure or the unique codeword closest to the received subspace in the subspace metric.*

Proof. We first show that Algorithm 5.5 returns the unique nearest codeword in $\mathcal{E}$ to the received subspace if it is at subspace distance at most $d-1$. For all $1 \leq k \leq \left\lfloor \frac{r}{d} \right\rfloor$ and $E_{u,v}^k \in \mathcal{E}^k$, Lemma 5.1 and (5.1) yield

$$d_{\mathrm{S}}(R(\mathbf{A}), E_{u,v}^k) \geq d_{\mathrm{S}}(R(\mathbf{A}_0), I(\mathbf{C}_u^k)) \geq |r - kd - \mathrm{rk}(\mathbf{A}_0)| = |(l-k)d + m|. \quad (5.3)$$

Similarly (5.1) yields $d_{\mathrm{S}}(R(\mathbf{A}), E_{0,v}^0) \geq ld + m$ for any v. Hence $d_{\mathrm{S}}(R(\mathbf{A}), \mathcal{E}^k) \geq d$ for $k \leq l-1$ or $k \geq l+2$. Therefore, the unique nearest codeword is either in $\mathcal{E}^l$ or $\mathcal{E}^{l+1}$ and applying Algorithm 5.3 for $\mathcal{E}^l$ and $\mathcal{E}^{l+1}$ always returns the nearest codeword.

We now show that when the distance from the received subspace to the code is at least d, Algorithm 5.5 either produces the unique nearest codeword or returns a failure. First, by (5.3), $d_{\mathrm{S}}(R(\mathbf{A}), \mathcal{E}^{l-1}) = d+m$ and $d_{\mathrm{S}}(R(\mathbf{A}), \mathcal{E}^{l+2}) = 2d-m$, while $d_{\mathrm{S}}(R(\mathbf{A}), \mathcal{E}^k) \geq 2d$ for $k \leq l-2$ or $k \geq l+3$. Also, by Lemma 5.4, $d_{\mathrm{S}}(R(\mathbf{A}), E_{u,v}^l) \geq f_l$ for all $(u,v) \neq (i,j)$ and $d_{\mathrm{S}}(R(\mathbf{A}), \mathcal{E}^{l+1}) \geq \min\{d_{l+1}, f_{l+1}\}$. Therefore, if $d_l < \min\{d+m, f_l, d_{l+1}, f_{l+1}, 2d-m\}$, then $E_{i,j}^l$ is the unique codeword closest to $R(\mathbf{A})$. Similarly, if $d_{l+1} < \min\{d+m, d_l, f_l, f_{l+1}, 2d-m\}$, then $E_{s,t}^{l+1}$ is the unique codeword closest to $R(\mathbf{A})$. □

We note that when $\mathrm{rk}(\mathbf{A}) < r - d + 1$, by (5.1) Steps 5.3.2 and 5.3.3 would both fail, and Algorithm 5.5 will return a failure. We also justify why Algorithm 5.5 returns a failure if $d_l \geq d$ and $m = 0$ in Step 5.5.3. Suppose $d_l \geq d$ and $m = 0$ and we apply Algorithm 5.3 for $\mathcal{E}^{l+1}$. Then we have $d_l \geq d + m$ and by (5.3)

$d_{l+1} \geq |d - m| = d + m$. Therefore, neither inequality in Step 5.5.5 is satisfied and the decoder returns a failure.

By Proposition 5.6, Algorithm 5.5 decodes beyond the half distance. However, the decoding radius of Algorithm 5.5 is at most $d + \left\lfloor \frac{d}{2} \right\rfloor$ due to the terms $d+m$ and $2d-m$ in the inequalities in Step 5.5.5. We emphasize that this is just an upper bound, and its tightness is unknown. Suppose $r - \mathrm{rk}(\mathbf{A}_0) = ld + m$, when Algorithm 5.5 decodes beyond half distance, it is necessary that f_l and f_{l+1} be both nonzero in Step 5.5.5. This implies that the row space of $(\mathbf{A}_1|\mathbf{A}_2)$ is at subspace distance no more than $d-1$ from $I(\mathcal{C}^l)$ and $I(\mathcal{C}^{l+1})$ and that the row spaces of $(\mathbf{A}_1|\mathbf{A}_3)$ are at subspace distance no more than $d-1$ from $I(\mathcal{D}^l)$ and $I(\mathcal{D}^{l+1})$.

We note that the inequalities in Step 5.5.5 are strict in order to ensure that the output of the decoder is the **unique** nearest codeword from the received subspace. However, if one of the nearest codewords is an acceptable outcome, then equality can be included in the inequalities in Step 5.5.5.

Our decoding algorithm can be readily simplified in order to obtain a bounded subspace distance decoder, by removing Step 5.5.5. We emphasize that the general decoding algorithm has the same order of complexity as this simplified bounded subspace distance decoding algorithm.

Finally, we note that the decoding algorithms and discussions above consider the subspace metric. It is also remarkable that our decoder remains the same if the injection metric is used instead. We formalize this by the following proposition.

Proposition 5.7. *If the received subspace is at injection distance at most $d-1$ from a codeword in $\mathcal{E}$, then Algorithm 5.5 returns this codeword. Otherwise, Algorithm 5.5 returns either a failure or the unique codeword closest to the received subspace in the*

injection metric.

The proof of Proposition 5.7 is based on the observation that a codeword in a CDC is closest to the received subspace in the subspace metric if and only if the codeword is closest to the received subspace in the injection metric by (4.1), and is hence omitted.

The complexity of the bounded subspace distance decoder in [9] for a KK code in $E(q,n)$ is on the order of $O(n^2)$ operations over $\mathrm{GF}(q)^{n-r}$ for $r \leq \frac{n}{2}$, which is hence the complexity of decoding $\mathcal{E}^0$. This algorithm can be easily generalized to include the case where $r > \frac{n}{2}$, and we obtain a complexity on the order of $O(n^2)$ operations over $\mathrm{GF}(q^{\max\{r,n-r\}})$. Thus the complexity of decoding $I(\mathcal{C}^k)$ and $I(\mathcal{D}^k)$ for $k \geq 1$ is on the order of $O(r^2)$ operations over $\mathrm{GF}(q^{\max\{kd,r-kd\}})$ and $O((n-kd)^2)$ operations over $\mathrm{GF}(q^{\max\{r,n-kd-r\}})$, respectively. The complexity of the decoding algorithm for $\mathcal{E}^k$ is on the order of the maximum of these two quantities. It is easily shown that the complexity is maximized for $k = 0$, that is, our decoding algorithm has the same order of complexity as the algorithm for the KK code $\mathcal{E}^0$.

5.3 Covering properties of CDCs

The packing properties of CDCs have been studied in [9,62,66,70,74]; an asymptotic rate of CDCs was defined and determined in [9]. Henceforth in this section, we focus on the covering properties of CDCs instead. We emphasize that we consider only the injection distance in this section. Furthermore, since $d_{\mathrm{I}}(U,V) = d_{\mathrm{I}}(U^{\perp},V^{\perp})$ for all $U,V \in E_r(q,n)$, without loss of generality we assume that $r \leq \left\lfloor \frac{n}{2} \right\rfloor$ in this section.

5.3.1 Properties of balls in the Grassmannian

We first investigate the properties of balls in the Grassmannian $E_r(q,n)$, which will be instrumental in our study of covering properties of CDCs. First, we derive bounds on the volume of balls in $E_r(q,n)$.

Lemma 5.8. *For all q, n, $r \leq \lfloor \frac{n}{2} \rfloor$, and $0 \leq t \leq r$, $q^{t(n-t)} \leq V_{\mathrm{C}}(t) < K_q^{-2} q^{t(n-t)}$.*

Proof. First, we have $V_{\mathrm{C}}(t) \geq N_{\mathrm{C}}(t) \geq q^{t(n-t)}$ by Corollary 2.3. Also, $N_{\mathrm{C}}(d) < K_q^{-1} N_{\mathrm{R}}(q, n-r, r, d)$, and hence $V_{\mathrm{C}}(t) < K_q^{-1} V_{\mathrm{R}}(q, n-r, r, t) < K_q^{-2} q^{t(n-t)}$ as $V_{\mathrm{R}}(q, n-r, r, t) < K_q^{-1} q^{t(n-t)}$ [29, Lemma 9]. □

We now determine the volume of the intersection of two **spheres** of radii u and s respectively and distance d between their centers, which is referred to as the intersection number $J_{\mathrm{C}}(u,s,d)$ of the association scheme [43]. The intersection number is an important parameter of an association scheme.

Lemma 5.9. *For all u, s, and d between 0 and r,*

$$J_{\mathrm{C}}(u,s,d) = \frac{1}{\begin{bmatrix} n \\ r \end{bmatrix} N_{\mathrm{C}}(d)} \sum_{i=0}^{r} \mu_i E_u(i) E_s(i) E_d(i),$$

where $\mu_i = \begin{bmatrix} n \\ i \end{bmatrix} - \begin{bmatrix} n \\ i-1 \end{bmatrix}$ and $E_j(i)$ is a q-Eberlein polynomial [46]:

$$E_j(i) = \sum_{l=0}^{j} (-1)^{j-l} q^{li + \binom{j-l}{2}} \begin{bmatrix} r-l \\ r-j \end{bmatrix} \begin{bmatrix} r-l \\ i \end{bmatrix} \begin{bmatrix} n-r+l-i \\ l \end{bmatrix}.$$

Although Lemma 5.9 is obtained by a direct application of Theorems 3.5 and 3.6 in [41, Chapter II], we present it formally here since it is a fundamental geometric property of the Grassmannian and is very instrumental in our study of CDCs. We also obtain a recursion formula for $J_{\mathrm{C}}(u,s,d)$.

Lemma 5.10. *$J_{\mathrm{C}}(u,s,d)$ satisfies the following recursion: $J_{\mathrm{C}}(0,s,d)=\delta_{s,d}$, $J_{\mathrm{C}}(u,0,d)=\delta_{u,d}$, and*

$$\begin{aligned} c_{u+1}J_{\mathrm{C}}(u+1,s,d) &= b_{s-1}J_{\mathrm{C}}(u,s-1,d)+(a_s-a_u)J_{\mathrm{C}}(u,s,d)+c_{s+1}J_{\mathrm{C}}(u,s+1,d) \\ &\quad -b_{u-1}J_{\mathrm{C}}(u-1,s,d), \end{aligned}$$

where $c_j = J_{\mathrm{C}}(1,j-1,j) = \begin{bmatrix} j \\ 1 \end{bmatrix}^2$, $b_j = J_{\mathrm{C}}(1,j+1,j) = q^{2j+1}\begin{bmatrix} r-j \\ 1 \end{bmatrix}\begin{bmatrix} n-r-j \\ 1 \end{bmatrix}$, and $a_j = J_{\mathrm{C}}(1,j,j) = N_{\mathrm{C}}(1)-b_j-c_j$ for $0 \le j \le r$.

The proof follows directly from [43, Lemma 4.1.7], [43, Theorem 9.3.3], and [43, Chapter 4, (1a)], and hence is omitted. Let $I_{\mathrm{C}}(u,s,d)$ denote the intersection of two **balls** in $E_r(q,n)$ with radii u and s and distance d between their centers. Since $I_{\mathrm{C}}(u,s,d) = \sum_{i=0}^{u}\sum_{j=0}^{s} J_{\mathrm{C}}(i,j,d)$, Lemma 5.9 also leads to an analytical expression for $I_{\mathrm{C}}(u,s,d)$. Proposition 2.22 below shows that $I_{\mathrm{C}}(u,s,d)$ decreases as d increases.

Proposition 5.11. *For all u and s, $I_{\mathrm{C}}(u,s,d)$ is a non-increasing function of d.*

The proof of Proposition 5.11 is given in Appendix 7.4.1. Therefore, the minimum nonzero intersection between two balls with radii u and s is given by $I_{\mathrm{C}}(u,s,u+s) = J_{\mathrm{C}}(u,s,u+s)$ for $u+s \le r$. By Lemma 5.10, it is easily shown that $J_{\mathrm{C}}(u,s,u+s) = \begin{bmatrix} u+s \\ u \end{bmatrix}^2$ for all u and s when $u+s \le r$.

We derive below an upper bound on the union of balls in $E_r(q,n)$ with the same radius.

Lemma 5.12. *The volume of the union of* any *K balls in $E_r(q,n)$ with radius ρ is at most*

$$\begin{aligned} B_{\mathrm{C}}(K,\rho) &= KV_{\mathrm{C}}(\rho)-[K-A_{\mathrm{C}}(q,n,r,r-l+1)]I_{\mathrm{C}}(\rho,\rho,r-l) \\ &\quad -\sum_{a=1}^{l}[A_{\mathrm{C}}(q,n,r,r-a+1)-A_{\mathrm{C}}(q,n,r,r-a+2)]I_{\mathrm{C}}(\rho,\rho,r-a+1), \end{aligned}$$

where $l = \max\{a : K \geq A_{\mathrm{C}}(q, n, r, r-a+1)\}$.

Proof. Let $\{U_i\}_{i=0}^{K-1}$ denote the centers of K balls with radius ρ and let $\mathcal{V}_j = \{U_i\}_{i=0}^{j-1}$ for $1 \leq j \leq K$. Without loss of generality, we assume that the centers are labeled such that $d_{\mathrm{I}}(U_j, \mathcal{V}_j)$ is non-increasing for $j \geq 1$. For $1 \leq a \leq l$ and $A_{\mathrm{C}}(q, n, r, r-a+2) \leq j < A_{\mathrm{C}}(q, n, r, r-a+1)$, we have $d_{\mathrm{I}}(U_j, \mathcal{V}_j) = d_{\mathrm{I}}(\mathcal{V}_{j+1}) \leq r-a+1$. By Proposition 2.22, U_j hence covers at most $V_{\mathrm{C}}(\rho) - I_{\mathrm{C}}(\rho, \rho, r-a+1)$ subspaces that are not previously covered by balls centered at $\mathcal{V}_j$. □

We remark that using any upper bound on $A_{\mathrm{C}}(q, n, r, r-a+1)$ in the proof of Lemma 5.12 gives a valid upper bound on $B_{\mathrm{C}}(K, \rho)$. Hence, although the value of $A_{\mathrm{C}}(q, n, r, r-a+1)$ is unknown in general, the upper bound in (4.5) can be used in Lemma 5.12 in order to obtain an upper bound on the volume of the union on balls in the Grassmannian.

5.3.2 Covering CDCs

The *covering radius* of a CDC $\mathcal{C} \subseteq E_r(q, n)$ is defined as $\rho = \max_{U \in E_r(q,n)} d_{\mathrm{I}}(U, \mathcal{C})$. We denote the minimum cardinality of a CDC in $E_r(q, n)$ with covering radius ρ as $K_{\mathrm{C}}(q, n, r, \rho)$. Since $K_{\mathrm{C}}(q, n, n-r, \rho) = K_{\mathrm{C}}(q, n, r, \rho)$, we assume $r \leq \left\lfloor \frac{n}{2} \right\rfloor$. Also, $K_{\mathrm{C}}(q, n, r, 0) = \begin{bmatrix} n \\ r \end{bmatrix}$ and $K_{\mathrm{C}}(q, n, r, r) = 1$, hence we assume $0 < \rho < r$ henceforth. We first derive lower bounds on $K_{\mathrm{C}}(q, n, r, \rho)$.

Lemma 5.13. *For all* q, n, $r \leq \left\lfloor \frac{n}{2} \right\rfloor$, *and* $0 < \rho < r$, $K_{\mathrm{C}}(q, n, r, \rho) \geq \min\left\{K : B_{\mathrm{C}}(K, \rho) \geq \begin{bmatrix} n \\ r \end{bmatrix}\right\} \geq \frac{\begin{bmatrix} n \\ r \end{bmatrix}}{V_{\mathrm{C}}(\rho)}$.

Proof. Let $\mathcal{C}$ be a CDC with cardinality $K_{\mathrm{C}}(q, n, r, \rho)$ and covering radius ρ. Then the balls around the codewords cover the $\begin{bmatrix} n \\ r \end{bmatrix}$ subspaces in $E_r(q, n)$; however, by

Lemma 5.12, they cannot cover more than $B_{\mathrm{C}}(|\mathcal{C}|, \rho)$ subspaces. Therefore, $\begin{bmatrix} n \\ r \end{bmatrix} \leq B_{\mathrm{C}}(K_{\mathrm{C}}(q, n, r, \rho), \rho)$ and we obtain the first inequality. Since $B_{\mathrm{C}}(K, \rho) \leq KV_{\mathrm{C}}(\rho)$ for all K, we obtain the second inequality. □

The second lower bound in Lemma 5.13 is referred to as the sphere covering bound for CDCs. This bound can also be refined by considering the distance distribution of a covering code.

Proposition 5.14. *For $0 \leq \delta \leq \rho$, let $T_\delta = \min \sum_{i=0}^{r} A_i(\delta)$, where the minimum is taken over all integer sequences $\{A_i(\delta)\}$ which satisfy $A_i(\delta) = 0$ for $0 \leq i \leq \delta - 1$, $1 \leq A_\delta(\delta) \leq N_{\mathrm{C}}(\delta)$, $0 \leq A_i(\delta) \leq N_{\mathrm{C}}(i)$ for $\delta + 1 \leq i \leq r$, and $\sum_{i=0}^{r} A_i(\delta) \sum_{s=0}^{\rho} J_{\mathrm{C}}(l, s, i) \geq N_{\mathrm{C}}(l)$ for $0 \leq l \leq r$. Then $K_{\mathrm{C}}(q, n, r, \rho) \geq \max_{0 \leq \delta \leq \rho} T_\delta$.*

Proof. Let $\mathcal{C}$ be a CDC with covering radius ρ. For any $U \in E_r(q, n)$ at distance δ from $\mathcal{C}$, let $A_i(\delta)$ denote the number of codewords at distance i from U. Then $\sum_{i=0}^{r} A_i(\delta) = |\mathcal{C}|$ and we easily obtain $A_i(\delta) = 0$ for $0 \leq i \leq \delta - 1$, $1 \leq A_\delta(\delta) \leq N_{\mathrm{C}}(\delta)$, and $0 \leq A_i(\delta) \leq N_{\mathrm{C}}(i)$ for $\delta + 1 \leq i \leq r$. Also, for $0 \leq l \leq r$, all the subspaces at distance l from U are covered, hence $\sum_{i=0}^{r} A_i(\delta) \sum_{s=0}^{\rho} J_{\mathrm{C}}(l, s, i) \geq N_{\mathrm{C}}(l)$. □

We remark that Proposition 5.14 is a tighter lower bound than the sphere covering bound. However, determining T_δ is computationally infeasible for large parameter values.

Another set of linear inequalities is obtained from the inner distribution $\{a_i\}$ of a covering code $\mathcal{C}$, defined as $a_i \stackrel{\text{def}}{=} \frac{1}{|\mathcal{C}|} \sum_{C \in \mathcal{C}} |\{D \in \mathcal{C} : d_{\mathrm{I}}(C, D) = i\}|$ for $0 \leq i \leq r$ [15].

Proposition 5.15. *Let $t = \min \sum_{i=0}^{r} a_i$, where the minimum is taken over all sequences $\{a_i\}$ with $a_0 = 1$, $0 \leq a_i \leq N_{\mathrm{C}}(i)$ for $1 \leq i \leq r$, $\sum_{i=0}^{r} a_i \sum_{s=0}^{\rho} J_{\mathrm{C}}(l, s, i) \geq N_{\mathrm{C}}(l)$ for $0 \leq l \leq r$, and $\sum_{i=0}^{r} a_i \frac{E_i(l)}{N_{\mathrm{C}}(i)} \geq 0$ for $0 \leq l \leq r$. Then $K_{\mathrm{C}}(q, n, r, \rho) \geq t$.*

Proof. Let $\mathcal{C}$ be a CDC with covering radius ρ and inner distribution $\{a_i\}$. Proposition 5.14 yields $0 \leq a_i \leq N_{\mathrm{C}}(i)$ for $1 \leq i \leq r$, $\sum_{i=0}^{r} a_i \sum_{s=0}^{\rho} J_{\mathrm{C}}(l,s,i) \geq N_{\mathrm{C}}(l)$ for $0 \leq l \leq r$, while $a_0 = 1$ follows the definition of a_i. By the generalized MacWilliams inequalities [15, Theorem 3], $\sum_{i=0}^{r} a_i F_l(i) \geq 0$, where $F_l(i) = \frac{\mu_l}{N_{\mathrm{C}}(i)} E_i(l)$ are the q-numbers of the association scheme [15, (15)], which yields $\sum_{i=0}^{r} a_i \frac{E_i(l)}{N_{\mathrm{C}}(i)} \geq 0$. Since $\sum_{i=0}^{r} a_i = |\mathcal{C}|$ we obtain that $|\mathcal{C}| \geq t$. □

Lower bounds on covering codes with the Hamming metric can be obtained through the concept of the excess of a code [49]. This concept being independent of the underlying metric, it was adapted to the rank metric in [80]. We adapt it to the injection metric for CDCs below, thus obtaining the lower bound in Proposition 5.16.

Proposition 5.16. *For all q, n, $r \leq \left\lfloor \frac{n}{2} \right\rfloor$, and $0 < \rho < r$, $K_{\mathrm{C}}(q,n,r,\rho) \geq \frac{\begin{bmatrix} n \\ r \end{bmatrix}}{V_{\mathrm{C}}(\rho) - \frac{\epsilon}{\delta} N_{\mathrm{C}}(\rho)}$, where $\epsilon \stackrel{def}{=} \left\lceil \frac{b_\rho}{c_{\rho+1}} \right\rceil c_{\rho+1} - b_\rho$ and $\delta \stackrel{def}{=} N_{\mathrm{C}}(1) - c_\rho + 2\epsilon$.*

The proof of Proposition 5.16 is similar to that of Proposition 2.35 and is hence omitted. We now derive upper bounds on $K_{\mathrm{C}}(q,n,r,\rho)$. First, we investigate how to expand covering CDCs.

Lemma 5.17. *For all q, n, $r \leq \left\lfloor \frac{n}{2} \right\rfloor$, and $0 < \rho < r$, $K_{\mathrm{C}}(q,n,r,\rho) \leq K_{\mathrm{C}}(q,n-1,r,\rho-1) \leq \begin{bmatrix} n-\rho \\ r \end{bmatrix}$, and $K_{\mathrm{C}}(q,n,r,\rho) \leq K_{\mathrm{C}}(q,n,r-1,\rho-1) \leq \begin{bmatrix} n \\ r-\rho \end{bmatrix}$.*

The proof of Lemma 5.17 is given in Appendix 7.4.2. The next upper bound is a straightforward adaptation of [80, Proposition 12].

Proposition 5.18. *For all q, n, $r \leq \left\lfloor \frac{n}{2} \right\rfloor$, and $0 < \rho < r$, $K_{\mathrm{C}}(q,n,r,\rho) \leq \left\{ 1 - \log_{\begin{bmatrix} n \\ r \end{bmatrix}} \left(\begin{bmatrix} n \\ r \end{bmatrix} - V_{\mathrm{C}}(\rho) \right) \right\}^{-1} + 1$.*

The proof of Proposition 5.18 is similar to that of Proposition 2.43 and is hence omitted. The next bound is a direct application of [37, Theorem 12.2.1].

Proposition 5.19. *For all q, n, $r \leq \left\lfloor \frac{n}{2} \right\rfloor$, and $0 < \rho < r$, $K_{\mathrm{C}}(q,n,r,\rho) \leq \frac{\begin{bmatrix} n \\ r \end{bmatrix}}{V_{\mathrm{C}}(\rho)} \{1 + \ln V_{\mathrm{C}}(\rho)\}$.*

The bound in Proposition 5.19 can be refined by applying the greedy algorithm described in [51] to CDCs.

Proposition 5.20. *Let k_0 be the cardinality of an augmented KK code with minimum distance $2\rho+1$ in $E_r(q,n)$ for $2\rho < r$ and $k_0 = 1$ for $2\rho \geq r$. Then for all $k \geq k_0$, there exists a CDC with cardinality k which covers at least $\begin{bmatrix} n \\ r \end{bmatrix} - u_k$ subspaces, where $u_{k_0} \stackrel{def}{=} \begin{bmatrix} n \\ r \end{bmatrix} - k_0 V_{\mathrm{C}}(\rho)$ and $u_{k+1} = u_k - \left\lceil \frac{u_k V_{\mathrm{C}}(\rho)}{\min\left\{\begin{bmatrix} n \\ r \end{bmatrix} - k, B_{\mathrm{C}}(u_k,\rho)\right\}} \right\rceil$ for all $k \geq k_0$. Thus $K_{\mathrm{C}}(q,n,r,\rho) \leq \min\{k : u_k = 0\}$.*

The proof of Proposition 5.20 is similar to that of Lemma 2.46 and is hence omitted.

Using the bounds derived above, we finally determine the asymptotic behavior of $K_{\mathrm{C}}(q,n,r,\rho)$. The rate of a covering CDC $\mathcal{C} \subseteq E_r(q,n)$ is defined as $\frac{\log_q |\mathcal{C}|}{\log_q |E_r(q,n)|}$. We remark that this rate is different from the one introduced in [81] for packing CDCs, where CDCs are compared to subspace codes. Since we are concerned here about how CDCs cover the Grassmannian, this rate is more appropriate for covering CDCs. We use the following normalized parameters: $r' = \frac{r}{n}$, $\rho' = \frac{\rho}{n}$, and the asymptotic rate $k_{\mathrm{C}}(r',\rho') = \liminf_{n\to\infty} \frac{\log_q K_{\mathrm{C}}(q,n,r,\rho)}{\log_q \begin{bmatrix} n \\ r \end{bmatrix}}$.

Proposition 5.21. *For all $0 \leq \rho' \leq r' \leq \frac{1}{2}$, $k_{\mathrm{C}}(r',\rho') = 1 - \frac{\rho'(1-\rho')}{r'(1-r')}$.*

Proof. The bounds on $V_{\mathrm{C}}(\rho)$ in Lemma 5.8 together with the sphere covering bound yield $K_{\mathrm{C}}(q,n,r,\rho) > K_q^2 q^{r(n-r)-\rho(n-\rho)}$. Using the bounds on the Gaussian polynomial in Corollary 2.3, we obtain $k_{\mathrm{C}}(r',\rho') \geq 1 - \frac{\rho'(1-\rho')}{r'(1-r')}$. Also, Proposition 5.19 leads to $K_{\mathrm{C}}(q,n,r,\rho) < K_q^{-1} q^{r(n-r)-\rho(n-\rho)}[1 + \ln(K_q^{-2}) + \rho(n-\rho)\ln q]$, which asymptotically becomes $k_{\mathrm{C}}(r',\rho') \leq 1 - \frac{\rho'(1-\rho')}{r'(1-r')}$. □

We finish this section by studying the covering properties of liftings of rank metric codes. We first prove that they have maximum covering radius.

Lemma 5.22. *Let $I(\mathcal{C}) \subseteq E_r(q,n)$ be the lifting of a rank metric code in $\mathrm{GF}(q)^{r\times(n-r)}$. Then $I(\mathcal{C})$ has covering radius r.*

Proof. Let $D \in E_r(q,n)$ be generated by $(\mathbf{0}|\mathbf{D}_1)$, where $\mathbf{D}_1 \in \mathrm{GF}(q)^{r\times(n-r)}$ has rank r. Then, for any codeword $I(\mathbf{C})$ generated by $(\mathbf{I}_r|\mathbf{C})$, it is easily seen that $d_{\mathrm{I}}(D, I(\mathbf{C})) = \mathrm{rk}(\mathbf{D}_1) = r$. □

Lemma 5.22 is significant for code design. It is shown in [9] that liftings of rank metric codes can be used to construct nearly optimal packing CDCs. However, Lemma 5.22 indicates that for any lifting of a rank metric code, there exists a subspace at distance r from the code. Hence, adding this subspace to the code leads to a supercode with higher cardinality and the same minimum distance. Thus an optimal CDC cannot be designed from a lifting of a rank metric code.

Although liftings of rank metric codes are poor covering codes, we construct below a class of covering CDCs by using permuted liftings of rank metric covering codes. We thus relate the minimum cardinality of a covering CDC to that of a covering code with the rank metric. For all n and r, we denote the set of subsets of $\{0,1,\ldots,n-1\}$ with cardinality r as S_n^r. For all $J \in S_n^r$ and all $\mathbf{C} \in \mathrm{GF}(q)^{r\times(n-r)}$, let $I(J,\mathbf{C}) = R(\pi(\mathbf{I}_r|\mathbf{C})) \in E_r(q,n)$, where π is the permutation of $\{0,1,\ldots,n-1\}$ satisfying $J = \{\pi(0),\pi(1),\ldots,\pi(r-1)\}$, $\pi(0) < \pi(1) < \ldots < \pi(r-1)$, and $\pi(r) < \pi(r+1) < \ldots < \pi(n-1)$. We remark that π is uniquely determined by J. It is easily shown that $d_{\mathrm{I}}(I(J,\mathbf{C}), I(J,\mathbf{D})) = d_{\mathrm{R}}(\mathbf{C},\mathbf{D})$ for all $J \in S_n^r$ and all $\mathbf{C},\mathbf{D} \in \mathrm{GF}(q)^{r\times(n-r)}$.

Proposition 5.23. *For all q, n, $r \leq \left\lfloor \frac{n}{2} \right\rfloor$, and $0 < \rho < r$, $K_{\mathrm{C}}(q, n, r, \rho) \leq \begin{bmatrix} n \\ r \end{bmatrix} K_{\mathrm{R}}(q, n-r, r, \rho)$.*

Proof. Let $\mathcal{C} \subseteq \mathrm{GF}(q)^{r \times (n-r)}$ have cardinality $K_{\mathrm{R}}(q, n-r, r, \rho)$ and rank covering radius ρ. We show below that $L(\mathcal{C}) = \{I(J, \mathbf{C}) : J \in S_n^r, \mathbf{C} \in \mathcal{C}\}$ is a CDC with covering radius ρ. Any $U \in E_r(q, n)$ can be expressed as $I(J, \mathbf{V})$ for some $J \in S_n^r$ and some $\mathbf{V} \in \mathrm{GF}(q)^{r \times (n-r)}$. Also, by definition, there exists $\mathbf{C} \in \mathcal{C}$ such that $d_{\mathrm{R}}(\mathbf{C}, \mathbf{V}) \leq \rho$ and hence $d_{\mathrm{I}}(U, I(J, \mathbf{C})) = d_{\mathrm{R}}(\mathbf{C}, \mathbf{V}) \leq \rho$. Thus $L(\mathcal{C})$ has covering radius ρ and cardinality $\leq \begin{bmatrix} n \\ r \end{bmatrix} K_{\mathrm{R}}(q, n-r, r, \rho)$. □

In order to illustrate the result in Proposition 5.23, we consider $L(\mathcal{C})$, where $\mathcal{C}$ is the code introduced in (2.9). Since $\mathcal{C}$ is a code in $\mathrm{GF}(2)^{3\times 3}$ with rank covering radius 2, $L(\mathcal{C})$ is a CDC in $E_3(2, 6)$ with covering radius 2. Proposition 5.23 indicates that $|L(\mathcal{C})| \leq 4\begin{bmatrix} 6 \\ 3 \end{bmatrix} = 80$; however, since several liftings $I(J, \mathbf{C})$ for different J and the same $\mathbf{C}$ are equal, it can be shown that $|L(\mathcal{C})| = 70 < 80$.

It is shown in [80] that for $r \leq n - r$, $K_{\mathrm{R}}(q, n-r, r, \rho)$ is on the order of $q^{r(n-r)-\rho(n-\rho)}$, which is also the order of $K_{\mathrm{C}}(q, n, r, \rho)$. Therefore, the construction in Proposition 5.23 leads to good covering CDCs for large q. However, for $q = 2$, the $\begin{bmatrix} n \\ r \end{bmatrix}$ term is not negligible, and the upper bound in Proposition 5.23 is not tight.

5.4 Properties of subspace codes with the subspace metric

We now investigate the properties of subspace codes. We shall use the notation $\nu = \left\lfloor \frac{n}{2} \right\rfloor$ in the rest of this chapter.

5.4.1 Properties of balls with subspace radii

We first investigate the properties of balls with subspace radii in $E(q,n)$, which will be instrumental in our study of packing and covering properties of subspace codes with the subspace metric. We first derive bounds on $|E(q,n)|$ below.

Lemma 5.24. *For all n, we have $q^{\nu(n-\nu)} \leq |E(q,n)| < 2K_q^{-1}N_q q^{\nu(n-\nu)}$, where $N_q \stackrel{def}{=} \sum_{i=0}^{\infty} q^{-i^2}$.*

Proof. We have $|E(q,n)| = \sum_{r=0}^{n} \begin{bmatrix} n \\ r \end{bmatrix} \geq \begin{bmatrix} n \\ \nu \end{bmatrix} \geq q^{\nu(n-\nu)}$, which proves the lower bound. In order to prove the upper bound, we distinguish two cases. First, if $n = 2\nu + 1$, then $\sum_{r=0}^{2\nu+1} \begin{bmatrix} 2\nu+1 \\ r \end{bmatrix} = 2\sum_{i=0}^{\nu} \begin{bmatrix} 2\nu+1 \\ \nu-i \end{bmatrix} < 2K_q^{-1} \sum_{i=0}^{\nu} q^{\nu(\nu+1)-i(i+1)} < 2K_q^{-1}N_q q^{\nu(n-\nu)}$. Second, if $n = 2\nu$, then $\sum_{r=0}^{2\nu} \begin{bmatrix} 2\nu \\ r \end{bmatrix} = \begin{bmatrix} 2\nu \\ \nu \end{bmatrix} + 2\sum_{i=1}^{\nu} \begin{bmatrix} 2\nu \\ \nu-i \end{bmatrix} < 2K_q^{-1} \sum_{i=0}^{\nu} q^{\nu^2-i^2} < 2K_q^{-1}N_q q^{\nu(n-\nu)}$. □

We now determine the number of subspaces at a given distance from a fixed subspace.

Lemma 5.25. *The number of subspaces $N_{\mathrm{S}}(r,s,d)$ with dimension s at subspace distance d from a subspace with dimension r is given by $q^{u(d-u)} \begin{bmatrix} r \\ u \end{bmatrix} \begin{bmatrix} n-r \\ d-u \end{bmatrix}$ when $u \stackrel{def}{=} \frac{r+d-s}{2}$ is an integer, and 0 otherwise.*

Proof. For $U \in E_r(q,n)$ and $V \in E_s(q,n)$, $d_{\mathrm{S}}(U,V) = d$ if and only if $\dim(U \cap V) = r - u$. Thus there are $\begin{bmatrix} r \\ u \end{bmatrix}$ choices for $U \cap V$. The subspace V can then be completed in $q^{u(d-u)} \begin{bmatrix} n-r \\ d-u \end{bmatrix}$ ways. □

We remark that this result is implicitly contained in [61, Theorem 5], where no proof is given. We also denote the volume of a ball with subspace radius t around a subspace with dimension r as $V_{\mathrm{S}}(r,t) \stackrel{\mathrm{def}}{=} \sum_{d=0}^{t} \sum_{s=0}^{n} N_{\mathrm{S}}(r,s,d)$.

The following technical lemma will be instrumental in Section 5.4.3.

Lemma 5.26. *For all r, s, and $t \leq \min\{r+s, \nu\}$, $\sum_{d=0}^{t} N_{\mathrm{S}}(r,s,d) < K_q^{-2} L_q q^{f(t)}$, where $4f(d) = d(2n-d) - (r-s)(2n-r-3s)$ and $L_q = \sum_{i=0}^{\infty} q^{-\frac{3}{4}i^2}$. Therefore, $\sum_{d=0}^{t} N_{\mathrm{S}}(r,s,d) < K_q^{-2} L_q q^{t(n-s)}$ for $s \leq \nu$.*

Proof. By Lemma 5.25 and Corollary 2.3, we have $N_{\mathrm{S}}(r,s,d) < K_q^{-2} q^{f(d)}$, and hence

$$\sum_{d=0}^{t} N_{\mathrm{S}}(r,s,d) < K_q^{-2} q^{f(t)} \sum_{i=0}^{t} q^{-\frac{i}{4}(2n-2t+i)} \leq K_q^{-2} q^{f(t)} \sum_{i=0}^{t} q^{-\frac{3}{4}i^2} < K_q^{-2} L_q q^{f(t)}.$$

Maximizing f for $s \leq \nu$ and $s-t \leq r \leq s+t$, we easily obtain $\sum_{d=0}^{t} N_{\mathrm{S}}(r,s,d) < K_q^{-2} L_q q^{t(n-s)}$. □

We now derive bounds on the volume of a ball with subspace radius. Since $V_{\mathrm{S}}(r,t) = V_{\mathrm{S}}(n-r,t)$ for all r and t, we only consider $r \leq \nu$. Also, we assume $t \leq \nu$, for only this case will be instrumental to our derivations.

Proposition 5.27. *For all q, n, $r \leq \nu$, and $t \leq \nu$, we have $q^{-\frac{3}{4}} q^{g(t)} \leq V_{\mathrm{S}}(r,t) \leq 2M_q K_q^{-2} L_q q^{g(t)}$, where $M_q = \sum_{i=0}^{\infty} q^{-3i^2}$, $L_q = \sum_{i=0}^{\infty} q^{-\frac{3i^2}{4}}$, and*

$$g(t) = \begin{cases} t(n-r-t) & \text{for } t \leq \frac{n-2r}{3}, \\ \frac{1}{12}(n-2r)^2 + \frac{1}{4}t(2n-t) & \text{for } \frac{n-2r}{3} \leq t \leq \frac{n+4r}{3}, \\ (t-r)(n-t+r) & \text{for } \frac{n+4r}{3} \leq t \leq \frac{n}{2}. \end{cases} \tag{5.4}$$

The proof of Proposition 5.27 is given in Appendix 7.4.3. We remark that the bounds in Proposition 5.27 are tight up to a scalar, and depend on both r and t.

For all $A \in E_a(q,n), B \in E_b(q,n)$, we denote the number of subspaces with dimension c in the intersection of two spheres with subspace radii u and s centered at A and B, respectively, as $J_{\mathrm{S}}(q,n;u,s;A,B,c) = |\{C \in E_c(q,n) : d_{\mathrm{S}}(A,C) = u, d_{\mathrm{S}}(B,C) = s\}|$.

Theorem 5.28. *For all $A \in E_a(q,n), B \in E_b(q,n)$ with $d_{\mathrm{S}}(A,B) = w$, the intersection $J_{\mathrm{S}}(q,n;u,s;A,B,c)$ depends on A and B only through a, b, and w. We thus have $J_{\mathrm{S}}(q,n;u,s;A,B,c) = J_{\mathrm{S}}(q,n;u,s,w;a,b,c)$.*

The proof of Theorem 5.28 is given in Appendix 7.4.4. The intersection of spheres with subspace radii is related to the volume of these spheres in Corollary 5.29 below.

Corollary 5.29. *For all parameter values,*

$$N_{\mathrm{S}}(a,b,w)J_{\mathrm{S}}(q,n;u,s,w;a,b,c) = N_{\mathrm{S}}(a,c,u)J_{\mathrm{S}}(q,n;w,s,u;a,c,b), \quad (5.5)$$

$$\sum_{u=0}^{n} J_{\mathrm{S}}(q,n;u,s,w;a,b,c) = N_{\mathrm{S}}(b,c,s). \quad (5.6)$$

Proof. Let $A \in E_a(q,n)$. By counting the number of pairs of subspaces (B,C) such that $\dim(B) = b$, $\dim(C) = c$, $d_{\mathrm{S}}(A,B) = w$, $d_{\mathrm{S}}(A,C) = u$, and $d_{\mathrm{S}}(B,C) = s$ in two different ways, we obtain (5.5). Also, $\sum_{u=0}^{n} J_{\mathrm{S}}(q,n;u,s,w;a,b,c)$ is the number of subspaces $C \in E_c(q,n)$ such that $d_{\mathrm{S}}(B,C) = s$ for a given $B \in E_b(q,n)$, hence it is equal to $N_{\mathrm{S}}(b,c,s)$. □

The set of all subspaces of $\mathrm{GF}(q)^n$, endowed with the subspace (or injection) metric, does not form an association scheme. Indeed, the intersection of two spheres does not only depend on the radii of the spheres and on the distance between their respective centers. Theorem 5.28 is a fundamental property of spheres in the subspace metric, as it shows that the intersection only depends on the parameters mentioned above and the dimension of the centers.

Theorem 5.28 also implies that the intersection of two balls in $E(q,n)$ with subspace radii, represented as the shaded area in Figure 5.1, only depends on a, b, u, s, and w. Furthermore, for all c, the number of subspaces with dimension c in

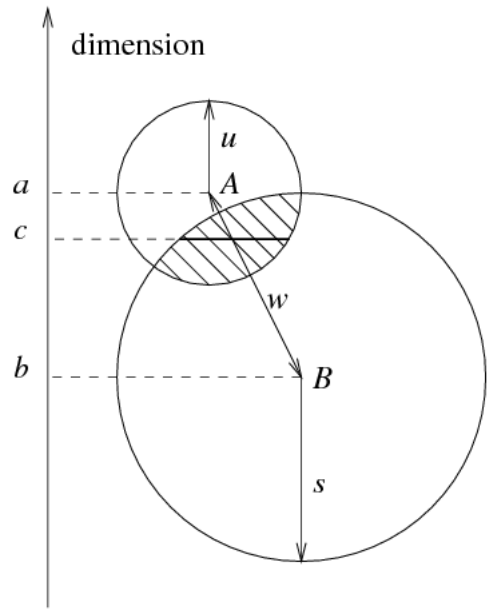

Figure 5.1: Intersection of balls in the subspace metric.

the intersection, represented as the black line in Figure 5.1, only depends on the parameters above and c.

Although the value of $J_{\mathrm{S}}(q,n;u,s,w;a,b,c)$ is unknown in general, we remark that for $a=b=c$, $J_{\mathrm{S}}(q,n;2u,2s,2w;a,a,a) = J_{\mathrm{C}}(q,n,a,u,s,w)$, the intersection number of the association scheme for $E_a(q,n)$. We also determine its value when $w=u+s$ below.

Proposition 5.30. *When $w=u+s$, we have*

$$J_{\mathrm{S}}(q,n;u,s,u+s;a,b,c) = \begin{bmatrix} \frac{a-b+u+s}{2} \\ \frac{c-b+s}{2} \end{bmatrix} \begin{bmatrix} \frac{b-a+u+s}{2} \\ \frac{c-a+u}{2} \end{bmatrix}. \tag{5.7}$$

Proof. Let $A \in E_a(q,n)$, $B \in E_b(q,n)$, and $C \in E_c(q,n)$ satisfy $d_{\mathrm{S}}(A,B) = u+s$, $d_{\mathrm{S}}(A,C) = u$, and $d_{\mathrm{S}}(B,C) = s$; hence $\dim(A \cap B) = \frac{a+b-u-s}{2}$, $\dim(C \cap A) = \frac{a+c-u}{2}$, and $\dim(C \cap B) = \frac{b+c-s}{2}$. Since $c = \dim(C) \geq \dim(C \cap A + C \cap B) = c + \frac{a+b-u-s}{2} -$

$\dim(C \cap A \cap B)$ and $\dim(C \cap A \cap B) \leq \dim(A \cap B) = \frac{a+b-u-s}{2}$, we $C \cap A \cap B = A \cap B$ and $C = C \cap A + C \cap B$. There are $N_{\mathrm{S}}(q, a, \frac{a+b-u-s}{2}, \frac{a+c-u}{2}, \frac{c-b+s}{2})$ choices for $C \cap A$; similarly, there are $N_{\mathrm{S}}(q, b, \frac{a+b-u-s}{2}, \frac{b+c-s}{2}, \frac{c-a+u}{2})$ choices for $C \cap B$. Thus, there are $N_{\mathrm{S}}(q, a, \frac{a+b-u-s}{2}, \frac{a+c-u}{2}, \frac{c-b+s}{2}) N_{\mathrm{S}}(q, b, \frac{a+b-u-s}{2}, \frac{b+c-s}{2}, \frac{c-a+u}{2}) = \begin{bmatrix} \frac{a-b+u+s}{2} \\ \frac{c-b+s}{2} \end{bmatrix} \begin{bmatrix} \frac{b-a+u+s}{2} \\ \frac{c-a+u}{2} \end{bmatrix}$ choices for C. □

It is easy to show that $J_{\mathrm{S}}(q, n; u, s, u+s; a, b, c) = 0$ when $u > \min\{a + c, a + 2b - c\}$, $s > \min\{b + c, 2a + b - c\}$, or $u + s > \min\{a + b, n\}$.

5.4.2 Packing properties of subspace codes with the subspace metric

We are interested in packing subspace codes used with the subspace metric. The maximum cardinality of a code in $E(q, n)$ with minimum subspace distance d is denoted as $A_{\mathrm{S}}(q, n, d)$. Since $A_{\mathrm{S}}(q, n, 1) = |E(q, n)|$, we assume $d \geq 2$ henceforth.

We can relate $A_{\mathrm{S}}(q, n, d)$ to $A_{\mathrm{C}}(q, n, r, d)$. For all $J \subseteq \{0, 1, \ldots, n\}$, we denote the maximum cardinality of a code with minimum subspace distance d and codewords having dimensions in J as $A_{\mathrm{S}}(q, n, d, J)$. For $2 \leq d \leq 2\nu$, we denote $R_d = \left\{ \left\lceil \frac{d}{2} \right\rceil, \left\lceil \frac{d}{2} \right\rceil + 1, \ldots, n - \left\lceil \frac{d}{2} \right\rceil \right\}$.

Proposition 5.31. *For $n = d = 2\nu + 1$, $A_{\mathrm{S}}(q, 2\nu + 1, 2\nu + 1) = 2$ and for $2 \leq d \leq 2\nu$, $A_{\mathrm{S}}(q, n, d) \leq A_{\mathrm{S}}(q, n, d, R_d) + 2$. Also, we have $\max_{\lceil \frac{d}{2} \rceil \leq r \leq \nu} A_{\mathrm{C}}(q, n, r, \lceil \frac{d}{2} \rceil) \leq A_{\mathrm{S}}(q, n, d) \leq 2 + \sum_{r \in R_d} A_{\mathrm{C}}(q, n, r, \lceil \frac{d}{2} \rceil)$.*

Proof. Let $\mathcal{C}$ be a code in $E(q, n)$ with minimum subspace distance d. For $C, D \in \mathcal{C}$, we have $\dim(C) + \dim(D) \geq d_{\mathrm{S}}(C, D) \geq d$; therefore there is at most one codeword with dimension less than $\frac{d}{2}$. Similarly, $\dim(C) + \dim(D) \leq 2n - d_{\mathrm{S}}(C, D) \leq 2n - d$,

therefore there is at most one codeword with dimension greater than $\frac{2n-d}{2}$. Thus $A_{\mathrm{S}}(q,n,d) \leq A_{\mathrm{S}}(q,n,d,R_d)+2$ for $d \leq 2\nu$ and $A_{\mathrm{S}}(q,2\nu+1,2\nu+1) \leq 2$. Since the code $\{\{\mathbf{0}\},\mathrm{GF}(q)^{2\nu+1}\}$ has minimum subspace distance $2\nu+1$, we obtain $A_{\mathrm{S}}(q,2\nu+1,2\nu+1)=2$.

A CDC in $E_r(q,n)$ with minimum injection distance $\left\lceil \frac{d}{2} \right\rceil$ has minimum subspace distance $\geq d$, and hence $A_{\mathrm{C}}(q,n,r,\left\lceil \frac{d}{2} \right\rceil) \leq A_{\mathrm{S}}(q,n,d)$ for all r. Also, the codewords with dimension r in a code with minimum subspace distance d form a CDC in $E_r(q,n)$ with minimum distance at least $\left\lceil \frac{d}{2} \right\rceil$, and hence $A_{\mathrm{S}}(q,n,d) \leq A_{\mathrm{S}}(q,n,d,R_d)+2 \leq 2+\sum_{r\in R_d} A_{\mathrm{C}}(q,n,r,\left\lceil \frac{d}{2} \right\rceil)$. □

The relation between $A_{\mathrm{S}}(q,n,d)$ and $A_{\mathrm{C}}(q,n,r,d)$ is tightened in Proposition 5.32 below.

Proposition 5.32. *For $2 \leq d \leq 2\nu$ and $\left\lceil \frac{d}{2} \right\rceil \leq r \leq \nu$,*

$$\begin{aligned} & K_q q^{(\nu-r)(\nu-r+\left\lceil \frac{d}{2} \right\rceil-1)} A_{\mathrm{C}}\left(q,n,r,\left\lceil \frac{d}{2} \right\rceil\right) \\ & < A_{\mathrm{S}}(q,n,d) \\ & < 2K_q^{-1} N_q q^{(\nu-r)(\nu-r+\left\lceil \frac{d}{2} \right\rceil-1)} A_{\mathrm{C}}\left(q,n,r,\left\lceil \frac{d}{2} \right\rceil\right) \end{aligned} \tag{5.8}$$

where $N_q = \sum_{i=0}^{\infty} q^{-i^2}$.

Proof. By Proposition 5.31 and (4.5), we have $A_{\mathrm{S}}(q,n,d) \geq A_{\mathrm{C}}(q,n,\nu,\left\lceil \frac{d}{2} \right\rceil) \geq q^{(n-\nu)(\nu-\left\lceil \frac{d}{2} \right\rceil)} > K_q q^{(\nu-r)(\nu-r+\left\lceil \frac{d}{2} \right\rceil-1)} A_{\mathrm{C}}\left(q,n,r,\left\lceil \frac{d}{2} \right\rceil\right)$. Proposition 5.31, (4.5), and Corollary 2.3 also lead to

$$\begin{aligned} A_{\mathrm{S}}(q,n,d) &< 2 + 2K_q^{-1} \sum_{r=\left\lceil \frac{d}{2} \right\rceil}^{\nu} q^{(n-r)(r-\left\lceil \frac{d}{2} \right\rceil+1)} \\ &< 2 + 2K_q^{-1} N_q q^{(n-\nu)(\nu-\left\lceil \frac{d}{2} \right\rceil+1)} \\ &\leq 2K_q^{-1} N_q q^{(\nu-r)(\nu-r+\left\lceil \frac{d}{2} \right\rceil-1)} A_{\mathrm{C}}\left(q,n,r,\left\lceil \frac{d}{2} \right\rceil\right), \end{aligned} \tag{5.9}$$

where (5.9) follows (4.5). □

Proposition 5.32 indicates that CDCs with constant dimension half of n are optimal subspace codes up to a scalar. Therefore, CDCs can be used for error correction with random linear network coding with a limited rate loss. The bounds above help us determine the asymptotic behavior of $A_{\mathrm{S}}(q,n,d)$. The rate of a subspace code $\mathcal{C} \subseteq E(q,n)$ is defined as $\frac{\log_q |\mathcal{C}|}{\log_q |E(q,n)|}$, which can be seen as a combinatorial rate at the subspace level. This differs from the rate introduced in [9] for CDCs, where the amount of data sent by each codeword is considered, and which seems appropriate for CDCs only. On the other hand, we believe our rate is more appropriate to compare general subspace codes, since all the subspaces are treated equally, regardless of their dimension. Using the normalized parameter $d' \stackrel{\text{def}}{=} \frac{d}{n}$, the asymptotic rate $a_{\mathrm{S}}(d') = \limsup_{n\to\infty} \frac{\log_q A_{\mathrm{S}}(q,n,d)}{\log_q |E(q,n)|}$ can be easily determined from Proposition 5.32 and Lemma 5.24.

Proposition 5.33. *For $0 \leq d' \leq 1$, $a_{\mathrm{S}}(d') = 1 - d'$.*

On the other hand, Proposition 5.32 also indicates that using CDCs with dimension $r < \nu$ leads to a decrease in rate on the order of $(1-2r')(d'+1-2r')$, where $r' = \frac{r}{n}$.

The lower bound in Proposition 5.31 can be tightened by adapting the algorithm used in the proof of the Gilbert bound for the Hamming metric.

Proposition 5.34. *For all q, n, $2 \leq d \leq n$, and any permutation π of $\{0,1,\ldots,n\}$, there exists a code in $E(q,n)$ with minimum subspace distance d and $A_{\pi(r)}$ codewords with dimension $\pi(r)$ for $0 \leq r \leq n$, where $A_{\pi(0)} = A_{\mathrm{C}}\left(q,n,\pi(0),\left\lceil \frac{d}{2} \right\rceil\right)$ and*

$$A_{\pi(r)} = \max\left\{0, \left\lceil \frac{\begin{bmatrix} n \\ \pi(r) \end{bmatrix} - \sum_{i=0}^{r-1} A_{\pi(i)} \sum_{e=0}^{d-1} N_{\mathrm{S}}(\pi(i),\pi(r),e)}{\sum_{e=0}^{d-1} N_{\mathrm{S}}(\pi(r),\pi(r),e)} \right\rceil\right\}. \tag{5.10}$$

Proof. We show that there exists such a code by recursion on r. First, for $r = 0$, this follows from the definition of $A_{\mathrm{C}}\left(q, n, \pi(0), \left\lceil \frac{d}{2} \right\rceil\right)$. Second, suppose there exists a code with minimum subspace distance d and $A_{\pi(l)}$ codewords with dimension $\pi(l)$ for $0 \leq l \leq r-1$. These codewords cover at most $N = \sum_{i=0}^{r-1} A_{\pi(i)} \sum_{e=0}^{d-1} N_{\mathrm{S}}(\pi(i), \pi(r), e)$ subspaces of dimension $\pi(r)$. If $N \leq \begin{bmatrix} n \\ r \end{bmatrix}$, we can select at least $\left\lceil \frac{\begin{bmatrix} n \\ r \end{bmatrix} - N}{\sum_{e=0}^{d-1} N_{\mathrm{S}}(\pi(r), \pi(r), e)} \right\rceil$ codewords with dimension $\pi(r)$. □

Although the bound in Proposition 5.34 holds for any permutation π, we remark that not all choices for π lead to tight bounds. However, choosing $\pi(0)$ to maximize $A_{\pi(0)}$ leads to a tighter bound than the one in Proposition 5.31.

We finally compare our lower bounds on $A_{\mathrm{S}}(q, n, d)$ to the Gilbert bound in [61]. The latter shows that $A_{\mathrm{S}}(q, n, d) \geq \frac{|E(q,n)|}{\mathrm{avg} V_{\mathrm{S}}(r, d-1)}$, where the average is taken over all subspaces in $E(q, n)$. Using the bounds on $V_{\mathrm{S}}(r, d-1)$ in Proposition 5.27, it can be shown that this lower bound is at most $2K_q^{-1} N_q q^{\frac{3}{4}} q^{\nu(n-\nu) - \frac{1}{4}(d-1)(2n-d+1)}$. On the other hand, Proposition 5.31 and (4.5) yield $A_{\mathrm{S}}(q, n, d) \geq q^{\nu(n-\nu) - \frac{1}{4}(d-1)(n+1)}$. The ratio between our bound and the Gilbert bound is hence at least $\frac{1}{2} K_q N_q^{-1} q^{\frac{1}{4}(d-1)(n-d)}$. Therefore, our bounds outperform the Gilbert bound for nontrivial cases.

5.4.3 Covering properties of subspace codes with the subspace metric

We now consider the covering properties of subspace codes with the subspace metric. The subspace covering radius of a code $\mathcal{C} \subseteq E(q, n)$ is defined as $\max_{U \in E(q,n)} d_{\mathrm{S}}(U, \mathcal{C})$. We denote the minimum cardinality of a subspace code in $E(q, n)$ with subspace covering radius ρ as $K_{\mathrm{S}}(q, n, \rho)$. Since $K_{\mathrm{S}}(q, n, 0) = |E(q, n)|$ and $K_{\mathrm{S}}(q, n, n) = 1$, we assume $0 < \rho < n$ henceforth. We determine below the minimum cardinality of

a code with subspace covering radius $\rho \geq \nu$.

Proposition 5.35. *For $\nu \leq \rho < n$, $K_{\mathrm{S}}(q, n, \rho) = 2$.*

Proof. For all $V \in E(q, n)$ there exists $\bar{V}$ such that $V \oplus \bar{V} = \mathrm{GF}(q)^n$ and hence $d_{\mathrm{S}}(V, \bar{V}) = n$. Therefore, one subspace cannot cover the whole $E(q, n)$ with radius $\rho < n$, hence $K_{\mathrm{S}}(q, n, \rho) > 1$. Let $\mathcal{C} = \{\{\mathbf{0}\}, \mathrm{GF}(q)^n\}$, then for all $D \in E(q, n)$, $d_{\mathrm{S}}(D, \mathcal{C}) = \min\{\dim(D), n - \dim(D)\} \leq \nu$. Thus $\mathcal{C}$ has covering radius ν and $K_{\mathrm{S}}(q, n, \rho) \leq 2$ for all $\rho \geq \nu$. □

We thus consider $0 < \rho < \nu$ henceforth. Proposition 5.36 below is the sphere covering bound for subspace codes with the subspace metric.

Proposition 5.36. *For all q, n, and $0 < \rho < \nu$, $K_{\mathrm{S}}(q, n, \rho) \geq \min \sum_{i=0}^{n} A_i$, where the minimum is taken over all integer sequences $\{A_i\}$ satisfying $0 \leq A_i \leq \begin{bmatrix} n \\ i \end{bmatrix}$ for all $0 \leq i \leq n$ and $\sum_{i=0}^{n} A_i \sum_{d=0}^{\rho} N_{\mathrm{S}}(i, r, d) \geq \begin{bmatrix} n \\ r \end{bmatrix}$ for $0 \leq r \leq n$.*

Proof. Let $\mathcal{C}$ be a subspace code with covering radius ρ and let A_i denote the number of subspaces with dimension i in $\mathcal{C}$. Then $0 \leq A_i \leq \begin{bmatrix} n \\ i \end{bmatrix}$ for all $0 \leq i \leq n$. All subspaces with dimension r are covered; however, a codeword with dimension i covers exactly $\sum_{d=0}^{\rho} N_{\mathrm{S}}(i, r, d)$ subspaces with dimension r, hence $\sum_{i=0}^{n} A_i \sum_{d=0}^{\rho} N_{\mathrm{S}}(i, r, d) \geq \begin{bmatrix} n \\ r \end{bmatrix}$ for $0 \leq r \leq n$. □

We now derive upper bounds on $K_{\mathrm{S}}(q, n, \rho)$.

Proposition 5.37. *For all q, n, $0 < \rho < \nu$, $K_{\mathrm{S}}(q, n, \rho) \leq 2 + 2 \sum_{r=\rho+1}^{\nu} \lfloor k_r \rfloor$, where*

$$k_r = \frac{\begin{bmatrix} n \\ r \end{bmatrix}}{\begin{bmatrix} n-r+\rho \\ \rho \end{bmatrix}} + \frac{\begin{bmatrix} n \\ r-\rho \end{bmatrix}}{\begin{bmatrix} r \\ \rho \end{bmatrix}} \ln \begin{bmatrix} n-r+\rho \\ \rho \end{bmatrix}.$$

Proof. We show that there exists a code with cardinality $2 + 2\sum_{r=\rho+1}^{\nu} \lfloor k_r \rfloor$ and covering radius ρ. We choose $\{\mathbf{0}\}$ to be in the code, hence all subspaces with dimension $0 \leq r \leq \rho$ are covered. For $\rho + 1 \leq r \leq \nu$, let $\mathbf{A}$ be the $\begin{bmatrix} n \\ r \end{bmatrix} \times \begin{bmatrix} n \\ r-\rho \end{bmatrix}$ binary matrix whose rows represent the subspaces $U_i \in E_r(q, n)$ and whose columns represent the subspaces $V_j \in E_{r-\rho}(q, n)$, and where $a_{i,j} = 1$ if and only if $d_{\mathrm{S}}(U_i, V_j) = \rho$. Then there are exactly $N_{\mathrm{S}}(r, r-\rho, \rho) = \begin{bmatrix} r \\ \rho \end{bmatrix}$ ones on each row and $N_{\mathrm{S}}(r-\rho, r, \rho) = \begin{bmatrix} n-r+\rho \\ \rho \end{bmatrix}$ ones on each column. By [37, Theorem 12.2.1], there exists an $\begin{bmatrix} n \\ r \end{bmatrix} \times \lfloor k_r \rfloor$ submatrix of $\mathbf{A}$ with no all-zero rows. Thus, all subspaces of dimension r can be covered using $\lfloor k_r \rfloor$ codewords. Summing for all r, all subspaces with dimension $0 \leq r \leq \nu$ can be covered with $1+\sum_{r=\rho+1}^{\nu} \lfloor k_r \rfloor$ subspaces. Similarly, it can be shown that all subspaces with dimension $\nu+1 \leq r \leq n$ can be covered with $1+\sum_{r=\rho+1}^{\nu} \lfloor k_r \rfloor$ subspaces. □

We remark that the upper bound in Proposition 5.37 can be further tightened by using the greedy algorithm described in [51,82]. We now give an explicit construction of a subspace covering code.

Proposition 5.38. *For all q, n, and $0 < \rho < \nu$, let $J_1 = \{0\} \cup \{\nu - \rho - \lfloor \frac{\nu-\rho}{2\rho+1} \rfloor (2\rho + 1), \ldots, \nu - 3\rho - 1, \nu - \rho\}$ and $J_2 = \{n\} \cup \{n - \nu + \rho + \lfloor \frac{\nu-\rho}{2\rho+1} \rfloor (2\rho + 1), \ldots, n - \nu + 3\rho + 1, n - \nu + \rho\}$. Then the code $\bigcup_{r \in J_1 \cup J_2} E_r(q, n)$ has subspace covering radius ρ, and hence $K_{\mathrm{S}}(q, n, \rho) \leq \sum_{r \in J_1 \cup J_2} \begin{bmatrix} n \\ r \end{bmatrix}$.*

Proof. We prove that $\bigcup_{r \in J_1} E_r(q, n)$ covers all subspaces with dimension $\leq \nu$. First, all subspaces $D_0 \in E(q, n)$ with dimension $0 \leq \dim(D_0) < \nu - 2\rho - \lfloor \frac{\nu-\rho}{2\rho+1} \rfloor (2\rho+1) \leq \rho$ are covered by the subspace with dimension 0. Second, for all $D_1 \in E(q, n)$ with dimension $\nu - 2\rho - i(2\rho + 1) \leq \dim(D_1) \leq \nu - \rho - i(2\rho + 1)$, there exists C_1 with dimension $\nu - \rho - i(2\rho + 1)$ such that $D_1 \subseteq C_1$. Thus $d_{\mathrm{S}}(C_1, D_1) = \dim(C_1) -$

$\dim(D_1) \leq \rho$. Similarly, for all $D_2 \in E(q,n)$ with dimension $\nu - \rho - i(2\rho+1) < \dim(D_2) \leq \nu - i(2\rho+1)$, there exists C_2 with dimension $\nu - \rho - i(2\rho+1)$ such that $C_2 \subset D_2$. Thus $d_{\mathrm{S}}(C_2, D_2) = \dim(D_2) - \dim(C_2) \leq \rho$. Therefore, $\bigcup_{r \in J_1} E_r(q,n)$ covers all subspaces with dimension $\leq \nu$. Similarly, all the subspaces with dimension $\geq n - \nu$ are covered by $\bigcup_{r \in J_2} E_r(q,n)$. □

Using the bounds derived above, we finally determine the asymptotic behavior of $K_{\mathrm{S}}(q,n,\rho)$. We define $k_{\mathrm{S}}(\rho') = \liminf_{n\to\infty} \frac{\log_q K_{\mathrm{S}}(q,n,\rho)}{\log_q |E(q,n)|}$, where $\rho' = \frac{\rho}{n}$.

Proposition 5.39. *For* $0 \leq \rho' \leq \frac{1}{2}$, $k_{\mathrm{S}}(\rho') = 1 - 2\rho'$. *For* $\frac{1}{2} \leq \rho' \leq 1$, $k_{\mathrm{S}}(\rho') = 0$.

Proof. By Proposition 5.35, $k_{\mathrm{S}}(\rho') = 0$ for $\frac{1}{2} \leq \rho' \leq 1$. Let $\mathcal{C}$ be a code with subspace covering radius $\rho < \nu$ and for $0 \leq l \leq n$, let A_l denote the number of codewords in $\mathcal{C}$ with dimension l. All the subspaces in $E_\nu(q,n)$ are covered, hence $\begin{bmatrix} n \\ \nu \end{bmatrix} \leq \sum_{l=0}^{n} A_l \sum_{d=0}^{\rho} N_{\mathrm{S}}(l,\nu,d)$. Using Lemma 5.26, we obtain $\sum_{d=0}^{\rho} N_{\mathrm{S}}(l,\nu,d) < K_q^{-2} L_q q^{\rho(n-\nu)}$ for all l, and hence $\begin{bmatrix} n \\ \nu \end{bmatrix} < K_q^{-2} L_q q^{\rho(n-\nu)} |\mathcal{C}|$. Therefore $K_{\mathrm{S}}(q,n,\rho) > K_q^2 L_q^{-1} q^{(n-\nu)(\nu-\rho)}$, which asymptotically becomes $k_{\mathrm{S}}(\rho') \geq 1 - 2\rho'$.

Also, by Proposition 5.37, it can be easily shown that $K_{\mathrm{S}}(q,n,\rho) \leq 2 + (n+1)[1 - \ln K_q + \rho(n-\rho-1)\ln q] K_q^{-1} q^{(n-\nu)(\nu-\rho)}$, which asymptotically becomes $k_{\mathrm{S}}(\rho') \leq 1 - 2\rho'$. □

5.5 Properties of subspace codes with the injection metric

5.5.1 Properties of balls with injection radii

We first investigate the properties of balls with injection radii in $E(q,n)$, which will be instrumental in our study of packing and covering properties of subspace codes with the injection distance.

Lemma 5.40. *The number of subspaces with dimension s at injection distance d from a subspace with dimension r is given by $N_{\mathrm{I}}(r,s,d) = N_{\mathrm{S}}(r,s,2d-|r-s|)$. Hence, $N_{\mathrm{I}}(r,s,d) = q^{d(d+s-r)}\begin{bmatrix} r \\ d \end{bmatrix}\begin{bmatrix} n-r \\ d+s-r \end{bmatrix}$ for $r \geq s$ and $N_{\mathrm{I}}(r,s,d) = q^{d(d+r-s)}\begin{bmatrix} r \\ d+r-s \end{bmatrix}\begin{bmatrix} n-r \\ d \end{bmatrix}$ for $r \leq s$.*

Proof. If $U \in E_r(q,n)$ and $V \in E_s(q,n)$, then $d_{\mathrm{I}}(U,V) = d$ if and only if $d_{\mathrm{S}}(U,V) = 2d - |r-s|$. Therefore, $N_{\mathrm{I}}(r,s,d) = N_{\mathrm{S}}(r,s,2d-|r-s|)$, and the formula for $N_{\mathrm{I}}(r,s,d)$ is easily obtained from Lemma 5.25. □

Hence $N_{\mathrm{I}}(r,s,d) = q^{d(d-\delta)}\begin{bmatrix} \omega \\ d \end{bmatrix}\begin{bmatrix} n-\omega \\ d-\delta \end{bmatrix}$, where $\delta = |r-s|$ and $\omega = r$ if $r \geq s$ and $\omega = n-r$ otherwise. We denote the volume of a ball with injection radius t around a subspace with dimension r as $V_{\mathrm{I}}(r,t) \stackrel{\mathrm{def}}{=} \sum_{d=0}^{t}\sum_{s=0}^{n} N_{\mathrm{I}}(r,s,d)$. We derive bounds on $V_{\mathrm{I}}(r,t)$ below.

Proposition 5.41. *For all q, n, r, and $t \leq \nu$, $q^{t(n-t)} \leq V_{\mathrm{I}}(r,t) < N_q(2N_q - 1)K_q^{-2}q^{t(n-t)}$, where $N_q = \sum_{i=0}^{\infty} q^{-i^2}$.*

The proof of Proposition 5.41 is given in Appendix 7.4.5. We remark that the bounds in Proposition 5.41 are tight up to a scalar, which will greatly facilitate our asymptotic studies of subspace codes with the injection metric. Also, these bounds

do not depend on r, which differs from the bounds on the volume of a ball with subspace radius in Proposition 5.27. This illustrates a clear geometric distinction between the two metrics.

We now prove a technical upper bound on the volume of spheres, which will be instrumental in Section 5.6.2.

Lemma 5.42. *For all r and s, let $\delta = |r-s|$ and $\omega = r$ if $r \geq s$ and $\omega = n - r$ otherwise. Then for all $t \leq \min\left\{r+s, \frac{n}{2}\right\}$, $\sum_{d=0}^{t} N_{\mathrm{I}}(r,s,d) < K_q^{-2} N_q q^{g(t)}$, where $g(d) = d(n+\delta-d) - \delta(n-\omega+\delta)$ and $N_q = \sum_{i=0}^{\infty} q^{-i^2}$.*

Proof. We have $N_{\mathrm{I}}(r,s,d) = q^{d(d-\delta)} \begin{bmatrix} \omega \\ d \end{bmatrix} \begin{bmatrix} n-\omega \\ d-\delta \end{bmatrix} < K_q^{-2} q^{g(d)}$ by Corollary 2.3, and hence $\sum_{d=0}^{t} N_{\mathrm{I}}(r,s,d) < K_q^{-2} q^{g(t)} \sum_{i=0}^{t} q^{-i(n+\delta-2t+i)} < K_q^{-2} q^{g(t)} N_q$. □

For all $A \in E_a(q,n), B \in E_b(q,n)$, we denote $J_{\mathrm{I}}(q,n;u,s;A,B,c) = |\{C \in E_c(q,n) : d_{\mathrm{I}}(A,C) = u, d_{\mathrm{I}}(B,C) = s\}|$. Proposition 5.43 below is the counterpart of Theorem 5.28 for the injection metric.

Proposition 5.43. *For all $A \in E_a(q,n), B \in E_b(q,n)$ with $d_{\mathrm{I}}(A,B) = w$, we have $J_{\mathrm{I}}(q,n;u,s;A,B,c) = J_{\mathrm{S}}(q,n;2u-|a-c|, 2s-|b-c|, 2w-|a-b|; a,b,c) = J_{\mathrm{I}}(q,n;u,s,w;a,b,c)$.*

Proof. For any $C \in E_c(q,n)$, $d_{\mathrm{I}}(A,C) = u$ and $d_{\mathrm{I}}(B,C) = s$ if and only if $d_{\mathrm{S}}(A,C) = 2u-|a-c|$ and $d_{\mathrm{S}}(B,C) = 2s-|b-c|$. Therefore, $J_{\mathrm{I}}(q,n;u,s;A,B,c) = J_{\mathrm{S}}(q,n;2u-|a-c|, 2s-|b-c|; A,B,c) = J_{\mathrm{S}}(q,n;2u-|a-c|, 2s-|b-c|, 2w-|a-b|; a,b,c)$ by Theorem 5.28, which is a function of q, n, u, s, w, a, b, and c. □

Corollary 5.44. *For all parameter values,*

$$N_{\mathrm{I}}(a,b,w) J_{\mathrm{I}}(q,n;u,s,w;a,b,c) = N_{\mathrm{I}}(a,c,u) J_{\mathrm{I}}(q,n;w,s,u;a,c,b), \quad (5.11)$$

$$\sum_{u=0}^{n} J_{\mathrm{I}}(q,n;u,s,w;a,b,c) = N_{\mathrm{I}}(b,c,s). \quad (5.12)$$

The proof of Corollary 5.44 is similar to that of Corollary 5.29 and is hence omitted. Although the value of $J_{\mathrm{I}}(q,n;u,s,w;a,b,c)$ is unknown in general, we have $J_{\mathrm{I}}(q,n;u,s,w;a,a,a) = J_{\mathrm{C}}(q,n,a,u,s,w)$. We also determine a special value below.

Proposition 5.45. *For all* $u \leq \min\left\{\max\{a,c\}, \frac{3a-c+|a-c|}{2}\right\}$, $s \leq \min\left\{\max\{a,c\}, \frac{3a-c+|a-c|}{2}\right\}$, *such that* $u+s-|a-c| \leq \min\left\{a, \frac{n}{2}\right\}$, $J_{\mathrm{I}}(q,n;u,s,w;a,a,c) = 0$ *for* $w > u+s-|a-c|$ *and*

$$J_{\mathrm{I}}(q,n;u,s,u+s-|a-c|;a,a,c) = \begin{bmatrix} u+s-|a-c| \\ u \end{bmatrix} \begin{bmatrix} u+s-|a-c| \\ s \end{bmatrix}. \quad (5.13)$$

Proof. By Proposition 5.43, $J_{\mathrm{I}}(q,n;u,s,w;a,a,c) = J_{\mathrm{S}}(q,n;2u-|a-c|,2s-|a-c|,2w;a,a,c)$. For $w > u+s-|a-c|$, we have $2w > 2u-|a-c|+2s-|a-c|$, and hence $J_{\mathrm{S}}(q,n;2u-|a-c|,2s-|a-c|,2w;a,a,c) = 0$. (5.13) then follows Proposition 5.30. □

5.5.2 Packing properties of subspace codes with the injection metric

We are interested in packing subspace codes used with the injection metric. The maximum cardinality of a code in $E(q,n)$ with minimum injection distance d is denoted as $A_{\mathrm{I}}(q,n,d)$. Since $A_{\mathrm{I}}(q,n,1) = |E(q,n)|$, we assume $d \geq 2$ henceforth. When $d > \nu$, the maximum cardinality of a code with minimum injection distance d is determined and a code with maximum cardinality is given. For all $J \subseteq \{0,1,\ldots,n\}$, we denote the maximum cardinality of a code with minimum injection distance d and codewords having dimensions in J as $A_{\mathrm{I}}(q,n,d,J)$. For $2 \leq d \leq \nu$, we denote $Q_d = \{d, d+1, \ldots, n-d\}$.

Proposition 5.46. *For $d > \nu$, $A_{\mathrm{I}}(q,n,d) = 2$ and for $2 \le d \le \nu$, $A_{\mathrm{I}}(q,n,d) = A_{\mathrm{I}}(q,n,d,Q_d) + 2$.*

Proof. Let $\mathcal{C}$ be a code in $E(q,n)$ with minimum injection distance d and let $C, D \in \mathcal{C}$. We have $\max\{\dim(C), \dim(D)\} = d_{\mathrm{I}}(C,D) + \dim(C \cap D) \ge d$, therefore there is at most one codeword with dimension less than d. Also, $\min\{\dim(C), \dim(D)\} = \dim(C+D) - d_{\mathrm{I}}(C,D) \le n - d$, therefore there is at most one codeword with dimension greater than $n-d$. Thus $A_{\mathrm{I}}(q,n,d) \le 2$ for $d > \nu$ and $A_{\mathrm{I}}(q,n,d) \le A_{\mathrm{I}}(q,n,d,Q_d) + 2$ for $d \le \nu$. Also, adding $\{\mathbf{0}\}$ and $\mathrm{GF}(q)^n$ to a code with minimum distance $d \le \nu$ and codewords of dimensions in Q_d does not decrease the minimum distance. Thus $A_{\mathrm{I}}(q,n,d) = A_{\mathrm{I}}(q,n,d,Q_d) + 2$ for $d \le \nu$. Similarly, the code $\{\{\mathbf{0}\}, \mathrm{GF}(q)^n\}$ has minimum distance n and hence $A_{\mathrm{I}}(q,n,d) = 2$ for $d > \nu$. □

Lemma 5.47 below relates $A_{\mathrm{I}}(q,n,d)$ to $A_{\mathrm{S}}(q,n,d)$ and $A_{\mathrm{C}}(q,n,r,d)$.

Lemma 5.47. *For all q, n, and $2 \le d \le \nu$, $A_{\mathrm{S}}(q,n,2d-1) \le A_{\mathrm{I}}(q,n,d) \le A_{\mathrm{S}}(q,n,d)$ and for $d \ge \frac{n}{3}$, $A_{\mathrm{I}}(q,n,d) \le A_{\mathrm{S}}(q,n,4d-n,Q_d) + 2$. Also,*

$$\max_{d \le r \le \nu} A_{\mathrm{C}}(q,n,r,d) \le A_{\mathrm{I}}(q,n,d) \le 2 + \sum_{r=d}^{n-d} A_{\mathrm{C}}(q,n,r,d).$$

Proof. A code with minimum subspace distance $2d-1$ has minimum injection distance $\ge d$ by (4.4) and hence $A_{\mathrm{S}}(q,n,2d-1) \le A_{\mathrm{I}}(q,n,d)$. Similarly, a code with minimum injection distance d has minimum subspace distance $\ge d$ and hence $A_{\mathrm{I}}(q,n,d) \le A_{\mathrm{S}}(q,n,d)$.

Let $\mathcal{C}$ be a code with minimum injection distance d whose codewords have dimensions in Q_d. For all codewords U and V, $d_{\mathrm{S}}(U,V) = 2d_{\mathrm{I}}(U,V) - |\dim(U) - \dim(V)| \ge 2d - (n-2d)$. Thus $\mathcal{C}$ has subspace distance $4d - n \ge d$ for $d \ge \frac{n}{3}$,

and hence $A_{\mathrm{I}}(q,n,d,Q_d) \leq A_{\mathrm{S}}(q,n,4d-n,Q_d)$. Proposition 5.46 finally yields $A_{\mathrm{I}}(q,n,d) = A_{\mathrm{I}}(q,n,d,Q_d)+2 \leq A_{\mathrm{S}}(q,n,4d-n,Q_d)+2$.

Any CDC in $E_r(q,n)$ with minimum distance d is a subspace code with minimum injection distance d, hence $A_{\mathrm{C}}(q,n,r,d) \leq A_{\mathrm{I}}(q,n,d)$ for all r. Also, the codewords with dimension r in a subspace code with minimum distance d form a CDC in $E_r(q,n)$ with minimum distance at least d, hence $A_{\mathrm{I}}(q,n,d) = A_{\mathrm{I}}(q,n,d,Q_d)+2 \leq 2+\sum_{r=d}^{n-d} A_{\mathrm{C}}(q,n,r,d)$. □

Proposition 5.48. *For $2 \leq d \leq r \leq \nu$,*

$$q^{(\nu-r)(r-d+1)} A_{\mathrm{C}}\left(q,n,r,d\right) \leq A_{\mathrm{I}}(q,n,d) < 2K_q^{-1} N_q q^{(\nu-r)(r-d+1)} A_{\mathrm{C}}\left(q,n,\nu,d\right), \tag{5.14}$$

where $N_q = \sum_{i=0}^{\infty} q^{-i^2}$.

The proof of Proposition 5.48 is similar to that of Proposition 5.32 and is hence omitted. Proposition 5.48 indicates that CDCs with constant dimension half of n are optimal subspace codes with the injection codes up to a scalar. Therefore, these codes can be used for either error correction with network coding and for error correction against adversarial channels. We can hence determine the asymptotic maximum rate $a_{\mathrm{I}}(d') = \limsup_{n\to\infty} \frac{\log_q A_{\mathrm{I}}(q,n,r,d)}{\log_q |E(q,n)|}$ of a subspace code used with the injection metric.

Proposition 5.49. *For $0 \leq d' \leq \frac{1}{2}$, $a_{\mathrm{I}}(d') = 1-2d'$. For $\frac{1}{2} \leq d' \leq 1$, $a_{\mathrm{I}}(d') = 0$.*

Proposition 5.48 also indicates that using CDCs with dimension r leads to a decrease in cardinality on the order of $q^{(\nu-r)(\nu-r+d-1)}$, i.e., a decrease in rate on the order of $(1-2r')(2d'+1-2r')$.

We finish our discussion of packing subspace codes with the injection metric with more bounds on $A_{\mathrm{I}}(q,n,d)$. Proposition 5.50 below is the analogue of Proposition 5.34 for the injection metric and its proof is hence omitted.

Proposition 5.50. *For all q, n, $2 \leq d \leq \nu$, and any permutation π of $\{0,1,\ldots,n\}$, there exists a code with minimum injection distance d and $A_{\pi(r)}$ codewords with dimension $\pi(r)$ for $0 \leq r \leq n$, where $A_{\pi(0)} = A_{\mathrm{C}}(q,n,\pi(0),d)$ and*

$$A_{\pi(r)} = \max\left\{0, \left\lceil \frac{\begin{bmatrix} n \\ \pi(r) \end{bmatrix} - \sum_{i=0}^{r-1} A_{\pi(i)} \sum_{e=0}^{d-1} N_{\mathrm{I}}(\pi(i),\pi(r),e)}{\sum_{e=0}^{d-1} N_{\mathrm{I}}(\pi(r),\pi(r),e)} \right\rceil \right\}. \tag{5.15}$$

By extending the puncturing of subspaces introduced in [9], we finally derive below a Singleton bound for injection metric codes.

Proposition 5.51. *For all q, n, and $2 \leq d \leq \nu$, $A_{\mathrm{I}}(q,n,d) \leq A_{\mathrm{I}}(q,n-1,d-1) \leq \sum_{r=0}^{n-d+1} \begin{bmatrix} n-d+1 \\ r \end{bmatrix}$.*

Proof. We define the puncturing $H(V)$ from $E(q,n)$ to $E(q,n-1)$ as follows. First, we fix W, a subspace of $\mathrm{GF}(q)^n$ of dimension $n-1$. If $\dim(V) = 0$, then $\dim(H(V)) = 0$; otherwise, if $\dim(V) = r > 0$, then $H(V)$ is a fixed $(r-1)$-subspace of $V \cap W$. For all $U, V \in E(q,n)$, it is easily shown that $d_{\mathrm{I}}(H(U),H(V)) \geq d_{\mathrm{I}}(U,V) - 1$, and hence $H(U) \neq H(V)$ if $d_{\mathrm{I}}(U,V) \geq 2$.

Therefore, if $\mathcal{C}$ is a code in $E(q,n)$ with minimum injection distance $d \geq 2$, then $\{H(V) : V \in \mathcal{C}\}$ is a code in $E(q,n-1)$ with minimum injection distance $\geq d-1$ and cardinality $|\mathcal{C}|$. The first inequality follows. Applying it $d-1$ times yields $A_{\mathrm{I}}(q,n,d) \leq A_{\mathrm{I}}(q,n-d+1,1) = \sum_{r=0}^{n-d+1} \begin{bmatrix} n-d+1 \\ r \end{bmatrix}$. □

5.5.3 Covering properties of subspace codes with the injection metric

We now consider the covering properties of subspace codes with the injection metric. The injection covering radius of $\mathcal{C} \subseteq E(q,n)$ is defined as $\max_{U \in E(q,n)} d_{\mathrm{I}}(U, \mathcal{C})$. We denote the minimum cardinality of a subspace code in $E(q,n)$ with injection covering radius ρ as $K_{\mathrm{I}}(q,n,\rho)$. Since $K_{\mathrm{I}}(q,n,0) = |E(q,n)|$ and $K_{\mathrm{I}}(q,n,n) = 1$, we assume $0 < \rho < n$ henceforth. When $\rho \geq \nu$, we determine the minimum cardinality of a code with injection covering radius ρ.

Proposition 5.52. *For $n - \nu \leq \rho < n$, $K_{\mathrm{I}}(q,n,\rho) = 1$. If $n = 2\nu + 1$, then $K_{\mathrm{I}}(q, 2\nu+1, \nu) = 2$.*

Proof. Let C be a subspace with dimension ν. Then for all D_1 with $\dim(D_1) \leq \dim(C)$, we have $d_{\mathrm{I}}(C, D_1) \leq \dim(C) = \nu$ by (4.2); similarly, for all D_2 with $\dim(D_2) \geq \dim(C) + 1$, we have $d_{\mathrm{I}}(C, D_2) \leq n - \dim(C) = n - \nu$ by (4.3). Thus C covers $E(q,n)$ with radius $n - \nu$ and $K_{\mathrm{I}}(q,n,\rho) = 1$ for $n - \nu \leq \rho < n$.

If $n = 2\nu + 1$, then it is easily shown that $\{C, C^{\perp}\}$ has covering radius ν, and hence $K_{\mathrm{I}}(q, 2\nu+1, \nu) \leq 2$. However, for any $D \in E(q, 2\nu+1)$, then either $d_{\mathrm{I}}(\{\mathbf{0}\}, D) > \nu$ or $d_{\mathrm{I}}(\mathrm{GF}(q)^n, D) > \nu$. Thus no subspace can cover the projective space with radius ν and $K_{\mathrm{I}}(q, 2\nu+1, \nu) \geq 2$. □

We thus consider $0 < \rho < \nu$ henceforth. Lemma 5.53 relates $K_{\mathrm{I}}(q,n,\rho)$ to $K_{\mathrm{S}}(q,n,\rho)$ and $K_{\mathrm{C}}(q,n,r,\rho)$.

Lemma 5.53. *For all q, n, and $0 < \rho < \nu$, $K_{\mathrm{S}}(q,n,2\rho) \leq K_{\mathrm{I}}(q,n,\rho) \leq K_{\mathrm{S}}(q,n,\rho)$ and $K_{\mathrm{I}}(q,n,\rho) \leq 2 + \sum_{r=\rho+1}^{n-\rho-1} K_{\mathrm{C}}(q,n,r,\rho)$.*

Proof. A code with injection covering radius ρ has subspace covering radius $\leq 2\rho$, hence $K_{\mathrm{S}}(q,n,2\rho) \leq K_{\mathrm{I}}(q,n,\rho)$. Also, a code with subspace covering radius ρ has injection covering radius $\leq \rho$, hence $K_{\mathrm{I}}(q,n,\rho) \leq K_{\mathrm{S}}(q,n,\rho)$. The last inequality is trivial. □

Proposition 5.54 below is the analogue of Proposition 5.36 for the injection metric.

Proposition 5.54. *For all q, n, and $0 < \rho < \nu$, $K_{\mathrm{I}}(q,n,\rho) \geq \min \sum_{i=0}^{n} A_i$, where the minimum is taken over all integer sequences $\{A_i\}$ satisfying $0 \leq A_i \leq \begin{bmatrix} n \\ i \end{bmatrix}$ for all $0 \leq i \leq n$ and $\sum_{i=0}^{n} A_i \sum_{d=0}^{\rho} N_{\mathrm{I}}(i,r,d) \geq \begin{bmatrix} n \\ r \end{bmatrix}$ for $0 \leq r \leq n$.*

Proposition 5.55 below parallels Proposition 5.37. Its proof is a direct application of [37, Theorem 12.2.1], and is hence omitted.

Proposition 5.55. $K_{\mathrm{I}}(q,n,\rho) \leq \frac{|E(q,n)|}{\min_{0\leq r\leq n} V_{\mathrm{I}}(r,\rho)} \left[1 + \ln\left(\max_{0\leq r\leq n} V_{\mathrm{I}}(r,\rho)\right)\right]$.

We finally determine the asymptotic behavior of $K_{\mathrm{I}}(q,n,\rho)$ by using the asymptotic rate $k_{\mathrm{I}}(\rho') = \liminf_{n\to\infty} \frac{\log_q K_{\mathrm{I}}(q,n,\rho)}{\log_q |E(q,n)|}$.

Proposition 5.56. *For $0 \leq \rho' \leq \frac{1}{2}$, $k_{\mathrm{I}}(\rho') = (1-2\rho')^2$. For $\frac{1}{2} \leq \rho' \leq 1$, $k_{\mathrm{I}}(\rho') = 0$.*

Proof. By Proposition 5.52, $k_{\mathrm{I}}(\rho') = 0$ for $\frac{1}{2} \leq \rho' \leq 1$. We have $K_{\mathrm{I}}(q,n,\rho) \geq \frac{|E(q,n)|}{\max_{0\leq r\leq n} V_{\mathrm{I}}(r,\rho)} > \frac{K_q^2}{N_q(2N_q-1)} q^{\nu(n-\nu)-\rho(n-\rho)}$ by Lemma 5.24 and Proposition 5.41. This asymptotically becomes $k_{\mathrm{I}}(\rho') \geq (1-2\rho')^2$ for $0 \leq \rho' \leq \frac{1}{2}$. Similarly, Proposition 5.55, Lemma 5.24, and Proposition 5.41 yield

$$K_{\mathrm{I}}(q,n,\rho) < 2K_q^{-1} N_q q^{\nu(n-\nu)-\rho(n-\rho)} \left[1 + \ln(N_q(2N_q-1)K_q^{-2}) + \rho(n-\rho)\ln q\right]$$

which asymptotically becomes $k_{\mathrm{I}}(\rho') \leq (1-2\rho')^2$ for $0 \leq \rho' \leq \frac{1}{2}$. □

Proposition 5.56 shows that asymptotically optimal covering codes in the injection metric can be constructed from covering CDCs.

5.6 DEP of CDCs used over a symmetric operator channel

5.6.1 DEP of CDCs using a bounded subspace distance decoder

We study the DEP of a CDC in $E_r(q,n)$ using a bounded subspace distance decoder in $E(q,n)$ over a *symmetric operator channel*, defined below. Without loss of generality, we assume $2r \leq n$ as in [9]. An operator channel is a channel where the inputs and outputs are subspaces in $E(q,n)$. As assumed in [9], the channel may erase some dimensions of the transmitted subspace as well as inject some erroneous dimensions. We refer to these as erasures and errors, respectively. If the input has dimension r and ϵ errors and ρ erasures occur, the output has dimension $v = r - \epsilon + \rho$ and is at subspace distance $u = \epsilon + \rho$ from the input. We refer to an operator channel as a *symmetric operator channel* when all outputs corresponding to ϵ errors and ρ erasures are equiprobable. Since the dimension of the output and its subspace distance from the transmitted subspace are both determined by ϵ and ρ, a symmetric operator channel implies that all outputs with the same dimension and at the same subspace distance from the input are equiprobable, and vice versa.

The code $\mathcal{C} \in E_r(q,n)$ has minimum subspace distance $2d$, and given any subspaces at subspace distance up to $d-1$ from the codeword, a bounded distance decoder will produce the codeword. Thus, the DEP of the bounded distance decoder depends on both ϵ and ρ, or equivalently on both u and v. The bounded subspace distance decoder will result in a failure when $v < r-d+1$ or $v > r+d-1$. The DEP depends on both ϵ and ρ, or equivalently on both u and v. The decoder

decodes correctly if and only if $u \leq d-1$, and returns a failure for $u = d$. The DEP when $u \geq d+1$ and $r-d+1 \leq v \leq r+d-1$ is based on the distance distribution of the code, denoted as $A_w(C) = |\{D \in \mathcal{C} : d_{\mathrm{I}}(D, C) = w\}| = |\{D \in \mathcal{C} : d_{\mathrm{S}}(D, C) = 2w\}|$.

Proposition 5.57. *When $u \geq d+1$ and $r-d+1 \leq v \leq r+d-1$, the DEP of a bounded subspace distance decoder for a CDC in $E_r(q, n)$ with minimum subspace distance $2d$ over a symmetric operator channel is given by*

$$P_{\mathrm{S}}(C, u, v) = \frac{1}{N_{\mathrm{S}}(r, v, u)} \sum_{w=d}^{r} A_w(C) \sum_{s=0}^{d-1} J_{\mathrm{S}}(q, n; u, s, 2w; r, r, v). \tag{5.16}$$

Furthermore, if the CDC is the lifting of a rank metric code, then

$$\begin{aligned} P_{\mathrm{S}}(I(\mathbf{C}), u, v) &\leq \frac{1}{N_{\mathrm{S}}(r, v, u)} \sum_{w=d}^{r} \begin{bmatrix} r \\ w \end{bmatrix} \alpha(n-r, w-d+1) \\ &\quad \sum_{s=0}^{d-1} J_{\mathrm{S}}(q, n; u, s, 2w; r, r, v) \qquad (5.17) \\ &< K_q^{-3} L_q q^{-\tau(n-r-v+\tau)}, \qquad (5.18) \end{aligned}$$

where $\tau = \frac{d-1+v-r}{2}$.

Proof. We have $P_{\mathrm{S}}(C, u, v) = \frac{D(C,u,v)}{N_{\mathrm{S}}(r,v,u)}$, where $D(C, u, v)$ is the number of decodable subspaces with dimension v and at subspace distance u from C. For a codeword C' at subspace distance $2w$ from C, there are exactly $\sum_{s=0}^{d-1} J_{\mathrm{S}}(q, n; u, s, 2w; r, r, v)$ subspaces with dimension v, at distance u from C, and at distance $\leq d-1$ from C' by Theorem 5.28. Summing for all C', we obtain (5.16).

Let $I(\mathcal{C})$ be the lifting of a rank metric code $\mathcal{C}$ in $\mathrm{GF}(q)^{r \times (n-r)}$. For $\mathbf{C} \in \mathcal{C}$, $\{I(\mathbf{D} - \mathbf{C}) : \mathbf{D} \in \mathcal{C}, d_{\mathrm{R}}(\mathbf{D}, \mathbf{C}) = w\}$ is the lifting of a CRC in $\mathrm{GF}(q)^{r \times (n-r)}$ with minimum rank distance at least d and rank w, and hence $A_w(I(\mathbf{C})) \leq A_{\mathrm{R}}(q, n-r, r, d, w) \leq \begin{bmatrix} r \\ w \end{bmatrix} \alpha(n-r, w-d+1)$ by Proposition 4.11, which leads to (5.17). By

(4.21),

$$A_w(I(\mathbf{C})) < K_q^{-1} q^{-(n-r)(d-1)} N_{\mathrm{S}}(r, r, 2w). \tag{5.19}$$

We obtain

$$\begin{aligned} P_{\mathrm{S}}(I(\mathbf{C}), u, v) &= \sum_{w=d}^{r} A_w(I(\mathbf{C})) \sum_{s=0}^{d-1} \frac{J_{\mathrm{S}}(q, n; 2w, s, u; r, v, r)}{N_{\mathrm{S}}(r, r, 2w)} && (5.20) \\ &< K_q^{-1} q^{-(n-r)(d-1)} \sum_{w=d}^{r} \sum_{s=0}^{d-1} J_{\mathrm{S}}(q, n; 2w, s, u; r, v, r) && (5.21) \\ &\leq K_q^{-1} q^{-(n-r)(d-1)} \sum_{s=0}^{d-1} N_{\mathrm{S}}(v, r, s) && (5.22) \\ &< K_q^{-3} L_q q^{\frac{d-1}{2}\left(2r-n-\frac{d-1}{2}\right)-\frac{v-r}{2}\left(n-2r-\frac{v-r}{2}\right)}, && (5.23) \end{aligned}$$

where (5.20), (5.21), (5.22), and (5.23) follow (5.5), (5.19), (5.6), and Lemma 5.26, respectively. □

We remark that the bound in (5.18) is trivial for $v = r - d + 1$ or $r = \frac{n}{2}$ and $v = \frac{n}{2} - d + 1$. This is due to the fact that CDCs in $E_r(q, n)$ with minimum subspace distance $2d$ and maximum cardinality produce asymptotically tight packings of $E_{r-d+1}(q, n)$, and CDCs in $E_{\frac{n}{2}}(q, n)$ with maximum cardinality produce asymptotically tight packings of $E_{\frac{n}{2}-d+1}(q, n)$.

We now show that liftings of MRD codes have the highest DEP among all liftings up to a scalar in all nontrivial cases. We denote the DEP of the lifting of an MRD code in $\mathrm{GF}(q)^{r\times(n-r)}$ with minimum rank distance d as $P_{\mathrm{S,MRD}}(u, v)$.

Corollary 5.58. *Let $\mathcal{C}$ be any rank metric code in $\mathrm{GF}(q)^{r\times(n-r)}$ ($r \leq n - r$) with minimum rank distance d and let $\mathbf{C} \in \mathcal{C}$. Then if $q > 2$, $r < n-r$, or $d \neq n-r-1$, $P_{\mathrm{S}}(I(\mathbf{C}), u, v) < H_q P_{\mathrm{S,MRD}}(u, v)$, where $H_2 = 3.5$ and $H_q = \frac{q-1}{q-2}$ for $q > 2$.*

The proof of Corollary 5.58 is similar to that of Corollary 4.25 and is hence omitted. If the probability that the received subspace is at subspace distance u from

the sent codeword decreases rapidly with u, then the overall DEP is dominated by $P_{\mathrm{S}}(C, d+1, v)$. Proposition 5.59 below determines this value, and shows that it asymptotically reaches the upper bound in (5.18) for liftings of MRD codes.

Proposition 5.59. *The DEP of a CDC in $E_r(q,n)$ with minimum subspace distance $2d$ using a bounded subspace distance decoder over a symmetric operator channel, provided the received subspace is at subspace distance $d+1$ from the sent codeword, is given by*

$$P_{\mathrm{S}}(C, d+1, v) = q^{-(d-\tau)(\tau+1)} \frac{\begin{bmatrix} d \\ \tau \end{bmatrix} \begin{bmatrix} d \\ \tau+1 \end{bmatrix}}{\begin{bmatrix} r \\ d-\tau \end{bmatrix} \begin{bmatrix} n-r \\ \tau+1 \end{bmatrix}} A_d(C). \tag{5.24}$$

In particular, the DEP of the lifting of an MRD code satisfies $P_{\mathrm{S,MRD}}(d+1, v) > K_q^2 q^{-\tau(n-r-v+\tau)}$.

The proof of Proposition 5.59 is similar to that of Proposition 4.26 and is hence omitted. Proposition 5.59 and (5.18) indicate that when the received subspace has dimension $v \leq r$, the DEP of a lifting of an MRD code in $\mathrm{GF}(q)^{r\times(n-r)}$ with minimum rank distance d is on the same order of that of its puncturing in $\mathrm{GF}(q)^{v\times(n-r)}$ with minimum distance $d+v-r$.

We remark that on a symmetric operator channel, all outputs with the same dimension and at the same subspace distance from the input are equiprobable. Note that if we assume that all channel outputs with the same distance to the transmitted subspace are equiprobable, it implies a symmetric operator channel and thus the results derived above for the symmetric operator channel still hold.

5.6.2 DEP of CDCs using a bounded injection distance decoder

We now study the DEP of a CDC using a bounded injection distance decoder over a symmetric operator channel. Again since the dimension of the output and its injection distance from the transmitted subspace are both determined by ϵ and ρ, a symmetric operator channel implies that all outputs with the same dimension $v = r + \epsilon - \rho$ and at the same injection distance $\mu = \max\{\epsilon, \rho\}$ from the input are equiprobable, and vice versa.

The DEP of a bounded distance decoder depends on both μ and v. The code has minimum injection distance d and can correct subspaces at injection distance up to $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ from the codeword. As a result, the bounded injection distance decoder produces a failure if $v < r - t$ or $v > r + t$. The decoder decodes correctly if and only if $\mu \leq t$, and returns a failure for $t < \mu < d - t$. We determine below the DEP for $\mu \geq d - t$.

Proposition 5.60. *The DEP of using a bounded injection distance decoder for a CDC in $E_r(q, n)$ with minimum injection distance d over a symmetric operator channel is given by $P_{\mathrm{I}}(C, \mu, v) = 0$ for $\mu < d - t + |r - v|$ and*

$$P_{\mathrm{I}}(C, \mu, v) = \frac{1}{N_{\mathrm{I}}(r, v, \mu)} \sum_{w=d}^{r} A_w(C) \sum_{s=0}^{t} J_{\mathrm{I}}(q, n; \mu, s, w; r, r, v) \tag{5.25}$$

otherwise. Furthermore, if the CDC is the lifting of a rank metric code, then

$$\begin{aligned} P_{\mathrm{I}}(I(\mathbf{C}), \mu, v) &\leq \frac{1}{N_{\mathrm{I}}(r, v, \mu)} \sum_{w=d}^{r} \begin{bmatrix} r \\ w \end{bmatrix} \alpha(n - r, w - d + 1) \\ &\quad \sum_{s=0}^{t} J_{\mathrm{I}}(q, n; \mu, s, w; r, r, v) \qquad (5.26) \\ &< K_q^{-3} N_q q^{-t(n-2r-\delta+t)-\delta(n-\omega+\delta)}, \qquad (5.27) \end{aligned}$$

where $\delta = |r - v|$ *and* $\omega = v$ *if* $v \geq r$ *and* $\omega = n - v$ *otherwise.*

Proof. The proofs of (5.25) and (5.26) are similar to those of (5.16) and (5.17), respectively, and are hence omitted. Since $N_{\mathrm{I}}(r, r, w) = N_{\mathrm{S}}(r, r, 2w)$, (5.19) yields

$$A_w(I(\mathbf{C})) < K_q^{-1} q^{-(n-r)(d-1)} N_{\mathrm{I}}(r, r, w). \tag{5.28}$$

We obtain

$$\begin{aligned} P_{\mathrm{I}}(I(\mathbf{C}), \mu, v) &= \sum_{w=d}^{r} A_w(I(\mathbf{C})) \sum_{s=0}^{t} \frac{J_{\mathrm{I}}(q, n; w, s, \mu; r, v, r)}{N_{\mathrm{I}}(r, r, w)} && (5.29) \\ &< K_q^{-1} q^{-(n-r)(d-1)} \sum_{w=d}^{r} \sum_{s=0}^{t} J_{\mathrm{I}}(q, n; w, s, \mu; r, v, r) && (5.30) \\ &\leq K_q^{-1} q^{-(n-r)(d-1)} \sum_{s=0}^{t} N_{\mathrm{I}}(v, r, s) && (5.31) \\ &< K_q^{-3} N_q q^{-t(n-2r-\delta+t)-\delta(n-\omega+\delta)}, && (5.32) \end{aligned}$$

where (5.29), (5.30), (5.31), and (5.32) follow (5.11), (5.28), (5.12), and Lemma 5.42, respectively. □

We remark that $\mu \geq d - t + |r - v|$ is equivalent to $\min\{\epsilon, \rho\} \geq d - t$. Therefore, Proposition 5.60 indicates that both $d - t$ errors and $d - t$ erasures have to occur for the bounded injection distance decoder to decode erroneously.

We show below that liftings of MRD codes have the highest maximum decoder error probability up to a scalar for nontrivial cases. We denote the DEP of the lifting of an MRD code in $\mathrm{GF}(q)^{r \times (n-r)}$ with minimum rank distance d as $P_{\mathrm{I,MRD}}(\mu, v)$.

Corollary 5.61. *Let* $\mathcal{C}$ *be a rank metric code in* $\mathrm{GF}(q)^{r \times (n-r)}$ *(*$r \leq n - r$*) with minimum rank distance* d *and let* $\mathbf{C} \in \mathcal{C}$*. Then if* $q > 2$ *or* $r < n - r$ *or* $d \neq n - r - 1$*,* $P_{\mathrm{I}}(I(\mathbf{C}), \mu, v) < H_q P_{\mathrm{I,MRD}}(\mu, v)$*, where* $H_2 = 3.5$ *and* $H_q = \frac{q-1}{q-2}$ *for* $q > 2$*.*

The proof of Corollary 5.61 is similar to that of Corollary 4.25 and is hence omitted. If the probability that the received subspace is at injection distance μ from the sent codeword decreases rapidly with μ, then the overall DEP is dominated by $P_{\mathrm{I}}(C, d-t+\delta, v)$. Proposition 5.62 below determines this value, and shows that it asymptotically reaches the upper bound in (5.27) for liftings of MRD codes.

Proposition 5.62. *The DEP of a CDC in $E_r(q,n)$ with minimum injection distance d using a bounded injection distance decoder over a symmetric operator channel provided the received subspace is at injection distance $\mu = d-t+\delta$ from the sent codeword is given by*

$$P_{\mathrm{I}}(C, d-t+\delta, v) = q^{-(d-t)(d-t+\delta)} \frac{\begin{bmatrix} d \\ t-\delta \end{bmatrix} \begin{bmatrix} d \\ t \end{bmatrix}}{\begin{bmatrix} \omega \\ d-t+\delta \end{bmatrix} \begin{bmatrix} n-\omega \\ d-t \end{bmatrix}} A_d(C). \tag{5.33}$$

In particular, the DEP of the lifting of an MRD code satisfies $P_{\mathrm{M,MRD}}(d-t+\delta, v) > K_q^2 q^{-t(n-2r-\delta+t)-\delta(n-\omega+\delta)}$.

The proof of Proposition 5.62 is similar to that of Proposition 4.26 and is hence omitted.

Chapter 6

Conclusion and Future Work

Conclusion

In this dissertation, we investigated the properties of algebraic codes proposed for error control in random linear network coding, namely rank metric codes, subspace codes, and CDCs.

Chapters 2 and 3 investigated some fundamental properties of rank metric codes. We studied the geometric problems of sphere packing and sphere covering in the rank metric. We determined the solution to the sphere packing problem, and derived the order of the solution to the sphere covering problem. These results provide guidelines on the design of rank metric codes. We also derived the MacWilliams identity and related identities for rank metric codes which parallel the binomial and power moment identities derived for codes with the Hamming metric. These identities are fundamental relationships between linear rank metric codes and their dual.

In Chapter 4, we showed that the problem of determining the cardinality of an

optimal CDC can be solved by studying constant-rank codes instead. Constant-rank codes are also a useful tool to investigate the DEP of rank metric codes. We thus showed that the maximum DEP of rank metric codes used over an equal row or an equal column space channel decreases exponentially with t^2, where t is the error correction capability of the code.

In Chapter 5, we investigated the geometric properties of CDCs and subspace codes. We first constructed a new class of CDCs with cardinalities greater than previously proposed CDCs, and investigated the covering properties of CDCs. We then proved that optimal packing CDCs are nearly optimal packing subspace codes for both metrics. However, optimal covering CDCs can be used to construct asymptotically optimal covering subspace codes only for the injection metric. We finally determined the DEP of any lifting of a rank metric code over a symmetric operator channel and showed that the liftings of MRD codes have the highest DEP among all liftings up to a scalar.

Future work

Random linear network coding is a very promising means to efficiently propagate information through a network. However, it is yet to be implemented for real-life applications. Such implementation would certainly rise previously unconsidered issues on the design of error control codes for random linear network coding. Also, the error correction capability of an error control code depends on the given operator channel. However, the characteristics of the operator channel depend on the network and may change over time, and how to characterize the expected number of errors and erasures due to the operator channel is still unknown.

Our study of rank metric codes leaves many questions open. For instance, we proposed a class of covering codes optimal up to a constant, but only for a limited range of parameters. Outside this range, how to construct covering codes optimal up to a scalar, or even whether the sphere covering bound is tight up to a scalar remain open problems. In a broader sense, the elegance of the theory of the rank metric and the already wide range of applications of rank metric codes suggest that further applications and theoretic significance are still to be discovered for rank metric codes.

Despite an intense research, CDCs remain a young research topic and hence still offer many open problems. New constructions of packing and covering CDCs and bounds on the cardinality of a CDC are crucial for code design. Also, the decoding of previously proposed classes of CDCs is of the highest importance when it comes to applications. Since the proposed constructions of CDCs are based on rank metric codes, the decoding of rank metric codes is also important. Finally, the relation between constant-rank codes and constant-dimension codes needs to be clarified in order to further our understanding of the relation between CDCs and rank metric codes.

Codes in the projective space are in many aspects a thought-provoking problem. Many geometric properties typically encountered in coding theory, such as regularity and distance-regularity, are absent in the projective space. However, we have shown that the projective space offers some regularity, which should be clarified and if possible, taken advantage of. The study of codes in the projective space may also shed light on CDCs and on other coding theoretic problems.

Chapter 7

Appendix

7.1 Appendix of Chapter 2

7.1.1 Proof of Proposition 2.35

We first establish a key lemma.

Lemma 7.1. *If* $\mathbf{z} \in \mathcal{Z}$ *and* $0 < \rho < n$, *then* $|\mathcal{A} \cap B_1(\mathbf{z})| \leq V_{\mathrm{R}}(1) - q^{\rho-1}\begin{bmatrix}\rho\\1\end{bmatrix}$.

Proof. By definition of ρ, there exists $\mathbf{c} \in \mathcal{C}$ such that $d_{\mathrm{R}}(\mathbf{z}, \mathbf{c}) \leq \rho$. By Proposition 2.22, $|B_1(\mathbf{z}) \cap B_{\rho-1}(\mathbf{c})|$ gets its minimal value for $d_{\mathrm{R}}(\mathbf{z}, \mathbf{c}) = \rho$, which is $q^{\rho-1}\begin{bmatrix}\rho\\1\end{bmatrix}$ by Proposition 2.25. A vector at distance $\leq \rho - 1$ from any codeword does not belong to $\mathcal{A}$. Therefore, $B_1(\mathbf{z}) \cap B_{\rho-1}(\mathbf{c}) \subseteq B_1(\mathbf{z})\backslash\mathcal{A}$, and hence $|\mathcal{A} \cap B_1(\mathbf{z})| = |B_1(\mathbf{z})| - |B_1(\mathbf{z})\backslash\mathcal{A}| \leq V_{\mathrm{R}}(1) - |B_1(\mathbf{z}) \cap B_{\rho-1}(\mathbf{c})|$. □

We now give a proof of Proposition 2.35.

Proof. For a code $\mathcal{C}$ with covering radius ρ and $\epsilon \geq 1$,

$$\begin{aligned}
\gamma &\stackrel{\text{def}}{=} \epsilon\left[q^{mn} - |\mathcal{C}|V_{\mathrm{R}}(\rho-1)\right] - (\epsilon-1)\left[|\mathcal{C}|V_{\mathrm{R}}(\rho) - q^{mn}\right] && (7.1)\\
&\leq \epsilon|\mathcal{A}| - (\epsilon-1)|\mathcal{Z}| && (7.2)\\
&\leq \epsilon|\mathcal{A}| - (\epsilon-1)|\mathcal{A}\cap\mathcal{Z}| = \epsilon|\mathcal{A}\backslash\mathcal{Z}| + |\mathcal{A}\cap\mathcal{Z}|,
\end{aligned}$$

where (7.2) follows from $|\mathcal{Z}| \leq |\mathcal{C}|V_{\mathrm{R}}(\rho) - q^{mn}$.

$$\begin{aligned}
\gamma &\leq \sum_{\mathbf{a}\in\mathcal{A}\backslash\mathcal{Z}} E_{\mathcal{C}}(B_1(\mathbf{a})) + \sum_{\mathbf{a}\in\mathcal{A}\cap\mathcal{Z}} E_{\mathcal{C}}(B_1(\mathbf{a})) && (7.3)\\
&= \sum_{\mathbf{a}\in\mathcal{A}} E_{\mathcal{C}}(B_1(\mathbf{a})),
\end{aligned}$$

where (7.3) follows from Lemma 2.33 and $|\mathcal{A}\cap\mathcal{Z}| \leq E_{\mathcal{C}}(\mathcal{A}\cap\mathcal{Z})$.

$$\begin{aligned}
\gamma &\leq \sum_{\mathbf{a}\in\mathcal{A}}\sum_{\mathbf{x}\in B_1(\mathbf{a})\cap\mathcal{Z}} E_{\mathcal{C}}(\{\mathbf{x}\}) && (7.4)\\
&= \sum_{\mathbf{x}\in\mathcal{Z}}\sum_{\mathbf{a}\in B_1(\mathbf{x})\cap\mathcal{A}} E_{\mathcal{C}}(\{\mathbf{x}\}) = \sum_{\mathbf{x}\in\mathcal{Z}} |\mathcal{A}\cap B_1(\mathbf{x})|E_{\mathcal{C}}(\{\mathbf{x}\}),
\end{aligned}$$

where (7.4) follows the fact that the second summation is over disjoint sets $\{\mathbf{x}\}$. By Lemma 7.1, we obtain

$$\begin{aligned}
\gamma &\leq \sum_{\mathbf{x}\in\mathcal{Z}} \left(V_{\mathrm{R}}(1) - q^{\rho-1}\begin{bmatrix}\rho\\1\end{bmatrix}\right) E_{\mathcal{C}}(\{\mathbf{x}\})\\
&= \left(V_{\mathrm{R}}(1) - q^{\rho-1}\begin{bmatrix}\rho\\1\end{bmatrix}\right) E_{\mathcal{C}}(\mathcal{Z})\\
&= \left(V_{\mathrm{R}}(1) - q^{\rho-1}\begin{bmatrix}\rho\\1\end{bmatrix}\right) (|\mathcal{C}|V_{\mathrm{R}}(\rho) - q^{mn}). && (7.5)
\end{aligned}$$

Combining (7.5) and (7.1), we obtain the bound in Proposition 2.35. □

7.1.2 Proof of Corollary 2.36

For $\rho = n-1$, (7.5) becomes $\phi\left[q^{mn} - |\mathcal{C}|V_{\mathrm{R}}(n-2)\right] - (\phi-1)\left[|\mathcal{C}|V_{\mathrm{R}}(n-1) - q^{mn}\right] \leq \left(V_{\mathrm{R}}(1) - q^{n-2}\begin{bmatrix} n-1 \\ 1 \end{bmatrix}\right)(|\mathcal{C}|V_{\mathrm{R}}(n-1) - q^{mn})$. Substituting $\phi = \alpha|\mathcal{C}| - \beta$ and rearranging, we obtain the quadratic inequality in Corollary 2.36.

7.1.3 Proof of Proposition 2.43

Given a radius ρ and a code $\mathcal{C}$, denote the set of vectors in $\mathrm{GF}(q^m)^n$ at distance $> \rho$ from $\mathcal{C}$ as $P_\rho(\mathcal{C})$. To simplify notations, $Q \stackrel{\text{def}}{=} q^{mn}$ and $p_\rho(\mathcal{C}) \stackrel{\text{def}}{=} Q^{-1}|P_\rho(\mathcal{C})|$. Let us denote the set of all codes over $\mathrm{GF}(q^m)$ of length n and cardinality K as S_K. Clearly $|S_K| = \binom{Q}{K}$. The average value of $p_\rho(\mathcal{C})$ for all codes $\mathcal{C} \in S_K$ is given by

$$\begin{aligned}
\frac{1}{|S_K|}\sum_{\mathcal{C}\in S_K} p_\rho(\mathcal{C}) &= \frac{1}{|S_K|}Q^{-1}\sum_{\mathcal{C}\in S_K}|P_\rho(\mathcal{C})| \\
&= \frac{1}{|S_K|}Q^{-1}\sum_{\mathcal{C}\in S_K}\sum_{\mathbf{x}\in F|d_{\mathrm{R}}(\mathbf{x},\mathcal{C})>\rho} 1 \\
&= \frac{1}{|S_K|}Q^{-1}\sum_{\mathbf{x}\in F}\sum_{\mathcal{C}\in S_K|d_{\mathrm{R}}(\mathbf{x},\mathcal{C})>\rho} 1 \\
&= \frac{1}{|S_K|}Q^{-1}\sum_{\mathbf{x}\in F}\binom{Q - V_{\mathrm{R}}(\rho)}{K} \qquad (7.6) \\
&= \binom{Q - V_{\mathrm{R}}(\rho)}{K}\Big/\binom{Q}{K}
\end{aligned}$$

Eq. (7.6) comes from the fact that there are $\binom{Q-V_{\mathrm{R}}(\rho)}{K}$ codes with cardinality K that do not cover $\mathbf{x}$. For all K, there exists a code $\mathcal{C}' \in S_K$ for which $p_\rho(\mathcal{C}')$ is no more than the average, that is:

$$p_\rho(\mathcal{C}') \leq \binom{Q}{K}^{-1}\binom{Q - V_{\mathrm{R}}(\rho)}{K} \leq \left(1 - Q^{-1}V_{\mathrm{R}}(\rho)\right)^K.$$

Let us choose $K = \left\lfloor -\frac{1}{\log_Q(1-Q^{-1}V_{\mathrm{R}}(\rho))}\right\rfloor + 1$ so that $K\log_Q\left(1 - Q^{-1}V_{\mathrm{R}}(\rho)\right) < -1$

and hence $p_\rho(\mathcal{C}') = (1 - Q^{-1}V_{\mathrm{R}}(\rho))^K < Q^{-1}$. It follows that $|P_\rho(\mathcal{C}')| < 1$, and $\mathcal{C}'$ has covering radius at most ρ.

7.1.4 Numerical results

We now present the codes, obtained by computer search, that achieve the tightest upper bounds in Tables 2.1 and 2.2. The finite fields use the default generator polynomials from MATLAB [83]. First, the linear code used to show that $K_{\mathrm{R}}(2, 5, 5, 3) \leq 32$ has a generator matrix given by $\mathbf{G} = (1, \alpha, \alpha^2, 0, 0)$, where α is a primitive element of $\mathrm{GF}(2^5)$. We use the *skip-vector* form [84] to represent the other codes obtained by computer search. The skip-vector form of a code $\mathcal{C} = \{\mathbf{c}_i\}_{i=0}^{K-1}$ over $\mathrm{GF}(q^m)^n$ can be obtained as follows. First, each codeword $\mathbf{c}_i \in \mathrm{GF}(q^m)^n$ is represented by an integer x_i in $[0, q^{mn} - 1]$ according to the lexicographical order. Second, the integers x_i are sorted in ascending order; the resulting integers are denoted as x'_i. Third, calculate y_i defined as $y_0 = x'_0$ and $y_i = x'_i - x'_{i-1} - 1$ for $1 \leq i \leq K - 1$. Fourth, if $y_i = y_{i+1} = \ldots = y_{i+k-1}$, then we write y_i^k.

Below are the codes obtained by the JSL algorithm.

$\mathbf{K_R(2, 2, 2, 1) = 3}$ 0^3

$\mathbf{K_R(2, 3, 3, 1) \leq 16}$ 5 25 66 21 51 9 20 5 85 21 2 25 49 9 84 5

$\mathbf{K_R(2, 4, 3, 2) \leq 7}$ 135 689 34 420 477 522 759

$\mathbf{K_R(2, 4, 4, 1) \leq 722}$ For brevity, the details of this code are omitted. They are available at `http://arxiv.org/PS_cache/cs/pdf/0701/0701098v4.pdf`

Below is the code obtained by a local search algorithm.

$\mathbf{K_R(2, 4, 4, 2) \leq 48}$ 1493 1124 265 285 1030 2524 1366 493 6079 968 2145 848 312 473 1307 712 1088 2274 1380 1114 1028 567 422 1462 699 203 180 4669 146 978 3933 1810 2083 345 354 659 1054 2314 1443 2660 2675 1512 756 1229 95 2144 1624

1148

7.2 Appendix of Chapter 3

The proofs in this section use some well-known properties of Gaussian polynomials [42]: $\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ n-k \end{bmatrix}$, $\begin{bmatrix} n \\ k \end{bmatrix}\begin{bmatrix} k \\ l \end{bmatrix} = \begin{bmatrix} n \\ l \end{bmatrix}\begin{bmatrix} n-l \\ n-k \end{bmatrix}$, and

$$\begin{aligned} \begin{bmatrix} n \\ k \end{bmatrix} &= \begin{bmatrix} n-1 \\ k \end{bmatrix} + q^{n-k}\begin{bmatrix} n-1 \\ k-1 \end{bmatrix} && (7.7)\\ &= q^k\begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} && (7.8)\\ &= \frac{q^n-1}{q^{n-k}-1}\begin{bmatrix} n-1 \\ k \end{bmatrix} && (7.9)\\ &= \frac{q^{n-k+1}-1}{q^k-1}\begin{bmatrix} n \\ k-1 \end{bmatrix}. && (7.10) \end{aligned}$$

7.2.1 Proof of Lemma 3.9

We consider homogeneous polynomials $f(x,y;m) = \sum_{i=0}^{r} f_i y^i x^{r-i}$ and $u(x,y;m) = \sum_{i=0}^{r} u_i y^i x^{r-i}$ of degree r as well as $g(x,y;m) = \sum_{j=0}^{s} g_j y^j x^{s-j}$ and $v(x,y;m) = \sum_{j=0}^{s} v_j y^j x^{s-j}$ of degree s. First, we need a technical lemma.

Lemma 7.2. *If $u_r = 0$, then*

$$\frac{1}{x}(u(x,y;m) * v(x,y;m)) = \frac{u(x,y;m)}{x} * v(x,y;m). \tag{7.11}$$

If $v_s = 0$, then

$$\frac{1}{x}(u(x,y;m) * v(x,y;m)) = u(x,qy;m) * \frac{v(x,y;m)}{x}. \tag{7.12}$$

Proof. Suppose $u_r = 0$. Then $\frac{u(x,y;m)}{x} = \sum_{i=0}^{r-1} u_i y^i x^{r-1-i}$. Hence

$$\begin{aligned}\frac{u(x,y;m)}{x} * v(x,y;m) &= \sum_{k=0}^{r+s-1} \left(\sum_{l=0}^{k} q^{ls} u_l(m) v_{k-l}(m-l) \right) y^k x^{r+s-1-k} \\ &= \frac{1}{x}(u(x,y;m) * v(x,y;m)).\end{aligned}$$

Suppose $v_s = 0$. Then $\frac{v(x,y;m)}{x} = \sum_{j=0}^{s-1} v_j y^j x^{s-1-j}$. Hence

$$\begin{aligned}u(x,qy;m) * \frac{v(x,y;m)}{x} &= \sum_{k=0}^{r+s-1} \left(\sum_{l=0}^{k} q^{l(s-1)} q^l u_l(m) v_{k-l}(m-l) \right) y^k x^{r+s-1-k} \\ &= \frac{1}{x}(u(x,y;m) * v(x,y;m)).\end{aligned}$$

□

We now give a proof of Lemma 3.9.

Proof. In order to simplify notations, we omit the dependence of the polynomials f and g on the parameter m. The proof goes by induction on ν. For $\nu = 0$, the result is trivial. For $\nu = 1$, we have

$$\begin{aligned}&[f(x,y) * g(x,y)]^{(1)} \\ &= \frac{1}{(q-1)x}\big[f(qx,y) * g(qx,y) - f(qx,y) * g(x,y) \\ &+ f(qx,y) * g(x,y) - f(x,y) * g(x,y)\big] \\ &= \frac{1}{(q-1)x}\left[f(qx,y) * (g(qx,y) - g(x,y)) + (f(qx,y) - f(x,y)) * g(x,y)\right] \\ &= f(qx,qy) * \frac{g(qx,y) - g(x,y)}{(q-1)x} + \frac{f(qx,y) - f(x,y)}{(q-1)x} * g(x,y) \qquad (7.13) \\ &= q^r f(x,y) * g^{(1)}(x,y) + f^{(1)}(x,y) * g(x,y), \qquad (7.14)\end{aligned}$$

where (7.13) follows Lemma 7.2.

Now suppose (3.2) is true for $\nu = \bar{\nu}$. In order to further simplify notations, we omit the dependence of the various polynomials in x and y. We have

$$
\begin{aligned}
&(f*g)^{(\bar{\nu}+1)} \\
&= \sum_{l=0}^{\bar{\nu}} \begin{bmatrix} \bar{\nu} \\ l \end{bmatrix} q^{(\bar{\nu}-l)(r-l)} \left[f^{(l)} * g^{(\bar{\nu}-l)} \right]^{(1)} \\
&= \sum_{l=0}^{\bar{\nu}} \begin{bmatrix} \bar{\nu} \\ l \end{bmatrix} q^{(\bar{\nu}-l)(r-l)} \left(q^{r-l} f^{(l)} * g^{(\bar{\nu}-l+1)} + f^{(l+1)} * g^{(\bar{\nu}-l)} \right) \qquad (7.15) \\
&= \sum_{l=0}^{\bar{\nu}} \begin{bmatrix} \bar{\nu} \\ l \end{bmatrix} q^{(\bar{\nu}+1-l)(r-l)} f^{(l)} * g^{(\bar{\nu}-l+1)} + \sum_{l=1}^{\bar{\nu}+1} \begin{bmatrix} \bar{\nu} \\ l-1 \end{bmatrix} q^{(\bar{\nu}+1-l)(r-l+1)} f^{(l)} * g^{(\bar{\nu}-l+1)} \\
&= \sum_{l=1}^{\bar{\nu}} \left(\begin{bmatrix} \bar{\nu} \\ l \end{bmatrix} + q^{\bar{\nu}+1-l} \begin{bmatrix} \bar{\nu} \\ l-1 \end{bmatrix} \right) q^{(\bar{\nu}+1-l)(r-l)} f^{(l)} * g^{(\bar{\nu}-l+1)} \\
&+ q^{(\bar{\nu}+1)r} f * g^{(\bar{\nu}+1)} + f^{(\bar{\nu}+1)} * g \\
&= \sum_{l=0}^{\bar{\nu}+1} \begin{bmatrix} \bar{\nu}+1 \\ l \end{bmatrix} q^{(\bar{\nu}+1-l)(r-l)} f^{(l)} * g^{(\bar{\nu}-l+1)}, \qquad (7.16)
\end{aligned}
$$

where (7.15) follows (7.14), and (7.16) follows (7.7). □

7.2.2 Proof of Lemma 3.12

We consider homogeneous polynomials $f(x,y;m) = \sum_{i=0}^{r} f_i y^i x^{r-i}$ and $u(x,y;m) = \sum_{i=0}^{r} u_i y^i x^{r-i}$ of degree r as well as $g(x,y;m) = \sum_{j=0}^{s} g_j y^j x^{s-j}$ and $v(x,y;m) = \sum_{j=0}^{s} v_j y^j x^{s-j}$ of degree s. First, we need a technical lemma.

Lemma 7.3. *If $u_0 = 0$, then*

$$\frac{1}{y}(u(x,y;m)) * v(x,y;m)) = q^s \frac{u(x,y;m)}{y} * v(x,y;m-1). \qquad (7.17)$$

If $v_0 = 0$, then

$$\frac{1}{y}(u(x,y;m) * v(x,y;m)) = u(x,qy;m) * \frac{v(x,y;m)}{y}. \qquad (7.18)$$

Proof. Suppose $u_0 = 0$. Then $\frac{u(x,y;m)}{y} = \sum_{i=0}^{r-1} u_{i+1} x^{r-1-i} y^i$. Hence

$$\begin{aligned} q^s \frac{u(x,y;m)}{y} * v(x,y;m-1) &= q^s \sum_{k=0}^{r+s-1} \left(\sum_{l=0}^{k} q^{ls} u_{l+1} v_{k-l}(m-1-l) \right) x^{r+s-1-k} y^k \\ &= q^s \sum_{k=1}^{r+s} \left(\sum_{l=1}^{k} q^{(l-1)s} u_l v_{k-l}(m-l) \right) x^{r+s-k} y^{k-1} \\ &= \frac{1}{y}(u(x,y;m) * v(x,y;m)). \end{aligned}$$

Suppose $v_0 = 0$. Then $\frac{v(x,y;m)}{y} = \sum_{j=0}^{s-1} v_{j+1} x^{s-1-j} y^j$. Hence

$$\begin{aligned} u(x,qy;m) * \frac{v(x,y;m)}{y} &= \sum_{k=0}^{r+s-1} \left(\sum_{l=0}^{k} q^{l(s-1)} q^l u_l v_{k-l+1}(m-l) \right) x^{r+s-1-k} y^k \\ &= \sum_{k=1}^{r+s} \left(\sum_{l=0}^{k-1} q^{ls} u_l v_{k-l}(m-l) \right) x^{r+s-k} y^{k-1} \\ &= \frac{1}{y}(u(x,y;m) * v(x,y;m)). \end{aligned}$$

□

We now give a proof of Lemma 3.12.

Proof. The proof goes by induction on ν, and is similar to that of Lemma 3.9. For $\nu = 0$, the result is trivial. For $\nu = 1$ we can easily show, by using Lemma 7.3, that

$$[f(x,y;m) * g(x,y;m)]^{\{1\}} = f(x,y;m) * g^{\{1\}}(x,y;m) + q^s f^{\{1\}}(x,y;m) * g(x,y;m-1). \tag{7.19}$$

It is thus easy to verify the claim by induction on ν. □

7.2.3 Proof of Proposition 3.19

Proof. It was shown in [46] that the q-Krawtchouk polynomials are the only solutions to the recurrence

$$P_{j+1}(i+1;m+1,n+1) = q^{j+1} P_{j+1}(i+1;m,n) - q^j P_j(i;m,n) \tag{7.20}$$

with initial conditions $P_j(0;m,n) = \begin{bmatrix} n \\ j \end{bmatrix} \alpha(m,j)$. Clearly, our polynomials satisfy these initial conditions. We hence show that $P_j(i;m,n)$ satisfy the recurrence in (7.20). We have

$$
\begin{aligned}
&P_{j+1}(i+1;m+1,n+1) \\
&= \sum_{l=0}^{i+1} \begin{bmatrix} i+1 \\ l \end{bmatrix} \begin{bmatrix} n-i \\ j+1-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(m+1-l, j+1-l) \\
&= \sum_{l=0}^{i+1} \begin{bmatrix} i+1 \\ l \end{bmatrix} \begin{bmatrix} m+1-l \\ j+1-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(n-i, j+1-l) \\
&= \sum_{l=0}^{i+1} \left\{ q^l \begin{bmatrix} i \\ l \end{bmatrix} + \begin{bmatrix} i \\ l-1 \end{bmatrix} \right\} \left\{ q^{j+1-l} \begin{bmatrix} m-l \\ j+1-l \end{bmatrix} + \begin{bmatrix} m-l \\ j-l \end{bmatrix} \right\} \\
&\cdot (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(n-i, j+1-l) \qquad (7.21) \\
&= \sum_{l=0}^{i} \begin{bmatrix} i \\ l \end{bmatrix} q^{j+1} \begin{bmatrix} m-l \\ j+1-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(n-i, j+1-l) \\
&+ \sum_{l=0}^{i} q^l \begin{bmatrix} i \\ l \end{bmatrix} \begin{bmatrix} m-l \\ j-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(n-i, j+1-l) \\
&+ \sum_{l=1}^{i+1} \begin{bmatrix} i \\ l-1 \end{bmatrix} q^{j+1-l} \begin{bmatrix} m-l \\ j+1-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(n-i, j+1-l) \\
&+ \sum_{l=1}^{i+1} \begin{bmatrix} i \\ l-1 \end{bmatrix} \begin{bmatrix} m-l \\ j-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(n-i, j+1-l), \qquad (7.22)
\end{aligned}
$$

where (7.21) follows (7.8). Let us denote the four summations in the right hand side of (7.22) as A, B, C, and D respectively. We have $A = q^{j+1}P_{j+1}(i;m,n)$, and

$$B = \sum_{l=0}^{i} \begin{bmatrix} i \\ l \end{bmatrix} \begin{bmatrix} m-l \\ j-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(n-i, j-l)(q^{n-i+l} - q^j), \tag{7.23}$$

$$\begin{aligned} C &= \sum_{l=0}^{i} \begin{bmatrix} i \\ l \end{bmatrix} q^{j-l} \begin{bmatrix} m-l-1 \\ j-l \end{bmatrix} (-1)^{l+1} q^{\sigma_{l+1}} q^{(l+1)(n-i)} \alpha(n-i, j-l) \\ &= -q^{j+n-i} \sum_{l=0}^{i} \begin{bmatrix} i \\ l \end{bmatrix} \begin{bmatrix} m-l \\ j-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(n-i, j-l) \frac{q^{m-j}-1}{q^{m-l}-1}, \end{aligned} \tag{7.24}$$

$$D = -q^{n-i} \sum_{l=0}^{i} \begin{bmatrix} i \\ l \end{bmatrix} \begin{bmatrix} m-l \\ j-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(n-i, j-l) q^l \frac{q^{j-l}-1}{q^{m-l}-1}, \tag{7.25}$$

where (7.24) follows (7.9) and (7.25) follows both (7.9) and (7.10). Combining (7.23), (7.24), and (7.25), we obtain

$$\begin{aligned} B + C + D &= \sum_{l=0}^{i} \begin{bmatrix} i \\ l \end{bmatrix} \begin{bmatrix} m-l \\ j-l \end{bmatrix} (-1)^l q^{\sigma_l} q^{l(n-i)} \alpha(n-i, j-l) \\ &\quad \cdot \left\{ q^{n-i+l} - q^j - q^{n-i} \frac{q^m - q^j}{q^{m-l}-1} - q^{n-i} \frac{q^j - q^l}{q^{m-l}-1} \right\} \\ &= -q^j P_j(i;m,n). \end{aligned}$$

□

7.2.4 Proof of Proposition 3.22

Before proving Proposition 3.22, we need two technical lemmas.

Lemma 7.4. *For all m, ν, and l, we have*

$$\delta(m,\nu,j) \stackrel{def}{=} \sum_{i=0}^{j} \begin{bmatrix} j \\ i \end{bmatrix} (-1)^i q^{\sigma_i} \alpha(m-i, \nu) = \alpha(\nu, j)\alpha(m-j, \nu-j) q^{j(m-j)}. \tag{7.26}$$

Proof. The proof goes by induction on j. The claim trivially holds for $j = 0$. Let us suppose it holds for $j = \bar{j}$. We have

$$\begin{aligned}
\delta(m,\nu,\bar{j}+1) &= \sum_{i=0}^{\bar{j}+1} \begin{bmatrix} \bar{j}+1 \\ i \end{bmatrix} (-1)^i q^{\sigma_i} \alpha(m-i,\nu) \\
&= \sum_{i=0}^{\bar{j}+1} \left(q^i \begin{bmatrix} \bar{j} \\ i \end{bmatrix} + \begin{bmatrix} \bar{j} \\ i-1 \end{bmatrix} \right) (-1)^i q^{\sigma_i} \alpha(m-i,\nu) \qquad (7.27) \\
&= \sum_{i=0}^{\bar{j}} q^i \begin{bmatrix} \bar{j} \\ i \end{bmatrix} (-1)^i q^{\sigma_i} \alpha(m-i,\nu) + \sum_{i=1}^{\bar{j}+1} \begin{bmatrix} \bar{j} \\ i-1 \end{bmatrix} (-1)^i q^{\sigma_i} \alpha(m-i,\nu) \\
&= \sum_{i=0}^{\bar{j}} q^i \begin{bmatrix} \bar{j} \\ i \end{bmatrix} (-1)^i q^{\sigma_i} \alpha(m-i,\nu) - \sum_{i=0}^{\bar{j}} \begin{bmatrix} \bar{j} \\ i \end{bmatrix} (-1)^i q^{\sigma_{i+1}} \alpha(m-1-i,\nu) \\
&= \sum_{i=0}^{\bar{j}} q^i \begin{bmatrix} \bar{j} \\ i \end{bmatrix} (-1)^i q^{\sigma_i} \alpha(m-1-i,\nu-1) q^{m-1-i} (q^\nu - 1) \\
&= q^{m-1}(q^\nu - 1)\delta(m-1,\nu-1,\bar{j}) \\
&= \alpha(\nu,\bar{j}+1)\alpha(m-\bar{j}-1,\nu-\bar{j}-1) q^{(\bar{j}+1)(m-\bar{j}-1)},
\end{aligned}$$

where (7.27) follows (7.8). □

Lemma 7.5. *For all n, ν, and j, we have*

$$\theta(n,\nu,j) \stackrel{def}{=} \sum_{l=0}^{j} \begin{bmatrix} j \\ l \end{bmatrix} \begin{bmatrix} n-j \\ \nu-l \end{bmatrix} q^{l(n-\nu)} (-1)^l q^{\sigma_l} \alpha(\nu-l, j-l) = (-1)^j q^{\sigma_j} \begin{bmatrix} n-j \\ n-\nu \end{bmatrix}. \quad (7.28)$$

Proof. The proof goes by induction on j. The claim trivially holds for $j = 0$. Let

us suppose it holds for $j = \bar{j}$. We have

$$
\begin{aligned}
&\theta(n,\nu,\bar{j}+1)\\
&=\sum_{l=0}^{\bar{j}+1}\begin{bmatrix}\bar{j}+1\\ l\end{bmatrix}\begin{bmatrix}n-1-\bar{j}\\ \nu-l\end{bmatrix}q^{l(n-\nu)}(-1)^l q^{\sigma_l}\alpha(\nu-l,\bar{j}+1-l)\\
&=\sum_{l=0}^{\bar{j}+1}\left(\begin{bmatrix}\bar{j}\\ l\end{bmatrix}+q^{\bar{j}+1-l}\begin{bmatrix}\bar{j}\\ l-1\end{bmatrix}\right)\begin{bmatrix}n-1-\bar{j}\\ \nu-l\end{bmatrix}q^{l(n-\nu)}(-1)^l q^{\sigma_l}\alpha(\nu-l,\bar{j}+1-l) \quad (7.29)\\
&=\sum_{l=0}^{\bar{j}}\begin{bmatrix}\bar{j}\\ l\end{bmatrix}\begin{bmatrix}n-1-\bar{j}\\ \nu-l\end{bmatrix}q^{l(n-\nu)}(-1)^l q^{\sigma_l}\alpha(\nu-l,\bar{j}-l)(q^{\nu-l}-q^{\bar{j}-l})\\
&+\sum_{l=1}^{\bar{j}+1}q^{\bar{j}-l+1}\begin{bmatrix}\bar{j}\\ l-1\end{bmatrix}\begin{bmatrix}n-1-\bar{j}\\ \nu-l\end{bmatrix}q^{l(n-\nu)}(-1)^l q^{\sigma_l}\alpha(\nu-l,\bar{j}-l+1), \quad (7.30)
\end{aligned}
$$

where (7.29) follows (7.7). Let us denote the first and second summations in the right hand side of (7.30) as A and B, respectively. We have

$$
\begin{aligned}
A &= (q^\nu-q^{\bar{j}})\sum_{l=0}^{\bar{j}}\begin{bmatrix}\bar{j}\\ l\end{bmatrix}\begin{bmatrix}n-1-\bar{j}\\ \nu-l\end{bmatrix}q^{l(n-1-\nu)}(-1)^l q^{\sigma_l}\alpha(\nu-l,\bar{j}-l)\\
&= (q^\nu-q^{\bar{j}})\theta(n-1,\nu,\bar{j})\\
&= (q^\nu-q^{\bar{j}})(-1)^{\bar{j}}q^{\sigma_{\bar{j}}}\begin{bmatrix}n-1-\bar{j}\\ n-1-\nu\end{bmatrix}, \quad (7.31)
\end{aligned}
$$

and

$$
\begin{aligned}
B &= \sum_{l=0}^{\bar{j}}q^{\bar{j}-l}\begin{bmatrix}\bar{j}\\ l\end{bmatrix}\begin{bmatrix}n-1-\bar{j}\\ \nu-1-l\end{bmatrix}q^{(l+1)(n-\nu)}(-1)^{l+1}q^{\sigma_{l+1}}\alpha(\nu-1-l,\bar{j}-l)\\
&= -q^{\bar{j}+n-\nu}\sum_{l=0}^{\bar{j}}\begin{bmatrix}\bar{j}\\ l\end{bmatrix}\begin{bmatrix}n-1-\bar{j}\\ \nu-1-l\end{bmatrix}q^{l(n-\nu)}(-1)^l q^{\sigma_l}\alpha(\nu-1-l,\bar{j}-l)\\
&= -q^{\bar{j}+n-\nu}\theta(n-1,\nu-1,\bar{j})\\
&= -q^{\bar{j}+n-\nu}(-1)^{\bar{j}}q^{\sigma_{\bar{j}}}\begin{bmatrix}n-1-\bar{j}\\ n-\nu\end{bmatrix}. \quad (7.32)
\end{aligned}
$$

Combining (7.29), (7.31), and (7.32), we obtain

$$\begin{aligned}\theta(n,\nu,\bar{j}+1) &= (-1)^{\bar{j}}q^{\sigma_{\bar{j}}}\left\{(q^{\nu}-q^{\bar{j}})\begin{bmatrix}n-1-\bar{j}\\ n-1-\nu\end{bmatrix}-q^{\bar{j}+n-\nu}\begin{bmatrix}n-1-\bar{j}\\ n-\nu\end{bmatrix}\right\}\\ &= (-1)^{\bar{j}+1}q^{\sigma_{\bar{j}+1}}\begin{bmatrix}n-1-\bar{j}\\ n-\nu\end{bmatrix}\left\{-(q^{\nu-\bar{j}}-1)\frac{q^{n-\nu}-1}{q^{\nu-\bar{j}}-1}+q^{n-\nu}\right\} \qquad (7.33)\\ &= (-1)^{\bar{j}+1}q^{\sigma_{\bar{j}+1}}\begin{bmatrix}n-1-\bar{j}\\ n-\nu\end{bmatrix}, \qquad (7.34)\end{aligned}$$

where (7.33) follows (7.10). □

We now give a proof of Proposition 3.22.

Proof. We apply the q^{-1}-derivative with respect to y to (3.10) ν times, and we apply $x=y=1$. By Lemma 3.11 the LHS becomes

$$\sum_{i=\nu}^{n} q^{\nu(1-i)+\sigma_\nu}\beta(i,\nu)A_i = q^{\nu(1-n)+\sigma_\nu}\beta(\nu,\nu)\sum_{i=\nu}^{n}\begin{bmatrix}i\\ \nu\end{bmatrix}q^{\nu(n-i)}A_i. \qquad (7.35)$$

The RHS becomes $q^{m(k-n)}\sum_{j=0}^{n}B_j\psi_j(1,1)$, where

$$\begin{aligned}\psi_j(x,y) &\stackrel{\text{def}}{=} [b_j(x,y;m) * a_{n-j}(x,y;m)]^{\{\nu\}}\\ &= \sum_{l=0}^{\nu}\begin{bmatrix}\nu\\ l\end{bmatrix}q^{l(n-j-\nu+l)}b_j^{\{l\}}(x,y;m) * a_{n-j}^{\{\nu-l\}}(x,y;m-l) \qquad (7.36)\\ &= \sum_{l=0}^{\nu}\begin{bmatrix}\nu\\ l\end{bmatrix}q^{l(n-j-\nu+l)}(-1)^l\beta(j,l)\beta(n-j,\nu-l)q^{-\sigma_{\nu-l}}\\ &\quad\cdot b_{j-l}(x,y;m) * \alpha(m-l,\nu-l)a_{n-j-\nu+l}(x,y;m-\nu) \qquad (7.37)\\ &= \beta(\nu,\nu)q^{-\sigma_\nu}\sum_{l=0}^{\nu}\begin{bmatrix}j\\ l\end{bmatrix}\begin{bmatrix}n-j\\ \nu-l\end{bmatrix}q^{l(n-j)}(-1)^l q^{\sigma_l}\\ &\quad\cdot b_{j-l}(x,y;m) * \alpha(m-l,\nu-l)a_{n-j-\nu+l}(x,y;m-\nu),\end{aligned}$$

where (7.36) and (7.37) follow Lemmas 3.12 and 3.11 respectively.

We have

$$\begin{aligned}
&[b_{j-l} * \alpha(m-l, \nu-l) a_{n-j-\nu+l}]\,(1,1; m-\nu) \\
&= \sum_{u=0}^{n-\nu} \sum_{i=0}^{u} q^{i(n-j-\nu+l)} \begin{bmatrix} j-l \\ i \end{bmatrix} (-1)^i q^{\sigma_i} \alpha(m-i-l, \nu-l) \\
&\cdot \begin{bmatrix} n-j-\nu+l \\ u-i \end{bmatrix} \alpha(m-\nu-i, u-i) \\
&= q^{(m-\nu)(n-\nu-j+l)} \sum_{i=0}^{j-l} \begin{bmatrix} j-l \\ i \end{bmatrix} (-1)^i q^{\sigma_i} \alpha(m-l-i, \nu-l) \\
&= q^{(m-\nu)(n-\nu-j+l)} \alpha(\nu-l, j-l) \alpha(m-j, \nu-j) q^{(j-l)(m-j)}, \qquad (7.38)
\end{aligned}$$

where (7.38) follows Lemma 7.4. Hence

$$\begin{aligned}
\psi_j(1,1) &= \beta(\nu,\nu) q^{m(n-\nu)+\nu(1-n)+\sigma_\nu} \alpha(m-j, \nu-j) q^{j(\nu-j)} \\
&\cdot \sum_{l=0}^{j} \begin{bmatrix} j \\ l \end{bmatrix} \begin{bmatrix} n-j \\ \nu-l \end{bmatrix} q^{l(n-\nu)} (-1)^l q^{\sigma_l} \alpha(\nu-l, j-l) \\
&= \beta(\nu,\nu) q^{m(n-\nu)+\nu(1-n)+\sigma_\nu} \alpha(m-j, \nu-j) q^{j(\nu-j)} (-1)^j q^{\sigma_j} \begin{bmatrix} n-j \\ n-\nu \end{bmatrix}, \qquad (7.39)
\end{aligned}$$

where (7.39) follows Lemma 7.5. Incorporating this expression for $\psi_j(1,1)$ in the definition of the RHS and rearranging both sides, we obtain the result. □

7.2.5 Proof of Proposition 3.26

Proof. Eq. (3.12) can be expressed in terms of the $\alpha_p(m,u)$ and $\begin{bmatrix} n \\ u \end{bmatrix}_p$ functions as

$$\sum_{i=\nu}^{n} \begin{bmatrix} i \\ \nu \end{bmatrix}_p A_i = (-1)^\nu p^{-mk-\sigma_\nu} \sum_{j=0}^{\nu} \begin{bmatrix} n-j \\ n-\nu \end{bmatrix}_p p^{j(m+n-j)} \alpha_p(m-j, \nu-j) B_j. \qquad (7.40)$$

We obtain

$$p^{mk}\sum_{i=0}^{n}\begin{bmatrix}i\\1\end{bmatrix}_p^{\nu}A_i = p^{mk}\sum_{l=0}^{\nu}p^{\sigma_l}\beta_p(l,l)S_p(\nu,l)\sum_{i=l}^{n}\begin{bmatrix}i\\l\end{bmatrix}_p A_i \tag{7.41}$$

$$= \sum_{l=0}^{\nu}\beta_p(l,l)S_p(\nu,l)(-1)^l\sum_{j=0}^{l}\begin{bmatrix}n-j\\n-l\end{bmatrix}_p p^{j(m+n-j)}\alpha_p(m-j,l-j)B_j \tag{7.42}$$

$$= \sum_{j=0}^{\nu}B_j p^{j(m+n-j)}\sum_{l=j}^{\nu}\beta_p(l,l)S_p(\nu,l)(-1)^l\begin{bmatrix}n-j\\n-l\end{bmatrix}_p\alpha_p(m-j,l-j),$$

where (7.41) and (7.42) follow (3.15) and (7.40) respectively. □

7.2.6 Proof of Lemma 3.28

Proof. We first prove (3.22):

$$\begin{aligned} q^{-mk}\sum_{i=0}^{n}\begin{bmatrix}i\\\lambda\end{bmatrix}q^{\nu(n-i)}A_i &= \frac{q^{-mk}}{\alpha(\lambda,\lambda)}\sum_{i=0}^{n}q^{\nu(n-i)}A_i\sum_{l=0}^{\lambda}\begin{bmatrix}\lambda\\l\end{bmatrix}(-1)^l q^{\sigma_l}q^{i(\lambda-l)} \qquad (7.43)\\ &= \frac{q^{-mk}}{\alpha(\lambda,\lambda)}\sum_{l=0}^{\lambda}\begin{bmatrix}\lambda\\l\end{bmatrix}(-1)^l q^{\sigma_l}q^{n(\lambda-l)}\sum_{i=0}^{n}q^{(\nu-\lambda+l)(n-i)}A_i\\ &= \frac{1}{\alpha(\lambda,\lambda)}\sum_{l=0}^{\lambda}\begin{bmatrix}\lambda\\l\end{bmatrix}(-1)^l q^{\sigma_l}q^{n(\lambda-l)}T_{0,0,\nu-\lambda+l}(\mathcal{C}),\end{aligned}$$

where (7.43) follows $\alpha(i,\lambda)=\sum_{l=0}^{\lambda}\begin{bmatrix}\lambda\\l\end{bmatrix}(-1)^l q^{\sigma_l}q^{i(\lambda-l)}$. We now prove (3.23): since

$$\begin{bmatrix}i\\1\end{bmatrix}^{\mu} = \left(\frac{1-q^i}{1-q}\right)^{\mu} = \frac{1}{(1-q)^{\mu}}\sum_{a=0}^{\mu}\binom{\mu}{a}(-1)^a q^{ia}, \tag{7.44}$$

we obtain

$$\begin{aligned} T_{1,\mu,\nu}(\mathcal{C}) &= \frac{q^{-mk}}{(1-q)^{\mu}}\sum_{i=0}^{n}q^{\nu(n-i)}A_i\sum_{a=0}^{\mu}\binom{\mu}{a}(-1)^a q^{ia}\\ &= \frac{q^{-mk}}{(1-q)^{\mu}}\sum_{a=0}^{\mu}\binom{\mu}{a}(-1)^a q^{an}\sum_{i=0}^{n}q^{(\nu-a)(n-i)}A_i\\ &= (1-q)^{-\mu}\sum_{a=0}^{\mu}\binom{\mu}{a}(-1)^a q^{an}T_{0,0,\nu-a}(\mathcal{C}).\end{aligned}$$

□

7.2.7 Proof of Proposition 3.29

Proof. From [42, (3.3.6)], we obtain $\begin{bmatrix} n-i \\ \nu \end{bmatrix} = \frac{1}{\alpha(\nu,\nu)} \sum_{l=0}^{\nu} \begin{bmatrix} \nu \\ l \end{bmatrix} (-1)^{\nu-l} q^{\sigma_{\nu-l}} q^{l(n-i)}$, and hence

$$\begin{aligned} q^{-mk} \sum_{i=0}^{n} \begin{bmatrix} n-i \\ \nu \end{bmatrix} A_i &= q^{-mk} \sum_{i=0}^{n} A_i \frac{1}{\alpha(\nu,\nu)} \sum_{l=0}^{\nu} \begin{bmatrix} \nu \\ l \end{bmatrix} (-1)^{\nu-l} q^{\sigma_{\nu-l}} q^{l(n-i)} \\ &= \frac{q^{-mk}}{\alpha(\nu,\nu)} \sum_{l=0}^{\nu} \begin{bmatrix} \nu \\ l \end{bmatrix} (-1)^{\nu-l} q^{\sigma_{\nu-l}} \sum_{i=0}^{n} q^{l(n-i)} A_i \\ &= \frac{1}{\alpha(\nu,\nu)} \sum_{l=0}^{\nu} \begin{bmatrix} \nu \\ l \end{bmatrix} (-1)^{\nu-l} q^{\sigma_{\nu-l}} T_{0,0,l}(\mathcal{C}), \end{aligned} \tag{7.45}$$

where (7.45) follows (3.21). By Corollary 3.21, we have for $\nu < d'_{\mathrm{R}}$, $\sum_{l=0}^{\nu} \begin{bmatrix} \nu \\ l \end{bmatrix} (-1)^{\nu-l}$ $q^{\sigma_{\nu-l}} T_{0,0,l}(\mathcal{C}) = q^{-m\nu} \alpha(n,\nu)$, and we obtain

$$\begin{aligned} \sum_{j=0}^{\nu} \begin{bmatrix} \nu \\ j \end{bmatrix} \alpha(n,j) q^{-mj} &= \sum_{j=0}^{\nu} \begin{bmatrix} \nu \\ j \end{bmatrix} \sum_{l=0}^{j} \begin{bmatrix} j \\ l \end{bmatrix} (-1)^{j-l} q^{\sigma_{j-l}} T_{0,0,l}(\mathcal{C}) \\ &= \sum_{l=0}^{\nu} T_{0,0,l}(\mathcal{C}) \begin{bmatrix} \nu \\ l \end{bmatrix} \sum_{j=0}^{\nu} \begin{bmatrix} \nu-l \\ j-l \end{bmatrix} (-1)^{j-l} q^{\sigma_{j-l}} \\ &= T_{0,0,\nu}(\mathcal{C}), \end{aligned} \tag{7.46}$$

where (7.46) follows $\sum_{j=0}^{\nu-l} \begin{bmatrix} \nu-l \\ j \end{bmatrix} (-1)^j q^{\sigma_j} = \delta_{\nu,l}$, which in turn is a special case of [42, (3.3.6)]. This proves (3.24). Thus, $T_{0,0,\nu}(\mathcal{C})$ is transparent to the code, and (3.25) can be shown by choosing $\mathcal{C} = \mathrm{GF}(q^m)^n$ without loss of generality.

Suppose $S(\nu,n,m) \stackrel{\mathrm{def}}{=} \sum_{j=0}^{\nu} \begin{bmatrix} \nu \\ j \end{bmatrix} \alpha(n,j) q^{-mj}$. Then $S(\nu,n,m) = S(n,\nu,m)$ since $\begin{bmatrix} \nu \\ j \end{bmatrix} \alpha(n,j) = \begin{bmatrix} n \\ j \end{bmatrix} \alpha(\nu,j)$. Also, combining (3.24) and (3.25) yields $S(\nu,n,m) = q^{n(\nu-m)} S(n,m,\nu)$. Therefore, we obtain $S(\nu,n,m) = q^{\nu(n-m)} S(\nu,m,n)$, which proves (3.26). □

7.3 Appendix of Chapter 4

7.3.1 Proof of Proposition 4.12

Proof. For all $\mathbf{X} \in \mathrm{GF}(q)^{l\times k}$ with rank s and $\mathbf{C} \in \mathcal{C}$, we define $f_r(\mathbf{X},\mathbf{C}) = 1$ if $d_{\mathrm{R}}(\mathbf{X},\mathbf{c}) = r$ and $f_r(\mathbf{X},\mathbf{C}) = 0$ otherwise. Note that $\sum_{\mathbf{X}:\mathrm{rk}(\mathbf{X})=s} f_r(\mathbf{X},\mathbf{C}) = J_{\mathrm{R}}(q,l,k,s,r,\mathrm{rk}(\mathbf{C}))$ for all $\mathbf{C}\in\mathcal{C}$ and

$$\sum_{\mathbf{c}\in C} f_r(\mathbf{X},\mathbf{C}) = |\{\mathbf{Y}\in\mathcal{C}-\mathbf{X} : \mathrm{rk}(\mathbf{Y}) = r\}| \le A_{\mathrm{R}}(q,l,k,d,r)$$

for all $\mathbf{X}\in\mathrm{GF}(q)^{l\times k}$. We obtain

$$\begin{aligned}\sum_{\mathbf{C}\in\mathcal{C}}\sum_{\mathbf{X}:\mathrm{rk}(\mathbf{X})=s} f_r(\mathbf{X},\mathbf{C}) &= \sum_{i=0}^{n} A_i J_{\mathrm{R}}(q,l,k,s,r,i), &(7.47)\\ \sum_{\mathbf{X}:\mathrm{rk}(\mathbf{X})=s}\sum_{\mathbf{C}\in\mathcal{C}} f_r(\mathbf{X},\mathbf{C}) &\le N_{\mathrm{R}}(q,l,k,s) A_{\mathrm{R}}(q,l,k,d,r). &(7.48)\end{aligned}$$

Combining (7.47) and (7.48), we obtain

$$A_{\mathrm{R}}(q,m,n,d,r) \ge \frac{\sum_{i=0}^{n} A_i J_{\mathrm{R}}(q,l,k,s,r,i)}{N_{\mathrm{R}}(q,l,k,s)}. \tag{7.49}$$

Suppose $d > r+1$. For all $\mathbf{C}\in\mathcal{C}$, let us denote the set of matrices with rank s at distance at most $d-r-1$ from $\mathbf{C}$ as $S_{\mathbf{C}}$, and $S \stackrel{\mathrm{def}}{=} \bigcup_{\mathbf{C}\in\mathcal{C}} S_{\mathbf{C}}$. For $\mathbf{X}\in S_{\mathbf{C}}$, we have $d_{\mathrm{R}}(\mathbf{X},\mathbf{C}) \le d-r-1 < r$. We have for $\mathbf{C}'\in\mathcal{C}$ and $\mathbf{C}'\neq\mathbf{C}$, $d_{\mathrm{R}}(\mathbf{X},\mathbf{C}') \ge d_{\mathrm{R}}(\mathbf{C},\mathbf{C}') - d_{\mathrm{R}}(\mathbf{X},\mathbf{C}) \ge r+1$; and hence $f_r(\mathbf{X},\mathbf{C}') = 0$ for all $\mathbf{C}'\in\mathcal{C}$. Therefore, $\sum_{\mathbf{C}\in\mathcal{C}} f_r(\mathbf{X},\mathbf{C}) = 0$ for all $\mathbf{X}\in S$ and

$$\begin{aligned}\sum_{\mathbf{X}:\mathrm{rk}(\mathbf{X})=s}\sum_{\mathbf{C}\in\mathcal{C}} f_r(\mathbf{X},\mathbf{C}) &= \sum_{\mathbf{X}\in S}\sum_{\mathbf{C}\in C} f_r(\mathbf{X},\mathbf{C}) + \sum_{\substack{\mathbf{X}\notin S\\ \mathrm{rk}(\mathbf{X})=s}}\sum_{\mathbf{C}\in\mathcal{C}} f_r(\mathbf{X},\mathbf{C})\\ &\le [N_{\mathrm{R}}(q,l,k,s) - |S|]\, A_{\mathrm{R}}(q,l,k,d,r). &(7.50)\end{aligned}$$

Since $d-r-1 < \frac{d}{2}$, the balls with radius $d-r-1$ around the codewords are disjoint and hence $|S| = \sum_{i=0}^{n} A_i \sum_{t=0}^{d-r-1} J_{\mathrm{R}}(q,l,k,s,t,i)$. Combining (7.47)

and (7.50), we obtain

$$A_{\mathrm{R}}(q,l,k,d,r) \geq \frac{\sum_{i=0}^{n} A_i J_{\mathrm{R}}(q,l,k,s,r,i)}{N_{\mathrm{R}}(q,l,k,s) - \sum_{i=0}^{n} A_i \sum_{t=0}^{d-r-1} J_{\mathrm{R}}(q,l,k,s,t,i)}. \tag{7.51}$$

Note that (7.49) and (7.51) both hold for any s and rank spectrum $\{A_i\}$. Furthermore, since $A_{\mathrm{R}}(q,l,k,d,r)$ is a non-decreasing function of l and k, $A_{\mathrm{R}}(q,m,n,d,r) \geq A_{\mathrm{R}}(q,l,k,d,r)$ for all $\max\{r,d\} \leq k \leq n$ and $k \leq l \leq m$. Thus, we have (4.8) and (4.9). □

7.3.2 Proof of Proposition 4.17

Proof. By Proposition 4.11, we obtain $A_{\mathrm{R}}(q,m,m,d,m) \leq \alpha(m,m-d+1)$ for $r = n = m$ and $A_{\mathrm{R}}(q,m,n,d,r) \leq \begin{bmatrix} n \\ r \end{bmatrix} \alpha(m,r-d+1) < \begin{bmatrix} n \\ r \end{bmatrix} q^{m(r-d+1)}$ otherwise. We now derive lower bounds on $M(q,m,n,d,r)$. Again, $M(q,m,n,d,r) = \begin{bmatrix} n \\ r \end{bmatrix} \sum_{j=d}^{r} (-1)^j \mu_j$ where $\mu_j > \mu_{j-1}$ for $d+1 \leq j \leq r$. Therefore, when needed, we shall only consider the last terms in the summation.

First, $M(q,m,m,m-1,m) = (q^{2m}-1) - \frac{q^m-1}{q-1}(q^m-1) > \frac{q-2}{q-1}(q^{2m}-1) > \frac{q-2}{q-1}\alpha(m,2)$, which leads to (4.11). For $q=2$, $M(2,m,m,m-1,m) = 2(2^m-1) = (2^{m-1}-1)^{-1}\alpha(m,2)$, which results in (4.10). Second, when $r = n = m$ and $d = m-2$,

$$\begin{aligned} M(q,m,m,m-2,m) &= (q^{3m}-1) - \frac{\alpha(m,1)}{q-1}(q^{2m}-1) + \frac{\alpha(m,2)}{(q^2-1)(q-1)}(q^m-1) \\ &> \frac{q-2}{q-1}\alpha(m,1)(q^{2m}-1) + \frac{1}{(q^2-1)(q-1)}\alpha(m,2)(q^m-1) \\ &> \frac{(q^2-1)(q-2)+1}{(q^2-1)(q-1)}\alpha(m,1), \end{aligned}$$

which leads to (4.12). Third, when $r = n = m$ and $d < m-2$, by considering the

last four terms in the summation, we obtain

$$\begin{aligned}
&M(q,m,m,d,m)\\
&> (q^{m(m-d+1)}-1) - \frac{\alpha(m,1)}{q-1}(q^{m(m-d)}-1)\\
&+ \frac{\alpha(m,2)}{(q^2-1)(q-1)}(q^{m(m-d-1)}-1) - \frac{\alpha(m,3)}{(q^3-1)(q^2-1)(q-1)}(q^{m(m-d-2)}-1)\\
&> \left\{\frac{q-2}{q-1} + \frac{q^3-2}{(q^3-1)(q^2-1)(q-1)}\right\}\alpha(m,m-d+1),
\end{aligned}$$

which results in (4.13). Fourth, when $d < r < m$, by considering the last two terms in the summation, we obtain

$$\begin{aligned}
M(q,m,n,d,r) &\geq \begin{bmatrix} n \\ r \end{bmatrix}\left((q^{m(r-d+1)}-1) - \begin{bmatrix} r \\ 1 \end{bmatrix}(q^{m(r-d)}-1)\right)\\
&\geq \begin{bmatrix} n \\ r \end{bmatrix}\left(q^{m(r-d+1)} - 1 - q^{m(r-d)+r} + q^r\right) \qquad (7.52)\\
&\geq \begin{bmatrix} n \\ r \end{bmatrix} q^{m(r-d+1)}(1-q^{r-m}). \qquad (7.53)
\end{aligned}$$

Therefore, since $r < m$, $B(q,m,n,d,r) < (1-q^{r-m})^{-1} \leq \frac{q}{q-1}$, which leads to (4.14). □

7.3.3 Proof of Proposition 4.22

Proof. We first derive a lower bound on $a_{\mathrm{R}}(\nu,\delta,\rho)$. For $d \leq r$, Proposition 4.15 yields $A_{\mathrm{R}}(q,m,n,d,r) \geq q^{r(n-r)+m(r-d)}$, which asymptotically becomes $a_{\mathrm{R}}(\nu,\delta,\rho) \geq \rho(1+\nu-\rho)-\delta$ for $\delta \leq \rho$. Similarly, for $d > r$, Proposition 4.20 yields $A_{\mathrm{R}}(q,m,n,d,r) \geq q^{r(n-r)+n(r-d+1)}$, which asymptotically becomes $a_{\mathrm{R}}(\nu,\delta,\rho) \geq \rho(2\nu-\rho)-\nu\delta$ for $\delta \geq \rho$.

Proposition 4.6 and (4.5) yield $\log_q A_{\mathrm{R}}(q,m,n,d,r) \geq \min\{(n-r)(2r-d-p+1),(m-r)(p+1)\}$ for $d > r$ and $2r \leq n$. Treating the two terms as functions and assuming that p is real, the lower bound is maximized when $p = \frac{(n-r)(2r-d+1)-m+r}{m+n-2r}$.

Using $p = \left\lfloor \frac{(n-r)(2r-d+1)-m+r}{m+n-2r} \right\rfloor$, asymptotically we obtain $a_{\mathrm{R}}(\nu,\delta,\rho) \geq \frac{(1-\rho)(\nu-\rho)}{1+\nu-2\rho}(2\rho-\delta)$ for $2\rho \leq \nu$.

For $d > r$ and $n \leq 2r \leq m$, Proposition 4.6 and (4.5) yield $\log_q A_{\mathrm{R}}(q,m,n,d,r) \geq \min\{r(n-d-p+1),(m-r)(p+1)\}$. After maximizing this expression over p, we asymptotically obtain $a_{\mathrm{R}}(\nu,\delta,\rho) \geq \rho(1-\rho)(\nu-\delta)$ for $\nu \leq 2\rho \leq 1$.

For $d > r$ and $2r \geq m$, Proposition 4.6 and (4.5) lead to $\log_q A_{\mathrm{R}}(q,m,n,d,r) \geq \min\{r(n-d-p+1), r(m-2r+p+1)\}$. After maximizing this expression over p, we asymptotically obtain $a_{\mathrm{R}}(\nu,\delta,\rho) \geq \frac{\rho}{2}(1+\nu-2\rho-\delta)$ for $2\rho \geq 1$.

We now derive an upper bound on $a_{\mathrm{R}}(\nu,\delta,\rho)$. First, Proposition 4.11 gives $A_{\mathrm{R}}(q,m,n,d,r) < \begin{bmatrix} n \\ r \end{bmatrix} q^{m(r-d+1)} < K_q^{-1} q^{r(n-r)+m(r-d+1)}$ for $d \leq r$, which asymptotically becomes $a_{\mathrm{R}}(\nu,\delta,\rho) \leq \rho(1+\nu-\rho)-\delta$ for $\rho \geq \delta$. Second, by Proposition 4.6, we obtain $a_{\mathrm{R}}(\nu,\delta,\rho) \leq \lim_{m\to\infty} \sup \left[\log_{q^{m^2}} A_{\mathrm{C}}(q,n,d-r,r)\right] = \min\{(\nu-\rho)(2\rho-\delta), \rho(\nu-\delta)\}$ for $\rho \leq \delta \leq \min\{2\rho,\nu\}$. □

7.3.4 Proof of Proposition 4.28

In order to prove Proposition 4.28, we need two technical lemmas. For any $\mathbf{R} \in \mathrm{GF}(q)^{m\times n}$, we denote the number of matrices with row space W and at rank distance s from $\mathbf{R}$ as $g(W,s,\mathbf{R})$. We prove below that $g(W,s,\mathbf{R})$ only depends on $\mathbf{R}$ through its row space.

Lemma 7.6. *For all $\mathbf{R},\mathbf{S} \in \mathrm{GF}(q)^{m\times n}$ with the same row space U, $g(W,s,\mathbf{R}) = g(W,s,\mathbf{S})$, and hence $g(W,s,\mathbf{R}) = g(W,s,U)$.*

Proof. Suppose $\mathbf{X} \in \mathrm{GF}(q)^{m\times n}$ has row space W and satisfies $\mathrm{rk}(\mathbf{X}-\mathbf{R}) = s$. We can express $\mathbf{S} = \mathbf{AR}$, where $\mathbf{A} \in \mathrm{GF}(q)^{m\times m}$ has full rank, hence $\mathbf{Y} = \mathbf{AX}$ has row space W and satisfies $\mathrm{rk}(\mathbf{Y}-\mathbf{S}) = \mathrm{rk}(\mathbf{X}-\mathbf{R}) = s$. Thus $g(W,s,\mathbf{S}) \geq g(W,s,\mathbf{R})$. Using

$\mathbf{R} = \mathbf{A}^{-1}\mathbf{S}$, we show that $g(W, s, \mathbf{S}) \leq g(W, s, \mathbf{R})$; hence $g(W, s, \mathbf{R}) = g(W, s, \mathbf{S})$. $\square$

Lemma 7.7. *For all $U \in E_u(q, n)$, $\sum_{W \in E_w(q,n)} g(U, s, W) = \frac{\begin{bmatrix} n \\ w \end{bmatrix}}{\begin{bmatrix} n \\ u \end{bmatrix}} J_{\mathrm{R}}(u, s, w)$.*

Proof. By counting the number of pairs of matrices $(\mathbf{R}, \mathbf{W})$ where $R(\mathbf{R}) = U$, $R(\mathbf{W}) = W$, and $d_{\mathrm{R}}(\mathbf{R}, \mathbf{W}) = s$ in two ways, we have $\alpha(m, u)g(W, s, U) = \alpha(m, w)$ $g(U, s, W)$. Hence

$$\sum_{W \in E_w(q,n)} g(U, s, W) = \frac{\alpha(m, u)}{\alpha(m, w)} \sum_{W \in E_w(q,n)} g(W, s, U) = \frac{\alpha(m, u)}{\alpha(m, w)} J_{\mathrm{R}}(w, s, u).$$

Using (2.2), we obtain $\sum_{W \in E_w(q,n)} g(U, s, W) = \frac{\begin{bmatrix} n \\ w \end{bmatrix}}{\begin{bmatrix} n \\ u \end{bmatrix}} J_{\mathrm{R}}(u, s, w)$. $\square$

We now give the proof of Proposition 4.28.

Proof. Let $\mathcal{C}$ be a rank metric code in $\mathrm{GF}(q)^{m \times n}$ with minimum rank distance d. We have $P_{\mathrm{R}}(\mathbf{C}, U) = \frac{1}{\alpha(m,u)} \sum_{s=0}^{t} \delta(U, s, \mathbf{C})$, where $\delta(U, s, \mathbf{C})$ is the number of matrices $\mathbf{X}$ at distance s from the code, and such that $R(\mathbf{X} - \mathbf{C}) = U$. Hence $\delta(U, s, \mathbf{C}) = \sum_{W : \dim(W) \geq d} A_W(\mathbf{C}) g(U, s, W)$, where $A_W(\mathbf{C}) = |\{\mathbf{D} \in \mathcal{C} : R(\mathbf{D} - \mathbf{C}) = W\}|$ for all $W \in E(q, n)$. We now give an upper bound on $A_W(\mathbf{C})$. Let $C_W = \{\mathbf{D} - \mathbf{C} : \mathbf{D} \in \mathcal{C}, R(\mathbf{D} - \mathbf{C}) = W\}$, then the restriction of C_W to W [29] forms a constant-rank code in $\mathrm{GF}(q)^{m \times w}$ with constant-rank w and minimum distance d. Therefore, $A_W(\mathbf{C}) \leq A_{\mathrm{R}}(q, m, w, d, w) \leq \alpha(m, w - d + 1)$ by Proposition 4.11. The DEP hence satisfies

$$\begin{aligned} P_{\mathrm{R}}(\mathbf{C}, U) &= \frac{1}{\alpha(m, u)} \sum_{s=0}^{t} \sum_{w=d}^{n} \sum_{W \in E_w(q,n)} A_W(\mathbf{C}) g(U, s, W) \\ &\leq \frac{1}{\alpha(m, u)} \sum_{s=0}^{t} \sum_{w=d}^{n} \alpha(m, w - d + 1) \sum_{W \in E_w(q,n)} g(U, s, W) \\ &= \frac{1}{N_{\mathrm{R}}(u)} \sum_{w=d}^{n} \begin{bmatrix} n \\ w \end{bmatrix} \alpha(m, w - d + 1) \sum_{s=0}^{t} J_{\mathrm{R}}(u, s, w), \end{aligned} \tag{7.54}$$

where (7.54) follows Lemma 7.7.

When C is an MRD code with minimum rank distance d, it can be shown that $A_W(\mathbf{C}) = M(q,m,w,d,w) = \begin{bmatrix} n \\ w \end{bmatrix}^{-1} M(q,m,n,d,w)$, and hence

$$\delta(U,s,\mathbf{C}) \;=\; \frac{\alpha(m,u)}{N_{\mathrm{R}}(u)} \sum_{w=d}^{n} M(q,m,n,d,w) J_{\mathrm{R}}(u,s,w),$$

which leads to (4.26). □

7.4 Appendix of Chapter 5

7.4.1 Proof of Proposition 5.11

Before proving Proposition 5.11, we introduce some useful notations. For $0 \le d \le r$, we denote $U_d = R(\mathbf{I}_r|\mathbf{P}_d) \in E_r(q,n)$, where $\mathbf{P}_d = \left(\begin{array}{c|c} \mathbf{I}_d & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} \end{array}\right) \in \mathrm{GF}(q)^{r\times(n-r)}$, hence $d_{\mathrm{I}}(U_0,U_d) = d$ for all $0 \le d \le r$. We also denote the set of all generator matrices of all subspaces in $B_u(U_0) \cap B_s(U_d)$ as $F(u,s,d)$, hence $|F(u,s,d)| = I_{\mathrm{C}}(u,s,d) \prod_{i=0}^{r-1}(q^r - q^i)$.

Lemma 7.8. *Let* $\mathbf{X} = (\mathbf{A}|\mathbf{B}) \in \mathrm{GF}(q)^{r\times n}$*, where* $\mathbf{A}$ *and* $\mathbf{B}$ *have* r *and* $n-r$ *columns, respectively. Furthermore, we denote* $\mathbf{A} = (\mathbf{A}_1|\mathbf{a}|\mathbf{A}_2)$ *and* $\mathbf{B} = (\mathbf{B}_1|\mathbf{b}|\mathbf{B}_2)$*, where* $\mathbf{a}$ *and* $\mathbf{b}$ *are the* d*-th columns of* $\mathbf{A}$ *and* $\mathbf{B}$*, respectively. Then* $\mathbf{X} \in F(u,s,d)$ *if and only if* $\mathrm{rk}(\mathbf{X}) = r$*,* $\mathrm{rk}(\mathbf{B}) \le u$*, and* $\mathrm{rk}(\mathbf{B}_1 - \mathbf{A}_1|\mathbf{b}-\mathbf{a}|\mathbf{B}_2) \le s$*.*

Proof. First, $\mathbf{X}$ is the generator matrix of some $V \in E_r(q,n)$ if and only if $\mathrm{rk}(\mathbf{X}) = r$. Also, it is easily shown that $d_{\mathrm{I}}(V,U_0) = \mathrm{rk}(\mathbf{B})$ and $d_{\mathrm{I}}(V,U_d) = \mathrm{rk}(\mathbf{B} - \mathbf{A}\mathbf{P}_d) = \mathrm{rk}(\mathbf{B}_1 - \mathbf{A}_1|\mathbf{b}-\mathbf{a}|\mathbf{B}_2)$. Therefore, $\mathbf{X} \in F(u,s,d)$ if and only if $\mathrm{rk}(\mathbf{X}) = r$, $\mathrm{rk}(\mathbf{B}) \le u$, and $\mathrm{rk}(\mathbf{B}_1 - \mathbf{A}_1|\mathbf{b}-\mathbf{a}|\mathbf{B}_2) \le s$. □

We now give the proof of Proposition 5.11.

Proof. It suffices to show that $I_{\mathrm{C}}(u,s,d) \leq I_{\mathrm{C}}(u,s,d-1)$ for any $d \geq 1$. We do so by first defining a mapping ϕ from $F(u,s,d)$ to $F(u,s,d-1)$ and then proving it is injective. Let $\mathbf{X} \in F(u,s,d)$, then by Lemma 7.8, $\mathrm{rk}(\mathbf{X}) = r$, $\mathrm{rk}(\mathbf{B}) \leq u$, and $\mathrm{rk}(\mathbf{B}_1 - \mathbf{A}_1|\mathbf{b}-\mathbf{a}|\mathbf{B}_2) \leq s$. Since the mapping ϕ only modifies $\mathbf{b}$, we shall denote $\phi(\mathbf{X}) = \mathbf{Y} = (\mathbf{A}|\mathbf{B}_1|\mathbf{c}|\mathbf{B}_2)$. We hence have to show that $\mathrm{rk}(\mathbf{Y}) = r$, $\mathrm{rk}(\mathbf{B}_1|\mathbf{c}|\mathbf{B}_2) \leq u$, and $\mathrm{rk}(\mathbf{B}_1 - \mathbf{A}_1|\mathbf{c}|\mathbf{B}_2) \leq s$. We need to distinguish three cases.

- Case I: $\mathrm{rk}(\mathbf{B}_1 - \mathbf{A}_1|\mathbf{B}_2) \leq s-1$. In this case, $\mathbf{c} = \mathbf{b}$. Note that $\mathrm{rk}(\mathbf{Y}) = r$, $\mathrm{rk}(\mathbf{B}) \leq u$, and $\mathrm{rk}(\mathbf{B}_1 - \mathbf{A}_1|\mathbf{c}|\mathbf{B}_2) \leq \mathrm{rk}(\mathbf{B}_1 - \mathbf{A}_1|\mathbf{B}_2) + 1 \leq s$.

- Case II: $\mathrm{rk}(\mathbf{B}_1 - \mathbf{A}_1|\mathbf{B}_2) = s$ and $\mathrm{rk}(\mathbf{B}_1|\mathbf{B}_2) \leq u-1$. In this case, $\mathbf{c} = \mathbf{b} - \mathbf{a}$. Note that $\mathrm{rk}(\mathbf{Y}) = r$, $\mathrm{rk}(\mathbf{B}_1|\mathbf{c}|\mathbf{B}_2) \leq \mathrm{rk}(\mathbf{B}) + 1 \leq u$, and $\mathrm{rk}(\mathbf{B}_1 - \mathbf{A}_1|\mathbf{c}|\mathbf{B}_2) = \mathrm{rk}(\mathbf{B}_1 - \mathbf{A}_1|\mathbf{b}-\mathbf{a}|\mathbf{B}_2) = s$.

- Case III: $\mathrm{rk}(\mathbf{B}_1 - \mathbf{A}_1|\mathbf{B}_2) = s$ and $\mathrm{rk}(\mathbf{B}_1|\mathbf{B}_2) = u$. We have $\mathbf{b} - \mathbf{a} \in C(\mathbf{B}_1 - \mathbf{A}_1|\mathbf{B}_2)$ and $\mathbf{b} \in C(\mathbf{B}_1|\mathbf{B}_2)$. Hence $\mathbf{a} \in C(\mathbf{B}_1|\mathbf{B}_2|\mathbf{B}_1 - \mathbf{A}_1)$. Denoting $C(\mathbf{B}_1|\mathbf{B}_2|\mathbf{B}_1 - \mathbf{A}_1) = C(\mathbf{B}_1|\mathbf{B}_2) \oplus S$, where S is a fixed subspace of $C(\mathbf{B}_1 - \mathbf{A}_1)$, $\mathbf{a}$ can be uniquely expressed as $\mathbf{a} = \mathbf{r} + \mathbf{s}$, where $\mathbf{r} \in C(\mathbf{B}_1|\mathbf{B}_2)$ and $\mathbf{s} \in S$. In this case, $\mathbf{c} = \mathbf{b} - \mathbf{r}$. Since $\mathbf{b} \in C(\mathbf{B}_1|\mathbf{B}_2)$, $\mathrm{rk}(\mathbf{X}) = \mathrm{rk}(\mathbf{A}|\mathbf{B}_1|\mathbf{B}_2) = r = \mathrm{rk}(\mathbf{Y})$. Also, since $\mathbf{c} \in C(\mathbf{B}_1|\mathbf{B}_2)$, $\mathrm{rk}(\mathbf{B}_1|\mathbf{c}|\mathbf{B}_2) = \mathrm{rk}(\mathbf{B}_1|\mathbf{B}_2) = u$. Finally, $\mathbf{c} = \mathbf{b} - \mathbf{a} + \mathbf{s} \in C(\mathbf{B}_1 - \mathbf{A}_1|\mathbf{B}_2)$, therefore $\mathrm{rk}(\mathbf{B}_1 - \mathbf{A}_1|\mathbf{c}|\mathbf{B}_2) = s$.

It is easy to show that ϕ is injective. Therefore, $|F(u,s,d)| \leq |F(u,s,d-1)|$ and $I_{\mathrm{C}}(u,s,d) \leq I_{\mathrm{C}}(u,s,d-1)$. □

7.4.2 Proof of Lemma 5.17

Proof. Let $\mathcal{C}$ be a code in $E_r(q, n-1)$ with covering radius $\rho - 1$ and cardinality $K_{\mathrm{C}}(q, n-1, r, \rho-1)$. Define the code $\mathcal{C}_1 \subseteq E_r(q,n)$ as $\mathcal{C}_1 = \{R(\mathbf{C}|\mathbf{0}) : R(\mathbf{C}) \in \mathcal{C}\}$. For any $U_1 \in E_r(q,n)$ with generator matrix $\mathbf{U}_1 = (\mathbf{U}|\mathbf{u})$, where $\mathbf{U} \in \mathrm{GF}(q)^{r\times n-1}$ and $\mathbf{u} \in \mathrm{GF}(q)^{r\times 1}$, we prove that there exists $C_1 \in \mathcal{C}_1$ generated by $\mathbf{C}_1 = (\mathbf{C}|\mathbf{0})$ such that $d_{\mathrm{I}}(C_1, U_1) \leq \rho$. We remark that $\mathrm{rk}(\mathbf{U})$ is equal to either r or $r-1$. First, if $\mathrm{rk}(\mathbf{U}) = r$, then there exists $C \in \mathcal{C}$ such that $\mathrm{rk}(\mathbf{C}^T|\mathbf{U}^T) \leq r + \rho - 1$. Second, if $\mathrm{rk}(\mathbf{U}) = r-1$, then let $\mathbf{U}_0$ be $r-1$ linearly independent rows of $\mathbf{U}$. For any $\mathbf{v} \in \mathrm{GF}(q)^{n-1}$, $\mathbf{v} \notin R(\mathbf{U}_0)$, there exists $C \in \mathcal{C}$ such that $r+\rho-1 \geq \mathrm{rk}(\mathbf{C}^T|\mathbf{U}_0^T|\mathbf{v}^T) \geq \mathrm{rk}(\mathbf{C}^T|\mathbf{U}_0^T) = \mathrm{rk}(\mathbf{C}^T|\mathbf{U}^T)$. Hence $\mathrm{rk}(\mathbf{C}_1^T|\mathbf{U}_1^T) \leq r+\rho$ and $d_{\mathrm{I}}(C_1, U_1) \leq \rho$. Thus $\mathcal{C}_1$ has covering radius at most ρ and hence $K_{\mathrm{C}}(q,n,r,\rho) \leq K_{\mathrm{C}}(q,n-1,r,\rho-1)$, which applied ρ times yields $K_{\mathrm{C}}(q,n,r,\rho) \leq K_{\mathrm{C}}(q,n-\rho,r,0) = \begin{bmatrix} n-\rho \\ r \end{bmatrix}$.

Similarly, let $\mathcal{C}$ be a code in $E_{r-1}(q,n)$ with covering radius $\rho-1$ and cardinality $K_{\mathrm{C}}(q,n,r-1,\rho-1)$. Define the code $\mathcal{C}_2 = \{R((\mathbf{C}^T|\mathbf{c}^T)^T) : R(\mathbf{C}) \subseteq \mathcal{C}\} \in E_r(q,n)$, where $\mathbf{c} \in \mathrm{GF}(q)^n$ is chosen at random such that $\mathrm{rk}(\mathbf{C}^T|\mathbf{c}^T) = r$. We remark that $|\mathcal{C}_2| \leq |\mathcal{C}|$. For any $U_2 \in E_r(q,n)$ with generator matrix $\mathbf{U}_2 = (\mathbf{U}^T|\mathbf{u}^T)^T$, there exists $C_2 \in \mathcal{C}_2$ with generator matrix $\mathbf{C}_2 = (\mathbf{C}^T|\mathbf{c}^T)^T$ with $\mathrm{rk}(\mathbf{C}^T|\mathbf{U}^T) \leq r+\rho-2$. Thus $\mathrm{rk}(\mathbf{C}_2^T|\mathbf{U}_2^T) \leq r+\rho$ and $\mathcal{C}_2$ has covering radius at most ρ. Thus $K_{\mathrm{C}}(q,n,r,\rho) \leq |\mathcal{C}_2| \leq K_{\mathrm{C}}(q,n,r-1,\rho-1)$ which applied ρ times yields $K_{\mathrm{C}}(q,n,r,\rho) \leq K_{\mathrm{C}}(q,n,r-\rho,0) = \begin{bmatrix} n \\ r-\rho \end{bmatrix}$. □

7.4.3 Proof of Proposition 5.27

Proof. First, by Lemma 5.25, $N_{\mathrm{S}}(r,s,d) = q^{u(d-u)} \begin{bmatrix} r \\ u \end{bmatrix} \begin{bmatrix} n-r \\ d-u \end{bmatrix}$, where $u = \frac{r+d-s}{2}$ satisfies $0 \leq u \leq \min\{r,d\}$. Thus by Corollary 2.3 $q^{f(u)} \leq N_{\mathrm{S}}(r,s,d) < K_q^{-2} q^{f(u)}$,

where $f(u) = u(2r + 3d - n - 3u) + d(n - r - d)$. Hence, $\sum_{d=0}^{t} S(d) \leq V_{\rm S}(r,t) < K_q^{-2} \sum_{d=0}^{t} S(d)$, where $S(d) = \sum_{u=0}^{\min\{r,d\}} q^{f(u)}$. Since f is maximized for $u = u_0 \stackrel{\rm def}{=} \frac{2r+3d-n}{6} \leq d$, we need to consider three cases.

- Case I: $0 \leq d \leq \frac{n-2r}{3}$. We have $u_0 \leq 0$ and hence f is maximized for $u = 0$: $f(0) = g(d) = d(n - r - d)$. Thus $S(d) \geq q^{g(d)}$, and it is easy to show that $S(d) = q^{g(d)} \sum_{u=0}^{r} q^{-u(n-2r-3d+3u)} < M_q q^{g(d)}$.

- Case II: $\frac{n-2r}{3} \leq d \leq \min\left\{\frac{n+4r}{3}, \frac{n}{2}\right\}$. We have $0 \leq u_0 \leq r$ and hence f is maximized for $u = u_0$: $f(u_0) = g(d) = \frac{1}{12}(n - 2r)^2 + \frac{1}{4}d(2n - d)$. Thus $S(d) \geq \max\{q^{f(\lfloor u_0 \rfloor)}, q^{f(\lceil u_0 \rceil)}\} \geq q^{g(d)-\frac{3}{4}}$, and it is easy to show that $S(d) = q^{g(d)} \sum_{u=0}^{r} q^{-3(u-u_0)^2} < 2M_q q^{g(d)}$.

- Case III: $\frac{n+4r}{3} \leq d \leq \frac{n}{2}$. We have $u_0 \geq r$ and hence f is maximized for $u = r$: $f(r) = g(d) = (d - r)(n - d + r)$. Thus $S(d) \geq q^{g(d)}$, and it is easy to show that $S(d) = q^{g(d)} \sum_{i=0}^{r} q^{-i(3d-4r-n+3i)} < M_q q^{g(d)}$.

From the discussion above, we obtain $V_{\rm S}(r,t) \geq S(t) \geq q^{-\frac{3}{4}+g(t)}$ and $V_{\rm S}(r,t) < K_q^{-2} \sum_{d=0}^{t} S(d) < 2M_q K_q^{-2} \sum_{d=0}^{t} q^{g(d)}$. It can be shown that $\sum_{d=0}^{t} q^{g(d)} < L_q q^{g(t)}$ for all $0 \leq t \leq \nu$, and hence $V_{\rm S}(r,t) < 2M_q L_q K_q^{-2} q^{g(t)}$. □

7.4.4 Proof of Theorem 5.28

In order to prove Theorem 5.28, we prove Lemma 7.9 and Corollary 7.10 first below. For all $0 \leq a \leq n$, we denote $\mathbf{U}_a = (\mathbf{I}_a|\mathbf{0}) \in {\rm GF}(q)^{a \times n}$ and $U_a = R(\mathbf{U}_a) \in E_a(q,n)$.

Lemma 7.9. *For any $B, B_0 \in E_b(q,n)$ with $\dim(U_a + B) = \dim(U_a + B_0) = n$, $J_{\rm S}(q,n;u,s;U_a,B,c) = J_{\rm S}(q,n;u,s;U_a,B_0,c)$.*

Proof. It suffices to show that $J_{\mathrm{S}}(q,n;u,s;U_a,B,c) \le J_{\mathrm{S}}(q,n;u,s;U_a,B_0,c)$ for any $B, B_0 \in E_b(q,n)$, both at distance $2n-a-b$ from U_a. For any matrix $\mathbf{X}$ with n columns, we denote $\mathbf{X} = (\mathbf{X}^a|\mathbf{X}^{n-a})$, where $\mathbf{X}^a$ and $\mathbf{X}^{n-a}$ have a and $n-a$ columns respectively. For any generator matrix $\mathbf{B}$ of B, we have $\mathrm{rk}(\mathbf{U}_a^T|\mathbf{B}^T) = n$ and hence $\mathrm{rk}(\mathbf{B}^{n-a}) = n-a$. Similarly, for any generator matrix $\mathbf{B}_0$ of B_0, we have $\mathrm{rk}(\mathbf{B}_0^{n-a}) = n-a$. Since all matrices in $\mathrm{GF}(q)^{b\times(n-a)}$ with full rank have the same row space, without loss of generality we assume $\mathbf{B}^{n-a} = \mathbf{B}_0^{n-a} = (\mathbf{I}_{n-a}|\mathbf{0})^T$, and

$$\mathbf{B} = \left(\begin{array}{c|c} \mathbf{B}^d & \mathbf{I}_{n-a} \\ \hline \mathbf{B}^e & \mathbf{0} \end{array}\right), \mathbf{B}_0 = \left(\begin{array}{c|c} \mathbf{B}_0^d & \mathbf{I}_{n-a} \\ \hline \mathbf{B}_0^e & \mathbf{0} \end{array}\right). \tag{7.55}$$

We have $\mathrm{rk}(\mathbf{B}^e) = \mathrm{rk}(\mathbf{B}_0^e) = b-n+a$. Hence $\mathbf{B}^e$ and $\mathbf{B}_0^e$ have the same column space and we can express $\mathbf{B}_0^e = \mathbf{B}^e\mathbf{E}$, where $\mathbf{E} \in \mathrm{GF}(q)^{a\times a}$ has full rank. Thus $\mathbf{B}_0 = \mathbf{B}\mathbf{F}$, where $\mathbf{F} = \left(\begin{array}{c|c} \mathbf{E} & \mathbf{0} \\ \hline \mathbf{B}_0^d - \mathbf{B}^d\mathbf{E} & \mathbf{I}_{n-a} \end{array}\right) \in \mathrm{GF}(q)^{n\times n}$ has full rank.

Let $C \in E_c(q,n)$ be generated by $\mathbf{C} \in \mathrm{GF}(q)^{c\times n}$. Then C satisfies $d_{\mathrm{S}}(U_a,C) = u$ and $d_{\mathrm{S}}(B,C) = s$ if and only if $\mathrm{rk}(\mathbf{C}^{n-a}) = \frac{u+c-a}{2}$ and $\mathrm{rk}(\mathbf{B}^T|\mathbf{C}^T) = \frac{s+c+b}{2}$. Let C_0 be generated by $\mathbf{C}_0 = \mathbf{C}\mathbf{F} \in \mathrm{GF}(q)^{c\times n}$. Since $\mathbf{C}_0$ has rank c, $C_0 \in E_c(q,n)$. Also, $\mathrm{rk}(\mathbf{C}_0^{n-a}) = \mathrm{rk}(\mathbf{C}^{n-a}) = \frac{u+c-a}{2}$ and $\mathrm{rk}(\mathbf{B}_0^T|\mathbf{C}_0^T) = \mathrm{rk}(\mathbf{B}^T|\mathbf{C}^T) = \frac{s+c+b}{2}$, and hence $d_{\mathrm{S}}(U_a,C_0) = u$ and $d_{\mathrm{S}}(B_0,C_0) = s$. Thus $J_{\mathrm{S}}(q,n;u,s;U_a,B,c) \le J_{\mathrm{S}}(q,n;u,s;U_a,B_0,c)$. □

Corollary 7.10. *For all $A \in E_a(q,n), B \in E_b(q,n)$ with $\dim(A+B) = n$ we have $J_{\mathrm{S}}(q,n;u,s;A,B,c) = J_{\mathrm{S}}(q,n;u,s,2n-a-b;a,b,c)$.*

Proof. Let $\mathbf{A}$ and $\mathbf{B}$ be generator matrices of A and B, respectively. Let $C \in E_c(q,n)$ be generated by $\mathbf{C}$, where $d_{\mathrm{S}}(C,A) = u$ and $d_{\mathrm{S}}(C,B) = s$. We can express $\mathbf{A}$ as $\mathbf{A}\mathbf{X}^{-1} = \mathbf{U}_a$, where $\mathbf{X} \in \mathrm{GF}(q)^{n\times n}$ has full rank. Let $Y \in E_b(q,n)$ and

$Z \in E_c(q,n)$ be generated by $\mathbf{B}\mathbf{X}^{-1}$ and $\mathbf{C}\mathbf{X}^{-1}$, respectively, then it is easily shown that $d_{\mathrm{S}}(A,B) = d_{\mathrm{S}}(U_a, Y)$, $d_{\mathrm{S}}(A,C) = d_{\mathrm{S}}(U_a, Z)$, and $d_{\mathrm{S}}(B,C) = d_{\mathrm{S}}(Y,Z)$. Thus $J_{\mathrm{S}}(q,n;u,s;A,B,c) \leq J_{\mathrm{S}}(q,n;u,s;U_a,Y,c)$. Since $\mathbf{X}$ is invertible, we easily obtain the reverse inequality, and hence $J_{\mathrm{S}}(q,n;u,s;A,B,c) = J_{\mathrm{S}}(q,n;u,s;U_a,Y,c) = J_{\mathrm{S}}(q,n;u,s,2n-a-b;a,b,c)$ by Lemma 7.9. □

We now give the proof of Theorem 5.28.

Proof. Let $C \in E_c(q,n)$ satisfy $d_{\mathrm{S}}(A,C) = u$ and $d_{\mathrm{S}}(B,C) = s$. We can express $C = C_1 \oplus C_2$, where $C_1 = C \cap (A+B)$ has dimension c_1 and $C_2 \cap (A+B) = \{\mathbf{0}\}$. Note that $u_1 = d_{\mathrm{S}}(A,C_1) = a + c_1 - a - c + u = u - c + c_1$ and $s_1 = d_{\mathrm{S}}(B,C_2) = s - c + c_1$. There are hence $J_{\mathrm{S}}(q,n_1;u_1,s_1,w;a,b,c_1)$ choices for C_1 by Corollary 7.10, where $n_1 = \dim(A+B)$. Once C_1 is fixed, there are $q^{c_1(c-c_1)}\begin{bmatrix} n-n_1 \\ c-c_1 \end{bmatrix}$ choices for C. We obtain

$$J_{\mathrm{S}}(q,n;u,s;A,B,c) = \sum_{c_1=0}^{c} q^{c_1(c-c_1)} \begin{bmatrix} n-n_1 \\ c-c_1 \end{bmatrix} J_{\mathrm{S}}(q,n_1;u_1,s_1,w;a,b,c_1),$$

which is a function of q, n, u, s, w, a, b, and c. □

7.4.5 Proof of Proposition 5.41

Proof. First, $V_{\mathrm{I}}(r,t) \geq N_{\mathrm{I}}(r,r,t) \geq q^{t(n-t)}$. We now prove the upper bound. Since $V_{\mathrm{I}}(r,t) = V_{\mathrm{I}}(n-r,t)$, we assume $r \leq \nu$ without loss of generality. By Lemma 5.40, we have $N_{\mathrm{I}}(r,s,d) < K_q^{-2} q^{s(n-d+r-s)-(r-d)(n-d)}$ for $s \leq r$ and $N_{\mathrm{I}}(r,s,d) < K_q^{-2}$

$q^{s(r-s+d)+d(n-r-d)}$ for $s \geq r$. Hence

$$
\begin{aligned}
& K_q^2 V_{\mathrm{I}}(r,t) \\
& < \sum_{d=0}^{r} \left\{ \sum_{s=r-d}^{r} q^{s(n-d+r-s)-(r-d)(n-d)} + \sum_{s=r+1}^{r+d} q^{s(r-s+d)+d(n-r-d)} \right\} \\
& + \sum_{d=r+1}^{t} \sum_{s=d}^{d+r} q^{s(r-s+d)+d(n-r-d)} \qquad (7.56) \\
& = \sum_{d=0}^{r} q^{d(n-d)} \left\{ \sum_{i=0}^{d} q^{-i(n-d-r+i)} + \sum_{j=1}^{d} q^{-j(r-d+j)} \right\} + \sum_{d=r+1}^{t} q^{d(n-d)} \sum_{k=0}^{r} q^{-k(d-r+k)} \\
& < (2N_q - 1) \sum_{d=0}^{r} q^{d(n-d)} + N_q \sum_{d=r+1}^{t} q^{d(n-d)} \\
& < (2N_q - 1) q^{t(n-t)} \sum_{l=0}^{t} q^{-l(n-2t+l)} \\
& < (2N_q - 1) N_q q^{t(n-t)}.
\end{aligned}
$$

□

Bibliography

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Info. Theory*, vol. 46, no. 4, pp. 1204–1216, July 2000.

[2] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang, *Network Coding Theory*, ser. Foundation and Trends in Communications and Information Theory. Hanover, MA: now Publishers, 2006, vol. 2, no. 4-5.

[3] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Info. Theory*, vol. 49, no. 2, pp. 371–381, February 2003.

[4] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Info. Theory*, vol. 52, no. 10, pp. 4413–4430, October 2006.

[5] C. Fragouli and E. Soljanin, *Network Coding Fundamentals*. Now Publishers Inc, 2007.

[6] T. Ho and D. S. Lun, *Network coding: an introduction*. New York NY: Cambridge University Press, 2008.

[7] N. Cai and R. W. Yeung, "Network coding and error correction," in *Proc. IEEE Information Theory Workshop*, Bangalore, India, October 2002, pp. 20–25.

[8] L. Song, R. W. Yeung, and N. Cai, "Zero-error network coding for acyclic networks," *IEEE Trans. Info. Theory*, vol. 49, no. 12, pp. 3129–3139, December 2003.

[9] R. Koetter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Info. Theory*, vol. 54, no. 8, pp. 3579–3591, August 2008.

[10] D. Silva, F. R. Kschischang, and R. Koetter, "A rank-metric approach to error control in random network coding," *IEEE Trans. Info. Theory*, vol. 54, no. 9, pp. 3951–3967, September 2008.

[11] D. Silva and F. R. Kschischang, "On metrics for error correction in network coding," 2008, available at http://arxiv.org/abs/0805.3824v1.

[12] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *Journal of Combinatorial Theory A*, vol. 25, no. 3, pp. 226–241, November 1978.

[13] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems of Information Transmission*, vol. 21, no. 1, pp. 1–12, January 1985.

[14] R. M. Roth, "Maximum-rank array codes and their application to crisscross error correction," *IEEE Trans. Info. Theory*, vol. 37, no. 2, pp. 328–336, March 1991.

[15] P. Delsarte and V. I. Levenshtein, "Association schemes and coding theory," *IEEE Trans. Info. Theory*, vol. 44, no. 6, pp. 2477–2504, October 1998.

[16] L. Hua, "A theorem on matrices over a field and its applications," *Chinese Mathematical Society*, vol. 1, no. 2, pp. 109–163, 1951.

[17] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Trans. Info. Theory*, vol. 44, pp. 774–765, March 1998.

[18] P. Lusina, E. M. Gabidulin, and M. Bossert, "Maximum rank distance codes as space-time codes," *IEEE Trans. Info. Theory*, vol. 49, no. 10, pp. 2757–2760, October 2003.

[19] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov, "Ideals over a non-commutative ring and their application in cryptology," in *Proc. Eurocrypt*, Brighton, UK, April 1991, pp. 482–489.

[20] E. M. Gabidulin, "Optimal codes correcting lattice-pattern errors," *Problems of Information Transmission*, vol. 21, no. 2, pp. 3–11, 1985.

[21] K. Chen, "On the non-existence of perfect codes with rank distance," *Mathematische Nachrichten*, vol. 182, pp. 89–98, 1996.

[22] R. M. Roth, "Probabilistic crisscross error correction," *IEEE Trans. Info. Theory*, vol. 43, no. 5, pp. 1425–1438, September 1997.

[23] W. B. Vasantha and N. Suresh Babu, "On the covering radius of rank-distance codes," *Ganita Sandesh*, vol. 13, no. 1, pp. 43–48, 1999.

[24] T. Berger, "Isometries for rank distance and permutation group of Gabidulin codes," *IEEE Trans. Info. Theory*, vol. 49, no. 11, pp. 3016–3019, November 2003.

[25] E. M. Gabidulin and P. Loidreau, "On subcodes of codes in the rank metric," in *Proc. IEEE Int. Symp. on Information Theory*, Adelaide, Australia, September 2005, pp. 121–123.

[26] A. Kshevetskiy and E. M. Gabidulin, "The new construction of rank codes," in *Proc. IEEE Int. Symp. Info. Theory*, Adelaide, Australia, September 2005, pp. 2105–2108.

[27] M. Gadouleau and Z. Yan, "Properties of codes with the rank metric," in *Proc. IEEE Globecom*, San Francisco, CA, November 2006, pp. 1–5.

[28] ——, "Decoder error probability of MRD codes," in *Proc. IEEE Information Theory Workshop*, Chengdu, China, October 2006, pp. 264–268.

[29] ——, "On the decoder error probability of bounded rank-distance decoders for maximum rank distance codes," *IEEE Trans. Info. Theory*, vol. 54, no. 7, pp. 3202–3206, July 2008.

[30] P. Loidreau, "Properties of codes in rank metric," available at http://arxiv.org/pdf/cs.DM/0610057.

[31] M. Schwartz and T. Etzion, "Two-dimensional cluster-correcting codes," *IEEE Trans. Info. Theory*, vol. 51, no. 6, pp. 2121–2132, June 2005.

[32] G. Richter and S. Plass, "Fast decoding of rank-codes with rank errors and column erasures," in *Proc. IEEE Int. Symp. on Information Theory*, Chicago, June-July 2004, p. 398.

[33] P. Loidreau, "A Welch-Berlekamp like algorithm for decoding Gabidulin codes," in *Proc. International Workshop on Coding and Cryptography*, Bergen, Norway, March 2005, pp. 36–45.

[34] P. Delsarte, "Four fundamental parameters of a code and their combinatorial significance," *Information and Control*, vol. 23, no. 5, pp. 407–438, December 1973.

[35] T. Berger, *Rate Distortion Theory: A Mathematical Basis for Data Compression*, ser. Information and System Sciences Series, T. Kailath, Ed. Englewood Cliffs, NJ: Prentice-Hall, 1971.

[36] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.

[37] G. D. Cohen, I. Honkala, S. Litsyn, and A. C. Lobstein, *Covering Codes*. Elsevier, 1997.

[38] N. Suresh Babu, "Studies on rank distance codes," Ph.D Dissertation, IIT Madras, India, February 1995.

[39] W. B. Vasantha and R. J. Selvaraj, "Multi-covering radii of codes with rank metric," in *Proc. IEEE Information Theory Workshop*, Bangalore, India, October 2002, p. 215.

[40] P. Loidreau, "Étude et optimisation de cryptosystèmes à clé publique fondés sur la théorie des codes correcteurs," Ph.D. Dissertation, École Polytechnique, Paris, France, May 2001.

[41] E. Bannai and T. Ito, *Algebraic Cominatorics I. Association Schemes*. The Benjamin/Cummings Publishing Company, 1983.

[42] G. E. Andrews, *The Theory of Partitions*, ser. Encyclopedia of Mathematics and its Applications, G.-C. Rota, Ed. Reading, MA: Addison-Wesley, 1976, vol. 2.

[43] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-Regular Graphs*, ser. A Series of Modern Surveys in Mathematics. Springer-Verlag, 1989, vol. 18, no. 3.

[44] S. Roman, *Advanced Linear Algebra*, 2nd ed., ser. Graduate Texts in Mathematics. Springer, 2005, vol. 135.

[45] D. J. Kleitman, "On a combinatorial conjecture of Erdös," *Journal of Combinatorial Theory*, vol. 1, no. 2, pp. 209–214, September 1966.

[46] P. Delsarte, "Properties and applications of the recurrence $F(i+1, k+1, n+1) = q^{k+1}F(i, k+1, n) - q^k F(i, k, n)$," *SIAM Journal of Applied Mathematics*, vol. 31, no. 2, pp. 262–270, September 1976.

[47] G. D. Cohen, A. C. Lobstein, and N. J. A. Sloane, "Further results on the covering radius of codes," *IEEE Trans. Info. Theory*, vol. 32, no. 5, pp. 680–694, September 1986.

[48] G. van Wee, "Improved sphere bounds on the covering radius of codes," *IEEE Trans. Info. Theory*, vol. 34, no. 2, pp. 237–245, March 1988.

[49] ——, "Bounds on packings and coverings by spheres in q-ary and mixed Hamming spaces," *Journal of Combinatorial Theory A*, vol. 57, no. 1, pp. 116–129, May 1991.

[50] C.-P. Chen and F. Qi, "The best bounds of harmonic sequence," June 2003, available at arxiv:math.ca/0306233v1.

[51] W. E. Clark and L. A. Dunning, "Tight upper bounds for the domination numbers of graphs with given order and minimum degree," *The Electronic Journal of Combinatorics*, vol. 4, 1997.

[52] V. Pless, "Power moment identities on weight distributions in error correcting codes," *Information and Control*, vol. 6, pp. 147–152, 1963.

[53] D. Grant and M. Varanasi, "Weight enumerators and a MacWilliams-type identity for space-time rank codes over finite fields," in *Proc. Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, 2005, pp. 2137–2146.

[54] ——, "Duality theory for space-time codes over finite fields," *Advance in Mathematics of Communications*, vol. 2, no. 2, pp. 131–145, May 2008.

[55] G. Gasper and M. Rahman, *Basic Hypergeometric Series*, 2nd ed., ser. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2004, vol. 96.

[56] L. Carlitz, "q-Bernoulli numbers and polynomials," *Duke Mathematical Journal*, vol. 15, no. 4, pp. 987–1000, 1948.

[57] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Médard, "Resilient network coding in the presence of Byzantine adversaries," in *Proc. IEEE Infocom*, Anchorage, AK, May 2007, pp. 616–624.

[58] P. Delsarte, "Association schemes and t-designs in regular semilattices," *Journal of Combinatorial Theory A*, vol. 20, no. 2, pp. 230–243, March 1976.

[59] L. Chihara, "On the zeros of the Askey-Wilson polynomials with applications to coding theory," *SIAM Journal on Mathematical Analysis*, vol. 8, no. 1, pp. 191–207, January 1987.

[60] P. A. Chou, Y. Wu, and K. Jain, "Practical network coding," in *Allerton Conf. on Comm., Control, and Computing*, Monticello, IL, October 2003.

[61] T. Etzion and A. Vardy, "Error-correcting codes in projective space," in *Proc. IEEE Int. Symp. Information Theory*, Toronto, ON, July 2008, pp. 871–875.

[62] E. M. Gabidulin and M. Bossert, "Codes for network coding," in *Proc. IEEE Int. Symp. on Information Theory*, Toronto, ON, July 2008, pp. 867–870.

[63] W. J. Martin and X. J. Zhu, "Anticodes for the Grassmann and bilinear forms graphs," *Designs, Codes and Cryptography*, vol. 6, no. 1, pp. 73–79, July 1995.

[64] R. Ahlswede, H. K. Aydinian, and L. H. Khachatrian, "On perfect codes and related concepts," *Designs, Codes and Cryptography*, vol. 22, no. 3, pp. 221–237, January 2001.

[65] M. Schwartz and T. Etzion, "Codes and anticodes in the Grassmann graph," *J. Combin. Theory Ser. A*, vol. 97, no. 1, pp. 27–42, January 2002.

[66] S.-T. Xia and F.-W. Fu, "Johnson type bounds on constant dimension codes," *Designs, Codes and Cryptography*, vol. 50, no. 2, pp. 163–172, February 2009.

[67] P. Frankl and R. M. Wilson, "The Erdös-Ko-Rado theorem for vector spaces," *Journal of Combinatorial Theory A*, vol. 43, no. 2, pp. 228–236, November 1986.

[68] T. Etzion, "Perfect byte-correcting codes," *IEEE Trans. Info. Theory*, vol. 44, no. 7, pp. 3140–3146, November 1998.

[69] H. Wang, C. Xing, and R. Safani-Naini, "Linear authentication codes: Bounds and constructions," *IEEE Trans. Info. Theory*, vol. 49, no. 4, pp. 866–872, April 2003.

[70] V. Skachek, "Recursive code construction for random networks," 2008, available at http://arxiv.org/abs/0806.3650v1.

[71] R. J. McEliece and L. Swanson, "On the decoder error probability for Reed-Solomon codes," *IEEE Trans. Info. Theory*, vol. 32, no. 5, pp. 701–703, September 1986.

[72] K.-M. Cheung, "More on the decoder error probability for Reed-Solomon codes," *IEEE Trans. Info. Theory*, vol. 35, no. 4, pp. 895–900, July 1989.

[73] L. Tolhuizen, "A universal upper bound on the miscorrection probability with bounded distance decoding for a code used on an error-value symmetric channel," in *Proc. Eurocode, Int. Symp. on Coding Theory and Applications*, 1992, pp. 313–320.

[74] A. Kohnert and S. Kurz, "Construction of large constant dimension codes with a prescribed minimum distance," *Mathematical Methods in Computer Science, LNCS*, vol. 5393, pp. 31–42, December 2008.

[75] A. R. Rao and P. Bhimasankaram, *Linear Algebra*, 2nd ed. Hindustan Book Agency, May 2000.

[76] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge; New York: Cambridge University Press, 1985.

[77] S. M. Johnson, "A new upper bound for error-correcting codes," *IRE Trans. Info. Theory*, vol. 8, no. 3, pp. 203–207, April 1962.

[78] L. A. Bassalygo, "New upper bounds for error correcting codes," *Problems of Information Transmission*, vol. 1, no. 4, pp. 32–35, October-December 1965.

[79] M. Gadouleau and Z. Yan, "Constant-rank codes and their connection to constant-dimension codes," *submitted to IEEE Trans. Info. Theory*, July 2008, available at http://arxiv.org/abs/0803.2262.

[80] ——, "Packing and covering properties of rank metric codes," *IEEE Trans. Info. Theory*, vol. 54, no. 9, pp. 3873–3883, September 2008.

[81] ——, "Packing and covering properties of subspace codes," *submitted to IEEE Trans. Info. Theory*, 2008, available at http://arxiv.org/abs/0811.4163.

[82] ——, "Bounds on covering codes with the rank metric," *submitted to IEEE Communications Letters*, September 2008, available at http://arxiv.org/abs/0809.2968.

[83] The MathWorks, Inc., "MATLAB communications toolbox function reference: gf," available at http://www.mathworks.com/access/helpdesk/help/toolbox/comm/ug/gf.html.

[84] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, "A new table of constant weight codes," *IEEE Trans. Info. Theory*, vol. 36, no. 6, pp. 1334–1380, November 1990.

Vita

Maximilien Rémy Gadouleau was born on December 28th, 1983, in Mont-Saint-Aignan, France. He is the son of Mr. Rémy Jean Gadouleau and Mrs. Viviane Simone Gadouleau, born Revert. He attended middle and high school in Institution du Sacré-Cœur, Rouen, France. He graduated from high school in June 1999, with honors. He then obtained a Diplôme d'Ingénieur from École Supérieure d'Ingénieurs en Génie Électrique (ESIGELEC), Mont-Saint-Aignan, France, in December 2004 and a Master of Science in Computer Engineering at Lehigh University, Bethlehem, Pennsylvania, in December 2005. Since January 2006, he is a doctoral candidate at Lehigh University. He is an IEEE Student Member, an IEEE IT Society Member, and a PC Rossin Doctoral Fellow.