Institut de Mathématiques
Faculté des Sciences
Université de Neuchâtel

UNIVERSITÉ DE NEUCHÂTEL

A thesis presented for the degree of

PhD in Mathematics

Codes with extremality properties in the Rank Metric and in the Sum-Rank Metric

Author : Cristina Landolina

Supervisor : Prof. Dr. Elisa Gorla

Jury member : Dr. Umberto Martínez-Peñas

Jury member : Prof. Dr. Joachim Rosenthal

Jury member : Prof. Dr. Alain Valette

Defense date : December 17, 2021

February 22, 2022

UNIVERSITÉ DE NEUCHÂTEL

Faculté des Sciences
Secrétariat-décanat de Faculté
Rue Emile-Argand 11
2000 Neuchâtel – Suisse
Tél : + 41 (0)32 718 21 00
E-mail : secretariat.sciences@unine.ch

IMPRIMATUR POUR THESE DE DOCTORAT

La Faculté des sciences de l'Université de Neuchâtel autorise l'impression de la présente thèse soutenue par

Madame Cristina LANDOLINA

Titre:

"Codes with extremality properties in the Rank Metric and in the Sum-Rank Metric"

sur le rapport des membres du jury composé comme suit:

- Prof. Elisa Gorla, directrice de thèse, Université de Neuchâtel, Suisse
- Prof. Alain Valette, Université de Neuchâtel, Suisse
- Dr Umberto Martinez-Penas, Université de Neuchâtel, Suisse
- Prof. Joachim Rosenthal, Université de Zürich

Neuchâtel, le 25 janvier 2022

Le Doyen, Prof. A. Bangerter

Meiner Familie gewidmet

Pietro Landolina, Morisetta Landolina,
Vincenzo Landolina und Großeltern

Alla mia famiglia

Pietro Landolina, Morisetta Landolina,
Vincenzo Landolina e nonni

Résumé

La thèse suivante est une contribution à la recherche dans le domaine de la théorie des codes. Le but de cette travail scientifique est de mieux comprendre les codes dans la métrique du rang, ainsi que ceux ayant la métrique du somme-rang. Les codes avec la métrique du rang [19, 22, 63] sont connus dans la théorie des codes pour être des codes linéaires et capables de corriger des erreurs dans appelée métrique du rang. Nous les considérerons comme des espaces vectoriels linéaires des matrices d'une certaine taille fixée avec entrées dans un corps fini. Cette famille de codes peut s'utiliser par example lors de control d'erreurs dans le codage aléatoire linéaire d'un réseau (random linear network coding). Dans ce codage, des informations sont diffusées et reçues sous forme d'un espace vectoriel sur un réseau inconnu. Les codes avec la métrique du somme-rang [55, 56] peuvent être considérés comme une généralisation des codes avec la métrique du rang. Par conséquent, l'étude des codes optimaux avec des métriques de rang et de somme de rang est aussi intéressante d'un point de vue pratique que théorique des mathématiques.
Ce travail de recherche a eu pour but de definir et classifier des codes optimaux dans les deux métriques, ainsi que de déterminer leurs invariants.
Plusieurs résultats fondamentaux sur la structure des espaces vectoriels des matrices sur des corps finis avec un certain rang maximal [17, 21, 53] ont donné lieu à une vaste classification des familles des codes avec la métrique du rang. En collaboration avec Elisa Gorla, nous avons fait partiellement usage de ces résultats pour pouvoir classifier une nouvelle famille de codes avec la métrique du rang. La nouvelle famille sera définie dans la première partie de la thèse comme étant des *quasi anticodes optimals*, à rang maximal extrême pour une dimension donnée. L'extrémalité des paramètres s'accompagne de l'introduction d'une borne qui est équivalente à la borne d'anticode déjà connue, mais plus générale. Nous verrons que les codes atteignant la borne d'anticode atteignent également cette nouvelle borne, alors que les codes atteignant la nouvelle limite n'atteignent pas la borne d'anticode en général. Nous considérons donc une classe plus large de codes avec la métrique du rang ayant un rang maximal extrémal pour leur dimension.
La deuxième partie du présent travail est le fruit d'une collaboration avec Eduardo Camps Moreno, Elisa Gorla, Elisa Lorenzo García, Umberto Martínez-Peñas et Flavio Salizzoni, et est consacrée aux codes dans la métrique du somme-rang. La métrique de la somme du rang a une histoire beaucoup plus courte que la métrique du rang et est donc moins bien comprise. Pour cette raison, la dérivation de bornes et l'étude des propriétés de base des codes dans la métrique du somme-rang sont d'un grand intérêt. À cette fin, nous donnons notre version pour la métrique du somme-rang de deux des bornes les plus étudiées dans la théorie des codes avec la métrique du rang: la borne de Singleton et la borne d'anticode. De plus, nous définissons et décrivons des codes atteignant respectivement une de ces bornes. Afin d'étudier les invariants, nous définissons les isométries pour la métrique du somme-rang et les caractérisons

toutes. Enfin, nous donnons une définition appropriée d'un invariant clé, à savoir les poids généralisés d'un code métrique de somme de rangs, puis nous examinons dans quels cas les poids d'un code déterminent ceux de son dual.

Mots clés: théorie des codes, métrique du rang, métrique du somme-rang, codage linéaire d'un réseau, espace vectoriel des matrices, codes optimales.

Summary

This thesis is a contribution to the research in coding theory. The aim of this work is to better understand codes in the rank metric, as well as those in the sum-rank metric. Rank metric codes [19, 22, 63] are known in coding theory for being linear error-correcting codes in the so called rank metric. We shall consider them as linear vector spaces of matrices of a given size with entries in a finite field. These type of codes find their application for instance in controlling errors in random linear network coding, where information is transmitted and received in form of a vector space over an unknown network. Sum-rank metric codes [55, 56] can be seen as a generalization of codes in the rank metric. The study of optimal rank-metric and sum-rank metric codes is therefore interesting both from a practical and from a mathematical theoretical point of view.

The present thesis is concentrated on defining and classifying optimal codes in both metrics, as well as on determining their invariants.

Several fundamental results on the structure of matrix spaces over finite fields with a certain maximum rank [17, 21, 53] give rise to a broad classification of families of rank-metric codes. In a joint work with Elisa Gorla we make partially use of these results to completely classify a new family of rank-metric codes, that will be defined in the first part of the thesis. This family of codes, that is the family of *quasi optimal anticodes*, has extremal maximum rank for a given dimension. The extremality of the parameters comes with the introduction of a bound which is equivalent to the already known anticode bound, yet more general. We will see that codes attaining the anticode bound do also attain this new bound, whereas codes attaining the new bound do not attain the anticode bound in general. We are therefore considering a larger class of rank-metric codes having extremal maximum rank for their dimension.

The second part of the current work is a collaboration with Eduardo Camps Moreno, Elisa Gorla, Elisa Lorenzo García, Umberto Martínez-Peñas and Flavio Salizzoni, and is dedicated to codes in the sum-rank metric. The sum-rank metric has a much shorter history than the rank metric and is therefore less well understood. For this, the derivation of bounds and the study of basic properties of sum-rank metric codes is of great interest. To this end, we give our sum-rank metric version of two of the most studied bounds in the theory of rank-metric codes: the Singleton bound and the anticode bound. Moreover, we define and describe codes attaining respectively one of these bounds. In order to study invariants we define sum-rank metric isometries and characterize them all. Finally, we give an appropriate definition of a key invariant, namely the generalized weights of a sum-rank metric code, and then explore in which cases the weights of a code determine those of its dual.

Keywords: coding theory, rank metric, sum-rank metric, linear network coding, vector space of matrices, optimal codes.

Acknowledgments

If I am able to present this thesis in the current form, it is due to my supervisor Professor Dr. Elisa Gorla. Over time I become aware of how lucky I was to have a supervisor following week by week my research progress. Every issue in my PhD life became less unsolvable after having talked to her. She was not only fundamental for my scientific work but also for my professional and personal development during the last four years. I have learned incredibly much from her. For me she is not only a professional and talented advisor, but also a caring friend. For this I would sincerely like to thank her.
I may also thank the coding theory group working under the supervision of Professor Dr. Joachim Rosenthal at the University of Zurich. Our weekly seminar was a great opportunity for meeting part of the coding theory community around the world. I got interesting mathematical inputs by several talks and enjoyed our social dinners, who give rise to a lot of interesting conversations. Thanks to Professor Dr. Joachim Rosenthal, Professor Dr. Anna-Lena Horlemann, Gianira Alfarano, Dr. Karan Khathuria, Dr. Julia Lieb, Dr. Alessandro Neri, Dr. Elif Saçikara, Simran Tinani and Dr. Violetta Wegner for having been part of this great group.
In Neuchâtel I have encountered incredible people who helped me to spent these four years in a memorable way. First of all I would like to thank Professor Dr. Alessio Camminata who was Maître Assistant in the mathematical departement in the first years of my PhD. He was the first one I had the opportunity to talk to about my mathematical brainteasers. He and his wife Elisa made me feel a little bit more at home in Neuchâtel delighting me with wonderful Italian dinners. Many thanks to both of them for having been so lovely with me.
Moreover I want to thank Dr. Hugues Mercier and Dr. Roberta Barbi for sharing their information theoretical research with my supervisor and me in a weekly meeting. A special thanks goes to Dr. Elisa Lorenzo García and Dr. Umberto Martínez-Peñas, both Maître Assistants in Neuchâtel, who worked together with me in part of the research project of this thesis. I also had pleasing and constructive conversations in many different occasions with Giuseppe Cotardo, Professor Dr. Heide Gluesing-Luerssen, Dr. Hiram H. López, Professor Dr. Felice Manganiello, Professor Dr. Gretchen L. Matthews, Professor Dr. Alberto Ravagnani and Dr. Oliver Kelsey Tough.
In my last year in Neuchâtel I had the pleasure to meet several colleagues who supported me until now: Flavio Salizzoni, Giulia Gaggero, Eduardo Camps Moreno and Leandro Di Caprio. I will for sure never forget all the mathematical conversations that I had with Flavio. Conversations that inspired my research very often. I wish him a brilliant career as a mathematician, that I am sure he will have. Together with Giulia they contributed meaningfully to the success of my personal aims in this last year of PhD. I want to thank Giulia for her zest for life making me escape very often mental ups and downs. Her art of being colored many black days and for this I have to thank her. I also had the pleasure to meet Eduardo, who has spent one year in Neuchâtel.

His fascinating stories about the Mexican culture gave me a lot of new social point of views. In addition to that he gave me the opportunity to improve my Spanish, even doing mathematics with him. Last but not least I want to thank Leandro Di Caprio, the only non mathematician among my colleagues at the University of Neuchâtel. The way he raised my spirit several times and supported me personally in difficult moments means a lot to me.
The entire mathematical department in Neuchâtel, headed by Professor Dr. Michel Benaïm, Professor Dr. Bruno Colbois, Professor Dr. Elisa Gorla, Professor Dr. Aleksandr Kolpakov, Professor Dr. Felix Schlenk and Professor Dr. Alain Valette, is made of incredible kind people creating a nice and cooperative atmosphere.I want to thank all of my french speaking PhD colleagues, who helped me improving my french exercise classes. I, and for sure also my students, have appreciated their help a lot. I arrived in Neuchâtel without speaking a single word of french but now I can at least tell you this: *Merci pour tous les beaux moments passés ensemble!*
Finally I wish to thank my family and friends, Martina Kupczynski and Alina Schuljak in particular, who always believed in me and motivated me to achieve my goals. Thank you for always being there.

Contents

Introduction and Motivation

Rank-metric codes are spaces of matrices, endowed with the rank metric, of a given size with entries in a finite field. The distance between two elements in the code is obtained by measuring the rank of their difference. The sum-rank metric can be considered as a natural generalization of both the Hamming metric and the rank metric. Indeed, elements of a sum-rank metric code can be seen as a list of matrices of given sizes with entries in a finite field.

Codes in the rank metric and in the sum-rank metric recently attracted interest due to their remarkable list of applications. In particular we mention linear network coding using rank-metric codes [39, 67] and multishot network coding using sum-rank metric codes [55, 56] in an analogous manner. In this setting both codes are proposed for error correction in noisy networks. Koetter and Kschischang in [39] consider reliable communication using the noncoherent transmission model for random linear network coding, where the underlying network topology and the linear functions performed at each internal node are unknown. Therein the proposed operator channel induces the transmission of vector spaces instead of just vectors, which justifies the introduction of the subspace metric and of subspace codes. The fact that a lifted optimal rank-metric code results in an almost optimal subspace code [67], motivates the interest of rank-metric codes in this area. As a generalization of using rank-metric codes for linear network coding Nóbrega and Uchoa-Filho in [56] were the first to propose sum-rank metric codes for multishot network coding. The only known way of improving the error-correction capability of an error-correction code in a single use of the network is to enlarge the base field or to increase the packet size. Sum-rank metric codes in a multi-shot scenario resolve this issue. In order to add some dependencies among the nodes sum-rank metric codes in multishot network coding are often constructed as convolutional codes, giving rise to the family of convolutional rank-metric codes [54]. Wachter-Zeh, Stinner and Sidorenko in [71] gave the first construction and decoding of convolutional rank-metric codes in the particular case of unit memory convolutional codes.

Another remarkable application of rank-metric codes can be found in code-based cryptography. Code-based cryptography is considered to be a major candidate for post-quantum resistant cryptosystems. After adapting some security parameters of the MacEliece public key cryptosystem [52] proposed 1978, one obtains an unbroken public key cryptosystem which is believed to be quantum-computer resistant. A significant drawback when using error-correcting codes for constructing cryptosystems is their large memory requirement. In fact, McEliece's public key sizes are close to a million bits, whereas RSA key sizes are about a few thousand bits [9]. Rank-metric versions of the McEliece public key cryptosystem mainly consist of substituting the secret Goppa code with a Gabidulin code [23–26, 45]. Whilst the matrix structure of a Gabidulin generator matrix makes it possible to reduce significantly the key sizes, it is exactly this strong structure of Gabidulin codes which leads to a series of structural attacks, for ex-

ample Gibson's attack [28] and Overbeck's attack [58]. Producing a valid rank-metric version of the original McEliece cryptosystem is the subject of current research. One of the most promising proposals is Loidreau's public-key encryption scheme presented in [45]. There are also rank-based cryptosystem candidates to NIST's competition for post-quantum cryptography: Rank-Ouroboros [1] and LAKE [3] in the category *post-quantum key exchange* and LOCKER [4] in the category *post-quantum public key encryption*. These three candidates merged to ROLLO [5] are 2nd round submissions to the NIST's standardization competition.
Other interesting applications of rank-metric and sum-rank metric codes can be found in the construction of space-time codes for wireless communications [60, 65, 70] and in the repair in distributed storage [12, 49].
The rank distance has been extensively studied since its first appearance in Delsarte's seminal paper in 1978 [19]. The author extended the concept of *arithmetic distance* introduced by Hua in [36], defining the rank distance on the set of bilinear forms, namely rectangular matrix spaces. Rank-metric codes were first considered as spaces of matrices defined over a finite field. Later in 1985, Gabidulin [22] and Roth [63] independently rediscovered a class of rank-metric codes which are represented as vectors over a field extension and are linear over the same larger field. We will see later that every rank-metric code in vector representation can be considered as a matrix rank-metric code up to the choice of basis of the extension field over the base field. As an extension of both the Hamming and the rank distance, the sum-rank distance has a much shorter history and is therefore less well understood. First constructions of sum-rank metric codes arise via convolutional codes and can be attributed to Nóbrega and Uchoa-Filho [55, 56] in the context of multishot network coding. However in the present thesis we shall consider linear sum-rank metric codes as block codes, namely as subspaces of the product of matrix spaces over a finite field equipped with the sum-rank distance.
Parameters of a rank-metric code have been related by several bounds. The most known one is the Singleton bound for rank-metric codes, originally introduced for codes in the Hamming metric [68]. Delsarte formulated the Singleton bound for rank-metric codes defined over the base field [19, Theorem 5.4] and Gabidulin derived the same bound for rank-metric codes defined over an extension field [22, Corollary of Lemma 1]. For the sum-rank metric one may derive a trivial Singleton bound directly from the original one in the Hamming metric as shown in [47, Proposition 34]. A more general Singleton bound for sum-rank metric codes defined over spaces of matrices with different numbers of rows and columns is given in [11], where other fundamental bounds for the sum-rank metric are also derived. The Singleton bound relates the dimension of a code with its minimum distance. Codes attaining this bound are the ones maximizing the minimum distance for a given dimension. The larger the minimum distance of an error-correcting code, the higher its error-correction capability in general, hence codes attaining the Singleton bound are the ones that are considered for applications. Optimal codes in the sense of the Singleton bound are called Maximum Rank Distance (MRD) codes in the rank metric and analogously Maximum Sum-Rank Distance (MSRD) codes in the sum-rank metric. Unlike Maximum Distance Separable

(MDS) codes in the Hamming metric, Delsarte showed that MRD codes exist for all field sizes, matrix sizes and minimum distances or dimensions [19, Theorem 6.3]. In fact, in the same paper he gives a construction of MRD codes for all parameters using bilinear forms. Later Gabidulin and Roth rediscovered the same family of MRD codes in vector representation [22, 63], which are since known as Gabidulin codes. For a long time there has been little interest in constructing new families of optimal rank-metric codes, since Gabidulin codes were sufficient for most applications. However, the matrix structure of Gabidulin codes appears to be unsuitable for some applications, for instance public key encryption schemes. This partially motivates the community to search for new constructions. An overview of MRD constructions different from Gabidulin codes can be found in [64, Section 3]. As one may guess, any MRD code is also an MSRD code. Yet this is not the only way to obtain an MSRD code. There are MSRD codes not coming from MRD codes, for example linearized Reed-Solomon codes defined in [47], which justifies the interest in finding new constructions of MSRD codes. Moreover it is not yet known if MSRD codes exist for all choices of parameters. This would solve in particular the MDS conjecture as pointed out in [50, Section VI]. Finally we wish to mention the family of quasi MRD codes defined in [15], which motivated part of the present thesis. These are codes with dimension not divisible by the maximum between the number of rows and columns, but still optimal in the sense of an equivalent Singleton bound.

Another relevant bound relating the dimension of a code to its maximum rank is the anticode bound. The anticode bound was stated in its current form by Meshulam in [53, Theorem 2] in the square case; the proof can easily be generalized to the rectangular case. The statement of the bound is that the dimension of a subspace of matrices can be at most its maximum rank times the maximum between the number of rows and columns. An anticode bound for the sum-rank metric is presented in [10, Theorem 2.2]. Codes attaining the anticode bound are called optimal anticodes. If we assume that we have more columns than rows and fix some column space V, it is easy to see that the set of matrices having column space contained in V is an optimal anticode in the rank metric. Meshulam in [53, Theorem 3] in the square case and de Seguins Pazzis in [17, Theorem 4 and Theorem 6] proved that these are exactly all optimal anticodes in the rank metric. A classification of optimal anticodes in vector representation was given by Ravagnani in [61, Theorema 18]. In [11, Theorem 3.1] the authors give a complete classification of optimal linear sum-rank anticodes in the sense of the anticode bound given in the same paper. The optimal linear sum-rank anticodes in [11] are essentially given by the product of the entire matrix space and the zero space.

Invariants are useful tools in the classification up to equivalence of codes. Before introducing some important rank-metric and sum-rank invariants, we wish to describe the notion of equivalence for the rank-metric. Two rank-metric codes are said to be equivalent if there is a rank-preserving linear map, an isometry, mapping one to the other. For codes in matrix representation we consider linear isometries over the base field, whereas for rank-metric codes in vector representation the isometry is linear over an extension field. It is easy to show for instance that if two matrix rank-metric codes

are equivalent, then so are their associated vector rank-metric codes, [31, Proposition 1.15]. Linear isometries of matrix rank-metric codes were completely classified by Wan for fields of characteristic 2 [72] and by Hua for fields of odd characteristic [36]. Berger in [7] characterized isometries over an extension field. As of yet, the only known equivalence notion in the sum-rank metric is the one given in Section 4.3.

One of the most studied invariants are generalized weights. These were introduced for linear block codes in the Hamming metric in [34]. Wei proposed them in the context of wire-tap channels to measure information leakage to an undesired wire-tapper [73]. In [41, Definition 2] the authors give a definition of relative generalized weights for rank-metric codes in vector representation, which are linear over an extension field. These weights measure information leakage to a wire-tapper in linear network coding. Other definitions of generalized weights for rank-metric codes linear over an extension field are given in [37,61]. In [51,61] the authors give two different definitions of generalized weights of rank-metric codes in matrix representation. On the one hand the weights in [61] define a rank-metric invariant of the codes, but they do not measure information leakage to a wire-tapper. On the other hand the weights in [51] are the right tool to measure information leakage, but they are not rank-metric code invariants. A detailed analysis of the differences between these two definitions can be found in [30, Section 5]. A first definition of generalized weights for the sum-rank metric can be found in [48, Section 4.1].

Another invariant that we shall consider in the first part of the present thesis are q-polymatroids, which are the q-analog of polymatroids (for a reference see [59, 74]). In [66] and [31] the authors independently associate a q-polymatroid to every rank-metric code, depending on the size of the space of matrices. Moreover they show how different properties, and even other invariants, can be captured by the associated q-polymatroids.

This work is a contribution to the study of rank-metric codes with extremality properties as well as to the discovery of fundamental properties and optimal codes in the sum-rank metric. We begin by introducing a new family of rank-metric codes, which is motivated by the following observation: The dimension of optimal anticodes in the rank metric is by definition divisible by the maximum between the number of rows and columns. We will consider the family of rank-metric codes whose dimension is not divisible by this number, but does still attain an equivalent anticode bound. We call these codes quasi optimal anticodes. If in addition to this the dual of a quasi optimal anticode is quasi optimal, we call it a dually quasi optimal anticode. We will see that in contrast to the already know optimal codes in the rank metric, the dual of a quasi optimal anticode is not quasi optimal in general. A complete classification of dually quasi optimal anticodes is given. Leaning on their classification we shall study some key invariants of these codes, namely generalized weights, the rank distribution and q-polymatroids. In the second part of this thesis we consider codes in the sum-rank metric giving a definition of generalized sum-rank weights of codes which are linear over the base field. This definition extends the generalized rank weights given in [61]. In the Appendix we demonstrate how to modify the definition in order to extend generalized weights as given in [51], and thereby to measure information leakage in

multishot network coding. Our definition of generalized sum-rank weights is based on optimal anticodes in the sum-rank metric, as in the rank-metric case [61]. To this end, we provide an anticode bound for the sum-rank metric extending the Hamming-metric anticode bound [61, Proposition 6] and the rank-metric anticode bound. We then provide a classification of optimal anticodes in the sum-rank metric.

This dissertation is organized as follows. In Section 1, we describe some basic properties and applications to linear network coding and code-based cryptography, in the rank metric. In Section 2, which is joint work with Elisa Gorla, we introduce the family of quasi optimal anticodes. In Subsection 2.1 we recall some matrix theoretical results on the structural classification of matrix spaces of a given maximum rank. We finally give in this subsection a full classification of dually quasi optimal anticodes. Subsections 2.2, 2.3 and 2.4 are devoted to the study of invariants such as generalized weights, rank distribution and rank functions of the q-polymatroid of a larger family of quasi optimal anticodes.

In Section 3 we collect some preliminaries on the sum-rank metric and describe their application to multishot network coding. Section 4, which is a collaboration with Eduardo Camps Moreno, Elisa Gorla, Elisa Lorenzo García, Umberto Martínez-Peñas and Flavio Salizzoni, we provide an anticode bound and generalized weights in the sum-rank metric. In Section 4.1 we establish a lower bound on the maximum rank of cosets of linear rank-metric codes, extending results from Meshulam [53] to cosets. Using these results, we provide in Section 4.2 an anticode bound for sum-rank metric codes and give an explicit description and classification of optimal anticodes for the sum-rank metric. In Section 4.3 we study isometries of sum-rank metric codes. Such isometries allow us to define the notion of equivalent codes, allowing us to say if a given parameter of a code is a sum-rank invariant. In Section 4.4, we use optimal anticodes to define and obtain the main properties of generalized sum-rank weights. Finally in Section 4.5, we use the aforementioned results to define and study MSRD codes and r-MSRD codes in the general scenario considered in this work, namely codes in matrix representation with different numbers of rows and columns.

Notation

q	A prime power
$\mathbb{F}_q$	The finite field of q elements
n, m	Positive integers
$[n]$	The set of integers $\{1, \ldots, n\}$
$u \in \mathbb{F}_q^n$	A row vector of length n with entries in $\mathbb{F}_q$
$u^t \in \mathbb{F}_q^n$	The transpose of a row vector $u \in \mathbb{F}_q^n$
e_i	The column vector with the only nonzero entry equal to 1 at position i
$\langle u_1, \ldots, u_i \rangle$	The $\mathbb{F}_q$-linear subspace spanned by $\{u_1, \ldots, u_i\}$
$V \subseteq \mathbb{F}_q^n$	An $\mathbb{F}_q$-linear subspace V of $\mathbb{F}_q^n$
$0 \subseteq \mathbb{F}_q^n$	The zero subspace $\{0\}$ of $\mathbb{F}_q^n$
$\mathcal{P}(X)$	The collection of all subspaces of a vector space X of fixed dimension
$A \oplus B$	The direct sum of vector spaces A and B
$\mathbb{F}_q^{n \times m}$	The set of $n \times m$ matrices with entries in $\mathbb{F}_q$
$\mathrm{GL}_n(\mathbb{F}_q)$	The set of invertible $n \times n$ matrices over $\mathbb{F}_q$
$0_{n \times m}$	The zero matrix of size $n \times m$
I_n	The identity matrix of size $n \times n$
$E_{i,j}$	The matrix with the only nonzero entry equal to 1 at position (i, j)
$M = (M_{i,j})_{(i,j)}$	A matrix M with entry $M_{i,j}$ at position (i, j)
$M^t = (M_{j,i})_{(i,j)}$	The transpose of a matrix M with entry $M_{j,i}$ at position (i, j)

$M(S, L)$	The submatrix of M with entries $M_{i,j}$ where $i \in S$ and $j \in L$
$\mathrm{rowsp}(M)$	The $\mathbb{F}_q$-linear space generated by the rows of a matrix $M \in \mathbb{F}_q^{n \times m}$
$\mathrm{colsp}(M)$	The $\mathbb{F}_q$-linear space generated by the columns of a matrix $M \in \mathbb{F}_q^{n \times m}$
$\mathrm{rank}(M)$	The rank of a matrix M
$\dim(V)$	The dimension of an $\mathbb{F}_q$-linear vector space V
ℓ	A positive integer
$n_1, \ldots, n_\ell, m_1, \ldots, m_\ell$	Positive integers
$\mathbb{M}$	The product of matrix spaces $\mathbb{F}_q^{m_1 \times n_1} \times \cdots \times \mathbb{F}_q^{m_\ell \times n_\ell}$
$C \in \mathbb{M}$	A list of matrices $C = (C_1, \ldots, C_\ell)$ with $C_i \in \mathbb{F}_q^{m_i \times n_i}$ for $i \in [\ell]$

1 Rank-Metric Codes and some Applications

1.1 Definitions and fundamental Properties

In the following we give an introduction to rank-metric codes and state some fundamental related results. Up to transposition, we may assume without loss of generality that $n \leq m$. In other words we will consider matrices to have more columns than rows.

Definition 1.1. The **rank distance** of $M, N \in \mathbb{F}_q^{n\times m}$ is given by the function

$$\begin{array}{rccl} d & : & \mathbb{F}_q^{n\times m} \times \mathbb{F}_q^{n\times m} & \longrightarrow & \mathbb{N} \\ & & (M, N) & \longmapsto & \mathrm{rank}(M - N). \end{array}$$

A **rank-metric code** $\mathcal{C}$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{n\times m}$ equipped with the rank distance. The **dimension** of $\mathcal{C}$ over $\mathbb{F}_q$ is denoted by $\dim(\mathcal{C})$. Further, we let $\mathrm{d}(\mathcal{C}) = \min\{\mathrm{rank}(M) : M \in \mathcal{C}, M \neq 0\}$ be the **minimum distance** of a nonzero rank-metric code $\mathcal{C}$. In a similar way, the **maximum rank** is given by $\mathrm{maxrk}(\mathcal{C}) = \max\{\mathrm{rank}(M) : M \in \mathcal{C}\}$.

In [22] and [63] the authors study a class of rank-metric codes defined over $\mathbb{F}_{q^m}$.

Definition 1.2. The rank distance of $u, v \in \mathbb{F}_{q^m}^n$ is given by the function

$$\begin{array}{rccl} d & : & \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n & \longrightarrow & \mathbb{N} \\ & & (u, v) & \longmapsto & \mathrm{rank}(u - v) = \dim(\langle u_1 - v_1, \ldots, u_n - v_n\rangle). \end{array}$$

A **vector rank-metric code** C is an $\mathbb{F}_{q^m}$-linear subspace of $\mathbb{F}_{q^m}^n$ equipped with the rank distance.

Every vector rank-metric code can be considered as a rank-metric code in the following way: Let $\Phi = \{\phi_1, \ldots, \phi_m\}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Then we can identify a vector rank-metric code $C \subseteq \mathbb{F}_{q^m}^n$ with a rank-metric code $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ by the relation

$$u_i = \sum_{j=1}^{m} M_{i,j}\phi_j, \tag{1}$$

where $u = (u_1, \ldots, u_n) \in C$ and $M = (M_{i,j})_{(i,j)\in[n]\times[m]} \in \mathcal{C}$ having in row i the $\mathbb{F}_q$-coordinates of u_i respect to the basis Φ.
In this thesis we will consider rank-metric codes defined over $\mathbb{F}_q^{n\times m}$. We decide to give the notion of vector rank-metric codes for the better understanding of Section 1.2 and Section 1.3, which describe applications of rank-metric codes.

In view of matrix classifications up to equivalence we introduce the notion of equivalence of rank-metric codes. Two rank-metric codes are equivalent if there is a linear rank-preserving homomorphism mapping one code into the other.

Definition 1.3. An $\mathbb{F}_q$**-linear isometry** φ of $\mathbb{F}_q^{n\times m}$ is an $\mathbb{F}_q$-linear rank-preserving homomorphism, i.e. $\mathrm{rank}(\varphi(A)) = \mathrm{rank}(A)$ for all $A \in \mathbb{F}_q^{n\times m}$. Let $\mathrm{Isom}_{\mathbb{F}_q}(\mathbb{F}_q^{n\times m})$ be the collection of $\mathbb{F}_q$-linear isometries of $\mathbb{F}_q^{n\times m}$. Two rank-metric codes $\mathcal{C}, \mathcal{D} \subseteq \mathbb{F}_q^{n\times m}$ are **equivalent** if there is $\varphi \in \mathrm{Isom}_{\mathbb{F}_q}(\mathbb{F}_q^{n\times m})$ such that $\mathcal{C} = \varphi(\mathcal{D})$. We denote the equivalence by $\mathcal{C} \sim \mathcal{D}$.

Linear isometries of $\mathbb{F}_q^{n\times m}$ are classified in [36] for odd characteristic and in [72] for characteristic equal to 2.

Theorem 1.4. Let $\varphi \in \mathrm{Isom}_{\mathbb{F}_q}(\mathbb{F}_q^{n\times m})$. Then

(a) if $n \neq m$, there exist $N \in \mathrm{GL}_n(\mathbb{F}_q)$ and $M \in \mathrm{GL}_m(\mathbb{F}_q)$ such that $\varphi(A) = NAM$ for all $A \in \mathbb{F}_q^{n\times m}$.

(b) if $n = m$, there exist $N, M \in \mathrm{GL}_n(\mathbb{F}_q)$ such that $\varphi(A) = NAM$ for all $A \in \mathbb{F}_q^{n\times m}$, or $\varphi(A) = NA^tM$ for all $A \in \mathbb{F}_q^{n\times m}$.

Further we define the dual of a rank-metric code $\mathcal{C}$ using the standard scalar product for matrices.

Definition 1.5. Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ be a rank-metric code and let $\mathrm{tr}(A)$ denote the trace of a square matrix A. The **dual** of $\mathcal{C}$ is defined as

$$\mathcal{C}^\perp = \{M \in \mathbb{F}_q^{n\times m} : \mathrm{tr}(MN^t) = 0 \text{ for all } N \in \mathcal{C}\}.$$

In the following we decide to adopt the notion of support given in [30, Definition 2.2] for $n \leq m$. Support spaces will be a useful tool in the classification of optimal anticodes (Definition 1.9).

Definition 1.6. Let $V \subseteq \mathbb{F}_q^n$ be a subspace. Then

$$\mathrm{Mat}(V) = \{M \in \mathbb{F}_q^{n\times m} : \mathrm{colsp}(M) \subseteq V\} \subseteq \mathbb{F}_q^{n\times m}$$

denotes the **matrix space supported on the vector space** V. For $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ a rank-metric code, let

$$\mathcal{C}(V) = \{M \in \mathcal{C} : \mathrm{colsp}(M) \subseteq V\} \subseteq \mathcal{C}$$

be the **subcode of** $\mathcal{C}$ **supported on** V.

Notice that whenever we want to refer to the matrix space supported by a certain row space we will consider the transposed version of the support given in Definition 1.6.

An important role in the motivation of this paper is taken by deriving bounds on rank-metric codes. In the sequel we give two of the most relevant inequalities, one relating the minimum distance and one relating the maximum rank to the dimension of a rank-metric code.

Theorem 1.7. (Singleton bound) Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ be a rank-metric code. Then

$$\dim(\mathcal{C}) \leq m(n - \mathrm{d}(\mathcal{C}) + 1). \tag{2}$$

The **Singleton bound** for rank-metric codes was presented by Delsarte in [19]. It is the rank-metric version of the well-known Singleton bound in the Hamming metric. Codes meeting bound (2) are known as **Maximum Rank Distance Codes (MRD codes)** and have been extensively studied. As we already pointed out in the introduction, these codes are demanded in applications since they have the maximum possible minimum distance for a given dimension and so the highest error-correction capability for several applications.
We shall present now an upper bound on the dimension involving the maximum rank, instead of the minimum distance as seen in (2). A classical theorem by Flanders in [21] states that the dimension of a linear space of matrices, whose rank is less than or equal to a given $r \leq n$, is upper bounded by mr. The results in [21] are proved under the assumption that the cardinality of the base field is strictly greater than r. The square case with $r = n - 1$ for an arbitrary field size was proved by Dieudonné in [20]. In particular Dieudonné proved that $n^2 - n$ is an upper bound for any subspace of singular square matrices with entries in an arbitrary commutative field. Subspaces attaining the bound are then those of maximaum rank equal to $n - 1$. Finally, Meshulam in [53] showed that the assumptions on the base field are unnecessary for deriving the bound on the dimension. In fact, the next bound was proved in [53] and goes under the name of **anticode bound**.

Theorem 1.8. (Anticode bound) Let $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ be a rank-metric code. Then

$$\dim(\mathcal{C}) \leq m \operatorname{maxrk}(\mathcal{C}). \tag{3}$$

Definition 1.9. An **optimal anticode** $\mathcal{A} \subseteq \mathbb{F}_q^{n \times m}$ is a rank-metric code which satisfies

$$\dim(\mathcal{A}) = m \operatorname{maxrk}(\mathcal{A}).$$

The classification of matrix spaces with least possible maximum rank for a given dimension follows the same history as the derivation of the anticode bound. Dieudonné in 1948 [20] gave a charaterization of optimal anticodes of maximum rank $n - 1$ in the square case. Flanders in [21] first classified optimal anticodes under the assumption that the cardinality of the base field is strictly greater than r and that the characteristic differs from 2. Atkinson and Lloyd in [6] obtained the same result with the assumption only on the field size. Meshulam in [53, Theorem 3] finally gives a complete classification of optimal anticodes without assumptions on the field size. Moreover the same result follows from [17, Theorem 4 and Theorem 6], where de Seguins Pazzis considers a lower bound on the dimension of the space. We present this result in a more general form in the next theorem.

Theorem 1.10. Let $\mathcal{A} \subseteq \mathbb{F}_q^{n \times m}$ be an optimal anticode of dimension mr with $r = \operatorname{maxrk}(\mathcal{A})$. Then $\mathcal{A} = \operatorname{Mat}(V)$ for some $V \subseteq \mathbb{F}_q^n$ of dimension r, or $A = \operatorname{Mat}(V)^t$ and $m = n$.

Some fundamental properties of optimal anticodes are stated in [62], for instance that $\mathcal{C}$ is an optimal anticode if and only if $\mathcal{C}^\perp$ is an optimal anticode.

In the end we want to introduce q-polymatroids, which are the q-analogue of polymatroids. Jurrius and Pellikaan in [38] defined a way to associate one of this combinatorial object to every vector rank-metric code. The authors in [31] extend this association to rank-metric codes.

Definition 1.11 ([31], Definition 4.1)**.** A **q-polymatroid** is a pair $P = (\mathbb{F}_q^n, \rho)$ where ρ is a function from $\mathcal{P}(\mathbb{F}_q^n)$ to $\mathbb{R}$, such that

(i) $0 \leq \rho(A) \leq \dim(A)$,

(ii) if $A \subseteq B$, then $\rho(A) \leq \rho(B)$,

(iii) $\rho(A + B) + \rho(A \cap B) \leq \rho(A) + \rho(B)$.

for all $A, B \in \mathcal{P}(\mathbb{F}_q^n)$.

1.2 Linear Network Coding

The remainder of this chapter is devoted to illustrating some of the main applications of rank-metric codes. We start by considering the problem of information flow over a network with intermediate nodes. In the following section we introduce the **single-source multicast problem**. The communication goal of the single-source multicast problem is to transmit a fixed set of packets from the source to *all* sinks. Communication networks in this setting may be modeled as finite directed multigraphs. Every directed edge between nodes represents a channel capable of delivering a single packet per time slot.
Traditional approaches consist of simply routing the packets from incoming channels to outgoing ones. An intermediate node is then only permitted to store the packet and forward copies of it to its outgoing edges. We illustrate the routing solution in the so-called **butterfly network**: consisting of packets x, y, the source s and two sinks d_1 and d_2.

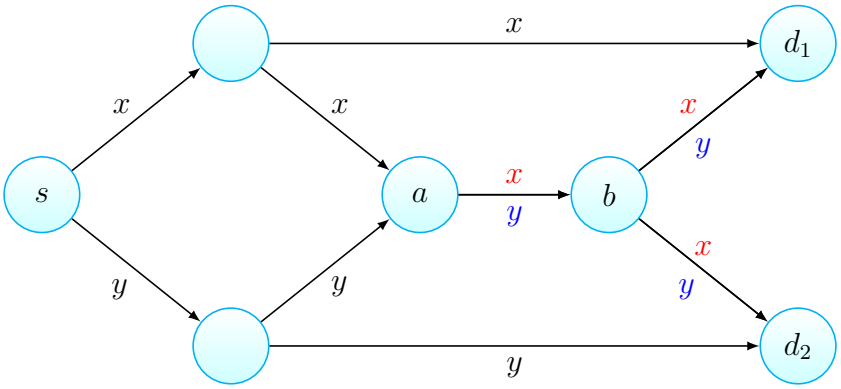

Figure 1: The butterfly network routing packets x and y from source node s to sinks d_1 and d_2.

The intermediate nodes a and b in Figure 1 form a bottleneck link. Indeed, node a receives both packets x and y, but only one of them may pass the bottleneck. Figure 1 represents both possible choices: Either a decides to forward packet x (red) or packet y is forwarded (blue). In the first case the sink node d_1 will not receive packet y, while in the second case the sink node d_2 will not receive packet x. Hence in both cases not all sinks will receive all sent packets.

Network coding was first introduced by Ahlswede et al. [2] in 2000. The network coding approach permits intermediate nodes to compute functions of the received packets. In this way intermediate nodes become coders forwarding functions of packets instead of simply routing them. In **linear network coding** these functions are linear over a finite field and packets are represented by vectors of a fixed length with entries in the finite field. The next figure describes the linear network coding solution in the butterfly network of Figure 1, where packets are considered as vectors over $\mathbb{F}_2$.

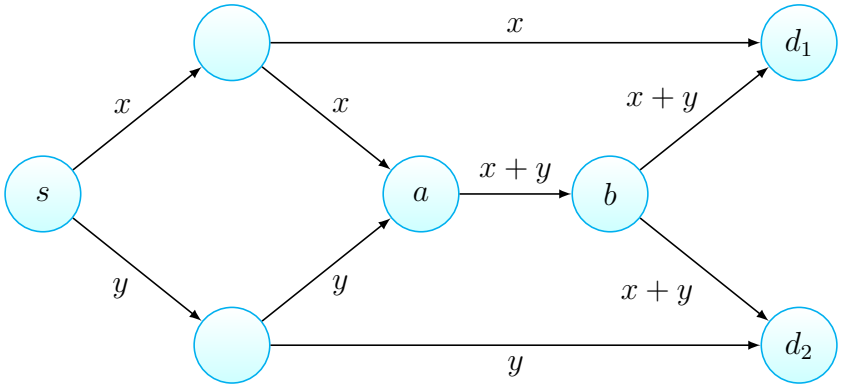

Figure 2: The butterfly network using the linear network coding strategy to transmit vectors x and y from source node s to sinks d_1 and d_2.

After a single time slot, sink d_1 now receives x and $x + y$, allowing it to recover the missing packet by performing the operation $x + (x + y)$ over $\mathbb{F}_2$; alike sink d_2 receiving $x + y$ and y. Hence a transmission rate of 2 packets per time slot is achieved. This is actually the best possible rate.

The butterfly-network example illustrates that network coding can increase the capacity of a network. In fact, the main theorem in [2] states that network coding achieves the multicast capacity. In particular, the optimum in transmission rate is achieved via linear network coding provided that the underlying finite field is sufficiently large, [43]. Linear network coding is an approach to so-called **coherent** transmission models where the network structure is completely known. The butterfly network in Figure 2 is an example of a coherent transmission model. However, there might be setups where the design of the transmission model is unknown. Regarding this issue, the authors of [35] introduce a new approach named **random linear network coding**. Unaware of the network topology this approach assumes that the packets at the intermediate nodes are linearly combined with random coefficients. In fact, it is shown in [35] that a deterministic network design is not needed in practice, as a completely random choice of the

linear coefficients is (with high probability) sufficient to perform a successful transmission. Random linear network coding is therefore proposed for so-called **noncoherent** transmission models where the underlying network topology is unknown.
Although network coding is an effective solution for communication over a network, it is an easy target for errors. Even a single error, when linearly combined with other packets, can corrupt all the sink's received ones. This motivates the research community to consider error-correcting codes to ensure an error-free communication over the channels.
Kötter and Kschischang take into account the problem of error-control in a noncoherent transmission model in [39]. The authors use random linear network coding where neither transmitter nor receiver have knowledge of the network topology and of the linear coding operations performed at each node. The transmission over this network is modeled via the **operator channel**

$$Y = AP + E, \tag{4}$$

where P is the transmitted matrix whose rows are packets, A is a random matrix representing the linear operations on the nodes, E is the error matrix and Y is the received matrix. Note that rank-metric codes can directly be applied for error-correction in coherent models, i.e. when the matrix A is determined. Indeed, packets may be sent in form of lines of a matrix with entries in a finite field. In this way the linear operations on each node are in fact linear row operations on the transmitted matrix and the rank of the received matrix may reveal something on the structure of the error matrix E. Let us consider now the case when A is a random matrix. Assuming that we are in an error-free situation, then the row space of the transmitted matrix P remains invariant over transmission. In fact, the row space of AP is in any case a subspace of the row space of P. This leads to consider (random) linear network coding as vector-space preserving, hence information here shall be encoded as a vector space rather than just as vectors. This gives rise to a metric, the **subspace metric**, which reflects the discrepancy between a transmitted and a received vector space. As a consequence, **subspace codes** are proposed as error-correcting codes for end-to-end coding, where only the source and the final receiver nodes are allowed to apply error control techniques.
In [67] Silva, Kschischang and Kötter explore the relationship between subspace codes and rank-metric codes. A **lifted construction of rank-metric codes** leads to a large class of constant-dimension subspace codes where the rank distance of two codewords is directly reflected in the subspace distance of their lifted images. The remarkable advantage of rewriting the random linear network problem in terms of rank-metric codes is the possibility to apply all of the powerful techniques of classical coding theory also known in the rank metric. Moreover in [67], as well as in [39], the authors show that subspace codes arising from lifted MRD codes are almost optimal for error correction in the operator channel.

We give a brief overview of the lifted construction.

Definition 1.12 ([39]). The **subspace distance** of $V, W \in \mathcal{P}(\mathbb{F}_q^n)$ is given by the function

$$\begin{array}{rccl} d_S & : & \mathcal{P}(\mathbb{F}_q^n) \times \mathcal{P}(\mathbb{F}_q^n) & \longrightarrow & \mathbb{N} \\ & & (V, W) & \longmapsto & \dim(V+W) - \dim(V \cap W). \end{array}$$

A **subspace code** $\mathcal{D}$ with ambient space $\mathbb{F}_q^n$ is a nonempty subset of $\mathcal{P}(\mathbb{F}_q^n)$ equipped with the subspace distance.

The next definition arises from [67] where lifted codes were first introduced.

Definition 1.13 ([67], Definition 3). Let $\mathcal{I} : \mathbb{F}_q^{n\times m} \to \mathcal{P}(\mathbb{F}_q^{n+m})$ be given by $M \mapsto \text{rowsp}\left(\begin{pmatrix} I_n & M \end{pmatrix}\right)$. The subspace $\mathcal{I}(M)$ is the lifting of the matrix M. Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ be a rank-metric code, then the subspace code $\mathcal{I}(\mathcal{C})$, obtained by lifting every codeword of $\mathcal{C}$, is the **lifting** of $\mathcal{C}$.

As mentioned earlier, the main advantage of using rank-metric codes to construct subspace codes is the fact that the rank metric is reflected in the subspace distance of liftings.

Proposition 1.14 ([67], Proposition 4). Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ be a rank-metric code and $M, N \in \mathcal{C}$, then

$$d_S(\mathcal{I}(M), \mathcal{I}(N)) = 2d(M, N)$$

and in particular the minimal subspace distance of $\mathcal{I}(\mathcal{C})$ is twice the minimal rank distance of $\mathcal{C}$.

There is another remarkable advantage in constructing constant-dimension subspace codes via rank-metric codes: lifting MRD codes results in finding almost optimal constant-dimension subspace codes, ([67], Proposition 5).

1.3 Rank-based Cryptography

In this section we give an introduction to code-based cryptography in the rank metric, describing some main cryptographic systems where the underlying algorithms are based on error-correcting rank-metric codes.
In the last years the research on quantum computers, machines that in contrast to conventional computers are able to solve difficult mathematical problems, has received a notable amount of interest. The possibility of building a large quantum computer would imply the downfall of number theoretic based approaches in public-key primitives, hence it would break most of the public-key cryptosystems in use nowadays. The list of possible alternatives is long: hash-based cryptography, lattice-based cryptography, multivariate-quadratic-equations cryptography, secret-key cryptography and last but not least code-based cryptography. All of these approaches have systems that are believed to resist classical computers as well as quantum ones.
The algorithmic primitives of code-based cryptosystems consist essentially in either computing a syndrome given a parity-check matrix of an error-correcting code or in

adding an error to a codeword. The main problem on which almost all code-based schemes rely is the **Syndrome Decoding Problem (SDP)** and its variations. For cryptographic purposes it is more convenient to consider the **Decision Syndrome Decoding Problem (DSDP)**. Let $k < n$ be a positive integer.

Problem 1.15. (Decision Syndrome Decoding Problem (DSDP)) Let $H \in \mathbb{F}_q^{(n-k)\times n}$ be a random matrix and let t be a positive integer. Given $e \in \mathbb{F}_q^n$ of weight t, is it possible to distinguish between He^t and r a random vector in $\mathbb{F}_q^{n-k}$ with a non-negligible advantage?

Coding-theoretical encryption schemes are very fast, as both encryption and decryption operations have a low complexity and their best known attacks are overall well-studied. Although, one of the main drawback of using code-based cryptography relies in the large memory requirements, in particular the large size of the public key. This connects us directly to one of the principal motivation for looking at rank-based cryptosystems, namely the possibility of reducing the public key size. In fact, cryptosystems in the rank metric have in general smaller key sizes.
In the following we present the first and unbroken (after adaptation) code-based public key cryptosystem together with its rank-metric versions.

The **McEliece public key encryption scheme** proposed 1978 by Robert J. McEliece in [52] is the first cryptosystem based on coding theory. It has resisted cryptoanalysis for adequate choices of parameters and is still considered secure by the cryptography community nowadays.
We denote by $[n, k, d_H]_2$ a k dimensional binary code $\mathcal{C}$ of length n and minimum distance d_H in the Hamming metric. In his original paper [52] McEliece proposed to use binary irreducible Goppa codes of length $n = 2^m$ and dimension $k \geq n - mt$, capable of correcting any pattern of at most t errors. We refer to these type of codes as t-correcting Goppa codes. In particular, he suggested $[1024, 524, 101]_2$, a 50-correcting Goppa code, where $k = 2^m - mt, d_H = 2t + 1$ for $m = 10$ and $t = 50$. An important advantage of these type of codes is, that it exists a fast decoding algorithm.
The McEliece cryptosystem can then be described as follows:

Algorithm 1.16. The McEliece Public-Key Encryption Scheme

Key Generation Given parameters $n, t \in \mathbb{N}$ with $t \ll n$, generate the following matrices:

$G \in \mathbb{F}_2^{k\times n}$ a generator matrix of a t-correcting Goppa code $\mathcal{C}$,

$S \in \mathrm{GL}_k(\mathbb{F}_2)$ a random matrix,

$P \in \mathrm{GL}_n(\mathbb{F}_2)$ a random permutation matrix.

Compute $G^{\mathrm{pub}} = SGP$. Return (G^{pub}, t) as the public key and $(S, \mathsf{D}_{\mathcal{C}}, P)$ as the secret key, where $\mathsf{D}_{\mathcal{C}}$ is an efficient decoding algorithm for $\mathcal{C}$.

Encryption To encrypt a plaintext $\mathrm{m} \in \mathbb{F}_2^k$ sample randomly $e \in \mathbb{F}_2^n$ of Hamming weight t and compute the ciphertext $c = \mathrm{m}G^{\mathrm{pub}} + e$.

Decryption To decrypt a ciphertext c first calculate $cP^{-1} = (\mathrm{m}S)G + eP^{-1}$ and decode $\mathrm{m}S$ using $\mathsf{D}_{\mathcal{C}}$. Then retrieve m from $\mathrm{m}S$ by multiplying it from the right with S^{-1}.

Correctness The vector eP^{-1} has weight t, so a decoding algorithm for $\mathcal{C}$ decodes correctly $\mathrm{m}S$ from $(\mathrm{m}S)G + eP^{-1}$.

This construction is based on masking the structure of a family of error-correcting codes. The security of the McEliece scheme relies on two assumptions: the indistinguishability of the hidden code structure from a random code, implying that the public key cannot be distinguished from a random one, and the hardness of decoding a generic linear code. As a consequence the security is then the security of decoding random codes, hence a variation of the SDP. In fact, for random binary codes the SDP together with its variations are proven NP-complete, [8].
Someone who is able to solve the DSDP is also able to solve the McEliece problem. Note that the opposite is not true, since solving the McEliece problem implies solving the DSDP for a specific class of codes and not for all codes. Motivated by this observation several generalized probabilistic decoding algorithms have been studied, one for instance in [42]. Another possible attack is analyzed in [13]: an algorithm that can find a minimum weight codeword of a linear code is an attack to the McEliece cryptosystem. The problem of finding codewords of given weight in a linear error-correcting code is known to be NP-complete, [8]. Hence attacks based on this NP-complete problem do not break the McEliece cryptosystem, but they force to exclude certain parameters, [13].

The main disadvantages of the McEliece encryption scheme are as already mentioned the large memory requirements for the public key and the plaintext, but also the existence of systematic attacks. The use of codes in the rank metric can partially overcome these disadvantages, as Gabidulin, Paramonov and Tretjakov in [25] have shown. In [25] the authors introduce a rank-metric version of the McEliece framework. We will refer to this scheme as the **GPT public-key encryption scheme**.
In the following a vector rank-metric code is an $\mathbb{F}_{q^n}$-linear subspace of $\mathbb{F}_{q^n}^n$, as given in Definition 1.2. A t-correcting vector rank-metric code is then capable of correcting any pattern of at most t vector-rank errors. The authors suggest to use t-correcting Gabidulin codes, i.e. the first family of MRD codes defined in [22].

Definition 1.17 ([22], Theorem 6 and Theorem 7)**.** Let $h_1, \ldots, h_n$ be $\mathbb{F}_q$-linear independent elements in $\mathbb{F}_{q^m}$ and $d \leq m$. We use the notation $[i] = q^i$ for $1 \leq i \leq d-1$. A code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ with parity check matrix

$$H = \begin{pmatrix} h_1 & h_2 & \ldots & h_n \\ h_1^{[1]} & h_2^{[1]} & \ldots & h_n^{[1]} \\ \vdots & \vdots & \ldots & \vdots \\ h_1^{[d-1]} & h_2^{[d-1]} & \ldots & h_n^{[d-1]} \end{pmatrix}$$

is an MRD code of length n and minimum distance d, in particular $\dim(\mathcal{C}) = k = n - d + 1$. Moreover the generating matrix $G \in \mathbb{F}_{q^m}^{k\times n}$ is of the form

$$G = \begin{pmatrix} g_1 & g_2 & \dots & g_n \\ g_1^{[1]} & g_2^{[1]} & \dots & g_n^{[1]} \\ \vdots & \vdots & \dots & \vdots \\ g_1^{[k-1]} & g_2^{[k-1]} & \dots & g_n^{[k-1]} \end{pmatrix},$$

where $g_1, \dots, g_n$ are $\mathbb{F}_q$-linearly independent elements in $\mathbb{F}_{q^m}$. A vector-rank metric code $\mathcal{C}$ with generator matrix G is a **Gabidulin code**.

The first question arising naturally when adapting the McEliece cryptosystem to the rank-metric is the choice of the scrambling matrices S and P. This question is strictly related to the study of linear equivalence maps of rank-metric codes.
The receiver, who knows exactly the equivalence map, should be able to apply his decoding algorithm also to a simplified scrambled version of it, i.e. to the code generated by SG. Yet an efficient decoding of the simplified scrambled version is only possible if it maintains the minimum-distance property of the original code. This is for instance the case when the original code and the simplified scrambled code are equivalent.

In its first version [25] the GPT scheme was proposed using a t-correcting Gabidulin code with generator matrix $G \in \mathbb{F}_{q^n}^{k\times n}$, a random row scrambler matrix $S \in \mathrm{GL}_k(\mathbb{F}_{q^n})$ and some random distorsion matrix $\alpha^t\epsilon_1 \in \mathbb{F}_{q^n}^{k\times n}$ where $0_{1\times k} \neq \alpha \in \mathbb{F}_q^k$ and $0_{1\times n} \neq \epsilon_1 \in \mathbb{F}_{q^n}^n$ with $\mathrm{rank}(\epsilon_1) \leq t_1 < t$ for some design parameter t_1. The public key is then given by $G^{\mathrm{pub}} = SG + \alpha^t\epsilon_1$. Obviously this is not equivalent to the original code, but the distance property is maintained when choosing a random error vector e of weight at most $t - t_1$ and encrypting a message m by $\mathrm{m}G^{\mathrm{pub}} + e$. The reason is that the legitimate receiver is able to correct the error $\mathrm{m}\alpha^t\epsilon_1 + e$, since it has weight at most t. This first version was attacked by Gibson in [28] using a structural attack. Later in [24] Gabidulin together with Ourivski suggested to use a random column scrambler $P \in \mathrm{GL}_n(\mathbb{F}_q)$, a random row scrambler $S \in \mathrm{GL}_k(\mathbb{F}_{q^n})$ and a distortion matrix $X \in \mathbb{F}_{q^n}^{k\times 2n}$ of rank at most t. The public key is then given by $S([0_{k\times n}\ G] + X)P$. The fact that the column scrambler P is defined over the base field, together with the observation that if G is the generator matrix of a Gabidulin code then G and $G^{[q]}$ look quite the same, are the central arguments for Overbeck's attack in [58].
In [23] and [26] the idea of using an appropriate column scrambler P over the extension field is proposed. The intention of the proposal is to avoid Overbeck's attack. Obviously P has to be chosen in a sophisticated way since in general multiplying G with a column scrambler over the extension field does not maintain the distance properties of the original code. Hence Gabidulin, later together with Rashwan and Honary, propose to take $P \in \mathrm{GL}_n(\mathbb{F}_{q^n})$ such that $P^{-1} = [Q_1\ Q_2]$ with Q_1 an $n \times (t - t_1)$ matrix over $\mathbb{F}_{q^n}$ and Q_2 an $n \times (n - t + t_1)$ matrix over the base field $\mathbb{F}_q$. The artificial error $e \in \mathbb{F}_{q^n}^n$ is chosen to have weight $t_1 \leq t$. The authors show that with these choices of the column scrambler and the artificial error set, the weight of eP^{-1} is at most t hence we can still decode.

However Otmani, Kalachi and Ndjeya in [57] showed that even if the column scrambler is defined over the extension field, it is still possible to recover a private Gabidulin code which can be used to recover the original one using exactly Overbeck's technique.
We so end up with [45], one of the latest rank-metric code-based encryption scheme proposed by Loidreau.

Algorithm 1.18. The Loidreau Public-Key Encryption Scheme

Key Generation Given parameters $n, m, \lambda \in \mathbb{N}$ with $n \leq m$, generate the following matrices:

$G \in \mathbb{F}_{2^m}^{k \times n}$ a generator matrix of a Gabidulin code $\mathcal{C}$ of length n and dimension k,

$S \in \mathrm{GL}_k(\mathbb{F}_{2^m})$ a random matrix,

$\mathcal{V} \subseteq \mathbb{F}_{2^m}$ a λ-dimensional subspace over $\mathbb{F}_2$,

$P \in \mathrm{GL}_n(\mathcal{V})$ a random matrix.

Compute $G^{\mathrm{pub}} = SGP^{-1}$. Return G^{pub} as the public key and $(S, P, \mathcal{V}, \mathsf{D}_{\mathcal{C}})$ as the secret key, where $\mathsf{D}_{\mathcal{C}}$ is an efficient decoding algorithm for $\mathcal{C}$.

Encryption To encrypt a plaintext $\mathrm{m} \in \mathbb{F}_{2^m}^k$ sample randomly $e \in \mathbb{F}_{2^m}^n$ of vector-rank weight $\lfloor (n-k)/(2\lambda) \rfloor$ and compute the ciphertext $c = \mathrm{m}G^{\mathrm{pub}} + e$.

Decryption To decrypt a ciphertext c first calculate $cP = (\mathrm{m}S)G + eP$ and decode $\mathrm{m}S$ using $\mathsf{D}_{\mathcal{C}}$. Then retrieve m from $\mathrm{m}S$ by multiplying it from the right with S^{-1}.

Correctness P has entries in $\mathcal{V}$ and eP has vector-rank weight $\leq \lambda \lfloor (n-k)/(2\lambda) \rfloor \leq \lfloor (n-k)/2 \rfloor$ as shown in Proposition 1 [45].

Loidreau's approach consists in scrambling the code via the choice of a randomly selected vector space $\mathcal{V}$ of $\mathbb{F}_{2^m}$ of fixed dimension. A detailed security analysis of Loidreau's scheme is made in [45], pointing out that the usual distinguisher for a Gabidulin code, i.e. that G and $G^{[q]}$ look quite similar, does not work here.
In the last years there have been two remarkable structural attacks to Loidreau's scheme. The first in [14] for $\lambda = 2$ and the second in [27] for $\lambda \geq 3$. More recently in 2021 the authors of [33] propose two modifications for the choice of the generator matrix: the first one is to use a certain subcode of G and the second one to add a random matrix $M \in \mathbb{F}_{q^m}^{k \times n}$ to G. In addition to that they use a systematic generator matrix of the public code to reduce the key size. The authors claim that this modified version would prevent all known structural attacks of Gabidulin codes.

2 Quasi Optimal Anticodes in the Rank Metric

The following section is a joined work with Elisa Gorla and introduces a new class of rank-metric codes. We start by motivating our definition.

It is intrinsic with the definition of an optimal anticode, that the dimension of the latter has to be divisible by m. In the following we give an alternative, but still equivalent bound to the anticode bound. Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ be a rank-metric code, then

$$\operatorname{maxrk}(\mathcal{C}) \geq \left\lceil \frac{\dim(\mathcal{C})}{m} \right\rceil. \tag{5}$$

Note that codes attaining (3) do also attain (5), whereas the converse is not true in general. In particular, when defining optimal anticodes as those attaining (3), we do not take into account codes having dimension not divisible by m. Studying optimal codes in the sense of (5) captures therefore a larger class of rank-metric codes, who can still be considered as a class of optimal rank-metric codes.

2.1 Quasi Optimal and Dually Quasi Optimal Anticodes

Definition 2.1. A **quasi optimal anticode (qOAC)** is a rank-metric code $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ with $m \nmid \dim(\mathcal{C})$ and

$$\operatorname{maxrk}(\mathcal{C}) = \left\lceil \frac{\dim(\mathcal{C})}{m} \right\rceil.$$

If $\mathcal{C}$ and $\mathcal{C}^\perp$ are both qOACs, then $\mathcal{C}$ is a **dually qOAC**.

Notation 2.2. For $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ a qOAC, write

$$\dim(\mathcal{C}) = \alpha m + \rho, \quad 0 < \rho < m, \quad 0 \leq \alpha < n \leq m, \quad \operatorname{maxrk}(\mathcal{C}) = \alpha + 1.$$

If in addition $\mathcal{C}$ is a dually qOAC, write

$$\dim(\mathcal{C}^\perp) = (n - \alpha - 1)m + (m - \rho), \quad 0 < m - \rho < m, \ \operatorname{maxrk}(\mathcal{C}^\perp) = n - \alpha.$$

It is well known that the dual of an optimal anticode is an optimal anticode. However, this is not the case for qOACs. In the next example, we produce dually qOACs, as well as qOACs which are not dually qOACs.

Example 2.3. Let $m \geq \max\{2, n\}$, let $0 < \alpha < n \leq m$, $0 < \rho < m$, $0 \leq k \leq m - \rho$. Let

$$\mathcal{C}_k = \left\{ \begin{pmatrix} A & B \\ u & 0_{1\times k} \\ w & 0_{1\times(m-\rho-k)} \\ 0_{(n-\alpha-1)\times(\rho+k)} & 0_{(n-\alpha-1)\times(m-\rho-k)} \end{pmatrix} : \begin{array}{l} A \in \mathbb{F}_q^{(\alpha-1)\times(m-k)}, B \in \mathbb{F}_q^{(\alpha-1)\times k}, \\ u \in \mathbb{F}_q^{m-k}, w \in \mathbb{F}_q^{\rho+k} \end{array} \right\},$$

with dual code

$$\mathcal{C}_k^\perp = \left\{ \begin{pmatrix} 0_{(\alpha-1)\times(m-k)} & 0_{(\alpha-1)\times k} \\ 0_{1\times(m-k)} & u \\ 0_{1\times(\rho+k)} & w \\ A & B \end{pmatrix} : \begin{array}{l} A \in \mathbb{F}_q^{(n-\alpha-1)\times(\rho+k)}, B \in \mathbb{F}_q^{(n-\alpha-1)\times(m-\rho-k)}, \\ u \in \mathbb{F}_q^{k}, w \in \mathbb{F}_q^{m-\rho-k} \end{array} \right\}.$$

Notice that $\mathcal{C}_k \sim \mathcal{C}_{m-\rho-k}$ for all k. We have $\operatorname{maxrk}(\mathcal{C}_0) = \alpha+1$ and $\operatorname{maxrk}(\mathcal{C}_0^\perp) = n-\alpha$, hence $\mathcal{C}_0 \sim \mathcal{C}_{m-\rho}$ are dually qOACs. If $\rho \geq m-2$, then $\operatorname{maxrk}(\mathcal{C}_1) = \alpha+1$ and $\operatorname{maxrk}(\mathcal{C}_1^\perp) = n-\alpha$, hence $\mathcal{C}_1 \sim \mathcal{C}_{m-\rho-1}$ are dually qOACs. If $\rho \leq m-3$, then $\operatorname{maxrk}(\mathcal{C}_1) = \alpha+1$ and $\operatorname{maxrk}(\mathcal{C}_1^\perp) = n-\alpha+1$. Hence $\mathcal{C}_1 \sim \mathcal{C}_{m-\rho-1}$ are qOACs, but not dually qOACs. For $k \neq 0, 1, m-\rho-1, m-\rho$, one has $\operatorname{maxrk}(\mathcal{C}_k) = \alpha+1$ and $\operatorname{maxrk}(\mathcal{C}_k^\perp) = n-\alpha+1$. Therefore $\mathcal{C}_k \sim \mathcal{C}_{m-\rho-k}$ are qOACs, but not dually qOACs.

The next proposition relates the maximum rank of a code with that of its dual. It also provides us with a simple characterization of dually qOACs.

Proposition 2.4. Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ be a rank-metric code. Then

$$\operatorname{maxrk}(\mathcal{C}) + \operatorname{maxrk}(\mathcal{C}^\perp) \geq n.$$

Moreover:

(a) $\mathcal{C}$ is an optimal anticode if and only if $\operatorname{maxrk}(\mathcal{C}) + \operatorname{maxrk}(\mathcal{C}^\perp) = n$.

(b) $\mathcal{C}$ is a dually qOAC if and only if $\operatorname{maxrk}(\mathcal{C}) + \operatorname{maxrk}(\mathcal{C}^\perp) = n+1$.

Proof. The anticode bound on $\mathcal{C}$ and $\mathcal{C}^\perp$ yields

$$mn = \dim(\mathcal{C}) + \dim(\mathcal{C}^\perp) \leq m(\operatorname{maxrk}(\mathcal{C}) + \operatorname{maxrk}(\mathcal{C}^\perp)). \tag{6}$$

(a) $\mathcal{C}$ is an optimal anticode if and only if $\mathcal{C}^\perp$ is an optimal anticode. Hence, if $\mathcal{C}$ is an optimal anticode, then equality holds in (6). Conversely, if equality holds in (6), then $\mathcal{C}$ and $\mathcal{C}^\perp$ meet the anticode bound, hence they are optimal anticodes.

(b) If $\mathcal{C}$ is a dually qOAC, then $\operatorname{maxrk}(\mathcal{C})+\operatorname{maxrk}(\mathcal{C}^\perp) = n+1$ by direct computation. To prove the converse, first observe that, if $\operatorname{maxrk}(\mathcal{C})+\operatorname{maxrk}(\mathcal{C}^\perp) = n+1$, then $\mathcal{C}$ and $\mathcal{C}^\perp$ are not optimal anticodes by part (a). If $m \mid \dim(\mathcal{C})$, then

$$\operatorname{maxrk}(\mathcal{C}) + \operatorname{maxrk}(\mathcal{C}^\perp) \geq \frac{\dim(\mathcal{C})}{m} + 1 + \frac{\dim(\mathcal{C}^\perp)}{m} + 1 = n+2,$$

since $\mathcal{C}$ and $\mathcal{C}^\perp$ are not optimal anticodes. If instead $m \nmid \dim(\mathcal{C})$, then

$$n+1 = \operatorname{maxrk}(\mathcal{C})+\operatorname{maxrk}(\mathcal{C}^\perp) \geq \left\lceil \frac{\dim(\mathcal{C})}{m} \right\rceil + \left\lceil \frac{\dim(\mathcal{C}^\perp)}{m} \right\rceil \geq \alpha+1+n-\alpha, \quad (7)$$

where $\dim(\mathcal{C}) = \alpha m+\rho$, $\dim(\mathcal{C}^\perp) = (n-\alpha-1)m+(m-\rho)$, and $\rho > 0$. Therefore the inequalities in (7) are equalities, which completes the proof.

□

A first approach to the problem of classifying large matrix spaces of bounded rank appears in [6], where Atkinson and Lloyd study linear spaces with dimension close to mr over fields of large cardinality. Their classification was extended to all fields and matrices of arbitrary size by de Seguins Pazzis in [17]. As a direct consequence of the results by de Seguins Pazzis, we can characterize the qOACs whose dimension is at least $\alpha(m-1)+n$.

Theorem 2.5 ([17], Theorem 4, Theorem 5 and Theorem 6)**.** Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ be a qOAC of $\dim(\mathcal{C}) = \alpha m+\rho$, $0 < \rho < m$.

(a) If $\rho > n-\alpha$, then $\mathcal{C}$ is equivalent to a linear subspace of $\operatorname{Mat}(\langle e_1, \ldots, e_{\alpha+1}\rangle)$.

(b) If $\rho = n-\alpha$, then one of the following holds:

(i) $\mathcal{C}$ is equivalent to a linear subspace of $\operatorname{Mat}(\langle e_1, \ldots, e_{\alpha+1}\rangle)$,

(ii) $\mathcal{C} \sim \operatorname{Mat}(\langle e_1, \ldots, e_\alpha\rangle) + \operatorname{Mat}(\langle e_1\rangle)^t$,

(iii) $m = n+1$ and $\mathcal{C} \sim \operatorname{Mat}(\langle e_1, \ldots, e_{\alpha+1}\rangle)^t$,

(iv) $m = n = 3$, $q = 2$, and $\mathcal{C} \sim \left\{ \begin{pmatrix} a & 0 & 0 \\ c & b & 0 \\ d & e & a+b \end{pmatrix} : (a,b,c,d,e) \in \mathbb{F}_2^5 \right\}$.

By Theorem 2.5 we can classify dually qOACs.

Theorem 2.6. Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ be a dually qOAC with $\dim(\mathcal{C}) = \alpha m+\rho$, $0 < \rho < m$. One of the following holds:

(a)

$$\mathcal{C} \sim \left\{ \begin{pmatrix} A & B \\ u & 0_{1\times(m-\rho)} \\ 0_{(n-\alpha-1)\times\rho} & 0_{(n-\alpha-1)\times(m-\rho)} \end{pmatrix} : A \in \mathbb{F}_q^{\alpha\times\rho}, B \in \mathbb{F}_q^{\alpha\times(m-\rho)}, u \in \mathbb{F}_q^\rho \right\},$$

(b) $\rho \leq n - \alpha$ and

$$\mathcal{C} \sim \left\{ \begin{pmatrix} u^t & A \\ v^t & 0_{\rho \times (m-1)} \\ 0_{(n-\alpha-\rho)\times 1} & 0_{(n-\alpha-\rho)\times(m-1)} \end{pmatrix} : A \in \mathbb{F}_q^{\alpha \times (m-1)}, u \in \mathbb{F}_q^{\alpha}, v \in \mathbb{F}_q^{\rho} \right\},$$

(c) $\rho \geq m - \alpha - 1$ and

$$\mathcal{C} \sim \left\{ \begin{pmatrix} A & u^t \\ B & 0_{(m-\rho)\times 1} \\ 0_{(n-\alpha-1)\times(m-1)} & 0_{(n-\alpha-1)\times 1} \end{pmatrix} : \begin{array}{l} A \in \mathbb{F}_q^{(\alpha+\rho+1-m)\times(m-1)}, \\ B \in \mathbb{F}_q^{(m-\rho)\times(m-1)}, u \in \mathbb{F}_q^{\alpha+\rho+1-m} \end{array} \right\},$$

(d) $m = n + 1$, $\rho = n - \alpha$, and

$$\mathcal{C} \sim \left\{ \begin{pmatrix} A & 0_{n\times(n-\alpha)} \end{pmatrix} : A \in \mathbb{F}_q^{n\times(\alpha+1)} \right\}.$$

Proof. It is easy to check that the codes in the statement of the theorem are dually qOACs. We now prove that, up to equivalence, they are the only ones. We start by analyzing the case when $\mathcal{C} \supseteq \mathrm{Mat}(U)$, for some $U \subseteq \mathbb{F}_q^n$ of $\dim(U) = \alpha$. Up to equivalence, we may assume that $U = \langle e_1, \ldots, e_\alpha \rangle$. Write $\mathcal{C} = \mathrm{Mat}(\langle e_1, \ldots, e_\alpha \rangle) + \langle M_1, \ldots, M_\rho \rangle$, where $M_1, \ldots, M_\rho \in \mathrm{Mat}(\langle e_1, \ldots, e_\alpha \rangle)^\perp = \mathrm{Mat}(\langle e_{\alpha+1}, \ldots, e_n \rangle)$ are linearly independent. Since $\mathcal{C}$ is a qOAC, then $\mathrm{maxrk}(\mathcal{C}) = \alpha + 1$. We claim that $\mathrm{maxrk}(\langle M_1, \ldots, M_\rho \rangle) = 1$. In fact, any $M \in \langle M_1, \ldots, M_\rho \rangle \subseteq \mathrm{Mat}(\langle e_{\alpha+1}, \ldots, e_n \rangle)$ has

$$\dim(\mathrm{rowsp}(M)) = \mathrm{rank}(M) \leq \mathrm{maxrk}(\mathrm{Mat}(\langle e_{\alpha+1}, \ldots, e_n \rangle)) = n - \alpha.$$

Let $L \in \mathrm{Mat}(\langle e_1, \ldots, e_\alpha \rangle)$ be a matrix whose first α rows are linearly independent vectors in a vector space V such that $V \oplus \mathrm{rowsp}(M) = \mathbb{F}_q^m$. Notice that one can always find such an L, since $\dim(V) = m - \dim(\mathrm{rowsp}(M)) \geq m - (n - \alpha) \geq \alpha$. Then $\mathrm{rowsp}(L) \cap \mathrm{rowsp}(M) = 0$, so $L + M \in \mathcal{C}$ has

$$\mathrm{rank}(L + M) = \mathrm{rank}(L) + \mathrm{rank}(M) \leq \mathrm{maxrk}(\mathcal{C}) = \alpha + 1,$$

which proves that $\mathrm{rank}(M) \leq 1$, since $\mathrm{rank}(L) = \alpha$. Since $\mathrm{maxrk}(\langle M_1, \ldots, M_\rho \rangle) = 1$, then either $\langle M_1, \ldots, M_\rho \rangle \subseteq \mathrm{Mat}(w)$ for some $w \in \langle e_{\alpha+1}, \ldots, e_n \rangle \subseteq \mathbb{F}_q^n$, or $\langle M_1, \ldots, M_\rho \rangle \subseteq \mathrm{Mat}(w)^t$ for some $w \in \mathbb{F}_q^m$. Since $\langle M_1, \ldots, M_\rho \rangle \subseteq \mathrm{Mat}(\langle e_{\alpha+1}, \ldots, e_n \rangle)$, the latter is only possible if

$$\rho = \dim(\langle M_1, \ldots, M_\rho \rangle) \leq \dim(\mathrm{Mat}(\langle e_{\alpha+1}, \ldots, e_n \rangle) \cap \mathrm{Mat}(w)^t) = n - \alpha.$$

If $\langle M_1, \ldots, M_\rho \rangle \subseteq \mathrm{Mat}(w)$, then, after suitable invertible operations involving the last $n - \alpha$ rows, we may suppose that $w = e_{\alpha+1}$. Moreover, after suitable invertible column operations

$$M_i = \begin{pmatrix} 0_{n\times(i-1)} & e_{\alpha+1} & 0_{n\times(m-i)} \end{pmatrix} \quad \text{for } 1 \leq i \leq \rho.$$

Since both types of operations fix $\mathrm{Mat}(\langle e_1, \ldots, e_\alpha \rangle)$, we have shown that

$$\mathcal{C} \sim \left\{ \begin{pmatrix} A & B \\ u & 0_{1\times(m-\rho)} \\ 0_{(n-\alpha-1)\times\rho} & 0_{(n-\alpha-1)\times(m-\rho)} \end{pmatrix} : A \in \mathbb{F}_q^{\alpha\times\rho}, B \in \mathbb{F}_q^{\alpha\times(m-\rho)}, u \in \mathbb{F}_q^{\rho} \right\}. \quad (8)$$

This yields the codes in part (a) of the statement.
If $\rho \leq n - \alpha$ and $\langle M_1, \ldots, M_\rho \rangle \subseteq \mathrm{Mat}(w)^t$, then, after suitable invertible operations involving the last $n - \alpha$ rows, we may suppose that M_i is the matrix whose rows are all zero, except for row $\alpha + i$ which is equal to w. Up to invertible column operations, we may further suppose that $w = e_1 \in \mathbb{F}_q^m$. Since both types of operations fix $\mathrm{Mat}(\langle e_1, \ldots, e_\alpha \rangle)$, we have that

$$\mathcal{C} \sim \left\{ \begin{pmatrix} u^t & A \\ v^t & 0_{\rho\times(m-1)} \\ 0_{(n-\alpha-\rho)\times 1} & 0_{(n-\alpha-\rho)\times(m-1)} \end{pmatrix} : A \in \mathbb{F}_q^{\alpha\times(m-1)}, u \in \mathbb{F}_q^{\alpha}, v \in \mathbb{F}_q^{\rho} \right\}.$$

This yields the codes in part (b) of the statement.
Suppose now that $\mathcal{C} \subseteq \mathrm{Mat}(U)$ for some $U \subseteq \mathbb{F}_q^n$ of $\dim(U) = \alpha+1$. Up to equivalence, we may assume that $U = \mathrm{Mat}(\langle e_{n-\alpha}, \ldots, e_n \rangle)$, that is, $\mathcal{C}^\perp \supseteq \mathrm{Mat}(\langle e_1, \ldots, e_{n-\alpha-1} \rangle)$. Then the above argument shows that either

$$\mathcal{C}^\perp \sim \left\{ \begin{pmatrix} A & B \\ u & 0_{1\times\rho} \\ 0_{\alpha\times(m-\rho)} & 0_{\alpha\times\rho} \end{pmatrix} : A \in \mathbb{F}_q^{(n-\alpha-1)\times(m-\rho)}, B \in \mathbb{F}_q^{(n-\alpha-1)\times\rho}, u \in \mathbb{F}_q^{m-\rho} \right\}$$

or

$$\mathcal{C}^\perp \sim \left\{ \begin{pmatrix} u^t & A \\ v^t & 0_{(m-\rho)\times(m-1)} \\ 0_{(\alpha+\rho+1-m)\times 1} & 0_{(\alpha+\rho+1-m)\times(m-1)} \end{pmatrix} : \begin{array}{l} A \in \mathbb{F}_q^{(n-\alpha-1)\times(m-1)}, \\ \qquad\qquad u \in \mathbb{F}_q^{n-\alpha-1}, v \in \mathbb{F}_q^{m-\rho} \end{array} \right\}.$$

Moreover, the latter is only possible when $\rho \geq m - \alpha - 1$. Taking duals, we obtain that either $\mathcal{C}$ has the form (8), or

$$\mathcal{C} \sim \left\{ \begin{pmatrix} A & u^t \\ B & 0_{(m-\rho)\times 1} \\ 0_{(n-\alpha-1)\times(m-1)} & 0_{(n-\alpha-1)\times 1} \end{pmatrix} : \begin{array}{l} A \in \mathbb{F}_q^{(\alpha+\rho+1-m)\times(m-1)}, \\ \qquad B \in \mathbb{F}_q^{(m-\rho)\times(m-1)}, u \in \mathbb{F}_q^{\alpha+\rho+1-m} \end{array} \right\}.$$

This yields the codes in part (c) of the statement.
Finally, suppose that $\mathcal{C} \not\supseteq \mathrm{Mat}(U)$ for any $U \subseteq \mathbb{F}_q^n$ of $\dim(U) = \alpha$ and $\mathcal{C} \not\subseteq \mathrm{Mat}(U)$ for any $U \subseteq \mathbb{F}_q^n$ of $\dim(U) = \alpha + 1$. This implies also that $\mathcal{C}^\perp \not\subseteq \mathrm{Mat}(U)$ for any $U \subseteq \mathbb{F}_q^n$ of $\dim(U) = n - \alpha$. Since $n \leq m$, then either $\rho \leq m - \alpha - 1$ or $\rho \geq n - \alpha$. This

implies that, for any $0 < \rho < m$, Theorem 2.5 applies to either $\mathcal{C}$ or $\mathcal{C}^\perp$. Because of our assumptions, and since the code of Theorem 2.5 (b) (iv) is not a dually qOAC, $\mathcal{C}$ or $\mathcal{C}^\perp$ is a code as in Theorem 2.5 (b) (iii). Therefore $m = n+1$ and $\rho = m-\alpha-1 = n-\alpha$ and we obtain the codes in part (d) of the statement.
Note that codes in Theorem 2.5 (b) (ii) are also dually qOACs and are a special case of codes in part (b) for $\rho = n-\alpha$.

□

Theorem 2.5 and Theorem 2.6 provide us with many examples of codes which are qOACs but not dually qOACs. In fact, any code as in Theorem 2.5 which is not one of the codes in Theorem 2.6 is of this kind. We now give some concrete examples of qOACs which are not dually qOACs.

Example 2.7. Let $1 \leq \alpha \leq n-1$ and $m-\alpha-1 \leq \rho \leq m-2$. Let

$$\mathcal{C} = \left\{ \begin{pmatrix} \mathcal{V} & B \\ A & C \\ 0_{(n-\alpha-1)\times(m-\rho)} & 0_{(n-\alpha-1)\times\rho} \end{pmatrix} : \mathcal{V} \subseteq \mathbb{F}_q^{(m-\rho)\times(m-\rho)} \text{ the set of matrices with 0 on the diagonal}, A \in \mathbb{F}_q^{(\alpha+1-m+\rho)\times(m-\rho)}, B \in \mathbb{F}_q^{(m-\rho)\times\rho}, C \in \mathbb{F}_q^{(\alpha+1-m+\rho)\times\rho} \right\}.$$

Then $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ has dimension $\alpha m + \rho$ and maximum rank $\alpha+1$, hence it is a qOAC. Its dual is given by

$$\mathcal{C}^\perp = \left\{ \begin{pmatrix} \mathcal{D} & 0_{(m-\rho)\times\rho} \\ 0_{(\alpha+1-m+\rho)\times(m-\rho)} & 0_{(\alpha+1-m+\rho)\times\rho} \\ A & B \end{pmatrix} : A \in \mathbb{F}_q^{(n-\alpha-1)\times(m-\rho)}, B \in \mathbb{F}_q^{(n-\alpha-1)\times\rho}, \mathcal{D} \subseteq \mathbb{F}_q^{(m-\rho)\times(m-\rho)} \text{ the set of diagonal matrices} \right\}.$$

$\mathcal{C}^\perp$ has dimension $(n-\alpha)m - \rho$ and maximum rank $m+n-\rho-\alpha-1 \geq n-\alpha+1$. Hence $\mathcal{C}^\perp$ is not a qOAC, that is, $\mathcal{C}$ is not a dually qOAC.

Note that if $m = n$ and $\rho = n-\alpha-1$, then the above example gives qOACs which are not classified in Theorem 2.5.

The structural question of qOACs with $\rho < n-\alpha$ is partially answered by a classification of matrix spaces given in [18]. Below we state the result in our language.

Theorem 2.8 ([18], Theorem 1.7)**.** Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ be a qOAC with $\dim(\mathcal{C}) = \alpha m + \rho$, $0 < \rho < m$. If $q = 2$ suppose that $\rho \geq 2(n-\alpha+1) - m$, else suppose that $\rho \geq 2(n-\alpha) - m$. Then $\mathcal{C}$ is equivalent to a linear subspace of $\mathrm{Mat}(\langle e_1, \ldots, e_i\rangle) + \mathrm{Mat}(\langle e_1, \ldots, e_{\alpha+1-i}\rangle)^t$, for some $0 \leq i \leq \alpha+1$.

If $\mathcal{C}$ is a qOAC of dimension $\dim(\mathcal{C}) = \alpha m + \rho$ and $\operatorname{maxrk}(\mathcal{C}) = \alpha + 1$, then $\mathcal{C}$ cannot be contained in a linear space of the form $\operatorname{Mat}(\langle e_1, \dots, e_i \rangle) + \operatorname{Mat}(\langle e_1, \dots, e_j \rangle)^t$ for some $i, j \geq 0$ with $i + j \leq \alpha$. Lemma 1 in [21] shows that, up to equivalence, $\mathcal{C}$ is contained in $\operatorname{Mat}(\langle e_1, \dots, e_{\alpha+1} \rangle) + \operatorname{Mat}(\langle e_1, \dots, e_{\alpha+1} \rangle)^t$. Theorem 2.5 and Theorem 2.8 prove that, under some assumptions on ρ, $\mathcal{C}$ is contained in a linear space of the form $\operatorname{Mat}(\langle e_1, \dots, e_i \rangle) + \operatorname{Mat}(\langle e_1, \dots, e_j \rangle)^t$ with $i + j = \alpha + 1$. In the next example, we exhibit a code which does not satisfy the assumptions of Theorem 2.5 or Theorem 2.8 and which is not contained in a linear space of the form above.
The following qOAC is inspired by an example given in [53]. It is the first example of a matrix space not being contained in a space of the form $\operatorname{Mat}(\langle e_1, \dots, e_i \rangle) + \operatorname{Mat}(\langle e_1, \dots, e_j \rangle)^t$ with $i + j$ the maximal rank of the matrix space. This shows, that the conditions on ρ in Theorem 2.5 and Theorem 2.8 are in general tight.

Example 2.9. Let $\mathcal{C} \subseteq \mathbb{F}_2^{4\times 4}$ be a linear code given by

$$\mathcal{C} = \left\{ \begin{pmatrix} a_1 & a_4 & a_5 & a_6 \\ 0 & a_2 & a_7 & a_8 \\ 0 & 0 & a_2 + a_3 & a_9 \\ 0 & 0 & 0 & a_3 \end{pmatrix} : a_i \in \mathbb{F}_2 \text{ for } 1 \leq i \leq 9 \right\}.$$

Then $\operatorname{maxrk}(\mathcal{C}) = 3$ and $\dim(\mathcal{C}) = 9$, hence $\mathcal{C}$ is a qOAC. In particular $\alpha = 2$ and $\rho = 1$, while Theorem 2.5 and Theorem 2.8 apply to codes with $\rho \geq 2$. We claim that $\mathcal{C}$ is not contained in any linear space of the form $\operatorname{Mat}(V)+\operatorname{Mat}(U)^t$ with $\dim(V)+\dim(U) = 3$. To see this, consider the following two elements of $\mathcal{C}$:

$$M_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ and } M_2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

We prove that if M_1 is contained in $\operatorname{Mat}(V)+\operatorname{Mat}(U)^t$ for some $V, U \subseteq \mathbb{F}_2^4$ of $\dim(V)+\dim(U) = 3$, then $V, U \subseteq \langle e_1, e_2, e_3 \rangle$. Note that this is sufficient to conclude, since M_2 is not contained in such a space.
The only non trivial case, up to transposition, is $\dim(V) = 2$ and $\dim(U) = 1$. Let $V = \langle (x_1, y_1, z_1, 0), (x_2, y_2, z_2, w) \rangle \subseteq \mathbb{F}_2^4$ and $U = \langle (a, b, c, d) \rangle \subseteq \mathbb{F}_2^4$. Note that by linearity we can directly assume that the last coordinate of one basis vector is 0. By assumption there are $A \in \operatorname{Mat}(\langle (x_1, y_1, z_1, 0), (x_2, y_2, z_2, w) \rangle)$ and $B \in \operatorname{Mat}(\langle (a, b, c, d) \rangle)^t$, such that $M_1 = A + B$. Hence the last column of M_1 describes the following homogeneous linear system for $(d, t_1, t_2) \in \mathbb{F}_2^3$:

$$\begin{array}{rcccccc} 0 & = & \alpha d & + & t_1 x_1 & + & t_2 x_2 \\ 0 & = & \beta d & + & t_1 y_1 & + & t_2 y_2 \\ 0 & = & \gamma d & + & t_1 z_1 & + & t_2 z_2 \\ 0 & = & \delta d & + & & + & t_2 w \end{array}, \tag{9}$$

for some $t_1, t_2, \alpha, \beta, \gamma, \delta \in \mathbb{F}_2$. The linear system in (9) has exactly one solution, i.e. the trivial one. To see this note that $(\alpha, \beta, \gamma, \delta) \notin V$, otherwise M_1 would be contained in $\operatorname{Mat}(V)$ which is a space of maximal rank 2. So we deduce that $d = 0$.

Applying the same argument to the last row of M_1 yields another homogeneous linear system for (δ, w). Yielding analogously $w = 0$. As a consequence we have proved that $V, U \subseteq \langle e_1, e_2, e_3 \rangle$.

In the sequel, we concentrate on linear spaces of the form $\mathrm{Mat}(\langle e_1, \ldots, e_i \rangle) + \mathrm{Mat}(\langle e_1, \ldots, e_j \rangle)^t$, as well as some of their linear subspaces.

Definition 2.10. Let $s, h, k \geq 0$ be integers such that $k \leq m$ and $0 < s + h \leq n$. Let

$$\mathcal{C}_{s,h,k} = \left\{ \begin{pmatrix} A & B \\ C & 0_{h\times(m-k)} \\ 0_{(n-s-h)\times k} & 0_{(n-s-h)\times(m-k)} \end{pmatrix} : A \in \mathbb{F}_q^{s\times k}, B \in \mathbb{F}_q^{s\times(m-k)}, C \in \mathbb{F}_q^{h\times k}, \right\}.$$

Remark 2.11. Up to equivalence, all the dually qOAC are of the form $\mathcal{C}_{s,h,k}$ for some s, h, k by Theorem 2.6. Moreover, one can check that $C_{s,h,k}$ is a dually qOAC if and only if there are parameters $0 \leq \alpha < n$ and $0 < \rho < m$ such that (s, h, k) is among $(\alpha, \rho, 1), (\alpha, 1, \rho), (0, n, \alpha + 1)$ if $m = n + 1$, or $(\alpha + \rho + 1 - m, m - \rho, m - 1)$ if $\rho \geq m - \alpha - 1$.

In the rest of the paper, we compute the invariants of the codes from Definition 2.10. In the next proposition, we characterize which codes of the form $\mathcal{C}_{s,h,k}$ are qOACs. Together with Theorem 2.6, Proposition 2.12 yields examples of qOACs which are not dually qOACs, beyond those of Example 2.7. Some examples of this kind are given in Example 2.13.

Proposition 2.12. Let s, h, k be non-negative integers such that $0 < s + h \leq n$ and $k < m$. Then $\mathcal{C}_{s,h,k}$ is a qOAC if and only if

$$0 < \min\{h, k\} \leq \left\lfloor \frac{m-1}{m - \max\{h,k\}} \right\rfloor.$$

Proof. The code $\mathcal{C}$ has dimension $\dim(\mathcal{C}) = sm + hk$ and maximum rank $s + \min\{h, k\}$. Then $\mathcal{C}$ is a qOAC iff $m \nmid hk$ and

$$\left\lceil \frac{sm + hk}{m} \right\rceil = s + \min\{h, k\} \quad \Longleftrightarrow \quad \left\lceil \frac{hk}{m} \right\rceil = \min\{h, k\}.$$

Therefore, $\mathcal{C}$ is a qOAC iff $\min\{h, k\} > 0$ and $(\min\{h, k\} - 1)m + 1 \leq hk \leq \min\{h, k\}m - 1$. A computation shows that $\mathcal{C}$ is a qOAC iff

$$0 < \min\{h, k\} \leq \left\lfloor \frac{m-1}{m - \max\{h,k\}} \right\rfloor.$$

Notice that $\max\{h, k\} < m$, since $m \nmid hk$. □

Example 2.13. Let $0 < k < m$ and let

$$\mathcal{C} = \left\{ \begin{pmatrix} A & 0_{n\times(m-k)} \end{pmatrix} : A \in \mathbb{F}_q^{n\times k}, \right\} \subseteq \mathbb{F}_q^{n\times m}.$$

By Theorem 2.6, $\mathcal{C}$ is a dually qOAC if and only if $m = n + 1$. By Proposition 2.12, $\mathcal{C}$ is a qOAC if and only if

$$k \leq \min\left\{ \left\lfloor \frac{m-1}{m-n} \right\rfloor, n \right\} \quad \text{or} \quad n \leq \min\left\{ \left\lfloor \frac{m-1}{m-n} \right\rfloor, k \right\}.$$

In the following sections, we compute the invariants of the codes from Definition 2.10. Since this does not affect the computation of the invariants, we always assume that $n = s + h$. This amounts to considering the codes $C_{s,k,n-s} = \mathrm{Mat}(\langle e_1, \dots, e_s \rangle) + \mathrm{Mat}(\langle e_1, \dots, e_k \rangle)^t$.

2.2 Generalized Weights

In this section we compute the generalized weights of codes of the form $\mathrm{Mat}(\langle e_1, \dots, e_s \rangle) + \mathrm{Mat}(\langle e_1, \dots, e_k \rangle)^t$. For what discussed in the previous section, this determines the weights of all dually qOACs and of certain qOACs. We start by recalling the definition of generalized weights.

Definition 2.14. ([61], Definition 23) Let $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ be a rank-metric code. For any integer $1 \leq i \leq \dim(\mathcal{C})$, the ith **generalized weight** of $\mathcal{C}$ is

$$d_i(\mathcal{C}) = \frac{1}{m} \min\{\dim(\mathcal{A}) \, : \, \mathcal{A} \subseteq \mathbb{F}_q^{n \times m} \text{ is an optimal anticode with } \dim(\mathcal{A} \cap \mathcal{C}) \geq i\}.$$

Generalized weights were defined in [61], where some of their basic properties were also established. A different - but related - definition of generalized weights was given in [51].
The next lemma is an easy result, that we will implicitly use in several proofs.

Lemma 2.15. Let $0 \leq s \leq n$ and let $S \subseteq ([n] \setminus [s]) \times [m]$ be such that for each $i \in [n] \setminus [s]$ there exists a $j_i \in [m]$ such that $(i, j_i) \in S$. Let

$$\mathcal{C} = \langle E_{i,j} \mid (i,j) \notin S \rangle.$$

Then the maximum dimension of an optimal anticode contained in $\mathcal{C}$ is sm.

Proof. The code $\mathcal{C} \supseteq \mathrm{Mat}(\langle e_1, \dots, e_s \rangle)$, which is an optimal anticode of dimension sm. Let $\mathrm{Mat}(V)$ be an optimal anticode with $\dim(V) > s$ and let $v \in V \setminus \langle e_1, \dots, e_s \rangle$. Let $M \in \mathbb{F}_q^{n \times m}$ be the matrix with all columns equal to v. Then $M \in \mathrm{Mat}(V) \setminus \mathcal{C}$, hence $\mathrm{Mat}(V) \not\subseteq \mathcal{C}$. □

This leads to a simple result, which will be used in the proof of Theorem 2.17.

Proposition 2.16. Let $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ be a rank-metric code which contains an optimal anticode of dimension sm for some $1 \leq s \leq n$. Then the following generalized weights are determined

$$d_{(i-1)m+1}(\mathcal{C}) = \cdots = d_{im}(\mathcal{C}) = i \text{ for } 1 \leq i \leq s.$$

Proof. Fix $0 \leq i \leq s$ and let $\mathcal{A}$ be an optimal anticode of dimension $\dim(\mathcal{A}) = im$ such that $\mathcal{A} \subseteq \mathcal{C}$. Then $d_{im}(\mathcal{C}) = i$, since $d_{im}(\mathcal{C}) \geq i$ by [61, Theorem 30] and $d_{im}(\mathcal{C}) \leq i$ since $\mathcal{C} \supseteq \mathcal{A}$. Using the properties of generalized weights from [61, Theorem 30], one easily obtains that

$$d_{(i-1)m+1}(\mathcal{C}) = \cdots = d_{im}(\mathcal{C}) = i.$$

□

We are now ready to state the main theorem of this section. The next theorem computes the generalized weights of all dually qOACs and some qOACs.

Theorem 2.17. Let $\mathcal{C} = \mathrm{Mat}(\langle e_1, \ldots, e_s \rangle) + \mathrm{Mat}(\langle e_1, \ldots, e_k \rangle)^t \subseteq \mathbb{F}_q^{n \times m}$. Then $\mathcal{C}$ has the following generalized weights,

$$\begin{array}{rcl} d_{(i-1)m+1}(\mathcal{C}) & = \cdots = & d_{im}(\mathcal{C}) \quad = i \qquad \text{for } 1 \leq i \leq s, \\ d_{sm+(i-1)k+1}(\mathcal{C}) & = \cdots = & d_{sm+ik}(\mathcal{C}) \quad = s+i \quad \text{for } 1 \leq i \leq n-s. \end{array}$$

Proof. By Lemma 2.15 and by direct inspection we find that $\mathcal{C} \supseteq \mathrm{Mat}(\langle e_1, \ldots, e_s \rangle)$. By Proposition 2.16 we obtain therefore

$$d_{(i-1)m+1}(\mathcal{C}) = \cdots = d_{im}(\mathcal{C}) = i \quad \text{for } 1 \leq i \leq s.$$

Fix $1 \leq i \leq n-s$ and let $\mathcal{A} = \mathrm{Mat}(V) \subseteq \mathbb{F}_q^{n \times m}$ be an optimal anticode with $V \subseteq \mathbb{F}_q^n$ of $\dim(V) = s+i$. We claim that $\dim(\mathcal{C} \cap \mathcal{A}) \leq sm + ik$. Since $\dim(V) = s+i$, then there exist i linearly independent vectors $v_1, \ldots, v_i \in V \setminus \langle e_1, \ldots, e_s \rangle$. Consider the linear subspace spanned by the following matrices,

$$M_j^1 = \begin{pmatrix} 0_{n \times k} & v_j & 0_{n \times m-k-1} \end{pmatrix}, \; M_j^2 = \begin{pmatrix} 0_{n \times k+1} & v_j & 0_{n \times m-k-2} \end{pmatrix}, \; \ldots$$

$$\ldots \; , M_j^{m-k} = \begin{pmatrix} 0_{n \times m-1} & v_j \end{pmatrix}$$

for $1 \leq j \leq i$. Clearly $\langle M_1^1, \ldots, M_i^1, \cdots, M_1^{m-k}, \ldots, M_i^{m-k} \rangle \subseteq \mathcal{A}$. Moreover,

$$\mathcal{C} \; \cap \; \langle M_1^1, \ldots, M_i^1, \cdots, M_1^{m-k}, \ldots, M_i^{m-k} \rangle = 0. \tag{10}$$

By (10) we deduce that $\mathcal{C} \oplus \langle M_1^1, \ldots, M_i^1, \cdots, M_1^{m-k}, \ldots, M_i^{m-k} \rangle \subseteq \mathcal{C} + \mathcal{A}$, hence

$$\begin{array}{rcl} \dim(\mathcal{C} + \mathcal{A}) & = & \dim(\mathcal{C}) + \dim(\mathcal{A}) - \dim(\mathcal{C} \cap \mathcal{A}) \\ & \geq & \dim(\mathcal{C}) + \dim(\langle M_1^1, \ldots, M_i^1, \cdots, M_1^{m-k}, \ldots, M_i^{m-k} \rangle). \end{array}$$

It follows directly that

$$d_{sm+ik+1}(\mathcal{C}) \geq s+i+1 \text{ for } 1 \leq i \leq n-s-1. \tag{11}$$

The inequality

$$d_{sm+1}(\mathcal{C}) \geq s+1 \tag{12}$$

follows from [61, Theorem 30].
In order to prove that all the previous inequalities are in fact equalities, consider $\mathcal{A} = \mathrm{Mat}(\langle e_1, \ldots, e_{s+i} \rangle)$. It is easy to check that $\dim(\mathcal{C} \cap \mathcal{A}) = sm + ik$. Therefore $d_{sm+ik}(\mathcal{C}) \leq s+i$ which, together with (11) and (12) yields

$$d_{sm+(i-1)k+1}(\mathcal{C}) = \cdots = d_{sm+ik}(\mathcal{C}) = s+i+1,$$

for $1 \leq i \leq n-s$. □

2.3 Rank Distribution

In this section we compute the rank distribution of codes of the form $\mathrm{Mat}(\langle e_1, \dots, e_s \rangle) + \mathrm{Mat}(\langle e_1, \dots, e_k \rangle)^t$. For what discussed in Section 2.1, this determines the rank distribution of all dually qOACs and of certain qOACs. We start by recalling a basic result from linear algebra.

Definition 2.18. The *Gaussian q-binomial coefficient* is the integer

$$\binom{n}{r}_q = \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{r-1})}{(q^r-1)(q^r-q)\cdots(q^r-q^{r-1})}.$$

Lemma 2.19. The number of rank r matrices in $\mathbb{F}_q^{n\times m}$ is

$$\phi_q(n,m,r) = \binom{n}{r}_q (q^m-1)(q^m-q)\cdots(q^m-q^{r-1}).$$

Theorem 2.20. Let $\mathcal{C} = \mathrm{Mat}(\langle e_1, \dots, e_s \rangle) + \mathrm{Mat}(\langle e_1, \dots, e_k \rangle)^t$. For $0 \le r \le n$ denote by A_r the number of elements of rank r in $\mathcal{C}$. Then

$$A_r = \phi_q(s,m,r) + \sum_{i=1}^{\min\{n-s,k,r\}} \binom{k}{i}_q \binom{m-i}{r-i}_q q^{si} \prod_{t=0}^{i-1}(q^{n-s}-q^t) \prod_{j=0}^{r-i-1}(q^s-q^j),$$

for $1 \le r \le \min\{s+k, n\}$.

Proof. The number of $n \times m$ matrices in $\mathcal{C}$ of rank $1 \le r \le n$ is the sum of the number of matrices of rank r in $\mathbb{F}_q^{s\times m}$ and the number of $n \times m$ matrices of rank r in $\mathbb{F}_q^{n\times m}$ which have at least one nonzero row among the last $n-s$. We denote the latter set of matrices by $\mathcal{C}_r$.
The first number is $\phi_q(s,m,r)$ by Lemma 2.19. We now compute the cardinality of $\mathcal{C}_r$. Let $1 \le i \le \min\{n-s, k, r\}$ and let $V \subseteq \mathbb{F}_q^m$ of $\dim(V) = i$. Let $U \subseteq \mathbb{F}_q^m$ be an r-dimensional vector space containing V. Since r-dimensional vector spaces U containing a given i-dimensional subspace are in one-to-one correspondence with $(r-i)$-dimensional vector spaces in $\mathbb{F}_q^{m-i}$, the number of r-dimensional vector spaces U such that of $\mathbb{F}_q^m \supseteq U \supseteq V$ is

$$\binom{m-i}{r-i}_q. \tag{13}$$

Next we determine the number of matrices with row space U and such that the row space of the last $n-s$ rows is V. Complete a basis $u_1, \dots, u_i$ of V to a basis $u_1, \dots, u_r$ of U. We observe that every such $M \in \mathcal{C}_r$ is of the form

$$M = D \cdot \begin{pmatrix} u_1 \\ \vdots \\ u_r \end{pmatrix} \in \mathcal{C}_r, \text{ where } D = \begin{pmatrix} A & B \\ C & 0_{(n-s)\times(r-i)} \end{pmatrix},$$

$A \in \mathbb{F}_q^{s\times i}, B \in \mathbb{F}_q^{s\times(r-i)}, C \in \mathbb{F}_q^{(n-s)\times i}$. Moreover B, C, and D must have full rank. Since there is a one-to-one correspondence between M and D, the number of matrices in $\mathcal{C}_r$ with row space U and such that the last $n-s$ rows generate V is

$$q^{si}\prod_{t=0}^{i-1}(q^{n-s}-q^t)\prod_{j=0}^{r-i-1}(q^s-q^j). \tag{14}$$

The product of (13) and (14) is then the number of matrices in $\mathcal{C}_r$, whose last $n-s$ rows span V.
Finally, observe that for a given $1 \le i \le \min\{n-s, k, r\}$ there are

$$\binom{k}{i}_q$$

i-dimensional subspaces V in $\mathbb{F}_q^k$. Hence the cardinality of $\mathcal{C}_r$ is

$$\sum_{i=1}^{\min\{n-s,k,r\}}\binom{k}{i}_q\binom{m-i}{r-i}_q q^{si}\prod_{t=0}^{i-1}(q^{n-s}-q^t)\prod_{j=0}^{r-i-1}(q^s-q^j).$$

□

2.4 Rank Functions of the q-Polymatroid

q-polymatroids are the q-analogs of polymatroids. They were introduced indipendently by Shiromoto in [66] and by Gorla, Jurrius, López Valdez, and Ravagnani in [31]. In this section we compute the rank functions of the q-polymatroids associated to codes of the form $\mathrm{Mat}(\langle e_1,\dots,e_s\rangle)+\mathrm{Mat}(\langle e_1,\dots,e_k\rangle)^t$. By Lemma 2.24 this determines the q-polymatroids associated to all dually qOACs and to certain qOACs.
We start by recalling the relevant definitions. The fact that the functions ρ_c and ρ_r define q-polymatroids is shown in [31, Theorem 5.3].

Definition 2.21. Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ be a rank-metric code, and let $J \subseteq \mathbb{F}_q^n$ and $K \subseteq \mathbb{F}_q^m$ be linear subspaces. The **q-polymatroids** associated to $\mathcal{C}$ are $(\mathbb{F}_q^n, \rho_c)$ and $(\mathbb{F}_q^m, \rho_r)$, where

$$\rho_c(\mathcal{C}, J) = \frac{\dim(\mathcal{C}) - \dim(\mathcal{C}\cap \mathrm{Mat}(J^\perp))}{m}$$

and

$$\rho_r(\mathcal{C}, K) = \frac{\dim(\mathcal{C}) - \dim(\mathcal{C}\cap \mathrm{Mat}(K^\perp)^t)}{n}.$$

The next proposition follows directly from the definition of the rank functions.

Proposition 2.22. Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ be a rank-metric code and assume that $m \nmid \dim(\mathcal{C})$. The following are equivalent:

1. $\mathcal{C}$ is a qOAC,

2. $\lceil \rho_c(\mathcal{C}, \mathbb{F}_q^n) \rceil = \operatorname{maxrk}(\mathcal{C})$,

3. $m = n$ and $\lceil \rho_r(\mathcal{C}, \mathbb{F}_q^m) \rceil = \operatorname{maxrk}(\mathcal{C})$.

Proof. Assume $n < m$. By Theorem 2.21 we find that

$$\lceil \rho_c(\mathcal{C}, \mathbb{F}_q^n) \rceil = \left\lceil \frac{\dim(\mathcal{C})}{m} \right\rceil. \tag{15}$$

Thus $\mathcal{C}$ is a qOAC if and only if $\lceil \rho_c(\mathcal{C}, \mathbb{F}_q^n) \rceil = \operatorname{maxrk}(\mathcal{C})$. If $n = m$ consider Proposition 6.1 [31], then

$$\rho_r(\mathcal{C}, \mathbb{F}_q^m) = \frac{m}{n} \rho_c(\mathcal{C}, \mathbb{F}_q^n) = \rho_c(\mathcal{C}, \mathbb{F}_q^n)$$

and the result follows immediately. □

The next lemma will be used in the proof of Theorem 2.25.

Lemma 2.23. Let $h \geq 0$, $0 \leq k \leq m$, and $0 \leq s \leq m-h$. Let $\mathcal{C} = \operatorname{Mat}(\langle e_1, \ldots, e_s \rangle) + \operatorname{Mat}(\langle e_1, \ldots, e_k \rangle)^t \subseteq \mathbb{F}_q^{(s+h)\times m}$ be a rank-metric code. Let $J \subseteq \mathbb{F}_q^{s+h}$ and $K \subseteq \mathbb{F}_q^m$. Then:

(a) If $J \cap \langle e_1, \ldots, e_s \rangle = 0$, then $\dim(\mathcal{C} \cap \operatorname{Mat}(J)) = k \cdot \dim(J)$.

(b) If $K \cap \langle e_1, \ldots, e_k \rangle = 0$, then $\dim(\mathcal{C} \cap \operatorname{Mat}(K)^t) = s \cdot \dim(K)$.

Proof. We only prove the first statement, as the second is proved similarly. Let $M \in \mathcal{C} \cap \operatorname{Mat}(J)$. The last $m - k$ columns of M belong to $J \cap \langle e_1, \ldots, e_s \rangle$, hence they are zero. Therefore $\mathcal{C} \cap \operatorname{Mat}(J) \subseteq \operatorname{Mat}(\langle e_1, \ldots, e_k \rangle)^t \cap \operatorname{Mat}(J) \subseteq \mathcal{C} \cap \operatorname{Mat}(J)$, where the second inclusion follows from $\mathcal{C} \supseteq \operatorname{Mat}(\langle e_1, \ldots, e_k \rangle)^t$. It follows that

$$\mathcal{C} \cap \operatorname{Mat}(J) = \operatorname{Mat}(\langle e_1, \ldots, e_k \rangle)^t \cap \operatorname{Mat}(J),$$

in particular $\dim(\mathcal{C} \cap \operatorname{Mat}(J)) = k \cdot \dim(J)$. □

The proof of the next lemma is immediate.

Lemma 2.24. Let $V \subseteq \mathbb{F}_q^n$ and let $\mathcal{C} \subseteq \operatorname{Mat}(V) \subseteq \mathbb{F}_q^{n\times m}$ be a rank-metric code. Then

$$\mathcal{C} \cap \operatorname{Mat}(J) = \mathcal{C} \cap \operatorname{Mat}(J \cap V)$$

for any $J \subseteq \mathbb{F}_q^n$. In particular, if $\mathcal{C} \subseteq \operatorname{Mat}(\langle e_1, \ldots, e_\ell \rangle)$ for some $\ell \leq n$, then one can regard $\mathcal{C}$ as a rank-metric subcode of $\mathbb{F}_q^{\ell\times m}$ by deleting the last $n - \ell$ rows of each matrix. Moreover, the q-polymatroid $(\mathbb{F}_q^m, \rho_r)$ is left unchanged by this operation and the q-polymatroid $(\mathbb{F}_q^\ell, \rho_c)$ determines the q-polymatroid $(\mathbb{F}_q^n, \rho_c)$ according to the formula above.

Theorem 2.25. Let $h \geq 0$, $0 \leq k \leq m$, and $0 \leq s \leq m-h$. Let $V = \langle e_1, \ldots, e_s \rangle, V' = \langle e_1, \ldots, e_{s+h} \rangle \subseteq \mathbb{F}_q^n$ and let $U = \langle e_1, \ldots, e_k \rangle \subseteq \mathbb{F}_q^m$. Let $\mathcal{C} = \mathrm{Mat}(V) + (\mathrm{Mat}(U)^t \cap \mathrm{Mat}(V')) \subseteq \mathbb{F}_q^{n \times m}$ be a rank-metric code. Let $J \subseteq \mathbb{F}_q^n$ and $K \subseteq \mathbb{F}_q^m$. The rank functions of the q-polymatroids associated to $\mathcal{C}$ are

$$\rho_r(\mathcal{C}, K) = \frac{h(k - \dim(U \cap K^\perp)) + s \cdot \dim(K)}{n}$$

and

$$\rho_c(\mathcal{C}, J) = s - \dim(V \cap J^\perp) + \frac{k(h + \dim(V \cap J^\perp) - \dim(V' \cap J^\perp))}{m}.$$

Proof. For any $J \subseteq \mathbb{F}_q^n$, one has

$$\mathcal{C} \cap \mathrm{Mat}(J) = \mathcal{C} \cap \mathrm{Mat}(J \cap V') \tag{16}$$

by Lemma 2.24, since $\mathcal{C} \subseteq \mathrm{Mat}(V')$. Write $J \cap V'$ as $(J \cap V) + J'$, where $J' \cap V = 0$. This can always be done by letting J' be the vector space generated by a set of vectors that, together with a basis of $J \cap V$, form a basis of $J \cap V'$. Then

$$\begin{aligned} \mathcal{C} \cap \mathrm{Mat}(J \cap V') &= \mathcal{C} \cap \mathrm{Mat}(J \cap V + J') = \mathcal{C} \cap [\mathrm{Mat}(J \cap V) + \mathrm{Mat}(J')] \\ &= \mathrm{Mat}(J \cap V) + \mathcal{C} \cap \mathrm{Mat}(J'). \end{aligned}$$

Since $J' \cap V = 0$, then

$$\dim(\mathrm{Mat}(J \cap V) + \mathcal{C} \cap \mathrm{Mat}(J')) = \dim(\mathrm{Mat}(J \cap V)) + \dim(\mathcal{C} \cap \mathrm{Mat}(J')). \tag{17}$$

Moreover $\dim(\mathcal{C} \cap \mathrm{Mat}(J')) = k \cdot \dim(J')$ by Lemma 2.23. Combining (16), (2.4), and (17) one gets

$$\begin{aligned} \dim(\mathcal{C} \cap \mathrm{Mat}(J)) &= m \cdot \dim(J \cap V) + k \cdot \dim(J') \\ &= m \cdot \dim(J \cap V) + k(\dim(J \cap V') - \dim(J \cap V)). \end{aligned}$$

Therefore

$$\begin{aligned} \rho_c(\mathcal{C}, J) &= \frac{\dim(\mathcal{C}) - \dim(\mathcal{C} \cap \mathrm{Mat}(J^\perp))}{m} \\ &= s - \dim(V \cap J^\perp) + \frac{k(h + \dim(V \cap J^\perp) - \dim(V' \cap J^\perp))}{m} \end{aligned}$$

as claimed. The other equality is proved similarly. □

3 Sum-Rank Metric Codes and an Application

3.1 Definitions and fundamental Properties

Throughout this section we will consider matrices in the space $\mathbb{F}_q^{m\times n}$, where $n \leq m$. Hence matrices having more rows than columns. This differs from the setup considered in Section 1 and 2. In particular, for $n \leq m$, rank-metric optimal anticodes in $\mathbb{F}_q^{m\times n}$ are different from those in $\mathbb{F}_q^{n\times m}$. This is accurately pointed out in [30, Section 11.2 and 11.3] through the existence of different notions of support. Concretely we have that in $\mathbb{F}_q^{m\times n}$ every optimal anticode of maximum rank r is of the form $\mathrm{Mat}(V)^t$ for some r-dimensional vector space $V \subseteq \mathbb{F}_q^n$. It is equivalent to the standard optimal anticode consisting of the matrices whose last $n-r$ columns are equal to zero. The difference between considering optimal anticodes in $\mathbb{F}_q^{n\times m}$ and in $\mathbb{F}_q^{m\times n}$ is also described in [30, Example 11.3.11].

Fix positive integers $\ell, n_1, \ldots, n_\ell, m_1, \ldots, m_\ell$ such that $m_1 \geq \ldots \geq m_\ell$ and $n_i \leq m_i$ for $i \in [\ell]$. We write $n = n_1 + \ldots + n_\ell$.

Definition 3.1. Let $C = (C_1, \ldots, C_\ell) \in \mathbb{M}$, where $C_i \in \mathbb{F}_q^{m_i\times n_i}$ for $i \in [\ell]$. We define the **sum-rank weight** of C as

$$\mathrm{srank}(C) = \sum_{i=1}^{\ell} \mathrm{rank}(C_i).$$

The **sum-rank metric** is then defined as

$$\begin{array}{rccl} d & : & \mathbb{M}\times\mathbb{M} & \longrightarrow & \mathbb{N} \\ & & (C,D) & \longmapsto & \mathrm{srank}(C-D). \end{array}$$

A **linear sum-rank metric code** $\mathcal{C}$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{M}$ endowed with the sum-rank metric. Throughout the paper, we will refer to it simply as a (sum-rank) code. A code $\mathcal{C} \subseteq \mathbb{M}$ is **non-trivial** if $\mathcal{C} \neq 0$. The **minimum distance** of a code $0 \neq \mathcal{C} \subseteq \mathbb{M}$ is

$$\mathrm{d}(\mathcal{C}) = \min\{\mathrm{srank}(C) : C \in \mathcal{C} \setminus \{0\}\}$$

and the **maximum sum-rank distance** is

$$\mathrm{maxsrk}(\mathcal{C}) = \max\{\mathrm{srank}(C) : C \in \mathcal{C}\}.$$

Notice that, if we let $\ell = 1$, then $\mathcal{C} \subseteq \mathbb{F}_q^{m_1\times n_1}$ is a rank-metric code. We refer the interested reader to [30] for an introduction to rank-metric codes and their invariants. If $m_1 = \ldots = m_\ell = 1$, then $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a linear block code endowed with the Hamming metric.

For a square matrix A, let $\mathrm{tr}(A)$ denote its trace. Then

$$\begin{array}{rccc} \mathrm{Tr} & : & \mathbb{M}\times\mathbb{M} & \longrightarrow & \mathbb{F}_q \\ & & (D,C) & \longmapsto & \sum_{i=1}^{\ell}\mathrm{tr}(D_iC_i^t) \end{array}$$

is a nondegenerate bilinear form. We define the dual of a code as the natural extension of the dual of a rank-metric code, as defined in [19].
In a similar way we define the dual of a sum-rank metric code $\mathcal{C}\subseteq\mathbb{M}$.

Definition 3.2. Let $\mathcal{C}\subseteq\mathbb{M}$ be a code. The dual of $\mathcal{C}$ is

$$\mathcal{C}^{\perp}=\{D\in\mathbb{M}:\mathrm{Tr}(D,C)=0 \text{ for all } C\in\mathcal{C}\}.$$

3.2 Multishot Network Coding

In Section 1.2 we introduced linear network coding in a one-shot variant, i.e. using the network only once. Therein we described how rank-metric codes are suitable for error correction in the transmission. The use of sum-rank metric codes for **multishot network coding** can be seen as a generalization of it. In multishot network coding the matrix channel is used several times which leads to idea of using codes consisting of a list of matrices. A main motivation of multishot network coding is the ability of detecting more errors when using the channel several times. An example of such a situation is reported in [55]. Nóbrega and Uchôa-Filho were the first to propose rank-metric codes for constructing error-correcting codes for the repeated transmission over the operator channel [56]. We present the multishot channel model for ℓ uses of the channel who was introduced in [56]:

$$Y^{(i)}=A^{(i)}P^{(i)}+E^{(i)}, \tag{18}$$

where $Y^{(i)}, A^{(i)}, P^{(i)}$ and $E^{(i)}$ are given as in (4) at every shot $i\in[\ell]$.
We use the same notation as in Definition 1.12 to extend the subspace distance. Denote by $\mathcal{P}(X)^{\ell}$ the collection of elements of the form $(U_1,\dots,U_\ell)$ where $U_i\in\mathcal{P}(X)$ for $i\in[\ell]$.

Definition 3.3 ([56])**.** The **extended subspace distance** of $V=(V_1,\dots,V_\ell), W=(W_1,\dots,W_\ell)\in\mathcal{P}(\mathbb{F}_q^n)^{\ell}$ is given by the function

$$\begin{array}{rccc} d_{ES} & : & \mathcal{P}(\mathbb{F}_q^n)^{\ell}\times\mathcal{P}(\mathbb{F}_q^n)^{\ell} & \longrightarrow & \mathbb{N} \\ & & (V,W) & \longmapsto & \sum_{j=1}^{\ell} d_S(V_i,W_i). \end{array}$$

An **extended subspace code** $\mathcal{D}$ is a nonempty subset of $\mathcal{P}(\mathbb{F}_q^n)^{\ell}$ equipped with the extended subspace distance.

In an analogous way as in Definition 1.13 we define the lifting of a list of matrices.

Definition 3.4. Let $\mathcal{I}_E:(\mathbb{F}_q^{m\times n})^{\ell}\to\mathcal{P}(\mathbb{F}_q^{m+n})^{\ell}$ be given by $M=(M_1,\dots,M_\ell)\mapsto\mathcal{I}_E(M)=(\mathcal{I}(M_1),\dots,\mathcal{I}(M_\ell))$. Let $\mathcal{C}\subseteq(\mathbb{F}_q^{m\times n})^{\ell}$ be a sum-rank metric code, then the extended subspace code $\mathcal{I}_E(\mathcal{C})$, obtained by lifting every codeword of $\mathcal{C}$, is the **extended lifting** of $\mathcal{C}$.

As one may expect the relation between the extended subspace distance and the sum-rank distance is maintained as in the rank-metric case.

Proposition 3.5 ([56]). Let $\mathcal{C} \subseteq (\mathbb{F}_q^{m\times n})^\ell$ be a sum-rank metric code and $M, N \in \mathcal{C}$, then

$$d_{ES}(\mathcal{I}_E(M), \mathcal{I}_E(N)) = 2d(M, N)$$

and in particular the minimal extended subspace distance of $\mathcal{I}_E(\mathcal{C})$ is twice the minimal sum-rank distance of $\mathcal{C}$.

The first pioneering construction and decoding of lifted sum-rank metric codes to use for error correction in multishot network coding was given in [71] by Wachter-Zeh, Stinner and Sidorenko. In order to create dependencies and to cope better with difficult error patterns in each shot, a particular family of linear convolutional codes with unite memory named **(Partial) Unit Memory Codes ((P)UM codes)** is proposed. In the following we give an overview of the lifted construction of (P)UM codes based on generator matrices of Gabidulin codes. For a detailed introduction to convolutional codes we refer the interested reader to [44].

Definition 3.6. Let $R = \mathbb{F}_q[x]$ be the ring of polynomials with coefficients in the field $\mathbb{F}_q$. A **convolutional code** $\mathcal{C}$ of rate k/n is an R-submodule of R^n of rank k. A $k \times n$ matrix with entries in R whose rows are a basis of $\mathcal{C}$ is called a **generator matrix** of $\mathcal{C}$. A generator matrix $G(x)$ is **left prime** if in all factorizations $G(x) = \Delta(x)\tilde{G}(x)$ with $\Delta(x) \in R^{k\times k}$ and $\tilde{G}(x) \in R^{k\times n}$, the factor $\Delta(x)$ is **unimodular**. We recall that a matrix $V(x) \in R^{k\times k}$ is unimodular if there is a $k \times k$ matrix $U(x)$ with entries in R such that $V(x)U(x) = U(x)V(x) = I_k$. We call a generator matrix **non-catastrophic** if it is left prime.

Let k and $k^{(1)}$ be positive integers such that $k^{(1)} < k \leq n$ and $\ell > 1$ (since we assume to use the channel more than once). A $\mathcal{PUM}(n, k, k^{(1)})$ code is a convolutional code of memory one with non-catastrophic generator matrix

$$G = \begin{pmatrix} G^{(0)} & G^{(1)} & 0_{k\times n} & \dots & 0_{k\times n} \\ 0_{k\times n} & G^{(0)} & G^{(1)} & \dots & 0_{k\times n} \\ \vdots & & \ddots & \ddots & \\ 0_{k\times n} & \dots & 0_{k\times n} & G^{(0)} & G^{(1)} \end{pmatrix} \in \mathbb{F}_{q^m}^{k(\ell-1)\times n\ell},$$

where $G^{(0)}, G^{(1)} \in \mathbb{F}_{q^m}^{k\times n}$.
A unit memory code $\mathcal{UM}(n, k)$ has full rank matrices $G^{(0)}$ and $G^{(1)}$, whereas a partial unit memory code $\mathcal{PUM}(n, k, k^{(1)})$ has only full rank matrix $G^{(0)}$ and $\operatorname{rank}(G^{(1)}) = k^{(1)}$. The generator matrix of (P)UM codes presented in [71] has matrices $G^{(0)}$ and $G^{(1)}$ composed by Gabidulin generator matrices as given in Definition 1.17 with different Frobenius powers (for a detailed construction see Definition 8 in [71]).
By the transposed version of (1), we can consider elements of a convolutional code $\mathcal{C}$ with generator matrix G as a list of matrices $C_i \in \mathbb{F}_q^{m\times n}$ for $i \in [\ell]$ of the form $C = (C_1, \dots, C_\ell) \in \mathcal{C}$. Let $\mathcal{C} \subseteq (\mathbb{F}_q^{m\times n})^\ell$ be a Gabidulin based $\mathcal{PUM}(n, k, k^{(1)})$ code

with codewords $(C_1, \ldots, C_\ell)$ and let $\mathcal{I}_E(\mathcal{C})$ be its extended lifting as given in Definition 3.4. Then the subspace $\mathcal{I}(C_i)$ is propagated over the operator channel at shot i for every $i \in [\ell]$. In other words the transmitted matrix at shot i in (18) is given by $P^{(i)} = \begin{pmatrix} I_m & C_i \end{pmatrix}$.

There are several distances proposed for determining the error-correction capability of a convolutional rank-metric code. In Definition 6 [71] the authors use the **active row rank distance** for their decoding algorithms. Notice that for non-catastrophic encoders the minimum of all the active row rank distances coincides with the **free rank distance**, which in turn is exactly the minimum sum-rank distance of a linear convolutional rank-metric code. However it turns out in [46] that the active row rank distance is not the right distance to consider for the error-correction capability of convolutional rank-metric codes of arbitrary memory. In fact in the same paper the authors propose the **column sum rank distance** given by

$$d^j(\mathcal{C}) = \min \left\{ \sum_{i=1}^{j+1} \operatorname{rank}(C_i) : C = (C_1, \ldots, C_\ell) \in \mathcal{C}, C \neq 0 \right\}$$

for $j \in [\ell]$. It is namely shown there that the column sum rank distance determines the maximum rank deficiency of the network.

Another contribution to the application of sum-rank metric codes in reliable and secure multishot network coding was made by Martínez-Peñas and Kschischang in [50]. The authors provide a coding scheme for error-free communication based on linearized Reed-Solomon codes and a decoding algorithm for sum-rank metric codes with quadratic complexity.

4 Optimal Anticodes and MSRD Codes in the Sum-Rank Metric

Section 4 arises in collaboration with Eduardo Camps Moreno, Elisa Gorla, Elisa Lorenzo García, Umberto Martínez-Peñas and Flavio Salizzoni and introduces optimal codes and generalized weights in the sum-rank metric.

4.1 Maximal Rank in Cosets of Rank-Metric Codes

In this section we provide lower bounds for the maximum rank of a coset of a rank-metric code. Our strategy is inspired by that used by Meshulam in [53] and extends it to cosets of a vector space. In the following we give alternative proofs to the ones given in [16, Theorem 4, Corollary 2].

We set up the definitions for the rest of the subsection.

Definition 4.1. Let $\prec$ be the lexicographic order on $\mathbb{N} \times \mathbb{N}$ and let

$$\begin{array}{rccl} \phi & : & \mathbb{F}_q^{m\times n} & \to & \mathbb{N}\times\mathbb{N} \\ & & M & \mapsto & \min_{\prec}\{(i,j) : M(i,j) \neq 0\}. \end{array}$$

For a collection $\mathcal{M} = \{M_1, \ldots, M_d\}$ of matrices in $\mathbb{F}_q^{m\times n}$, we define a matrix M whose entry in position (i,j) is

$$M(i,j) = \begin{cases} 1 & \text{if } (i,j) = \phi(M_k) \text{ for some } k \in [d], \\ 0 & \text{otherwise.} \end{cases}$$

Let a line be either a row or a column. Denote by $\rho(\mathcal{M})$ the minimal number of lines in M which cover all ones in M. A set of locations of entries in a matrix is **independent** if it contains no two locations on the same line.

König's Theorem relates the cardinality of an independent set of locations of entries of a zero-one matrix to the minimum number of lines containing all the nonzero entries.

Theorem 4.2 (König's Theorem, [40, 69])**.** If the entries of a rectangular matrix are zeros and ones, then the minimum number of lines containing all the entries equal to one is equal to the maximum cardinality of an independent set of these entries.

In [53] Meshulam uses König's Theorem to establish a lower bound for the maximum rank of a matrix in a given vector space. In this section, we extend Meshulam's result from vector spaces of matrices to cosets. We start with a preliminary result.

Lemma 4.3. Let $D_1, \ldots, D_r, A \in \mathbb{F}_q^{r\times r}$ be such that the first $i-1$ rows of D_i are zero and the ith row is e_i^t for all $i \in [r]$. Then there are $x_1, \ldots, x_r \in \{0,1\}$ such that

$$\operatorname{rank}\left(A + \sum_{i=1}^{r} x_i D_i\right) = r.$$

Proof. We proceed by induction on r. The case $r = 1$ is trivially true, hence assume that $r > 1$. For $i \in [r-1]$ let $D_i' = D_i([r-1],[r-1])$. By the induction hypothesis there are $x_1, \ldots, x_{r-1} \in \{0,1\}$ such that the matrix $A([r-1],[r-1]) + \sum_{i=1}^{r-1} x_i D_i'$ is non-singular. Since $D_r(i,j) = 0$ for all $(i,j) \neq (r,r)$ and $D_r(r,r) = 1$, by expanding with respect to the bottom row we obtain

$$\det\left(A + \sum_{i=1}^{r-1} x_i D_i + D_r\right) = \det\left(A + \sum_{i=1}^{r-1} x_i D_i\right) +$$
$$+ (-1)^{r+1} \det\left(A([r-1],[r-1]) + \sum_{i=1}^{r-1} x_i D_i'\right).$$

The last summand is nonzero, therefore

$$A + \sum_{i=1}^{r-1} x_i D_i + D_r \text{ and } A + \sum_{i=1}^{r-1} x_i D_i$$

cannot both be singular. □

The next theorem extends the main result of [53] from vector spaces to cosets.

Theorem 4.4. Let $A \in \mathbb{F}_q^{m\times n}$ and let $\mathcal{M} = \{M_1, \ldots, M_d\} \subseteq \mathbb{F}_q^{m\times n}$. Then there exist $x_1, \ldots, x_d \in \{0,1\}$ such that

$$\operatorname{rank}(A + x_1 M_1 + \cdots + x_d M_d) \geq \rho(\mathcal{M}).$$

Proof. Let $\rho(\mathcal{M}) = r$. By Theorem 4.2 there exist $i_1, \ldots, i_r \in [d]$ such that $\{\phi(M_{i_j}) : j \in [r]\}$ is independent. Let $\phi(M_{i_j}) = (s_j, l_j)$ for $j \in [r]$, then both $S = \{s_1, \ldots, s_r\}$ and $L = \{l_1, \ldots, l_r\}$ have cardinality equal to r. Let $B_j = M_{i_j}(S, L)$ for $j \in [r]$. We prove the theorem by showing that $A(S,L) + \langle B_1, \ldots, B_r\rangle$ contains a non-singular matrix. Assume that $s_1 < s_2 < \cdots < s_r$. Let σ be the permutation on $[r]$ such that $l_{\sigma(1)} < \cdots < l_{\sigma(r)}$. We denote the jth row of B_j by b_j.
Clearly the first $j-1$ rows of B_j are zero, $b_j(s) = 0$ for $s \in [\sigma^{-1}(j)-1]$ and $b_j(\sigma^{-1}(j)) \neq 0$. Let $C \in \mathbb{F}_q^{r\times r}$ be the matrix with rows $b_1, \ldots b_r$. Notice that C is non-singular, since we can obtain an upper triangular matrix with nonzero entries on the diagonal by permuting the rows of C. Let $D_j = B_j C^{-1}$ for $j \in [r]$. It easy to check that the first $j-1$ rows of D_j are zero and the jth row is e_j^t for all $j \in [r]$.
By Lemma 4.3 we have that $A(S,L)C^{-1} + \sum_{j=1}^{r} x_j D_j$ is non-singular for some $x_1, \ldots, x_r \in \{0,1\}$. Therefore

$$A(S,L) + \sum_{j=1}^{r} x_j B_j = \left(A(S,L)C^{-1} + \sum_{j=1}^{r} x_j D_j\right) C$$

is also non-singular. This implies that $\operatorname{rank}(A + \sum_{j=1}^{r} x_j M_{i_j}) \geq r$. □

The following lemma will be used in the proof of the next theorem.

Lemma 4.5. Let $f : \mathbb{F}_q^{r\times r} \to \mathbb{F}_q$ be a constant linear form on $\mathrm{GL}_r(\mathbb{F}_q)$. Suppose that either $r > 1$ or $q \neq 2$. Then $f = 0$.

Proof. Since f is linear, there exist $a_{i,j} \in \mathbb{F}_q$, $i, j \in [r]$, such that

$$f(X) = \sum_{1\leq i,j\leq r} a_{i,j}x_{i,j}$$

for any $X = (x_{i,j}) \in \mathbb{F}_q^{r\times r}$. If $r = 1$ and $q \neq 2$, let $1 \neq \alpha \in \mathbb{F}_q^*$. Then $f(\alpha) = f(1) - f(1-\alpha) = 0$, hence $f = 0$. If $r > 1$, fix $(k, l) \in [r] \times [r]$. Let $B = (b_{i,j})$ be a permutation matrix such that $b_{k,l} = 0$. Let $\bar{B} = B + E_{k,l}$. Both B and $\bar{B}$ are non-singular, so $f(B) = f(\bar{B})$. Therefore $f(E_{k,l}) = 0$ by linearity. Since this is the case for every $(k, l) \in [r] \times [r]$, we conclude that $f = 0$. □

The next proposition is a particular case of the anticode bound for affine spaces over $\mathbb{F}_2$.

Proposition 4.6. Let $n \geq 2$ and $m > 2$. Let $\mathcal{V} \subseteq \mathbb{F}_2^{m\times n}$ be an $\mathbb{F}_2$-linear subspace such that $\dim(\mathcal{V}) = m$. Let $A \in \mathbb{F}_2^{m\times n} \setminus \mathcal{V}$. Then there exists $B \in \mathcal{V}$ such that

$$\mathrm{rank}(A + B) \geq 2.$$

Proof. If $\mathrm{rank}(A) \geq 2$ the statement is trivially true taking $B = 0$. Hence consider $\mathrm{rank}(A) = 1$ and we can assume up to equivalence that $A = e_1 \cdot e_1^t$.
If $\mathrm{maxrk}(\mathcal{V}) = 1$, then $\mathcal{V}$ is an optimal anticode and the statement is true.
If $\mathrm{maxrk}(\mathcal{V}) > 2$, then there exists $B \in \mathcal{V}$ with $\mathrm{rank}(B) > 2$ and so $\mathrm{rank}(A + B) \geq 2$, since A has rank 1. Therefore, we shall prove the statement for $\mathrm{maxrk}(\mathcal{V}) = 2$.
In first instance we suppose that there are two different elements $V_1, V_2 \in \mathcal{V}$ of rank 1. Let $V_1 = v_1^t \cdot w_1$ and $V_2 = v_2^t \cdot w_2$ for some $v_1, v_2 \in \mathbb{F}_2^m$ and $w_1, w_2 \in \mathbb{F}_2^n$. If $\mathrm{rank}(A+V_1) = \mathrm{rank}(A+V_2) = 1$, then either $v_1^t = e_1$ or $w_1 = e_1^t$ and either $v_2^t = e_1$ or $w_2 = e_1^t$. If $v_1^t = e_1$ and $w_2 = e_1^t$ we obtain that $\mathrm{rank}(A+V_1+V_2) = 2$, since $V_1, V_2 \neq A$. The case $w_1 = e_1^t$ and $v_2^t = e_1$ is treated analogously. Instead, if $v_1^t = v_2^t = e_1$, we have that

$$\dim\left(\mathrm{rowsp}(A, A + V_1, A + V_1 + V_2)\right) = 3,$$

and every matrix in $\langle A, A + V_1, A + V_1 + V_2\rangle$ has rank 1. Let $B \in \mathcal{V}$ be an element of rank two. Then there exists $C \in \{A, A + V_1, A + V_2\}$ such that $\mathrm{rank}(C + B) = \dim(\mathrm{rowsp}(C + B)) \geq 2$. In the case where $w_1 = w_2 = e_1^t$ we proceed in an analogous way using the column space.
Suppose now that in $\mathcal{V}$ there is at most one element of rank 1. Then every linear combination with an element of maximum rank in $\mathcal{V}$ has again maximum rank. Hence, since $\dim(\mathcal{V}) > 2$, there are two linearly independent elements B_1, B_2 such that $\mathrm{rank}(B_1) = \mathrm{rank}(B_2) = \mathrm{rank}(B_1 + B_2) = 2$. Assume that $\mathrm{rank}(A + B_1) = \mathrm{rank}(A + B_2) = \mathrm{rank}(A + B_1 + B_2) = 1$, then we have without loss of generality that

$$B_1 = e_1 \cdot e_1^t + e_2 \cdot e_2^t,\ B_2 = e_1 \cdot e_1^t + v_2^t \cdot w_2,\ B_1 + B_2 = e_1 \cdot e_1^t + v_3^t \cdot w_3.$$

By doing linear combinations of these elements we see immediately that $v_2^t \neq e_1, e_2$ and $v_3^t \neq e_1, e_2$. Moreover,

$$B_1 + B_2 = e_1 \cdot e_1^t + v_3^t \cdot w_3 = e_2 \cdot e_2^t + v_2^t \cdot w_2,$$

and therefore,

$$e_1 \cdot e_1^t + e_2 \cdot e_2^t = v_2^t \cdot w_2 + v_3^t \cdot w_3.$$

We have that $\langle v_2^t, v_3^t \rangle = \langle e_1, e_2 \rangle$ The only possibility is that $v_2^t = v_3^t = e_1 + e_2$, but this is a contradiction since $B_1 = v_2^t \cdot w_2 + v_3^t \cdot w_3$ has rank 2. □

In the next example we show that the condition $m > 2$ in Proposition 4.6 is necessary.

Example 4.7. Consider the 2-dimensional subspace $\mathcal{V} \subseteq \mathbb{F}_2^{2\times 2}$ given by

$$\mathcal{V} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right\}$$

and let $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \notin \mathcal{V}$. Then $\max_{B\in\mathcal{V}}(\mathrm{rank}(A + B)) = 1$.

The next theorem generalizes Proposition 4.6 to any q. In particular we show that if $A \notin \mathcal{V}$, that is if $A + \mathcal{V} \neq \mathcal{V}$, then every $\mathcal{V}$ of $\dim(\mathcal{V}) = mt$ contains a B such that $\mathrm{rank}(A + B) \geq t + 1$.

Theorem 4.8. Let $0 \leq t < n$ and let $\mathcal{V} \subseteq \mathbb{F}_q^{m\times n}$ be an $\mathbb{F}_q$-linear subspace such that $\dim(\mathcal{V}) = mt$. Let $A \in \mathbb{F}_q^{m\times n} \setminus \mathcal{V}$. If either $t \neq 1$ or $m \neq 2$ or $q \neq 2$ or $\mathrm{rank}(A) \neq 1$, then there exists $B \in \mathcal{V}$ such that

$$\mathrm{rank}(A + B) \geq t + 1.$$

Proof. If $t = 0$, then $\mathcal{V} = 0$ and the thesis is readily verified. Suppose that $t \geq 1$ and let $\mathcal{M} = \{M_1, \ldots, M_{mt}\}$ be a basis of $\mathcal{V}$. Up to a change of basis, we may assume without loss of generality that $\phi(M_i) \neq \phi(M_j)$ if $i \neq j$. In particular, $\rho(\mathcal{M}) \geq t$. If $\rho(\mathcal{M}) \geq t + 1$, then we conclude by Theorem 4.4.
Suppose that $\rho(\mathcal{M}) = t$. Up to code equivalence, we may assume that the t lines that cover $\phi(M_i)$ for all i are the first t columns. If $t = 1$ and $\mathrm{rank}(A) \geq 2$, then let $B = 0$. If $t = 1$, $\mathrm{rank}(A) = 1$ and $q \neq 2$ it is trivial, if $q = 2$ we apply Proposition 4.6.
Suppose now that $\rho(\mathcal{M}) = t \geq 2$. For every $t + 1 \leq l \leq n$ and every $k \in [m]$ there exists a linear form $f_{k,l} \in \mathbb{F}_q[x_{i,j} : (i, j) \in [m] \times [t]]$ such that

$$\mathcal{V} = \{(x_{k,l}) \in \mathbb{F}_q^{m\times n} : x_{k,l} = f_{k,l}(x_{i,j}) \text{ for all } k \in [m], l \in [n] \setminus [t]\}.$$

Assume that $\max_{B\in\mathcal{V}}(\mathrm{rank}(A + B)) = t$ for some $A \in \mathbb{F}_q^{m\times n}$. It suffices to show that $A \in \mathcal{V}$. Up to reducing A modulo $\mathcal{V}$, we may assume without loss of generality that $a_{i,j} = 0$ for $(i, j) \in [m] \times [t]$. Fix $(k, l) \in [m] \times [n]$ with $l \geq t + 1$. Let $X = (x_{i,j}) \in \mathcal{V}$. We have that

$$x_{k,l} + a_{k,l} = f_{k,l}(x_{i,j}) + a_{k,l}.$$

Let $L = [t]$ and let S be a subset of $[m] \setminus \{k\}$ of cardinality t. Let $x_{i,j} = 0$ for $i \notin S$ and $j \in L$. For any choice of $(x_{i,j})_{i \in S, j \in L}$ such that $X(S,L) + A(S,L) = X(S,L)$ is invertible, one has

$$0 = x_{k,l} + a_{k,l} = f_{k,l}(x_{i,j}) + a_{k,l}, \tag{19}$$

since every matrix in $(A + \mathcal{V})(S \cup \{k\}, L \cup \{l\})$ has rank smaller than or equal to t. Lemma 4.5 together with (19) implies that $a_{k,l} = 0$. This proves that $A \in \mathcal{V}$. □

Results on vector spaces are a special case of those on cosets. For example, the anticode bound for rank-metric codes in (3) is a direct consequence of Proposition 4.6 and Theorem 4.8. If $A \in \mathcal{V}$, then $A + \mathcal{V} = \mathcal{V}$ and there exist linear spaces $\mathcal{V} \subseteq \mathbb{F}_q^{m \times n}$ such that $\dim(\mathcal{V}) = mt$ and $\operatorname{rank}(A) \leq t$ for all $A \in \mathcal{V}$. These are exactly the optimal anticodes.

4.2 Anticode Bound and Optimal Anticodes

In this section we prove an anticode bound for sum-rank metric codes. Recently in [10, Theorem 2.2] a different anticode bound was given for the sum-rank metric. However, our bound is sharper and the resulting optimal anticodes lead to a definition of generalized weights that satisfy desirable properties, whereas generalized weights based on optimal anticodes as in [10] do not recover the minimum sum-rank distance of the code.

Theorem 4.9 (Anticode bound)**.** Let $\mathcal{C} \subseteq \mathbb{M}$ be an $\mathbb{F}_q$-linear subspace. Then

$$\dim(\mathcal{C}) \leq \max_{C \in \mathcal{C}} \left(\sum_{i=1}^{\ell} m_i \operatorname{rank}(C_i) \right). \tag{20}$$

In particular, if $m_1 = \ldots = m_\ell = m$, then

$$\dim(\mathcal{C}) \leq m \operatorname{maxsrk}(\mathcal{C}).$$

Proof. We proceed by induction on ℓ. If $\ell = 1$, then $\mathcal{C}$ is a rank-metric code, the sum-rank metric coincides with the rank metric, and the statement is the anticode bound in (3).
Let $\ell > 1$ and π be the canonical projection from $\mathbb{M}$ onto $\mathbb{F}_q^{m_1 \times n_1} \times \cdots \times \mathbb{F}_q^{m_{\ell-1} \times n_{\ell-1}}$ and let π_ℓ be the canonical projection from $\mathbb{M}$ onto $\mathbb{F}_q^{m_\ell \times n_\ell}$. Define $\mathcal{A} = \pi(\mathcal{C})$ and $\mathcal{B} = \pi_\ell(\pi^{-1}(0) \cap \mathcal{C})$ and let $\tilde{\mathcal{C}} = \mathcal{A} \times \mathcal{B}$. Since $\dim(\pi^{-1}(0) \cap \mathcal{C}) = \dim(\pi_\ell(\pi^{-1}(0) \cap \mathcal{C})) = \dim(\mathcal{B})$, we have that

$$\dim(\mathcal{C}) = \dim(\mathcal{A}) + \dim(\pi^{-1}(0) \cap \mathcal{C}) = \dim(\tilde{\mathcal{C}}).$$

By the induction hypothesis there is $(C_1, \ldots, C_{\ell-1}) \in \mathcal{A}$ such that

$$\sum_{i=1}^{\ell-1} m_i \operatorname{rank}(C_i) \geq \dim(\mathcal{A}) = \dim(\mathcal{C}) - \dim(\mathcal{B}).$$

Let $C_\ell \in \pi_\ell(\mathcal{C})$ such that $(C_1, \ldots, C_\ell) \in \mathcal{C}$. By Proposition 4.6 and Theorem 4.8 there is a $B \in \mathcal{B}$ such that

$$\operatorname{rank}(C_\ell + B) \geq \left\lceil \frac{\dim(\mathcal{B})}{m_\ell} \right\rceil.$$

Therefore

$$\begin{aligned}\sum_{i=1}^{\ell-1} m_i \operatorname{rank}(C_i) + m_\ell \operatorname{rank}(C_\ell + B) &\geq \dim(\mathcal{C}) - \dim(\mathcal{B}) + m_\ell \left\lceil \frac{\dim(\mathcal{B})}{m_\ell} \right\rceil \\ &\geq \dim(\mathcal{C}).\end{aligned}$$

The element $(C_1, \ldots, C_{\ell-1}, C_\ell + B)$ is in $\mathcal{C}$, since $(C_1, \ldots, C_{\ell-1}, C_\ell) \in \mathcal{C}$ and $B \in \mathcal{B}$. This concludes the proof. □

Optimal sum-rank metric anticodes may now be defined as the codes attaining the anticode bound for sum-rank metric codes.

Definition 4.10. A sum-rank metric code $\mathcal{C} \subseteq \mathbb{M}$ is an optimal anticode if

$$\dim(\mathcal{C}) = \max_{C \in \mathcal{C}} \left(\sum_{i=1}^{\ell} m_i \operatorname{rank}(C_i) \right).$$

Remark 4.11. In [10], the authors give a definition of r-anticode for r a non-negative integer. In [10, Theorem 2.2] they establish an upper bound for the dimension of an r-anticode. For a given $\mathcal{C} \subseteq \mathbb{M}$ and $r = \operatorname{maxsrk}(\mathcal{C})$, [10, Theorem 2.2] yields

$$\dim(\mathcal{C}) \leq \max \left\{ \sum_{i=1}^{\ell} m_i u_i : \sum_{i=1}^{\ell} u_i = \operatorname{maxsrk}(\mathcal{C}), u_i \leq n_i \text{ for all } i \right\}. \tag{21}$$

Notice that our anticode bound is tighter than (21), since for all $C = (C_1, \ldots, C_\ell) \in \mathcal{C}$ there exist $u_1, \ldots, u_\ell \in \mathbb{Z}$ such that $\sum_{i=1}^{\ell} u_i = \operatorname{maxsrk}(\mathcal{C})$ and $\operatorname{rank}(C_i) \leq u_i \leq n_i$ for all i. In particular, all codes that meet bound (21) also meet our anticode bound. Moreover the bounds are different, as one can easily check by comparing Theorem 4.20 in this paper and [10, Corollary 3.8]. In [10, Definition 2.3], the authors define optimal anticodes as those that meet the bound (21). In particular, an optimal anticode according to [10] is an optimal anticode according to Definition 4.10, but the converse is not true in general.

To clarify the evidence we give an example of the difference between our definition of optimal anticodes and the one given in [10, Definition 2.3]. In particular note that optimal anticodes as given in [10, Definition 2.3] are products of copies of the whole space and of the zero space if $r \geq n_1$.

Example 4.12. Consider $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^{2\times 2} \times \mathbb{F}_q$ given by

$$\mathcal{C}_1 = \left\{ \left(\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}, c \right) : (a, b, c) \in \mathbb{F}_q^3 \right\}$$

and

$$\mathcal{C}_2 = \mathbb{F}_q^{2\times 2} \times 0.$$

It is easy to check that both $\mathcal{C}_1$ and $\mathcal{C}_2$ attain our anticode bound in (20), whereas $\mathcal{C}_1$ is not an optimal anticode in the sense of the bound in (21).

A simple computation allows one to show that if $\mathcal{C}_i \subseteq \mathbb{F}_q^{m_i\times n_i}$ is an optimal anticode with respect to the rank metric for $i \in [\ell]$, then $\mathcal{C}_1 \times \cdots \times \mathcal{C}_\ell \subseteq \mathbb{M}$ is an optimal anticode with respect to the sum-rank metric. Moreover, one has the following.

Proposition 4.13. Let $\mathcal{C} \subseteq \mathbb{M}$ be an optimal anticode and assume that $m_1 = \ldots = m_\ell = m$. For $i \in [\ell]$ let $\pi_i : \mathbb{M} \to \mathbb{F}_q^{m_i\times n_i}$ be the canonical projection. The following are equivalent:

1. $\mathcal{C} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_\ell$ and $\mathcal{C}_i$ is an optimal rank-metric anticode for $i \in [\ell]$.
2. $\operatorname{maxsrk}(\mathcal{C}) = \sum_{i=1}^{\ell} \operatorname{maxrk}(\pi_i(\mathcal{C}))$.

Proof. (1) $\implies$ (2) follows from a simple computation.
(2) $\implies$ (1) Clearly, $\mathcal{C} \subseteq \prod_{i=1}^{\ell} \pi_i(\mathcal{C})$, so

$$m \operatorname{maxsrk}(\mathcal{C}) = \dim(\mathcal{C}) \leq \sum_{i=1}^{\ell} \dim(\pi_i(\mathcal{C})) \leq \sum_{i=1}^{\ell} m \operatorname{maxrk}(\pi_i(\mathcal{C})).$$

Since $\operatorname{maxsrk}(\mathcal{C}) = \sum_{i=1}^{\ell} \operatorname{maxrk}(\pi_i(\mathcal{C}))$, we have that

$$\dim(\mathcal{C}) = \dim\left(\prod_{i=1}^{\ell} \pi_i(\mathcal{C})\right) \text{ and } \dim(\pi_i(C)) = m \operatorname{maxrk}(\pi_i(\mathcal{C})).$$

Therefore $\mathcal{C} = \prod_{i=1}^{\ell} \pi_i(\mathcal{C})$ and $\mathcal{C}_i$ is an optimal rank-metric anticode for all $i \in [\ell]$. □

We will prove that optimal anticodes in the sum-rank metric are generated by their elements of maximum sum rank. We start by proving the result in the special case of rank-metric anticodes.

Lemma 4.14. Let $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ be an optimal anticode. Then $\mathcal{C}$ is generated by its elements of maximum rank.

Proof. Let $t = \operatorname{maxrk}(\mathcal{C})$, then $\dim(\mathcal{C}) = mt$. Up to code equivalence we may assume that $\mathcal{C}$ consists of all matrices whose rowspace is contained in $\langle e_1, \ldots, e_t\rangle^t$. Therefore it suffices to prove the statement for $\mathcal{C} = \mathbb{F}_q^{m\times t}$. Let $\{E_{i,j}\}_{(i,j)\in[m]\times[t]}$ be the standard basis of $\mathbb{F}_q^{m\times t}$. Let $I = \sum_{i=1}^{t} E_{i,i} \in \mathbb{F}_q^{m\times t}$. For each $(i,j) \in [m] \times [t]$ there exists a permutation matrix $S_{i,j} \in \mathbb{F}_q^{m\times m}$ such that $(S_{i,j}I)_{i,j} = 0$. Therefore one can write $E_{i,j} = (S_{i,j}I + E_{i,j}) - S_{i,j}I$, with $\operatorname{rank}(S_{i,j}I) = \operatorname{rank}(S_{i,j}I + E_{i,j}) = t$. This implies that $\{S_{i,j}I + E_{i,j}, S_{i,j}I\}_{(i,j)\in[m]\times[t]}$ is a set of matrices of rank t which generates $\mathbb{F}_q^{m\times t}$. □

The next observations will be useful in order to extend the result of Lemma 4.14 to optimal anticodes in the sum-rank metric.

Lemma 4.15. Let $m \geq 2$ and let $\mathcal{C} \subseteq \mathbb{F}_2^{m\times n}$ be an optimal rank-metric anticode of $\operatorname{maxrk}(\mathcal{C}) = t$. Then every element of $\mathcal{C}$ of rank t can be written as the sum of two elements of $\mathcal{C}$ of rank t.

Proof. Up to code equivalence we may assume that $\mathcal{C}$ consists of all matrices whose rowspace is contained in $\langle e_1, \dots, e_t\rangle^t$. Therefore, it suffices to show that every element of full rank in $\mathbb{F}_2^{m\times t}$ can be written as the sum of two elements of $\mathbb{F}_2^{m\times t}$ of full rank. Let $C = (c_1, \dots, c_t)$ be the matrix whose columns are $c_1, \dots, c_t \in \mathbb{F}_2^m$. Assume that $\operatorname{rank}(C) = t$. If $t = 1$, let $\tilde{C} \in \mathcal{C} \setminus \{C, 0\}$. Notice that $\tilde{C}$ exists, since $m \geq 2$. Then $\tilde{C}, C + \tilde{C}$ are elements of rank 1 and $C = \tilde{C} + (C + \tilde{C})$. If t is even, then $C = C_1 + C_2$ where

$$\begin{aligned} C_1 &= (c_1 + c_2, c_1, c_3 + c_4, c_3, \dots, c_{t-1} + c_t, c_{t-1}),\\ C_2 &= (c_2, c_1 + c_2, c_4, c_3 + c_4, \dots, c_t, c_{t-1} + c_t). \end{aligned}$$

If $t \neq 1$ is odd, then $C = C_1 + C_2$ where

$$\begin{aligned} C_1 &= (c_1 + c_2, c_3, c_1, c_4 + c_5, c_4, \dots, c_{t-1} + c_t, c_{t-1}),\\ C_2 &= (c_2, c_3 + c_2, c_1 + c_3, c_5, c_4 + c_5, \dots, c_t, c_{t-1} + c_t). \end{aligned}$$

Since C_1 and C_2 have the same column space as C, they are in $\mathcal{C}$ and they have full rank. □

Theorem 4.16. Let $\mathcal{C} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_\ell \subseteq \mathbb{M}$ be a code. Let $\mathcal{C}_i$ be an optimal anticode for all $i \in [\ell]$. If either $m_{\ell-1} \geq 2$ or $q \neq 2$, then $\mathcal{C}$ is generated by its elements of maximum sum-rank.

Proof. Let $C = (C_1, \dots, C_\ell) \in \mathcal{C}$ be such that

$$\sum_{i=1}^{\ell} m_i \operatorname{rank}(C_i) = \max_{D\in\mathcal{C}} \left(\sum_{i=1}^{\ell} m_i \operatorname{rank}(D_i) \right).$$

Since $\mathcal{C}$ is a product, C_i is an element of maximum rank in $\mathcal{C}_i$ for all $i \in [\ell]$. If $q \neq 2$, let $\alpha \in \mathbb{F}_q \setminus \{0, 1\}$. Then

$$(0, \dots, 0, C_i, 0, \dots, 0) \in \langle (C_1, \dots, C_\ell), (C_1, \dots, C_{i-1}, \alpha C_i, C_{i+1}, \dots, C_\ell)\rangle.$$

Therefore $\mathcal{C}$ is generated by its element of maximum sum-rank, since each $\mathcal{C}_i$ is generated by its elements of maximum rank by Lemma 4.14.
If $q = 2$ and $i \neq \ell$, then by Lemma 4.15 there exist $C_i', C_i'' \in \mathcal{C}_i$ of maximum rank such that $C_i = C_i' + C_i''$. Let $C' = (C_1, \dots, C_{i-1}, C_i', C_{i+1}, \dots, C_\ell)$ and $C'' = (C_1, \dots, C_{i-1}, C_i'', C_{i+1}, \dots, C_\ell)$. Then

$$(0, \dots, 0, C_i, 0, \dots, 0) \in \langle C', C''\rangle.$$

Since C and $(0, \dots, 0, C_i, 0, \dots, 0)$ for $i \in [\ell - 1]$, belong to the subcode of $\mathcal{C}$ generated by its codewords of maximum sum-rank, then also $(0, \dots, 0, C_\ell)$ does. Therefore $\mathcal{C}$ is generated by its element of maximum sum-rank. □

Example 4.17. For $\ell \geq 2$ and $m_{\ell-1} = 1$, the code $\mathcal{C} = 0 \times \ldots \times 0 \times \mathbb{F}_2 \times \mathbb{F}_2$ is an optimal anticode, which is not generated by its unique element $(0, \ldots, 0, 1, 1)$ of maximum sum-rank.

The next result on generating sets of optimal binary anticodes in the Hamming metric will also be useful.

Lemma 4.18. Let $\mathcal{C} \subseteq \mathbb{F}_2^\ell$ be an optimal anticode of $\dim(\mathcal{C}) = t$. Then $\mathcal{C}$ is generated by its elements of weight t and $t-1$.

Proof. Let G be a generator matrix of $\mathcal{C}$ and assume that G is in reduced row echelon form. Denote by $g_1, \ldots, g_t$ the rows of G. Let $v = g_1 + \ldots + g_t$. Then the vectors $v, v + g_1, \ldots, v + g_t$ have weight $t-1$ or t and are a system of generators of $\mathcal{C}$, since $g_i = v + (v + g_i)$ for all i. □

From here on, let π be the canonical projection from $\mathbb{M}$ onto $\mathbb{F}_q^{m_2 \times n_2} \times \cdots \times \mathbb{F}_q^{m_\ell \times n_\ell}$ and let π_i be the canonical projection from $\mathbb{M}$ onto $\mathbb{F}_q^{m_i \times n_i}$. The following technical lemma will be used in the proof of Theorem 4.20.

Lemma 4.19. Let $\mathcal{C} \subseteq \mathbb{M}, \mathcal{A} = \pi(\mathcal{C}), \mathcal{B} = \pi_1(\pi^{-1}(0) \cap \mathcal{C})$ and $k = \max\{i \in [\ell] : m_i > 1\}$. Further, let $q = 2, \ell \geq 2$ and $m_1 = n_1 = 2$. If $\dim(\mathcal{B}) = 2$ and $\mathcal{A} = \prod_{i=2}^k \mathcal{C}_i \times \mathcal{C}'$ for optimal anticodes $\mathcal{C}_i \subseteq \mathbb{F}_q^{m_i \times n_i}$ for all $i \in [k] \setminus \{1\}$ and an optimal anticode $\mathcal{C}' \subseteq \mathbb{F}_q^{\ell-k}$, then one of the followings holds:

(i) $\mathcal{B}$ is an optimal anticode.

(ii) There is $B \in \mathcal{B}$ and $C = (C_1, \ldots, C_\ell) \in \mathcal{C}$ with $\sum_{i=2}^\ell m_i \operatorname{rank}(C_i) \geq \sum_{i=2}^\ell m_i \operatorname{maxrk}(\mathcal{C}_i) - 1$, such that

$$\operatorname{rank}(B + C_1) = 2.$$

Proof. If $\operatorname{maxrk}(\mathcal{B}) = 1$, then $\mathcal{B}$ is an optimal anticode and we conclude immediately. Hence $\operatorname{maxrk}(\mathcal{B}) = 2$. If $\ell - k \leq 2$ consider $(D_2, \ldots, D_k), (E_2, \ldots, E_k) \in \mathcal{A}$ with maximal rank in each component, such that their sum also has maximal rank in each component. Let $D_1, E_1 \in \mathcal{C}_1$ and $v, w \in \mathcal{C}'$ be such that $(D_1, \ldots, D_k, v)$, $(E_1, \ldots, E_k, w) \in \mathcal{C}$. If $\ell - k = 1$ we take $v = 1$ and $w = 0$, then $(D_2 + E_2, \ldots, D_k + E_k, 1)$ has maximal rank in each component. If $\ell - k = 2$ we take $v = (1, 0)$ and $w = (0, 1)$, then $(D_2 + E_2, \ldots, D_k + E_k, 1, 1)$ has maximal rank in each component. In this way we have found elements satisfying the condition in (ii).
If there is a rank 0 element among D_1, E_1 and $D_1 + E_1$ then we conclude by taking B of rank 2. If there is a rank 2 element among D_1, E_1 and $D_1 + E_1$ then we conclude by taking $B = 0$. If $D_1, E_1, D_1 + E_1$ all have rank 1, then either $\langle D_1, E_1 \rangle \cap \mathcal{B} \neq 0$, or

$$|(D_1 + \mathcal{B}) \cup (E_1 + \mathcal{B}) \cup (D_1 + E_1 + \mathcal{B})| = 3 \cdot |\mathcal{B}| = 12,$$

but in $\mathbb{F}_2^{2\times 2}$ we have only 9 elements of rank 1.
Let $\ell - k > 2$. Let G be a generator matrix of $\mathcal{C}'$ and assume that G is in reduced row echelon form and that $\dim(\mathcal{C}') = t$. Let $g_1, \ldots, g_t, v$ be given as in Lemma 4.18.

For every $i \in [t]$, there exists $G_1^i \in \mathbb{F}_2^{2\times 2}$ such that $G^i = (G_1^i, 0, \ldots, 0, g_i) \in \mathcal{C}$. If for every $i \in [t]$, $G_1^i \in \mathcal{B}$, then we proceed as in the case $l - k \leq 2$. Therefore, without loss of generality, assume that $G_1^1 \notin \mathcal{B}$. Let $C = (C_1, 0, \ldots, 0, v) = \sum_{i=1}^t G^i$ and $D = (D_1, D_2, \ldots, D_k, 0, \ldots, 0)$ such that D_i has maximum rank in $\mathcal{C}_i$ for every $i \in [k] \setminus \{1\}$. Note that $D + C$ and $D + C + G^1$ satisfy the condition in (ii). If $D_1 + C_1$,$D_1 + C_1 + G_1^1 \notin \mathcal{B}$, then since $G_1^1 \notin \mathcal{B}$, we have that

$$(D_1 + C_1 + G_1^1 + \mathcal{B}) \cap (D_1 + C_1 + \mathcal{B}) = \emptyset,$$

and

$$((D_1 + C_1 + G_1^1 + \mathcal{B}) \cup (D_1 + C_1 + \mathcal{B})) \cap \langle G_1^1, \mathcal{B}\rangle = \emptyset.$$

Hence

$$|(D_1 + C_1 + G_1^1 + \mathcal{B}) \cup (D_1 + C_1 + \mathcal{B}) \cup \langle G_1^1, \mathcal{B}\rangle| = 3 \cdot |\mathcal{B}| = 12,$$

and again we observe that there are 9 elements of rank 1 in $\mathbb{F}_2^{2\times 2}$. Therefore, since in $\langle G_1^1, \mathcal{B}\rangle$ there are at least two elements of rank 1, in $(D_1 + C_1 + G_1^1 + \mathcal{B}) \cup (D_1 + C_1 + \mathcal{B})$ there must be at least an element of rank 2. □

In the next theorem we show that the optimal anticodes in the sum-rank metric are products of optimal anticodes in the rank metric and an optimal anticode in the Hamming metric.

Theorem 4.20. Let $k = \max\{i \in [\ell] : m_i > 1\}$. A code $\mathcal{C} \subseteq \mathbb{M}$ is an optimal anticode if and only if there is an optimal anticode $\mathcal{C}' \subseteq \mathbb{F}_q^{\ell-k}$ and optimal anticodes $\mathcal{C}_i \subseteq \mathbb{F}_q^{m_i\times n_i}$ for all $i \in [k]$ such that $\mathcal{C} = \prod_{i=1}^k \mathcal{C}_i \times \mathcal{C}'$.

Proof. Assume that $\mathcal{C}' \subseteq \mathbb{F}_q^{\ell-k}$ is an optimal Hamming-metric anticode and $\mathcal{C}_i \subseteq \mathbb{F}_q^{m_i\times n_i}$ are optimal rank-metric anticodes for $i \in [k]$. It is straightforward to prove that $\mathcal{C} = \prod_{i=1}^k \mathcal{C}_i \times \mathcal{C}' \subseteq \mathbb{M}$ is an optimal anticode. Further, the statement of the theorem holds for $m_1 = \ldots = m_\ell = 1$. Therefore, we may assume that $m_1 > 1$, hence also $k \geq 1$. We proceed by induction on ℓ. For $\ell = 1$, the theorem holds trivially.
We suppose that the theorem holds for $\ell - 1$ and we prove it for $\ell > 1$. Let $\mathcal{A} = \pi(\mathcal{C})$, $\mathcal{B} = \pi_1(\pi^{-1}(0) \cap \mathcal{C})$, and $\tilde{\mathcal{C}} = \mathcal{B} \times \mathcal{A}$. As in the proof of Theorem 4.9, we have

$$\dim(\mathcal{C}) = \dim(\mathcal{B}) + \dim(\mathcal{A}) \leq m_1 \operatorname{rank}(C_1) + \sum_{i=2}^{\ell} m_i \operatorname{rank}(C_i), \tag{22}$$

where $(C_1, \ldots, C_\ell) \in \mathcal{C}$, $(C_2, \ldots, C_\ell)$ maximizes $\sum_{i=2}^{\ell} m_i \operatorname{rank}(C_i)$ on $\mathcal{A}$, and $m_1 \operatorname{rank}(C_1) \geq \dim(\mathcal{B})$. Since $(C_1, C_2, \ldots, C_\ell) \in \mathcal{C}$ and $\mathcal{C}$ is an optimal anticode, (22) is an equality. In particular,

$$m_1 \operatorname{rank}(C_1) = \dim(\mathcal{B}) \quad \text{and} \quad \sum_{i=2}^{\ell} m_i \operatorname{rank}(C_i) = \dim(\mathcal{A}). \tag{23}$$

This proves that $\mathcal{A}$ is an optimal anticode. Therefore, by the induction hypothesis, there is an optimal anticode $\mathcal{C}' \subseteq \mathbb{F}_q^{\ell-k}$ and optimal anticodes $\mathcal{C}_i \subseteq \mathbb{F}_q^{m_i\times n_i}$ for $2 \leq i \leq k$ such that $\mathcal{A} = \prod_{i=2}^k \mathcal{C}_i \times \mathcal{C}'$.

We claim that $C_1 \in \mathcal{B}$. In fact, if $C_1 \notin \mathcal{B}$ and either $\dim(\mathcal{B}) \neq 2$ or $m \neq 2$ or $q \neq 2$ or $n \neq 2$ or $\operatorname{rank}(C_1) \neq 1$, then by Theorem 4.8 there exists $B \in \mathcal{B}$ such that

$$\operatorname{rank}(C_1 + B) > \dim(\mathcal{B})/m_1 = \operatorname{rank}(C_1 + B).$$

Since $B \in \mathcal{B}$, then $(C_1 + B, C_2, \ldots, C_\ell) \in \mathcal{C}$. However, this contradicts the optimality of $\mathcal{C}$, since $m_1 \operatorname{rank}(C_1 + B) + \sum_{i=2}^{\ell} m_i \operatorname{rank}(C_i) > \sum_{i=1}^{\ell} m_i \operatorname{rank}(C_i) = \dim(\mathcal{C})$. Since $C_1 \in \mathcal{B}$, then $C_1 + B \in \mathcal{B}$, hence $\mathcal{B}$ is an optimal anticode by (23). If $\dim(\mathcal{B}) = 2$, $m = n = 2$, $q = 2$, $\operatorname{rank}(C_1) = 1$ by Lemma 4.19, if $\mathcal{B}$ is not an optimal anticode, then there exists $B \in \mathcal{B}$ and $\bar{C} = (\bar{C}_1, \ldots, \bar{C}_\ell)$ such that

$$m_1 \operatorname{rank}(\bar{C}_1 + B) + \sum_{i=2}^{\ell} m_i \operatorname{rank}(\bar{C}_i) \geq 4 + \dim(\mathcal{A}) - 1 \geq \dim(\mathcal{C}) + 1.$$

This is a contradiction, since $\mathcal{C}$ is an optimal anticode. We conclude that also in this case $\mathcal{B}$ is an optimal anticode.
In order to conclude the proof, it suffices to show that $\mathcal{C} = \mathcal{B} \times \mathcal{A}$. Since $\mathcal{C} \supseteq \mathcal{B} \times 0$, it suffices to show that $\mathcal{C} \supseteq 0 \times \mathcal{A}$. If either $k \geq \ell - 1$ or $q \neq 2$, then $0 \times \mathcal{A}$ is generated by its element of maximum sum-rank by Theorem 4.16. Since these belong to $\mathcal{C}$, we have that $0 \times \mathcal{A} \subseteq \mathcal{C}$. Therefore, assume that $k \leq \ell - 2$ and $q = 2$. Let $2 \leq i \leq k$. By Lemma 4.15, if $C_i \in \mathcal{C}_i$ is an element of maximum rank, then $C_i = D_i + D_i'$ for some $D_i, D_i' \in \mathcal{C}_i$ of maximum rank. Hence

$$(0, \ldots, 0, C_i, 0, \ldots, 0) = (0, D_2, \ldots, D_k, D) + (0, D_2', \ldots, D_k', D)$$

where $D_j = D_j' \in \mathcal{C}_j$ is an element of maximum rank for any $j \in \{2, \ldots, k\} \setminus \{i\}$ and D is an element of maximum rank of $\mathcal{C}'$. Since $(0, D_2, \ldots, D_k, D)$, $(0, D_2', \ldots, D_k', D)$ are elements of maximum sum-rank in $0 \times \mathcal{A}$, they belong to $\mathcal{C}$. This proves that, for any $2 \leq i \leq k$, if C_i has maximum rank among the elements of $\mathcal{C}_i$, then

$$(0, \ldots, 0, C_i, 0, \ldots, 0) \in \mathcal{C}. \tag{24}$$

Since $\mathcal{C}_i$ is generated by its elements of maximum rank by Lemma 4.14, then

$$0 \times \ldots \times 0 \times \mathcal{C}_i \times 0 \times \ldots \times 0 \subseteq \mathcal{C}$$

for all $2 \leq i \leq k$.
In addition, it follows from (24) that $(0, \ldots, 0, D) \in \mathcal{C}$ for any $D \in \mathcal{C}'$ of maximum Hamming weight. We claim that $0 \times \ldots \times 0 \times \mathcal{C}' \subseteq \mathcal{C}$. Let t be the maximum weight of a codeword in $\mathcal{C}'$ and let $D' \in \mathcal{C}'$ be an element of weight $t - 1$. By Lemma 4.18 it suffices to show that $(0, \ldots, 0, D') \in \mathcal{C}$. Let $(D_2, \ldots, D_k, D') \in \mathcal{A}$ with $\operatorname{rank}(D_i) = \operatorname{maxrk}(\mathcal{C}_i)$ for $2 \leq i \leq k$. Let D_1 be such that $(D_1, D_2, \ldots, D_k, D') \in \mathcal{C}$. Since $0 \times \mathcal{C}_2 \times \ldots \times \mathcal{C}_k \times 0 \subseteq \mathcal{C}$, then $(D_1, 0, \ldots, 0, D') \in \mathcal{C}$. If $D_1 \in \mathcal{B}$ the claim follows, since $(D_1, 0, \ldots, 0) \in \mathcal{B} \times 0 \subseteq \mathcal{C}$. If $D_1 \notin \mathcal{B}$, then by Theorem 4.8 there exists $B \in \mathcal{B}$ such that $\operatorname{rank}(B + D_1) \geq \operatorname{maxrk}(\mathcal{B}) + 1$. Then the element $(B + D_1, D_2, \ldots, D_k, D') \in \mathcal{C}$

has sum rank

$$m_1 \operatorname{rank}(B + D_1) + \sum_{j=2}^{k} m_j \operatorname{rank}(D_j) + \operatorname{wt}(D') \geq$$
$$m_1(\operatorname{maxrk}(\mathcal{B}) + 1) + \sum_{j=2}^{k} m_j \operatorname{maxrk}(\mathcal{C}_j) + t - 1 =$$
$$\dim(\mathcal{C}) + m_1 - 1 > \dim(\mathcal{C}),$$

where $\operatorname{wt}(D')$ denotes the Hamming weight of D', and the inequality follows from the assumption that $m_1 > 1$. This contradicts the assumption that $\mathcal{C}$ is an optimal anticode, completing the proof of the claim and of the theorem. □

The next result is an easy consequence of Theorem 4.20.

Corollary 4.21. Assume that either $q \neq 2$ or $m_{\ell-2} \geq 2$. An $\mathbb{F}_q$-linear space $\mathcal{C} \subseteq \mathbb{M}$ is an optimal anticode if and only if for all $i \in [\ell]$ there is $\mathcal{C}_i \subseteq \mathbb{F}_q^{m_i \times n_i}$ optimal anticode such that $\mathcal{C} = \prod_{i=1}^{\ell} \mathcal{C}_i$.

Proof. By Theorem 4.20 $\mathcal{C} = \prod_{i=1}^{k} \mathcal{C}_i \times \mathcal{C}'$, where $\mathcal{C}' \subseteq \mathbb{F}_q^{\ell-k}$ is an optimal anticode, $k = \max\{i \in [\ell] \mid m_i > 1\}$, and $\mathcal{C}_i \subseteq \mathbb{F}_q^{m_i \times n_i}$ are optimal anticodes for all $i \in [k]$. If $q \neq 2$, then $\mathcal{C}'$ is a product of zeroes and copies of $\mathbb{F}_q$ by [61, Proposition 9]. If $q = 2$ and $\ell - k \leq 2$, the same is true by direct inspection. □

We conclude this section with a proof that the dual of an optimal anticode in the sum-rank metric is an optimal anticode, if $q \neq 2$ or $m_{\ell-2} \geq 2$.

Proposition 4.22. Let $q \neq 2$ or $m_{\ell-2} \geq 2$. Then $\mathcal{A} \subseteq \mathbb{M}$ is an optimal anticode if and only if $\mathcal{A}^{\perp} \subseteq \mathbb{M}$ is an optimal anticode.

Proof. The dual of an optimal anticode in the rank-metric is an optimal anticode by [62, Theorem 54]. The result now follows from Corollary 4.21, after observing that the dual of a product is the product of the duals. □

Notice that Proposition 4.22 cannot be extended to the case $q = 2$ and $m_{\ell-2} = 1$, since for $n \geq 3$ there exist optimal anticodes in $\mathbb{F}_2^n$ whose dual is not an optimal anticode.

Example 4.23. Let $n \geq 3$ be odd and let $\mathcal{C} \subseteq \mathbb{F}_2^n$ be the even-weight code. Then $\mathcal{C}$ is an optimal anticode and its dual $\mathcal{C}^{\perp}$ is the repetition code, which is not an optimal anticode.

4.3 Isometries

In this section we characterize the linear isometries of $\mathbb{M}$ and use them to define a notion of equivalence between sum-rank metric codes. In the next section we define and study generalized weights and show that they are equivalence invariants. With our notion of equivalence, we also obtain that an optimal anticode is equivalent to a product of standard optimal anticodes in the rank metric.

Definition 4.24. An $\mathbb{F}_q$**-linear isometry** φ in the sum-rank metric is an $\mathbb{F}_q$-linear homomorphism of $\mathbb{M}$ such that $\operatorname{srank}(\varphi(C)) = \operatorname{srank}(C)$ for all $C \in \mathbb{M}$. Two sum-rank metric codes $\mathcal{C}, \mathcal{D} \subseteq \mathbb{M}$ are **equivalent** if there is an $\mathbb{F}_q$-linear isometry $\varphi : \mathbb{M} \to \mathbb{M}$ such that $\varphi(\mathcal{C}) = \mathcal{D}$.

Recall that every $\mathbb{F}_q$-linear isometry in the rank metric $\psi : \mathbb{F}_q^{m\times n} \to \mathbb{F}_q^{m\times n}$ has the form $\psi(A) = MAN$, or $\psi(A) = MA^tN$ if $m = n$, for some $M \in \mathrm{GL}_m(\mathbb{F}_q)$ and $N \in \mathrm{GL}_n(\mathbb{F}_q)$ as given in Theorem 1.4. This allows us to characterize the $\mathbb{F}_q$-linear isometries in the sum-rank metric as follows.

Theorem 4.25. Let $\varphi : \mathbb{M} \longrightarrow \mathbb{M}$ be an $\mathbb{F}_q$-linear isometry. Then there is a permutation

$$\sigma : [\ell] \longrightarrow [\ell]$$

with the property that $\sigma(i) = j$ implies $m_i = m_j$ and $n_i = n_j$ and there are rank-metric $\mathbb{F}_q$-linear isometries $\psi_i : \mathbb{F}_q^{m_i\times n_i} \longrightarrow \mathbb{F}_q^{m_i\times n_i}$ for $i \in [\ell]$ such that

$$\varphi(C_1, \ldots, C_\ell) = (\psi_1(C_{\sigma(1)}), \ldots, \psi_\ell(C_{\sigma(\ell)}))$$

for all $(C_1, \ldots, C_\ell) \in \mathbb{M}$.

Proof. For $i \in [\ell]$, let $M_i = 0 \times \ldots \times 0 \times \mathbb{F}_q^{m_i\times n_i} \times 0 \times \ldots \times 0 \subseteq \mathbb{M}$ where the ith component is the only nonzero one. Let $\{(0, \ldots, 0, E_{k,l}, 0, \ldots, 0)\}_{(k,l)\in[m_i]\times[n_i]}$ be the standard basis of M_i. Then

$$\operatorname{srank}(\varphi(0, \ldots, 0, E_{k,l}, 0, \ldots, 0)) = 1$$

for all $(k, l) \in [m_i] \times [n_i]$, implying that $\varphi(0, \ldots, 0, E_{k,l}, 0, \ldots, 0)$ has only one nonzero component for each choice of k and l, say $i_{k,l}$. Further, we notice that for a given $k \in [m_i]$

$$\operatorname{srank}\left(\varphi\left(0, \ldots, 0, \sum_{l=1}^{n_i} E_{k,l}, 0, \ldots, 0\right)\right) = 1, \tag{25}$$

and similarly for a given $l \in [n_i]$ we have that

$$\operatorname{srank}\left(\varphi\left(0, \ldots, 0, \sum_{k=1}^{m_i} E_{k,l}, 0, \ldots, 0\right)\right) = 1. \tag{26}$$

By (25) we have that

$$\operatorname{srank}\left(\sum_{l=1}^{n_i} \varphi(0, \ldots, 0, E_{k,l}, 0, \ldots, 0)\right) = 1,$$

implying that $i_{k,l}$ does not depend on k. The same argument together with equation (26) shows that $i_{k,l}$ does not depend on l either. It follows that for all i there is a j such that $\varphi(M_i) \subseteq M_j$. Since φ^{-1} is a linear isometry and $M_i \subseteq \varphi^{-1}(M_j) \subseteq M_{j'}$ for some j', it follows that $i = j'$ and $M_i = \varphi^{-1}(M_j)$, i.e. $\varphi(M_i) = M_j$. In particular, the map that sends i to j is a permutation of $[\ell]$, which we denote by σ^{-1}. Note that M_i

and M_j have the same weight distribution if and only if $m_i = m_j$ and $n_i = n_j$. To see this just note that φ is a surjective map.
Therefore

$$\begin{array}{rccc} \varphi\,|_{M_i} & : & M_i & \longrightarrow & M_j \\ & & (0,\dots,0,C_i,0,\dots,0) & \longmapsto & (0,\dots,0,\psi_j(C_i),0,\dots,0) \end{array}$$

for $j = \sigma^{-1}(i)$ and for some linear rank-metric isometry $\psi_j : \mathbb{F}_q^{m_j \times n_j} \to \mathbb{F}_q^{m_j \times n_j}$. Hence by linearity

$$\begin{array}{rccc} \varphi & : & \mathbb{M} & \longrightarrow & \mathbb{M} \\ & & (C_1,\dots,C_\ell) & \longmapsto & (\psi_1(C_{\sigma(1)}),\dots,\psi_\ell(C_{\sigma(\ell)})). \end{array}$$

□

The next corollary is immediate, after observing that every optimal anticode in the rank metric is equivalent to a standard optimal anticode, see e.g. [30, Section 3].

Corollary 4.26. For $i \in [\ell]$ let $\mathcal{A}_i \subseteq \mathbb{F}_q^{m_i \times n_i}$ be an optimal anticode and let $\mathcal{A} = \mathcal{A}_1 \times \cdots \times \mathcal{A}_\ell \subseteq \mathbb{M}$. Then $\mathcal{A}$ is equivalent to

$$\prod_{i=1}^{\ell} \langle E_{k,l} \mid k \in [m_i], l \in [u_i] \rangle,$$

where $u_i = \operatorname{maxrk}(\mathcal{A}_i)$.

It is natural to ask whether a result along the lines of the MacWilliams Extension Theorem holds in the sum-rank metric. It is clear that, since we do not have a MacWilliams Extension Theorem for rank-metric codes, we also cannot have a MacWilliams Extension Theorem for sum-rank metric codes. Moreover, in the sum-rank metric we have more pathologies than just those coming from the rank metric, as the next examples show.

Example 4.27. Let $\ell = 3$, $m_1 = n_1 = 3, m_2 = m_3 = n_2 = n_3 = 1$. Let

$$\mathcal{C} = \left\{ \left(\begin{pmatrix} a & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, b, c \right) : a, b, c \in \mathbb{F}_q \right\}$$

and

$$\mathcal{D} = \left\{ \left(\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}, 0, 0 \right) : a, b, c \in \mathbb{F}_q \right\}.$$

Then $\varphi : \mathcal{C} \to \mathcal{D}$ defined as

$$\varphi\left(\begin{pmatrix} a & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, b, c \right) = \left(\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}, 0, 0 \right)$$

is an $\mathbb{F}_q$-linear isometry between $\mathcal{C}$ and $\mathcal{D}$, which does not extend to an $\mathbb{F}_q$-linear isometry of $\mathbb{M}$ by Theorem 4.25.

Example 4.28. Let $\ell = 2$, $m_1 = n_1 = m_2 = n_2 = 2$. Let

$$\mathcal{C} = \left\{ \left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \right) : a, b, c, d \in \mathbb{F}_q \right\}.$$

Then $\varphi : \mathcal{C} \to \mathcal{C}$ defined as

$$\varphi\left(\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \right) \right) = \left(\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}, \begin{pmatrix} b & 0 \\ 0 & d \end{pmatrix} \right)$$

is an $\mathbb{F}_q$-linear isometry between $\mathcal{C}$ and itself, which does not extend to an $\mathbb{F}_q$-linear isometry of $\mathbb{M}$ by Theorem 4.25.

4.4 Generalized Weights

In this section we define generalized weights in the sum-rank metric and establish some of their basic properties, including a weak monotonicity along the lines of the corresponding result for rank-metric codes. In addition, we prove that they satisfy Wei's Duality if $m_1 = \ldots = m_\ell$. For general m_i's, we show by means of an example that the generalized weights of a code do not determine those of its dual, hence Wei's Duality cannot hold.

Definition 4.29. Let $\mathcal{C} \subseteq \mathbb{M}$ be a sum-rank metric code. For each $r \in [\dim(\mathcal{C})]$, we define the r-th generalized sum-rank weight of $\mathcal{C}$ as

$$d_r(\mathcal{C}) = \min\{\operatorname{maxsrk}(\mathcal{A}) : \mathcal{A} = \mathcal{A}_1 \times \cdots \times \mathcal{A}_\ell \text{ where } \mathcal{A}_i \subseteq \mathbb{F}_q^{m_i \times n_i} \text{ are optimal anticodes and } \dim(\mathcal{C} \cap \mathcal{A}) \geq r\}.$$

Notice that if $m_1 = \cdots = m_\ell = m$, then

$$d_r(\mathcal{C}) = \frac{1}{m} \min\{\dim(\mathcal{A}) : \mathcal{A} = \mathcal{A}_1 \times \cdots \times \mathcal{A}_\ell \text{ where } \mathcal{A}_i \subseteq \mathbb{F}_q^{m \times n_i} \text{ are optimal anticodes and } \dim(\mathcal{C} \cap \mathcal{A}) \geq r\}. \tag{27}$$

Remark 4.30. We could have defined $d_r(\mathcal{C})$ to be

$$d'_r(\mathcal{C}) = \min\{\operatorname{maxsrk}(\mathcal{A}) : \mathcal{A} \text{ an optimal anticode and } \dim(\mathcal{C} \cap \mathcal{A}) \geq r\}.$$

For either $q \neq 2$ or $m_{\ell-2} > 1$ we have that $d_r(\mathcal{C}) = d'_r(\mathcal{C})$ as, by Corollary 4.21, $\mathcal{A}$ is an optimal anticode if and only if $\mathcal{A} = \mathcal{A}_1 \times \cdots \times \mathcal{A}_\ell$ for $\mathcal{A}_i$ optimal anticode in $\mathbb{F}_q^{m_i \times n_i}$. In the case $q = 2$ and $m_{\ell-2} = 1$ one has

$$d'_r(\mathcal{C}) \leq d_r(\mathcal{C}).$$

Notice moreover that $d_r(\mathcal{C})$ recovers the Hamming weights, while $d'_r(\mathcal{C})$ does not. See also the example following Theorem 10 in [61].

Remark 4.31. It follows from the definition that the generalized weights are invariant under code equivalence.

As an example, we compute the generalized weights of optimal anticodes.

Example 4.32. For $i \in [\ell]$ let $\mathcal{A}_i \subseteq \mathbb{F}_q^{m_i \times n_i}$ be an optimal anticode and let $\mathcal{A} = \mathcal{A}_1 \times \cdots \times \mathcal{A}_\ell \subseteq \mathbb{M}$ with $\dim(\mathcal{A}_i) = m_i u_i$. By Corollary 4.26 and the previous remark, $d_r(\mathcal{A}) = d_r(\mathcal{A}')$ for $r \in [\dim(\mathcal{A})]$, where $\mathcal{A}' = \prod_{i=1}^{\ell} \langle E_{k,l} \mid (k,l) \in [m_i] \times [u_i] \rangle$. Let $j \in [\ell]$, $0 \leq \delta \leq u_j - 1$, $r = \sum_{i=1}^{j-1} m_i u_i + m_j \delta$. Then

$$d_{r+1}(\mathcal{A}) = \ldots = d_{r+m_j}(\mathcal{A}) = u_1 + \ldots + u_{j-1} + \delta + 1.$$

In the next proposition we establish some basic properties of generalized weights. Notice that in the case $m_1 = \ldots = m_\ell$ one gets inequalities of the same form as those in [61, Theorem 30].

Proposition 4.33. Let $0 \neq \mathcal{C} \subseteq \mathcal{D} \subseteq \mathbb{M}$, then

1. $d_1(\mathcal{C}) = \mathrm{d}(\mathcal{C})$,
2. $d_r(\mathcal{C}) \leq d_s(\mathcal{C})$ for $1 \leq r \leq s \leq \dim(\mathcal{C})$,
3. $d_r(\mathcal{C}) \geq d_r(\mathcal{D})$ for $r \in [\dim(\mathcal{C})]$,
4. $d_{\dim(\mathcal{C})}(\mathcal{C}) \leq n_1 + \cdots + n_\ell$,
5. $d_{r+n_1 m_1 + \cdots + n_{j-1} m_{j-1} + \delta m_j}(\mathcal{C}) \geq d_r(\mathcal{C}) + n_1 + \cdots + n_{j-1} + \delta$
   for $j \in [\ell], r \in [\dim(\mathcal{C}) - (n_1 m_1 + \cdots + n_{j-1} m_{j-1} + \delta m_j)]$ and $0 \leq \delta \leq n_j - 1$.

Proof. 1. Let $C = (C_1, \ldots, C_\ell) \in \mathcal{C}$ be an element of minimum sum-rank. Let $\mathcal{A}_i$ be an optimal anticode of $\dim(\mathcal{A}_i) = m_i \operatorname{rank}(C_i)$ containing C_i and let $\mathcal{A} = \mathcal{A}_1 \times \cdots \times \mathcal{A}_\ell$. Then $\mathcal{C} \cap \mathcal{A} \neq 0$, hence $d_1(\mathcal{C}) \leq \mathrm{d}(\mathcal{C})$. To prove that they are equal, observe that if $\mathcal{A}'$ is an optimal anticode with $\operatorname{maxsrk}(\mathcal{A}') < \mathrm{d}(\mathcal{C})$, then $\mathcal{C} \cap \mathcal{A}' = 0$.

2. , 3. and 4. follow directly from the definition.

5. Let $s = r + n_1 m_1 + \cdots + n_{j-1} m_{j-1} + \delta m_j$. Let $\mathcal{A} = \mathcal{A}_1 \times \cdots \times \mathcal{A}_\ell$ be an optimal anticode such that $\dim(\mathcal{C} \cap \mathcal{A}) \geq s$ and $d_s(\mathcal{C}) = \operatorname{maxsrk}(\mathcal{A})$. For $i \in [\ell]$, write $\dim(\mathcal{A}_i) = m_i u_i$. Then $d_s(\mathcal{C}) = u_1 + \ldots + u_\ell > n_1 + \cdots + n_{j-1} + \delta$, since $m_1 \geq \cdots \geq m_\ell$ and

$$\sum_{i=1}^{\ell} m_i u_i = \dim(\mathcal{A}) \geq \dim(\mathcal{C} \cap \mathcal{A}) \geq s > n_1 m_1 + \cdots + n_{j-1} m_{j-1} + \delta m_j.$$

Let $v_1, \ldots, v_\ell$ be such that $n_1 + \cdots + n_{j-1} + \delta = v_1 + \cdots + v_\ell$ and $v_i \leq u_i$ for $i \in [\ell]$. We have that $n_1 m_1 + \cdots + n_{j-1} m_{j-1} + \delta m_j \geq v_1 m_1 + \cdots + v_\ell m_\ell$,

since $m_1 \geq \cdots \geq m_\ell$. For all $i \in [\ell]$ there exist optimal anticodes $\mathcal{A}'_i \subseteq \mathcal{A}_i$ of $\dim(\mathcal{A}'_i) = m_i(u_i - v_i)$. Let $\mathcal{A}' = \mathcal{A}'_1 \times \cdots \times \mathcal{A}'_\ell$, then

$$\begin{aligned}\dim(\mathcal{C} \cap \mathcal{A}') &\geq s - (v_1 m_1 + \cdots + v_\ell m_\ell) \\ &\geq s - (n_1 m_1 + \cdots + n_{j-1} m_{j-1} + \delta m_j) \\ &= r\end{aligned}$$

hence

$$d_r(\mathcal{C}) \leq \sum_{i=1}^{\ell} (u_i - v_i) = d_s(\mathcal{C}) - (n_1 + \cdots + n_{j-1} + \delta). \qquad \square$$

From parts 4. and 5. of Proposition 4.33, we easily obtain the following Singleton-type bound.

Corollary 4.34. Let $j \in [\ell]$, $0 \leq \delta \leq n_j - 1$, $0 \leq s \leq m_j - 1$, and let $\mathcal{C} \subseteq \mathbb{M}$ be a non-trivial code of

$$\dim(\mathcal{C}) = \sum_{i=1}^{j-1} m_i n_i + \delta m_j + s.$$

Then

$$\mathrm{d}(\mathcal{C}) \leq \sum_{i=j}^{\ell} n_i - \delta + \begin{cases} 1 & \text{if } s = 0 \\ 0 & \text{otherwise.} \end{cases}$$

The next lemma will be useful in Section 4.5 for computing the generalized weights of an MSRD code.

Lemma 4.35. Let $\mathcal{C} \subseteq \mathbb{M}$ be a code and let $k \in [\ell]$, $r + m_k \in [\dim(\mathcal{C})]$. If

$$d_{r+m_k}(\mathcal{C}) > \sum_{i=1}^{k-1} n_i$$

then

$$d_{r+m_k}(\mathcal{C}) \geq d_r(\mathcal{C}) + 1.$$

Proof. Let $\mathcal{A} = \mathcal{A}_1 \times \cdots \times \mathcal{A}_\ell$ be an optimal anticode such that $\mathrm{maxsrk}(\mathcal{A}) = d_{r+m_k}(\mathcal{C})$ and $\dim(\mathcal{C} \cap \mathcal{A}) \geq r + m_k$. We claim that there exists $k \leq j \leq \ell$ such that $\mathcal{A}_j \neq 0$. In fact, if this were not the case, then

$$\sum_{i=1}^{k-1} n_i \geq \mathrm{maxsrk}(\mathcal{A}) = d_{r+m_k}(\mathcal{C}).$$

Let $\mathcal{A}' \subseteq \mathcal{A}$ be an optimal anticode such that

$$\dim(\mathcal{A}') = \dim(\mathcal{A}) - m_j \quad \text{and} \quad \mathrm{maxsrk}(\mathcal{A}') = \mathrm{maxsrk}(\mathcal{A}) - 1.$$

One has

$$\dim(\mathcal{C} \cap \mathcal{A}') \geq \dim(\mathcal{C} \cap \mathcal{A}) - m_j \geq r + m_k - m_j \geq r,$$

hence

$$d_r(\mathcal{C}) \leq \mathrm{maxsrk}(\mathcal{A}') = d_{r+m_k}(\mathcal{C}) - 1.$$

$\square$

The next theorem extends Wei's Duality Theorem [73, Theorem 3] and [61, Corollary 38]. Let $m_1 = \ldots = m_\ell = m$ and let $\mathcal{C} \subseteq \mathbb{M}$ be a sum-rank metric code. For any $r \in \mathbb{Z}$ define

$$W_r(\mathcal{C}) = \{d_{r+sm}(\mathcal{C}) : s \in \mathbb{Z}, r + sm \in [\dim(\mathcal{C})]\},$$
$$\overline{W}_r(\mathcal{C}) = \{n + 1 - d_{r+sm}(\mathcal{C}) : s \in \mathbb{Z}, r + sm \in [\dim(\mathcal{C})]\}.$$

The same arguments as in [61, Corollary 38] together with Proposition 4.33 prove the next theorem.

Theorem 4.36. Let $m_1 = \ldots = m_\ell = m$, $r \in [m]$, and let $\mathcal{C} \subseteq \mathbb{M}$ be a sum-rank metric code. Then

$$W_r(\mathcal{C}^\perp) = [n] \backslash \overline{W}_{r+\dim(\mathcal{C})}(\mathcal{C}).$$

In particular the generalized weights of a sum rank metric code $\mathcal{C}$ determine the generalized weights of $\mathcal{C}^\perp$.

The next example shows that the generalized weights of a code do not determine those of its dual for arbitrary m_i's.

Example 4.37. Let $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_2^{3\times 1} \times \mathbb{F}_2^{2\times 2}$ be given by

$$\mathcal{C}_1 = 0 \times \mathbb{F}_2^{2\times 2}$$
$$\mathcal{C}_2 = \left\{ \left(\begin{pmatrix} a \\ b \\ 0 \end{pmatrix}, \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \right) : (a, b, c, d) \in \mathbb{F}_2^4 \right\}.$$

One can check that $d_1(\mathcal{C}_i) = d_2(\mathcal{C}_i) = 1$ and $d_3(\mathcal{C}_i) = d_4(\mathcal{C}_i) = 2$ for $i = 1, 2$. The corresponding duals

$$\mathcal{C}_1^\perp = \mathbb{F}_2^{3\times 1} \times 0$$
$$\mathcal{C}_2^\perp = \left\{ \left(\begin{pmatrix} 0 \\ 0 \\ a \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ b & c \end{pmatrix} \right) : (a, b, c) \in \mathbb{F}_2^3 \right\}$$

have different generalized weights, as $d_3(\mathcal{C}_1^\perp) = 1$ and $d_3(\mathcal{C}_2^\perp) = 2$.

Remark 4.38. Notice that the first code in the previous example is an optimal anticode, while the second one is not. Therefore, the example also shows that in the sum-rank metric there exist codes which have the same dimension and generalized weights as an optimal anticode, without being one. This is in contrast with codes endowed with the rank metric or the Hamming metric, where a code which has the same dimension and generalized weights as an optimal anticode is an optimal anticode.

Remark 4.39. There is another simple situation in which the generalized weights of the dual code are determined by numerical data on the original code. Let $\mathcal{C} = \mathcal{C}_1 \times \ldots \times \mathcal{C}_\ell$, then the generalized weights of $\mathcal{C}$ satisfy

$$d_r(\mathcal{C}) = \min \left\{ \sum_{i=1}^{\ell} d_{r_i}(\mathcal{C}_i) : \sum_{i=1}^{\ell} r_i = r, r_i \in [\dim(\mathcal{C}_i)] \right\}.$$

The generalized weights of the rank-metric codes $\mathcal{C}_1, \ldots, \mathcal{C}_\ell$ determine those of $\mathcal{C}_1^\perp, \ldots, \mathcal{C}_\ell^\perp$, hence they determine the generalized weights of $\mathcal{C}^\perp$.

We conclude this section with a result on the weights of a code which is $\mathbb{F}_{q^m}$-linear or, more generally, $\mathbb{F}_{q^k}$-linear.
Let $k = \gcd\{m_1, \ldots, m_\ell\}$. If $k \mid m_i$ for all $i \in [\ell]$, then $\mathbb{F}_{q^{m_1}}^{n_1} \times \cdots \times \mathbb{F}_{q^{m_\ell}}^{n_\ell}$ is a vector space over $\mathbb{F}_{q^k}$. For $i \in [\ell]$, let $\Gamma_i = \{\gamma_{1,i}, \ldots, \gamma_{m_i,i}\}$ be a basis of $\mathbb{F}_{q^{m_i}}$ over $\mathbb{F}_q$. For every $w \in \mathbb{F}_{q^{m_i}}^{n_i}$ define $\Gamma_i(w) \in \mathbb{F}_q^{m_i \times n_i}$ via the identity

$$\begin{pmatrix} \gamma_{1,i} & \ldots & \gamma_{m_i,i} \end{pmatrix} \Gamma_i(w) = w.$$

For every $v = (v_1, \ldots, v_\ell) \in \mathbb{F}_{q^{m_1}}^{n_1} \times \cdots \times \mathbb{F}_{q^{m_\ell}}^{n_\ell}$, define $\Gamma(v) \in \mathbb{M}$ as

$$(\Gamma(v))_i = \Gamma_i(v_i).$$

Let $\mathcal{V} \subseteq \mathbb{F}_{q^{m_1}}^{n_1} \times \cdots \times \mathbb{F}_{q^{m_\ell}}^{n_\ell}$ be a vector space over $\mathbb{F}_{q^k}$. The set $\Gamma(\mathcal{V}) = \{\Gamma(v) : v \in \mathcal{V}\}$ is the sum-rank metric code associated to $\mathcal{V}$ with respect to $\{\Gamma_1, \ldots, \Gamma_\ell\}$. We say that $\Gamma(\mathcal{V})$ is $\mathbb{F}_{q^k}$-linear, see also [30, Definition 11.1.3].
In the next theorem we extend the result in [61, Theorem 28] to the sum-rank metric case. The statement in particular applies to $\mathbb{F}_{q^m}$-linear codes in the case when $m_1 = \ldots = m_\ell = m$.

Theorem 4.40. Let $k = \gcd\{m_1, \ldots, m_\ell\}$ and let $\mathcal{V} \subseteq \mathbb{F}_{q^{m_1}}^{n_1} \times \cdots \times \mathbb{F}_{q^{m_\ell}}^{n_\ell}$ be an $\mathbb{F}_{q^k}$-linear vector space with $\dim_{\mathbb{F}_{q^k}}(\mathcal{V}) = t$. If $m_i > n_i$ for $i \in [\ell]$, then

$$d_{kr+1}(\Gamma(\mathcal{V})) = \ldots = d_{k(r+1)}(\Gamma(\mathcal{V}))$$

for $0 \leq r < t$.

Proof. For ease of notation we write $\mathcal{C}$ for $\Gamma(\mathcal{V})$. By Proposition 4.33, $d_{kr+1}(\mathcal{C}) \leq \ldots \leq d_{k(r+1)}(\mathcal{C})$. Therefore it suffices to show that $d_{kr+1}(\mathcal{C}) = d_{k(r+1)}(\mathcal{C})$. Since $m_i > n_i$ for $i \in [\ell]$, $\mathcal{A}$ is an $\mathbb{F}_{q^k}$-linear code and so $\mathcal{C} \cap \mathcal{A}$ is also $\mathbb{F}_{q^k}$-linear. Since the dimension over $\mathbb{F}_q$ of an $\mathbb{F}_{q^k}$-linear vector space is divisible by k, if $\dim(\mathcal{C} \cap \mathcal{A}) \geq kr + 1$, then $\dim(\mathcal{C} \cap \mathcal{A}) \geq k(r + 1)$. Therefore we conclude that $d_{kr+1}(\mathcal{C}) \geq d_{k(r+1)}(\mathcal{C})$. □

Remark 4.41. Although the condition that $m > n$ is missing in the statement of [61, Theorem 28], it is necessary for the result to hold. In fact, [29, Example 6.15] is a counterexample to the statement of [61, Theorem 28] for square matrices.

4.5 Singleton-type Bound and MSRD Codes

In this section we define MSRD and r-MSRD codes, and compute their generalized weights.

Notation 4.42. For $\mu \in [n]$ we denote by $\mathbb{A}(\mu)$ the set of optimal anticodes of the form $\mathcal{A} = \mathcal{A}_1 \times \ldots \times \mathcal{A}_\ell \subseteq \mathbb{M}$, with $\mathcal{A}_i \subseteq \mathbb{F}_q^{m_i \times n_i}$ an optimal anticode for all $i \in [\ell]$ and $\operatorname{maxsrk}(\mathcal{A}) = \sum_{i=1}^{\ell} \operatorname{maxrk}(\mathcal{A}_i) = \mu$.

The next lemma is immediate.

Lemma 4.43. Let $\mu \in [n]$ and write $\mu = \sum_{i=1}^{j-1} n_i + \delta = \sum_{i=l+1}^{\ell} n_i + \delta'$ for some $j, l \in [\ell]$, $\delta \in [n_j]$, and $\delta' \in [n_l]$. Then

$$\min_{\mathcal{A} \in \mathbb{A}(\mu)} (\dim(\mathcal{A})) = \sum_{i=l+1}^{\ell} m_i n_i + \delta' m_l$$

and

$$\max_{\mathcal{A} \in \mathbb{A}(\mu)} (\dim(\mathcal{A})) = \sum_{i=1}^{j-1} m_i n_i + \delta m_j.$$

Moreover, if

$$\min_{\mathcal{A} \in \mathbb{A}(\mu)} (\dim(\mathcal{A})) = \max_{\mathcal{A} \in \mathbb{A}(\mu)} (\dim(\mathcal{A})),$$

then either $\mu = n$ or $m_1 = \ldots = m_\ell$.

Notation 4.44. Let $\mu \in [n]$ and write $\mu = \sum_{i=1}^{j-1} n_i + \delta + 1$, $0 \leq \delta \leq n_j - 1$. Throughout the section, we denote

$$r_\mu = \max_{\mathcal{A} \in \mathbb{A}(\mu)} (\dim(\mathcal{A})) = \sum_{i=1}^{j-1} m_i n_i + (\delta + 1) m_j.$$

The Singleton bound for rank-metric codes was first proved in [19, Theorem 5.4]. A Singleton bound for sum-rank metric codes was established in [11, Theorem 3.2], for codes which are not necessarily linear. Our next theorem generalizes the previous results in the case of linear sum-rank metric codes.

Theorem 4.45. Let $\mathcal{C} \subseteq \mathbb{M}$ and let $r \in [\dim(\mathcal{C})]$. Let $j \in [\ell]$ and $0 \leq \delta \leq n_j - 1$ be such that

$$d_r(\mathcal{C}) - 1 \geq \sum_{i=1}^{j-1} n_i + \delta.$$

Then

$$\dim(\mathcal{C}) \leq \sum_{i=j}^{\ell} m_i n_i - m_j \delta + r - 1. \tag{28}$$

Proof. Let $\mathcal{A}_i = \mathbb{F}_q^{m_i \times n_i}$ for $i \in [j-1]$, let $\mathcal{A}_j \subseteq \mathbb{F}_q^{m_j \times n_j}$ be an optimal anticode of dimension δm_j, and let $\mathcal{A}_i = 0$ for $j+1 \leq i \leq \ell$. Let $\mathcal{A} = \mathcal{A}_1 \times \cdots \times \mathcal{A}_\ell$, then

$$\dim(\mathcal{C} \cap \mathcal{A}) \leq r - 1.$$

Therefore

$$\begin{aligned} \dim(\mathcal{C}) + \sum_{i=1}^{j-1} m_i n_i + m_j \delta - r + 1 &\leq \dim(\mathcal{C}) + \dim(\mathcal{A}) - \dim(\mathcal{C} \cap \mathcal{A}) \\ &= \dim(\mathcal{C} + \mathcal{A}) \leq \sum_{i=1}^{\ell} m_i n_i. \end{aligned}$$

□

Theorem 4.45 yields upper bounds on all the generalized weights of $\mathcal{C}$.

Corollary 4.46. Let $\mathcal{C} \subseteq \mathbb{M}$ and let $r \in [\dim(\mathcal{C})]$, $j \in [\ell]$, and $0 \leq \delta \leq n_j - 1$ be such that $\dim(\mathcal{C}) \geq \sum_{i=j}^{\ell} m_i n_i - m_j \delta + r$. Then

$$d_r(\mathcal{C}) \leq \sum_{i=1}^{j-1} n_i + \delta.$$

In particular, if $\dim(\mathcal{C}) = \sum_{i=j}^{\ell} m_i n_i - \delta m_j$, then

$$d_1(\mathcal{C}) \leq \ldots \leq d_{m_j}(\mathcal{C}) \leq \sum_{i=1}^{j-1} n_i + \delta + 1.$$

Corollary 4.46 suggests the following definition of MSRD code. The same definition was given in [11, Definition 3.3] for codes which are not necessarily linear.

Definition 4.47. A linear code $\mathcal{C} \subseteq \mathbb{M}$ is MSRD if there exist $j \in [\ell]$ and $0 \leq \delta \leq n_j - 1$ such that

$$\mathrm{d}(\mathcal{C}) = \sum_{i=1}^{j-1} n_i + \delta + 1 \quad \text{and} \quad \dim(\mathcal{C}) = \sum_{i=j}^{\ell} m_i n_i - \delta m_j.$$

Next we study some properties which are closely related to being MSRD.

($C0$) For any optimal anticode $\mathcal{A}$ of $\mathrm{maxsrk}(\mathcal{A}) = \mathrm{d}(\mathcal{C}) - 1$ and $\dim(\mathcal{A}) = r_{\mathrm{d}(\mathcal{C})-1}$ one has $\mathcal{C} + \mathcal{A} = \mathbb{M}$.

($C1$) The code $\mathcal{C}$ has $\dim(\mathcal{C}) = \sum_{i=j}^{\ell} m_i n_i - m_j \delta$ and for any $\mathcal{A}$ optimal anticode of $\mathrm{maxsrk}(\mathcal{A}) \leq \sum_{i=1}^{j-1} n_i + \delta$ we have $\mathcal{C} \cap \mathcal{A} = 0$.

($C2$) For any $\mathcal{A} \in \mathbb{A}(\mathrm{d}(\mathcal{C}))$, let $k = \max\{i \in [\ell] \ : \ \mathcal{A}_i \neq 0\}$. Then

$$\dim(\mathcal{C} \cap \mathcal{A}) \geq m_k.$$

($C3$) The code $\mathcal{C}$ has $\mathrm{d}(\mathcal{C}) + \mathrm{d}(\mathcal{C}^{\perp}) = n + 2$.

It is clear that being MSRD is equivalent to satisfying ($C0$). We now show that it is also equivalent to satisfying ($C1$).

Proposition 4.48. Let $j \in [\ell]$ and $0 \leq \delta \leq n_j - 1$. Let $0 \neq \mathcal{C} \subseteq \mathbb{M}$, then $\mathcal{C}$ is MSRD if and only if it satisfies ($C1$).

Proof. Suppose that $\mathcal{C}$ is MSRD of $\dim(\mathcal{C}) = \sum_{i=j}^{\ell} m_i n_i - \delta m_j$. Let $\mathcal{A}$ be an optimal anticode of $\mathrm{maxsrk}(\mathcal{A}) \leq \mathrm{d}(\mathcal{C}) - 1$. Then $\mathcal{C} \cap \mathcal{A} = 0$ since, for every $0 \neq C \in \mathcal{C}$, one has $\mathrm{srank}(C) \geq \mathrm{d}(C) > \mathrm{maxsrk}(\mathcal{A})$, so $C \notin \mathcal{A}$.
Suppose now that $\mathcal{C}$ satisfies ($C1$). Then $\mathrm{d}(\mathcal{C}) \leq \sum_{i=1}^{j-1} n_i + \delta + 1$ by Corollary 4.46. Let $C = (C_1, \ldots, C_\ell) \in \mathcal{C}$. For every $i \in [\ell]$, there is an optimal anticode $\mathcal{A}_i \subseteq \mathbb{F}_q^{m_i \times n_i}$ of $\dim(\mathcal{A}_i) = m_i \,\mathrm{rank}(C_i)$ which contains C_i. Therefore $\mathcal{A} = \mathcal{A}_1 \times \ldots \times \mathcal{A}_\ell$ is an optimal sum-rank metric anticode of $\mathrm{maxsrk}(\mathcal{A}) = \mathrm{srank}(C)$ which contains C. Since $\mathcal{C} \cap \mathcal{A} \neq 0$, we have that $\mathrm{maxsrk}(\mathcal{A}) = \mathrm{srank}(C) \geq \sum_{i=1}^{j-1} n_i + \delta + 1$, therefore $\mathcal{C}$ is MSRD. □

Proposition 4.49. Let $0 \neq \mathcal{C} \subseteq \mathbb{M}$ and write its minimum distance as $d = \mathrm{d}(\mathcal{C}) = \sum_{i=1}^{j-1} n_i + \delta + 1$, where $j \in [\ell]$ and $0 \leq \delta \leq n_j - 1$. For $S \subseteq [n]$, denote by $\mathbb{F}_q[S]$ the set of elements of $\mathbb{M}$ which are zero outside of the columns indexed by S. For any $d \leq h \leq n$, let $S_h = [d-1] \cup \{h\}$. The following hold:

1. $\mathcal{C}$ is MSRD if and only if for any $d \leq h \leq n$ we have
$$\dim(\mathcal{C} \cap \mathbb{F}_q[S_h]) = m_k$$
where $k = \max\{\nu \ : \ \sum_{i=1}^{\nu-1} n_i < h\}$.
2. If $\mathcal{C}$ satisfies $(C2)$, then $\mathcal{C}$ is MSRD.

Proof. 1. Assume that $\mathcal{C}$ is MSRD and let $d \leq h \leq n$. We have
$$\begin{aligned}\dim(\mathcal{C} \cap \mathbb{F}_q[S_h]) &\geq \dim(\mathcal{C}) + \dim(\mathbb{F}_q[S_h]) - \sum_{i=1}^{\ell} m_i n_i \\ &= \sum_{i=j}^{\ell} m_i n_i - \delta m_j + \sum_{i=1}^{j-1} m_i n_i + \delta m_j + m_k - \sum_{i=1}^{\ell} m_i n_i \\ &= m_k.\end{aligned}$$
Conversely, suppose that for $d \leq h \leq n$ one has $\dim(\mathcal{C} \cap \mathbb{F}_q[S_h]) \geq m_k$. Let $d \leq h' \leq n$, $h \neq h'$. Then
$$\dim(\mathcal{C} \cap \mathbb{F}_q[S_h] \cap \mathbb{F}_q[S_{h'}]) = \dim(\mathcal{C} \cap \mathbb{F}_q[[d-1]]) = 0$$
hence
$$\dim(\mathcal{C}) \geq \sum_{h=d}^{n} \dim(\mathcal{C} \cap \mathbb{F}_q[S_h]) \geq \sum_{i=j}^{\ell} m_i n_i - \delta m_j. \tag{29}$$
Theorem 4.45 implies that (29) is an equality, hence $\mathcal{C}$ is MSRD.
This proves that $\mathcal{C}$ is MSRD if and only if $\dim(\mathcal{C} \cap \mathbb{F}_q[S_h]) \geq m_k$ for all $d \leq h \leq n$. Notice moreover that (29) and Theorem 4.45 imply that, if $\dim(\mathcal{C} \cap \mathbb{F}_q[S_h]) \geq m_k$ for all $d \leq h \leq n$, then in fact $\dim(\mathcal{C} \cap \mathbb{F}_q[S_h]) = m_k$ for all $d \leq h \leq n$. This concludes the proof of the first part of the statement.
2. Suppose that $\mathcal{C}$ satisfies (C2). For any $d \leq h \leq n$, letting $\mathcal{A} = \mathbb{F}_q[S_h] \in \mathbb{A}(d)$, one has that $\dim(\mathcal{C} \cap \mathbb{F}_q[S_h]) \geq m_k$. As shown in 1., combining (29) and Theorem 4.45 one obtains that $\mathcal{C}$ is MSRD. □

The next examples show that there exist nontrivial codes which satisfy property $(C2)$ and that not every MSRD code satisfies $(C2)$.

Example 4.50. In $\mathbb{F}_2^{2\times 2} \times \mathbb{F}_2$, let
$$\mathcal{C} = \left\langle \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, 1 \right), \left(\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, 1 \right), \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, 1 \right) \right\rangle.$$
We have $\mathrm{d}(\mathcal{C}) = 2$ and $\mathcal{C}$ satisfies $(C2)$.

Example 4.51. Let $\mathcal{C} \subseteq \mathbb{F}_2^{3\times 3} \times \mathbb{F}_2^{2\times 2} \times \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$ be given by

$$\mathcal{C} = \left\langle \left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, 1, 1, 0 \right), \left(\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, 0, 1, 1 \right) \right\rangle.$$

The code $\mathcal{C}$ has dimension 2 with $\mathrm{d}(\mathcal{C}) = 7$, hence it is an MSRD code. Consider now the optimal anticode

$$\mathcal{A} = \langle E_{i,1}, E_{i,2} \ : \ i \in [3] \rangle \times \mathbb{F}_2^{2\times 2} \times \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2.$$

We have $\mathrm{maxsrk}(\mathcal{A}) = 7$ and $\mathcal{A} \cap \mathcal{C} = 0$. Hence $\mathcal{C}$ does not satisfy $(C2)$.

Proposition 4.52. Let $\mathcal{C} \subseteq \mathbb{M}$ be a non-trivial code. Then $\mathcal{C}$ satisfies $(C3)$ if and only if both $\mathcal{C}$ and $\mathcal{C}^\perp$ are MSRD.

Proof. Write $\dim(\mathcal{C}) = \sum_{i=j}^{\ell} m_i n_i - \delta m_j - s$ for some $j \in [\ell]$, $0 \leq \delta \leq n_j - 1$, and $0 \leq s \leq m_j - 1$. By Corollary 4.46

$$d_1(\mathcal{C}) \leq \sum_{i=1}^{j-1} n_i + \delta + 1. \tag{30}$$

Moreover, $\dim(C^\perp) = \dim(\mathbb{M}) - \dim(\mathcal{C}) = \sum_{i=1}^{j-1} m_i n_i + \delta m_j + s$, which by Corollary 4.34 implies that

$$d_1(\mathcal{C}^\perp) \leq \sum_{i=j}^{\ell} n_j - \delta + \begin{cases} 1 & \text{if } s = 0 \\ 0 & \text{otherwise.} \end{cases} \tag{31}$$

Therefore

$$\mathrm{d}(\mathcal{C}) + \mathrm{d}(\mathcal{C}^\perp) \leq \begin{cases} n+2 & \text{if } s = 0 \\ n+1 & \text{otherwise.} \end{cases}$$

If $\mathcal{C}$ satisfies $(C3)$, then $s = 0$ and both $\mathcal{C}$ and $\mathcal{C}^\perp$ are MSRD. Conversely, if $\mathcal{C}$ and $\mathcal{C}^\perp$ are MSRD, then $s = 0$ and both (30) and (31) are equalities. It follows that $\mathcal{C}$ satisfies $(C3)$. □

In the next proposition we prove that, if $m_1 = \ldots = m_\ell$, then properties $(C2)$ and $(C3)$ are equivalent to being MSRD.

Proposition 4.53. Let $\mathcal{C} \subseteq \mathbb{M}$ be a non-trivial code. If $m_1 = \ldots = m_\ell = m$, then both $(C2)$ and $(C3)$ are equivalent to being MSRD. In particular, the dual of an MSRD code is MSRD.

Proof. Let $\mathcal{C} \subseteq \mathbb{M}$ be a non-trivial code. If $\mathcal{C}$ is MSRD, then it satisfies $(C3)$ by [11, Theorem 6.1]. If $\mathcal{C}$ satisfies property $(C3)$, then it is MSRD by Proposition 4.52.
If $\mathcal{C}$ satisfies $(C2)$, then it is MSRD by Proposition 4.49. We now prove that if $\mathcal{C}$ is MSRD, then it satisfies $(C2)$. Let $\mathcal{A} \in \mathbb{A}(\mathrm{d}(\mathcal{C}))$, then

$$\dim(\mathcal{C}) + \dim(\mathcal{A}) \leq mn + \dim(\mathcal{C} \cap \mathcal{A}).$$

Hence by Lemma 4.43 we have

$$mn + m \leq mn + \dim(\mathcal{C} \cap \mathcal{A}),$$

so $\mathcal{C}$ satisfies $(C2)$. □

Moreover, one can prove that $(C3)$ defines a trivial family of codes, unless $m_1 = \cdots = m_\ell$. Notice that this shows in particular that the dual of a non-trivial MSRD code can never be MSRD, unless $m_1 = \cdots = m_\ell$.

Proposition 4.54. If there exists a non-trivial code $\mathcal{C} \subseteq \mathbb{M}$ that satisfies $(C3)$, then $m_1 = \cdots = m_\ell$.

Proof. Write $\mathrm{d}(\mathcal{C}^\perp) - 1 = \sum_{i=1}^{k-1} n_i + \varepsilon$ for some $k \in [\ell]$ and $0 \leq \varepsilon \leq n_k - 1$. Since $\mathrm{d}(\mathcal{C}) + \mathrm{d}(\mathcal{C}^\perp) - 2 = n$ we find that

$$\mathrm{d}(\mathcal{C}) - 1 = \sum_{i=1}^{j-1} n_i + \delta = \sum_{i=k}^{\ell} n_i - \varepsilon \tag{32}$$

for some $j \in [\ell]$ and $0 \leq \delta \leq n_j - 1$. Since $\mathcal{C}$ and $\mathcal{C}^\perp$ are MSRD by Proposition 4.52, one has

$$\dim(\mathcal{C}) = \sum_{i=j}^{\ell} n_i m_i - \delta m_j = \sum_{i=1}^{k-1} n_i m_i + \varepsilon m_k = \dim(\mathbb{M}) - \dim(\mathcal{C}^\perp). \tag{33}$$

Lemma 4.43, together with (33), implies that

$$\max\{\dim(\mathbb{A}(\mathrm{d}(\mathcal{C}) - 1))\} = \min\{\dim(\mathbb{A}(\mathrm{d}(\mathcal{C}) - 1))\},$$

which by Lemma 4.43 implies that $m_1 = \cdots = m_\ell$. □

In the remainder of this section, we study the generalized weights of MSRD codes and propose a definition of r-MSRD codes, analogous to that of r-MRD codes. The next theorem states that the generalized weights of an MSRD code are determined by its parameters. This generalizes similar results for MDS codes in the Hamming metric and MRD codes in the rank metric. We postpone the proof, since in Theorem 4.60 we will prove a more general result.

Theorem 4.55. Let $\mathcal{C} \subseteq \mathbb{M}$ be an MSRD code and write $\mathrm{d}(\mathcal{C}) = \sum_{i=1}^{j-1} n_i + \delta + 1$ for some $j \in [\ell]$ and $0 \leq \delta \leq n_j - 1$. Let $\mathrm{d}(\mathcal{C}) \leq h \leq n$ and let $k = \max\{\nu \ : \ \sum_{i=1}^{\nu-1} n_i < h\}$. Let $r \in [\dim(\mathcal{C})]$ be of the form

$$r = r_h - r_{\mathrm{d}(\mathcal{C})-1} - m_k + 1.$$

Then

$$d_r(\mathcal{C}) = \cdots = d_{r+m_k-1}(\mathcal{C}) = h.$$

Remark 4.56. One can also write down the generalized weights computed in Theorem 4.55 as follows. Let $j \in [\ell]$, $0 \leq \delta \leq n_j - 1$, and let $\mathcal{C} \subseteq \mathbb{M}$ be an MSRD code with $\mathrm{d}(\mathcal{C}) = \sum_{i=1}^{j-1} n_i + \delta + 1$ and $\dim(\mathcal{C}) = \sum_{i=j}^{\ell} m_i n_i - \delta m_j$. Write

$$h = \sum_{i=1}^{k-1} n_i + \varepsilon + 1$$

where $k \geq j$. Since $\mathrm{d}(\mathcal{C}) \leq h \leq n$, one has that $\delta \leq \varepsilon \leq n_j - 1$ if $k = j$, and $0 \leq \varepsilon \leq n_k - 1$ if $k > j$. Then

$$r = \begin{cases} (\varepsilon - \delta)m_j + 1 & \text{if } k = j,\ \delta \leq \varepsilon \leq n_j - 1, \\ (n_j - \delta)m_j + \sum_{i=j+1}^{k-1} m_i n_i + \varepsilon m_k + 1 & \text{if } j < k \leq \ell,\ 0 \leq \varepsilon \leq n_k - 1. \end{cases}$$

Remark 4.57. It follows from Theorem 4.55 that both bounds in the statement of Theorem 4.45 are met for $r \in [\dim(\mathcal{C})]$ of the form $r = 1, m_j+1, \ldots, (n_j-\delta-1)m_j+1$, and

$$r = (n_j - \delta)m_j + \sum_{i=j+1}^{k-1} m_i n_i + \varepsilon m_k + 1$$

with $j < k \leq \ell$ and $0 \leq \varepsilon \leq n_k - 1$.

Remark 4.58. Let $d_0(\mathcal{C}) = 0$ and $d_{\dim(\mathcal{C})+1}(\mathcal{C}) = n+1$. Theorem 4.55 states that, for any $\mathrm{d}(\mathcal{C}) \leq h \leq n$ and r of the form $r = r_h - r_{\mathrm{d}(\mathcal{C})-1} - m_k + 1$, we have

$$d_{r-1}(\mathcal{C}) < d_r(\mathcal{C}) = \ldots = d_{r+m_k-1}(\mathcal{C}) < d_{r+m_k}(\mathcal{C}).$$

Inspired by Remark 4.58 and by the definition of r-MRD codes, we define a notion of r-MSRD code as follows. Notice that being 1-MSRD is equivalent to being MSRD.

Definition 4.59. Let $j \in [\ell]$, $0 \leq \delta \leq n_j - 1$, and let $\mathcal{C} \subseteq \mathbb{M}$ be a code of $\dim(\mathcal{C}) = \sum_{i=j}^{\ell} m_i n_i - \delta m_j$. Define $d_{\max} = \sum_{i=1}^{j-1} n_i + \delta + 1$, let $d_{\max} \leq h \leq n$ and

$$r = r_h - r_{d_{\max}-1} - m_k + 1,$$

where $k = \max\{\nu \ : \ \sum_{i=1}^{\nu-1} n_i < h\}$. We say that $\mathcal{C}$ is r**-MSRD** if

$$d_r(\mathcal{C}) = h.$$

We conclude this section by showing that, if $\mathcal{C}$ is r-MSRD, then $\mathcal{C}$ is r'-MSRD for all $r' \geq r$, where r, r' are integers of the form given in Definition 4.59. This observation allows us to compute the generalized weights of an r-MSRD code. Since an MSRD code is 1-MSRD, the proof of next theorem also proves Theorem 4.55.

Theorem 4.60. Let $j \in [\ell]$, $0 \leq \delta \leq n_j - 1$, and let $\mathcal{C} \subseteq \mathbb{M}$ be a non-trivial code of $\dim(\mathcal{C}) = \sum_{i=j}^{\ell} m_i n_i - \delta m_j$. Define $d_{\max} = \sum_{i=1}^{j-1} n_i + \delta + 1$, let $d_{\max} \leq h \leq n$ and

$$r = r_h - r_{d_{\max}-1} - m_k + 1,$$

where $k = \max\{\nu \ : \ \sum_{i=1}^{\nu-1} n_i < h\}$. If $\mathcal{C}$ is r-MSRD, then

$$d_r(\mathcal{C}) = \ldots = d_{r+m_k-1}(\mathcal{C}) = h.$$

Moreover, $\mathcal{C}$ is $(r + m_k)$-MSRD.

Proof. We have

$$h = d_r(\mathcal{C}) \leq \ldots \leq d_{r+m_k-1}(\mathcal{C}) \leq h,$$

where the equality follows from the definition of r-MSRD code, the first and second inequalities from Proposition 4.33, and the third from Corollary 4.46. Therefore $d_r(\mathcal{C}) = \ldots = d_{r+m_k-1}(\mathcal{C}) = h$.
Since $d_{r+m_k}(\mathcal{C}) \geq d_r(\mathcal{C}) = h > \sum_{i=1}^{k-1} n_i$, then by Lemma 4.35

$$d_{r+m_k}(\mathcal{C}) \geq d_r(\mathcal{C}) + 1 = h + 1.$$

The reverse inequality follows from Corollary 4.46, hence $d_{r+m_k}(\mathcal{C}) = h+1$. Since

$$\max\left\{\nu \ : \ \sum_{i=1}^{\nu-1} n_i < h+1\right\} = \begin{cases} k & \text{if } \varepsilon < n_k - 1, \\ k+1 & \text{if } \varepsilon = n_k - 1, \end{cases}$$

we let

$$m' = \begin{cases} m_k & \text{if } \varepsilon < n_k - 1, \\ m_{k+1} & \text{if } \text{ if } \varepsilon = n_k - 1. \end{cases}$$

Since $m' = r_{h+1} = r_h$, one has that $r + m_k = r_{h+1} - r_{d_{\max}-1} - m' + 1$, hence we proved that $\mathcal{C}$ is $(r+m_k)$-MSRD. □

Remark 4.61. We follow the notation of the last theorem. If a code $\mathcal{C}$ is such that $d_r < h$ but $d_{r+s}(\mathcal{C}) = h$ for some $1 \leq s \leq m_k - 1$ then by Corollary 4.46 we have

$$d_{r+s}(\mathcal{C}) = \cdots = d_{r+m_k-1}(\mathcal{C}) = h.$$

However, this does not imply that $\mathcal{C}$ is an $(r+m_k)$-MSRD code, as the next example shows.

Example 4.62. An MSRD code $\mathcal{D}$ of dimension 4 in $\mathbb{F}_2^{4\times 4} \times \mathbb{F}_2^{4\times 2} \times \mathbb{F}_2^{2\times 2}$ has weights $d_1(\mathcal{D}) = d_2(\mathcal{D}) = 7$, $d_3(\mathcal{D}) = d_4(\mathcal{D}) = 8$. Let $\mathcal{C}$ be generated by the following set of elements

$$\left\{ \left(\begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0\\0&1\\0&0\\0&0 \end{pmatrix}, \begin{pmatrix} 1&0\\0&0 \end{pmatrix} \right), \right.$$
$$\left(\begin{pmatrix} 0&0&0&1\\1&0&0&1\\0&1&0&0\\0&0&1&0 \end{pmatrix}, \begin{pmatrix} 0&1\\1&1\\0&0\\0&0 \end{pmatrix}, \begin{pmatrix} 0&0\\1&0 \end{pmatrix} \right),$$
$$\left(\begin{pmatrix} 0&0&1&0\\0&0&1&1\\1&0&0&1\\0&1&0&0 \end{pmatrix}, \begin{pmatrix} 0&0\\0&0\\1&0\\0&1 \end{pmatrix}, 0_{2\times 2} \right),$$
$$\left. \left(0_{4\times 4}, 0_{4\times 2}, \begin{pmatrix} 0&0\\0&1 \end{pmatrix} \right) \right\}.$$

The code $\mathcal{C}$ has dimension 4 and $d_1(\mathcal{C}) = 1$, so $\mathcal{C}$ is not MSRD. We checked using the computer algebra system Macaulay2 [32] that the only nonzero codewords of $\mathcal{C}$ of sum-rank less than 7 are the third and the fourth element in the previous list. Hence $d_2(\mathcal{C}) = d_2(\mathcal{D}) = 7$. Taking $\mathcal{A} = \mathbb{F}_2^{4\times 4} \times \mathbb{F}_2^{4\times 2} \times \left\{ \begin{pmatrix} a&0\\b&0 \end{pmatrix} \ : \ a,b \in \mathbb{F}_2 \right\}$ we can see that $d_3(\mathcal{C}) = 7 < 8 = d_3(\mathcal{D})$. In particular, $\mathcal{C}$ is not 3-MSRD.

References

[1] C. Aguilar-Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, A. Hauteville, and G. Zémor. Ouroboros-r. *First round submission to the NIST post-quantum cryptography call: https://pqc-ouroborosr.org*, 2017.

[2] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung. Network information flow. *IEEE Trans. Inf. Theory*, 46(4):1204–1216, 2000.

[3] N. Aragon, O. Blazy, J.-C. Deneuville, P. Gaborit, A. Hauteville, O. Ruatta, J.-P. Tillich, and G. Zémor. Lake - low rank parity check codes key exchange. *First round submission to the NIST post-quantum cryptography call*, 2017.

[4] N. Aragon, O. Blazy, J.-C. Deneuville, P. Gaborit, A. Hauteville, O. Ruatta, J.-P. Tillich, and G. Zémor. Locker - low rank parity check codes encryption. *First round submission to the NIST post-quantum cryptography call*, 2017.

[5] N. Aragon, O. Blazy, J.-C. Deneuville, P. Gaborit, A. Hauteville, O. Ruatta, J.-P. Tillich, G. Zémor, C. Aguilar-Melchor, S. Bettaieb, L. Bidoux, B. Magali, and A. Otmani. Rollo (merger of rank-ouroboros, lake and locker). *Second round submission to the NIST post-quantum cryptography call: https://pqc-rollo.org/*, 2019.

[6] M. Atkinson and S. Lloyd. Large spaces of matrices of bounded rank. *The Quarterly Journal of Mathematics*, 31(2):253–262, 1980.

[7] T. P. Berger. Isometries for rank distance and permutation group of gabidulin codes. *IEEE Trans. Inf. Theory*, 49(11):3016–3019, 2002.

[8] E. R. Berlekamp, R. McEliece, and H. C. A. van Tilborg. On the inherent intractability of certain coding problems. *IEEE Trans. Inf. Theory*, 24:384–386, 1978.

[9] D. J. Bernstein, J. Buchmann, and E. Dahmen. *Post-Quantum Cryptography*. Springer, 2009.

[10] E. Byrne, H. Gluesing-Luerssen, and A. Ravagnani. Anticodes in the sum-rank metric. *Preprint arXiv:2012.13706v1*, 2020.

[11] E. Byrne, H. Gluesing-Luerssen, and A. Ravagnani. Fundamental properties of sum-rank metric codes. *Preprint arXiv:2010.02779*, 2020.

[12] H. Cai, M. S. Y. Miao, and X. Tang. A construction of maximally recoverable codes with order-optimal field size. *Preprint, arXiv:2011.13606*, 2020.

[13] F. Chaubaud. On the security of some cryptosystems based on error-correcting codes. *Advances in Cryptology - EUROCRYPT '94 , Lecture Notes in Computer Science, Springer*, 950:131–139, 1994.

[14] D. Coggia and A. Couvreur. On the security of a loidreau's rank metric code based encryption scheme. *Designs, Codes and Cryptography*, 9(88):1941–1957, 2020.

[15] J. de la Cruz, E. Gorla, H. H. López, and A. Ravagnani. Weight distribution of rank-metric codes. *Design, Codes and Cryptography*, 2018.

[16] C. de Seguins Pazzis. The affine preservers of non-singular matrices. *Arch. Math.*, 95:333–342, 2010.

[17] C. de Seguins Pazzis. The classification of large spaces of matrices with bounded rank. *Israel Journal of Mathematics 208*, 2013.

[18] C. de Seguins Pazzis. Large spaces of bounded rank matrices revisited. *Israel Journal of Mathematics 208*, 2016.

[19] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *Journal of combinatorial theory*, (Serie A 25):226–241, 1978.

[20] J. Dieudonné. Sur une généralisation du groupe orthogonal à quatre variables. *Archiv der Mathematik*, 1:282–287, 1948.

[21] H. Flanders. On spaces of linear transformations with bounded rank. *London Mathematical Society*, (1):10–16, 1962.

[22] E. M. Gabidulin. Theory of codes with maximum rank distance. *Problems of Information Transmission*, 21(1):1–12, 1985.

[23] E. M. Gabidulin. Attacks and counter-attacks on the gpt public key cryptosystem. *Designs, Codes and Cryptography*, 48(2):171–177, 2008.

[24] E. M. Gabidulin and A. V. Ourivski. Column scrambler for the gpt cryptosystem. *Discrete Applied Mathematics*, 128:207–221, 2003.

[25] E. M. Gabidulin, A. Paramonov, and O. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. *LNCS*, 573:482–489, 1991.

[26] E. M. Gabidulin, H. Rashwan, and B. Honary. On improving security of gpt cryptosystems. *The Proceedings of IEEE International Symposium on Information Theory (ISIT)*, pages 1110–1114, 2009.

[27] A. Ghatak. Extending coggia-couvreur attack on loidreau's rank-metric cryptosystem. *arXiv:2007.07354 [cs.IT]*, 2020.

[28] J. K. Gibson. Severely denting the gabidulin version of the mceliece public key cryptosystem. *Des Codes Crypt*, 6:37–45, 1995.

[29] H. Gluesing-Luerssen and B. Jany. q-polymatroids and their relation to rank-metric codes. Preprint, 2021. arXiv:2104.06570.

[30] E. Gorla. Rank-metric codes. In W. C. Huffman, J.-L. Kim, and P. Solé, editors, *Concise Encyclopedia of Coding Theory*, pages 227–250. Chapman and Hall/CRC, 2021.

[31] E. Gorla, R. Jurrius, H. H. López, and A. Ravagnani. Rank-metric codes and q-polymatroids. *Journal of Algebraic Combinatorics*, 2019.

[32] D. R. Grayson and M. E. Stillman. Macaulay2, a software system for research in algebraic geometry. Available at `http://www.math.uiuc.edu/Macaulay2/`.

[33] W. Guo and F. Fu. Two modifications for loidreau's code-based cryptosystem. *arXiv:2104.02254 [cs.IT]*, 2021.

[34] T. Helleseth, T. Kløve, and J. Mykkeltveit. The weights distribution of irreducible cyclic codes with block lengths $n_1((q^\ell - 1)/n)$. *Discrete Math.*, 18:179–211, 1977.

[35] 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. Inf. Theory*, 52(10):4413–4430, 2006.

[36] L. Hua. A theorem on matrices over a sfield and its applications. *Acta Mathematica Sinica*, (1):109–163, 1951.

[37] R. Jurrius and R. Pellikaan. On defining generalized rank weights. *Advances in Mathematics of Communications*, 11:225–235, 2017.

[38] R. Jurrius and R. Pellikaan. Defining the q-analogue of a matroid. *Electronic Journal of Combinatorics*, 25(3):1–32, 2018.

[39] R. Koetter and F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Trans. Inf. Theory*, 54(8):3579–3591, 2008.

[40] D. König. Graphok és matrixok. *Mat. Fiz. Lapok*, 38:116–119, 1931.

[41] J. Kurihara, R. Matsumoto, and T. Uyematsu. Relative generalized rank weight of linear codes and its applications to network coding. *IEEE Trans. Inf. Theory*, 61(7):3912–3936, 2015.

[42] P. Lee and E. F. Brickell. An observation on the security of mceliece's public key cryptosystem. *Advances in Cryptology - EUROCRYPT '88 , Lecture Notes in Computer Science, Springer*, 330, 1988.

[43] S.-Y. R. Li, R. W. Yeung, and N. Cai. Linear network coding. *IEEE Trans. Inf. Theory*, 49(2):371–381, 2003.

[44] J. Lieb, R. Pinto, and J. Rosenthal. Convolutional codes. In W. C. Huffman, J.-L. Kim, and P. Solé, editors, *Concise Encyclopedia of Coding Theory*, pages 197–226. Chapman and Hall/CRC, 2021.

[45] P. Loidreau. A new rank metric codes based encryption scheme. *8th International Conference on Post-Quantum Cryptography, PQCrypto 2017*, pages 3–17, 2017.

[46] R. Mahmood, A. Badr, and A. Khisti. Convolutional codes with maximum column sum rank for network streaming. *IEEE Trans. Inf. Theory*, 62(6):3039–3052, 2016.

[47] U. Martínez-Peñas. Skew and linearized reed-solomon codes and maximum sum rank distance codes over any division ring. *J. Algebra*, 504:587–612, 2018.

[48] U. Martínez-Peñas. Theory of supports for linear codes endowed with the sum-rank metric. *Designs, Codes and Cryptography*, 87(10):2295–2320, 2019.

[49] U. Martínez-Peñas and F. Kschischang. Universal and dynamic locally repairable codes with maximal recoverability via sum-rank codes. *IEEE Trans. Inf. Theory*, 65(12):7790–7805, 2019.

[50] U. Martínez-Peñas and F. R. Kschischang. Reliable and secure multishot network coding using linearized reed-solomon codes. *Proc. 56th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2018.

[51] U. Martínez-Peñas and R. Matsumoto. Relative generalized matrix weights codes for universal security on write-tap networks. *IEEE Trans. Inf. Theory*, 64(4):2529–2549, 2018.

[52] R. J. McEliece. A public-key system based on algebraic coding theory. *DSN Progress Report*, (44):114–116, 1978.

[53] R. Meshulam. On the maximal rank in a subspace of matrices. *The Quarterly Journal of Mathematics*, 36(2):225–229, 1985.

[54] D. Napp, R. Pinto, J. Rosenthal, and P. Vettori. Rank metric convolutional codes. *22nd International Symposium on Mathematical Theory of Networks and Systems, Minneapolis*, 2016.

[55] R. W. Nóbrega and B. F. Uchôa-Filho. Multishot codes for network coding: Bounds and a multilevel construction. *Proc. IEEE International Symposium on Information Theory, Seoul*, 2009.

[56] R. W. Nóbrega and B. F. Uchôa-Filho. Multishot codes for network coding using rank-metric codes. *IEEE Wireless Network Coding Conference (WiNC)*, pages 1–6, 2010.

[57] A. Otmani, H. T. Kalachi, and S. Ndjeya. Improved cryptanalysis of rank metric schemes based on gabidulin codes. *Designs, Codes and Cryptography*, 86:1983–1996, 2018.

[58] R. Overbeck. A new structural attack for gpt and variants. *Progress in Cryptology - Mycrypt 2005, Lecture Notes in Computer Science, Springer*, 3715:50–63, 2005.

[59] J. Oxley. *Matroid Theory*. Oxford University Press, 1992.

[60] S. Puchinger, S. Stern, M. Bossert, and R. F. Fischer. Space-time codes based on rank-metric codes and their decoding. *International Symposium on Wireless Communication Systems (ISWCS)*, 2016.

[61] A. Ravagnani. Generalized weights: An anticode approach. *Journal of Pure and Applied Algebra*, Vol. 220(5):1946–1962, 2016.

[62] A. Ravagnani. Rank-metric codes and their duality theory. *Designs, Codes and Cryptography*, 80:197–216, 2016.

[63] R. M. Roth. Maximum-rank array codes and their application to crisscross error correction. *IEEE Trans. Inf. Theory*, 37(2):328–336, 1991.

[64] J. Sheekey. Mrd codes: constructions and connections. *Combinatorics and Finite Fields: Difference Sets, Polynomials, Pseudorandomness and Applications*, pages 255–286, 2019.

[65] M. Shehadeh and F. Kschischang. Rate-diversity optimal multiblock space-time codes via sum-rank codes. *Proc. IEEE International Symposium on Information Theory, Los Angeles*, pages 3055–3060, 2020.

[66] K. Shiromoto. Codes with the rank metric and matroids. *Designs, Codes and Cryptography*, 87:1765–1776, 2019.

[67] D. Silva, F. R. Kschischang, and R. Kötter. A rank-metric approach to error control in random network coding. *IEEE Trans. Inf. Theory*, 54(9):3951–3967, 2008.

[68] R. C. Singleton. Maximum distance q-nary codes. *IEEE Trans. Inf. Theory*, 10:116–118, 1964.

[69] G. Szárnyas. Graphs and matrices: A translation of “Graphok és matrixok" by Dénes König (1931). Preprint, 2020. arXiv:2009.03780.

[70] V. Tarokh, N. Seshadri, and A. R. Calderbank. Space-time codes for high data rate wireless communication: performance criterion and code construction. *IEEE Trans. Inf. Theory*, 44(2):744–765, 1998.

[71] A. Wachter-Zeh, M. Stinner, and V. Sidorenko. Convolutional codes in rank metric with application to random network coding. *IEEE Trans. Inf. Theory*, 61(6):3199–3213, 2015.

[72] Z. X. Wan. A proof of the automorphisms of linear groups over a sfield of characteristic 2. *Scientia Sinica*, (11):1183–1194, 1978.

[73] V. K. Wei. Generalized hamming weights for linear codes. *IEEE Trans. Inf. Theory*, 37(5):1412–1418, 1991.

[74] D. J. A. Welsh. *Matroid Theory.* Academic Press, 1976.