UNIVERSITÉ DE NEUCHÂTEL

Properties and Constructions of Codes with the Rank and the Subspace Metric

THÈSE DE DOCTORAT

présenté à la Faculté des Sciences de l'Université de Neuchâtel par

Alberto Ravagnani

et soutenue avec succes le 1er Septembre 2016 devant le jury composé par:

Prof. Dr. Elisa Gorla, Université de Neuchâtel (directrice de thèse)
Dr. Hugues Mercier, Université de Neuchâtel (rapporteur)
Prof. Dr. Joachim Rosental, Universität Zürich (rapporteur)
Prof. Dr. Alain Valette, Université de Neuchâtel (rapporteur)

Institut de Mathématiques, Université de Neuchâtel
Emile-Argand 11, CH-2000 Neuchâtel (Suisse)

UNIVERSITÉ DE NEUCHÂTEL

Faculté des sciences
Secrétariat-décanat de Faculté
Rue Emile-Argand 11
2000 Neuchâtel - Suisse
Tél: + 41 (0)32 718 2100
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

Monsieur Alberto RAVAGNANI

Titre:

"Properties and Constructions of Codes with the Rank and the Subspace Metric"

sur le rapport des membres du jury composé comme suit:

- Prof. Elisa Gorla, directrice de thèse, Université de Neuchâtel, Suisse
- Dr Hugues Mercier, Université de Neuchâtel, Suisse
- Prof. Joachim Rosenthal, Université de Zürich, Suisse
- Prof. Alain Valette, Université de Neuchâtel, Suisse

Neuchâtel, le 8 septembre 2016

Le Doyen, Prof. R. Bshary

Summary

In 2000 Ahlswede, Cai, Li, and Yeung discovered that employing coding techniques in network transmissions at the intermediate nodes of the network may give substantial gains in information throughput. These results originated a new research field, called *network coding*, concerned with efficiency and reliability of communications over networks. Network coding started to draw the attention of the mathematical community in 2008, when Kötter and Kschischang proposed a rigorous mathematical setup for errors and erasures correction over networks. Their approach is based on rank-metric and subspace codes, mathematical objects that guarantee the reliability of a network communication.

In this dissertation we concentrate on mathematical problems motivated by network coding applications, studying structural properties and constructions of rank-metric and subspace codes.

In the first part of the dissertation we investigate constructions of subspace codes. We start presenting a family of codes, which we call *partial spread codes*, that have maximum correction capability and asymptotically optimal cardinality. We show that partial spread codes exist for all parameters, that are maximal with respect to containment, and that can be efficiently decoded.

Then we concentrate on *equidistant codes*, i.e., codes where every two codewords are at the same distance. We provide an almost complete classification of such codes, proving in particular that the optimal ones have a very simple structure. Then we show how to construct equidistant codes of asymptotically optimal cardinality, and how to decode them efficiently.

Finally, we focus on a specific technique that produces subspace codes of large cardinality (the so-called *multilevel construction*) and study a related mathematical conjecture by T. Etzion and N. Silberstein concerning matrices over finite fields with given shape and rank bounded from below. We establish the conjecture in the cases that are most relevant from the point of view of network coding, and use our results to produce new examples of subspace codes with the largest known cardinality for their parameters. We also investigate the Etzion-Silberstein conjecture over algebraically closed fields, and disprove it in this case using methods from algebraic geometry.

The second part of the dissertation is devoted to structural properties of rank-metric codes. We start comparing the duality theories of Delsarte and Gabidulin rank-metric codes, proving that the former generalizes the latter. Then we give a simple proof for the MacWilliams identities for the general family of Delsarte codes, originally established by Delsarte using sophisticated methods from combinatorics. We also show that the most important properties of rank-metric codes can be regarded as simple consequences of such identities. In a second part of the chapter we study optimal anticodes in the rank-metric, and prove some new bounds on the parameters of rank-metric codes, characterizing those attaining them. As an application of our results, we answer some questions concerning matrices over finite fields.

Then we introduce and study algebraic invariants for rank-metric codes (which we call *generalized Delsarte weights*), that extend known invariants defined on the special sub-class of Gabidulin rank-metric codes. We show that our invariants characterize optimal codes and anticodes, and that behave well with respect to the duality theory of rank-metric codes. More precisely, we prove that

the generalized Delsarte weights of a code and the generalized Delsarte weights of its dual code determine each other via a precise relation, which we explicitly derive.

Finally, in the last chapter we investigate some connections between the theory of codes over finite abelian groups and the combinatorial theory of finite posets and lattices, extending in particular some results for classical and rank-metric codes established by other authors to a more general framework. More precisely, we introduce a general family of weight functions on finite abelian groups that give rise to invertible MacWilliams identities for additive codes, and study such weight functions employing lattice theory methods. This will also allow us to provide a computationally effective viewpoint on the theory of MacWilliams identities for codes over groups.

Throughout the whole dissertation the main emphasis is on the mathematical aspects of the problems under study.

Keywords: coding theory, network coding, rank-metric code, subspace code, rank distance, subspace distance, equidistant code, matrix profile, multilevel construction, MacWilliams identities, enumerative combinatorics, anticode, generalized weights, lattice (poset), codes over groups.

Résumé

En 2000, Ahlswede, Cai, Li et Yeung ont découvert que l'utilisation de techniques de codage dans la transmission des données aux niveau des noeuds intermédiaires d'un réseaux peut significativement augmenter le débit d'information transmis. Ces résultats sont à l'origine d'une nouvelle branche de recherche, appelée *Network coding*, qui s'occupe de l'efficacité et de la fiabilité des communications sur les réseaux.

La théorie des codes pour les réseaux a commencé à attirer l'attention de la communauté mathématique lorsqu'en 2008 Kötter et Kschischang ont proposé un setup mathématique rigoureux pour la correction des erreurs et des effacements sur les réseaux. Leur approche est basée sur deux classes de codes correcteurs, appelées *rank-metric codes* et *subspace codes*.

Dans cette thèse, nous nous concentrons principalement sur des problèmes mathématiques motivés par des applications en *network coding*. Plus précisement, on étudie des propriétés structurelles et des constructions de *rank-metric codes* et de *subspace codes*.

Dans la première partie de la thèse, nous étudions differentes constructions de *subspace codes*. Nous commençons avec une famille de codes, que nous appelons *partial spread codes*, qui ont une capacité de correction maximale et cardinalité asymptotiquement optimale. Nous montrons que les *partial spread codes* existent pour tous les paramètres, sont maximales par rapport à l'inclusion et qui peuvent être décodés efficacement.

Ensuite, nous nous concentrons sur les *equidistant codes*, une classe de *subspace codes* où deux éléments du code sont à égale distance l'un de l'autre. Nous fournissons une classification presque complète de tels codes, et montrons en particulier que les *equidistant codes* optimaux ont une structure très simple. Puis, nous montrons comment construire des *equidistant codes* de cardinalité asymptotiquement optimale et comment les décoder de manière efficace.

Enfin, nous nous concentrons sur une technique spécifique qui produit des *subspace codes* de grande cardinalité (la *multilevel construction*) et y étudions une conjecture énoncée par T. Etzion et N. Siberstein concernant les matrices sur les corps finis avec un profil donné et dont le rang est borné par une constante. Nous prouvons la conjecture dans les cas les plus importants du point de vue du *network coding* et utilisons nos résultats pour construire de nouveaux *subspace codes* avec la plus grande cardinalité connue pour leurs paramètres. Nous étudions également la conjecture de Etzion-Silberstein sur les corps algébriquement fermés et montrons que dans ce cas elle est fausse. Pour cela, nous utilisons des méthodes de géométrie algébrique.

La deuxième partie de la thèse est dediée aux propriétés structurelles des *rank-metric codes*. Nous comparons les deux théories de la dualité des codes de Delsarte et de Gabidulin et montrons que la première généralise la seconde. Ensuite, nous donnons une preuve simple des identités de MacWilliams pour la famille générale des codes de Delsarte. Ces identités ont été montrées par Delsarte en utilisant des méthodes sophistiquées de combinatoire.

Nous montrons également que les propriétés les plus importantes des *rank-metric codes* peuvent être vues comme de simples conséquences de ces identitées. Dans la deuxième partie du chapitre,

nous étudions les anticodes optimaux pour la métrique du rang, et obtenons de nouvelles bornes pour les paramètres des *rank-metric codes*. Nous décrivons également les codes qui atteignent ces bornes. Comme application de nos résultats, nous répondons à des questions de combinatoire concernant les matrices sur les corps finis.

Ensuite, nous définissons et étudions des invariants algébriques pour les *rank-metric codes* (que nous appelons *Delsarte generalized weights*) qui généralisent des invariants connus définis pour la sous-classe spéciale des codes de Gabidulin. Nous montrons que nos invariants décrivent les codes et anticodes optimaux et étudions leur comportement par rapport à la théorie de la dualité des *rank-metric codes*. Plus précisément, nous montrons que les *Delsarte generalized weights* d'un code et les *Delsarte generalized weights* de son code dual se déterminent les uns les autres via une relation précise que nous décrivons explicitement.

Finalement nous examinons dans le dernier chapitre certains liens entre la théorie des codes sur les groupes abéliens finis et la théorie combinatoire des ensembles partiellement ordonnés. Nous généralisons des résultats pour les codes classiques et les *rank-metric codes* établies par d'autres auteurs. Plus précisément, nous définissons une famille générale des *fonctions poids* sur les groupes abéliens finis qui donnent des identités de MacWilliams inversibles pour les codes additifs. Nous étudions ces fonctions poids en utilisant des méthodes de la théorie des treillis. Cela nous permettra également de fournir une métodologie efficace pour obtenir les identités de MacWilliams pour les codes sur les groupes.

Tout au long de la thèse, l'accent est mis sur les aspects mathématiques des différent problèmes traités.

Mots clés: théorie des codes, codes pour les réseaux, rank-metric code, subspace code, métrique du rang, subspace distance, code équidistant, profil d'une matrice, multilevel construction, identités de MacWilliams, combinatoire énumérative, anticode, poids généralisés, théorie des treillis (ensembles partiellement ordonnés), codes sur le groupes.

Acknowledgments

First of all, I would like to express my vivid gratitude to my advisor, Elisa Gorla, for the incredible work she did with me in these four years. Elisa, you have been the best supervisor I could ever imagine! Your knowledge, dedication, hard work and ideas have been an infinite source of inspiration for me. This work would not have been possible without your support and guidance.

Your enthusiasm and positive attitude made these years in Neuchâtel not just a period of intense study and research, but also an extremely enjoyable experience from a personal point of view.

You have always valued my opinions and thoughts, encouraging me to pursue my scientific, professional and personal objectives. I am grateful for the very concrete support you continuously provided throughout my studies: I really had incredible opportunities as a PhD student.

Your daily example taught me how to conduct mathematical research, and the value of other important aspects of the research activity, such as giving talks, writing articles, participating to conferences and meetings, collaborating with colleagues, and enriching my background with knowledge from different areas of mathematics. You taught me to be critical about my work, and took care of every aspect of my scientific and professional development in the best possible way. All of this made me a much more mature and independent researcher.

I would also like to thank you for having shared with me your personal viewpoint on many occasions, helping me to avoid mistakes more than once. Your opinions and comments made me think about myself in a very constructive way.

I am grateful for all our discussions about mathematics, research, and many other topics. The incredible amount of time and energy you dedicated to me went way beyond your responsibilities as an advisor. I always felt you believed in me, and truly cared about my future. This helped me very much throughout these four years to be self-confident, and to take on my PhD studies with optimism and enthusiasm. As you know me, you can certainly imagine how important this must have been to me. I really appreciated the patience you had with me on several occasions: you always found time to discuss about scientific, professional and personal issues, even when you were very busy with other tasks.

Your friendly attitude and the way you organize your research group made me feel home at work every single day. I am convinced that this had a strong positive impact on my approach to research and work in general. I enjoyed everything I did in collaboration with you: I will really miss all our mathematics discussions, and the nice conversations we had on several occasions.

I would also like to thank the friends who shared their office with me in these four years in Neuchâtel: Giulia, Hiram, and Alessio. You have been my second family in Switzerland. I really enjoyed all our conversations about life, research and mathematics. I could always count on you for a friendly advice and support. In particular, I am grateful to Giulia, who has been my officemate for more than three years, and listened to me whenever I had a personal issue that I wanted to share. You have been always available whenever I needed help.

I would like to thank all the researchers who supported me throughout my PhD studies, sharing their valuable opinion and experience. In particular, I am grateful to Joachim Rosenthal for the support and advice he provided on several occasions. I would like to thank very much Alain Valette, Joachim Rosenthal and Hugues Mercier for accepting to be part of my thesis committee.

I also want to express my vivid gratitude to all the researchers who discussed with me about mathematics in Neuchâtel and at international conferences, sharing their viewpoint and suggesting interesting ideas. In particular, I am grateful to Eimear Byrne for her enthusiastic support and valuable opinions, and for proposing a very interesting collaboration.

A very special "Thank You!" goes to Eleonora, who is the primary source of happiness in my life, and the best partner I can imagine. Throughout these four years you have always showed interest and enthusiasm towards what I was doing, and made me feel special in every circumstance. I feel you know me much better than I know myself, and that I can count on you for any personal problem. Your opinions and comments made me think about myself on several occasions, without feeling judged. This helped me to improve many aspects of my personality, and to become a better person.

I wish to express my gratitude to my family, and in particular to my parents, Daniela and Maurizio. You always made me feel your support and enthusiasm for what I was studying, encouraging me to pursue my inclinations and interests. You participated in every event that was important to me, and I could count on your concrete help whenever I encountered difficulties.

Finally, I would like to thank my colleagues of the Mathematics Institute of the University of Neuchâtel and all my friends, for making these four years in Neuchâtel a very delightful experience from a personal viewpoint. In particular, I would like to thank Relinde, Josua, Camilo, Vincenzo, Corina, Johannes, Gizem, Alex, Linus, Darya, Natalia, Marek, Ana, and Alex.

During my graduate studies I was supported by the Mathematics Institute of the University of Neuchâtel and by the Swiss National Science Foundation. I would also like to acknowledge the financial support provided by the Swiss Mathematical Society, the ICT COST action in *Random Network Coding and Designs over GF(q)*, the Society for Industrial and Applied Mathematics (SIAM), the Swiss Doctoral School (CUSO) and the Horizon 2020 programme.

List of Symbols and Notation

$\mathbb{N}$	The natural numbers (with zero)
$\mathbb{Z}$	The integers
$\mathbb{Q}$	The rationals
$\mathbb{R}$	The reals
$\mathbb{C}$	The complex numbers
$[n]$	The set $\{1, ..., n\}$ for $n \in \mathbb{N}$
$\binom{s}{t}$	The binomial coefficient of s and t
$\mathbb{F}_q$	The finite field with q elements, with q a prime power
d_{rk}	The rank distance of matrices
d_{G}	The rank distance of vectors with entries from a field extension $\mathbb{F}_{q^m}$
d_{s}	The subspace distance
d_{H}	The Hamming distance
$\mathrm{Mat}_{k\times m}(\mathbb{F})$	The space of $k \times m$ matrices over a field $\mathbb{F}$ (sometimes just Mat)
$\mathrm{rowsp}(M)$	The rowspace of the matrix M
$\mathrm{colsp}(M)$	The columnspace of the matrix M
M^t	The transpose of the matrix M
$\mathrm{RRE}(M)$	The reduced row echelon form of the matrix M
$\mathrm{RRE}(X)$	The reduced row echelon form of the vector space X
$\begin{bmatrix} s \\ t \end{bmatrix}_q$	The q-binomial coefficient of s and t (subscript q often omitted)
$\mu_{\mathcal{L}}(\cdot, \cdot)$	The Möbius function of the poset $\mathcal{L}$

Introduction

In this dissertation we investigate constructions and mathematical properties of error-correcting codes endowed with the rank and the subspace metric. Our motivation is linear network coding, an emerging research field that lies in the intersection of algebra and communication theory, and comes as an answer to the problem of efficient and reliable communications over networks.

Recent studies (see e.g. [14]) estimate that the annual global IP traffic will pass the zettabyte threshold by the end of 2016, and will reach 2.3 zettabytes per year by 2020. Overall, IP traffic will grow at a compound annual growth rate of 22% from 2015 to 2020. Moreover, the number of networked devices on earth will reach 26.3 billion by 2020, up from 16.3 billion in 2015. According to the technology company Cisco, by 2020 approximately 65% of Internet traffic will be carried by content delivery networks. Similar scenarios are envisaged by the European Commission (see [73]). These studies, along with many others, indicate that efficiency and reliability of digital network communications will be crucial issues in the future.

In 2000 it was discovered in [1] that encoding data in network communications gives substantial gains in information throughput. These novel results spawned a new research area called *network coding*, which represents a concrete solution to the increasing bandwidth demand. In [76] it was also demonstrated that implementation of network coding methods is already feasible on certain commercial devices (e.g. on Nokia® N95 phones), and [89] shows that network coding is a promising solution for developing a 5G communication technology. Other potential applications can be found in [69].

The idea behind network coding is quite simple, and can be efficiently illustrated by an example. Assume that a source of information $\mathbf{S}$ attempts to transmit messages $v_1, ..., v_k$ to certain receivers $\mathbf{R}_1, ..., \mathbf{R}_N$. Notice that each of the receivers demands all the messages $v_1, ..., v_k$, which are usually vectors with entries from a finite field $\mathbb{F}_q$. A naive communication strategy would consist in transmitting each message v_i to each of the receivers $\mathbf{R}_j$, as illustrated in Figure 1.

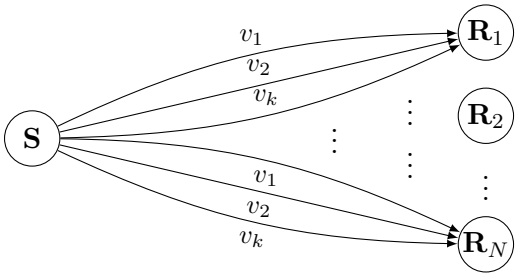


Figure 1: Point-to-point communication

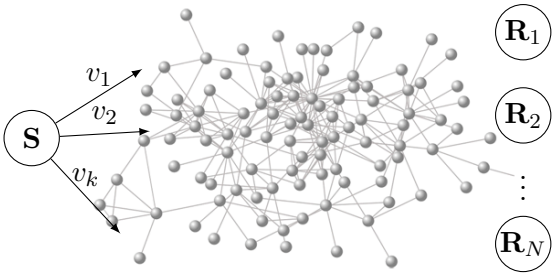


Figure 2: Network multicasting

In many practical situations however, the source and the receivers are connected via a network of intermediate nodes, as shown in Figure 2. This is the case e.g. for peer-to-peer and cellular networks. In this scenario, a network coding strategy consists in injecting the messages in the network, and let the intermediate nodes "cooperate" to spread information faster towards the

receivers. This natural idea allows in practice to considerably increase the amount of transmitted messages per single use of the channel, i.e., the **communication rate**.

Overall, this dissertation is divided into three parts. Chapter 1 contains preliminary definitions and results about network coding, rank-metric codes and subspace codes. In Chapters 2, 3 and 4 we study properties, bounds and constructions of subspace codes. Chapters 5, 6 and 7 are devoted to structural properties and invariants of rank-metric codes. The results contained in Chapter 7 do not hold only for rank-metric codes, but for several different classes of error-correcting codes. They are stated in the general language of codes over finite abelian groups.

A general overview on network coding is given in Chapter 1, where we summarize some foundational contributions from [1], [54], and [62] among many others. In particular, we provide a rigorous graph-theoretic definition of network, and state two major results in theoretical network coding. The first important statement that we illustrate is an upper bound for the multicast rate over a network $\mathcal{N}$ in terms of a mathematical invariant of $\mathcal{N}$ called the *min-cut*. The second fundamental result (the *Max-Flow-Min-Cut Theorem*) states that this upper bound can be actually achieved, over sufficiently large alphabets, by letting the intermediate nodes of the network $\mathcal{N}$ perform linear operations on the inputs they receive, and then forward the output of these operations in the direction of the receivers.

In Chapter 1 we also describe the two fundamental approaches to linear network coding, namely, *coherent* and *random* network coding. In coherent network coding the linear operations performed by the intermediate nodes are carefully designed in order to maximize the information throughput, and are known to source and receivers. In random network coding instead, the operations performed by the nodes are chosen randomly among all possible linear operations, and are unknown. Random network coding is particularly useful in practice as a transmission protocol. Moreover, it achieves the maximum multicast rate with high probability over sufficiently large alphabets.

In this dissertation we concentrate on mathematical aspects of the theory of rank-metric codes and subspace codes, which are the main objects studied throughout the thesis. Rank-metric codes and subspace codes were proposed in [54] and [55] for error correction in the framework of network transmissions. Indeed, a major problem in any digital transmission is that information can get lost or corrupted, resulting in unreliable communications. To solve this issue, source and receivers may agree on a set of "legitimate" messages that can be transmitted over the communication channel, called the (**error correcting**) **code**. When a "non-legitimate" message is obtained, the receiver realizes that some errors occurred in the transmission process. If the number of such errors is small and the code was carefully designed, then it is possible in general to uniquely recover the original message from the corrupted one. This process is called **decoding**.

Clearly, the structure of the error-correcting code selected by source and receivers needs to be compatible with the communication channel that is used. Rank-metric codes are sets of matrices of prescribed size, and can be applied in coherent network coding. Subspace codes are sets of vector subspaces $V \subseteq \mathbb{F}_q^n$ of the same dimension, and are compatible with random network coding. The definitions of rank-metric code and subspace code are motivated more in detail in Section 1.4. In Sections 1.5 and 1.6 we recall their main mathematical properties.

In Chapter 2 we present a code construction that produces subspace codes with the largest possible correction capability for their parameters. Our codes, which we call *partial spread codes*, generalize the *spread codes* proposed in [71] by F. Manganiello, E. Gorla, and J. Rosenthal, and are defined as the vector spaces generated by the rows of matrices having a convenient block structure. Exploiting such specific block description, we are able to provide a closed formula for the cardinality of our codes, and to prove that they are maximal with respect to inclusion. This proves in particular that one cannot enlarge our codes without lowering their correction capability.

Finally, we show how to adapt existing decoding algorithms to partial spread codes, obtaining in particular an efficient decoding algorithm for our codes.

In Chapter 3 we study a class of subspace codes that generalize partial spreads, namely, *equidistant codes*. An equidistant code is a subspace code where every two codewords intersect in the same dimension. They were proposed for use in distributed storage by Etzion and Raviv in [28]. A very simple family of equidistant codes are *sunflowers*, i.e., equidistant codes in which any two codewords intersect exactly in the same vector space. The main result that we present in Chapter 3 is a structural classification of optimal equidistant codes over sufficiently large fields. More precisely, in Theorem 3.24 we show that, for most choices of the parameters, an equidistant code of maximum cardinality is either a sunflower, or the orthogonal of a sunflower (see Section 1.6 for the definition of orthogonal of a subspace code). This proves in particular that the most interesting equidistant codes from an applied viewpoint have a very simple structure. We also show a precise relation between partial spreads and sunflowers, and extend our construction from Chapter 2 to produce sunflowers of asymptotically optimal cardinality. By our classification theorem, this produces in particular equidistant codes of asymptotically optimal cardinality for most choices of the parameters.

In Chapter 4 we concentrate on the so-called *multilevel construction*, a general technique to produce subspace codes proposed by Etzion and Silberstein in [29]. The multilevel construction generalizes the *lifting* procedure introduced in [55], and produces subspace codes combining several rank-metric codes with special properties. More precisely, it relies on the existence of linear spaces of matrices with a Ferrers diagram shape and rank bounded from below by a given parameter δ. The cardinality of the resulting subspace code increases with the dimension of the constituent linear spaces of matrices. As a consequence, from a mathematical viewpoint it is very natural to ask how large these linear spaces can be. This is the main problem that we address in Chapter 4. In [29] Etzion and Silberstein derive a bound on the dimension of such linear spaces, and conjecture that the bound is sharp over any finite field.

We start with a survey of the literature, summarizing the cases in which the Etzion-Silberstein conjecture is known to hold, giving simple proofs. Then we establish several new cases of the conjecture, including those that are most relevant in the context of network coding. Using methods from algebraic geometry, we also show that the Etzion-Silberstein conjecture does not hold over algebraically closed fields. Then we completely solve the natural dual problem of determining the maximum dimension of a linear space of matrices with given profile and rank bounded from above by a given parameter δ. Finally, we combine our results with the multilevel construction from [29], and obtain several examples of subspace codes with the largest known cardinality for their parameters. Our codes were recently included in the database of codes with the best parameters of the University of Bayreuth (see `http://subspacecodes.uni-bayreuth.de/cdctoplist/`).

With Chapter 5 we start the study of structural properties of linear codes endowed with the rank metric. More precisely, Chapter 5 focuses on the duality theory of rank-metric codes. We first compare two families of rank-metric codes, namely, *Delsarte* and *Gabidulin codes*, and prove that the duality theory of Delsarte codes generalizes the duality theory of Gabidulin codes (see Section 1.5 for the definitions). Then we give a simple combinatorial proof for the MacWilliams identities for linear rank-metric codes. Recall that the MacWilliams identities are invertible linear relations between the weight distribution of a code and the weight distribution of the dual code. They were first established in the context of (additive) rank-metric codes by Delsarte in [20] using the theory of association schemes and designs. Our proof for linear rank-metric codes is simpler, and essentially based on a double-counting argument. In the second part of Chapter 5 we prove some new bounds on the parameters of a rank-metric code, and characterize the codes attaining them. Then we define and investigate optimal rank-metric anticodes, which will play a crucial role in Chapter 6 in studying certain algebraic invariants of rank-metric codes.

In the last section of Chapter 5 we also show some applications of the duality theory of rank-metric codes to enumerative combinatorics problems concerning matrices over finite fields. We provide, employing simple arguments, closed formulas for the number of matrices over $\mathbb{F}_q$ whose entries satisfy certain linear conditions. In particular, we answer a generalized question of Stanley concerning matrices with zero diagonal entries (see Corollary 5.37) with a simple method.

The properties of optimal anticodes established in Chapter 5 are exploited in Chapter 6 to define certain algebraic invariants of Delsarte rank-metric codes, which we call *Delsarte generalized weights*. In [57], Kurihara, Matsumoto and Uyematsu define algebraic invariants, called *generalized rank-weights*, for the special sub-class of Gabidulin rank-metric codes. Our algebraic invariants extend those of [57] to the larger family of Delsarte codes. The Delsarte generalized weights of a code are defined in terms of the intersection of the code with optimal linear anticodes, and have interesting mathematical properties. In particular, as we show, they completely characterize optimal rank-metric codes and anticodes, and are compatible with the duality theory of Delsarte codes. More precisely, the Delsarte generalized weights of a code completely determine the Delsarte generalized weights of the dual code via a relation that we explicitly derive. The results of Chapter 6 rely on the properties of optimal anticodes established in Chapter 5.

In the last chapter (Chapter 7) we investigate some connections between coding theory and combinatorics, focusing in particular on the theory of partially ordered sets and lattices. Following e.g. [10], [43] and [92], we define a code as a subgroup $\mathcal{C} \subseteq G$ of a finite abelian group G, and its dual as the character-theoretic annihilator

$$\mathcal{C}^* = \{\chi : G \to \mathbb{C}^*,\ \chi \text{ group homomorphism},\ \chi(g) = 1 \text{ for all } g \in \mathcal{C}\} \subseteq \hat{G}.$$

Recall that if G is a finite abelian group, and $\omega : G \to X$ is any function (where X is a set) then the ω-distribution of a code $\mathcal{C} \subseteq G$ is defined to be the collection $\{W_a(\mathcal{C}, \omega) : a \in X\}$, where $W_a(\mathcal{C}, \omega) := |\{g \in \mathcal{C} : \omega(g) = a\}|$ for all $a \in X$.

As opposed to other setups, in the framework of codes over groups code and dual code are subsets of different ambient spaces, G and $\hat{G}$, that are not canonically isomorphic in general. As a consequence, the distributions of $\mathcal{C}$ and $\mathcal{C}^*$ refer in general to different functions, say ω and τ, defined on G and $\hat{G}$ respectively. A central problem in the area of codes over groups is the following: Construct pairs (ω, τ) of functions on G and $\hat{G}$ such that, for any code $\mathcal{C} \subseteq G$, the ω-distribution of $\mathcal{C}$ and the τ-distribution of $\mathcal{C}^*$ determine each other via an invertible linear transformation, called *MacWilliams identity*. Such a pair is called *compatible*. The problem is motivated by an analogy with the theory of classical codes endowed with the Hamming metric.

In Chapter 7, using techniques from lattice theory, we construct a family of weight functions on finite abelian groups that are compatible, and therefore automatically produce MacWilliams identities for codes over groups. More precisely, we define a regular support as a function, say σ, over a finite abelian group G with values in a graded lattice $\mathcal{L}$ with certain regularity properties. A regular support induces a weight function on G via the rank function of $\mathcal{L}$. Then we show that a regular support σ on G with values in $\mathcal{L}$ induces a regular support σ^* on the character group $\hat{G}$ with values in the dual lattice $\mathcal{L}^*$. This produces in particular a weight function on the character group $\hat{G}$ via the rank function of $\mathcal{L}^*$. In this setup, we prove that the weight functions on G and $\hat{G}$ induced by σ and σ^*, respectively, form a compatible pair. Moreover, we express the corresponding MacWilliams identity in terms of certain combinatorial invariants of the lattice $\mathcal{L}$.

We also show that compatible pairs of weights can be constructed over any finite abelian group, and that the most studied weight functions in coding theory belong, up to equivalence, to the family of weights that we introduce. In all these examples the underlying lattice is very simple, and its combinatorial invariants can be easily computed. This allows in particular to explicitly derive the most important MacWilliams identities in coding theory with a unified combinatorial method. We

also derive some new MacWilliams identities for codes endowed with the homogeneous weight over some simple Frobenius rings.

After having studied MacWilliams identities, we establish an upper bound on the cardinality of (not necessarily additive) codes in finite abelian groups, and call *optimal* the codes whose parameters attain the bound. Then we show that the weight and distance distribution of an optimal code is determined by its parameters. This generalizes a result by Delsarte on the distance distribution of optimal rank-metric codes. We also prove that the dual of an optimal additive code is optimal.

Finally, as an application, we show a concise technique based on lattice regularity to count symmetric and skew-symmetric matrices of given rank over a finite field.

Each chapter of this dissertation contains a more detailed introduction to the contents. The structure of every chapter is outlined in such introductions.

Contents

Chapter 1

Network coding

This first chapter of the dissertation contains a short introduction to network coding, and includes some preliminary definitions and results on rank-metric codes and subspace codes that will be needed in the sequel. It is structured as follows: In Section 1.1 we illustrate the idea that originated network coding as a research field, via the celebrated "Butterfly network". This simple example gives evidence that the information rate of a network communication may be improved by employing coding at the intermediate nodes of the network. In Section 1.2 we present a graph-theoretic model that describes single-source network communications, and state the two major results in theoretical network coding. The so called "random approach" to network coding is described in Section 1.3. Error correction in the context of network communications is treated in Section 1.4, where we also present and motivate the definitions of rank-metric code and subspace code. In Section 1.5 and Section 1.6 we state some preliminary results on rank-metric and subspace codes, which will be the main objects studied in this dissertation. In Section 1.7 we recall some linear algebra definitions.

1.1 The Butterfly network

Network coding can be defined as a branch of mathematics and communication theory concerned with efficient and reliable communications over networks. In this dissertation we concentrate on the scenario where one source of information $\mathbf{S}$ attempts to transmit a collection of messages $v_1, ..., v_k \in \mathbb{F}_q^m$ to multiple receivers $\mathbf{R}_1$,...,$\mathbf{R}_N$ via a network of intermediate nodes. Notice that each of the receivers is interested in all the messages. In communication theory terminology, this is a so-called "multicast" problem. Applications include peer-to-peer and cellular networking, patches distribution, and Long Time Evolution networking. We refer the reader interested in applications and implementations to Chapters 3, 4 and 5 of [69].

The first problem that we address in this chapter is the efficiency of network multicasting, disregarding error correction in the first place. We therefore assume for the moment that our network transmissions are not affected by any noise. Errors and erasures correction will be discussed later in Section 1.4. The main reference for this Chapter is [69, Chapter 1].

In the seminal paper [1], Ahlswede, Cai, Li, and Yeung discovered that the information rate of a network communication may be improved employing coding at the nodes of a network, instead of simply routing the messages. Recall that the **rate** of a communication may be roughly defined as the amount of transmitted messages per single use of the communication channel (see [17] for a rigorous definition). The following example is proposed in [1] to illustrate the phenomenon.

The network in Figure 1.1 has one source $\mathbf{S}$, two receivers $\mathbf{R}_1$ and $\mathbf{R}_2$, and four intermediate nodes connected as shown in the picture. It is called the Butterfly network. Source $\mathbf{S}$ attempts to transmit some messages to both receivers as efficiently as possible.

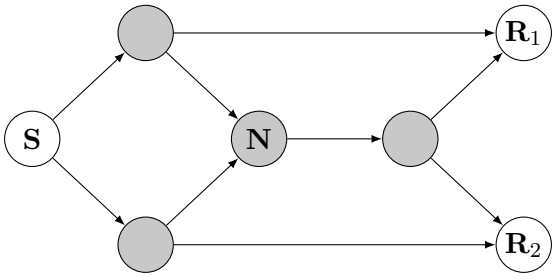


Figure 1.1: The Butterfly network

Employing a classical "routing solution", in time slot 1 the source may emit two messages v_1 and v_2, routing message v_1 to both receivers, and routing message v_2 only to $\mathbf{R}_2$ (see Figure 1.2). Notice that node $\mathbf{N}$ is forced to transmit only one of the two incoming messages, say v_1 without loss of generality. In time slot 2 the source emits messages v_2 and v_3, routing message v_3 to both receivers, and message v_2 only to $\mathbf{R}_1$ (see Figure 1.3). The communication scheme delivers three messages in two time slots, achieving an average rate of 1.5 transmitted messages per channel use in average. One can show that this is the maximum rate that can be achieved employing any routing solution.

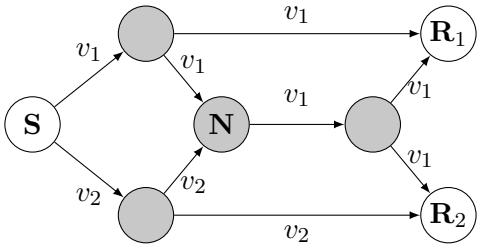


Figure 1.2: Routing solution: time slot 1

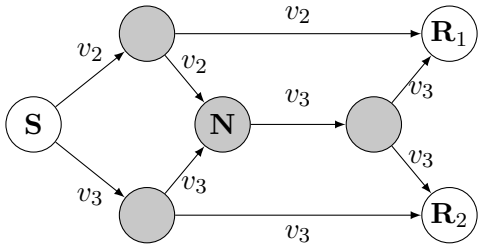


Figure 1.3: Routing solution: time slot 2

In Figure 1.4 a "network coding strategy" is presented that delivers two messages in one time slot, achieving a rate of 2 messages per channel use. This time the node $\mathbf{N}$ is allowed to transmit the sum of the two incoming messages v_1 and v_2, instead of routing only one of the two. Receiver $\mathbf{R}_1$ obtains v_1 and $v_1 + v_2$, and receiver $\mathbf{R}_2$ obtains v_2 and $v_1 + v_2$. So both receivers can easily compute v_1 and v_2. It is possible to show that 2 is the maximum rate that can be achieved with any transmission strategy (see the following Theorem 1.2).

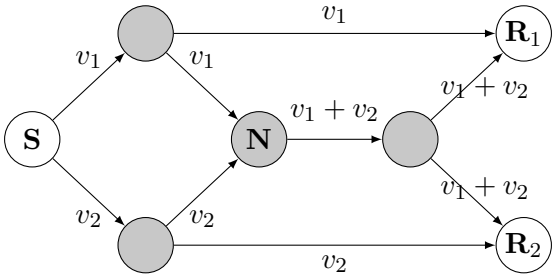


Figure 1.4: A network coding solution

A fundamental result in network coding, which we present in the next section, states that the technique illustrated above can be applied to *any* network, resulting in an optimal general communication strategy for network transmission.

1.2 Linear network coding

In this section we show how a network can be modeled by a directed graph, and state two major results in theoretical network coding. The first theorem that we present is the so-called min-cut bound, which gives an upper bound on the rate of any network transmission in terms of a graph-theoretic invariant of the network. The second result shows that there exist *linear* network coding solutions that achieve the min-cut bound. We start with a formal definition of network.

Definition 1.1 (see [54])**.** A **single-source network** is a 4-tuple $\mathcal{N} = (V, E, \mathbf{S}, R)$ where:

- (V, E) is a finite directed acyclic multigraph,
- $\mathbf{S} \in V$ is the source,
- $R = \{\mathbf{R}_1, ..., \mathbf{R}_N\} \subseteq V$ is the set of receivers, $N \geq 1$.

We also assume the following:

- the source does not have any incoming edge,
- the receivers do not have any outgoing edge,
- there exists a directed path from $\mathbf{S}$ to each of the receivers.

The vertices that are neither the source nor receivers of $\mathcal{N}$ are the **intermediate nodes** of the network. The **messages** that can be transmitted over $\mathcal{N}$ are vectors of given length, say m, with entries from a finite field $\mathbb{F}_q$.

Recall that if s and t are two connected vertices of a directed graph, then an $\{s, t\}$-separating **cut** is a collection of edges, say S, such that any directed path connecting s and t contains a directed edge from S. The minimum cardinality of an $\{s, t\}$-separating cut is denoted by min-cut(s, t). We can now state the major result on the capacity of a network.

Theorem 1.2 (Min-cut bound, [1], Section II)**.** Let $\mathcal{N} = (V, E, \mathbf{S}, R)$ be a single-source network. The information rate of any communication over $\mathcal{N}$ satisfies

$$\text{rate} \leq \min_{\mathbf{R} \in R} \text{min-cut}(\mathbf{S}, \mathbf{R}).$$

A more rigorous formulation and proof for Theorem 1.2 was given later in [56] employing the theory of stochastic processes and entropy functions.

Example 1.3. By Theorem 1.2, the rate of any communication over the Butterfly network of Figure 1.1 is at most 2. Thus the network coding solution illustrated in Figure 1.4 is optimal.

The second fundamental result that we present in this section states that the bound of Theorem 1.2 is achievable employing *linear* network coding over sufficiently large fields, i.e., allowing the intermediate nodes of the network $\mathcal{N} = (V, E, \mathbf{S}, R)$ to perform linear combinations of the received inputs before forwarding them towards the receivers. Let us describe such transmission strategy in more mathematical terms.

In order to transmit messages $v_1, ..., v_k \in \mathbb{F}_q^m$ the source $\mathbf{S}$ organizes them into a **message matrix** M as follows:

$$M := \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{bmatrix} \in \mathrm{Mat}_{k\times m}(\mathbb{F}_q).$$

If $\sigma_1, ..., \sigma_k$ are the outgoing edges from $\mathbf{S}$, then the j-th row of M is transmitted over edge σ_j. Let $\mathbf{N}$ be an intermediate node with i incoming edges $\varepsilon_1, ..., \varepsilon_i$ and o outgoing edges $\eta_1, ..., \eta_o$. In practice, the node $\mathbf{N}$ organizes incoming inputs $r_1, ..., r_i \in \mathbb{F}_q^m$ into an $i \times m$ input matrix $Y(\mathbf{N}) \in \mathrm{Mat}_{i\times m}(\mathbb{F}_q)$ having $r_1, ..., r_i$ as rows. The input r_j is collected over the incoming edge ε_j. Then $\mathbf{N}$ performs linear combinations of the received messages, i.e., linear combinations of the rows of $Y(\mathbf{N})$. This corresponds to a matrix multiplication on the left:

$$C(\mathbf{N}) \cdot Y(\mathbf{N}) \in \mathrm{Mat}_{o\times m}(\mathbb{F}_q),$$

where the matrix $C(\mathbf{N}) \in \mathrm{Mat}_{o\times i}(\mathbb{F}_q)$ keeps track of the operations performed by $\mathbf{N}$. Each row of the output matrix $O(\mathbf{N}) := C(\mathbf{N}) \cdot Y(\mathbf{N})$ is then sent over an outgoing edge from $\mathbf{N}$. More precisely, the j-th row of $O(\mathbf{N})$ is sent over the outgoing edge η_j.

Since the linear operation performed by the intermediate nodes of the network all correspond to matrix multiplications of the left, each receiver $\mathbf{R}$ obtains as input a matrix of the form

$$Y(\mathbf{R}) = G(\mathbf{R}) \cdot M,$$

where $G(\mathbf{R})$ is the **global transfer matrix** at $\mathbf{R}$ that describes all the linear operation performed by the intermediate nodes. Clearly, if $G(\mathbf{R})$ is left-invertible then $\mathbf{R}$ can compute its left-inverse and recover the message matrix M, i.e., the original messages $v_1, ..., v_k$.

In [62] it was shown that for all integers $k \leq \min_{\mathbf{R}\in R} \text{min-cut}(\mathbf{S}, \mathbf{R})$ it is possible to make each $G(\mathbf{R})$ a $k \times k$ invertible matrix, provided that q is sufficiently large (here k is the number of transmitted messages). This proves in particular that linear network coding achieves the maximum information rate over sufficiently large fields.

Theorem 1.4 ([62] and [69], Theorem 1 of Chapter 1)**.** Let $\mathcal{N} = (V, E, \mathbf{S}, R)$ be a single-source network. A multicast rate of $\min_{\mathbf{R}\in R} \text{min-cut}(\mathbf{S}, \mathbf{R})$ is achievable, for sufficiently large q, with linear network coding.

The proof of Theorem 1.4 provided in [69] is an elegant argument based on the algebraic approach to network coding proposed in [56].

In network coding terminology, the operations performed by the intermediate nodes of a network $\mathcal{N}$ are called the **network code**, and thus Theorem 1.4 can be re-stated as follows: Every single-source network $\mathcal{N}$ admits a linear network code that achieves the maximum rate of Theorem 1.2, provided that the base field for the messages, $\mathbb{F}_q$, is sufficiently large.

1.3 Random linear network coding

In [49], Ho, Médard, Kötter, Karger, Effros, Shi and Leong showed that in order to produce a good network code for a given single-source network $\mathcal{N}$ it suffices to let the intermediate nodes perform random linear operations on the inputs they receive, instead of carefully designed operations.

The random approach, which we now briefly describe, is particularly useful in practice, and can be employed also as a transmission protocol.

Let $\mathcal{N} = (V, E, \mathbf{S}, R)$ be a single-source network, and let M denote the message matrix sent by the source $\mathbf{S}$. As in Section 1.2, each receiver $\mathbf{R}$ obtains a matrix of the form

$$Y(\mathbf{R}) = G(\mathbf{R}) \cdot M,$$

where $G(\mathbf{R})$ is the global transfer matrix at $\mathbf{R}$. This time the linear operations performed by the nodes are chosen at random, and therefore the global matrix $G(\mathbf{R})$ is unknown to the receiver $\mathbf{R}$, and not necessarily left-invertible.

To solve this practical issue, the authors of [49] propose to slightly modify the communication scheme as follows. Assume $k = \min_{\mathbf{R} \in R} \text{min-cut}(\mathbf{S}, \mathbf{R})$. Instead of just sending the message matrix $M \in \text{Mat}_{k \times m}(\mathbb{F}_q)$ as in Section 1.2, the source $\mathbf{S}$ transmits the matrix $[I_k \ M] \in \text{Mat}_{k \times (k+m)}(\mathbb{F}_q)$, where I_k denotes the identity $k \times k$ matrix. In other words, each message v_i is sent together with a **packet header** e_i in front, where $\{e_1, ..., e_k\}$ is the canonical basis of $\mathbb{F}_q^k$. In this way the receiver $\mathbf{R}$ obtains as input the matrix

$$Y(\mathbf{R}) = G(\mathbf{R}) \cdot [I_k \ M] = [G(\mathbf{R}) \ \ G(\mathbf{R}) \cdot M].$$

Now the first k columns of $Y(\mathbf{R})$ yield the transfer matrix $G(\mathbf{R})$. Notice that the role of the identity matrix in this approach is just to keep track of the operations performed in the network by the intermediate nodes. A major result in this context states that the matrix $G(\mathbf{R})$ is left-invertible with probability that goes to 1 as q grows. More precisely, the following hold.

Theorem 1.5 ([69], page 20)**.** Let $\mathcal{N} = (V, E, \mathbf{S}, R)$ be a single-source network. A randomly chosen linear network code over $\mathcal{N}$ achieves the maximum multicast rate with probability

$$\mathbb{P}[\text{success}] \geq \left(1 - \frac{|R|}{q}\right)^{|E|}.$$

An interesting and original approach to random network coding based on subspaces transmission was later proposed by Kötter and Kschischang in [54]. Assume that the message matrix M is sent by the source without packet headers. As shown before, a receiver $\mathbf{R}$ obtains the matrix

$$Y(\mathbf{R}) = G(\mathbf{R}) \cdot M,$$

where the transfer matrix $G(\mathbf{R})$ is random and left-invertible with high probability. In particular, the matrices M and $G(\mathbf{R}) \cdot M$ have the same rowspace with high probability. This simple observation suggests to transmit over the network "message spaces" rather than "message matrices". As a natural consequence, one may define the actual message to be the vector space spanned by the rows of M, instead of the matrix M itself. Notice that this strategy also eliminates the necessity of transmitting packet headers, thereby reducing the length of the vectors sent over the network. As we will see in the next sections, the subspace transmission approach is particularly interesting from the point of view of error correction.

1.4 Error correction

We now concentrate on error correction in network communications, and consider the scenario where some of the information packets transmitted by the source may get corrupted or lost in the transmission process. These two phenomena are called **errors** and **erasures**, respectively.

We start by investigating coherent linear network coding, assuming that the transfer matrix at any receiver is known, as described in Section 1.2. Following [84], when linear network coding

is employed at the nodes of a single-source network, the channel equation at any receiver has the form

$$Y = GM + DZ,$$

where Y is the matrix obtained by the receiver, $M \in \mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ is the message matrix, G is the invertible transfer matrix, Z is an error matrix and D is a matrix that describes the propagation of the errors in the network. In [84, Lemma 4] Silva and Kschischang argue that the "minimum effort" needed to transform the message matrix M into the matrix Y (of the same size) is measured by the quantity

$$\Delta_G(M, Y) = \mathrm{rk}(Y - GM) = \mathrm{rk}(G^{-1}Y - M),$$

where G^{-1} denotes the inverse of G. Thus if $\mathcal{C}$ denotes the set of admissible message matrices, a receiver may attempt to "repair" the received matrix Y employing the following simple algorithm:

1. compute $N := G^{-1}Y$,
2. find $\hat{M} \in \mathcal{C}$ such that $\mathrm{rk}(N - \hat{M})$ is minimum.

The process of recovering the original matrix from the corrupted one is called **decoding**. Now if the number of corrupted packets is small and $\mathcal{C}$ is properly designed, then $\hat{M} = M$, the original message matrix. More precisely, the following hold.

Proposition 1.6. Let $\mathcal{C} \subseteq \mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ be a set of matrices with $|\mathcal{C}| \geq 2$, and define

$$d_{\mathrm{rk}}(\mathcal{C}) := \min\{\mathrm{rk}(N - M) : N, M \in \mathcal{C},\ N \neq M\}.$$

Denote by M the matrix that is sent over the network, and let $Y = GM + DZ$ be the received matrix. Then M is the unique element of $\mathcal{C}$ such that $\mathrm{rk}(G^{-1}Y - M)$ is minimum, provided that $\Delta_G(M, Y) \leq \lfloor (d_{\mathrm{rk}}(\mathcal{C}) - 1)/2 \rfloor$.

Proposition 1.6 immediately follows from the fact that the map that sends a pair of matrices $(N, M) \in \mathrm{Mat}_{k\times m}(\mathbb{F}_q) \times \mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ to the rank of their difference is a distance function on $\mathrm{Mat}_{k\times m}(\mathbb{F}_q)$. Proposition 1.6 also motivates the following formal definition of rank-metric code.

Definition 1.7. Let q be a prime power, and let $k, m \geq 1$ be integers. A q-ary **rank-metric code** is a non-empty subset $\mathcal{C} \subseteq \mathrm{Mat}_{k\times m}(\mathbb{F}_q)$. The **rank distance** between matrices $M, N \in \mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ is $d_{\mathrm{rk}}(M, N) := \mathrm{rk}(M - N)$, and the **minimum distance** of a rank-metric code with $|\mathcal{C}| \geq 2$ is $d_{\mathrm{rk}}(\mathcal{C}) := \min\{d_{\mathrm{rk}}(M, N) : M, N \in \mathcal{C},\ M \neq N\}$.

Codes endowed with the rank distance were studied for the first time by Delsarte in [20] for combinatorial interest before network coding. The author mostly concentrates on codes that are closed under addition, or $\mathbb{F}_q$-linear. For this reason $\mathbb{F}_q$-linear rank-metric codes will be also called "Delsarte codes" in the sequel. More details on rank-metric codes will be given in Section 1.5.

In the reminder of the section we focus on error correction in random linear network coding, illustrating the algebraic framework proposed in [54]. As explained in Section 1.3, in this context a message is a vector space over $\mathbb{F}_q$. This motivates the following definition of subspace code.

Definition 1.8. Let q be a prime power, and let $n > 1$ be an integer. Denote by $\mathcal{P}(\mathbb{F}_q^n)$ the **projective geometry** of $\mathbb{F}_q^n$, i.e., the set of all the vector subspaces of $\mathbb{F}_q^n$. A q-ary **subspace code** of **length** n is a subset $\mathcal{C} \subseteq \mathcal{P}(\mathbb{F}_q^n)$ with $|\mathcal{C}| \geq 2$. The **maximum dimension** of $\mathcal{C}$ is denoted and defined by $\ell(\mathcal{C}) := \max_{V\in\mathcal{C}} \dim(V)$.

The elements of a subspace code $\mathcal{C}$ should be regarded as the legitimate "message spaces" that can be emitted by the source over a network $\mathcal{N}$.

Errors and erasures in the context of subspaces are modeled as follows. If $1 \leq e < n$ is an integer, an e-**erasure** on an element $V \in \mathcal{P}(\mathbb{F}_q^n)$ such that $\dim(V) \geq e$ is the projection of V onto an e-dimensional subspace $\mathcal{H}_e(V) \subseteq V$. In other words, an e-erasure $\mathcal{H}_e$ replaces the vector space V with an e-dimensional subspace of V. Notice that $\mathcal{H}_e$ is not a deterministic function, but just a notation for an erasure operator. A t-dimensional **error** E on an element $V \in \mathcal{P}(\mathbb{F}_q^n)$ corresponds to the direct sum $V \oplus E$, where $E \in \mathcal{P}(\mathbb{F}_q^n)$, $\dim(E) = t$ and $E \cap V = \{0\}$.

Now assume that an element $V \subseteq \mathcal{P}(\mathbb{F}_q^n)$ is sent by the source over a network. As shown in [54], a receiver obtains a vector space of the form

$$U = \mathcal{H}_e(V) \oplus E,$$

where $1 \leq e \leq \dim(V)$, $\mathcal{H}_e$ is an e-erasure operator, and $E \in \mathcal{P}(\mathbb{F}_q^n)$ is the error. The **decoding** problem in this context consists in recovering V from U. The following metric on $\mathcal{P}(\mathbb{F}_q^n)$ was proposed in [54] for subspace correction.

Definition 1.9. The **subspace distance** on $\mathcal{P}(\mathbb{F}_q^n)$ is the map $d_{\mathrm{s}} : \mathcal{P}(\mathbb{F}_q^n) \times \mathcal{P}(\mathbb{F}_q^n) \to \mathbb{N}$ defined, for any $U, V \in \mathcal{P}(\mathbb{F}_q^n)$, by $d_{\mathrm{s}}(U, V) := \dim(U) + \dim(V) - 2\dim(U \cap V)$. The **minimum distance** of a subspace code $\mathcal{C} \subseteq \mathcal{P}(\mathbb{F}_q^n)$ is $d_{\mathrm{s}}(\mathcal{C}) := \min\{d(U, V) : U, V \in \mathcal{C}, U \neq V\}$.

The correction capability of a subspace code endowed with the subspace distance is described by the following result.

Theorem 1.10 ([54], Theorem 2)**.** Let $\mathcal{C} \subseteq \mathcal{P}(\mathbb{F}_q^n)$ be a subspace code of minimum subspace distance d. Assume that an input $V \in \mathcal{C}$ and its output $U \in \mathcal{P}(\mathbb{F}_q^n)$ are related by $U = \mathcal{H}_e(V) \oplus E$, where $e \leq \ell(\mathcal{C})$, $\mathcal{H}_e(V)$ is an e-erasure, and $E \in \mathcal{P}(\mathbb{F}_q^n)$ is an error with $t := \dim(E)$. A minimum subspace distance decoder corrects U in V, provided that $2(t + \ell(\mathcal{C}) - e) < d$.

Theorem 1.10 may be regarded as the analogue of Proposition 1.6 in the context of subspace codes. Notice moreover that these two results allow one to translate problems about error correction in network communications into precise questions about matrices and vector spaces. The last two sections of this introductory chapter are devoted to mathematical preliminaries on rank-metric codes and subspace codes.

1.5 Rank-metric codes

In this section we describe the main properties of rank-metric codes. In particular, we introduce Delsarte and Gabidulin codes. As already observed, codes endowed with the rank metric existed before network coding in the mathematical literature (see in particular [20] and [32]). Codes equipped with the rank metric were independently re-discovered and applied in the context of network coding by Kötter and Kschischang in [54] and [55].

Notation 1.11. Throughout this section, q denotes a prime power, and k and m are integers with $0 < k \leq m$ without loss of generality. In this dissertation we mainly focus on linear rank-metric codes. All dimensions in this section are computed over $\mathbb{F}_q$, unless specified differently.

We start with a simple bound on the cardinality of a rank-metric code, and include a short proof for completeness.

Proposition 1.12. Let $\mathcal{C} \subseteq \mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ be rank-metric code with $|\mathcal{C}| \geq 2$. We have

$$\log_q |\mathcal{C}| \leq m(k - d_{\mathrm{rk}}(\mathcal{C}) + 1).$$

Proof. Set $d := d_{\mathrm{rk}}(\mathcal{C})$ for ease of notation. Let $\pi : \mathcal{C} \to \mathrm{Mat}_{(k-d+1)\times m}(\mathbb{F}_q)$ be the map that sends a matrix $M \in \mathcal{C}$ to the matrix having as rows the last $k - d + 1$ rows of M. Since $\mathcal{C}$ has minimum distance d, the map π is injective. Therefore $|\mathcal{C}| = |\pi(\mathcal{C})| \leq q^{m(k-d+1)}$, and the result follows. □

Definition 1.13. A code attaining the bound of Proposition 1.12 is called a **maximum rank distance** code (**MRD** code in short). The zero code is also considered MRD.

In [20] Delsarte showed that for any admissible choice of the parameters q, k m and d there exists a linear rank-metric code $\mathcal{C} \subseteq \mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ that attains the bound of Proposition 1.12.

Theorem 1.14 ([20], Theorem 5.4)**.** Let q be any prime power, and let k, m and d be integers with $1 \leq d \leq k \leq m$. There exists an $\mathbb{F}_q$-linear rank-metric code $\mathcal{C} \subseteq \mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ with minimum distance d and $\dim(\mathcal{C}) = m(k - d + 1)$.

In Remark 1.33 we will provide a simple proof for Theorem 1.14 based on the theory of Gabidulin codes.

Definition 1.15. A **Delsarte code** is an $\mathbb{F}_q$-linear rank-metric code $\mathcal{C}$. The **dual** of $\mathcal{C}$ is the Delsarte code defined by $\mathcal{C}^\perp := \{N \in \mathrm{Mat}_{k\times m}(\mathbb{F}_q) : \mathrm{Tr}(MN^t) = 0 \text{ for all } M \in \mathcal{C}\}$, where Tr denotes the trace of a square matrix.

Remark 1.16. A Delsarte code is in particular a subgroup of $\mathrm{Mat}_{k\times m}(\mathbb{F}_q)$. Thus the minimum distance of a non-zero Delsarte code $\mathcal{C}$ can be expressed as $d_{\mathrm{rk}}(\mathcal{C}) = \min\{\mathrm{rk}(M) : M \in \mathcal{C},\ M \neq 0\}$.

One can easily check that the map $(M, N) \mapsto \mathrm{Tr}(MN^t)$ is a scalar product on $\mathrm{Mat}_{k\times m}(\mathbb{F}_q)$, i.e., it is symmetric, bilinear and non-degenerate. In particular, the following properties hold.

Lemma 1.17. Let $\mathcal{C}, \mathcal{D} \subseteq \mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ be Delsarte codes. We have:

$$(\mathcal{C}^\perp)^\perp = \mathcal{C}, \qquad \dim(\mathcal{C}^\perp) = km - \dim(\mathcal{C}), \qquad (\mathcal{C} \cap \mathcal{D})^\perp = \mathcal{C}^\perp + \mathcal{D}^\perp, \text{ and } \quad (\mathcal{C} + \mathcal{D})^\perp = \mathcal{C}^\perp \cap \mathcal{D}^\perp.$$

A fundamental result in the theory of Delsarte codes states that the MRD property is preserved under dualization. More precisely, the following hold.

Proposition 1.18 ([20], Theorem 5.5)**.** The dual of an MRD Delsarte code $\mathcal{C} \subseteq \mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ is MRD. In particular, if $0 < \dim(\mathcal{C}) < km$, then $\mathcal{C}^\perp$ has minimum distance $k - d_{\mathrm{rk}}(\mathcal{C}) + 1$.

An important and well-studied algebraic invariant of a Delsarte code is its rank distribution. It is defined as follows.

Definition 1.19. Let $\mathcal{C} \subseteq \mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ be a Delsarte code. Given an integer $i \in \mathbb{N}$, we define $W_i(\mathcal{C}) := |\{M \in \mathcal{C} : \mathrm{rk}(M) = i\}|$. The collection $(W_i(\mathcal{C}))_{i\in\mathbb{N}_{\geq 0}}$ is the **rank distribution** of $\mathcal{C}$.

By definition, the minimum distance of a non-zero Delsarte code $\mathcal{C} \subseteq \mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ is the smallest $i > 0$ such that $W_i(\mathcal{C}) > 0$. Notice that we define $W_i(\mathcal{C})$ for any $i \in \mathbb{N}$, even if we clearly have $W_i(\mathcal{C}) = 0$ for all integers $i > k$. This choice will simplify the statements in the sequel.

We also need the following definition from combinatorics.

Definition 1.20. Let s and t be integers. The q-**binomial coefficient** of s and t is defined by

$$\begin{bmatrix} s \\ t \end{bmatrix}_q = \begin{cases} 0 & \text{if } s < 0,\ t < 0, \text{ or } t > s, \\ 1 & \text{if } t = 0 \text{ and } s \geq 0, \\ \prod_{i=1}^{t} \frac{q^{s-i+1}-1}{q^i-1} & \text{otherwise.} \end{cases}$$

It is well-known that the q-binomial coefficient of s and t counts the number of t-dimensional $\mathbb{F}_q$-subspaces of an s-dimensional $\mathbb{F}_q$-space. In particular we have

$$\begin{bmatrix} s \\ t \end{bmatrix}_q = \begin{bmatrix} s \\ s-t \end{bmatrix}_q$$

for all integers s, t. As we work with a fixed prime power, we omit the subscript q in the sequel.

In [20] Delsarte showed that the rank distribution of a code $\mathcal{C}$ and the rank distribution of its dual code $\mathcal{C}^\perp$ determine each other via an invertible linear transformation. The proof of [20] relies on the combinatorial theory of designs and codesigns in association schemes. The statement is as follows.

Theorem 1.21 ([20], Theorem 3.3)**.** Let $\mathcal{C} \subseteq \mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ be a Delsarte code. We have

$$W_j(\mathcal{C}^\perp) = \frac{1}{|\mathcal{C}|} \sum_{i=0}^{k} W_i(\mathcal{C}) \sum_{s=0}^{k} (-1)^{j-s} q^{ms+\binom{j-s}{2}} \begin{bmatrix} k-s \\ k-j \end{bmatrix} \begin{bmatrix} k-i \\ s \end{bmatrix}$$

for all $j = 0, ..., k$.

The identities in Theorem 1.21 are called **MacWilliams identities** for the rank metric. They are named after J. MacWilliams, who first established analogous identities for classical codes endowed with the Hamming metric. When studying the duality theory of rank-metric codes, in Chapter 5 we will give in particular a concise proof for Theorem 1.21 using a simple double-counting argument.

In [32] Gabidulin proposed a different definition of rank-metric code, in which the codewords are vectors with entries in an extension field $\mathbb{F}_{q^m}$.

Definition 1.22 (see [32])**.** Let $\mathbb{F}_{q^m}/\mathbb{F}_q$ be a finite field extension. A **Gabidulin code** of length k over $\mathbb{F}_{q^m}$ is an $\mathbb{F}_{q^m}$-linear subspace $C \subseteq \mathbb{F}_{q^m}^k$. The **rank** of a vector $v = (v_1, ..., v_k) \in \mathbb{F}_{q^m}^k$ is defined as $\mathrm{rk}(v) := \dim_{\mathbb{F}_q} \mathrm{Span}\{v_1, ..., v_k\}$, and the **rank distance** between vectors v and w is given by $d_{\mathrm{G}}(v, w) := \mathrm{rk}(v - w)$. The **minimum distance** of a non-zero Gabidulin code is $d_{\mathrm{G}}(C) := \min\{\mathrm{rk}(v) : v \in C,\ v \neq 0\}$, and the **dual** of a Gabidulin code C is defined by $C^\perp := \{w \in \mathbb{F}_{q^m}^k : \langle v, w\rangle = 0 \text{ for all } v \in C\}$, where $\langle \cdot, \cdot \rangle$ is the standard inner product of $\mathbb{F}_{q^m}^k$.

Notice that the duality symbol "$\perp$" is the same for Delsarte and Gabidulin codes, even if the scalar products considered in the two contexts are different. This will not create ambiguity in the sequel.

In analogy with the theory of Delsarte codes, the rank distribution of a Gabidulin code is defined as follows.

Definition 1.23. The **rank distribution** of any Gabidulin code $C \subseteq \mathbb{F}_{q^m}^k$ is the collection $(W_i(C))_{i\in\mathbb{N}}$, where $W_i(C) := |\{v \in C : \mathrm{rk}(v) = i\}|$.

We now describe a natural way to associate to a Gabidulin code a Delsarte code with the same cardinality and metric properties.

Definition 1.24. Let $\mathcal{G} = \{\gamma_1, ..., \gamma_m\}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. The matrix **associated** to a vector $v \in \mathbb{F}_{q^m}^k$ with respect to $\mathcal{G}$ is the $k \times m$ matrix $M_{\mathcal{G}}(v)$ with entries in $\mathbb{F}_q$ defined by $v_i = \sum_{j=1}^m M_{\mathcal{G}}(v)_{ij}\gamma_j$ for all $i = 1, ..., k$. The Delsarte code **associated** to a Gabidulin code $C \subseteq \mathbb{F}_{q^m}^k$ with respect to the basis $\mathcal{G}$ is $\mathcal{C}_{\mathcal{G}}(C) := \{M_{\mathcal{G}}(v) : v \in C\} \subseteq \mathrm{Mat}_{k\times m}(\mathbb{F}_q)$.

Notice that, in the previous definition, the i-th row of $M_{\mathcal{G}}(v)$ is just the expansion of the entry v_i over the basis $\mathcal{G}$. The following result is therefore immediate.

Proposition 1.25. Let $C \subseteq \mathbb{F}_{q^m}^k$ be a Gabidulin code. For any basis $\mathcal{G}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, the set $\mathcal{C}_{\mathcal{G}}(C) \subseteq \mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ is a Delsarte rank-metric code with

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

Moreover, the codes $\mathcal{C}_{\mathcal{G}}(C)$ and C have the same rank distribution, and if $C \neq 0$ then $d_{\mathrm{G}}(C) = d_{\mathrm{rk}}(\mathcal{C}_{\mathcal{G}}(C))$. In particular, different choices of $\mathcal{G}$ give rise to codes with the same parameters and rank distributions.

Proposition 1.25 shows that any Gabidulin code can be regarded as a Delsarte rank-metric code with the same cardinality and rank distribution. Clearly, since Gabidulin codes are $\mathbb{F}_{q^m}$-linear spaces and Delsarte codes are $\mathbb{F}_q$-linear spaces, not all Delsarte rank-metric codes arise from a Gabidulin code in this way. In fact, only a few of them do. For example, a Delsarte code $\mathcal{C} \subseteq \mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ such that $\dim(\mathcal{C}) \not\equiv 0 \mod m$ cannot arise from a Gabidulin code.

Combining Proposition 1.12 and Proposition 1.25 we obtain the following bound.

Proposition 1.26. Let $C \subseteq \mathbb{F}_{q^m}^k$ be a non-zero Gabidulin code. Then $\dim_{\mathbb{F}_{q^m}}(C) \leq k - d_{\mathrm{G}}(C) + 1$.

Definition 1.27. A Gabidulin code is called **MRD** if it is the zero code, or if its parameters attain the bound of Proposition 1.26.

In [32], Gabidulin showed that the dual of a Gabidulin MRD code is also MRD. Therefore, as for Delsarte codes, the MRD properties is preserved under dualization.

Proposition 1.28 (see [32])**.** The dual of an MRD Gabidulin code C is an MRD Gabidulin code. Moreover, if $0 < \dim_{\mathbb{F}_{q^m}}(C) < k$ then $d_{\mathrm{G}}(C^\perp) = k - d_{\mathrm{G}}(C) + 1$.

In Chapter 5 we will show that Proposition 1.28 is a special instance of Proposition 1.18. In [32] Gabidulin also showed that for all choices of the parameters there exists an MRD code having those parameters. More precisely, the following hold.

Theorem 1.29 (see [32])**.** For any prime power q and for all integers k, m, d with $1 \leq d \leq k \leq m$ there exists a Gabidulin code $C \subseteq \mathbb{F}_{q^m}^k$ with minimum distance d and $\dim_{\mathbb{F}_{q^m}}(C) = k - d + 1$.

We include a short and elegant proof for Theorem 1.29 from [54].

Definition 1.30. A **linearized polynomial** p over $\mathbb{F}_{q^m}$ is a polynomial of the form

$$p(x) = \alpha_0 x + \alpha_1 x^q + \alpha_2 x^{q^2} + \cdots + \alpha_s x^{q^s}, \qquad \alpha_i \in \mathbb{F}_{q^m}, \quad i = 0, ..., s.$$

The **degree** of p, denoted by $\deg(p)$, is the largest integer $i \geq 0$ such that $\alpha_i \neq 0$. The $\mathbb{F}_{q^m}$-vector space of linearized polynomials over $\mathbb{F}_{q^m}$ of degree at most s is denoted by $\mathrm{Lin}_q(m, s)$. It is easy to see that $\dim_{\mathbb{F}_{q^m}}(\mathrm{Lin}_q(m, s)) = s + 1$.

Remark 1.31. The roots of a linearized polynomial p over $\mathbb{F}_{q^m}$ form an $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^m}$, which we denote by $V(p) \subseteq \mathbb{F}_{q^m}$ ([63], Theorem 3.50). Clearly, for any non-zero linearized polynomial p we have $\dim_{\mathbb{F}_q} V(p) \leq \deg(p)$ by the Fundamental Theorem of Algebra.

Proof of Theorem 1.29. Let $E = \{\beta_1, ..., \beta_k\} \subseteq \mathbb{F}_{q^m}$ be a set of $\mathbb{F}_q$-independent elements. Such elements exist since $k \leq m$ by assumption (see Notation 1.11). Define the $\mathbb{F}_{q^m}$-linear map $\mathrm{ev}_E : \mathrm{Lin}_q(m, k-d) \to \mathbb{F}_{q^m}^k$ by $\mathrm{ev}_E(p) := (p(\beta_1), ..., p(\beta_k))$ for all $p \in \mathrm{Lin}_q(m, k-d)$. In the remainder of the proof we show that $C := \mathrm{ev}_E(\mathrm{Lin}_q(m, k-d)) \subseteq \mathbb{F}_{q^m}^k$ is a Gabidulin code with the expected property. Clearly, C is an $\mathbb{F}_{q^m}$-linear space. Now let $p \in \mathrm{Lin}_q(m, k-d)$ be a non-zero linearized polynomial, and let $W \subseteq \mathbb{F}_{q^m}$ denote the space generated over $\mathbb{F}_q$ by the evaluations $p(\beta_1), ..., p(\beta_k)$. The polynomial p can be viewed as an $\mathbb{F}_q$-linear map $p : \langle \beta_1, ..., \beta_k \rangle_{\mathbb{F}_q} \to \mathbb{F}_{q^m}$. The image of p is W, and thus by the rank-nullity theorem we have $\dim_{\mathbb{F}_q}(W) = k - \dim_{\mathbb{F}_q} V(p)$. By Remark 1.31 we conclude $\dim_{\mathbb{F}_q}(W) \geq k - (k-d) = d$. This shows that C has $d_{\mathrm{G}}(C) \geq d$. In particular, as $d \geq 1$, the map ev_E is injective, and so the dimension of C is $\dim_{\mathbb{F}_{q^m}}(C) = k - d + 1$ (see Definition 1.30). By Proposition 1.26 this implies $d_{\mathrm{G}}(C) \leq d$, and thus $d_{\mathrm{G}}(C) = d$. □

Remark 1.32. We denote the Gabidulin code constructed in the proof of Theorem 1.29 by $\mathrm{Gab}_q(m, k, d, E)$. In the literature some researchers call "Gabidulin codes" only the rank-metric codes of type $\mathrm{Gab}_q(m, k, d, E)$. For practical reasons we will not make this distinction here, and simply call "Gabidulin code" any $\mathbb{F}_{q^m}$-subspace $C \subseteq \mathbb{F}_{q^m}^k$ (according to our Definition 1.22).

Remark 1.33. A proof for Theorem 1.14 can now be easily obtained combining Theorem 1.29 and Proposition 1.25.

In the last fifteen years, Gabidulin codes were widely investigated by many mathematicians, computer scientists, and electrical engineers. We conclude this section on rank-metric codes mentioning a result from [33] on the weight distribution of a Gabidulin code.

Theorem 1.34 ([33], Proposition 3)**.** Let $C \subseteq \mathbb{F}_{q^m}^k$ be a Gabidulin code. Then for all integers $0 \leq \nu \leq k$ we have

$$\sum_{i=0}^{k-\nu} W_i(C) \begin{bmatrix} k-i \\ \nu \end{bmatrix} = \frac{|C|}{q^{m\nu}} \sum_{j=0}^{\nu} W_j(C^\perp) \begin{bmatrix} k-j \\ \nu-j \end{bmatrix}.$$

In Chapter 5 we will study how the trace product on $\mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ and the standard inner product on $\mathbb{F}_{q^m}^k$ relate to each other. This will allow us to compare the duality theories of Delsarte and Gabidulin codes, proving that the former generalizes the latter. In particular, we will show that Theorem 1.34 can be regarded as a special instance of Theorem 1.21.

1.6 Subspace codes

This section of the chapter is devoted to subspace codes. Recall from Definition 1.8 that a subspace code is a collection $\mathcal{C}$ of vector subspaces of $\mathbb{F}_q^n$ of cardinality $|\mathcal{C}| \geq 2$.

Notation 1.35. Throughout this section q is a prime power, and k and n are two integers with $0 < k \leq n-1$. The set of all $\mathbb{F}_q$-subspaces of $\mathbb{F}_q^n$ is denoted by $\mathcal{P}(\mathbb{F}_q^n)$. All dimensions in this section are computed over $\mathbb{F}_q$.

A very natural class of subspace codes is obtained by considering subsets of $\mathcal{P}(\mathbb{F}_q^n)$ all of whose elements have the same dimension k. Such codes are called "constant dimension" codes, and are the most studied in the framework of network coding. Introducing the Grassmannian variety

$$\mathcal{G}_q(k,n) := \{V \in \mathcal{P}(\mathbb{F}_q^n) : \dim(V) = k\},$$

a q-ary **constant dimension** subspace code of length n and dimension k is a subset $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ with at least two elements. It follows from the definition that any constant dimension subspace code has even minimum distance. Recall that the cardinality of $\mathcal{G}_q(k,n)$ is given by

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

(see Definition 1.20). The cardinality of a constant dimension subspace code of given minimum distance can be upper bounded as follows.

Theorem 1.36 (Singleton-like bound, Theorem 9 of [54])**.** Let $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ be a subspace code. We have

$$|\mathcal{C}| \leq \begin{bmatrix} n-(d_{\mathrm{s}}(\mathcal{C})-2)/2 \\ \max\{k,n-k\} \end{bmatrix}.$$

The following notion of orthogonality was introduced in the context of subspace codes by Kötter and Kschischang in [54].

Definition 1.37. The **orthogonal** of a code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ is $\mathcal{C}^\perp := \{U^\perp : U \in \mathcal{C}\} \subseteq \mathcal{G}_q(n-k,n)$, where $U^\perp$ is the orthogonal of U with respect to the standard inner product of $\mathbb{F}_q^n$.

A subspace code and its orthogonal relate as follows.

Proposition 1.38. Let $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ be a subspace code. Then $d_{\mathrm{s}}(\mathcal{C}) = d_{\mathrm{s}}(\mathcal{C}^\perp)$ and $|\mathcal{C}| = |\mathcal{C}^\perp|$.

Proof. Let $U, V \in \mathcal{C}$ be subspaces with $U \neq V$. By definition of subspace distance we have

$$\begin{aligned} d_{\mathrm{s}}(U^\perp, V^\perp) \;=\; 2(n-k) - 2\dim(U^\perp \cap V^\perp) &= 2(n-k) - 2(n-\dim(U+V)) \\ &= -2k + 2\dim(U+V) \\ &= 2k - \dim(U \cap V) \\ &= d_{\mathrm{s}}(U,V). \end{aligned}$$

Therefore $d_{\mathrm{s}}(\mathcal{C}) = d_{\mathrm{s}}(\mathcal{C}^\perp)$. Now the map that sends a subspace $U \subseteq \mathbb{F}_q^n$ into $U^\perp$ is a bijection $\mathcal{G}_q(k,n) \to \mathcal{G}_q(n-k,n)$. Thus $|\mathcal{C}| = |\mathcal{C}^\perp|$, and the proposition follows. □

The first family of subspace codes was constructed in [54], along with an efficient decoding algorithm. A different decoding procedure based on rank-metric codes was proposed later in [55]. The codes introduced in [54] are called "Reed-Solomon-like codes" because of a structural analogy with the family of Reed-Solomon codes of the classical theory of codes (see e.g. Chapter 10 of [68]). Reed-Solomon-like codes play a central role in random linear network coding. For completeness we include their construction and main properties in this section.

We start by illustrating a connection between rank distance and subspace distance.

Proposition 1.39 ([55], Proposition 4)**.** Let $m \geq 0$ be an integer, and let $M, N \in \mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ be matrices. We have

$$d_{\mathrm{s}}\left(\mathrm{rowsp}\begin{bmatrix} I & M \end{bmatrix}, \mathrm{rowsp}\begin{bmatrix} I & M \end{bmatrix}\right) = 2d_{\mathrm{rk}}(M,N).$$

In particular, if $\mathcal{C} \subseteq \mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ is a rank-metric code with $|\mathcal{C}| \geq 2$, then the set

$$\mathrm{lift}(\mathcal{C}) = \left\{\mathrm{rowsp}\begin{bmatrix} I_k & M \end{bmatrix} \ : \ M \in \mathcal{C}\right\} \subseteq \mathcal{G}_q(k, k+m)$$

is a subspace code with $d_{\mathrm{s}}(\mathrm{lift}(\mathcal{C})) = 2d_{\mathrm{rk}}(\mathcal{C})$.

Proof. As simple consequence of the definitions we have

$$\begin{aligned} d_{\mathrm{s}}\left(\mathrm{rowsp}\begin{bmatrix} I & M \end{bmatrix}, \mathrm{rowsp}\begin{bmatrix} I & M \end{bmatrix}\right) &= 2 \cdot \mathrm{rk}\begin{bmatrix} I_k & M \\ I_k & N \end{bmatrix} - 2k \\ &= 2 \cdot \mathrm{rk}\begin{bmatrix} 0_k & M-N \\ I_k & N \end{bmatrix} - 2k \\ &= 2(\mathrm{rk}(M-N)+k) - 2k \\ &= 2d_{\mathrm{rk}}(M,N). \end{aligned}$$

The last part of the statement easily follows. □

Definition 1.40. The subspace code $\mathrm{lift}(\mathcal{C})$ in the statement of Proposition 1.39 is called the **lifting** of the rank-metric code $\mathcal{C}$.

Reed-Solomon-like codes can now be easily described as the liftings of the Delsarte codes associated to a Gabidulin code of type $\mathrm{Gab}_q(m,k,d,E)$. See Definition 1.24, Notation 1.32 and Definition 1.40 for the terminology.

Definition 1.41 (Reed-Solomon-like codes)**.** Assume $n \geq 2k$, and set $m := n-k$. Let $\mathcal{G} = \{\gamma_1, ..., \gamma_m\}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and $E = \{\beta_1, ..., \beta_k\} \subseteq \mathbb{F}_{q^m}$ be a set of $\mathbb{F}_q$-independent elements. The **Reed-Solomon-like** code associated to the tuple $(q,k,n,d,\mathcal{G},E)$ is

$$\mathbf{KK}_q(k,n,d,\mathcal{G},E) := \mathrm{lift}(\mathcal{C}_{\mathcal{G}}(\mathrm{Gab}_q(n-k,k,d,E))) \subseteq \mathcal{G}_q(k,n).$$

Remark 1.42. By Proposition 1.39, Proposition 1.29 and Proposition 1.25, the cardinality of a Reed-Solomon-like code $\mathbf{KK}_q(k,n,d,\mathcal{G},E)$ is $q^{(n-k)(k-d+1)}$. Moreover, by Proposition 1.39, its minimum subspace distance is $2d$. It can be shown that

$$\begin{bmatrix} n-d+1 \\ n-k \end{bmatrix} < 4q^{(n-k)(k-d+1)}$$

(see [54], Lemma 4). As a consequence, by Theorem 1.36 any subspace code $\mathcal{C}$ with the same parameters as $\mathbf{KK}_q(k,n,d,\mathcal{G},E)$ has cardinality $|\mathcal{C}| < 4 \cdot |\mathbf{KK}_q(k,n,d,\mathcal{G},E)|$. This shows that Reed-Solomon-like codes have optimal cardinality, up to a constant factor 4.

1.7 Some linear algebra and coding theory preliminaries

In this short section we briefly recall some notions from linear algebra and classical coding theory that we will need in the sequel.

Definition 1.43. Let $1 \leq t \leq n$ be an integer. A matrix M of size $t \times n$ over a field $\mathbb{F}$ is in **reduced row echelon form** if:

1. M is in row-echelon form;
2. the first non-zero entry of each row of M is a 1 and the only non-zero entry in its column.

Notation 1.44. It is well-known that for any $1 \leq t \leq n$ and any t-dimensional $\mathbb{F}$-subspace $X \subseteq \mathbb{F}^n$, there exists a unique $t \times n$ matrix M in reduced row echelon form with entries in $\mathbb{F}$ such that $\mathrm{rowsp}(M) = X$. See e.g. Chapter 2.2 of [72]. We denote the matrix M by $\mathrm{RRE}(X)$. Moreover, for any matrix M we call $\mathrm{RRE}(M) := \mathrm{RRE}(\mathrm{rowsp}(M))$ the **reduced row echelon form** of M.

Definition 1.45. Let $\mathbb{F}$ be a field and $n \geq 1$ an integer. The **Hamming weight** of a vector $v \in \mathbb{F}^n$ is $\mathrm{wt}_{\mathrm{H}}(v) := |\{i \in [n] : v_i \neq 0\}|$, the number of its non-zero components. The **Hamming distance** between vectors $v, w \in \mathbb{F}^n$ is defined by $d_{\mathrm{H}}(v, w) := |\{i \in [n] : v_i \neq w_i\}|$. A **classical code** in $\mathbb{F}^n$ is a non-empty subset $C \subseteq \mathbb{F}^n$. We say that C is **linear** of **dimension** k if it is a k-dimensional $\mathbb{F}$-linear space. We say that C is a **q-ary code** if $\mathbb{F} = \mathbb{F}_q$. When $|C| \geq 2$, the **minimum Hamming distance** of C is the positive integer

$$d_{\mathrm{H}}(C) := \min\{d_{\mathrm{H}}(v, w) : v, w \in C,\ v \neq w\}.$$

Chapter 2

Partial spread codes

In discrete geometry, a k-spread in $\mathbb{F}_q^n$ is a collection of k-dimensional subspaces of $\mathbb{F}_q^n$ having trivial pairwise intersections and whose union is the whole space $\mathbb{F}_q^n$. By definition, a k-spread in $\mathbb{F}_q^n$ can be viewed as a constant dimension subspace code in $\mathcal{G}_q(k,n)$ of minimum distance $2k$ (see page 32 for the definition of subspace code). It is well-known that a k-spread in $\mathbb{F}_q^n$ exists if and only if k divides n. More details on spreads will be given later in Section 2.1.

In [71], F. Manganiello, E. Gorla, and J. Rosenthal propose a systematic construction for k-spreads to be used in the context of random linear network coding. In the approach of [71], the subspaces that constitute the spread are represented as the rowspace of matrices in reduced row echelon form having a prescribed block structure. The construction makes use of the companion matrix associated to a monic polynomial over a finite field.

The codes introduced in [71], called "spread codes", have larger cardinality than the Reed-Solomon-like codes with the same parameters (see Section 1.6 for the properties of Reed-Solomon-like codes). An efficient decoding algorithm for spread codes was presented in [40].

In this chapter we generalize the construction of [71], introducing a new family of subspace codes, which we call "partial spread codes". As opposed to spread codes, partial spread codes exist for all values of k and n. After presenting our code construction, we explicitly compute the parameters of partial spread codes, proving in particular that they are asymptotically optimal and maximal with respect to inclusion. This also shows that our partial spread codes cannot be enlarged by adding new codewords without lowering their minimum subspace distance.

Then we show how partial spread codes decoding can be efficiently reduced to spread codes decoding. This will provide in particular an efficient decoding algorithm for partial spread codes based on the results of [40].

The structure of this chapter is as follows: In Section 2.1 we briefly recall some Discrete Geometry definitions, and in Section 2.2 we illustrate our codes construction. In Section 2.3 we compute the parameters of partial spread codes, and in Sections 2.4 and 2.5 we provide an efficient decoding algorithm for them.

The results of this chapter have been published in [37].

Notation 2.1. Throughout this chapter, q is a prime power and $\mathbb{F}_q$ the finite field with q elements. Moreover, k and n denote two integers with $0 < k < n$.

2.1 Spreads and partial spreads

We start recalling some preliminary definitions from Discrete Geometry.

Definition 2.2. A k-**spread** of $\mathbb{F}_q^n$ is a collection of subspaces $\{V_i\}_{i=1}^t$ of $\mathbb{F}_q^n$ such that:

1. $\dim V_i = \dim V_j = k$ for any $i, j \in \{1, ..., t\}$,
2. $V_i \cap V_j = \{0\}$ whenever $i \neq j$,
3. $\mathbb{F}_q^n = \bigcup_{i=1}^t V_i$.

It is well-known that a k-spread of $\mathbb{F}_q^n$ exists if and only if k divides n (see [48], Corollary 4.17). From the definition we see that if $\{V_i\}_{i=1}^t$ is a k-spread of $\mathbb{F}_q^n$, then $t = (q^n - 1)/(q^k - 1)$. Being a subset of the Grassmannian $\mathcal{G}_q(k, n)$, a k-spread in $\mathbb{F}_q^n$ is a q-ary subspace code of length n, constant dimension k and minimum distance $2k$. It is easy to check that a spread meets the Singleton-like bound stated in Theorem 1.36.

Partial spreads are defined as follows.

Definition 2.3. A **partial** k**-spread** of $\mathbb{F}_q^n$ is a subset $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ such that $U \cap V = \{0\}$ for any $U, V \in \mathcal{C}$ with $U \neq V$.

A partial k-spread of $\mathbb{F}_q^n$ with at least two elements is a q-ary subspace code of length n, dimension k and minimum distance $2k$. A bound on the cardinality of a partial spread can be derived as follows. The result is well-known, but we include a short proof for completeness.

Lemma 2.4. Let $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ be a partial spread code. Denote by r the remainder obtained dividing n by k. We have

$$|C| \leq \frac{q^n - q^r}{q^k - 1}.$$

Proof. Since $\mathcal{C}$ is a set of k-dimensional vector subspaces of $\mathbb{F}_q^n$ with trivial pairwise intersections, we have $|\mathcal{C}| \cdot (q^k - 1) + 1 \leq q^n$. Since k divides $n - r$, the number $(q^{n-r} - 1)/(q^k - 1)$ is an integer. Thus

$$|\mathcal{C}| \leq \left\lfloor \frac{q^n - 1}{q^k - 1} \right\rfloor = \left\lfloor \frac{q^r(q^{n-r} - 1)}{q^k - 1} + \frac{q^r - 1}{q^k - 1} \right\rfloor = \frac{q^n - q^r}{q^k - 1},$$

as claimed. □

The upper bound given in Lemma 2.4 admits some non-trivial improvements for special values of the parameters (see [5] and [23] for details). The following lower bound for a partial k-spread in $\mathbb{F}_q^n$ was proved by A. Beutelspacher.

Lemma 2.5 (see [4])**.** Write $n = hk + r$ with $0 \leq r \leq k - 1$. There exists a partial k-spread of $\mathbb{F}_q^n$ of cardinality

$$\frac{q^n - q^r}{q^k - 1} - q^r + 1.$$

A different proof of Lemma 2.5 is given in [31], Theorem 11. For interesting discussions on the sharpness of the bound see [26] and [42].

2.2 Construction of partial spread codes

In this section we present our construction of partial spread codes. We start with two preliminary results that will be needed in the sequel.

Lemma 2.6 ([66], Chapter 2.5)**.** Let $p \in \mathbb{F}_q[x]$ be an irreducible monic polynomial of degree $k \geq 1$. Write $p = x^k + \sum_{i=0}^{k-1} p_i x^i$, and define the **companion matrix** of p as

$$\mathbf{M}(p) := \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & & 1 \\ -p_0 & -p_1 & -p_2 & \cdots & -p_{k-1} \end{bmatrix}.$$

The $\mathbb{F}_q$-algebra $\mathbb{F}_q[P]$ is a finite field with q^k elements.

Throughout this chapter, if V is a vector space over $\mathbb{F}_q$ and $S \subseteq V$ is any subset, we denote by $\langle S \rangle$ the vector subspace of V generated by S.

Lemma 2.7. Let V be a finite-dimensional vector space over $\mathbb{F}_q$. Let $D \subseteq V$ be a subset, and set $d := \dim\langle D \rangle$. Choose any subset $S \subseteq D$. Then $\dim\langle D \setminus S \rangle \geq d - |S|$.

Proof. Clearly, D and S are finite. Since $D = (D \setminus S) \cup S$, we have $\langle D \setminus S \rangle + \langle S \rangle = \langle D \rangle$. It follows that $\dim\langle D \setminus S \rangle + \dim\langle S \rangle = d + \dim\langle D \setminus S \rangle \cap \langle S \rangle$. Since $\dim\langle S \rangle \leq |S|$, we conclude $\dim\langle D \setminus S \rangle + |S| \geq d$. □

Partial spread codes are constructed as in the following theorem.

Theorem 2.8. Write $n = hk + r$ with $0 \leq r \leq k - 1$, and assume $h \geq 2$. Let $p, p' \in \mathbb{F}_q[x]$ be irreducible monic polynomials of degree k and $k + r$ respectively, and let $P := \mathbf{M}(p)$, $P' := \mathbf{M}(p')$ be their companion matrices. For any $1 \leq i \leq h - 1$ let

$$\mathcal{M}_i(p, p') := \left\{ \begin{bmatrix} 0_k & \cdots & 0_k & I_k & A_{i+1} & \cdots & A_{h-1} & A_{(k)} \end{bmatrix} \,:\, A_{i+1}, ..., A_{h-1} \in \mathbb{F}_q[P],\ A \in \mathbb{F}_q[P'] \right\},$$

where 0_k is the $k \times k$ matrix with zero entries, I_k is the $k \times k$ identity matrix, and $A_{(k)}$ denotes the last k rows of A. The set

$$\mathcal{C} := \bigcup_{i=1}^{h-1} \left\{ \mathrm{rowsp}(M) : M \in \mathcal{M}_i(p, p') \right\} \cup \left\{ \mathrm{rowsp} \begin{bmatrix} 0_k & \cdots & 0_k & 0_{k \times r} & I_k \end{bmatrix} \right\}$$

is a partial spread in $\mathbb{F}_q^n$ of dimension k. In particular, the minimum subspace distance of $\mathcal{C}$ as a subspace code is $2k$.

Proof. Choose matrices $M_1 \neq M_2 \in \mathcal{M}_i(p, p')$, and set $V_1 := \mathrm{rowsp}(M_1)$, $V_2 := \mathrm{rowsp}(M_2)$. Since by definition $d(V_1, V_2) = 2k - 2\dim(V_1 \cap V_2)$, we have $d(V_1, V_2) = 2k$ if and only if

$$\mathrm{rk} \begin{bmatrix} M_1 \\ M_2 \end{bmatrix} = 2k.$$

Since $M_1 \neq M_2$, it is possible to find either in $\begin{bmatrix} M_1 \\ M_2 \end{bmatrix}$ or in $\begin{bmatrix} M_2 \\ M_1 \end{bmatrix}$ a submatrix in one of the following three forms:

$$N_1 := \begin{bmatrix} I_k & B \\ 0_k & I_k \end{bmatrix}, \qquad N_2 := \begin{bmatrix} I_k & B_1 \\ I_k & B_2 \end{bmatrix}, \qquad N_3 := \begin{bmatrix} I_k & X_{(k)} \\ I_k & Y_{(k)} \end{bmatrix},$$

with $B_1 \neq B_2 \in \mathbb{F}_q[P]$ and $X \neq Y \in \mathbb{F}_q[P']$. Let us compute the ranks of such matrices case by case. The rank of N_1 is given by

$$\dim(\text{rowsp}\begin{bmatrix} I_k & B \end{bmatrix}) + \dim(\text{rowsp}\begin{bmatrix} 0_k & I_k \end{bmatrix}) - \dim\left(\text{rowsp}\begin{bmatrix} I_k & B \end{bmatrix} \cap \text{rowsp}\begin{bmatrix} 0_k & I_k \end{bmatrix}\right) = 2k.$$

The rank of N_2 is equal to the rank of

$$\begin{bmatrix} I_k & B_1 \\ 0_k & B_2 - B_1 \end{bmatrix}.$$

Since $B_1 \neq B_2$, by Lemma 2.6 we have that $B_2 - B_1$ is an invertible matrix, and so

$$\det \begin{bmatrix} I_k & B_1 \\ 0_k & B_2 - B_1 \end{bmatrix} = \det(B_2 - B_1) \neq 0.$$

It follows that $\text{rk}(N_2) = 2k$. In order to study N_3, consider the $2(k+r) \times 2(k+r)$ matrix

$$H := \begin{bmatrix} I_{k+r} & X \\ I_{k+r} & Y \end{bmatrix}.$$

Using the same argument as above one finds $\text{rk}(H) = 2(k+r)$. Delete from H the rows from one to r and from $k+r+1$ to $k+2r$, obtaining a matrix $\tilde{H}$ of size $2k \times (2k+2r)$. We observe that the rows of $\tilde{H}$ are exactly the rows of N_3 with r extra zeroes in the beginning. In particular, $\text{rk}(\tilde{H}) = \text{rk}(N_3)$. By Lemma 2.7 we have $\text{rk}(\tilde{H}) \geq 2(k+r) - 2r = 2k$, and so $\text{rk}(N_3) = 2k$. To conclude the proof, let $M_1 \in \mathcal{M}_i(p, p')$ and set $M_2 := \begin{bmatrix} 0_k & \cdots & 0_k & 0_{k\times r} & I_k \end{bmatrix}$. We clearly have

$$\text{rk}\begin{bmatrix} M_1 \\ M_2 \end{bmatrix} = 2k.$$

All of this shows that $\mathcal{C}$ is a set of k-dimensional vector subspaces of $\mathbb{F}_q^n$ whose pairwise intersections are trivial. The theorem follows. □

Notation 2.9. The partial spread code $\mathcal{C}$ constructed in Theorem 2.8 is denoted by $\mathcal{C}_q(k, n; p, p')$. We will assume $0 < k \leq n/2$ without loss of generality, as for any code $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ the orthogonal code $\mathcal{C}^\perp \subseteq \mathcal{G}_q(n-k, n)$ has the same cardinality and minimum distance as $\mathcal{C}$ (see Definition 1.37 and Proposition 1.38).

Remark 2.10. Our construction of partial spread codes generalizes that of spread codes proposed in [71, Definition 2]. It is easy to see that spread codes are obtained taking $r := 0$ and $p' := p$ in the statement of Theorem 2.8. Notice moreover that, as opposed to spread codes, partial spread codes exist also when k does not divide n.

Example 2.11. We construct a partial spread code of length 7 and dimension 2 over the binary field $\mathbb{F}_2$. Let $(q, k, n) := (2, 2, 7)$. We have $n \equiv 1 \mod k$. Hence, in the notation of Theorem 2.8, $r = 1$. Take irreducible monic polynomials $p := x^2 + x + 1 \in \mathbb{F}_2[x]$, $p' := x^3 + x + 1 \in \mathbb{F}_2[x]$ of degree k and $k + r$, respectively. The companion matrices of p and p' are

$$P := \mathbf{M}(p) = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \qquad P' := \mathbf{M}(p') = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

The elements of $\mathcal{C}_2(2,7;p,p')$ are the rowspaces of all the matrices in the following forms:

$$\begin{bmatrix} 1 & 0 & & \\ 0 & 1 & A_1 & A_{(2)} \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 1 & 0 & \\ 0 & 0 & 0 & 1 & B_{(2)} \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

where A_1 is any matrix in $\mathbb{F}_q[P]$ and $A_{(2)}, B_{(2)}$ denote the last two rows of any $A, B \in \mathbb{F}_q[P']$. It can be checked that $\mathcal{C}_2(2,7;p,p')$ has $2^2 \cdot 2^3 + 2^3 + 1 = 41$ elements. The cardinality computation will be generalized in Proposition 2.12.

2.3 Properties of partial spread codes

In this section we study the properties of partial spread codes. In Proposition 2.12 we compute their cardinality, and in Proposition 2.14 we show that they are maximal with respect to containment.

Proposition 2.12. Let $\mathcal{C} := \mathcal{C}_q(k,n;p,p')$ be a partial spread code. The size of $\mathcal{C}$ is given by

$$|\mathcal{C}| = \frac{q^n - q^r}{q^k - 1} - q^r + 1.$$

Proof. We follow the notation of Theorem 2.8. Let X, Y be matrices in $\mathbb{F}_q[P']$, and assume $X_{(k)} = Y_{(k)}$. If $X \neq Y$ we have

$$\operatorname{rk} \begin{bmatrix} I_{k+r} & X \\ I_{k+r} & Y \end{bmatrix} = 2(k+r)$$

and so, as in the proof of Theorem 2.8,

$$\operatorname{rk} \begin{bmatrix} I_k & X_{(k)} \\ I_k & Y_{(k)} \end{bmatrix} = 2k,$$

a contradiction. It follows that $X = Y$. As a consequence, the cardinality of $\{X_{(k)} : X \in \mathbb{F}_q[P']\}$ is exactly $|\mathbb{F}_q[P']| = q^{k+r}$. Now we observe that the matrices in the statement of Theorem 2.8 are all in reduced row echelon form, which is a canonical invariant of their rowspace by Notation 1.44. As a consequence, the size of $\mathcal{C}$ is

$$|\mathcal{C}| = 1 + q^{k+r} \sum_{i=0}^{h-2} q^{ki} = (q^n - q^r)/(q^k - 1) - q^r + 1,$$

as claimed. □

Corollary 2.13. Let $\mathcal{C} := \mathcal{C}_q(k,n;p,p')$ be a partial spread code. Denote by $\mathcal{A}_q(k,n,2k)$ the largest possible size of a subspace code in $\mathcal{G}_q(k,n)$ of minimum distance $2k$. Let r be the remainder obtained dividing n by k. Then

$$\mathcal{A}_q(k,n,2k) - |\mathcal{C}| \leq q^r - 1.$$

Proof. Combine Lemma 2.4 and Proposition 2.12. □

In [31] T. Etzion and A. Vardy propose a different construction of partial spreads to be used in random linear network coding (see the proof of [31, Theorem 11]). Their codes have the same cardinality and minimum distance as our partial spread codes, but no decoding algorithm for them is proposed in [31]. Exploiting the convenient block structure of our codes, in Section 2.5 we will show how they can be efficiently decoded.

Proposition 2.14. Let $\mathcal{N}_q(k,n,2k)$ be the set of all partial k-spreads, and let $\mathcal{C} := \mathcal{C}_q(k,n;p,p')$ be a partial spread code. Then $\mathcal{C}$ is a maximal element of $\mathcal{N}_q(k,n,2k)$ with respect to inclusion.

Proof. We will show that there is no partial k-spread $\mathcal{C}'$ in $\mathbb{F}_q^n$ such that $\mathcal{C}' \supseteq \mathcal{C}$ and $|\mathcal{C}'| > |\mathcal{C}|$. Write $n = hk + r$ with $0 \leq r < k$ and $h \geq 2$ (see Notation 2.9). Define the partial k-spread

$$\overline{\mathcal{C}} := \mathcal{C} \setminus \left\{ \text{rowsp} \begin{bmatrix} 0_k & \cdots & 0_k & 0_{k\times r} & I_k \end{bmatrix} \right\}.$$

Assume, by contradiction, that there exists a partial k-spread $\mathcal{C}'$ in $\mathbb{F}_q^n$ such that $\mathcal{C}' \supseteq \overline{\mathcal{C}}$ and $|\mathcal{C}'| \geq |\overline{\mathcal{C}}| + 2$. Set $S := \bigcup_{V\in\overline{\mathcal{C}}} V \setminus \{0\}$. With the aid of Theorem 2.8 and Proposition 2.12 one computes

$$|\overline{\mathcal{C}}| = (q^n - q^r)/(q^k - 1) - q^r, \qquad |S| = (q^k - 1)\cdot|\overline{\mathcal{C}}| = q^n - q^{k+r}.$$

The set $X := \{x \in \mathbb{F}_q^n : x_i = 0 \text{ for any } i = 1, ..., (h-1)k\}$ is a vector subspace of $\mathbb{F}_q^n$ of dimension $k + r$. We clearly have an inclusion $X \subseteq \mathbb{F}_q^n \setminus S$. Since

$$|\mathbb{F}_q^n \setminus S| = q^n - (q^n - q^{k+r}) = q^{k+r},$$

we have $X = \mathbb{F}_q^n \setminus S$ and $\mathbb{F}_q^n = X \sqcup S$, with X a $(k+r)$-dimensional subspace. Since: 1) $\mathcal{C}' \supseteq \mathcal{C} \supseteq \overline{\mathcal{C}}$, 2) $|\mathcal{C}'| \geq \overline{\mathcal{C}} + 2$, and 3) for any $s \in S$ there exists a $V_s \in \overline{\mathcal{C}}$ such that $s \in V_s$, we deduce that there exist two k-dimensional vector subspaces $V_1, V_2 \in \mathcal{C}'$ such that $V_1 \cap V_2 = \{0\}$ and $V_1, V_2 \subseteq X$. Since X is a vector subspace of $\mathbb{F}_q^n$ containing $V_1 \cup V_2$ and, by definition, $V_1 + V_2$ is the smallest vector subspace of $\mathbb{F}_q^n$ containing both V_1 and V_2, we have $V_1 + V_2 \subseteq X$. It follows

$$\dim(V_1) + \dim(V_2) - \dim(V_1 \cap V_2) \leq \dim(X),$$

and therefore $2k \leq k + r$, a contradiction. □

Proposition 2.14 ensures that a partial spread code $\mathcal{C}_q(k,n;p,p')$ cannot be improved, as a subspace code in $\mathcal{G}_q(k,n)$, by adding new codewords without lowering its minimum distance.

2.4 The block structure

In this section we investigate the block structure of partial spread codes, presenting two fundamental lemmas. These results will allow us to give an efficient decoding algorithm for our codes, which we present in the next section. The results of this section extend those of in [40].

Lemma 2.15. Let $\mathcal{C} := \mathcal{C}_q(k,n;p,p')$ be a partial spread code and let $V \in \mathcal{C}$ be a codeword, say

$$V := \text{rowsp} \begin{bmatrix} S_1 & \cdots & S_{h-1} & S \end{bmatrix},$$

where the S_i's are $k \times k$ matrices and S is a $k \times (k + r)$ matrix. Let $X \subseteq \mathbb{F}_q^n$ be a t-dimensional vector subspace given as the rowspace of a matrix of the form

$$\begin{bmatrix} M_1 & \cdots & M_{h-1} & M \end{bmatrix},$$

where the M_i's are $k \times k$ matrices and M is a $k \times (k+r)$ matrix[1]. If $d_s(V,X) < k$, then X decodes to V. Moreover, for any $1 \leq i \leq h-1$ the following are equivalent:

[1]Notice that $t \leq k$. This assumption is not restrictive from the following point of view: the decoder can stop collecting incoming vectors as soon as it receives k inputs (as an alternative, k linearly independent inputs); then it can attempt to decode the collected data.

(1) $S_i = 0_k$,
(2) $\mathrm{rk}(M_i) \leq (t-1)/2$.

Proof. Since the minimum distance of $\mathcal{C}$ is $2k$ (Theorem 2.8) and $d(V,X) < k$, the space X decodes to V. Let us prove (1) $\Rightarrow$ (2). Without loss of generality, we assume that the matrix $\begin{bmatrix} S_1 & \cdots & S_{h-1} & S \end{bmatrix}$ is in reduced row echelon form. Assume that for a fixed index $1 \leq i \leq h-1$ we have $S_i = 0_k$. Since $d(V,X) = t + k - 2\dim(V \cap X) < k$, we have $\dim(V \cap X) > t/2$. By definition of $\mathcal{C}$, exactly one of the following cases occurs:

(a) there exists an index $1 \leq j \leq h-1$ with $j \neq i$ such that $S_j = I_k$;
(b) $S_j = 0_k$ for any $1 \leq j \leq h-1$.

In the former case, let us consider the matrix M_{ij} defined by

$$M_{ij} := \begin{bmatrix} 0_k & I_k \\ M_i & M_j \end{bmatrix}.$$

We have $\mathrm{rk}(M_{ij}) \leq \dim(V+X) = k+t-\dim(V \cap X) < k+t/2$. Since $\mathrm{rk}(M_{ij}) = k+\mathrm{rk}(M_i)$, we have $\mathrm{rk}(M_i) < t/2$. In the latter case, by definition of $\mathcal{C}$, we have $V = \mathrm{rowsp}\begin{bmatrix} 0_k & \cdots & 0_k & 0_{k\times r} & I_k \end{bmatrix}$. Hence

$$k + \mathrm{rk}(M_i) \leq \mathrm{rk}\begin{bmatrix} 0_k & 0_{k\times r} I_k \\ M_i & M \end{bmatrix} \leq \dim(V+X) = k + t - \dim(V \cap X) < k + t/2,$$

and so $\mathrm{rk}(M_i) < t/2$. Now we prove (2) $\Rightarrow$ (1). Assume $\mathrm{rk}(M_i) \leq (t-1)/2$ for some index $1 \leq i \leq h-1$. If $S_i \neq 0_k$ then, by definition of $\mathcal{C}$, $\mathrm{rk}(S_i) = k$. Denote by $\pi : \mathbb{F}_q^n \to \mathbb{F}_q^k$ the projection on the coordinates $ki+1, ki+2, ..., k(i+1)$. Since $\mathrm{rowsp}(S_i) = \pi(V)$ and $\mathrm{rk}(S_i) = k$, we get that $\pi_{|V}$ is surjective. Since $\dim(V) = k$, it follows that $\pi_{|V}$ is also injective. As a consequence,

$$\dim(V \cap X) = \dim(\pi(V \cap X)) \leq \dim(\pi(X)) = \mathrm{rk}(M_i) \leq (t-1)/2,$$

which contradicts the assumption that $d_s(V,X) = k + t - 2\dim(V \cap X) < k$. □

Remark 2.16. Lemma 2.15 has the following useful interpretation. Assume that a partial spread code $\mathcal{C} := \mathcal{C}_q(k,n;p,p')$ is employed for random network coding, and that a t-dimensional vector space, say $X := \mathrm{rowsp}\begin{bmatrix} M_1 & \cdots & M_{h-1} & M \end{bmatrix}$, is received. Assume that there exists a (unique) codeword $V \in \mathcal{C}$ such that $d(V,X) < k$ (i.e., X decodes to V). If $\mathrm{rk}(M_i) \leq (t-1)/2$ for all $1 \leq i \leq h-1$, then $V = \mathrm{rowsp}\begin{bmatrix} 0_k & \cdots & 0_k & 0_{k\times r} & I_k \end{bmatrix}$. Otherwise, let i denote the smallest integer $1 \leq i \leq h-1$ such that $\mathrm{rk}(M_i) > (t-1)/2$. Then there exist unique matrices $A_{i+1}, ..., A_{h-1} \in \mathbb{F}_q[P]$ and a unique matrix $A \in \mathbb{F}_q[P']$ such that $V = \mathrm{rowsp}\begin{bmatrix} 0_k & \cdots & 0_k & I_k & A_{i+1} & \cdots & A_{h-1} & A_{(k)} \end{bmatrix}$, where the identity matrix I_k is the i-th $k \times k$ block.

Lemma 2.17. Following the setup of Remark 2.16, assume $V \neq \mathrm{rowsp}\begin{bmatrix} 0_k & \cdots & 0_k & 0_{k\times r} & I_k \end{bmatrix}$. For any $i+1 \leq j \leq h-1$ we have

$$d_s\left(\mathrm{rowsp}\begin{bmatrix} I_k & A_j \end{bmatrix}, \mathrm{rowsp}\begin{bmatrix} M_i & M_j \end{bmatrix}\right) < k, \qquad d_s\left(\mathrm{rowsp}\begin{bmatrix} I_k & A_{(k)} \end{bmatrix}, \mathrm{rowsp}\begin{bmatrix} M_i & M \end{bmatrix}\right) < k.$$

Proof. Fix an integer j such that $i+1 \leq j \leq h-1$ and denote by $\pi : \mathbb{F}_q^n \to \mathbb{F}_q^{2k}$ the projection on the coordinates $ki+1, ki+2, ..., k(i+1), kj+1, kj+2, ..., k(j+1)$. We have $\pi(V) = \mathrm{rowsp}\begin{bmatrix} I_k & A_j \end{bmatrix}$, and $\pi(X) = \mathrm{rowsp}\begin{bmatrix} M_i & M_j \end{bmatrix}$. In particular $\mathrm{rk}(\pi_{|V}) = k$, hence $\pi_{|V}$ is injective. By the trivial inclusion of vector spaces $\pi(V \cap X) \subseteq \pi(V) \cap \pi(X)$ it follows $\dim \pi(V \cap X) \leq \dim(\pi(V) \cap \pi(X))$.

Therefore

$$\begin{aligned} d(\pi(V),\pi(X)) &= k+\dim\pi(X)-2\dim(\pi(V)\cap\pi(X)) \\ &\leq k+t-2\dim\pi(V\cap X) \\ &= k+t-2\dim(V\cap X) \\ &= d_{\mathrm{s}}(V,X) \\ &< k. \end{aligned}$$

In order to prove that $d_{\mathrm{s}}\left(\mathrm{rowsp}\begin{bmatrix} I_k & A_{(k)}\end{bmatrix},\ \mathrm{rowsp}\begin{bmatrix} M_i & M\end{bmatrix}\right) < k$, we notice that the same argument still works if we choose as $\pi : \mathbb{F}_q^n \to \mathbb{F}_q^{2k+r}$ the projection on the coordinates $ki+1, ki+2, ..., k(i+1), k(h-1)+1, k(h-1)+2, ..., kh, kh+1, ..., kh+r$. □

Remark 2.18. By Lemma 2.17, when decoding a partial spread code we may restrict to one of the two the cases $n = 2k$ and $n = 2k+r$, with $1 \leq r \leq k-1$. Moreover, the lemma allows us to parallelize the computation, reducing the decoding complexity to the case $n = 2k+r$. Notice however that, in the notation of Lemma 2.17 and Remark 2.16, the conditions

$$d_{\mathrm{s}}\left(\mathrm{rowsp}\begin{bmatrix} I_k & A_{(k)}\end{bmatrix},\ \mathrm{rowsp}\begin{bmatrix} M_i & M\end{bmatrix}\right) < k \quad \text{and} \quad d_{\mathrm{s}}\left(\mathrm{rowsp}\begin{bmatrix} I_k & A_j\end{bmatrix},\ \mathrm{rowsp}\begin{bmatrix} M_i & M_j\end{bmatrix}\right) < k$$

for all $i+1 \leq j \leq h-1$ do not guarantee in general that $d_{\mathrm{s}}(X,V) < k$. This is the case for example for the spaces

$$V = \mathrm{rowsp}\begin{bmatrix} 1&0&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0&0\end{bmatrix} \quad \text{and} \quad X = \mathrm{rowsp}\begin{bmatrix} 1&0&0&1&0&0&0&0&0\\ 0&1&0&0&0&0&1&0&0\\ 0&0&1&0&0&0&0&0&0\end{bmatrix}$$

over $\mathbb{F}_2$. In this case the decoding algorithm that we will propose in the next section returns V, even if $d_{\mathrm{s}}(V,X) = 4 > 3 = k$.

2.5 Decoding partial spread codes

In [40] Gorla, Manganiello and Rosenthal propose two efficient decoding procedures for spread codes. The first procedure relies on the decoding algorithm for Reed-Solomon-like codes of [55]. The second procedure is independent from the results of [55], and is more efficient when $k \ll n$. In this section we apply the results of in Section 2.4 to adapt all of the above decoding algorithms to partial spread codes of the form $\mathcal{C}_q(k,n;p,p')$. We start with a preliminary lemma from [40].

Lemma 2.19 ([40], Proposition 15)**.** Let p be an irreducible monic polynomial $p \in \mathbb{F}_q[x]$ of degree k, and denote by $P := \mathbf{M}(p)$ its companion matrix. Choose a root $\lambda \in \mathbb{F}_{q^k}$ of p. Denote by $\varphi : \mathbb{F}_{q^n} \to \mathbb{F}_q^n$ the $\mathbb{F}_q$-isomorphism defined, for any $0 \leq i \leq k-1$, by $\lambda^i \mapsto e_{i+1}$, where $\{e_1, ..., e_k\}$ is the canonical basis of $\mathbb{F}_q^k$. Let $A \in \mathbb{F}_q[P]$ and, for any $1 \leq i \leq k$, let $r_i \in \mathbb{F}_q^k$ denote the i-th row of A. For any $1 \leq i \leq k$ we have $\varphi^{-1}(r_i) = \lambda^{i-1}\varphi^{-1}(r_1)$. In particular, if $f \in \mathbb{F}_{q^k}[x]$ is defined by $f(x) := \varphi^{-1}(r_1)x$, then

$$A = \begin{bmatrix} \varphi(f(\lambda^0)) \\ \varphi(f(\lambda)) \\ \varphi(f(\lambda^2)) \\ \vdots \\ \varphi(f(\lambda^{k-1})) \end{bmatrix}.$$

Notation 2.20. According to Theorem 2.8, in the construction of a partial spread code of the form $\mathcal{C}_q(k, 2k+r, p, p')$ with $0 \leq r \leq k-1$ the companion matrix of p is never involved. Therefore we will simply write $\mathcal{C}_q(k, 2k+r; p')$ in this case.

By Remark 2.18, in order to decode a partial spread code $\mathcal{C}_q(k, n; p, p')$ we may restrict to decoding partial spread codes of the form $\mathcal{C}_q(k, 2k+r; p)$, with $0 \leq r \leq k-1$. The case $r = 0$ can be solved easily. Indeed, by Lemma 2.19, the code $\mathcal{C}_q(k, 2k; p) \setminus \{\text{rowsp}\begin{bmatrix} 0_k & I_k \end{bmatrix}\}$ is a Reed-Solomon-like code (see Definition 1.41) and thus we may simply proceed as in the following Algorithm 1.

Algorithm 1: Decoding a $\mathcal{C}_q(k, 2k; p)$ code.

Data: A decodable[a] t-dimensional space, say X, given as the rowspace of a $(k \times 2k)$-matrix $\begin{bmatrix} M_1 & M_2 \end{bmatrix}$.
Result: The unique $V \in \mathcal{C}_q(k, 2k; p)$ such that $d_s(V, X) < k$, given as a matrix in reduced row echelon form whose rowspace is V.
if $rk(M_1) \leq (t-1)/2$ **then**
  $V = \text{rowsp}\begin{bmatrix} 0_k & I_k \end{bmatrix}$.
else
  Use a decoding algorithm on $\mathcal{C}_q(k, 2k; p) \setminus \{\text{rowsp}\begin{bmatrix} 0_k & I_k \end{bmatrix}\}$ (e.g. the algorithm of [40]).
end

[a] Recall that a vector space X is **decodable** with respect to a subspace code $\mathcal{C}$ if there exists a codeword $V \in \mathcal{C}$ such that $d_s(V, X) \leq \lfloor (d_s(\mathcal{C}) - 1)/2 \rfloor$, $d_s(\mathcal{C})$ being the minimum distance of $\mathcal{C}$. Such a codeword is clearly unique.

Now we focus on the decoding of partial spread codes of the form $\mathcal{C}_q(k, 2k+r; p)$ with $1 \leq r \leq k-1$. In the following Proposition 2.21 we construct a canonical embedding of a partial spread code $\mathcal{C}_q(k, 2k+r; p)$ into the spread code $\mathcal{C}_q(k+r, 2(k+r); p)$. Then we show that any decoding procedure for $\mathcal{C}_q(k+r, 2(k+r); p)$ gives, via this embedding, a decoding procedure for $\mathcal{C}_q(k, 2k+r; p)$.

Proposition 2.21. Let $\mathcal{C} := \mathcal{C}_q(k, 2k+r; p)$ be a partial spread code, with $1 \leq r \leq k-1$. Denote by P the companion matrix of p. Let $X := \text{rowsp}\begin{bmatrix} M_1 & M \end{bmatrix}$ be a t-dimensional vector space in $\mathbb{F}_q^{2k+r}$, where M_1 is a $(k \times k)$-matrix and M is a matrix of size $k \times (k+r)$. Assume that there exists a matrix $A \in \mathbb{F}_q[P]$ such that $d_s\left(\text{rowsp}\begin{bmatrix} I_k & A_{(k)} \end{bmatrix}, \text{rowsp}\begin{bmatrix} M_1 & M \end{bmatrix}\right) < k$. Define the following two $(k+r) \times (k+r)$-matrices:

$$\overline{M}_1 := \begin{bmatrix} 0_r & 0_{r \times k} \\ 0_{k \times r} & M_1 \end{bmatrix}, \qquad \overline{M} := \begin{bmatrix} 0_{r \times (k+r)} \\ M \end{bmatrix}.$$

We have

$$d_s\left(\text{rowsp}\begin{bmatrix} I_{k+r} & A \end{bmatrix}, \text{rowsp}\begin{bmatrix} \overline{M}_1 & \overline{M} \end{bmatrix}\right) < k + r.$$

Proof. Set $V := \text{rowsp}\begin{bmatrix} I_k & A_{(k)} \end{bmatrix}$ and observe that the hypothesis $d_s(V, X) < k$ can be restated as $\dim(V \cap X) > t/2$. Define $\overline{V} := \text{rowsp}\begin{bmatrix} I_{k+r} & A \end{bmatrix}$ and $\overline{X} := \text{rowsp}\begin{bmatrix} \overline{M}_1 & \overline{M} \end{bmatrix}$. By construction,

$\dim_{\mathbb{F}_q} X = \dim_{\mathbb{F}_q} \overline{X} = t$ and $\dim_{\mathbb{F}_q}(\overline{V} \cap \overline{X}) \geq \dim_{\mathbb{F}_q}(V \cap X)$. It follows that

$$\begin{aligned} d_{\mathrm{s}}(\overline{V}, \overline{X}) &= \dim_{\mathbb{F}_q} \overline{V} + \dim_{\mathbb{F}_q} \overline{X} - 2\dim_{\mathbb{F}_q}(\overline{V} \cap \overline{X}) \\ &= k + r + t - 2\dim_{\mathbb{F}_q}(\overline{V} \cap \overline{X}) \\ &\leq k + r + t - 2\dim_{\mathbb{F}_q}(V \cap X) \\ &< k + r + t - 2(t/2) \\ &= k + r, \end{aligned}$$

as claimed. □

Remark 2.22. Proposition 2.21 has the following useful interpretation. Assume that a partial spread code $\mathcal{C}_q(k, 2k + r; p)$ is given, with $1 \leq r \leq k - 1$, and $X := \mathrm{rowsp}\begin{bmatrix} M_1 & M \end{bmatrix}$ is received (M_1 and M being as in the statement of the proposition). Then we may construct the matrices $\overline{M}_1$ and $\overline{M}$ as described, and consider the vector space $\overline{X} := \mathrm{rowsp}\begin{bmatrix} \overline{M}_1 & \overline{M} \end{bmatrix}$. The minimum distance of the (partial) spread code $\mathcal{C}_q(k + r, 2(k + r); p)$ is $2(k + r)$. By Proposition 2.21, if X decodes to $V := \mathrm{rowsp}\begin{bmatrix} I_k & A_{(k)} \end{bmatrix}$ in $\mathcal{C}_q(k, 2k + r; p)$, then $\overline{X}$ decodes to $\overline{V} := \mathrm{rowsp}\begin{bmatrix} I_{k+r} & A \end{bmatrix}$ in $\mathcal{C}_q(k+r, 2(k+r); p)$. It follows that Algorithm 1 (with $k \leftarrow k+r$) applied to $\overline{X}$ produces $\begin{bmatrix} I_{k+r} & A \end{bmatrix}$. Finally, V is the rowspace of the matrix obtained by deleting the first r rows and the first r columns of $\begin{bmatrix} I_{k+r} & A \end{bmatrix}$. All of this leads to the following Algorithm 2.

Algorithm 2: Decoding a $\mathcal{C}_q(k, 2k + r; p)$ code with $1 \leq r \leq k - 1$.

Data: A decodable t-dimensional space, say X, given as the rowspace of a $(k \times 2k + r)$-matrix $\begin{bmatrix} M_1 & M \end{bmatrix}$.

Result: The unique $V \in \mathcal{C}_q(k, 2k + r; p)$ such that $d_{\mathrm{s}}(V, X) < k$, given as a matrix in reduced row echelon form whose rowspace is V.

if $rk(M_1) \leq (t - 1)/2$ **then**

  $V = \mathrm{rowsp}\begin{bmatrix} 0_k & 0_{k\times r} & I_k \end{bmatrix}$.

else

  Construct the matrix $\begin{bmatrix} \overline{M}_1 & \overline{M} \end{bmatrix}$ as explained in Lemma 2.21. Use Algorithm 1 with $\mathcal{C}_q(k + r, 2(k + r); p)$ on $\begin{bmatrix} \overline{M}_1 & \overline{M} \end{bmatrix}$. Delete the first r rows and the first r columns of the output.

end

By Proposition 2.21, in Algorithm 2 we may replace the use of Algorithm 1 with any other decoding algorithm for spread codes.

Chapter 3

Equidistant subspace codes

In this chapter we study equidistant subspace codes, i.e., constant dimension subspace codes with the property that the distance between of any pair of codewords is the same. Equidistant codes can be viewed as a natural generalization of partial spread codes, which we treated in Chapter 2.

Equidistant subspace codes were shown to have relevant applications in distributed storage in [28]. In the same paper, Etzion and Raviv identify two trivial families of equidistant codes, namely, sunflowers and balls. A ball is a subspace code in the Grassmannian $\mathcal{G}_q(k,n)$ of k-dimensional subspaces of $\mathbb{F}_q^n$ with the property that all the elements of the code are contained in a fixed $(k+1)$-dimensional subspace of $\mathbb{F}_q^n$. Sunflowers will be defined in Section 3.1. They then proceed to study the question of when an equidistant code belongs to one of the two families. Starting from the observation that the orthogonal of a ball is a sunflower, in this chapter we study the question of when an equidistant code is either a sunflower, or the orthogonal of a sunflower.

One of our main results, presented in Section 3.3, is a structural classification of equidistant subspace codes over finite fields of sufficiently large cardinality. More precisely, in Theorem 3.24 we prove that, for most choices of the parameters, an equidistant code of maximum cardinality is either a sunflower or the orthogonal of a sunflower. In addition, for most values of the parameters we show that the two possibilities are mutually exclusive.

In Section 3.2 we also study extremal equidistant codes, i.e., codes for which every two distinct codewords intersect in codimension one. We show that each such code is either a sunflower or the orthogonal of a sunflower, over finite fields of any size and for a code of any cardinality.

Section 3.4 is devoted to general properties of equidistant codes that are not sunflowers. We define the number of centers of a subspace code $\mathcal{C}$ to be the integer $t(\mathcal{C}) = |\{U \cap V : U, V \in \mathcal{C},\ U \neq V\}|$, and provide an asymptotic estimate for such number for the class of equidistant codes that are not sunflowers. Our result shows that if $\mathcal{C}$ is an equidistant code of large cardinality, then either $\mathcal{C}$ is a sunflower, or it has a large number of centers.

In Section 3.5 we give a systematic construction of asymptotically optimal equidistant codes based on the construction of partial spread codes of Chapter 2. In Sections 3.6 and 3.7 we exploit the structure of our codes to design an efficient decoding algorithm for them and for their orthogonals.

The results of this chapter have been published in [39].

Notation 3.1. In the sequel q denotes a prime power, and k, n two integers with $0 < k < n$. Recall that $\mathcal{G}_q(k,n)$ is the set of k-dimensional subspaces of $\mathbb{F}_q^n$. All dimensions are computed over $\mathbb{F}_q$.

3.1 Equidistant codes, partial spreads, and sunflowers

We start by presenting some preliminary definitions and results concerning equidistant codes.

Definition 3.2. A subspace code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ is **equidistant** if for all $U, V \in \mathcal{C}$ with $U \neq V$ we have $d_s(U,V) = d_s(\mathcal{C})$. An equidistant code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ is **c-intersecting** if $d_s(\mathcal{C}) = 2(k-c)$. Notice that in this case one has $\dim(U \cap V) = c$ for all $U, V \in \mathcal{C}$ with $U \neq V$ by Definition 1.9.

Equidistant c-intersecting codes only exist for $n \geq 2k-c$, since subspace codes contain at least two codewords by Definition 1.8.

Given an integer $0 \leq c \leq k-1$, we denote by $e_q(k,n,c)$ the largest cardinality of an equidistant c-intersecting subspace code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$.

Definition 3.3. An equidistant c-intersecting code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ is **optimal** if $|\mathcal{C}| = e_q(k,n,c)$. A family of codes $\mathcal{C}_q \subseteq \mathcal{G}_q(k,n)$ is **asymptotically optimal** if $\lim_{q\to\infty} |\mathcal{C}_q|/e_q(k,n,c) = 1$.

The partial spreads of Definition 2.3 are a first example of equidistant subspace codes. The maximum cardinality of a partial spread $\mathcal{S} \subseteq \mathcal{G}_q(k,n)$ is $e_q(k,n,0)$ by definition. Combining Lemma 2.4 and Lemma 2.5 from Chapter 2 we obtain the following result.

Theorem 3.4. Let r denote the remainder obtained dividing n by k. We have

$$\frac{q^n - q^r}{q^k - 1} - q^r + 1 \leq e_q(k,n,0) \leq \frac{q^n - q^r}{q^k - 1}.$$

The lower and upper bound of Theorem 3.4 agree when $r = 0$. In this case k divides n and the bound is always attained by spreads (see Definition 2.2). Sunflowers are a main source of examples of equidistant codes.

Definition 3.5. A subspace code $\mathcal{F} \subseteq \mathcal{G}_q(k,n)$ is a **sunflower** if there exists a subspace $C \subseteq \mathbb{F}_q^n$ such that for all $U, V \in \mathcal{F}$ with $U \neq V$ we have $U \cap V = C$. The space C is called the **center** of the sunflower $\mathcal{F}$.

A sunflower $\mathcal{F} \subseteq \mathcal{G}_q(k,n)$ with center C of dimension c is an equidistant c-intersecting subspace code with minimum distance $2(k-c)$. The connection between partial spreads and sunflowers is described in the following remark. The same observation appears in [28], Theorems 10 and 11.

Remark 3.6. Let $\mathcal{F} \subseteq \mathcal{G}_q(k,n)$ be a sunflower with center C of dimension c, and let $\varphi : \mathbb{F}_q^n/C \to \mathbb{F}_q^{n-c}$ be an isomorphism. Then the subspace code

$$\mathcal{S} := \{\varphi(U/C) : U \in \mathcal{F}\} \subseteq \mathcal{G}_q(k-c, n-c)$$

is a partial spread with $|\mathcal{S}| = |\mathcal{F}|$. Conversely, given an integer $0 \leq c \leq k-1$, a partial spread $\mathcal{S} \subseteq \mathcal{G}_q(k-c, n-c)$, and a subspace $C \subseteq \mathbb{F}_q^n$, the subspace code $\mathcal{F} := \{C \oplus U : U \in \mathcal{S}\} \subseteq \mathcal{G}_q(k,n)$ is a sunflower with center C and $|\mathcal{F}| = |\mathcal{S}|$.

By Remark 3.6 one easily obtains the following corollary.

Corollary 3.7. For all $0 \leq c \leq k-1$ we have $e_q(k,n,c) \geq e_q(k-c,n-c,0)$.

The following result shows that equidistant codes of large cardinality are sunflowers. The proof is based on a result by Deza on classical codes (see [21] and [22]), applied in the context of network coding by Etzion and Raviv.

Theorem 3.8 ([28], Theorem 1)**.** Let $0 \leq c \leq k-1$ be an integer, and let $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ be a c-intersecting equidistant code. Assume that

$$|\mathcal{C}| \geq ((q^k - q^c)/(q-1))^2 + (q^k - q^c)/(q-1) + 1.$$

Then $\mathcal{C}$ is a sunflower.

Remark 3.9. Deza conjectured that any c-intersecting equidistant code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ with $|\mathcal{C}| > (q^{k+1}-1)/(q-1)$ is a sunflower (see [28], Conjecture 1). The conjecture was disproved in [28], Section 3.2, where the authors give an example of an equidistant code $\mathcal{C} \subseteq \mathcal{G}_2(3,6)$ of minimum distance 4 and cardinality 16, which is not a sunflower. The example was found employing exhaustive computer search.

Recall that the orthogonal of a subspace code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ is $\mathcal{C}^\perp := \{U^\perp : U \in \mathcal{C}\} \subseteq \mathcal{G}_q(n-k,n)$, where $U^\perp$ is the orthogonal of U with respect to the standard inner product of $\mathbb{F}_q^n$.

Remark 3.10. For any $U, V \in \mathcal{G}_q(k,n)$ we have $\dim(U^\perp \cap V^\perp) = n - 2k + \dim(U \cap V)$. In particular, $d_{\mathrm{s}}(\mathcal{C}) = d_{\mathrm{s}}(\mathcal{C}^\perp)$ for any subspace code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ Moreover, the orthogonal of a c-intersecting equidistant code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ is a $(n-2k+c)$-intersecting equidistant code (see also Theorem 13 and Theorem 14 of [28]). Notice that $n - 2k + c \geq 0$, since $\mathcal{C}$ contains at least two distinct codewords by definition. This proves that

$$e_q(k,n,c) = e_q(n-k,n,n-2k+c)$$

for all $0 \leq c \leq k-1$, and that the orthogonal of an optimal equidistant code is an optimal equidistant code.

We close this section with the definition of span of a code.

Definition 3.11. The **span** of a subspace code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ is $\mathrm{span}(\mathcal{C}) := \sum_{U \in \mathcal{C}} U \subseteq \mathbb{F}_q^n$.

3.2 Extremal equidistant codes

In this section we study $(k-1)$-intersecting codes in $\mathcal{G}_q(k,n)$. We call such codes **extremal**, as $k-1$ is the largest possible value of c, for given k and n. These codes are equidistant with minimum distance 2. In particular, the orthogonal of an extremal code is extremal. Our main result shows that every extremal equidistant code is either a sunflower, or the orthogonal of a sunflower. In Section 3.3 we establish a similar result for most choices of (k,n,c) and for sufficiently large q.

Proposition 3.12. Let $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ be a c-intersecting equidistant code. The following are equivalent:

1. $\mathcal{C}$ is a sunflower,
2. $\dim \mathrm{span}(\mathcal{C}^\perp) = n - c$,
3. for all $A, B \in \mathcal{C}$ with $A \neq B$ we have $\mathrm{span}(\mathcal{C}^\perp) = A^\perp + B^\perp$.

Proof. Properties (2) and (3) are clearly equivalent. The code $\mathcal{C}$ is a sunflower if and only if there exists $C \subseteq \mathbb{F}_q^n$ with $\dim(C) = c$ such that $A \cap B = C$ for all $A, B \in \mathcal{C}$ with $A \neq B$. The condition $A \cap B = C$ is equivalent to $A^\perp + B^\perp = C^\perp$. Hence (1) and (3) are equivalent. □

The following is a simple classification of $(k-1)$-intersecting codes in $\mathcal{G}_q(k,n)$.

Proposition 3.13. Let $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ be a $(k-1)$-intersecting equidistant code. Then either $\mathcal{C}$ is a sunflower, or $\mathcal{C}^\perp$ is a sunflower.

Proof. If $|\mathcal{C}| = 2$ the result is trivial. Assume $|\mathcal{C}| \geq 3$ and that $\mathcal{C}$ is not a sunflower. Let $A, B \in \mathcal{C}$ with $A \neq B$. By Proposition 3.12 it suffices to show that $\mathrm{span}(\mathcal{C}) = A + B$. Since $\mathcal{C}$ is not a sunflower, there exists $D \in \mathcal{C} \setminus \{A, B\}$ such that $D \cap A \neq D \cap B$. Since $D \supseteq D \cap A + D \cap B$ and $\dim(D \cap A + D \cap B) \geq \dim(D \cap A) + 1 = k$, then $D = D \cap A + D \cap B \subseteq A + B$. For any $E \in \mathcal{C} \setminus \{A, B, D\}$ we have $E \supseteq E \cap A + E \cap B + E \cap D$. Since $\dim(A \cap B \cap D) < k-1$, then $E \cap A$, $E \cap B$, and $E \cap D$ are not all equal. Hence $\dim(E \cap A + E \cap B + E \cap D) \geq \dim(E \cap A) + 1 = k$ and $E = E \cap A + E \cap B + E \cap D \subseteq A + B$. Therefore $\mathrm{span}(\mathcal{C}) = A + B$. □

As a corollary, we obtain an improvement of Theorem 12 and Corollary 1 of [28].

Corollary 3.14. Let $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ be a $(k-1)$-intersecting equidistant code. If $\mathcal{C}$ is not a sunflower, then it is a subset of the set of k-dimensional subspaces of a given $(k+1)$-dimensional space. In particular, if $|\mathcal{C}| > \begin{bmatrix} k+1 \\ k \end{bmatrix}$, then $\mathcal{C}$ is a sunflower.

Proof. If $\mathcal{C}$ is not a sunflower, then by Proposition 3.13 the orthogonal code $\mathcal{C}^\perp$ is a sunflower. By Proposition 3.12 this is equivalent to $\dim(\mathrm{span}(\mathcal{C})) = k+1$. Then all the codewords of $\mathcal{C}$ are contained in a fixed $(k+1)$-dimensional space of $\mathbb{F}_q^n$. In particular, their number cannot exceed the number of k-dimensional subspaces of a $(k+1)$-dimensional space. □

Remark 3.15. Combining Theorem 3.4, Corollary 3.7, and Corollary 3.14, we have that if $\mathcal{C}$ has maximum cardinality $e_q(k, n, k-1)$ and $n \gg 0$, then $\mathcal{C}$ is a sunflower. Moreover, as observed in [28], the bound of Corollary 3.14 is optimal for any k, n. In fact, let $\mathcal{C}$ be the set of k-dimensional subspaces of a fixed $(k+1)$-dimensional space of $\mathbb{F}_q^n$. $\mathcal{C}$ is a constant dimension $(k-1)$-intersecting code of cardinality

$$\begin{bmatrix} k+1 \\ k \end{bmatrix} = \frac{q^{k+1}-1}{q-1}$$

which is not a sunflower.

3.3 A classification of equidistant codes

In this section we provide a classification of optimal equidistant codes for most values of the parameters. More precisely we prove that, for $q \gg 0$ and for most values of k and n, every optimal equidistant code is either a sunflower or the orthogonal of a sunflower. We start by studying the case when k is small with respect to n.

Proposition 3.16. Let $q \gg 0$ and $n \geq 3k-1$. Then

$$e_q(k, n, c) = e_q(k-c, n-c, 0).$$

Moreover, any c-intersecting equidistant code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ of cardinality $e_q(k, n, c)$ is a sunflower.

Proof. Let $0 \leq r \leq k-c-1$ denote the remainder obtained dividing $n-c$ by $k-c$. Since $n > 3k-2 \geq 2k-1$, we have $r \leq k-1 < n-k$. Therefore

$$\lim_{q\to\infty} \frac{\frac{q^{n-c}-q^r}{q^{k-c}-1} - q^r + 1}{q^{n-k}} = 1.$$

Since $k < (n+2)/3$ we have $n-k > 2k-2$. Thus

$$\lim_{q\to\infty} \frac{\left(\frac{q^k-q^c}{q-1}\right)^2 + \frac{q^k-q^c}{q-1} + 1}{q^{n-k}} = 0.$$

Therefore

$$\lim_{q\to\infty} \frac{\frac{q^{n-c}-q^r}{q^{k-c}-1} - q^r + 1 - \left[\left(\frac{q^k-q^c}{q-1}\right)^2 + \frac{q^k-q^c}{q-1} + 1\right]}{q^{n-k}} = 1.$$

In particular, for $q \gg 0$ we have

$$\frac{q^{n-c}-q^r}{q^{k-c}-1} - q^r + 1 \geq \left(\frac{q^k-q^c}{q-1}\right)^2 + \frac{q^k-q^c}{q-1} + 1.$$

By Theorem 3.4 and Corollary 3.7 we have

$$|\mathcal{C}| \geq \frac{q^{n-c}-q^r}{q^{k-c}-1} - q^r + 1 \geq \left(\frac{q^k-q^c}{q-1}\right)^2 + \frac{q^k-q^c}{q-1} + 1.$$

Thus $\mathcal{C}$ is a sunflower by Theorem 3.8. By Remark 3.6 we have $e_q(k,n,c) = e_q(k-c, n-c, 0)$. □

Notice that the case $n \gg k$ is the most relevant from the point of view of network coding. For completeness we also examine the case when n is small with respect to k.

Proposition 3.17. Let $q \gg 0$ and $n \leq (3k+1)/2$. Then

$$e_q(k,n,c) = e_q(k-c, 2k-c, 0).$$

Moreover, every c-intersecting equidistant code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ of cardinality $e_q(k,n,c)$ is of the form $\mathcal{S}^\perp$, where $\mathcal{S}$ is a sunflower.

Proof. By Remark 3.10 we have $e_q(k,n,c) = e_q(n-k, n, n-2k+c)$. Since $n \geq 3(n-k)-1$, the result follows from Proposition 3.16. □

Proposition 3.16 and Proposition 3.17 imply that for $n \leq (3k+1)/2$ or for $n \geq 3k-1$ and $q \gg 0$, every equidistant code of maximum cardinality $e_q(k,n,c)$ is either a sunflower, or the orthogonal of a sunflower. We now show that these families are almost always disjoint.

Lemma 3.18. Let $\mathcal{S} \subseteq \mathcal{G}_q(k,n)$ be a sunflower with center C of dimension $0 \leq c \leq k-1$ and $\operatorname{span}(\mathcal{S}) = \mathbb{F}_q^n$. Assume that $n > 2k-c$. Then $\mathcal{S}^\perp$ is not a sunflower.

Proof. By contradiction, assume that $\mathcal{S}^\perp \subseteq \mathcal{G}_q(n-k,n)$ is a sunflower with center D. By Remark 3.10 we have $\dim(D) = n-2k+c > 0$. Moreover, $D \subseteq U^\perp$ for all $U \in \mathcal{S}$, i.e., $U \subseteq D^\perp$ for all $U \in \mathcal{S}$. Then $\mathbb{F}_q^n = \operatorname{span}(\mathcal{S}) \subseteq D^\perp$, which contradicts the assumption that $D \neq 0$. □

Remark 3.10 and Lemma 3.18 allow us to construct a family of equidistant codes which are not sunflowers and have maximum cardinality for their parameters.

Example 3.19. Let $n = \ell k$, $\ell > 2$. Let $\mathcal{S} \subseteq \mathcal{G}_q(k, \ell k)$ be a spread. Then $\mathcal{S}^\perp$ is an optimal equidistant code which is not a sunflower by Lemma 3.18. We have

$$|\mathcal{S}^\perp| = |\mathcal{S}| = e_q(k, \ell k, 0) = e_q((\ell-1)k, \ell k, (\ell-2)k),$$

where the last equality follows from Remark 3.10.

Setting $k = 1$ we recover two well-known examples of equidistant codes: $\mathcal{S}$ is the set of lines in $\mathbb{F}_q^\ell$ and $\mathcal{S}^\perp$ is the set of $(\ell-1)$-dimensional subspaces of $\mathbb{F}_q^\ell$.

Now we prove that a c-intersecting sunflower $\mathcal{S} \subseteq \mathcal{G}_q(k, n)$ with maximum cardinality $e_q(k, n, c)$ is never contained in a proper subspace of $\mathbb{F}_q^n$.

Proposition 3.20. Let $\mathcal{S} \subseteq \mathcal{G}_q(k, n)$ be a sunflower with center of dimension $0 \leq c \leq k-1$. Let r denote the remainder obtained dividing $n-c$ by $k-c$. If

$$|\mathcal{S}| \geq \frac{q^{n-c} - q^r}{q^{k-c} - 1} - q^r + 1,$$

then $\operatorname{span}(\mathcal{S}) = \mathbb{F}_q^n$. In particular, if $|\mathcal{S}| = e_q(k, n, c)$ then $\operatorname{span}(\mathcal{S}) = \mathbb{F}_q^n$.

Proof. Since $\mathcal{S}$ is a sunflower with center of dimension c, we have

$$\begin{aligned} |\bigcup_{V \in \mathcal{S}} V| &= q^c + |\mathcal{S}|(q^k - q^c) \\ &\geq q^c + q^c(q^{k-c} - 1)\left(\frac{q^{n-c} - q^r}{q^{k-c} - 1} - q^r + 1\right) \\ &= q^n + q^k - q^{k+r} \\ &\geq q^n + q^k - q^{2k-c-1}. \end{aligned}$$

Since $|\mathcal{S}| \geq 2$, then $n \geq 2k - c$, hence $q^n + q^k - q^{2k-c-1} \geq q^n + q^k - q^{n-1} > q^{n-1}$. Therefore $\mathcal{S}$ cannot be contained in a proper subspace of $\mathbb{F}_q^n$. The second part of the statement follows from Corollary 3.7 and Theorem 3.4. □

Corollary 3.21. Let $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ be a c-intersecting equidistant code with $|\mathcal{C}| = e_q(k, n, c)$. Then $\mathcal{C}$ and $\mathcal{C}^\perp$ are both sunflowers if and only if $n = 2k$ and both $\mathcal{C}$ and $\mathcal{C}^\perp$ are spreads.

Proof. Assume that both $\mathcal{C}$ and $\mathcal{C}^\perp$ are sunflowers. By Remark 3.10 the center of $\mathcal{C}^\perp$ has dimension $c' = n - 2k + c \geq 0$. Since $|\mathcal{C}| = e_q(k, n, c)$, Proposition 3.20 and Lemma 3.18 applied to $\mathcal{C}$ give $c' = 0$. In particular, $\mathcal{C}^\perp$ is a partial spread. Since $\mathcal{C}$ is optimal, then $\mathcal{C}^\perp$ is optimal by Remark 3.10. By Proposition 3.20 and Lemma 3.18, $c = n - 2(n-k) + c' = 0$. Hence $n = 2k$ and $\mathcal{C}$ is a partial spread. Since $n = 2k$ and $\mathcal{C}$ and $\mathcal{C}^\perp$ have maximum cardinality, they are spreads. □

By Corollary 3.21, when $n = 2k$ and $c = 0$ every 0-intersecting equidistant code $\mathcal{C} \subseteq \mathcal{G}_q(k, 2k)$ of maximum cardinality is a spread, and its orthogonal is again a spread with the same parameters. Thus in this case every equidistant code of maximum cardinality is a sunflower, as well as its orthogonal.

Remark 3.22. For $n = 2k$ and $c > 0$ we have $e_q(k, 2k, c) \geq e_q(k-c, 2k-c, 0)$ by Corollary 3.7, and the two quantities do not always agree, e.g.

$$e_q(3, 6, 1) > e_q(2, 5, 0),$$

as shown in the next example. Moreover, for any k, c for which $e_q(k, 2k, c) = e_q(k-c, 2k-c, 0)$, let $\mathcal{C} \subseteq \mathcal{G}_q(k, 2k)$ be a c-intersecting sunflower of cardinality $e_q(k, 2k, c)$. Then by Corollary 3.21 we also have a c-intersecting equidistant code $\mathcal{C}^\perp \subseteq \mathcal{G}_q(k, 2k)$ of maximum cardinality which is not a sunflower. Hence for any k, c we have c-intersecting equidistant codes $\mathcal{C} \subseteq \mathcal{G}(k, 2k)$ of maximum cardinality which are not sunflowers, but we may not always have sunflower codes of the same cardinality.

In addition, it may be possible to also have an equidistant code $\mathcal{C} \subseteq \mathcal{G}_q(k, 2k)$ of maximum cardinality $e_q(k, 2k, c)$ such that neither $\mathcal{C}$ nor $\mathcal{C}^\perp$ are sunflowers. This is the case of the following example.

Example 3.23 ([6], Example 1.2)**.** The hyperbolic Klein set $\mathcal{C} \subseteq \mathcal{G}(3, 6)$ is an equidistant code with $c = 1$ and $|\mathcal{C}| = q^3 + q^2 + q + 1$. The code $\mathcal{C}$ is not a sunflower, nor the orthogonal of a sunflower, since the largest possible cardinality of a sunflower with $k = 3, n = 6, c = 1$ is

$$e_q(2, 5, 0) \leq \frac{q^5 - q}{q^2 - 1} = q^3 + q < |\mathcal{C}| = |\mathcal{C}^\perp|,$$

where the inequality follows from Theorem 3.4. In particular, $e_q(3, 6, 1) > e_q(2, 5, 0)$.

The hyperbolic Klein set of Example 3.23 is a well-known object in discrete mathematics. Given a hyperbolic quartic $\mathcal{Q}$ in a 5-dimensional projective space over $\mathbb{F}_q$, one can consider a special family of planes, called $\mathcal{Q}$-planes, arising from $\mathcal{Q}$. It can be shown that such family of $\mathcal{Q}$-planes splits into two equivalent classes, one of which is precisely the hyperbolic Klein set of Example 3.23. We refer the interested reader to [7], Chapter 4.

Combining Propositions 3.13, 3.16, 3.17, 3.20, and Corollary 3.21 one easily obtains the following classification of equidistant codes of maximum cardinality.

Theorem 3.24. Let $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ be a c-intersecting equidistant code with $|\mathcal{C}| = e_q(k, n, c)$. Assume that one of the following conditions holds:

- $c \in \{0, k-1, 2k-n\}$,
- $n \leq (3k+1)/2$ and $q \gg 0$,
- $n \geq 3k+1$ and $q \gg 0$.

Then either $\mathcal{C}$ is a sunflower or $\mathcal{C}^\perp$ is a sunflower, and the two facts are mutually exclusive unless $c = 0$ and $n = 2k$.

Recall that $n \gg k$ is the relevant situation within network coding. Moreover, one needs to assume $q \gg 0$ in order to have a solution to the network coding problem (see Chapter 1).

3.4 Other properties of equidistant codes

We devote this section to equidistant codes that are not sunflowers. The property of having a center characterizes sunflowers among equidistant codes.

Definition 3.25. Let $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ be a c-intersecting equidistant code, $0 \leq c \leq k-1$. The **set of centers** of $\mathcal{C}$ is $T(\mathcal{C}) := \{U \cap V : U, V \in \mathcal{C},\ U \neq V\}$, and the **number of centers** of $\mathcal{C}$ is $t(\mathcal{C}) := |T(\mathcal{C})|$. The **set of petals** attached to a center $A \in T(\mathcal{C})$ is $\mathcal{P}(A) := \{U \in \mathcal{C} : A \subseteq U\}$.

In the next proposition we show that equidistant codes of sufficiently large cardinality are either sunflowers, or they have a large number of centers.

Proposition 3.26. Let $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ be an c-intersecting equidistant code, $0 \leq c \leq k-1$. One of the following properties holds:

1. $\mathcal{C}$ is a sunflower, or
2. $t(\mathcal{C}) \geq |\mathcal{C}| \frac{q^c - q^{c-1}}{q^k - q^{c-1}}$.

Proof. If $\mathcal{C}$ is not a sunflower, then $t := t(\mathcal{C}) \geq 2$. Choose an enumeration $T(\mathcal{C}) = \{A_1, ..., A_t\}$. Since $\mathcal{C} = \bigcup_{i=1}^{t} \mathcal{P}(A_i)$, we have

$$|\mathcal{C}| \leq \sum_{i=1}^{t} |\mathcal{P}(A_i)|. \tag{3.1}$$

For any $i \in \{1, ..., t\}$, $\mathcal{P}(A_i)$ is a sunflower with c-dimensional center A_i, minimum distance $2(k-c)$, and cardinality $s_i := |\mathcal{P}(A_i)|$. If $V \in \mathcal{C} \setminus \mathcal{P}(A_i)$, then

$$|V| \geq \left| V \cap \bigcup_{U \in \mathcal{P}(A_i)} U \right| = \sum_{U \in \mathcal{P}(A_i)} |V \cap U| - (s_i - 1)|V \cap A_i| = s_i|A_i| - (s_i - 1)|V \cap A_i|$$

hence $q^k \geq s_i q^c - (s_i - 1)q^{c-1} = s_i(q^c - q^{c-1}) + q^{c-1}$. Therefore we have shown that

$$|\mathcal{P}(A_i)| \leq \frac{q^k - q^{c-1}}{q^c - q^{c-1}}$$

for all $1 \leq i \leq t$, and the result follows by (3.1). □

In particular, for a code with maximum cardinality which is not a sunflower, we can give the following asymptotic estimate of the number of centers as q grows.

Corollary 3.27. Let $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ be a c-intersecting equidistant code. Assume that $|\mathcal{C}| = e_q(k,n,c)$ and that $\mathcal{C}$ is not a sunflower. Denote by r the remainder of the division of $n-c$ by $k-c$. Then

$$t(\mathcal{C}) \geq e_q(k,n,c) \frac{q^c - q^{c-1}}{q^k - q^{c-1}} \geq \left(\frac{q^{n-c} - q^r}{q^{k-c} - 1} - q^r + 1 \right) \frac{q^c - q^{c-1}}{q^k - q^{c-1}}.$$

In particular, $\lim_{q \to \infty} t(\mathcal{C}) q^{-(n-2k+c)} \in [1, +\infty]$.

Proof. The inequality follows by Proposition 3.26, Corollary 3.7, and Theorem 3.4. Hence

$$\lim_{q \to \infty} t(\mathcal{C}) q^{-(n-2k+c)} \geq \lim_{q \to \infty} \left(\frac{q^{n-c} - q^r}{q^{k-c} - 1} - q^r + 1 \right) \frac{q^c - q^{c-1}}{q^k - q^{c-1}} q^{-(n-2k+c)} = 1,$$

as claimed. □

The orthogonal of a sunflower is often an example of an optimal code with a large number of centers.

Example 3.28. Let $0 < c \leq k-1$, $\mathcal{S} \subseteq \mathcal{G}_q(n-k,n)$ be a sunflower of maximum cardinality with $(n-2k+c)$-dimensional center. Let $\mathcal{C} = \mathcal{S}^\perp \subseteq \mathcal{G}_q(k,n)$, then $\mathcal{C}$ is c-intersecting and $|\mathcal{C}| = |\mathcal{S}|$. The code $\mathcal{C}$ is not a sunflower by Corollary 3.21 and it has

$$t(\mathcal{C}) = \binom{|\mathcal{C}|}{2}.$$

In fact, for any $A, B, D \in \mathcal{S}$ pairwise distinct one has

$$\dim(A+B)^\perp = n-2k+c > n-3k+2c = \dim(A+B+D)^\perp,$$

hence

$$A^\perp \cap B^\perp \neq A^\perp \cap B^\perp \cap D^\perp.$$

In particular, there exist no distinct $A^\perp, B^\perp, D^\perp \in \mathcal{C}$ such that $A^\perp \cap D^\perp = B^\perp \cap D^\perp$. Similarly one shows that there exist no distinct $A^\perp, B^\perp, D^\perp, E^\perp \in \mathcal{C}$ such that $A^\perp \cap D^\perp = B^\perp \cap E^\perp$.

3.5 Construction of sunflower codes

In this section we modify the construction of partial spreads proposed in Chapter 2 to systematically produce sunflower codes for any choice of the parameters k, n, c. An efficient decoding algorithm for our codes is given in Section 3.6.

In the following we denote by I_m an identity matrix of size $m \times m$, by 0_m a zero matrix of size $m \times m$, and by $0_{m\times\ell}$ a zero matrix of size $m \times \ell$. Recall from Lemma 2.6 that the companion matrix of an irreducible monic polynomial $p \in \mathbb{F}_q[x]$ of degree $s \geq 1$ is the $s \times s$ matrix

$$\mathbf{M}(p) := \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & & 1 \\ -p_0 & -p_1 & -p_2 & \cdots & -p_{s-1} \end{bmatrix}.$$

The construction of sunflower codes which we propose is based on companion matrices of polynomials. It extends the construction of partial spread codes presented in Chapter 2.

Theorem 3.29. Let $1 \leq k < n$ and $\min\{0, 2k-n\} \leq c \leq k-1$ be integers. Write $n-c = h(k-c)+r$, with $0 \leq r \leq k-c-1$, $h \geq 2$. Choose irreducible monic polynomials $p, p' \in \mathbb{F}_q[x]$ of degree $k-c$ and $k-c+r$, respectively. Set $P := \mathbf{M}(p)$ and $P' := \mathbf{M}(p')$. For $1 \leq i \leq h-1$ let $\mathcal{M}_i(p,p')$ be the set of $k \times n$ matrices of the form

$$\begin{bmatrix} I_c & 0_{c\times(k-c)} & \cdots & \cdots & \cdots & \cdots & \cdots & 0_{c\times(k-c)} & 0_{c\times(k-c+r)} \\ 0_{(k-c)\times c} & 0_{k-c} & \cdots & 0_{k-c} & I_{k-c} & A_{i+1} & \cdots & A_{h-1} & A_{(k-c)} \end{bmatrix},$$

where we have $i-2$ consecutive copies of 0_{k-c}, the matrices $A_{i+1}, ..., A_{h-1} \in \mathbb{F}_q[P]$, $A \in \mathbb{F}_q[P']$, and $A_{(k-c)}$ denotes the last $k-c$ rows of A. The set

$$\begin{aligned} \mathcal{C} := \quad & \bigcup_{i=1}^{h-1} \{\mathrm{rowsp}(M) : M \in \mathcal{M}_i(p,p')\} \\ \cup \quad & \left\{ \mathrm{rowsp} \begin{bmatrix} I_c & 0_{c\times(k-c)} & \cdots & 0_{c\times(k-c)} & 0_{c\times(k-c+r)} & 0_{c\times(k-c)} \\ 0_{(k-c)\times c} & 0_{k-c} & \cdots & 0_{k-c} & 0_{(k-c)\times(k-c+r)} & I_{k-c} \end{bmatrix} \right\} \end{aligned}$$

is a sunflower in $\mathcal{G}_q(k,n)$ of cardinality

$$|\mathcal{C}| = \frac{q^{n-c}-q^r}{q^{k-c}-1} - q^r + 1.$$

Proof. Let $C := \{v \in \mathbb{F}_q^n : v_i = 0 \text{ for } i > c\}$. To simplify the notation, let B denote the matrix

$$\begin{bmatrix} I_c & 0_{c\times k-c} & \cdots & 0_{c\times k-c} & 0_{c\times k-c+r} & 0_{c\times k-c} \\ 0_{k-c\times c} & 0_{k-c} & \cdots & 0_{k-c} & 0_{k-c\times k-c+r} & I_{k-c} \end{bmatrix}.$$

Given a matrix $M \in \mathcal{M}_i(p,p') \cup \{B\}$, let $\overline{M}$ be the matrix obtained from M by deleting the first c rows. We identify $\mathbb{F}_q^{n-c}$ with $\{v \in \mathbb{F}_q^n : v_i = 0 \text{ for } i = 1,...,c\}$, so that $\mathbb{F}_q^n = C \oplus \mathbb{F}_q^{n-c}$. For any $M \in \mathcal{M}_i(p,p') \cup \{B\}$ we have $\mathrm{rowsp}(\overline{M}) \subseteq \mathbb{F}_q^{n-c}$. It follows

$$\mathcal{C} = \{C \oplus \mathrm{rowsp}(\overline{M}) : M \in \mathcal{M}_i(p,p') \cup \{B\}\}.$$

By Theorem 2.8 and Proposition 2.12 of Chapter 2, the set $\{\mathrm{rowsp}(\overline{M}) : M \in \mathcal{M}_i(p,p') \cup \{B\}\}$ is a partial spread in $\mathcal{G}_q(k-c,n-c)$ of cardinality $(q^{n-c}-q^r)/(q^{k-c}-1)-q^r+1$. The theorem now follows from Remark 3.6. □

Notation 3.30. We denote the sunflower of Theorem 3.29 by $\mathcal{F}_q(k,n,c,p,p')$, and we call it a **sunflower code**. If $h = 2$, then the construction does not depend on p and we denote the code by $\mathcal{F}_q(k,n,c,p')$. In the sequel we will work with a fixed integer $0 \leq c \leq k-1$ and with fixed polynomials p and p' as in Theorem 3.29.

Example 3.31. Let $q = 2$, $c = 1$, $k = 3$ and $n = 6$. Let $p' := x^3 + x + 1 \in \mathbb{F}_2[x]$. The companion matrix of p' is

$$P' = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

A codeword of $\mathcal{F}_q(3,6,1,p')$ is either the space generated by the rows of the matrix

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

or the space generated by the rows of a matrix of the form

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & & I_2 & & A_{(2)} & \\ 0 & & & & & \end{bmatrix},$$

where I_2 is the 2×2 identity matrix, and $A_{(2)}$ denotes the last two rows of a matrix $A \in \mathbb{F}_2[P']$. One can easily check that $|\mathcal{F}_2(3,6,1,p,p')| = 2^3 + 1$.

For most choices of the parameters, sunflower codes have asymptotically optimal cardinality, as the following result shows.

Proposition 3.32. Let $n \geq 3k-1$, and let r denote the remainder obtained dividing $n-c$ by $k-c$. For $q \gg 0$ we have

$$e_q(k,n,c) - |\mathcal{F}_q(k,n,c,p,p')| \leq q^r - 1.$$

In particular,

$$\lim_{q\to\infty} \frac{|\mathcal{F}_q(k,n,c,p,p')|}{e_q(k,n,c)} = 1.$$

Proof. By Proposition 3.16 and Theorem 3.4 we have $e_q(k,n,c) = e_q(k-c,n-c,0) \leq \frac{q^{n-c}-q^r}{q^{k-c}-1}$. By Theorem 3.29 it follows that

$$e_q(k,n,c) - |\mathcal{F}_q(k,n,c,p,p')| \leq \frac{q^{n-c}-q^r}{q^{k-c}-1} - |\mathcal{F}_q(k,n,c,p,p')| = q^r - 1.$$

By definition $|\mathcal{F}_q(k,n,c,p,p')| \leq e_q(k,n,c)$. Thus for $q \gg 0$ we have

$$e_q(k,n,c) - q^r + 1 \leq |\mathcal{F}_q(k,n,c,p,p')| \leq e_q(k,n,c). \tag{3.2}$$

Since $r \leq k-c-1 \leq k-1 < n-k$, the second part of the proposition easily follows taking the limit of (3.2). □

3.6 Decoding sunflowers codes

In this section we provide an efficient decoding algorithm for the sunflower codes that we constructed in Section 3.5, by reducing decoding sunflower codes to decoding partial spread codes. Our algorithm is based on the following result.

Theorem 3.33. Let $V \in \mathcal{F}_q(k, n, c, p, p')$, $V = \mathrm{rowsp}(M)$ where M is as in Theorem 3.29:

$$M = \mathrm{rowsp}\begin{bmatrix} I_c & 0_{c\times n-c} \\ 0_{k-c\times c} & B \end{bmatrix},$$

with B of size $(k-c)\times(n-c)$. Let $X \subseteq \mathbb{F}_q^n$ be a subspace of dimension $1 \leq t \leq k$. Assume that X decodes to V, i.e., $d_{\mathrm{s}}(V, X) < k - c$. Then:

1. $t > c$, and there exist matrices X_1, X_2, X_3 of size $c \times c$, $c \times (n-c)$ and $(t-c)\times(n-c)$ respectively, such that
$$\mathrm{RRE}(X) = \begin{bmatrix} X_1 & X_2 \\ 0_{(t-c)\times c} & X_3 \end{bmatrix},$$
where $\mathrm{RRE}(X)$ is defined in Notation 1.44.
2. $d_{\mathrm{s}}(\mathrm{rowsp}(B), \mathrm{rowsp}(X_3)) < k - c$.

Proof. The condition $d_{\mathrm{s}}(V, X) < k-c$ is equivalent to $\dim(V+X) < k+(t-c)/2$. In particular we have $k = \dim(V) \leq \dim(V+X) < k+(t-c)/2$, and so $t > c$. Notice moreover that by Definition 1.43 the i-th row of any matrix in reduced row-echelon form contains at least $i-1$ zeros. As a consequence,

$$\mathrm{RRE}(X) = \begin{bmatrix} X_1 & X_2 \\ 0_{t-c\times c} & X_3 \end{bmatrix}$$

for some matrices X_1, X_2 and X_3 of size $c\times c$, $c\times(n-c)$ and $(t-c)\times(n-c)$ respectively. To simplify the notation, we omit the size of the zero matrices in the sequel. The condition $\dim(V+X) < k+(t-c)/2$ may be written as

$$\mathrm{rk}\begin{bmatrix} I_c & 0 \\ 0 & B \\ X_1 & X_2 \\ 0 & X_3 \end{bmatrix} < k + (t-c)/2.$$

Hence we have

$$\mathrm{rk}\begin{bmatrix} B \\ X_3 \end{bmatrix} = \mathrm{rk}\begin{bmatrix} I_c & 0 \\ 0 & B \\ 0 & X_3 \end{bmatrix} - c \leq \mathrm{rk}\begin{bmatrix} I_c & 0 \\ 0 & B \\ X_1 & X_2 \\ 0 & X_3 \end{bmatrix} - c < (k-c) + (t-c)/2.$$

Since $\dim(X) = t$, we have $\mathrm{rk}(X_3) = t - c$. It follows that

$$\begin{aligned} d_{\mathrm{s}}(\mathrm{rowsp}(B), \mathrm{rowsp}(X_3)) &= 2\mathrm{rk}\begin{bmatrix} B \\ X_3 \end{bmatrix} - \mathrm{rk}(B) - \mathrm{rk}(X_3) \\ &< 2(k-c) + t - c - (k-c) - (t-c) \\ &= k - c, \end{aligned}$$

as claimed. □

Theorem 3.33 provides as a simple corollary the following efficient algorithm to decode a sunflower code of the form $\mathcal{F}_q(k,n,c,p,p')$.

Algorithm 3: Decoding a $\mathcal{F}_q(k,n,c,p,p')$ code.

Data: A decodable subspace $X \subseteq \mathbb{F}_q^n$ of dimension $t \leq k$.

Result: The unique $V \in \mathcal{F}_q(k,n,c,p,p')$ such that $d_s(V,X) < k-c$, given as a matrix in reduced row echelon form whose rowspace is V.

1. Compute $M := \mathrm{RRE}(X)$.
2. Delete from M the first c rows and columns, obtaining a $k-c \times n-c$ matrix $\overline{M}$.
3. Apply partial spread decoding to $\mathrm{rowsp}(\overline{M})$ as described in Chapter 2, and obtain a matrix N of size $k-c \times n-c$.

The result is $V = \mathrm{rowsp}\begin{bmatrix} I_c & 0 \\ 0 & N \end{bmatrix}$.

Remark 3.34. For any decodable subspace X we have $\dim(X) > c$ by Theorem 3.33. Moreover, as in Section 2.4, our assumption $t \leq k$ in Algorithm 3 is not restrictive from the following point of view: The receiver may collect incoming vectors until the received subspace has dimension k, and then attempt to decode the collected data. We also notice that the computation of $\mathrm{RRE}(X)$ has a low computational cost. Indeed, the receiver obtains the subspace V as the span of incoming vectors, i.e., as the rowspace of a matrix. The reduced row-echelon form of such matrix can be computed by performing Gaussian elimination.

3.7 The orthogonal of a sunflower code

By Proposition 3.20 and Lemma 3.18, the orthogonals of sunflower codes of Theorem 3.29 are equidistant codes that are not sunflowers. Moreover, they are asymptotically optimal equidistant codes for sufficiently large parameters (Remark 3.10 and Theorem 3.24). We can easily write them as rowspaces of matrices, as we show in this section. We will need the following preliminary lemma, whose proof is left to the reader.

Lemma 3.35. Let N be a $t \times (n-t)$ matrix over $\mathbb{F}_q$. We have

$$\mathrm{rowsp}\left(\begin{bmatrix} I_t & N \end{bmatrix}\right)^{\perp} = \mathrm{rowsp}\left(\begin{bmatrix} -N^t & I_{(n-t)\times(n-t)} \end{bmatrix}\right).$$

Remark 3.36. Lemma 3.35 allows us to easily construct the orthogonal of a vector space V given as the rowspace of a full-rank matrix M in reduced row-echelon form. Indeed, if M is such a matrix of size, say, $t \times n$, then there exists a permutation $\pi : \{1,...,n\} \to \{1,...,n\}$ such that M^π has the form $\begin{bmatrix} I_t & N \end{bmatrix}$, where M^π is the matrix whose $\pi(i)$-th columns is the i-th column of M. By Lemma 3.35 we have

$$V^{\perp} = \mathrm{rowsp}\left(\begin{bmatrix} -N^t & I_{(n-t)\times(n-t)} \end{bmatrix}^{\pi^{-1}}\right).$$

Using Remark 3.36 one can now describe in matrix form the orthogonal of a sunflower code $\mathcal{C} = \mathcal{F}_q(k,n,c,p,p')$. Following the notation of Theorem 3.29, the orthogonal of the rowspace of the matrix

$$\begin{bmatrix} I_c & 0_{c\times(k-c)} & \cdots & \cdots & \cdots & \cdots & \cdots & 0_{c\times(k-c)} & 0_{c\times(k-c+r)} \\ 0_{(k-c)\times c} & 0_{k-c} & \cdots & 0_{k-c} & I_{k-c} & A_{i+1} & \cdots & A_{h-1} & A_{[k-c]} \end{bmatrix}$$

is the rowspace of the matrix

$$\begin{bmatrix} 0_{(k-c)\times c} & & & & 0_{k-c} & \cdots & \cdots & \cdots & \cdots \\ \vdots & & I_{(i-1)(k-c)} & & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & & & & 0_{k-c} & \vdots & \vdots & \vdots & \vdots \\ \vdots & 0_{k-c} & \cdots & 0_{k-c} & -A_{i+1}^t & & & & \\ \vdots & \vdots & \vdots & \vdots & \vdots & & I_{n-k-(i-1)(k-c)} & & \\ \vdots & \vdots & \vdots & \vdots & -A_{h-1}^t & & & & \\ 0_{(k-c+r)\times c} & 0_{(k-c+r)\times(k-c)} & \cdots & \cdots & -A_{[k-c]}^t & & & & \end{bmatrix}.$$

Finally, Algorithm 3 and Remark 3.36 can be combined to efficiently decode the orthogonal of a sunflower code as follows.

Remark 3.37. Let $\mathcal{C} = \mathcal{F}_q(k, n, c, p, p')$ be a sunflower code, and let $X \subseteq \mathbb{F}_q^k$ be a received t-dimensional space. Since $d_s(\mathcal{C}) = d_s(\mathcal{C}^\perp)$ and $d_s(X, V^\perp) = d_s(X^\perp, V)$ for all $V \in \mathcal{C}$, the space X decodes to $V^\perp$ in $\mathcal{C}^\perp$ if and only if $X^\perp$ decodes to V in $\mathcal{C}$. This gives the following Algorithm 4 to decode the orthogonal of a sunflower code.

Algorithm 4: Decoding a $\mathcal{F}_q(k, n, c, p, p')^\perp$ code.

Data: A decodable subspace $X \subseteq \mathbb{F}_q^n$ of dimension $t \geq n - k$.

Result: The unique $V \in \mathcal{F}_q(k, n, c, p, p')$ such that $d_s(V^\perp, X) < k - c$, given as a matrix whose rowspace is V.

1. Compute $L := \mathrm{RRE}(X)$.
2. Use Remark 3.36 to construct a matrix L' such that $\mathrm{rowsp}(L') = X^\perp$.
3. Compute the reduced row-echelon form, say M, of L'. Since $t \geq n - k$, M will have at most k rows, as required by Algorithm 3.
4. Delete from M the first c rows and columns, obtaining a matrix $\overline{M}$ of size $(k - c) \times (n - c)$.
5. Apply partial spread decoding to $\mathrm{rowsp}(\overline{M})$ as described in Chapter 2, and obtain a matrix N of size $k - c \times n - c$.
6. We have $V^\perp = \mathrm{rowsp}\begin{bmatrix} I_c & 0 \\ 0 & N \end{bmatrix}$. Use Remark 3.36 to describe V as the rowspace of a matrix.

Chapter 4

Subspace codes from Ferrers diagrams

In this chapter we concentrate on a specific technique to construct subspace codes, called "multilevel construction", that produces subspace codes starting from special rank-metric codes. The technique was proposed in [29] by Etzion and Silberstein, and it extends the lifting procedure described in Proposition 1.39 and Definition 1.40 from Chapter 1. The multilevel construction will be briefly illustrated in Section 4.4 for convenience of the reader.

The construction from [29] relies on the existence of linear rank-metric codes in which the matrices that constitute the code have their non-zero entries contained in a Ferrers diagram shape $\mathcal{F}$. The cardinality of the codes obtained via the multilevel construction increases with the dimension of such rank-metric codes. It is therefore natural to ask what the maximum possible dimension of such linear spaces is. This the main mathematical problem that we address in this chapter.

In [29] Etzion and Silberstein derived an upper bound on the largest possible dimension of a linear space of matrices supported on a Ferrers diagram, and conjectured that the bound is sharp over finite fields. We are not aware of any counterexample to the conjecture.

The main goal of this chapter is to present a detailed study of the conjecture, and to establish it in the cases that are most relevant in the context of linear network coding.

Using results from algebraic geometry, we will also prove that the bound from [29] can be improved over an algebraically closed field. In particular, we provide a sharp bound for the dimension of a linear space of full-rank matrices with a given Ferrers diagram as support.

We also study the natural dual problem of computing the maximum dimension of linear spaces of matrices with rank bounded above by $\delta - 1$ and an arbitrary profile $\mathcal{P}$ as shape (see Section 4.3 for a precise definition of profile). Such spaces appear in the literature under the name of $\overline{\delta}$-spaces or linear anticodes. We determine their largest possible dimension for any profile and over any field. As a simple consequence, we obtain an upper bound on the dimension of a rank-metric code of given minimum distance δ and any given profile $\mathcal{P}$ as shape.

We then apply our results to construct codes of the largest known cardinality via the multilevel construction of [29], for many choices of the parameters and arbitrary q. Our codes were included in the database of codes with best parameters (`http://subspacecodes.uni-bayreuth.de/cdctoplist/`). We also show with an example that using lexicodes in the multilevel construction of [29] may not the best choice, in contrast to what is suggested in previous works.

The chapter is organized as follows. In Section 4.1 we recall some definitions and known results, and we prove a simple lower bound on the maximum dimension of a linear rank-metric code supported on a given Ferrers diagram. We also discuss the conjecture by Etion and Silberstein over algebraically closed fields, showing that the upper bound can be improved in this case. In Section 4.2 we study the conjecture by Ezion and Silberstein, and establish it in the most relevant cases to network coding. Section 4.3 is concerned with $\overline{\delta}$-spaces, for which we compute the maximum dimension for all possible shapes and over any field. Finally, in Section 4.4 we show how the results from Section 4.2 together with the multilevel construction of [29] provide new lower bounds for the maximum possible size of subspace codes.

The results of this chapter have been published in [38] and [27].

Notation 4.1. Throughout the chapter q denotes a fixed prime power, and δ, k, m are integers with $1 \leq \delta \leq k \leq m$.

4.1 Preliminary results and notation

Throughout this chapter we denote by $[k]$ the set $\{1, \ldots, k\}$. A set V of $k \times m$ matrices over a field is a **$\underline{\delta}$-space** (resp., a **$\overline{\delta}$-space**) if it is a linear space and every non-zero element of V has rank at least δ (resp., at most δ).

Remark 4.2. By Definition 1.7, a non-zero $\underline{\delta}$-space V over a finite field $\mathbb{F}_q$ is a linear rank-metric code with $d_{\mathrm{rk}}(V) \geq \delta$. Throughout this chapter we prefer to use the name "$\underline{\delta}$-space" instead of "rank-metric code". This is because we will sometimes work over fields that are not necessarily finite. The terminology "$\underline{\delta}$-space" is standard and commonly used in matrix theory (see e.g. [70]).

We study linear spaces of matrices whose shape is a Ferrers diagram in the sense of [29]. For the convenience of the reader, we start by recalling the definitions and results that we will use.

Definition 4.3. Given positive integers k and m, a **Ferrers diagram** $\mathcal{F}$ of **size** $k \times m$ is a subset of $[k] \times [m]$ with the following properties:

1. if $(i, j) \in \mathcal{F}$ and $i > 1$, then $(i-1, j) \in \mathcal{F}$,
2. if $(i, j) \in \mathcal{F}$ and $j < m$, then $(i, j+1) \in \mathcal{F}$.

For any $1 \leq i \leq k$, the i-th **row** of $\mathcal{F}$ is the set of $(i, j) \in \mathcal{F}$ with $j \in [m]$. Similarly, for any $1 \leq j \leq m$ the j-th **column** of $\mathcal{F}$ is the set of $(i, j) \in \mathcal{F}$ with $i \in [k]$. Notice that we do not require $(1, 1) \in \mathcal{F}$ or $(k, m) \in \mathcal{F}$.

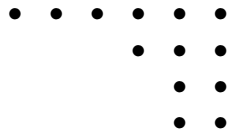
Notation 4.4. We often identify a Ferrers diagram $\mathcal{F}$ with the cardinalities of its rows. Indeed, given positive integers m, k and $m \geq r_1 \geq r_2 \geq \cdots \geq r_k \geq 0$, there exists a unique Ferrers diagram $\mathcal{F}$ of size $k \times m$ such that the i-th row of $\mathcal{F}$ has cardinality r_i for any $1 \leq i \leq k$. In this case we write $\mathcal{F} = [r_1, ..., r_k]$.

Remark 4.5. Let $\mathcal{F} = [r_1, ..., r_k]$ and $\mathcal{F}' = [r'_1, ..., r'_k]$ be Ferrers diagrams of size $k \times m$. We have $\mathcal{F}' \subseteq \mathcal{F}$ if and only if $r'_i \leq r_i$ for all $i = 1, ..., k$.

Ferrers diagrams may be graphically represented as rows of right-justified dots of decreasing cardinalities. If $\mathcal{F} = [r_1, ..., r_k]$, the first row of the graphical representation of $\mathcal{F}$ contains r_1 dots,

the second row r_2 dots, and so on.

Example 4.6. Let $\mathcal{F} := [6, 3, 2, 2]$ be a Ferrers diagram of size 6×4. The graphical representation of $\mathcal{F}$ is as follows:



Definition 4.7. Let $M = (M_{i,j})$ be a $k \times m$ matrix. The **support** of M is the set of positions corresponding to its non-zero entries, i.e., $\mathrm{supp}(M) := \{(i, j) \in [k] \times [m] \mid M_{i,j} \neq 0\}$. Let $\mathcal{F}$ be a Ferrers diagram of size $k \times m$. We say that M has **shape** $\mathcal{F}$ if $\mathrm{supp}(M) \subseteq \mathcal{F}$.

Example 4.8. The two 4×6 matrices over $\mathbb{F}_2$

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

have shape $\mathcal{F} := [6, 3, 2, 2]$.

Notation 4.9. Fix a Ferrers diagram $\mathcal{F}$. The set of matrices with entries in a field $\mathbb{F}$ which have shape $\mathcal{F}$ form a $|\mathcal{F}|$-dimensional $\mathbb{F}$-vector space, which we denote by $\mathbb{F}[\mathcal{F}]$. Equivalently,

$$\mathbb{F}[\mathcal{F}] = \{M \in \mathrm{Mat}_{k \times m}(\mathbb{F}) \mid \mathrm{supp}(M) \subseteq \mathcal{F}\}.$$

A main open problem from [29, Section VI] is the following.

Question 4.10. Given integers $1 \leq \delta \leq k \leq m$ and a Ferrers diagram $\mathcal{F}$ of size $k \times m$, what is the largest dimension of a $\underline{\delta}$-space of $k \times m$ matrices with shape $\mathcal{F}$ and entries in a finite field $\mathbb{F}_q$?

Remark 4.11. Up to a transposition, the assumption $k \leq m$ in Question 4.10 is not restrictive. In the sequel we always work with Ferrers diagrams of size $k \times m$ with $k \leq m$. This is also the relevant case for network coding applications.

Notice that Question 4.10 makes sense over any field $\mathbb{F}$. Later in this section we show that the answer actually depends on the choice of the field. We denote by

$$\mathrm{MaxDim}_{\underline{\delta}}(\mathcal{F}, \mathbb{F}) = \max\{\dim V \mid V \subseteq \mathbb{F}[\mathcal{F}] \text{ is a } \underline{\delta}\text{-space}\}$$

the largest possible dimension of a $\underline{\delta}$-space of $k \times m$ matrices with shape $\mathcal{F}$ and entries in $\mathbb{F}$.

Notation 4.12. Given integers $1 \leq \delta \leq k \leq m$, $0 \leq i \leq \delta - 1$, and a Ferrers diagram $\mathcal{F}$ of size $k \times m$, we denote by $T_\delta(\mathcal{F}, i)$ the cardinality of the set obtained from $\mathcal{F}$ by removing the topmost i rows and the rightmost $\delta - i - 1$ columns. Moreover, we set

$$T_\delta(\mathcal{F}) := \min_{0 \leq i \leq \delta - 1} T_\delta(\mathcal{F}, i).$$

One always has $T_1(\mathcal{F}) = |\mathcal{F}| = T_1(\mathcal{F}, 0)$.

Example 4.13. Let $\mathcal{F} := [6, 3, 2, 2]$. We have $T_4(\mathcal{F}, 0) = 3$, $T_4(\mathcal{F}, 1) = 1$, $T_4(\mathcal{F}, 2) = 2$, $T_4(\mathcal{F}, 3) = 2$. Hence $T_4(\mathcal{F}) = 1$. Similarly one can check that $T_3(\mathcal{F}) = 4$ and $T_2(\mathcal{F}) = 7$.

The following lemma collects two properties that will be useful in the sequel.

Lemma 4.14. Let $\mathbb{F}$ be a field, $\mathcal{F}$ and $\mathcal{F}'$ be Ferrers diagrams. Assume that $\mathcal{F}' \subseteq \mathcal{F}$. We have:

1. $T_\delta(\mathcal{F}) \geq T_\delta(\mathcal{F}')$,
2. $\mathrm{MaxDim}_{\underline{\delta}}(\mathcal{F}, \mathbb{F}) \geq \mathrm{MaxDim}_{\underline{\delta}}(\mathcal{F}', \mathbb{F})$.

The authors of [29] prove that $T_\delta(\mathcal{F})$ is an upper bound for $\mathrm{MaxDim}_{\underline{\delta}}(\mathcal{F}, \mathbb{F})$ for any δ. Moreover, they conjecture that the bound is attained when the field $\mathbb{F} = \mathbb{F}_q$ is finite, for any choice of δ and $\mathcal{F}$. Notice that while in [29] the upper bound is stated only for finite fields, the proof works over an arbitrary field. Here we state the result in the general form.

Theorem 4.15 ([29], Theorem 1)**.** We have

$$\mathrm{MaxDim}_{\underline{\delta}}(\mathcal{F}, \mathbb{F}) \leq T_\delta(\mathcal{F})$$

for any field $\mathbb{F}$, any Ferrers diagram $\mathcal{F}$, and any $\delta \geq 1$.

Conjecture 4.16 ([29], Conjecture 1)**.** When $\mathbb{F} = \mathbb{F}_q$ is a finite field, equality holds in Theorem 4.15 for any choice of the parameters q, $\mathcal{F}$ and δ.

A well-studied case of Question 4.10 is when $\mathcal{F} = [k] \times [m]$. It was solved by Delsarte in 1978 and presented in our introductory chapter (see Section 1.5). More precisely, Theorem 1.14 of Section 1.5 can be re-stated as follows.

Theorem 4.17. Let $1 \leq \delta \leq k \leq m$ be integers. We have

$$\mathrm{MaxDim}_{\underline{\delta}}([k] \times [m], \mathbb{F}_q) = m(k - \delta + 1)$$

for any finite field $\mathbb{F}_q$. In particular, Conjecture 4.16 holds for $\mathcal{F} = [k] \times [m]$.

The properties of finite fields play a central role in the proof of the previous theorem. It is interesting to observe that the answer to Question 4.10 (hence the validity of Conjecture 4.16) actually depends on the choice of the field $\mathbb{F}$. Using some results in algebraic geometry, we will now show that for $\delta = k$ the upper bound of Theorem 4.15 can be improved over an algebraically closed field.

Theorem 4.18. Let $\mathbb{F}$ be an algebraically closed field, let $\mathcal{F} = [r_1, \ldots, r_k]$ be a Ferrers diagram. Let $r := \min\{r_i + i \mid 1 \leq i \leq k\}$. Then

$$\mathrm{MaxDim}_{\underline{k}}(\mathcal{F}, \mathbb{F}) = \begin{cases} 0 & \text{if } r \leq k, \\ r - k & \text{if } k \leq r \leq m + 1, \\ m - k + 1 & \text{if } r \geq m + 1. \end{cases}$$

Proof. Let $X = (x_{ij})$ be a $k \times m$ matrix of zeroes and variables supported on $\mathcal{F}$, i.e. $x_{ij} = 0$ if $(i, j) \notin \mathcal{F}$ and the nonzero entries of X are distinct variables. Let $N = |X| = mk - \sum_{i=1}^{k} r_i$ and let $R = \mathbb{F}[X]$ be the polynomial ring in the variables from X with coefficients in $\mathbb{F}$. Denote by $I_k(X) \subseteq R$ the ideal generated by the maximal minors of X. Then $I_k(X)$ is a radical ideal by [15, Theorem 3.2], hence it defines a projective variety $W \subseteq \mathbb{P}^{N-1}$. In [36, Theorem 1.3], Giusti and Merle compute the codimension c of W as

$$c = m - k + 1 - (\min\{t, m + 1\} - \min\{t, k\}),$$

where

$$t := \max\{m - r_i + k - i + 1 \mid 1 \leq i \leq k\} = m + k - r + 1$$

is half of the maximum perimeter of a rectangle of zeroes contained in X. Therefore

$$c = \begin{cases} 0 & \text{if } r \leq k, \\ r - k & \text{if } k \leq r \leq m + 1, \\ m - k + 1 & \text{if } r \geq m + 1. \end{cases} \tag{4.1}$$

Let $V \subseteq \mathbb{F}[\mathcal{F}]$ be a vector subspace of dimension d, and denote by $L \subseteq \mathbb{P}^{N-1}$ its projectivization. Assume that V consists of matrices of rank k. This is equivalent to $L \cap W = \emptyset$, since the points of W correspond by definition to matrices of rank smaller than k. Since $\dim(\emptyset) = -1$ and

$$\dim(W \cap L) \geq d - c - 1, \tag{4.2}$$

then $d \leq c$. Moreover, equality holds in (4.2) for a generic L. Therefore, if we let V be a generic c-dimensional subspace of $\mathbb{F}[\mathcal{F}]$, then $L \cap W = \emptyset$. So we have shown that $\mathrm{MaxDim}_{\underline{k}}(\mathcal{F}, \mathbb{F}) = c$ and the result follows from (4.1). □

Since Theorem 4.15 holds over any field, it is clear that the quantity computed in the above theorem must be smaller than or equal to the upper bound from Theorem 4.15. In fact, it is easy to show that in many cases it is strictly smaller. This implies in particular that Conjecture 4.16 is false over an algebraically closed field.

Proposition 4.19. Let $\mathbb{F}$ be an algebraically closed field and assume that $k \geq 2$. Then Conjecture 4.16 and Theorem 4.17 do not hold over $\mathbb{F}$.

Proof. Let $\mathbb{F}$ be an algebraically closed field. It suffices to show that $\mathrm{MaxDim}_{\underline{k}}([k] \times [m], \mathbb{F}) < m$ for some k and m. We will show more generally that the conjecture does not hold for every $\mathcal{F} = [r_1, \ldots, r_k]$ such that $m \geq 2k - 2$, $r_i \geq m - i + 1$ for $1 \leq i \leq k - 1$, and $r_k \geq m - k + 2$. Let $\mathcal{F}$ be such a Ferrers diagram and let V be a $\underline{k}$-space of $k \times m$ matrices supported on $\mathcal{F}$ of maximum dimension. By Theorem 4.18, $\dim(V) \leq m - k + 1$. We claim that $T_k(\mathcal{F}) = r_k$.

By assumption, $r_k \geq m - k + 2 \geq k$, hence $r_j \geq k$ for all $1 \leq j \leq k$. It follows that

$$T_k(\mathcal{F}, i) = r_{i+1} + \ldots + r_k - k(k - i - 1) \geq r_k$$

for $0 \leq i \leq k - 1$. Since $T_k(\mathcal{F}, k - 1) = r_k$, then $T_k(\mathcal{F}) = r_k$. Therefore $T_k(\mathcal{F}) = r_k > \dim(V) = \mathrm{MaxDim}_{\underline{k}}(\mathcal{F}, \mathbb{F})$. □

We conclude the section with a simple lower bound for the maximum dimension of a $\underline{\delta}$-space of $k \times m$ matrices with a given shape $\mathcal{F}$. Let V be a $\underline{\delta}$-space of arbitrary $k \times m$ matrices and let $\mathbb{F}[\mathcal{F}]$ be the set of $k \times m$ matrices with entries in $\mathbb{F}$ and shape $\mathcal{F}$. Then $V \cap \mathbb{F}[\mathcal{F}]$ is a $\underline{\delta}$-space of matrices with shape $\mathcal{F}$, whose dimension can be lower bounded as follows.

Proposition 4.20. Let $1 \leq \delta \leq k \leq m$ be integers, and let $\mathcal{F}$ be a Ferrers diagram of size $k \times m$. Then for any field $\mathbb{F}$ we have

$$\mathrm{MaxDim}_{\underline{\delta}}(\mathcal{F}, \mathbb{F}) \geq \mathrm{MaxDim}_{\underline{\delta}}([k] \times [m], \mathbb{F}) - km + |\mathcal{F}|.$$

In particular, if $\mathbb{F} = \mathbb{F}_q$ we have

$$\mathrm{MaxDim}_{\underline{\delta}}(\mathcal{F}, \mathbb{F}_q) \geq |\mathcal{F}| - m(\delta - 1).$$

Proof. Let $\mathbb{F}[\mathcal{F}]$ be the $\mathbb{F}$-vector space of $k \times m$ matrices with entries in $\mathbb{F}$ and shape $\mathcal{F}$. Clearly, $\dim \mathbb{F}[\mathcal{F}] = |\mathcal{F}|$. Let V be a $\underline{\delta}$-space of $k \times m$ matrices of dimension $\mathrm{MaxDim}_{\underline{\delta}}([k] \times [m], \mathbb{F})$. Then

$$\dim V \cap \mathbb{F}[\mathcal{F}] \geq \mathrm{MaxDim}_{\underline{\delta}}([k] \times [m], \mathbb{F}) + |\mathcal{F}| - km. \tag{4.3}$$

If $\mathbb{F} = \mathbb{F}_q$, the inequality follows from (4.3) and Theorem 4.17. □

We then obtain the following easy consequence of Proposition 4.20.

Corollary 4.21 ([29], Theorem 2)**.** Let $1 \leq \delta \leq k \leq m$ be integers, and let $\mathcal{F}$ be a Ferrers diagram of size $k \times m$ with $r_{\delta-1} = m$. Then Conjecture 4.16 holds.

Remark 4.22. Corollary 4.21 implies that Conjecture 4.16 holds for any Ferrers diagram, if $\delta = 2$. Indeed, up to a transposition of the diagram, one can always assume $m = r_1$ $(\geq k)$ without loss of generality.

Remark 4.23. Notice that the dimension of $V \cap \mathbb{F}[\mathcal{F}]$ depends on the choice of V, where V is a $\underline{\delta}$-space of unrestricted matrices of maximum dimension. Let e.g. $\mathcal{F} := [3, 2, 1]$. The linear spaces

$$V_1 := \langle \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \rangle, \qquad V_2 := \langle \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \rangle$$

are both $\underline{3}$-spaces of unrestricted matrices over $\mathbb{F}_2$ of maximal dimension 3. However we have

$$V_1 \cap \mathbb{F}_2[\mathcal{F}] = \langle \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \rangle \quad \text{and} \quad V_2 \cap \mathbb{F}_2[\mathcal{F}] = \{0\}.$$

4.2 Evidence for the Etzion-Silberstein conjecture

Theorem 2 of [29] establishes Conjecture 4.16 for any Ferrers diagram $\mathcal{F}$ of size $k \times m$ such that $m \geq k$ and $r_1 = r_2 = \cdots r_{d-1} = m$. The conjecture is also known to be true for any Ferrers diagram $\mathcal{F}$ and $\delta = 2$ (see [29], page 2913). For $\delta = 1$ Conjecture 4.16 trivially holds. In this section, we give some explicit constructions of $\underline{\delta}$-spaces of matrices with prescribed shapes. This will allow us to compute the value of $\mathrm{MaxDim}_{\underline{\delta}}(\mathcal{F}, \mathbb{F})$ for many choices of $\mathcal{F}$ and $\mathbb{F}$.

Theorem 4.24. Let $2 \leq \delta \leq k \leq m$ be integers, and let $\mathcal{F} = [r_1, ..., r_k]$ be a Ferrers diagram of size $k \times m$. Assume $r_{\delta-1} \geq k$. We have

$$\mathrm{MaxDim}_{\underline{\delta}}(\mathcal{F}, \mathbb{F}_q) = T_\delta(\mathcal{F}) = \sum_{i=\delta}^{k} r_i$$

for any finite field $\mathbb{F}_q$. In particular, Conjecture 4.16 holds.

Proof. Define the Ferrers diagram of size $k \times r_{\delta-1}$

$$\mathcal{F}' := [\underbrace{r_{\delta-1}, ..., r_{\delta-1}}_{\delta-1}, r_\delta, r_{\delta+1}, ..., r_k] \subseteq \mathcal{F}.$$

Since $r_{\delta-1} \geq k$, by Corollary 4.21 we have $\mathrm{MaxDim}_{\underline{\delta}}(\mathcal{F}', \mathbb{F}_q) = T_\delta(\mathcal{F}') = \sum_{i=\delta}^{k} r_i$. Therefore

$$\sum_{i=\delta}^{k} r_i \geq T_\delta(\mathcal{F}) \geq \mathrm{MaxDim}_{\underline{\delta}}(\mathcal{F}, \mathbb{F}_q) \geq \mathrm{MaxDim}_{\underline{\delta}}(\mathcal{F}', \mathbb{F}_q) = \sum_{i=\delta}^{k} r_i \ , \tag{4.4}$$

where the first inequality follows from the definition of $T_\delta(\mathcal{F})$, the second from Theorem 4.15, and the third from Lemma 4.14. Therefore all the inequalities in (4.4) are equalities. □

Remark 4.25. As we will see in Section 4.4, to construct applicable subspace codes via the multilevel construction of [29], we usually need Ferrers diagrams with $m \gg k$. In addition, the vector spaces of matrices that contribute the most to the cardinality of the resulting subspace code correspond to Ferrers diagrams of large cardinality. Hence the case treated in Theorem 4.24 is most relevant in the applications.

For some Ferrers diagrams of size $k \times k$, the maximum dimension of a $\underline{\delta}$-space of matrices can be lower-bounded as follows.

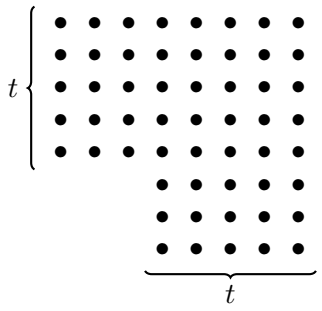
Theorem 4.26. Let $k \geq 1$ be an integer, and let $\mathcal{F}$ be a Ferrers diagram of size $k \times k$. Assume that $k/2 \leq T_k(\mathcal{F}) \leq k-1$. We have

$$\mathrm{MaxDim}_{\underline{k}}(\mathcal{F}, \mathbb{F}_q) \geq \max\left\{2T_k(\mathcal{F}) - k + 1, \left\lfloor \frac{k}{2} \right\rfloor\right\}.$$

In particular, Conjecture 4.16 holds in the following cases:

- $\delta = k = m$ even and $T_k(\mathcal{F}) = k/2$,
- $\delta = k = m$ and $T_k(\mathcal{F}) = k-1$.

Proof. By definition of $T_k(\mathcal{F})$, both the first column and the k-th row of $\mathcal{F}$ have cardinality at least $t := T_k(\mathcal{F})$. As a consequence, $\mathcal{F}$ contains the Ferrers diagram $\mathcal{F}' := [\underbrace{k, ..., k}_{t}, \underbrace{t, ..., t}_{k-t}]$. Since $\mathcal{F}' \subseteq \mathcal{F}$ and $T_k(\mathcal{F}') = t$, by Lemma 4.14 it suffices to prove the result for $\mathcal{F}'$. The graphical representation of $\mathcal{F}'$ is:



Let $k_1 = \lfloor k/2 \rfloor$ and $k_2 = \lceil k/2 \rceil$. We have $t \geq k_2$ by assumption. By Theorem 4.17 there exists a $\underline{k_1}$-space V_1 (resp., a $\underline{k_2}$-space V_2) of $k_1 \times k_1$ (resp., $k_2 \times k_2$) matrices with entries in $\mathbb{F}_q$ of dimension k_1 (resp., k_2). Let $\{M_1, ..., M_{k_1}\}$ be a basis of V_1 and let $\{N_1, ..., N_{k_2}\}$ be a basis of V_2. The matrices

$$H_i := \begin{bmatrix} M_i & 0 \\ 0 & N_i \end{bmatrix}, \quad i = 1, ..., k_1$$

span a $\underline{k}$-space of matrices with entries in $\mathbb{F}_q$ and shape $\mathcal{F}'$, of dimension $k_1 = \lfloor k/2 \rfloor$. Therefore $\mathrm{MaxDim}_{\underline{k}}(\mathcal{F}', \mathbb{F}_q) \geq \lfloor k/2 \rfloor$.

Let us prove that $\mathrm{MaxDim}_{\underline{k}}(\mathcal{F}', \mathbb{F}_q) \geq 2t - k + 1$. If $k = t + 1$, then by Proposition 4.20 $\mathrm{MaxDim}_{\underline{k}}(\mathcal{F}', \mathbb{F}_q) \geq |\mathcal{F}'| - k(k-1) = k - 1 = 2t - k + 1$. If $k \geq t + 2$, let $\{1, \alpha, ..., \alpha^{k-1}\}$ be an

$\mathbb{F}_q$-basis of $\mathbb{F}_{q^k} = \mathbb{F}_q(\alpha)$. For $0 \leq i \leq 2t-k$ define the $\mathbb{F}_q$-linear map

$$\begin{array}{rccc} f_i : \mathbb{F}_{q^k} & \to & \mathbb{F}_{q^k} \\ x & \mapsto & \alpha^i x. \end{array}$$

Let $W := \mathrm{Span}_{\mathbb{F}_q}\{f_0, \ldots, f_{2t-k}\} \subseteq \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_{q^k}, \mathbb{F}_{q^k})$. Since $t < k$, then $\dim W = 2t-k+1$, and any $f \in W \setminus \{0\}$ is invertible. Moreover, the matrices associated to the elements of W with respect to the basis $\{\alpha^{k-1}, \ldots, \alpha, 1\}$ and putting the images in the rows have shape $\mathcal{F}'$. In fact, for $0 \leq i \leq 2t-k$ we have $f_i(\alpha^{k-j}) = \alpha^{k+i-j}$ with $0 \leq k+i-j \leq t-1$ for $t+1 \leq j \leq k$. This proves that $\mathrm{MaxDim}_{\underline{k}}(\mathcal{F}', \mathbb{F}_q) \geq \dim W = 2t-k+1$. □

Example 4.27. Let $q := 5$, $k := 4$ and $\mathcal{F} := [4,4,2,2]$. We apply the first part of the proof of Theorem 4.26 to construct a 2-dimensional $\underline{4}$-space of shape $\mathcal{F}$. Let $V = V_1 = V_2$ be the vector space generated over $\mathbb{F}_5$ by

$$\begin{bmatrix} 0 & 1 \\ 3 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 3 & 1 \\ 3 & 4 \end{bmatrix}.$$

V is a $\underline{2}$-space, hence the vector space generated by the two matrices

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 3 & 1 \end{bmatrix}, \quad \begin{bmatrix} 3 & 1 & 0 & 0 \\ 3 & 4 & 0 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 3 & 4 \end{bmatrix}$$

is a 2-dimensional $\underline{4}$-space.

Remark 4.28. The lower bound of Theorem 4.26 is not sharp for all choices of the parameters. Let e.g. $k := 5$, $q := 3$ and $\mathcal{F} := [5,5,5,3,3]$. We have $T_5(\mathcal{F}) = 3$, hence

$$\max\{2T_5(\mathcal{F}) - 5 + 1, \lfloor 5/2 \rfloor\} = 2.$$

On the other hand, the three matrices over $\mathbb{F}_3$

$$\begin{bmatrix} 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

span a 3-dimensional $\underline{5}$-space. Hence $\mathrm{MaxDim}_{\underline{5}}(\mathcal{F}, \mathbb{F}_3) = 3$.

The remainder of this section is concerned with Ferrers diagrams with an "upper triangular" profile. We will give a lower-bound on $\mathrm{MaxDim}_{\underline{\delta}}(\mathcal{F}, \mathbb{F})$ in terms of the lengths of the diagonals of $\mathcal{F}$, provided that the field $\mathbb{F}$ is large enough. As a corollary, we compute the maximum possible dimension of $\underline{\delta}$-spaces of upper triangular matrices over sufficiently large fields. This establishes Conjecture 4.16 for some families of diagrams. Before proving the next theorem, we recall some elementary results from classical coding theory.

Lemma 4.29. Let $\mathbb{F}$ be a field. For any integers $1 \leq \delta \leq n$ there exists a classical code $C \subseteq \mathbb{F}^n$ of minimum Hamming distance δ and dimension $n-\delta+1$, provided that $|\mathbb{F}| \geq n-1$.

Proof. If $|\mathbb{F}| = n-1$ the result follows from [68, Theorem 9 of Chapter 11]. If $|\mathbb{F}| \geq n$ then one may simply take as C a Reed-Solomon code with the appropriate parameters. More precisely, let $\alpha_1, ..., \alpha_n \in \mathbb{F}$ distinct. Denote by $\mathbb{F}[x]_{\leq n-\delta}$ the $\mathbb{F}$-space of polynomials with coefficients in $\mathbb{F}$ and degree at most $n-\delta$. Then the $\mathbb{F}$-linear evaluation map $\varphi : \mathbb{F}[x]_{\leq n-\delta} \to \mathbb{F}^n$ defined by $\varphi(f) = (f(\alpha_1), ..., f(\alpha_n))$ for all $f \in \mathbb{F}[x]_{\leq n-\delta}$ is injective by the Fundamental Theorem of Algebra. The image of φ is therefore a code with the expected properties. □

Definition 4.30. Let $\mathcal{F}$ be a Ferrers diagram of size $k \times m$. The r-th **diagonal** of $\mathcal{F}$ is the set of elements of $\mathcal{F}$ of the form (i, j) with $i - j + m = r$. Notice that we enumerate diagonals from right to left. Similarly, if M is a matrix with shape $\mathcal{F}$, we define the r-th **$\mathcal{F}$-diagonal** of M as the vector with entries $M_{i,i+m-r}$ such that $(i, i + m - r) \in \mathcal{F}$.

Example 4.31. Let $\mathcal{F} := [4, 2, 2, 1]$. The second diagonal of $\mathcal{F}$ has cardinality two, the third and the fourth have cardinality three. Consider the matrix M of shape $\mathcal{F}$ given by

$$M := \begin{bmatrix} a & b & c & d \\ 0 & 0 & e & f \\ 0 & 0 & g & h \\ 0 & 0 & 0 & i \end{bmatrix}.$$

The second $\mathcal{F}$-diagonal of M is (c, f), the third is (b, e, h), and the fourth is (a, g, i).

A similar construction to the one that we use to prove the next theorem appears in [80]. We thank T. Etzion for bringing this work to our attention.

Theorem 4.32. Let $1 \leq \delta \leq k \leq m$ be integers, and let $\mathcal{F}$ be a Ferrers diagram of size $k \times m$. Assume that $\mathcal{F}$ has n diagonals $D_1, ..., D_n$ of cardinality at least $\delta - 1$. D_i is the α_i-th diagonal of $\mathcal{F}$, for some $\alpha_1 < \ldots < \alpha_n$. If $|\mathbb{F}| \geq \max_{i=1}^{n} |D_i| - 1$, then

$$\mathrm{MaxDim}_{\underline{\delta}}(\mathcal{F}, \mathbb{F}) \geq \sum_{i=1}^{n} (|D_i| - \delta + 1).$$

Proof. First we notice that the summands corresponding to diagonals of cardinality $\delta - 1$ give no contribution to the lower bound. Hence we may assume without loss of generality that $|D_i| \geq \delta$ for $i = 1, ..., n$. By Lemma 4.29, for any $i = 1, ..., n$ there exists a code $C_i \subseteq \mathbb{F}^{|D_i|}$ of minimum distance δ and dimension $|D_i| - \delta + 1$. Given vectors $v_1, ..., v_n$ of lengths $|D_1|, ..., |D_n|$ respectively, denote by $M(v_1, ..., v_n, \mathcal{F})$ the unique $k \times m$ matrix with the following properties:

1. the shape of $M(v_1, ..., v_n, \mathcal{F})$ is $\mathcal{F}$,
2. the vector v_i is the α_i-th $\mathcal{F}$-diagonal of $M(v_1, ..., v_n, \mathcal{F})$,
3. all the remaining entries of $M(v_1, ..., v_n, \mathcal{F})$ are zero.

We claim that the linear space

$$V := \mathrm{Span}_{\mathbb{F}} \{ M(v_1, ..., v_n, \mathcal{F}) \ : \ (v_1, ..., v_n) \in C_1 \times \cdots \times C_n \}$$

is a $\underline{\delta}$-space of $k \times m$ matrices with shape $\mathcal{F}$, of dimension $\sum_{i=1}^{n} (|D_i| - \delta + 1)$. To compute $\dim V$, observe that the map $C_1 \times \cdots \times C_n \to V$ given by $(v_1, ..., v_n) \mapsto M(v_1, ..., v_n, \mathcal{F})$ is an $\mathbb{F}$-isomorphism. Since $\dim(C_i) = |D_i| - \delta + 1$ for all i, then $\dim V = \sum_{i=1}^{n} (|D_i| - \delta + 1)$. It remains to show that an arbitrary non-zero matrix in V has rank at least δ. Fix $M \in V \setminus \{0\}$, and let r denote the maximum integer such that the r-th diagonal of M is non-zero. By definition of V, we have $r = \alpha_i$ for some i. Since C_i has minimum distance δ, the r-th diagonal of M has at least δ non-zero entries. By the maximality of r, the entries of M which lie below such diagonal are all zero. It is easy to see that a matrix M of this form has rank at least δ. □

Corollary 4.33. Let $1 \leq \delta \leq k \leq m$ be integers, and let $\mathcal{F} = [r_1, ..., r_k]$ be a Ferrers diagram of size $k \times m$. Assume $r_i \geq m - i + 1$ for $i = 1, ..., \delta - 1$ and $r_i \leq m - i + 1$ for $i = \delta, ..., k$. We have

$$\mathrm{MaxDim}_{\underline{\delta}}(\mathcal{F}, \mathbb{F}) = T_{\delta}(\mathcal{F})$$

for any field $\mathbb{F}$ such that $|\mathbb{F}| \geq \max_{i=\delta}^{m} |D_i| - 1$, where D_i denotes the i-th diagonal of $\mathcal{F}$. In particular, Conjecture 4.16 holds.

Proof. Since $r_i \geq m - i + 1$ for $i = 1, ..., \delta - 1$, we have $|D_\delta|, ..., |D_m| \geq \delta - 1$. By Theorem 4.32, $\text{MaxDim}_{\underline{\delta}}(\mathcal{F}, \mathbb{F}) \geq \sum_{i=\delta}^{m}(|D_i| - \delta + 1)$. By Theorem 4.15 and the definition of $T_\delta(\mathcal{F})$, it suffices to prove that $T_\delta(\mathcal{F}, \delta - 1) = \sum_{i=\delta}^{m}(|D_i| - \delta + 1)$. Since $r_i \leq m - i + 1$ for $i = \delta, ..., k$, and $r_i \geq m - i + 1$ for $i = 1, ..., \delta - 1$, when we remove from $\mathcal{F}$ the first $\delta - 1$ rows we obtain a set of cardinality $\sum_{i=\delta}^{m}(|D_i| - \delta + 1)$, as claimed. □

Corollary 4.34. Let $1 \leq \delta \leq k$ be integers. The maximum dimension of a δ-space of $k \times k$ upper (or lower) triangular matrices over any field $\mathbb{F}$ is $\binom{k-\delta+2}{2}$, provided that $|\mathbb{F}| \geq k - 1$. In particular, Conjecture 4.16 holds.

Proof. Clearly, the Ferrers diagram that corresponds to upper triangular $k \times k$ matrices is $\mathcal{F} := [k, k-1, ..., 1]$, which satisfies the assumptions of Corollary 4.33. Hence we only need to check that $T_\delta(\mathcal{F}) = \binom{k-\delta+2}{2}$. Fix any $0 \leq i \leq \delta - 1$. It is easy to check that

$$T_\delta(\mathcal{F}, i) = 1 + 2 + \cdots + (k - \delta + 1) = \binom{k - \delta + 2}{2}.$$

It follows that $T_\delta(\mathcal{F}) = \binom{k-\delta+2}{2}$. □

Remark 4.35. The requirement $|\mathbb{F}| \geq k - 1$ in the statement of Corollary 4.34 is not necessary, in general, for the existence of a $\underline{\delta}$-space of $k \times k$ upper triangular matrices of dimension $\binom{k-\delta+2}{2}$. For example, the three upper triangular 4×4 matrices over $\mathbb{F}_2$

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

span a 3-dimensional $\underline{3}$-space.

4.3 Optimal $\overline{\delta}$-spaces

The problem stated in Question 4.10 has the following natural dual version in terms of $\overline{\delta}$-spaces of matrices. Recall from Section 4.1 that a $\overline{\delta}$-space V is a linear space of matrices such that every matrix in V has rank at most δ. Vector spaces with this property are usually called "linear anticodes" in coding terminology, and play an important role in determining codes performance in some applied contexts. The duality theory of linear rank-metric anticodes of unrestricted matrices will be studied in details in Chapters 5 and 6.

Question 4.36. Given integers $1 \leq \delta \leq k \leq m$ and a Ferrers diagram $\mathcal{F}$ of size $k \times m$, what is the largest possible dimension of a $\overline{\delta}$-space of $k \times m$ matrices with shape $\mathcal{F}$ and entries in a finite field $\mathbb{F}_q$?

In this section, we answer the following generalized version of Question 4.36, where we consider arbitrary fields and general profiles instead of Ferrers diagrams. The method that we employ uses an idea from [70].

Question 4.37. Given integers $1 \leq \delta \leq k \leq m$ and a profile $\mathcal{P}$ of size $k \times m$, what is the largest possible dimension of a $\overline{\delta}$-space of $k \times m$ matrices with shape $\mathcal{P}$ and entries in a field $\mathbb{F}$?

We start by giving a definition of profile.

Definition 4.38. Given positive integers k and m, define a **profile** of size $k \times m$ as a subset $\mathcal{P} \subseteq [k] \times [m]$. For any $1 \leq i \leq k$, the i-th **row** of $\mathcal{P}$ is the set of $(i,j) \in \mathcal{P}$ with $j \in [m]$. Similarly, for any $1 \leq j \leq m$ the j-th **column** of $\mathcal{P}$ is the set of $(i,j) \in \mathcal{P}$ with $i \in [k]$. A $k \times m$ matrix M has **shape** $\mathcal{P}$ when $\mathrm{supp}(M) \subseteq \mathcal{P}$.

Let $\mathbb{F}$ be a field and $\mathcal{P}$ be a profile of size $k \times m$. We denote by

$$\mathrm{MaxDim}_{\overline{\delta}}(\mathcal{P}, \mathbb{F})$$

the maximum dimension of a $\overline{\delta}$-space of $k \times m$ matrices with entries in $\mathbb{F}$ and shape $\mathcal{P}$.

Notation 4.39. Let $1 \leq \delta \leq k \leq m$ be integers, and let $\mathcal{P}$ be a profile of size $k \times m$. Given subsets $I \subseteq [k]$, $J \subseteq [m]$ such that $|I| + |J| = \delta - 1$, we denote by $T_\delta(\mathcal{P}, I, J)$ the cardinality of the set obtained from $\mathcal{P}$ by removing the rows of index $i \in I$ and the columns of index $j \in J$. Moreover, we set

$$T_\delta(\mathcal{P}) := \min \left\{ T_\delta(\mathcal{P}, I, J) \mid I \subseteq [k], J \subseteq [m] \text{ and } |I| + |J| = \delta - 1 \right\}.$$

Finally, recall that by definition a **line** of a matrix is either a row, or a column of the matrix.

Remark 4.40. When $\mathcal{P} = \mathcal{F}$ is a Ferrers diagram, the definition of $T_\delta(\mathcal{F})$ given in Notation 4.12 and the definition of $T_\delta(\mathcal{P})$ given in Notation 4.39 coincide.

Lemma 4.41. Let $1 \leq \delta \leq k \leq m$ be integers, and let $\mathcal{P}$ be a profile of size $k \times m$. We have

$$\mathrm{MaxDim}_{\overline{\delta-1}}(\mathcal{P}, \mathbb{F}) \geq |\mathcal{P}| - T_\delta(\mathcal{P})$$

for any field $\mathbb{F}$.

Proof. Choose $I \subseteq [k]$ and $J \subseteq [m]$ such that $|I| + |J| = \delta - 1$ and $T_\delta(\mathcal{P}, I, J) = T_\delta(\mathcal{P})$. Let

$$\mathcal{P}' = \{(i,j) \in \mathcal{P} \mid i \in I \text{ or } j \in J\}.$$

Because of the choice of I and J, $|\mathcal{P}'| = |\mathcal{P}| - T_\delta(\mathcal{P})$. Denote by $\mathbb{F}[\mathcal{P}']$ the vector space of $k \times m$ matrices over $\mathbb{F}$ with shape $\mathcal{P}'$. We have $\dim_{\mathbb{F}} \mathbb{F}[\mathcal{P}'] = |\mathcal{P}'| = |\mathcal{P}| - T_\delta(\mathcal{P})$. Since the support of any $M \in \mathbb{F}[\mathcal{P}'] \subseteq \mathbb{F}[\mathcal{P}]$ is contained in at most $\delta - 1$ lines, we have $\mathrm{rank}(M) \leq \delta - 1$. Hence $\mathrm{MaxDim}_{\overline{\delta-1}}(\mathcal{P}, \mathbb{F}) \geq |\mathcal{P}| - T_\delta(\mathcal{P})$, as claimed. □

It is now easy to prove the following generalization of Theorem 4.15.

Theorem 4.42. Let $1 \leq \delta \leq k \leq m$ be integers, and let $\mathcal{P}$ be a profile of size $k \times m$. For any field $\mathbb{F}$ we have

$$\mathrm{MaxDim}_{\underline{\delta}}(\mathcal{P}, \mathbb{F}) \leq T_\delta(\mathcal{P}).$$

Proof. Let V be a $\underline{\delta}$-space of matrices with shape $\mathcal{P}$ of dimension $\mathrm{MaxDim}_{\underline{\delta}}(\mathcal{P}, \mathbb{F})$. Similarly, let W be a $\overline{\delta-1}$-space of matrices with shape $\mathcal{P}$ of dimension $\mathrm{MaxDim}_{\overline{\delta-1}}(\mathcal{P}, \mathbb{F})$. Denote by $\mathbb{F}[\mathcal{P}]$ the $|\mathcal{P}|$-dimensional $\mathbb{F}$-vector space of $k \times m$ matrices with shape $\mathcal{P}$ and entries in $\mathbb{F}$. We have $V \cap W = \{0\}$ and $V \oplus W \subseteq \mathbb{F}[\mathcal{P}]$. By Lemma 4.41, $\dim V \leq |\mathcal{P}| - (|\mathcal{P}| - T_\delta(\mathcal{P}))$. □

Remark 4.43. By Lemma 4.41, Conjecture 4.16 can be restated as follows: Over a finite field $\mathbb{F}_q$ and for any δ, the vector space $\mathbb{F}_q[\mathcal{F}]$ of matrices of fixed shape $\mathcal{F}$ decomposes as

$$\mathbb{F}_q[\mathcal{F}] = \underline{V} \oplus \overline{V},$$

where $\underline{V}$ is a $\underline{\delta}$-space and $\overline{V}$ is a $\overline{\delta-1}$-space. We stress that this is in general false when the underlying field is not finite (see Proposition 4.19).

Notation 4.44. For integers $1 \leq k \leq m$, let $\prec$ denote the lexicographic order on $[k] \times [m]$, i.e., $(i,j) \prec (i',j')$ if and only if either $i < i'$ or $i = i'$ and $j < j'$. For a $k \times m$ matrix M over a field $\mathbb{F}$ we set

$$p(M) := \min\{(i,j) \mid M_{i,j} \neq 0\}.$$

For a set $\mathcal{A}$ of $k \times m$ matrices define the 0-1 matrix $M(\mathcal{A})$ over $\mathbb{F}$ as follows:

1. $M(\mathcal{A})_{i,j} = 1$ if $(i,j) = p(A)$ for some $A \in \mathcal{A}$,
2. $M(\mathcal{A})_{i,j} = 0$ otherwise.

Finally, denote by $\rho(\mathcal{A})$ the minimal cardinality of a set of lines of $M(\mathcal{A})$ which contain all the 1's appearing in $M(\mathcal{A})$.

Lemma 4.45. ([70], Theorem 1) Let $\mathcal{A}$ be a set of $k \times m$ matrices over a field $\mathbb{F}$. Then $\mathrm{Span}_{\mathbb{F}}(\mathcal{A})$ contains a matrix of rank at least $\rho(\mathcal{A})$.

The following theorem provides an answer to Question 4.36 and Question 4.37.

Theorem 4.46. Let $1 \leq \delta \leq k \leq m$ be integers, and let $\mathcal{P}$ be a profile of size $k \times m$. We have

$$\mathrm{MaxDim}_{\overline{\delta-1}}(\mathcal{P}, \mathbb{F}) = |\mathcal{P}| - T_{\delta}(\mathcal{P})$$

for any field $\mathbb{F}$.

Proof. By Lemma 4.41 it suffices to show that $\mathrm{MaxDim}_{\overline{\delta-1}}(\mathcal{P}, \mathbb{F}) \leq |\mathcal{P}| - T_{\delta}(\mathcal{P})$. Let V be a $\overline{\delta-1}$-space of $k \times m$ matrices over $\mathbb{F}$ with shape $\mathcal{P}$ of dimension $r := \mathrm{MaxDim}_{\overline{\delta-1}}(\mathcal{P}, \mathbb{F})$. Choose a basis $\{N_1, ..., N_r\}$ of V. Let φ be the $\mathbb{F}$-isomorphism that sends a $k \times m$ matrix M to the vector of length km whose entries are the entries of M ordered lexicographically. Define $w_i := \varphi(N_i)$ for $i = 1, ..., r$. Perform Gaussian elimination on $w_1, ..., w_r$ and get vectors $v_1, ..., v_r$. Set $M_i := \varphi^{-1}(v_i)$ for $i = 1, ..., r$. It is clear that $\mathcal{A} := \{M_1, ..., M_r\}$ is a basis of V. Since $p(M_i) \neq p(M_j)$ for $i \neq j$, the support $\mathcal{P}'$ of $M(\mathcal{A})$ has cardinality exactly r.

Since V is a $\overline{\delta-1}$-space, by Lemma 4.45 the support $\mathcal{P}'$ is contained in a set of i rows and $\delta - i - 1$ columns for some $0 \leq i \leq \delta - 1$. Since $\mathcal{P}' \subseteq \mathcal{P}$, we conclude that $|\mathcal{P}'| \leq |\mathcal{P}| - T_{\delta}(\mathcal{P})$. □

We close this section by showing an interesting connection between Conjecture 4.16 and anticodes. Generalizing Definition 1.7 we let $d_{\mathrm{rk}}(M,N) := \mathrm{rank}(M-N)$ denote the **rank distance** between matrices $M, N \in \mathrm{Mat}_{k\times m}(\mathbb{F})$. Notice that we do not restrict ourselves to finite fields. Given an integer $1 \leq \delta \leq k$, a **$\overline{\delta}$-anticode** in $\mathrm{Mat}_{k\times m}(\mathbb{F})$ is a non-empty subset $\mathcal{A} \subseteq \mathrm{Mat}_{k\times m}(\mathbb{F})$ such that $d_{\mathrm{rk}}(M,N) \leq \delta$ for all $M, N \in \mathcal{A}$. For a profile $\mathcal{P} \subseteq [k] \times [m]$, we define

$$\mathrm{MaxCard}_{\overline{\delta}}(\mathcal{P}, \mathbb{F}) := \log_q \max\{|\mathcal{A}| : \mathcal{A} \subseteq \mathbb{F}[\mathcal{P}] \text{ is a } \overline{\delta}\text{-anticode}\}.$$

Since every $\overline{\delta}$-space $\mathcal{A} \subseteq \mathbb{F}[\mathcal{P}]$ is a $\overline{\delta}$-anticode, we have $\mathrm{MaxCard}_{\overline{\delta}}(\mathcal{P}, \mathbb{F}) \geq \mathrm{MaxDim}_{\overline{\delta}}(\mathcal{P}, \mathbb{F})$. In the following we show that, if Conjecture 4.16 holds, then the two quantities agree when $\mathbb{F} = \mathbb{F}_q$ and $\mathcal{P} = \mathcal{F}$ is a Ferrers diagram.

Lemma 4.47 (Code-anticode bound)**.** Let $V \subseteq \mathbb{F}_q[\mathcal{F}]$ be a $\underline{\delta+1}$-space, and let $\mathcal{A}$ be a $\overline{\delta}$ anticode. Then $|V| \cdot |\mathcal{A}| \leq q^{|\mathcal{F}|}$.

Proof. For $M \in \mathcal{A}$ let $\overline{M} := \{M + N : N \in V\}$. Then $\overline{M} \neq \overline{M'} = \emptyset$ whenever $M \neq M'$. Since $\overline{M}$ has cardinality $|V|$ for all $M \in \mathcal{A}$ we have $|V| \cdot |\mathcal{A}| = \sum_{M \in \mathcal{A}} |\overline{M}| \leq |\mathbb{F}_q[\mathcal{F}]| = q^{|\mathcal{F}|}$, as claimed. □

Proposition 4.48. If Conjecture 4.16 holds, then

$$\mathrm{MaxCard}_{\overline{\delta}}(\mathcal{F}, \mathbb{F}_q) = \mathrm{MaxDim}_{\overline{\delta}}(\mathcal{F}, \mathbb{F}_q)$$

for any $1 \leq \delta \leq k$, any Ferrers diagram $\mathcal{F}$ and any finite field $\mathbb{F}_q$.

Proof. The result is trivial when $\delta = k$. Assume $\delta \leq k - 1$, and let $\mathcal{A} \subseteq \mathbb{F}_q[\mathcal{F}]$ be a $\overline{\delta}$-anticode of maximum size. Take a $\underline{\delta + 1}$-space $V \subseteq \mathbb{F}_q[\mathcal{F}]$ of maximum dimension $T_{\delta+1}(\mathcal{F})$. We have

$$\begin{aligned} |\mathcal{F}| - T_{\delta+1}(\mathcal{F}) &= \mathrm{MaxDim}_{\overline{\delta}}(\mathcal{F}, \mathbb{F}_q) && (4.5) \\ &\leq \mathrm{MaxCard}_{\overline{\delta}}(\mathcal{F}, \mathbb{F}_q) \\ &= \log_q |\mathcal{A}| \\ &\leq |\mathcal{F}| - \dim(V) && (4.6) \\ &= |\mathcal{F}| - T_{\delta+1}(\mathcal{F}), \end{aligned}$$

where (4.5) follows from Theorem 4.46, and (4.6) follows from Lemma 4.47. □

4.4 Applications and examples

In this section we show how one can apply the results of Section 4.2 to construct large subspace codes with given parameters via the multilevel construction of [29]. In particular we show how to construct the largest known codes for $q \geq 3$ and many choices of the parameters. Being systematic, the constructions that we propose may be useful for designing efficient decoding algorithms.

For $q = 2$, $\delta = 2, 3$ and small values of n and k, there exist subspace codes which have larger cardinality than the codes we can construct using the results contained in this chapter (see e.g. [31], [82] and [53]). The techniques most commonly employed to produce such codes include a computer search, which is not feasible for large values of q and of the other parameters.

We now briefly recall the multilevel construction for subspace codes proposed by Etzion and Silberstein in [29].

Notation 4.49. Let X be a k-dimensional subspace of $\mathbb{F}_q^n$ and let $\mathrm{RRE}(X)$ be the unique $k \times n$ matrix in reduced row echelon form with rowspace X (see Notation 1.44). We associate to X the binary vector $v(X)$ of length n and weight k, which has a 1 in position i if and only if $\mathrm{RRE}(X)$ has a pivot in the i-th column. The vector $v(X)$ is the **pivot vector** associated to X and $\mathrm{RRE}(X)$.

We will need the following preliminary result from [29].

Lemma 4.50 ([29], Lemma 2)**.** Let $X, Y \in \mathcal{G}_q(k, n)$. Then $d_{\mathrm{s}}(X, Y) \geq d_{\mathrm{H}}(v(X), v(Y))$, where d_{s} denotes the subspace distance (see Definition 1.8), and d_{H} denotes the Hamming distance (see Definition 1.45).

Notation 4.51. Let v be a binary vector of length n and weight k, and let $1 \leq p_1 < p_2 < \cdots < p_k \leq n$ be the positions of the k ones of v. The **Ferrers diagram associated to** v is the Ferrars diagram $\mathcal{F}_v = [r_1, \ldots, r_k]$ of size $k \times (n - k)$ with $r_i = n - k - p_i + i$ for all $i = 1, ..., k$.

The following result is straightforward. See [29], Section III and IV for examples and details.

Lemma 4.52. Let v be a binary vector of length n and weight k, and let $1 \leq p_1 < p_2 < \cdots < p_k \leq n$ be the positions of the k ones of v. Let $M \in \mathbb{F}_q[\mathcal{F}_v]$. For $j = 1, ..., n$ define $n_j := |\{1 \leq i \leq k \mid p_i \leq j\}|$. There exists a unique $k \times n$ matrix N over $\mathbb{F}_q$ in reduced row echelon form having v as pivot vector and $N_{i,j} = M_{i,j-n_j}$ for all $i \in \{1, ..., k\}$ and $j \in \{1, ..., n\} \setminus \{p_1, ..., p_k\}$.

We denote the matrix N of Lemma 4.52 by $N(v, M)$. We sometimes call $N(v, M)$ a **lift** of M. The multilevel construction of [29] is summarized in the following result.

Theorem 4.53 ([29], Theorem 3)**.** Let C be a binary code of constant weight k, length n and minimum distance at least 2δ. For any $v \in C$ let $S(v) \subseteq \mathbb{F}_q[\mathcal{F}_v]$ be a $\underline{\delta}$-space. The set

$$\{\text{rowsp } N(v, M) \mid v \in C,\ M \in S(v)\} \subseteq \mathcal{G}_q(k, n)$$

is a subspace code of minimum subspace distance at least 2δ and cardinality $\sum_{v \in C} q^{\dim S(v)}$.

Remark 4.54. Large subspace codes for $\delta > 2$ were obtained in [29] combining the multilevel construction and a computer search, for small values of q. The computer search part is employed to find large spaces of matrices of rank at least δ and given shape. The results of Section 4.2 allow us to construct in a systematic way (i.e., without a computer search) linear spaces of matrices with the same parameters as those found via computer search in [29]. In particular, we can construct subspace codes with the same parameters for any q.

Remark 4.55. In [90], A-L. Trautmann and J. Rosenthal propose the **pending dots** construction to improve the multilevel construction of [29]. As the multilevel construction, the pending dots construction also depends on the existence of large spaces of matrices with bounded rank and given shape. Using the idea of pending dots, A-L. Trautmann and N. Silberstein construct large subspace codes in $\mathcal{G}_q(k, n)$ of minimum subspace distance 4 (Section IV of [82] and Section IV of [83]) and $2(k-1)$ (see Section V of [82] and Section III of [83]) for arbitrary values of q. The Ferrers diagrams they consider for the first case are covered by Remark 4.22, while the diagrams that they consider for the second case ([82], Lemma 23 and [83], Lemma 18) are special cases of the diagrams studied in Theorem 4.32.

We now give some examples of how to combine the results of Section 4.2 and the multilevel construction illustrated above to obtain subspace codes with the largest known cardinality for given k, n, and δ.

Example 4.56. Let $(n, k, \delta) := (10, 5, 3)$, and let q be any prime power. Consider the binary code

$$C := \{1111100000,\ 1100011100,\ 0011011010,\ 1000110011,\ 0010101101,\ 0101000111\} \subseteq \mathbb{F}_2^{10}.$$

Observe that C has constant weight 5 and minimum distance 6. Let $v_1, ..., v_6$ be the elements of C in the displayed order. It follows from Theorem 4.24 that:

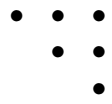
1. $\text{MaxDim}_{\underline{\delta}}(\mathcal{F}_{v_1}, \mathbb{F}_q) = 15$,
2. $\text{MaxDim}_{\underline{\delta}}(\mathcal{F}_{v_2}, \mathbb{F}_q) = 6$,
3. $\text{MaxDim}_{\underline{\delta}}(\mathcal{F}_{v_3}, \mathbb{F}_q) = 2$.

Notice moreover that $\mathcal{F}_{v_4}$ has the following graphical representation.

By Theorem 4.17 there exist a 2-dimensional $\underline{2}$-space V of 2×2 matrices over $\mathbb{F}_q$ and a 2-dimensional $\underline{1}$-space W of 1×2 matrices over $\mathbb{F}_q$. Let $\{M_1, M_2\}$ and $\{N_1, N_2\}$ be bases for V and W, respectively. Then

$$\mathrm{Span}_{\mathbb{F}_q}\left\{\begin{bmatrix} 0 & N_i & 0_{1\times 2} \\ 0 & 0_{2\times 2} & M_i \end{bmatrix} \mid i = 1, 2\right\}$$

is a 2-dimensional $\underline{\delta}$-space of matrices whose shape is $\mathcal{F}_{v_4}$. Since $T_\delta(\mathcal{F}_{v_4}) = 2$, it follows that $\mathrm{MaxDim}_{\underline{\delta}}(\mathcal{F}_{v_4}, \mathbb{F}_q) = 2$. Finally, $\mathcal{F}_{v_5}$ has $T_\delta(\mathcal{F}_{v_5}) = 1$ and contains the Ferrers diagram



Hence by Corollary 4.34 and Lemma 4.14 we have $\mathrm{MaxDim}_{\underline{\delta}}(\mathcal{F}_{v_5}, \mathbb{F}_q) = 1$. Using Theorem 4.53 we obtain a subspace code $\mathcal{C} \subseteq \mathcal{G}_q(5, 10)$ of minimum distance $\delta = 3$ with

$$|\mathcal{C}| = q^{15} + q^6 + 2q^2 + q + 1.$$

For $q \geq 3$ this is the subspace code of parameters $(n, k, \delta) = (10, 5, 3)$ with largest known cardinality.

Let us briefly recall the definition of **lexicode**. The vectors of $\mathbb{F}_2^n$ can be lexicographically ordered as follows. Let $v, w \in \mathbb{F}_2^n$, $v \neq w$, and let $i := \min\{j \mid v_j \neq w_j\}$. We say that $w \prec v$ if $v_i = 1$. Given a binary vector $v \in \mathbb{F}_2^n$ of weight k, the constant weight lexicode originated by v of minimum distance 2δ is constructed through iterated steps as follows. Start with $C = \{v\}$. List the elements of $\mathbb{F}_2^n$ in decreasing lexicographic order. At each step add to C the first vector of the list of weight k and Hamming distance at least 2δ from all the elements of C, until there is no such vector left.

According to Theorem 4.53, the cardinality of a subspace code obtained through the multilevel construction depends on the choice of the binary constant weight code. Since lexicodes are known to have large cardinality among constant weight binary codes with the same parameters, T. Etzion and N. Silberstein suggest in [29] to use the lexicode originated by the vector

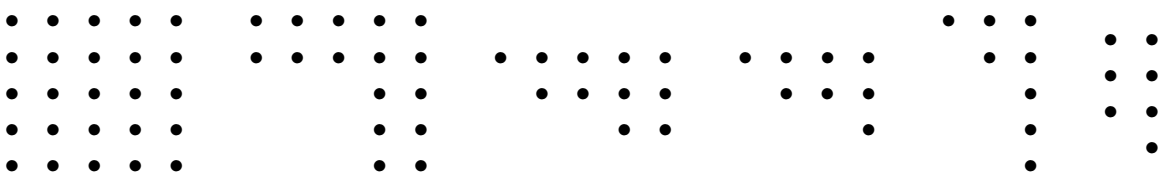
$$\underbrace{1\cdots 1}_{k}\underbrace{0\cdots 0}_{n-k}$$

in the multilevel construction. However this choice is not always optimal, as we show in the following example.

Example 4.57. Let $n := 10$, $k := 5$, $\delta = 3$. Consider the binary constant weight lexicode

$$C' := \{1111100000,\ 1100011100,\ 1010010011,\ 0101001011,\ 0010101110,\ 0001110101\} \subseteq \mathbb{F}_2^{10}.$$

Let $w_1, ..., w_6$ be the elements of C' in the displayed order. The graphical representations of the $\mathcal{F}_{w_i}$'s are as follows.



One can easily check that

$$T_3(\mathcal{F}_{w_1}) = 15, \quad T_3(\mathcal{F}_{w_2}) = 6, \quad T_3(\mathcal{F}_{w_3}) = 2, \quad T_3(\mathcal{F}_{w_4}) = 1, \quad T_3(\mathcal{F}_{w_5}) = 1, \quad T_3(\mathcal{F}_{w_6}) = 0.$$

Therefore, by Theorem 4.53 and Theorem 4.15, choosing C' as the pivot code produces a subspace code of cardinality at most

$$q^{15} + q^6 + q^2 + 2q + 1.$$

However, the binary code C considered in Example 4.56 produces a subspace code with the same parameters n, k, δ and larger cardinality, for all values of q.

Theorem 4.24 allows us to give a lower bound the cardinality of subspace codes obtained from given pivot vectors through the multilevel construction.

Theorem 4.58. Fix integers n, k, δ with $2 \leq \delta \leq k \leq n/2$. Let $D \subseteq \mathbb{F}_2^n$ be a code of constant weight k and minimum distance at least 2δ. For $v \in D$ let $p_i(v)$ denote the position of the i-th one of v. Let

$$D' := \{v \in D \mid p_{\delta-1}(v) \leq n - 2k + \delta - 1\}$$

and

$$D'' = \{v \in D \mid p_i(v) \leq n - k - \delta + 2i - 1,\ i = 1, \ldots, \delta\}.$$

Then there exists a subspace code $\mathcal{C}' \subseteq \mathcal{G}_q(k, n)$ of minimum subspace distance at least 2δ and

$$|\mathcal{C}'| = \sum_{v \in D'} q^{T_\delta(\mathcal{F}_v)} + \sum_{v \in D'' \setminus D'} q + |D \setminus D''|.$$

Moreover any subspace code $\mathcal{C}$ with minimum distance at least 2δ obtained from D through the multilevel construction has

$$|\mathcal{C}| \leq \sum_{v \in D''} q^{T_\delta(\mathcal{F}_v)} + |D \setminus D''| \leq |\mathcal{C}'| + \mathcal{O}\left(q^{(k-\delta+1)(k-1)}\right)$$

asymptotically in q.

Proof. For $v \in D$ we denote by $r_i(v)$ the cardinality of the i-th row of $\mathcal{F}_v$ for $i = 1, ..., k$. As in Notation 4.51, the cardinality of the i-th row of $\mathcal{F}_v$ is $r_i(v) = n - k - p_i(v) + i$.

Let $v \notin D''$, then there exists $j \in \{1, \ldots, \delta\}$ such that $r_j(v) \leq n-k-(n-k-\delta+2j)+j = \delta - j$. Therefore,

$$T_\delta(\mathcal{F}_v, j-1) = \sum_{u=j}^{k} \max\{r_u(v) - (\delta - j), 0\} = 0 = T_\delta(\mathcal{F}_v).$$

This proves that any subspace code $\mathcal{C}$ obtained from D through the multilevel construction has

$$|\mathcal{C}| \leq \sum_{v \in D''} q^{T_\delta(\mathcal{F}_v)} + |D \setminus D''|.$$

Let now $v \in D'$. Since $p_{\delta-1}(v) \leq n - 2k + \delta - 1$, we have $r_{\delta-1}(v) \geq k$. Combining Theorem 4.24 and the multilevel construction using the vectors of D', we construct a code of cardinality $\sum_{v \in D'} q^{T_\delta(\mathcal{F}_v)}$ and minimum distance at least δ. For any $v \in D''$, the associated Ferrers diagram $\mathcal{F}_v \supseteq [\delta, \delta - 1, \ldots, 1, 0, \ldots, 0]$ by the definition of D''. Hence there exists at least one matrix of rank δ and shape $\mathcal{F}_v$, namely the $k \times (n-k)$ matrix containing a top-right justified $\delta \times \delta$ identity matrix and zeroes everywhere else. Adding the lift of these matrices to the previous code through the multilevel construction, we construct a code $\mathcal{C}'$ with

$$|\mathcal{C}'| = \sum_{v \in D'} q^{T_\delta(\mathcal{F}_v)} + \sum_{v \in D'' \setminus D'} q + |D \setminus D''|,$$

as claimed.

It follows from the previous argument that the cardinality of a code $\mathcal{C}$ obtained from D through the multilevel construction can be increased only by producing larger linear spaces of matrices of rank at least δ and support contained in $\mathcal{F}_v$ for $v \in D'' \setminus D'$. Observe that for any such v we have $r_{\delta-1}(v) \leq k-1$, hence $r_i(v) \leq k-1$ for $i = \delta, ..., k$. Hence

$$T_\delta(\mathcal{F}_v) \leq \sum_{i=\delta}^{k} r_i(v) \leq (k-\delta+1)(k-1).$$

Since $|D \setminus D''|$ and $|D'' \setminus D'|$ are constant in k, we have

$$|\mathcal{C}| - |\mathcal{C}'| \in \mathcal{O}\left(q^{(k-\delta+1)(k-1)}\right).$$

□

Example 4.59. In Table 4.1 we give some cardinalities of subspace codes which we find combining the results of Section 4.2 with the multilevel construction of [29] as shown in Example 4.56. For $q \geq 3$ and the given values of k, n and δ, the codes have the largest known size.

n	k	δ	size
10	5	3	$q^{15} + q^6 + 2q^2 + q + 1$
11	5	3	$q^{18} + q^9 + q^6 + q^4 + 4q^3 + 3q^2$
14	5	4	$q^{18} + q^{10} + q^3 + 1$
15	6	5	$q^{18} + q^5 + 1$
12	5	3	$q^{21} + q^{12} + q^{11} + 2q^7 + 4q^6 + 2q^5$
13	5	3	$q^{24} + q^{15} + q^{14} + q^{12} + 3q^{10} + 2q^9 + 2q^8 + q^5 + q^4 + 1$
12	4	3	$q^{16} + q^{10} + q^6 + q^5 + q^3 + q^2 + q + 2$
13	5	4	$q^{16} + q^6 + 1$

Table 4.1: Cardinality of some large subspace codes in $\mathcal{G}_q(k, n)$ with minimum distance 2δ.

Chapter 5

Duality theory of rank-metric codes

This chapter is devoted to a foundational study of the duality theory of linear codes with the rank metric. As illustrated in Section 1.5, in the coding theory literature appear two different families of linear rank-metric codes, namely, Delsarte and Gabidulin codes. Proposition 1.25 shows how to associate to a Gabidulin code a Delsarte code with the same metric properties. Therefore Delsarte codes can be seen as a generalization of Gabidulin codes. It is not clear however how the duality theories of Delsarte and Gabidulin codes relate to each other, as the duals of Delsarte and Gabidulin codes are defined in two *a priori* unrelated ways (see Definitions 1.15 and 1.22).

In this chapter we first compare the duality theories of Delsarte and Gabidulin codes, and show that the former can be viewed as a generalization of the latter (Section 5.1). In particular, we prove that all the main properties of Gabidulin codes can be regarded as special instances of analogous (more general) properties of Delsarte codes.

We then provide in Section 5.2 a simple proof for the MacWilliams identities for the family of Delsarte codes. The same identities were shown (for general additive codes) by Delsarte in [20] employing sophisticated tools from combinatorics (in particular, using the theory of association schemes). Our approach is simpler, and essentially based on a double counting argument. Then we show that all the main properties of Delsarte codes can be viewed as straightforward consequences of the MacWilliams identities for the rank metric.

In Section 5.3 we establish new bounds on the parameters of Delsarte codes, and characterize the codes that attain them. Our bounds involve a new parameter associated to a Delsarte code, which we call "maximum rank" of the code.

In Section 5.4 we then study optimal linear anticodes in the rank metric, showing in particular that the dual of an optimal anticode is an optimal anticode. The result may be regarded as the analogue of Theorem 1.18 in the context of rank-metric anticodes.

Finally, we study applications of MacWilliams identities for the rank weight to enumerative problems of matrices. More in detail, we provide closed formulas for the number of $k \times m$ matrices over $\mathbb{F}_q$ with given rank and satisfying one of the following conditions: a prescribed set of their diagonal entries are zero, a prescribed set of their entries sum to zero, their entries are zero in a rectangular region. These formulas generalize some results obtained with much more sophisticated methods by other authors. As an application of our enumerative techniques, in Corollary 5.37 we answer a generalized question of R. Stanley employing a simple argument.

The results of this chapter have been published in [77] and in the last section of [79].

Notation 5.1. Throughout this chapter we work with a fixed prime power q and with integers k and m such that $0 < k \leq m$ without loss of generality. We simply denote by Mat the vector space $\mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ of $k \times m$ matrices over $\mathbb{F}_q$. The vector space generated over $\mathbb{F}_q$ by the columns of a matrix $M \in \mathrm{Mat}$ is denoted by $\mathrm{colsp}(M) \subseteq \mathbb{F}_q^k$. All dimensions in the chapter are computed over $\mathbb{F}_q$, unless differently specified. For all the rest we follow the notation of Section 1.5.

5.1 Delsarte and Gabidulin codes

Given a Gabidulin code $C \subseteq \mathbb{F}_{q^m}^k$ and a basis $\mathcal{G}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, it is natural to ask whether the Delsarte codes $\mathcal{C}_\mathcal{G}(C^\perp)$ and $\mathcal{C}_\mathcal{G}(C)^\perp$ coincide or not (see Definition 1.24 for the notation). The answer is unfortunately negative in general, as we show in the following example.

Example 5.2. Let $q = 3$, $k = m = 2$ and $\mathbb{F}_{3^2} = \mathbb{F}_3[\eta]$, where η is a root of the irreducible primitive polynomial $x^2 + 2x + 2 \in \mathbb{F}_3[x]$. Let $\xi := \eta^2$, so that $\xi^2 + 1 = 0$. Set $\alpha := (\xi, 2)$, and let $C \subseteq \mathbb{F}_{3^2}^2$ be the 1-dimensional Gabidulin code generated by α over $\mathbb{F}_{3^2}$. Take $\mathcal{G} := \{1, \xi\}$ as basis of $\mathbb{F}_{3^2}$ over $\mathbb{F}_3$. One can easily check that $\mathcal{C}_\mathcal{G}(C)$ is generated over $\mathbb{F}_3$ by the two matrices

$$M_\mathcal{G}(\alpha) = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}, \qquad M_\mathcal{G}(\xi\alpha) = \begin{bmatrix} -1 & 0 \\ 0 & 2 \end{bmatrix}.$$

Let $\beta := (\xi, 1) \in \mathbb{F}_{3^2}^2$. We have $\langle \alpha, \beta \rangle = 1 \neq 0$, and so $\beta \notin C^\perp$. It follows $M_\mathcal{G}(\beta) \notin \mathcal{C}_\mathcal{G}(C^\perp)$. On the other hand,

$$M_\mathcal{G}(\beta) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

and it is easy to see that $M_\mathcal{G}(\beta)$ is trace-orthogonal to both $M_\mathcal{G}(\alpha)$ and $M_\mathcal{G}(\xi\alpha)$. It follows $M_\mathcal{G}(\beta) \in \mathcal{C}_\mathcal{G}(C)^\perp$, and so $\mathcal{C}_\mathcal{G}(C)^\perp \neq \mathcal{C}_\mathcal{G}(C^\perp)$.

Although, for a fixed basis $\mathcal{G}$, the duality notions for Delsarte and Gabidulin codes do not coincide, we now show that there is a very simple relation between them via orthogonal bases of finite fields. A relation between the trace-product of Mat and the standard inner product of $\mathbb{F}_{q^m}^k$ was observed also in [41].

Definition 5.3. Let $\mathrm{Trace} : \mathbb{F}_{q^m} \to \mathbb{F}_q$ be **trace** map given by $\mathrm{Trace}(\alpha) := \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}$ for all $\alpha \in \mathbb{F}_{q^m}$. Bases $\mathcal{G} = \{\gamma_1, ..., \gamma_m\}$ and $\mathcal{G}' = \{\gamma'_1, ..., \gamma'_m\}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ are called **orthogonal** (or **dual**) if $\mathrm{Trace}(\gamma'_i\gamma_j) = \delta_{ij}$ for all $i, j \in \{1, ..., m\}$.

The following result on orthogonal bases is well-known.

Proposition 5.4 ([63], page 54)**.** Every basis $\mathcal{G}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ has a unique orthogonal basis $\mathcal{G}'$.

Theorem 5.5. Let $C \subseteq \mathbb{F}_{q^m}^k$ be a Gabidulin code, and let $\mathcal{G}$, $\mathcal{G}'$ be orthogonal bases of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. We have

$$\mathcal{C}_{\mathcal{G}'}(C^\perp) = \mathcal{C}_\mathcal{G}(C)^\perp.$$

In particular, if we set $\mathcal{C} := \mathcal{C}_\mathcal{G}(C)$, then C has the same rank distribution as $\mathcal{C}$, and $C^\perp$ has the same rank distribution as $\mathcal{C}^\perp$.

Proof. Let $\mathcal{G} = \{\gamma_1, ..., \gamma_m\}$ and $\mathcal{G}' = \{\gamma'_1, ..., \gamma'_m\}$. Take any $M \in \mathcal{C}_{\mathcal{G}'}(C^\perp)$ and $N \in \mathcal{C}_\mathcal{G}(C)$. There exist $\alpha \in C^\perp$ and $\beta \in C$ such that $M = M_{\mathcal{G}'}(\alpha)$ and $N = M_\mathcal{G}(\beta)$. According to Definition 4.51 we

have

$$0 = \langle \alpha, \beta \rangle = \sum_{i=1}^{k} \alpha_i \beta_i = \sum_{i=1}^{k} \sum_{j=1}^{m} M_{ij} \gamma'_j \sum_{t=1}^{m} N_{it} \gamma_t = \sum_{i=1}^{k} \sum_{j=1}^{m} \sum_{t=1}^{m} M_{ij} N_{it} \gamma'_j \gamma_t. \tag{5.1}$$

We now apply the function $\mathrm{Trace} : \mathbb{F}_{q^m} \to \mathbb{F}_q$ to both sides of equation (5.1), and obtain

$$0 = \mathrm{Trace}\left(\sum_{i=1}^{k} \sum_{j=1}^{m} \sum_{t=1}^{m} M_{ij} N_{it} \gamma'_j \gamma_t \right) = \sum_{i=1}^{k} \sum_{j=1}^{m} \sum_{t=1}^{m} M_{ij} N_{it} \mathrm{Trace}(\gamma'_j \gamma_t) = \mathrm{Tr}(M N^t).$$

By Definition 1.15, we have $\mathcal{C}_{\mathcal{G}'}(C^\perp) \subseteq \mathcal{C}_{\mathcal{G}}(C)^\perp$. Proposition 1.25 and Lemma 1.17 imply that $\mathcal{C}_{\mathcal{G}'}(C^\perp)$ and $\mathcal{C}_{\mathcal{G}}(C)^\perp$ have the same dimension over $\mathbb{F}_q$. Hence the two codes are equal. The second part of the statement easily follows from Proposition 1.25. □

Theorem 5.5 shows that the duality theory of Delsarte rank-metric codes can be regarded as a generalization of the duality theory of Gabidulin rank-metric codes. In particular, all the results on Delsarte codes which we will prove in the remainder of the chapter also apply to Gabidulin codes.

5.2 MacWilliams identities for rank-metric codes

In this section we present a simple proof of the MacWilliams identities for Delsarte rank-metric codes. The same identities were first shown in [20] by Delsarte himself using the machinery of association schemes for additive rank-metric codes. The formulas that we derive in the first place are different from those of [20], and are more straightforward. The proof that we present is essentially based on a double counting argument. We will also show how for the case of linear codes the identities in the form proposed by Delsarte can be obtained from our formulas.

Notation 5.6. For any matrices $M, N \in \mathrm{Mat}$ we have $\mathrm{colsp}(M+N) \subseteq \mathrm{colsp}(M) + \mathrm{colsp}(N)$. As a consequence, if $U \subseteq \mathbb{F}_q^k$ is a vector subspace, then the set of matrices $M \in \mathrm{Mat}$ with $\mathrm{colsp}(M) \subseteq U$ is a vector subspace of Mat, which we denote by $\mathrm{Mat}(U)$.

We start with a series of preliminary results.

Lemma 5.7. Let $U \subseteq \mathbb{F}_q^k$ be a subspace. We have $\dim(\mathrm{Mat}(U)) = m \cdot \dim(U)$.

Proof. Let $s := \dim(U)$. Define the s-dimensional space $V := \{x \in \mathbb{F}_q^k : x_i = 0 \text{ for } i > s\} \subseteq \mathbb{F}_q^k$. There exists an $\mathbb{F}_q$-isomorphism $g : \mathbb{F}_q^k \to \mathbb{F}_q^k$ that maps U into V. Let $G \in \mathrm{Mat}_{k \times k}(\mathbb{F}_q)$ be the invertible matrix associated to g with respect to the canonical basis $\{e_1, ..., e_k\}$ of $\mathbb{F}_q^k$, i.e.,

$$g(e_j) = \sum_{i=1}^{k} G_{ij} e_i \qquad \text{for all } j = 1, ..., k.$$

For any matrix $M \in \mathrm{Mat}$ we have $g(\mathrm{colsp}(M)) = \mathrm{colsp}(GM)$, and it is easy to check that the map $M \mapsto GM$ is an $\mathbb{F}_q$-isomorphism $\mathrm{Mat}(U) \to \mathrm{Mat}(V)$. Now we observe that $\mathrm{Mat}(V))$ is the vector space of matrices $M \in \mathrm{Mat}$ whose last $k - s$ rows equal zero. Therefore we have $\dim(\mathrm{Mat}(U)) = \dim(\mathrm{Mat}(V)) = km - m(k-s) = ms$, and the lemma follows. □

Notation 5.8. Given a subspace $U \subseteq \mathbb{F}_q^k$, in the sequel we denote by $U^\perp$ the orthogonal of U with respect to the standard inner product of $\mathbb{F}_q^k$. It will be clear from context if by "$\perp$" we mean the trace-dual in Mat or the standard dual in $\mathbb{F}_q^k$.

Lemma 5.9. Let $U \subseteq \mathbb{F}_q^k$ be a subspace. Then $\mathrm{Mat}(U)^\perp = \mathrm{Mat}(U^\perp)$.

Proof. Let $N \in \mathrm{Mat}(U^\perp)$ and $M \in \mathrm{Mat}(U)$. Using the definition of trace-product one sees that $\mathrm{Tr}(MN^t) = \sum_{i=1}^m \langle M_i, N_i \rangle$, where $\langle \cdot, \cdot \rangle$ is the standard inner product of $\mathbb{F}_q^k$ and M_i and N_i denote the i-th column of M and N, respectively. Each column of N belongs to $U^\perp$, and each column of M belongs to U. Thus $\mathrm{Tr}(MN^t) = 0$. This shows that $\mathrm{Mat}(U^\perp) \subseteq \mathrm{Mat}(U)^\perp$. By Lemma 5.7, the two spaces $\mathrm{Mat}(U^\perp)$ and $\mathrm{Mat}(U)^\perp$ have the same dimension over $\mathbb{F}_q$. Hence they are equal. □

Lemma 5.10. Let $\mathcal{C} \subseteq \mathrm{Mat}$ be a Delsarte code, and let $U \subseteq \mathbb{F}_q^k$ be a subspace. Denote by s the dimension of U over $\mathbb{F}_q$. We have

$$|\mathcal{C} \cap \mathrm{Mat}(U)| = \frac{|\mathcal{C}|}{q^{m(k-s)}} |\mathcal{C}^\perp \cap \mathrm{Mat}(U^\perp)|.$$

Proof. Combining Lemma 1.17 and Lemma 5.9 we obtain

$$(\mathcal{C} \cap \mathrm{Mat}(U))^\perp = \mathcal{C}^\perp + \mathrm{Mat}(U)^\perp = \mathcal{C}^\perp + \mathrm{Mat}(U^\perp).$$

Thus by Lemma 1.17 we have

$$|\mathcal{C} \cap \mathrm{Mat}(U)| \cdot |\mathcal{C}^\perp + \mathrm{Mat}(U^\perp)| = q^{km}. \tag{5.2}$$

On the other hand, Lemma 5.7 gives

$$\dim(\mathcal{C}^\perp + \mathrm{Mat}(U^\perp)) = \dim(\mathcal{C}^\perp) + m \cdot \dim(U^\perp) - \dim(\mathcal{C}^\perp \cap \mathrm{Mat}(U^\perp)),$$

and so, again by Lemma 1.17,

$$|\mathcal{C}^\perp + \mathrm{Mat}(U^\perp)| = \frac{q^{km} \cdot q^{m(k-s)}}{|\mathcal{C}| \cdot |\mathcal{C}^\perp \cap \mathrm{Mat}(U^\perp)|}. \tag{5.3}$$

Combining equation (5.2) and equation (5.3) one easily obtains the lemma. □

The following result is well-known, but we include it for completeness.

Lemma 5.11. Let $0 \leq t, s \leq k$ be integers, and let $X \subseteq \mathbb{F}_q^k$ be a subspace of dimension t over $\mathbb{F}_q$. The number of subspaces $U \subseteq \mathbb{F}_q^k$ such that $X \subseteq U$ and $\dim(U) = s$ is

$$\begin{bmatrix} k-t \\ s-t \end{bmatrix}.$$

Proof. Let $\pi : \mathbb{F}_q^k \to \mathbb{F}_q^k / X$ denote the projection on the quotient vector space $\mathbb{F}_q^k$ modulo X. It is easy to see that π induces a bijection between the s-dimensional vector subspaces of $\mathbb{F}_q^k$ containing X and the $(s-t)$-dimensional subspaces of $\mathbb{F}_q^k / X$. The lemma follows from the fact that $\mathbb{F}_q^k / X$ has dimension $k - t$. □

Lemma 5.12. Let $\mathcal{C} \subseteq \mathrm{Mat}$ be a Delsarte code, and let $0 \leq s \leq k$ be an integer. We have

$$\sum_{\substack{U \subseteq \mathbb{F}_q^k \\ \dim(U) = s}} |\mathcal{C} \cap \mathrm{Mat}(U)| = \sum_{i=0}^{k} W_i(\mathcal{C}) \begin{bmatrix} k-i \\ k-s \end{bmatrix}.$$

Proof. Define the set $\mathcal{A}(\mathcal{C}, s) := \{(U, M) : U \subseteq \mathbb{F}_q^k,\ \dim(U) = s,\ M \in \mathcal{C},\ \mathrm{colsp}(M) \subseteq U\}$. We will count the elements of $\mathcal{A}(\mathcal{C}, s)$ in two different ways. On the one hand, using Lemma 5.11 we find

$$\begin{aligned}
|\mathcal{A}(\mathcal{C}, s)| &= \sum_{M \in \mathcal{C}} |\{U \subseteq \mathbb{F}_q^k,\ \dim(U) = s,\ \mathrm{colsp}(M) \subseteq U\}| \\
&= \sum_{i=0}^{k} \sum_{\substack{M \in \mathcal{C} \\ \mathrm{rk}(M) = i}} |\{U \subseteq \mathbb{F}_q^k,\ \dim(U) = s,\ \mathrm{colsp}(M) \subseteq U\}| \\
&= \sum_{i=0}^{k} \sum_{\substack{M \in \mathcal{C} \\ \mathrm{rk}(M) = i}} \begin{bmatrix} k-i \\ s-i \end{bmatrix} = \sum_{i=0}^{k} A_i \begin{bmatrix} k-i \\ s-i \end{bmatrix} = \sum_{i=0}^{k} A_i \begin{bmatrix} k-i \\ k-s \end{bmatrix}.
\end{aligned}$$

On the other hand,

$$|\mathcal{A}(\mathcal{C}, s)| = \sum_{\substack{U \subseteq \mathbb{F}_q^k \\ \dim(U) = s}} |\{M \in \mathcal{C} : \mathrm{colsp}(M) \subseteq U\}| = \sum_{\substack{U \subseteq \mathbb{F}_q^k \\ \dim(U) = s}} |\mathcal{C} \cap \mathrm{Mat}(U)|,$$

and the lemma follows. □

We can now give a simple proof for an implicit formulation of MacWilliams identities for Delsarte codes.

Theorem 5.13. Let $\mathcal{C} \subseteq \mathrm{Mat}$ be a Delsarte code. For any integer $0 \leq \nu \leq k$ we have

$$\sum_{i=0}^{k-\nu} W_i(\mathcal{C}) \begin{bmatrix} k-i \\ \nu \end{bmatrix} = \frac{|\mathcal{C}|}{q^{m\nu}} \sum_{j=0}^{\nu} W_j(\mathcal{C}^\perp) \begin{bmatrix} k-j \\ \nu-j \end{bmatrix}.$$

Proof. Lemma 5.12 applied to $\mathcal{C}$ with $s = k - \nu$ gives

$$\sum_{\substack{U \subseteq \mathbb{F}_q^k \\ \dim(U) = k-\nu}} |\mathcal{C} \cap \mathrm{Mat}(U)| = \sum_{i=0}^{k} W_i(\mathcal{C}) \begin{bmatrix} k-i \\ \nu \end{bmatrix}.$$

The map $U \mapsto U^\perp$ is a bijection between the ν-dimensional and the $(k-\nu)$-dimensional subspaces of $\mathbb{F}_q^k$. Hence we have

$$\sum_{\substack{U \subseteq \mathbb{F}_q^k \\ \dim(U) = k-\nu}} |\mathcal{C}^\perp \cap \mathrm{Mat}(U^\perp)| = \sum_{\substack{U \subseteq \mathbb{F}_q^k \\ \dim(U) = \nu}} |\mathcal{C}^\perp \cap \mathrm{Mat}(U)| = \sum_{j=0}^{k} W_j(\mathcal{C}^\perp) \begin{bmatrix} k-j \\ k-\nu \end{bmatrix},$$

where the second equality follows from Lemma 5.12 applied to the code $\mathcal{C}^\perp$ with $s = \nu$. Lemma 5.10 with $s = k - \nu$ gives

$$\sum_{i=0}^{k} W_i(\mathcal{C}) \begin{bmatrix} k-i \\ \nu \end{bmatrix} = \frac{|\mathcal{C}|}{q^{m\nu}} \sum_{j=0}^{k} W_j(\mathcal{C}^\perp) \begin{bmatrix} k-j \\ \nu-j \end{bmatrix}.$$

By definition, for $i > k - \nu$ and for $j > \nu$ we have

$$\begin{bmatrix} k-i \\ \nu \end{bmatrix} = \begin{bmatrix} k-j \\ \nu-j \end{bmatrix} = 0,$$

and the theorem follows. □

Theorem 5.13 produces $k+1$ linear identities that relate the rank distribution of a dual code $\mathcal{C}^\perp$ to the rank distribution of $\mathcal{C}$. The following corollary gives a recursive method to compute the rank distribution of $\mathcal{C}^\perp$ from the rank distribution of $\mathcal{C}$ using these identities.

Corollary 5.14. Let $\mathcal{C} \subseteq \mathrm{Mat}$ be a Delsarte code. For $\nu = 0, ..., k$ define

$$a_\nu^k := \frac{q^{m\nu}}{|\mathcal{C}|} \sum_{i=0}^{k-\nu} W_i(\mathcal{C}) \begin{bmatrix} k-i \\ \nu \end{bmatrix}.$$

The $W_j(\mathcal{C}^\perp)$'s are given by the recursive formulas

$$\begin{cases} W_0(\mathcal{C}^\perp) = 1, \\ W_\nu(\mathcal{C}^\perp) = a_\nu^k - \sum_{j=0}^{\nu-1} W_j(\mathcal{C}^\perp) \begin{bmatrix} k-j \\ \nu-j \end{bmatrix} \quad \text{for } \nu = 1, ..., k, \\ W_\nu(\mathcal{C}^\perp) = 0 \quad \text{for } \nu > k. \end{cases}$$

Proof. Clearly, $W_0(\mathcal{C}^\perp) = 1$ and $W_\nu(\mathcal{C}^\perp) = 0$ for $\nu > k$. For any fixed integer $\nu \in \{1, ..., k\}$ Theorem 5.13 gives

$$a_\nu^k = \sum_{j=0}^{\nu-1} W_j(\mathcal{C}^\perp) \begin{bmatrix} k-j \\ \nu-j \end{bmatrix} + W_\nu(\mathcal{C}^\perp),$$

which proves the result. □

Now we show that Theorem 5.13 can be re-written in the form of Theorem 3.3 of [20].

Corollary 5.15 (see [20], Theorem 3.3)**.** Let $\mathcal{C} \subseteq \mathrm{Mat}$ be a Delsarte code. We have

$$W_j(\mathcal{C}^\perp) = \frac{1}{|\mathcal{C}|} \sum_{i=0}^{k} W_i(\mathcal{C}) \sum_{s=0}^{k} (-1)^{j-s} q^{ms+\binom{j-s}{2}} \begin{bmatrix} k-s \\ k-j \end{bmatrix} \begin{bmatrix} k-i \\ s \end{bmatrix}$$

for all $j = 0, ..., k$.

Proof. Throughout this proof the rows and columns of matrices are labeled from 0 to k for ease of notation (instead of from 1 to $k+1$). Define the $(k+1) \times (k+1)$ matrix P by

$$P_{ji} := \frac{1}{|\mathcal{C}|} \sum_{s=0}^{k} (-1)^{j-s} q^{ms+\binom{j-s}{2}} \begin{bmatrix} k-s \\ k-j \end{bmatrix} \begin{bmatrix} k-i \\ s \end{bmatrix}$$

for $j, i \in \{0, ..., k\}$. We can write the statement in matrix form as $(W_0(\mathcal{C}^\perp), ..., W_k(\mathcal{C}^\perp))^t = P \cdot (W_0(\mathcal{C}), ..., W_k(\mathcal{C}))^t$. Define $(k+1) \times (k+1)$ matrices S, T by

$$S_{ij} := \begin{bmatrix} k-j \\ i-j \end{bmatrix}, \qquad T_{ij} := \frac{q^{mi}}{|\mathcal{C}|} \begin{bmatrix} k-j \\ i \end{bmatrix}$$

for $i, j \in \{0, ..., k\}$. The matrix S is invertible, as it is lower-triangular and $S_{ii} = 1$ for $i = 0, ..., k$. Theorem 5.13 reads $S \cdot (W_0(\mathcal{C}^\perp), ..., W_k(\mathcal{C}^\perp))^t = T \cdot (W_0(\mathcal{C}), ..., W_k(\mathcal{C}))^t$. Thus it suffices to prove $T = SP$. Fix arbitrary integers $i, j \in \{0, ..., k\}$. We have

$$\begin{aligned} (SP)_{ij} &= \frac{1}{|\mathcal{C}|} \sum_{r=0}^{k} \begin{bmatrix} k-r \\ i-r \end{bmatrix} \sum_{s=0}^{k} (-1)^{r-s} q^{ms+\binom{r-s}{2}} \begin{bmatrix} k-s \\ k-r \end{bmatrix} \begin{bmatrix} k-j \\ s \end{bmatrix} \\ &= \frac{1}{|\mathcal{C}|} \sum_{s=0}^{k} q^{ms} \begin{bmatrix} k-j \\ s \end{bmatrix} \sum_{r=0}^{k} \begin{bmatrix} k-r \\ i-r \end{bmatrix} (-1)^{r-s} q^{\binom{r-s}{2}} \begin{bmatrix} k-s \\ k-r \end{bmatrix}. \end{aligned}$$

Clearly,

$$\begin{bmatrix} k-r \\ i-r \end{bmatrix} = \begin{bmatrix} k-r \\ k-i \end{bmatrix},$$

and using the definition of q-binomial coefficient one finds

$$\begin{bmatrix} k-s \\ k-r \end{bmatrix} \begin{bmatrix} k-r \\ k-i \end{bmatrix} = \begin{bmatrix} k-s \\ k-i \end{bmatrix} \begin{bmatrix} i-s \\ r-s \end{bmatrix}.$$

Hence we have

$$\begin{aligned}
\sum_{r=0}^{k} \begin{bmatrix} k-r \\ i-r \end{bmatrix} (-1)^{r-s} q^{\binom{r-s}{2}} \begin{bmatrix} k-s \\ k-r \end{bmatrix} &= \sum_{r=0}^{k} \begin{bmatrix} k-s \\ k-i \end{bmatrix} \begin{bmatrix} i-s \\ r-s \end{bmatrix} (-1)^{r-s} q^{\binom{r-s}{2}} \\
&= \begin{bmatrix} k-s \\ k-i \end{bmatrix} \sum_{r=0}^{k} \begin{bmatrix} i-s \\ r-s \end{bmatrix} (-1)^{r-s} q^{\binom{r-s}{2}} \\
&= \begin{bmatrix} k-s \\ k-i \end{bmatrix} \sum_{r=-s}^{k-s} \begin{bmatrix} i-s \\ r \end{bmatrix} (-1)^{r} q^{\binom{r}{2}} \\
&= \begin{bmatrix} k-s \\ k-i \end{bmatrix} \sum_{r=0}^{i-s} \begin{bmatrix} i-s \\ r \end{bmatrix} (-1)^{r} q^{\binom{r}{2}} \\
&= \begin{cases} 1 & \text{if } s = i, \\ 0 & \text{otherwise,} \end{cases}
\end{aligned}$$

where the last equality follows from the q-Binomial Theorem ([87], page 74). Therefore

$$(SP)_{ij} = \frac{1}{|\mathcal{C}|} q^{mi} \begin{bmatrix} k-j \\ i \end{bmatrix} = T_{ij},$$

as claimed. □

Remark 5.16. Identities in the form of our Theorem 5.13 were recently proved for the special family of Gabidulin codes in [33], Proposition 3. The proof of [33] is based on the Hadamard transform, q-products, q-derivatives and q-transforms of polynomials. By Theorem 5.5, our Theorem 5.13 also applies to the family of Gabidulin codes, providing in particular a simple proof for Proposition 3 of [33].

Theorem 5.13 and Corollary 5.14 allow us to re-establish the main results of the duality theory of rank-metric codes in a very concise way, as we show in the sequel. The following result immediately follows from Corollary 5.14.

Corollary 5.17. The rank distribution of a Delsarte code $\mathcal{C}$ determines the rank distribution of the dual code $\mathcal{C}^{\perp}$.

Example 5.18. Let $q = 3$, $k = 3$, $m = 4$. Consider the code $\mathcal{C}$ generated by the following three matrices:

$$\begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 2 \\ 1 & 1 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 2 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

It can be checked that $\dim(\mathcal{C}) = 3$ and that the rank distribution of $\mathcal{C}$ is $W_0(\mathcal{C}) = 1$, $W_1(\mathcal{C}) = 2$, $W_2(\mathcal{C}) = 0$, $W_3(\mathcal{C}) = 24$. The recursive formula of Corollary 5.14 allows us to compute:

$$W_0(\mathcal{C}^{\perp}) = 1, \quad W_1(\mathcal{C}^{\perp}) = 50, \quad W_2(\mathcal{C}^{\perp}) = 3432, \quad W_3(\mathcal{C}^{\perp}) = 16200.$$

Notice that $\sum_{i=0}^{3} W_i(\mathcal{C}^{\perp}) = 19683 = 3^9 = |\mathcal{C}^{\perp}|$, as expected.

Remark 5.19. Further properties of the rank distributions of Delsarte codes were investigated in [18] jointly with J. de la Cruz, E. Gorla, and H. Lopez.

Corollary 5.20 ([20], Theorem 5.5)**.** If a Delsarte code $\mathcal{C}$ is MRD, then $\mathcal{C}^\perp$ is also MRD.

Proof. Let $\mathcal{C} \subseteq \mathrm{Mat}$ be MRD. If $\mathcal{C} = \{0\}$ or $\mathcal{C} = \mathrm{Mat}$ then the result is immediate. Assume $0 < \dim(\mathcal{C}) < km$. Denote by d the minimum distance of $\mathcal{C}$, so that $|\mathcal{C}| = q^{m(k-d+1)}$. We have $W_0(\mathcal{C}) = W_0(\mathcal{C}^\perp) = 1$ and $W_i(\mathcal{C}) = 0$ for $1 \leq i \leq d-1$. Theorem 5.13 with $\nu = k-d+1$ gives

$$\begin{bmatrix} k \\ k-d+1 \end{bmatrix} = \begin{bmatrix} k \\ k-d+1 \end{bmatrix} + \sum_{j=1}^{k-d+1} W_j(\mathcal{C}^\perp) \begin{bmatrix} k-j \\ k-d+1-j \end{bmatrix},$$

i.e.,

$$\sum_{j=1}^{k-d+1} W_j(\mathcal{C}^\perp) \begin{bmatrix} k-j \\ k-d+1-j \end{bmatrix} = 0.$$

Since $d \geq 1$, for $1 \leq j \leq k-d+1$ we have $k-j \geq k-d+1-j \geq 0$, and so

$$\begin{bmatrix} k-j \\ k-d+1-j \end{bmatrix} > 0.$$

Thus $W_j(\mathcal{C}^\perp) = 0$ for $1 \leq j \leq k-d+1$, i.e., $d_{\mathrm{rk}}(\mathcal{C}^\perp) \geq k-d+2$. On the other hand, Theorem 1.14 gives $\dim(\mathcal{C}^\perp) = m(d-1) \leq m(k - d_{\mathrm{rk}}(\mathcal{C}^\perp) + 1)$, i.e., $d_{\mathrm{rk}}(\mathcal{C}^\perp) \leq k-d+2$. It follows $d_{\mathrm{rk}}(\mathcal{C}^\perp) = k-d+2$, and so $\mathcal{C}^\perp$ is MRD. □

Corollary 5.20 was first proved in [20] by Delsarte using the theory of designs and codesigns in association schemes. Theorem 5.13 allows us to give a short proof for the same result in the case of linear codes. Notice also that, by Theorem 5.5, Corollary 5.20 generalizes the analogous result for Gabidulin codes established in [32] (Theorem 1.28 of Chapter 1).

5.3 Minimum distance and maximum rank

In this section we define and study an invariant of a Delsarte code $\mathcal{C}$ which we call "maximum rank". In particular, we prove some bounds that relate the minimum distance and the maximum rank of a code. As an application, we give a recursive formula for the rank distribution of an MRD Delsarte code.

Definition 5.21. Let $\mathcal{C} \subseteq \mathrm{Mat}$ be a Delsarte code. The **maximum rank** of $\mathcal{C}$ is the integer $\mathrm{maxrk}(\mathcal{C}) := \max\{\mathrm{rk}(M) : M \in \mathcal{C}\}$.

Proposition 5.22. Let $\mathcal{C} \subseteq \mathrm{Mat}$ be a Delsarte code. We have

$$\dim(\mathcal{C}) \leq m \cdot \mathrm{maxrk}(\mathcal{C}).$$

Moreover, for any choice of $0 \leq D \leq k$ there exists a code $\mathcal{C} \subseteq \mathrm{Mat}$ with maximum rank equal to D and attaining the upper bound.

Proof. Fix $0 \leq D \leq k$. The set of all $k \times m$ matrices having the last $k-D$ rows equal to zero is an example of a code of maximum rank D and dimension mD over $\mathbb{F}_q$. Now we prove the first part of the statement. Let $\mathcal{C} \subseteq \mathrm{Mat}$ be a code with $\mathrm{maxrk}(\mathcal{C}) = D$. If $D = k$ then the bound is trivial. Hence we assume $D \leq k-1$. Theorem 1.14 gives a code $\mathcal{D} \subseteq \mathrm{Mat}$ with $d_{\mathrm{rk}}(\mathcal{D}) = D+1$ and $\dim(\mathcal{D}) = m(k-D)$. We clearly have $\mathcal{C} \cap \mathcal{D} = \{0\}$ and $\mathcal{C} \oplus \mathcal{D} \subseteq \mathrm{Mat}$. Hence $\dim(\mathcal{C}) \leq km - \dim(\mathcal{D}) = mD$. □

The following proposition relates the minimum distance of a Delsarte code to the maximum rank of the dual code.

Proposition 5.23. Let $\mathcal{C} \subseteq \mathrm{Mat}$ be a non-zero Delsarte code. We have

$$d_{\mathrm{rk}}(\mathcal{C}) \leq \mathrm{maxrk}(\mathcal{C}^\perp) + 1.$$

Proof. Applying Theorem 1.14 to $\mathcal{C}$ we obtain $\dim(\mathcal{C}) \leq m(k - d_{\mathrm{rk}}(\mathcal{C}) + 1)$, while Proposition 5.22 applied to $\mathcal{C}^\perp$ gives $\dim(\mathcal{C}^\perp) \leq m \cdot \mathrm{maxrk}(\mathcal{C}^\perp)$, i.e., $\dim(\mathcal{C}) \geq m(k - \mathrm{maxrk}(\mathcal{C}^\perp))$. Hence we have

$$m(k - \mathrm{maxrk}(\mathcal{C}^\perp)) \leq \dim(\mathcal{C}) \leq m(k - d_{\mathrm{rk}}(\mathcal{C}) + 1),$$

and the result follows. □

The minimum distance of a Delsarte code relates to the minimum distance of the dual code as in the following result.

Proposition 5.24. Let $\mathcal{C} \subsetneq \mathrm{Mat}$ be a non-zero Delsarte code. We have

$$d_{\mathrm{rk}}(\mathcal{C}^\perp) \leq k - d_{\mathrm{rk}}(\mathcal{C}) + 2.$$

Moreover, the bound is attained if and only if $\mathcal{C}$ is MRD.

Proof. Theorem 1.14 applied to the code $\mathcal{C}$ gives $\dim(\mathcal{C}) \leq m(k - d_{\mathrm{rk}}(\mathcal{C}) + 1)$. The same theorem applied to $\mathcal{C}^\perp$ gives $\dim(\mathcal{C}^\perp) \leq m(k - d_{\mathrm{rk}}(\mathcal{C}^\perp) + 1)$, i.e., $\dim(\mathcal{C}) \geq m(d_{\mathrm{rk}}(\mathcal{C}^\perp) - 1)$. Hence we have

$$m(d_{\mathrm{rk}}(\mathcal{C}^\perp) - 1) \leq \dim(\mathcal{C}) \leq m(k - d_{\mathrm{rk}}(\mathcal{C}) + 1). \tag{5.4}$$

In particular, $d_{\mathrm{rk}}(\mathcal{C}^\perp) - 1 \leq k - d_{\mathrm{rk}}(\mathcal{C}) + 1$, and the bound follows. Let us prove the second part of the statement. Assume that $\mathcal{C}$ is MRD, and let $d := d_{\mathrm{rk}}(\mathcal{C})$. We have $\dim(\mathcal{C}) = m(k - d + 1)$, and so $\dim(\mathcal{C}^\perp) = m(d-1)$. By Corollary 5.20, $\mathcal{C}^\perp$ is also MRD, and so $m(d-1) = m(k - d_{\mathrm{rk}}(\mathcal{C}^\perp) + 1)$. It follows $d_{\mathrm{rk}}(\mathcal{C}^\perp) = k - d + 2$. On the other hand, if $d_{\mathrm{rk}}(\mathcal{C}^\perp) = k - d_{\mathrm{rk}}(\mathcal{C}) + 2$ then both the inequalities in (5.4) are equalities, and so $\mathcal{C}$ is MRD. □

Corollary 5.25. The rank distribution of a non-zero MRD Delsarte code $\mathcal{C} \subseteq \mathrm{Mat}$ only depends on k, m and $d_{\mathrm{rk}}(\mathcal{C})$.

Proof. Let $d := d_{\mathrm{rk}}(\mathcal{C})$. By Proposition 5.24, $\mathcal{C}^\perp$ has minimum rank $k - d + 2$. Hence the equations of Theorem 5.13 for $0 \leq \nu \leq k - d$ reduce to

$$\begin{bmatrix} k \\ \nu \end{bmatrix} + \sum_{i=d}^{k-\nu} W_i(\mathcal{C}) \begin{bmatrix} k-i \\ \nu \end{bmatrix} = \frac{|\mathcal{C}|}{q^{m\nu}} \begin{bmatrix} k \\ \nu \end{bmatrix}, \qquad 0 \leq \nu \leq k - d.$$

These identities give a linear system of $k-d+1$ equations in the $k-d+1$ unknowns $W_d(\mathcal{C}), ..., W_k(\mathcal{C})$. The matrix associated to the system is triangular with all 1's on the diagonal. In particular, the solution to the system is unique. Hence $W_d(\mathcal{C}), ..., W_k(\mathcal{C})$ are uniquely determined by k, m and d. Since $W_0(\mathcal{C}) = 1$ and $W_i(\mathcal{C}) = 0$ for $0 < i < d$ and for $i > k$, the corollary follows. □

Remark 5.26. Using the same argument as in Corollary 5.14 it is easy to derive a recursive formula for the rank distribution of a non-zero MRD Delsarte code $\mathcal{C} \subseteq \mathrm{Mat}$ of given minimum distance d:

$$\begin{cases} W_0(\mathcal{C}) = 1, \quad W_d(\mathcal{C}) = (q^m - 1) \begin{bmatrix} k \\ k-d \end{bmatrix}, \\ W_{d+\ell}(\mathcal{C}) = (q^{m(1+\ell)} - 1) \begin{bmatrix} k \\ k-d-\ell \end{bmatrix} - \sum_{i=d}^{d+\ell-1} W_i(\mathcal{C}) \begin{bmatrix} k-i \\ k-d-\ell \end{bmatrix} \qquad \text{for } 1 \leq \ell \leq k-d. \end{cases}$$

We omit the details of the proof.

5.4 Optimal anticodes

In this section we define and study Delsarte optimal anticodes in the rank-metric. In particular, we provide a new characterization of optimal anticodes in terms of their intersection with MRD codes. As an application of such a description, we prove that the dual of an optimal anticode is an optimal anticode.

Definition 5.27. A Delsarte code $\mathcal{C} \subseteq \text{Mat}$ that attains the upper bound of Proposition 5.22 is called a (**Delsarte**) **optimal anticode**.

We start with a preliminary lemma whose proof uses linearized polynomials (see Definition 1.30 for details).

Lemma 5.28. Let $\mathcal{C} \subseteq \text{Mat}$ be a non-zero MRD Delsarte code with minimum distance d. Then $W_{d+\ell}(\mathcal{C}) > 0$ for all $0 \leq \ell \leq k-d$.

Proof. By Corollary 5.25, we shall prove the lemma for a given MRD Delsarte code $\mathcal{C} \subseteq \text{Mat}$ of our choice with minimum distance d. We will first produce a convenient MRD code with the prescribed parameters.

Let $C \subseteq \mathbb{F}_{q^m}^k$ be the Gabidulin code constructed in the proof of Theorem 1.29, with evaluation set $E = \{\beta_1, ..., \beta_k\}$ and evaluation map ev_E. Let $\mathcal{G}$ be any basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. By Proposition 1.25, $\mathcal{C} := \mathcal{C}_{\mathcal{G}}(C) \subseteq \text{Mat}$ is a Delsarte code with $\dim(\mathcal{C}) = m(k-d+1)$ and the same rank distribution as C. In particular, $\mathcal{C}$ is a non-zero MRD code with minimum rank d.

Now we prove the lemma for the MRD code $\mathcal{C}$ defined above. Fix $0 \leq \ell \leq k-d$. Define $t := k-d-\ell$, and let $U \subseteq \mathbb{F}_{q^m}$ be the $\mathbb{F}_q$-subspace generated by $\{\beta_1, ..., \beta_t\}$. If $t = 0$ we set U to be the zero space. By [63], Theorem 3.52,

$$p_U := \prod_{\gamma \in U} (x - \gamma)$$

is a linearized polynomial over $\mathbb{F}_{q^m}$ of degree $t = k-d-\ell \leq k-d$, i.e., $p_U \in \text{Lin}_q(n, k-d)$. By Proposition 1.25 it suffices to prove that $\text{ev}_E(p_U) = (p_U(\beta_1), ..., p_U(\beta_k))$ has rank $d+\ell = k-t$. Clearly, $V(p_U) = U$. In particular we have $\text{ev}_E(p_U) = (0, ..., 0, p_U(\beta_{t+1}), ..., p_U(\beta_k))$. We will prove that $p_U(\beta_{t+1}), ..., p_U(\beta_k)$ are linearly independent over $\mathbb{F}_q$. Assume that there exist $a_{t+1}, ..., a_k \in \mathbb{F}_q$ such that $\sum_{i=t+1}^k a_i p_U(\beta_i) = 0$. Then we have $p_U\left(\sum_{i=t+1}^k a_i \beta_i\right) = 0$, i.e., $\sum_{i=t+1}^k a_i \beta_i \in V(p_U) = U$. It follows that there exist $a_1, ..., a_t \in \mathbb{F}_q$ such that $\sum_{i=1}^t a_i \beta_i = \sum_{i=t+1}^k a_i \beta_i$, i.e., $\sum_{i=1}^t a_i \beta_i - \sum_{i=t+1}^k a_i \beta_i = 0$. Since $\beta_1, ..., \beta_k$ are linearly independent over $\mathbb{F}_q$, we have $a_i = 0$ for all $i = 1, ..., k$. In particular $a_i = 0$ for $i = t+1, ..., k$. Hence $p_U(\beta_{t+1}), ..., p_U(\beta_k)$ are linearly independent over $\mathbb{F}_q$, as claimed. □

In the following result we give a necessary and sufficient condition for a Delsarte code $\mathcal{C} \subseteq \text{Mat}$ with $\dim(\mathcal{C}) \equiv 0 \mod m$ to be an optimal anticode.

Proposition 5.29. Let $0 \leq D \leq k-1$ be an integer, and let $\mathcal{C} \subseteq \text{Mat}$ be an $\mathbb{F}_q$-subspace with $\dim(\mathcal{C}) = m \cdot D$. The following are equivalent.

1. $\mathcal{C}$ is a Delsarte optimal anticode.
2. $\mathcal{C} \cap \mathcal{D} = \{0\}$ for all non-zero MRD codes $\mathcal{D} \subseteq \text{Mat}$ with $d_{\text{rk}}(\mathcal{D}) = D+1$.

Proof. If $\mathcal{C}$ is an optimal anticode, then by Definition 5.27 we have $D = \text{maxrk}(\mathcal{C})$. Hence if $\mathcal{D}$ is any non-zero code with $d_{\text{rk}}(\mathcal{D}) = D+1$ we clearly have $\mathcal{C} \cap \mathcal{D} = \{0\}$. So (1) $\Rightarrow$ (2) is trivial. Let us prove (2) $\Rightarrow$ (1). By contradiction, assume that $\mathcal{C}$ is not an optimal anticode. Since $\text{maxrk}(\mathcal{C}) \geq D$ (see Proposition 5.22), we must have $s := \text{maxrk}(\mathcal{C}) \geq D+1$. Let $N \in \mathcal{C}$ with $\text{rk}(N) = s$. Let $\mathcal{D}'$ be a non-zero MRD code with $d_{\text{rk}}(\mathcal{D}') = D+1$ (see Theorem 1.14 for the existence of such a code). By Lemma 5.28 there exists $A \in \mathcal{D}'$ with $\text{rk}(A) = s$. There exist invertible matrices P and Q of size $k \times k$ and $m \times m$ (respectively) such that $N = PAQ$. Define $\mathcal{D} := P\mathcal{D}'Q := \{PMQ : M \in \mathcal{D}'\}$. Then $\mathcal{D} \subseteq \text{Mat}(k \times m, \mathbb{F}_q)$ is a non-zero MRD code with $d_{\text{rk}}(\mathcal{D}) = D+1$ and such that $N \in \mathcal{C} \cap \mathcal{D}$. Since $\text{rk}(N) = s \geq D+1 \geq 1$, N cannot be the zero matrix. This contradicts the hypothesis. □

The following result may be regarded as the analogue of Corollary 5.20 for rank-metric anticodes.

Theorem 5.30. If $\mathcal{C}$ is an optimal anticode, then $\mathcal{C}^\perp$ is also an optimal anticode.

Proof. Let $\mathcal{C} \subseteq \text{Mat}$ be an optimal anticode with $D := \text{maxrk}(\mathcal{C})$. If $D = k$ then the result is trivial. Hence from now on we assume $0 \leq D \leq k-1$. By Definition 5.27 we have $\dim(\mathcal{C}) = mD$, and so $\dim(\mathcal{C}^\perp) = m(k-D)$. By Proposition 5.29 it suffices to prove that $\mathcal{C}^\perp \cap \mathcal{D} = \{0\}$ for all non-zero MRD codes $\mathcal{D} \subseteq \text{Mat}(k \times m, \mathbb{F}_q)$ with $d_{\text{rk}}(\mathcal{D}) = k - D + 1$. If $\mathcal{D}$ is such an MRD code, then we have $\dim(\mathcal{D}) = m(k-(k-D+1)+1) = mD < mk$. Hence, by Proposition 5.24, $\mathcal{D}^\perp$ is an MRD code with $d_{\text{rk}}(\mathcal{D}^\perp) = k-(k-D+1)+2 = D+1$. Proposition 5.29 gives $\mathcal{C} \cap \mathcal{D}^\perp = \{0\}$. Since $\dim(\mathcal{C}) + \dim(\mathcal{D}^\perp) = mD + m(k-(D+1)+1) = mk$, it follows $\mathcal{C} \oplus \mathcal{D}^\perp = \text{Mat}$. Hence by Lemma 1.17 we have $\mathcal{C}^\perp \cap \mathcal{D} = \{0\}$, as claimed. □

We close this section with a bound that relates the maximum rank of a Delsarte code $\mathcal{C}$ to the maximum rank of the dual code $\mathcal{C}^\perp$.

Proposition 5.31. Let $\mathcal{C} \subseteq \text{Mat}$ be a Delsarte code. We have

$$\text{maxrk}(\mathcal{C}) \geq k - \text{maxrk}(\mathcal{C}^\perp).$$

Moreover, the bound is attained if and only if $\mathcal{C}$ is an optimal anticode.

Proof. Proposition 5.22 applied to $\mathcal{C}^\perp$ gives $\dim(\mathcal{C}^\perp) \leq m \cdot \text{maxrk}(\mathcal{C}^\perp)$, which is equivalent to $\dim(\mathcal{C}) \geq m(k - \text{maxrk}(\mathcal{C}^\perp))$. The same proposition applied to $\mathcal{C}$ gives $\dim(\mathcal{C}) \leq m \cdot \text{maxrk}(\mathcal{C})$. Hence we have

$$m(k - \text{maxrk}(\mathcal{C}^\perp)) \leq \dim(\mathcal{C}) \leq m \cdot \text{maxrk}(\mathcal{C}). \tag{5.5}$$

In particular, $k - \text{maxrk}(\mathcal{C}^\perp) \leq \text{maxrk}(\mathcal{C})$. Given the inequalities in (5.5), it is easy to see that the bound is attained if and only if both $\mathcal{C}$ and $\mathcal{C}^\perp$ are optimal anticodes, which occurs precisely when $\mathcal{C}$ is an optimal anticode by Theorem 5.30. □

5.5 Enumerative problems of matrices

In this section we present an application of a coding theory result to enumerative combinatorics. More in detail, we show how one can employ the MacWilliams identities for the rank distance discussed in the previous sections to answer some enumerative questions regarding matrices over finite fields.

The first enumerative technique that we describe is based on the following observation. If $f : \text{Mat} \to \mathbb{F}_q$ is a non-zero $\mathbb{F}_q$-linear function, then $\ker(f)^\perp$ is a linear code generated by one

matrix. Any two generating matrices have the same rank, say R_f. As a consequence, the rank distribution of the linear code $\mathcal{C} := \ker(f)^\perp$ is

$$W_i(\mathcal{C}) = \begin{cases} 1 & \text{if } i = 0 \\ q-1 & \text{if } i = R_f \\ 0 & \text{otherwise.} \end{cases}$$

Therefore applying Corollary 5.15 to $\mathcal{C} := \ker(f)^\perp$ one can explicitly compute the number of matrices of rank j in $\ker(f) = \mathcal{C}^\perp$ for all $0 \leq j \leq k$. More precisely, the following hold.

Corollary 5.32. Let $f : \mathrm{Mat} \to \mathbb{F}_q$ be a non-zero linear map, and let R_f be the rank of any matrix that generates $\ker(f)^\perp$. For all $0 \leq j \leq k$ the number of rank j matrices in $\ker(f)$ is

$$\frac{1}{q} \sum_{s=0}^{k} (-1)^{j-s} \, q^{ms+\binom{j-s}{2}} \begin{bmatrix} k-s \\ k-j \end{bmatrix} \left(\begin{bmatrix} k \\ s \end{bmatrix} + (q-1) \begin{bmatrix} k-R_f \\ s \end{bmatrix} \right).$$

Example 5.33. Let $f : \mathrm{Mat} \to \mathbb{F}_q$ be the linear map that sends a matrix to the sum of its entries. The orthogonal of $\ker(f)$ is generated by the matrix whose entries are all ones. The rank of such matrix is clearly one. Therefore for all $0 \leq j \leq k$ the number of rank j matrices over $\mathbb{F}_q$ of size $k \times m$ whose entries sum to zero is

$$\frac{1}{q} \sum_{s=0}^{k} (-1)^{j-s} \, q^{ms+\binom{j-s}{2}} \begin{bmatrix} k-s \\ k-j \end{bmatrix} \left(\begin{bmatrix} k \\ s \end{bmatrix} + (q-1) \begin{bmatrix} k-1 \\ s \end{bmatrix} \right).$$

It is now easy to extend Example 5.33 and obtain the following general result.

Corollary 5.34. Let $I \subseteq [k] \times [m]$ be a non-zero set of indices. For all $0 \leq j \leq k$ the number of $k \times m$ rank j matrices M over $\mathbb{F}_q$ such that $\sum_{(s,t)\in I} M_{st} = 0$ is

$$\frac{1}{q} \sum_{s=0}^{k} (-1)^{j-s} \, q^{ms+\binom{j-s}{2}} \begin{bmatrix} k-s \\ k-j \end{bmatrix} \left(\begin{bmatrix} k \\ s \end{bmatrix} + (q-1) \begin{bmatrix} k-\mathrm{rk}(M(I)) \\ s \end{bmatrix} \right),$$

where $M(I)$ denotes the $k \times m$ matrix defined, for all $(s,t) \in [k] \times [m]$, by $M(I)_{st} := 1$ if $(s,t) \in I$, and $M(I)_{st} := 0$ otherwise.

Corollary 5.34 generalizes the formulas of [3] and [8] for the number of matrices with given rank and h-trace over $\mathbb{F}_q$.

The computation of the number of matrices over $\mathbb{F}_q$ with given size, rank and zero entries in a prescribed region is an active research area in combinatorics and combinatorial statistics (see e.g. [46], [52], [61], [88] and the references within). It turns out that some instances of this type of problems can be investigated using MacWilliams identities for the rank metric, as we now show.

Extending the notation introduced in Chapter 4, given any subset $I \subseteq [k] \times [m]$ we define $\mathbb{F}_q[I] := \{M \in \mathrm{Mat} : M_{st} = 0 \text{ for all } (s,t) \notin I\}$. Clearly, $\mathbb{F}_q[I]$ is an $\mathbb{F}_q$-subspace of Mat of dimension $|I|$. The complement of a set $I \subseteq [k] \times [m]$ is denoted by I^c in the sequel.

Remark 5.35. One can easily check that for any subset $I \subseteq [k] \times [m]$ we have $\mathbb{F}_q[I]^\perp = \mathbb{F}_q[I^c]$. Therefore, by Corollary 5.15, the rank distributions of $\mathbb{F}_q[I]$ and $\mathbb{F}_q[I^c]$ determine each other.

For certain simple sets I the rank distribution of $\mathbb{F}_q[I]$ can be explicitly computed. In these cases Corollary 5.15 gives a formula for the number of matrices in Mat of any given rank and zero entries on I.

Corollary 5.36. Let $1 \leq k' \leq k$ and $1 \leq m' \leq m$ be integers. For all $0 \leq j \leq k$ the number of $k \times m$ rank j matrices M over $\mathbb{F}_q$ such that $M_{st} = 0$ for all $(s,t) \in \{1,...,k'\} \times \{1,...,m'\}$ is

$$q^{-k'm'} \sum_{i=0}^{\min\{k',m'\}} \begin{bmatrix} m' \\ i \end{bmatrix} \prod_{u=0}^{i-1}(q^{k'} - q^u) \sum_{s=0}^{k}(-1)^{j-s}\, q^{ms+\binom{j-s}{2}} \begin{bmatrix} k-s \\ k-j \end{bmatrix} \begin{bmatrix} k-i \\ s \end{bmatrix}.$$

Proof. Let $I := [k'] \times [m']$. The code $\mathcal{C} := \mathbb{F}_q[I]$ is the set of matrices whose entries are contained in the rectangular region described by I. As a consequence, for all $0 \leq i \leq \min\{k', m'\}$, the integer $W_i(\mathcal{C})$ is the number of $k' \times m'$ matrices over $\mathbb{F}_q$ with rank i, i.e,

$$W_i(\mathcal{C}) = \begin{bmatrix} m' \\ i \end{bmatrix} \prod_{u=0}^{i-1}(q^{k'} - q^u) \quad \text{for } 0 \leq i \leq \min\{k', m'\}$$

(the previous formula is well-known). For $\min\{k', m'\} < i \leq k'$ we have $W_i(\mathcal{C}) = 0$. Therefore the corollary easily follows from Remark 5.35 and Corollary 5.15. □

Again concerning matrices with prescribed zero entries, a question of R. Stanley asks for the number of invertible matrices over $\mathbb{F}_q$ having zero diagonal entries (see e.g. the Introduction of [61]). The question was answered in Proposition 2.2 of [61], where the authors provide a formula for the number of $k \times m$ full-rank matrices over $\mathbb{F}_q$ with zero diagonal entries. Notice that for diagonal entries of a rectangular matrix M we mean the entries of the form M_{ss} for $1 \leq s \leq k$. The following corollary extends Proposition 2.2 of [61], and computes the number of rectangular matrices over $\mathbb{F}_q$ of given size, rank, and having zeros in prescribed diagonal entries.

Corollary 5.37. Let $I \subseteq \{(s,t) \in [k] \times [m] : s = t\}$ be a set of diagonal entries. For all $0 \leq j \leq k$ the number of $k \times m$ matrices M over $\mathbb{F}_q$ having rank j and $M_{st} = 0$ for all $(s,t) \in I$ is

$$q^{-|I|} \sum_{i=0}^{|I|} \binom{|I|}{i} (q-1)^i \sum_{s=0}^{k}(-1)^{j-s}\, q^{ms+\binom{j-s}{2}} \begin{bmatrix} k-s \\ k-j \end{bmatrix} \begin{bmatrix} k-i \\ s \end{bmatrix}.$$

Proof. Define $\mathcal{C} := \mathbb{F}_q[I]$. It is easy to see that for $|I| < i \leq k$ we have $W_i(\mathcal{C}) = 0$, and for $0 \leq i \leq |I|$ we have

$$W_i(\mathcal{C}) = \binom{|I|}{i}(q-1)^i.$$

Thus the formula follows from Remark 5.35 and Corollary 5.15. □

Chapter 6

Generalized rank-weights

In this chapter we define and study algebraic invariants for Delsarte codes, which we call "Delsarte generalized weights". Our definition extends certain algebraic invariants defined on the sub-class of Gabidulin codes by other authors. We first establish the main properties of Delsarte generalized weights, and then show how they relate to the duality theory of Delsarte codes, which we investigated in Chapter 5.

Linear codes endowed with the Hamming metric can be employed in so-called "wiretap channels" to secure a communication against an eavesdropper (see e.g. [75]). In [91], Wei proved that in this context the performance of a code is measured by certain parameters of the code called "generalized Hamming weights". From a mathematical viewpoint, generalized Hamming weights can be viewed as algebraic invariants of a linear code that generalize the notion of minimum distance. A remarkable property is that the generalized Hamming weights of a linear code completely determine the generalized Hamming weights of the dual code.

Recently, Silva and Kschischang proposed a scheme based on Gabidulin rank-metric codes to secure a communication against an eavesdropper over a network in a universal way (see [85] for details). An important feature of the scheme is that it is compatible with linear network coding. Generalized rank weights were introduced later by Kurihara, Matsumoto and Uyematsu in [57] to measure the performance of a Gabidulin code when employed in the scheme of [85]. The generalized rank weights of a Gabidulin code are defined in terms of the intersections of the code with certain linear spaces usually called "Frobenius-closed spaces" in algebra. Generalized rank weights also have interesting mathematical properties, including a duality theory (see in particular [57] and [25]).

Since in Chapter 5 we showed that Delsarte codes generalize Gabidulin codes, from a mathematical viewpoint a very natural problem is to extend the definition of generalized rank weights from Gabidulin to Delsarte codes. It is not clear however how to generalize such definition in a convenient way, i.e., producing a well-behaving algebraic invariant. This is the main problem, more of mathematical flavor, that we address in this chapter.

In Section 6.2 and 6.3 we start investigating optimal anticodes in the Hamming and in the rank metric, and show that both the generalized Hamming weights and the generalized rank weights of a code can be characterized in terms of the intersection of the code with optimal anticodes in the respective metrics. In order to establish this characterization for the generalized rank weights of Gabidulin codes, we show in particular that Frobenius-closed spaces in $\mathbb{F}_{q^m}^k$ coincide with optimal

anticodes in the rank metric. The result says that the algebraic condition of being Frobenius-closed may be regarded as a metric condition. We also give a convenient method to compute a basis defined over $\mathbb{F}_q$ of a Frobenius-closed space $V \subseteq \mathbb{F}_{q^m}^k$.

Inspired by the characterizations illustrated above, in Section 6.4 we propose a definition of generalized weights for Delsarte rank-metric codes based on optimal anticodes in the linear space of $k \times m$ matrices over $\mathbb{F}_q$. Then we prove that Delsarte generalized weights extend, as an algebraic invariant, the notion of generalized rank weights for Gabidulin codes.

In Section 6.5 we then establish several properties of Delsarte generalized weights, which may be regarded as the analogue for Delsarte codes of the classical properties of generalized Hamming and rank weights. In particular, we show that Delsarte optimal codes and anticodes are characterized by their Delsarte generalized weights.

In Section 6.6 we show that our definition of Delsarte generalized weights behaves well with respect to the duality theory of Delsarte codes that we studied in Chapter 5. More precisely, we prove that the Delsarte generalized weights of a code determine the Delsarte generalized weights of the dual code.

Finally, in Section 6.7 we show that the generalized rank weights proposed by Kurihara, Matsumoto and Uyematsu in [57] measure the worst-case security drops of a Gabidulin code employed in the scheme of [85].

The results contained in this chapter have been published in [78].

Notation 6.1. Throughout this chapter, q denotes a prime power, and $\mathbb{F}_q$ the finite field with q elements. We also work with fixed positive integers n, k and m with $k \leq m$ without loss of generality. If M is a matrix over a field $\mathbb{F}$ we denote by $\mathrm{rowsp}(M)$ the space generated over $\mathbb{F}$ by the rows of M. If we work with a field extension $\mathbb{K} \supseteq \mathbb{F}$, to avoid ambiguity we may also write $\mathrm{rowsp}_{\mathbb{K}}(M)$ for the vector space generated over $\mathbb{K}$ by the rows of M.

6.1 Preliminaries on generalized weights

In this section we briefly recall some basic notions of coding theory. In particular, we give the definition of generalized weights for the Hamming and the rank metric.

We define the **maximum Hamming weight** of a classical code $C \subseteq \mathbb{F}_q^n$ is $\mathrm{maxwt}(C) := \max\{\mathrm{wt}(c) : c \in C\}$.

Definition 6.2. The **support** of an $\mathbb{F}_q$-subspace $D \subseteq \mathbb{F}_q^n$ is defined by

$$\chi(D) := \{i \in [n] : \exists\ d \in D \text{ with } d_i \neq 0\}.$$

Given a linear t-dimensional classical non-zero code $C \subseteq \mathbb{F}_q^n$ and an integer $1 \leq r \leq t$, the **r-th generalized Hamming weight** of C is

$$d_r(C) := \min\{|\chi(D)| : D \subseteq C,\ \dim_{\mathbb{F}_q}(D) = r\}.$$

In [91] Wei proved that generalized Hamming weights describe the performance of a linear classical code employed in the coding scheme for wiretap channels proposed in [75]. The main algebraic properties of generalized Hamming weights are summarized in the following result.

Theorem 6.3 (see [91])**.** Let $C \subseteq \mathbb{F}_q^n$ be a non-zero linear classical code of dimension $1 \leq t \leq n$ over $\mathbb{F}_q$. The following hold.

1. $d_1(C) = d_{\mathrm{H}}(C)$.
2. $d_t(C) \leq n$.
3. For any $1 \leq r \leq t-1$ we have $d_r(C) < d_{r+1}(C)$.
4. For any $1 \leq r \leq t$ we have $d_r(C) \leq n - t + r$.

We now recall the definition of generalized rank weights for Gabidulin codes. Given any vector $v = (v_1, ..., v_k) \in \mathbb{F}_{q^m}^k$, let $v^q := (v_1^q, ..., v_k^q)$.

Definition 6.4. A subspace $V \subseteq \mathbb{F}_{q^m}^k$ is **Frobenius-closed** if $v^q \in V$ whenever $v \in V$. We denote by $\Lambda_q(k, m)$ the set of Frobenius-closed spaces $V \subseteq \mathbb{F}_{q^m}^k$.

Definition 6.5. Let $C \subseteq \mathbb{F}_{q^m}^k$ be a t-dimensional non-zero Gabidulin code, and let $1 \leq r \leq t$ be an integer. The r**-th generalized rank weight** of C is

$$m_r(C) := \min\{\dim_{\mathbb{F}_{q^m}}(V) : V \in \Lambda_q(k, m),\ \dim_{\mathbb{F}_{q^m}}(V \cap C) \geq r\}.$$

In [85] Silva and Kschischang propose a coding scheme to secure a network communication against an eavesdropper based on Gabidulin codes. Generalized rank weights were introduced in [57] to measure the performance of a Gabidulin code when employed in the cited scheme. The following theorem summarizes the main properties of generalized rank weights.

Theorem 6.6 (see [57] and [25])**.** Let $C \subseteq \mathbb{F}_{q^m}^k$ be a non-zero Gabidulin code of dimension $1 \leq t \leq k$ over $\mathbb{F}_{q^m}$. The following hold.

1. $m_1(C) = d_{\mathrm{G}}(C)$.
2. $m_t(C) \leq k$.
3. For any $1 \leq r \leq t-1$ we have $m_r(C) < m_{r+1}(C)$.
4. For any $1 \leq r \leq t$ we have $m_r(C) \leq k - t + r$.

6.2 Generalized Hamming weights and anticodes

In this section we characterize the generalized Hamming weights of a linear classical code in terms of the intersections of the code with optimal anticodes in the Hamming metric.

If $C \subseteq \mathbb{F}_q^n$ is any non-zero linear classical code, then the sum of the rows of $\mathrm{RRE}(C)$ is a vector of Hamming weight at least $\dim(C)$. This shows the following bound.

Proposition 6.7. Let $C \subseteq \mathbb{F}_q^n$ be a linear classical code. We have $\dim_{\mathbb{F}_q}(C) \leq \mathrm{maxwt}(C)$.

Definition 6.8. A classical code $C \subseteq \mathbb{F}_q^n$ attaining the bound of Proposition 6.7 is an **optimal linear anticode** for the Hamming metric. We denote the set of optimal linear Hamming anticodes in $\mathbb{F}_q^n$ by $\mathcal{A}_q^H(n)$.

One can construct simple optimal linear anticodes as follows. Let $S \subseteq [n]$ be any subset. The **free code** over $\mathbb{F}_q$ of length n **supported** on S is $C_q(n, S) := \{v \in \mathbb{F}_q^n : v_i = 0 \text{ for all } i \in [n] \setminus S\}$.

Clearly, any free code $C_q(n,S)$ has $\dim_{\mathbb{F}_q}(C_q(n,S)) = \mathrm{maxwt}(C_q(n,S)) = |S|$. Thus free codes are optimal linear anticodes. Vice versa, we now show that for $q \geq 3$ all optimal linear anticodes are free codes.

Lemma 6.9. Assume $q \geq 3$. Let $t \geq 1$ be an integer, and let $c_1, ..., c_t \in \mathbb{F}_q$ be not all zero. There exist $a_1, ..., a_t \in \mathbb{F}_q \setminus \{0\}$ such that $\sum_{i=1}^t a_i c_i \neq 0$.

Proof. Choose $b_1, ..., b_t \in \mathbb{F}_q \setminus \{0\}$. If $\sum_{i=1}^t b_i c_i \neq 0$ then take $a_i = b_i$ for $i \in [t]$. Assume $\sum_{i=1}^t b_i c_i = 0$. By hypothesis, there exists $j \in [t]$ such that $c_j \neq 0$. Let $b \in \mathbb{F}_q \setminus \{0,1\}$. Define $a_j := bb_j$, and $a_i := b_i$ for $i \in [t] \setminus \{j\}$. Since $b \neq 0$ we have $a_i \neq 0$ for all $i \in [t]$. Moreover,

$$\sum_{i=1}^t a_i c_i = bb_j c_j + \sum_{i \neq j} b_i c_i = b_j c_j + (b-1)b_j c_j + \sum_{i \neq j} b_i c_i = \sum_{i=1}^t b_i c_i + (b-1)b_j c_j = (b-1)b_j c_j.$$

Since $b \neq 1$, $b_j \neq 0$ and $c_j \neq 0$ we have $(b-1)b_j c_j \neq 0$. □

Proposition 6.10. Assume $q \geq 3$. Let $C \subseteq \mathbb{F}_q^n$ be a linear classical code of dimension t. Then $C \in \mathcal{A}_q^H(n)$ if and only if $C = C_q(n,S)$ for some $S \subseteq [n]$ with $|S| = t$.

Proof. The implication ($\Leftarrow$) is clear. Let us prove ($\Rightarrow$). If $t = 0$ or $t = n$ then the result is trivial. Assume $0 < t < n$. If C is an optimal anticode we have $t = \mathrm{maxwt}(C)$. Let $M := \mathrm{RRE}(C)$. We will show that any non-pivot column of M is zero. By contradiction, let $j \in [n]$ be the index of a non-zero non-pivot column of M, and let $c_1^j, ..., c_t^j$ be the entries of such column. By Lemma 6.9 there exist $a_1, ..., a_t \in \mathbb{F}_q \setminus \{0\}$ with $\sum_{i=1}^t a_i c_i^j \neq 0$. Denote by $M_1, ..., M_t \in \mathbb{F}_q^n$ the rows of M. We have that $\sum_{i=1}^t a_i M_i \in C$ has Hamming weight at least $t+1$, a contradiction. It follows $c_i^j = 0$ for all $i \in [t]$. Hence we proved $C \subseteq C_q(n,S)$, where $S \subseteq [n]$ is the set of pivot columns of M. In particular, $|S| = t$, and so $C = C_q(n,S)$. □

Proposition 6.10 allows us to characterize the generalized Hamming weights of a linear classical code in terms of optimal anticodes as follows.

Theorem 6.11. Assume $q \geq 3$. Let $C \subseteq \mathbb{F}_q^n$ be a non-zero linear classical code of dimension $1 \leq t \leq n$. For any integer $1 \leq r \leq t$ we have $d_r(C) = \min\{\dim_{\mathbb{F}_q}(A) : A \in \mathcal{A}_q^H(n),\ \dim_{\mathbb{F}_q}(A \cap C) \geq r\}$.

Proof. Fix $1 \leq r \leq t$. Define $d'_r(C) := \min\{\dim_{\mathbb{F}_q}(A) : A \in \mathcal{A}_q^H(n),\ \dim_{\mathbb{F}_q}(A \cap C) \geq r\}$. Let $A \in \mathcal{A}_q^H(n)$ with $\dim_{\mathbb{F}_q}(A) = d'_r(C)$ and $\dim_{\mathbb{F}_q}(A \cap C) \geq r$. By Proposition 6.10, $A = C_q(n,S)$ for some $S \subseteq [n]$ with $|S| = \dim_{\mathbb{F}_q}(A)$. Let D be an r-dimensional subspace of $A \cap C$. We have $\chi(D) \subseteq \chi(A \cap C) \subseteq \chi(A) = \chi(C_q(n,S)) = S$, and so $|\chi(D)| \leq |S| = \dim_{\mathbb{F}_q}(A)$. This proves $d_r(C) \leq d'_r(C)$. Let now $D \subseteq C$ with $\dim_{\mathbb{F}_q}(D) = r$ and $|\chi(D)| = d_r(C)$. Define $A := C_q(n, \chi(D))$. Since $A \supseteq D$ and $D \subseteq C$, we have $\dim_{\mathbb{F}_q}(A \cap C) \geq \dim_{\mathbb{F}_q}(D \cap C) = \dim_{\mathbb{F}_q}(D) = r$. Moreover, $\dim_{\mathbb{F}_q}(A) = |\chi(D)| = d_r(C)$, and so $d'_r(C) \leq d_r(C)$. □

Notice that Theorem 6.11 and Proposition 6.10 do not hold in general when $q = 2$, as we show in the following example.

Example 6.12. Take $n = 3$, and let C be the linear code generated over $\mathbb{F}_2$ by $(1,0,1)$ and $(0,1,1)$. We have $d_2(C) = |\chi(C)| = 3$. On the other hand, C is an optimal linear anticode of maximum weight 2, even if it is not of the form $C_2(3,S)$ for some $S \subseteq [n]$ with $|S| = 2$. Following the notation of the proof of Theorem 6.11 we have $d'_2(C) = \dim_{\mathbb{F}_q}(C) = 2 \neq d_2(C)$.

6.3 Generalized rank weights and anticodes

In this section we establish the analogue of Theorem 6.11 for Gabidulin codes and generalized rank weights. We start with a bound on the dimension of optimal anticodes in the rank metric.

Definition 6.13. In analogy with Section 5.3, the **maximum rank** of a Gabidulin code C is defined by $\text{maxrk}(C) := \max\{\text{rk}(c) : c \in C\}$.

Proposition 6.14. Let $C \subseteq \mathbb{F}_{q^m}^k$ be a Gabidulin code. We have $\dim_{\mathbb{F}_{q^m}}(C) \leq \text{maxrk}(C)$.

Proof. If $C = 0$ the result is trivial. Assume $t := \dim_{\mathbb{F}_{q^m}}(C) \geq 1$ and let $M_1, ..., M_t$ denote the rows of $M := \text{RRE}(C) \in \text{Mat}_{t\times k}(\mathbb{F}_{q^m})$. Let $\alpha_1, ..., \alpha_t \in \mathbb{F}_{q^m}$ be independent over $\mathbb{F}_q$. Then $\sum_{i=1}^t \alpha_i M_i \in C$ has $\alpha_1, ..., \alpha_t$ among its components. In particular, $\text{rk}(\sum_{i=1}^t \alpha_i M_i) \geq t$. □

Definition 6.15. A code $C \subseteq \mathbb{F}_{q^m}^k$ attaining the bound of Proposition 6.14 is an **optimal Gabidulin anticode**. We denote the set of optimal Gabidulin anticodes in $\mathbb{F}_{q^m}^k$ by $\mathcal{A}_q^G(k, m)$.

We now present a series of preliminary results relating Frobenius-closed spaces, matrices in reduced row echelon form, and optimal anticodes.

Theorem 6.16 ([35], Theorem 1)**.** Let $V \subseteq \mathbb{F}_{q^m}^k$ be an $\mathbb{F}_{q^m}$-subspace. Then $V \in \Lambda_q(k, m)$ if and only if V has a basis made of vectors with entries in $\mathbb{F}_q$ (in short, **defined** over $\mathbb{F}_q$).

Combining Theorem 6.16 with the uniqueness of the reduced row echelon form we obtain the following criterion to test if a space is Frobenius-closed. The result also provides an efficient way to compute a basis defined over $\mathbb{F}_q$ of a Frobenius-closed space $V \subseteq \mathbb{F}_{q^m}^k$.

Corollary 6.17. Let $V \subseteq \mathbb{F}_{q^m}^k$ be a non-zero subspace. Then $V \in \Lambda_q(k, m)$ if and only if $\text{RRE}(V)$ is a matrix with entries in $\mathbb{F}_q$.

Example 6.18. Let $q = 2$ and $k = m = 4$. Write $\mathbb{F}_{2^4} = \mathbb{F}_2[\xi]$, where ξ satisfies $\xi^4 + \xi + 1 = 0$. Let $V \subseteq \mathbb{F}_{2^4}^4$ be the space generated by the vectors $v_1 := (\xi, \xi^2, \xi^5, \xi)$ and $v_2 := (\xi^2, \xi^4, \xi^{10}, \xi^2)$, and let M denote the matrix having v_1 and v_2 as rows. The reduced row echelon form of M is

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}.$$

Therefore V is Frobenius-closed, and $\{(1, 0, 1, 1), (0, 1, 1, 0)\}$ is a basis of V defined over $\mathbb{F}_2$.

We will need the following preliminary lemma.

Lemma 6.19. Let $H \subseteq \mathbb{F}_{q^m}$ be an $\mathbb{F}_q$-subspace of dimension h over $\mathbb{F}_q$, with $1 \leq h \leq m - 2$. Let $x \in \mathbb{F}_{q^m} \setminus H$, and $y \in \mathbb{F}_{q^m}$. There exists $\alpha \in \mathbb{F}_{q^m} \setminus H$ such that $x + \alpha y \notin H \oplus \langle\alpha\rangle$, where $\langle\alpha\rangle \subseteq \mathbb{F}_{q^m}$ denotes the space generated by α over $\mathbb{F}_q$.

Proof. Define the sets $U := \{a \in \mathbb{F}_q : a \neq y\}$ and $\mathcal{U} := \{\alpha \in \mathbb{F}_{q^m} : \exists\ v \in H,\ a \in U \text{ with } \alpha = (v - x)/(y - a)\}$. We claim that $x + \alpha y \in H \oplus \langle\alpha\rangle$ if and only if $\alpha \in \mathcal{U}$. Indeed, if $\alpha \in \mathcal{U}$ then $\alpha = (v - x)/(y - a)$ for some $v \in H$ and $a \in U \subseteq \mathbb{F}_q$. Hence $\alpha(y - a) = v - x$, and so $x + \alpha y = v + a\alpha \in H \oplus \langle\alpha\rangle$. Vice versa, if $x + \alpha y \in H \oplus \langle\alpha\rangle$ then there exist $v \in H$ and $a \in \mathbb{F}_q$ with $x + \alpha y = v + a\alpha$. If $a = y$ then $x = v \in H$, a contradiction. It follows $a \in U$, and $\alpha = (v - x)/(y - a) \in \mathcal{U}$, as claimed.

Now we conclude the proof. Since $|\mathcal{U}| \leq |H| \cdot |U| \leq q^h q = q^{h+1}$, we have $|\mathbb{F}_{q^m} \setminus \mathcal{U}| \geq q^m - q^{h+1}$. Since $m - h \geq 2$ by hypothesis, we have $q^{m-h} - q \geq q^2 - q > 1$. Multiplying both members of this inequality by q^h we obtain $q^m - q^{h+1} > q^h$. Hence we have $|\mathbb{F}_{q^m} \setminus \mathcal{U}| \geq q^m - q^{h+1} > q^h$. Since $|H| = q^h$, there exists $\alpha \in (\mathbb{F}_{q^m} \setminus \mathcal{U}) \setminus H$. Since $\alpha \notin \mathcal{U}$ we have $x + \alpha y \notin H \oplus \langle \alpha \rangle$ by the claim. □

Proposition 6.20. Let $1 \leq t < k$ be an integer, and let $M \in \mathrm{Mat}_{t \times k}(\mathbb{F}_{q^m})$ be a full-rank matrix in reduced row echelon form with rows $M_1, ..., M_t$. If M has at least one entry in $\mathbb{F}_{q^m} \setminus \mathbb{F}_q$, then there exist $\mathbb{F}_q$-linearly independent elements $\alpha_1, ..., \alpha_t \in \mathbb{F}_{q^m}$ such that $\mathrm{rk}(\sum_{i=1}^t \alpha_i M_i) \geq t + 1$.

Proof. Without loss of generality we may prove the result only for matrices M whose first row has at least one entry in $\mathbb{F}_{q^m} \setminus \mathbb{F}_q$. We proceed by induction on t. If $t = 1$ then M has only one row, $M_1 \in \mathbb{F}_{q^m}^k$. Such row has 1 and an element $M_{1j} \notin \mathbb{F}_q$ among its entries. In particular, it has rank ≥ 2, and we can take $\alpha_1 := 1$ to conclude the proof. Assume that the result holds for all non-negative integers smaller than t. Denote by $M' \in \mathrm{Mat}_{t-1 \times k}(\mathbb{F}_{q^m})$ the matrix obtained from M deleting the last row. Clearly, M' has full-rank and it is in reduced row echelon form. By induction hypothesis there are $\alpha_1, ..., \alpha_{t-1} \in \mathbb{F}_{q^m}$ independent over $\mathbb{F}_q$ with $\mathrm{rk}(\sum_{i=1}^{t-1} \alpha_i M_i) \geq t$. Since the vector $\sum_{i=1}^{t-1} \alpha_i M_i$ has $\alpha_1, ..., \alpha_{t-1}$ among its components, there exists $j \in [k]$ with $\sum_{i=1}^{t-1} \alpha_i M_{ij} \notin \langle \alpha_1, ..., \alpha_{t-1} \rangle$. Lemma 6.19 with $H = \langle \alpha_1, ..., \alpha_{t-1} \rangle$, $x = \sum_{i=1}^{t-1} \alpha_i M_{ij}$, $y = M_{tj}$ gives an element $\alpha_t \in \mathbb{F}_{q^m} \setminus \langle \alpha_1, ..., \alpha_{t-1} \rangle$ with $\sum_{i=1}^{t-1} \alpha_i M_{ij} + \alpha_t M_{tj} = \sum_{i=1}^{t} \alpha_i M_{ij} \notin \langle \alpha_1, ..., \alpha_t \rangle$. Thus $\sum_{i=1}^t \alpha_i M_i$ has rank $\geq t + 1$. □

The following theorem shows that Frobenius-closed spaces coincide with optimal Gabidulin anticodes. In particular, it shows that the algebraic condition of being Frobenius-closed may be regarded as a metric condition.

Theorem 6.21. We have $\Lambda_q(k, m) = \mathcal{A}_q^G(k, m)$.

Proof. Let $V \in \Lambda_q(k, m)$. Denote by t the dimension of V over $\mathbb{F}_{q^m}$. If $t = 0$ then clearly $V \in \mathcal{A}_q^G(k, m)$. Now assume $1 \leq t \leq k$. By Theorem 6.16 there exists a basis $\{v_1, ..., v_t\}$ of V defined over $\mathbb{F}_q$. Take any $v \in V$. There exist $\alpha_1, ..., \alpha_t \in \mathbb{F}_{q^m}$ with $v = \sum_{i=1}^t \alpha_i v_i$. The space generated over $\mathbb{F}_q$ by the entries of v is contained in $\mathrm{Span}_{\mathbb{F}_q}\{\alpha_1, ..., \alpha_t\}$. In particular $\mathrm{rk}(v) \leq t$. Since $v \in V$ is arbitrary, this proves $\mathrm{maxrk}(V) \leq t$. By Proposition 6.14 we have $\mathrm{maxrk}(V) = t = \dim_{\mathbb{F}_{q^m}}(V)$, and so $V \in \mathcal{A}_q^G(k, m)$. Now we prove $\mathcal{A}_q^G(k, m) \subseteq \Lambda_q(k, m)$. Let $A \in \mathcal{A}_q^G(k, m)$, and denote by t the dimension of A over $\mathbb{F}_{q^m}$. If $t = 0$ or $t = k$ then $A \in \Lambda_q(k, m)$. Assume $1 \leq t < k$, and set $M := \mathrm{RRE}(A)$. By Corollary 6.17 it suffices to show that M has entries in $\mathbb{F}_q$. By contradiction, assume that M has one entry, say M_{ij}, in $\mathbb{F}_{q^m} \setminus \mathbb{F}_q$. Exchanging the first and the i-th row of M we obtain a matrix, say N, in reduced row echelon form such that $\mathrm{rowsp}_{\mathbb{F}_{q^m}}(N) = \mathrm{rowsp}_{\mathbb{F}_{q^m}}(M) = A$. By Proposition 6.20 there exists $v \in \mathrm{rowsp}_{\mathbb{F}_{q^m}}(N) = A$ with $\mathrm{rk}(v) \geq t + 1$, and this contradicts the fact that A is an optimal anticode of dimension t. □

We can now state the main result of this section, characterizing generalized rank weights in terms of optimal Gabidulin anticodes. The result follows from Definition 6.5 and Theorem 6.21, and it may be regarded as the analogue of Theorem 6.11 for Gabidulin codes.

Corollary 6.22. Let $C \subseteq \mathbb{F}_{q^m}^n$ be a non-zero Gabidulin code of dimension $1 \leq t \leq k$ over $\mathbb{F}_{q^m}$. For all $1 \leq r \leq t$ we have $m_r(C) = \min\{\dim_{\mathbb{F}_{q^m}}(A) : A \in \mathcal{A}_q^G(k, m),\ \dim_{\mathbb{F}_{q^m}}(A \cap C) \geq r\}$.

6.4 An algebraic invariant for Delsarte codes

Recall from Definition 5.27 that a **Delsarte optimal anticode** is an $\mathbb{F}_q$-subspace $\mathcal{A} \subseteq \mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ such that $\dim_{\mathbb{F}_q}(\mathcal{A}) = m \cdot \mathrm{maxrk}(\mathcal{A})$, where $\mathrm{maxrk}(\mathcal{A}) := \max\{\mathrm{rk}(M) : M \in \mathcal{C}\}$.

Notation 6.23. In the sequel we work with fixed integers k and m with $1 \leq k \leq m$, and we denote $\mathrm{Mat}_{k\times m}(\mathbb{F}_q)$ simply by Mat.

Inspired by Theorem 6.11 and Corollary 6.22, we propose the following definition.

Definition 6.24. Let $\mathcal{C} \subseteq \mathrm{Mat}$ be a non-zero Delsarte code of dimension $1 \leq t \leq km$. For $1 \leq r \leq t$, the r**-th Delsarte generalized weight** of $\mathcal{C}$ is

$$a_r(\mathcal{C}) := \frac{1}{m}\min\{\dim_{\mathbb{F}_q}(\mathcal{A}) : \mathcal{A} \in \mathcal{A}_q^D(k,m),\ \dim_{\mathbb{F}_q}(\mathcal{A}\cap\mathcal{C}) \geq r\}.$$

By Definition 5.27, the dimension over $\mathbb{F}_q$ of any anticode $A \in \mathcal{A}_q^D(k,m)$ is a multiple of m. Thus Delsarte generalized weights are positive integers.

Before describing some general properties of Delsarte generalized weights we show how our invariant relates to the generalized rank weights for Gabidulin codes of [57]. Since Delsarte codes generalize Gabidulin codes (as shown in Chapter 5), one would expect that Delsarte generalized weights extend, as an invariant, generalized rank weights. This is what we show in the remainder of this section. We start introducing some rank-preserving transformations.

Notation 6.25. Given a Gabidulin code $C \subseteq \mathbb{F}_{q^m}^k$, a Delsarte code $\mathcal{C} \subseteq \mathrm{Mat}$, and matrices $A \in \mathrm{Mat}_{k\times k}(\mathbb{F}_q)$, $B \in \mathrm{Mat}_{m\times m}(\mathbb{F}_q)$, define:

$$CA := \{cA : c \in C\}, \quad A\mathcal{C} := \{AM : M \in \mathcal{C}\}, \quad \mathcal{C}B := \{MB : M \in \mathcal{C}\}.$$

It is easy to see that if A and B are invertible matrices, then the multiplication maps above are rank-preserving isomorphisms of Gabidulin and Delsarte codes. In particular, they preserve optimal anticodes in the respective metrics, generalized rank weights, and Delsarte generalized weights. When $k = m$ we also define the **transpose** of a Delsarte code $\mathcal{C} \subseteq \mathrm{Mat}_{k\times k}(\mathbb{F}_q)$ by $\mathcal{C}^t := \{M^t : M \in \mathcal{C}\} \subseteq \mathrm{Mat}_{k\times k}(\mathbb{F}_q)$. It is easy to check that $\mathcal{C}$ and $\mathcal{C}^t$ have the same Delsarte generalized weights.

One can construct a simple family of Delsarte optimal anticodes as follows. Let $0 \leq R \leq k$ be an integer. The **standard optimal anticode** $\mathcal{S}_q(k,m,R)$ of maximum rank R is the vector space of $k \times m$ matrices over $\mathbb{F}_q$ whose last $k-R$ rows equal zero. The following result shows that, up to the rank-preserving transformations introduced in Notation 6.25, all Delsarte optimal anticodes are standard optimal anticodes.

Theorem 6.26 ([81], Theorem 4 and Theorem 6)**.** Let $1 \leq R \leq k \leq m$ be integers, and let $\mathcal{A} \in \mathcal{A}_q^D(k,m)$ with $\mathrm{maxrk}(\mathcal{A}) = R$. The following hold.

1. If $k < m$ then there exist invertible matrices $A \in \mathrm{Mat}_{k\times k}(\mathbb{F}_q)$, $B \in \mathrm{Mat}_{m\times m}(\mathbb{F}_q)$ such that $A\mathcal{A}B = \mathcal{S}_q(k,m,R)$.
2. If $k = m$ then there exist invertible matrices $A, B \in \mathrm{Mat}_{k\times k}(\mathbb{F}_q)$ such that either $A\mathcal{A}B = \mathcal{S}_q(k,k,R)$, or $A\mathcal{A}B = \mathcal{S}_q(k,k,R)^t$.

Proof. If $R = 0$ or $R = k$ then the result is trivial. Assume $1 \leq R \leq k-1$. If $k < m$ the result follows (up to a transposition) from [81], Theorem 6(a). If $k = m$ and $R > 1$ then apply [81], Theorem 4(a). Finally, if $k = m$ and $R = 1$ the result follows from [81], Theorem 4(b). □

We will also need the following linear algebra result, whose proof is standard and left to the reader.

Lemma 6.27. Let $C \subseteq \mathbb{F}_{q^m}^k$ be a Gabidulin code. The following hold.

1. If $A \in \mathrm{Mat}_{k\times k}(\mathbb{F}_q)$ is an invertible matrix, then for any basis $\mathcal{G}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ we have $\mathcal{C}_{\mathcal{G}}(CA^t) = A\mathcal{C}_{\mathcal{G}}(C)$. In particular, $\mathcal{C}_{\mathcal{G}}(C)$ and $\mathcal{C}_{\mathcal{G}}(CA^t)$ have the same Delsarte generalized weights.
2. Let $\mathcal{G} = \{\gamma_1, ..., \gamma_m\}$, $\mathcal{F} := \{\varphi_1, ..., \varphi_m\}$ be bases of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and let $B \in \mathrm{Mat}_{m\times m}(\mathbb{F}_q)$ denote the invertible matrix defined by $\gamma_j = \sum_{s=1}^m B_{js}\varphi_s$ for all $j \in [m]$. We have $\mathcal{C}_{\mathcal{F}}(C) = \mathcal{C}_{\mathcal{G}}(C)B$. In particular, if $C \neq 0$ then the Delsarte generalized weights of $\mathcal{C}_{\mathcal{G}}(C)$ do not depend on the choice of the basis $\mathcal{G}$.
3. Let $D \subseteq \mathbb{F}_{q^m}^k$ be another Gabidulin code, and let $\mathcal{G}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. We have $\mathcal{C}_{\mathcal{G}}(C \cap D) = \mathcal{C}_{\mathcal{G}}(C) \cap \mathcal{C}_{\mathcal{G}}(D)$.

We can now prove that Delsarte generalized weights extend, as an algebraic invariant, generalized rank weights.

Theorem 6.28. Let $C \subseteq \mathbb{F}_{q^m}^k$ be a non-zero Gabidulin code of dimension $1 \leq t \leq k$. For any basis $\mathcal{G}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and for any integers $1 \leq r \leq t$ and $0 \leq \varepsilon \leq m-1$ we have

$$m_r(C) = a_{rm-\varepsilon}(\mathcal{C}_{\mathcal{G}}(C)).$$

In particular, the Delsarte generalized weights of a Delsarte $\mathcal{C}$ code arising from a Gabidulin code are fully determined by a suitable subset of them.

Proof. Fix $1 \leq r \leq t$ and $0 \leq \varepsilon \leq m-1$. Let $\overline{A} \in \mathcal{A}_q^G(k,m)$ with $\dim_{\mathbb{F}_{q^m}}(\overline{A}) = m_r(C)$ and $\dim_{\mathbb{F}_{q^m}}(\overline{A} \cap C) \geq r$. We have $\mathcal{C}_{\mathcal{G}}(\overline{A}) \in \mathcal{A}_q^D(k,m)$ and $\dim_{\mathbb{F}_q}(\mathcal{C}_{\mathcal{G}}(\overline{A})) = m \cdot \dim_{\mathbb{F}_{q^m}}(\overline{A}) = m \cdot m_r(C)$. By Lemma 6.27(3), $\mathcal{C}_{\mathcal{G}}(\overline{A}) \cap \mathcal{C}_{\mathcal{G}}(C) = \mathcal{C}_{\mathcal{G}}(\overline{A} \cap C)$. Hence we have

$$\dim_{\mathbb{F}_q}(\mathcal{C}_{\mathcal{G}}(\overline{A}) \cap \mathcal{C}_{\mathcal{G}}(C)) = \dim_{\mathbb{F}_q}(\mathcal{C}_{\mathcal{G}}(\overline{A} \cap C)) \geq rm \geq rm - \varepsilon.$$

It follows $a_{rm-\varepsilon}(\mathcal{C}_{\mathcal{G}}(C)) \leq m_r(C)$.

Now we prove $m_r(C) \leq a_{rm-\varepsilon}(\mathcal{C}_{\mathcal{G}}(C))$. Define $\mathcal{C} := \mathcal{C}_{\mathcal{G}}(C)$ to simplify the notation. Let $\overline{\mathcal{A}} \in \mathcal{A}_q^D(k,m)$ with $\dim_{\mathbb{F}_q}(\overline{\mathcal{A}} \cap \mathcal{C}) \geq rm - \varepsilon$ and $a_{rm-\varepsilon}(\mathcal{C}) = 1/m \cdot \dim_{\mathbb{F}_q}(\overline{\mathcal{A}})$. By Definition 5.27, $\dim_{\mathbb{F}_q}(\overline{\mathcal{A}}) = mR$, where $R = \mathrm{maxrk}(\overline{\mathcal{A}})$. Hence we need to prove $m_r(C) \leq R$. By Theorem 6.26 there exist invertible matrices $A \in \mathrm{Mat}_{k\times k}(\mathbb{F}_q)$ and $B \in \mathrm{Mat}_{m\times m}(\mathbb{F}_q)$ such that either $A\overline{\mathcal{A}}B = \mathcal{S}_q(k,m,R)$, or $k = m$ and $A\overline{\mathcal{A}}B = \mathcal{S}_q(k,k,R)^t$. By Remark 6.25 (replacing if necessary $\mathcal{C}$ with $\mathcal{C}^\perp$, $\overline{\mathcal{A}}$ with $\overline{\mathcal{A}}^\perp$, A with B^t and B with A^t) without loss of generality we may assume to be in the former case. Let $\mathcal{G} = \{\gamma_1, ..., \gamma_m\}$, and for $i \in [m]$ define $\varphi_i := \sum_{j=1}^m B_{ij}^{-1}\gamma_j$. It is clear that $\mathcal{F} := \{\varphi_1, ..., \varphi_m\}$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Define the optimal Gabidulin anticode $V := \{v \in \mathbb{F}_{q^m}^k : v_i = 0 \text{ for } i > R\} \subseteq \mathbb{F}_{q^m}^k$. Using Definition 4.51 one can check that $\mathcal{C}_{\mathcal{F}}(V) = \mathcal{S}_q(k,m,R) = A\overline{\mathcal{A}}B$. Since V is an optimal Gabidulin anticode of dimension R over $\mathbb{F}_{q^m}$, by Remark 6.25 $V(A^t)^{-1}$ is an optimal Gabidulin anticode of dimension R as well. Therefore by Corollary 6.22 it suffices to prove

$\dim_{\mathbb{F}_{q^m}}(V(A^t)^{-1} \cap C) \geq r$. By Lemma 6.27(3) we have

$$\begin{aligned}\dim_{\mathbb{F}_{q^m}}(V(A^t)^{-1} \cap C) &= \dim_{\mathbb{F}_{q^m}}(V(A^t)^{-1}A^t \cap CA^t) \\ &= \dim_{\mathbb{F}_{q^m}}(V \cap CA^t) \\ &= \frac{1}{m}\dim_{\mathbb{F}_q}(\mathcal{C}_{\mathcal{F}}(V \cap CA^t)) \\ &= \frac{1}{m}\dim_{\mathbb{F}_q}(\mathcal{C}_{\mathcal{F}}(V) \cap \mathcal{C}_{\mathcal{F}}(CA^t)).\end{aligned}$$

By Lemma 6.27, parts 1 and 2, we have $\mathcal{C}_{\mathcal{F}}(CA^t) = A\mathcal{C}_{\mathcal{F}}(C) = A\mathcal{C}_{\mathcal{G}}(C)B = A\mathcal{C}B$. It follows

$$\mathcal{C}_{\mathcal{F}}(V) \cap \mathcal{C}_{\mathcal{F}}(CA^t) = A\overline{\mathcal{A}}B \cap A\mathcal{C}B = A(\overline{\mathcal{A}} \cap \mathcal{C})B.$$

Since $\dim_{\mathbb{F}_q}(A(\overline{\mathcal{A}} \cap \mathcal{C})B) = \dim_{\mathbb{F}_q}(\overline{\mathcal{A}} \cap \mathcal{C})$, we have

$$\frac{1}{m}\dim_{\mathbb{F}_q}(\mathcal{C}_{\mathcal{F}}(V) \cap \mathcal{C}_{\mathcal{F}}(CA^t)) = \frac{1}{m}\dim_{\mathbb{F}_q}(\overline{\mathcal{A}} \cap \mathcal{C}) \geq \frac{1}{m}(rm - \varepsilon).$$

It follows $\dim_{\mathbb{F}_{q^m}}(V(A^t)^{-1} \cap C) \geq \lceil (rm-\varepsilon)/m \rceil = r$, as claimed. □

Remark 6.29. It is not true in general that for a Delsarte code $\mathcal{C} \subseteq \mathrm{Mat}$ of dimension t we have $a_{im}(\mathcal{C}) = a_{im-\varepsilon}(\mathcal{C})$ for all $i \geq 1$ and $1 \leq \varepsilon \leq m-1$ with $1 \leq im - \varepsilon \leq t$. For example, one can produce codes $\mathcal{C} \subseteq \mathrm{Mat}_{3\times 3}(\mathbb{F}_2)$ of dimension 6 having the Delsarte generalized weights given in Table 6.1. The examples reflect the fact that not all Delsarte codes $\mathcal{C}$ arise from a Gabidulin code, even when $\dim_{\mathbb{F}_q}(\mathcal{C}) \equiv 0 \mod m$.

	$a_1(\mathcal{C})$	$a_2(\mathcal{C})$	$a_3(\mathcal{C})$	$a_4(\mathcal{C})$	$a_5(\mathcal{C})$	$a_6(\mathcal{C})$
Code #1	1	1	1	2	2	3
Code #2	1	1	2	2	2	3
Code #3	1	1	1	2	3	3
Code #4	1	1	2	2	3	3
Code #5	1	1	2	3	3	3
Code #6	1	2	2	2	3	3

Table 6.1: Delsarte generalized weights of six different codes. Each line corresponds to a code.

6.5 Properties of Delsarte generalized weights

In this section we prove the analogue of Theorem 6.3 and Theorem 6.6 for Delsarte codes and Delsarte generalized weights, and characterize MRD Delsarte codes and optimal anticodes in terms of their generalized weights.

Lemma 6.30. Let $1 \leq k \leq m$ be integers, and let $\mathcal{A} \in \mathcal{A}_q^D(k,m)$ with $\mathrm{maxrk}(\mathcal{A}) \geq 1$. There exists $\mathcal{A}' \in \mathcal{A}_q^D(k,m)$ with $\mathcal{A}' \subseteq \mathcal{A}$ and $\dim_{\mathbb{F}_q}(\mathcal{A}') = \dim_{\mathbb{F}_q}(\mathcal{A}) - m$.

Proof. Let $R := \mathrm{maxrk}(\mathcal{A})$. By Theorem 6.26 there exist invertible matrices A and B over $\mathbb{F}_q$ of size $k \times k$ and $m \times m$ (respectively) such that either $A\mathcal{A}B = \mathcal{S}_q(k,m,R)$, or $k = m$ and $A\mathcal{A}B = \mathcal{S}_q(k,k,R)^t$. In the former case set $\mathcal{A}' := A^{-1}\mathcal{S}_q(k,m,R-1)B^{-1} \subseteq \mathcal{A}$, while in the latter case set $\mathcal{A}' := A^{-1}\mathcal{S}_q(k,k,R-1)^tB^{-1} \subseteq \mathcal{A}$. One can check that $\mathcal{A}'$ is a Delsarte code with the expected properties. □

Theorem 6.31. Let $1 \leq k \leq m$ be integers, and let $\mathcal{C} \subseteq \mathrm{Mat}$ be a non-zero Delsarte code of dimension $1 \leq t \leq km$ over $\mathbb{F}_q$. The following hold.

1. $a_1(\mathcal{C}) = d_{\mathrm{rk}}(\mathcal{C})$.
2. $a_t(\mathcal{C}) \leq k$.
3. For any $1 \leq r \leq t-1$ we have $a_r(\mathcal{C}) \leq a_{r+1}(\mathcal{C})$.
4. For any $1 \leq r \leq t-m$ we have $a_r(\mathcal{C}) < a_{r+m}(\mathcal{C})$.
5. For any $1 \leq r \leq t$ we have $a_r(\mathcal{C}) \leq k - \lfloor (t-r)/m \rfloor$.
6. For any $1 \leq r \leq t$ we have $a_r(\mathcal{C}) \geq \lceil r/m \rceil$.

Proof. We will prove the six properties separately.

1. Let $M \in \mathcal{C}$ with $d := \mathrm{rk}(M) = d_{\mathrm{rk}}(\mathcal{C}) \geq 1$. There are invertible matrices A and B over $\mathbb{F}_q$ of size $k \times k$ and $m \times m$, respectively, such that AMB is the matrix whose first d diagonal entries are ones and whose other entries equal zero. Clearly, $AMB \in \mathcal{S}_q(k,m,d)$. Set $\mathcal{A} := A^{-1}\mathcal{S}_q(k,m,d)B^{-1}$. By Notation 6.25, $\mathcal{A}$ is a Delsarte optimal anticode of dimension md such that $M \in \mathcal{C} \cap \mathcal{A}$. In particular $\dim_{\mathbb{F}_q}(\mathcal{C} \cap \mathcal{A}) \geq 1$, and so $a_1(\mathcal{C}) \leq d$. Since $\mathcal{C}$ has minimum rank d, it is clear that $a_1(\mathcal{C}) \geq d$.
2. Any anticode $\mathcal{A} \in \mathcal{A}_q^D(k,m)$ has dimension at most km.
3. Any anticode $\mathcal{A} \in \mathcal{A}_q^D(k,m)$ with $\dim_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{C}) \geq r+1$ satisfies $\dim_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{C}) \geq r$.
4. Let $\mathcal{A} \in \mathcal{A}_q^D(k,m)$ with $\dim_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{C}) \geq r+m$ and $\dim_{\mathbb{F}_q}(\mathcal{A}) = m \cdot a_{r+m}(\mathcal{C})$. By Lemma 6.30 there exists an optimal anticode $\mathcal{A}' \subseteq \mathcal{A}$ with $\dim_{\mathbb{F}_q}(\mathcal{A}') = \dim_{\mathbb{F}_q}(\mathcal{A}) - m$. It suffices to prove $\dim_{\mathbb{F}_q}(\mathcal{A}' \cap \mathcal{C}) \geq r$. Since $\mathcal{A}' \subseteq \mathcal{A}$, we have $\mathcal{A}' \cap \mathcal{C} = \mathcal{A}' \cap (\mathcal{A} \cap \mathcal{C})$. Hence $\dim_{\mathbb{F}_q}(\mathcal{A}' \cap \mathcal{C}) = \dim_{\mathbb{F}_q}(\mathcal{A}' \cap (\mathcal{A} \cap \mathcal{C})) = \dim_{\mathbb{F}_q}(\mathcal{A}') + \dim_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{C}) - \dim_{\mathbb{F}_q}(\mathcal{A}' + (\mathcal{A} \cap \mathcal{C}))$. Since $\mathcal{A}' + (\mathcal{A} \cap \mathcal{C}) \subseteq \mathcal{A}$, we have $\dim_{\mathbb{F}_q}(\mathcal{A}' + (\mathcal{A} \cap \mathcal{C})) \leq \dim_{\mathbb{F}_q}(\mathcal{A})$. As a consequence, $\dim_{\mathbb{F}_q}(\mathcal{A}' \cap \mathcal{C}) \geq \dim_{\mathbb{F}_q}(\mathcal{A}') + \dim_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{C}) - \dim_{\mathbb{F}_q}(\mathcal{A}) = \dim_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{C}) - m \geq r$.
5. Define $h := \lfloor (t-r)/m \rfloor$. By part (2) and (4) we find a strictly increasing sequence of integers $a_r(\mathcal{C}) < a_{r+m}(\mathcal{C}) < \cdots < a_{r+hm}(\mathcal{C}) \leq k$. It follows $k \geq a_r + h$, i.e., $a_r \leq k - h$.
6. If $\mathcal{A} \in \mathcal{A}_q^D(k,m)$ satisfies $\dim_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{C}) \geq r$ then, in particular, $\dim_{\mathbb{F}_q}(\mathcal{A}) \geq r$. Hence we have $a_r(\mathcal{C}) \geq r/m$, i.e., $a_r(\mathcal{C}) \geq \lceil r/m \rceil$. □

Remark 6.32. Following the notation of Theorem 6.31, if the Delsarte code $\mathcal{C}$ arises from a Gabidulin code C then we have $t \equiv 0 \mod m$. Hence, by Theorem 6.28, Theorem 6.31 generalizes Theorem 6.6 for Gabidulin codes.

Theorem 6.31 allows us to characterize MRD Delsarte codes and optimal anticodes in terms of their Delsarte generalized weights.

Corollary 6.33. Let $1 \leq R \leq k \leq m$ be integers, and let $\mathcal{C} \subseteq \mathrm{Mat}$ be a Delsarte code with $\dim_{\mathbb{F}_q}(\mathcal{C}) = mR$. The following facts are equivalent.

1. $\mathcal{C}$ is MRD,
2. $a_1(\mathcal{C}) = k - R + 1$,
3. for all $r \in [mR]$ we have $a_r(\mathcal{C}) = k - R + \lceil r/m \rceil$.

In particular, the Delsarte generalized weights of an MRD code $\mathcal{C} \subseteq \mathrm{Mat}$ only depend on k, m and $d_{\mathrm{rk}}(\mathcal{C})$.

Proof. By Definition 1.13 and Theorem 6.31, (1) and (2) are equivalent. Assume $a_1(\mathcal{C}) = k-R+1$. By Theorem 6.31, for all $r \in [mR]$ we have $a_r(\mathcal{C}) \leq k - \lfloor (mR-r)/m \rfloor = k - R + \lceil r/m \rceil$. Assume by contradiction that there exists $r \in [mR]$ with $a_r(\mathcal{C}) < k-R+\lceil r/m \rceil$. Define the non-negative integer $s := \max\{i \in \mathbb{N} : r - im \geq 1\}$. We have $1 \leq r - sm \leq m$. In particular, $s \geq (r-m)/m = r/m - 1$.

Hence $s \geq \lceil r/m \rceil - 1$. By Theorem 6.31 we have

$$\begin{aligned} k - R + 1 = a_1(\mathcal{C}) &\leq a_{1+sm}(\mathcal{C}) - s \\ &\leq a_r(\mathcal{C}) - s \\ &< k - R + \lceil r/m \rceil - s \\ &\leq k - R + \lceil r/m \rceil - \lceil r/m \rceil + 1 \\ &= k - R + 1, \end{aligned}$$

a contradiction. Hence we have $a_r(\mathcal{C}) = k - R + \lceil r/m \rceil$ for all $r \in [mR]$. This proves (2) $\Rightarrow$ (3). Finally, it is clear that (3) implies (2). □

Corollary 6.34. Let $1 \leq R \leq k \leq m$ be integers, and let $\mathcal{C} \subseteq \mathrm{Mat}$ be a Delsarte code with $\dim_{\mathbb{F}_q}(\mathcal{C}) = mR$. The following facts are equivalent.

1. $\mathcal{C}$ is a Delsarte optimal anticode,
2. $a_{mR}(\mathcal{C}) = R$,
3. for all $r \in [mR]$ we have $a_r(\mathcal{C}) = \lceil r/m \rceil$.

In particular, the Delsarte generalized weights of a Delsarte optimal anticode $\mathcal{C} \subseteq \mathrm{Mat}$ only depend on k, m and $\mathrm{maxrk}(\mathcal{C})$.

Proof. Assume that $\mathcal{C}$ is an optimal anticode. By Theorem 6.31, for all $r \in [mR]$ we have $a_r(\mathcal{C}) \geq \lceil r/m \rceil$. Let $r \in [mR]$. Since $\lceil r/m \rceil \leq \lceil mR/m \rceil = R$, by iterating the application of Lemma 6.30 we can find an optimal anticode $\mathcal{A} \subseteq \mathcal{C}$ with $\dim_{\mathbb{F}_q}(\mathcal{A}) = m\lceil r/m \rceil$. We have $\dim_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{C}) = \dim_{\mathbb{F}_q}(\mathcal{A}) = m\lceil r/m \rceil$, and so $a_r(\mathcal{C}) \leq \lceil r/m \rceil$. This proves (1) $\Rightarrow$ (3). It is clear that (3) implies (2). Let us prove (2) $\Rightarrow$ (1). Assume $a_{mR}(\mathcal{C}) = R$. By definition, there exists an optimal anticode $\mathcal{A} \in \mathcal{A}_q^D(k, m)$ such that $\dim_{\mathbb{F}_q}(\mathcal{A}) = mR$ and $\dim_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{C}) \geq mR$. Since $\dim_{\mathbb{F}_q}(\mathcal{C}) = mR$, we have $\mathcal{A} = \mathcal{C}$. In particular, $\mathcal{C} \in \mathcal{A}_q^D(k, m)$. □

6.6 Delsarte generalized weights and duality

In this section we recall the definition of Delsarte dual code, and show how the Delsarte generalized weights of a code $\mathcal{C}$ relate to the Delsarte generalized weights of the dual code $\mathcal{C}^\perp$.

Recall that if $C \subseteq \mathbb{F}_q^n$ is a linear code, then the **dual** of C is the code $C^\perp := \{v \in \mathbb{F}_q^n : \langle c, v \rangle = 0 \text{ for all } c \in C\} \subseteq \mathbb{F}_q^n$, where $\langle \cdot, \cdot \rangle$ is the standard inner product of $\mathbb{F}_q^n$. If $C \subseteq \mathbb{F}_{q^m}^k$ is a Gabidulin code, then the **dual** of C is the code $C^\perp := \{v \in \mathbb{F}_{q^m}^k : \langle c, v \rangle = 0 \text{ for all } c \in C\} \subseteq \mathbb{F}_{q^m}^k$, where $\langle \cdot, \cdot \rangle$ denotes the standard inner product of $\mathbb{F}_{q^m}^k$.

The first part of the following result was proved by Wei in [91], and the second part was proved by Ducoat in [25].

Theorem 6.35 ([91], Theorem 3, and [25])**.** The following hold.

1. Let $C \subseteq \mathbb{F}_q^n$ be a linear code of dimension $1 \leq t \leq n$ over $\mathbb{F}_q$. The generalized Hamming weights of $C^\perp$ are determined by the generalized Hamming weights of C.
2. Let $C \subseteq \mathbb{F}_{q^m}^k$ be a Gabidulin code of dimension $1 \leq t \leq k$ over $\mathbb{F}_{q^m}^k$. The generalized rank weights of $C^\perp$ are determined by the generalized rank weights of C.

In this section we prove the analogue of Theorem 6.35 for Delsarte codes and Delsarte generalized weights. The duality notion that we consider in Mat is trace-duality (see Definition 1.15 for details).

We start presenting a theorem that relates the Delsarte generalized weights of a code $\mathcal{C}$ to the Delsarte generalized weights of the dual code $\mathcal{C}^\perp$.

Theorem 6.36. Let $1 \leq k \leq m$ be integers, and let $\mathcal{C} \subseteq \mathrm{Mat}$ be a Delsarte code of dimension $1 \leq t \leq km-1$. Assume that $p, i, j \in \mathbb{Z}$ satisfy:

1. $1 \leq p + im \leq km - t$,
2. $1 \leq p + t + jm \leq t$.

Then $a_{p+im}(\mathcal{C}^\perp) \neq k + 1 - a_{p+t+jm}(\mathcal{C})$.

Proof. Define $r := p + im$ and $s := t + r - m \cdot a_r(\mathcal{C}^\perp)$. By Theorem 6.31 we have $a_r(\mathcal{C}^\perp) \geq r/m$, and so $s \leq t$. We split the proof into two parts. All dimensions are computed over $\mathbb{F}_q$.

1. Assume $p + t + jm \leq s$. Since $p + t + jm \geq 1$, we have $1 \leq p + t + jm \leq s \leq t$. Let $\mathcal{A} \in \mathcal{A}_q^D(k, m)$ with $\dim(\mathcal{A} \cap \mathcal{C}^\perp) \geq r$ and $\dim(\mathcal{A}) = m \cdot a_r(\mathcal{C}^\perp)$. By Lemma 1.17 we have
$$\begin{aligned} r \leq \dim(\mathcal{A} \cap \mathcal{C}^\perp) &= \dim(\mathcal{A}) + \dim(\mathcal{C}^\perp) - \dim(\mathcal{A} + \mathcal{C}^\perp) \\ &= m \cdot a_r(\mathcal{C}^\perp) + (km - t) - (km - \dim(\mathcal{A}^\perp \cap \mathcal{C})) \\ &= m \cdot a_r(\mathcal{C}^\perp) - t + \dim(\mathcal{A}^\perp \cap \mathcal{C}). \end{aligned}$$
This implies $s = t + r - m \cdot a_r(\mathcal{C}^\perp) \leq \dim(\mathcal{A}^\perp \cap \mathcal{C})$. Therefore by Theorem 5.30 we have $a_s(\mathcal{C}) \leq \dim(\mathcal{A}^\perp)/m = (km - \dim(\mathcal{A}))/m = (km - m \cdot a_r(\mathcal{C}^\perp))/m = k - a_r(\mathcal{C}^\perp)$, i.e., $a_r(\mathcal{C}^\perp) \leq k - a_s(\mathcal{C})$. Since $p + t + jm \leq s$, by Theorem 6.31 we have $a_s(\mathcal{C}) \geq a_{p+t+jm}(\mathcal{C})$. As a consequence, $a_r(\mathcal{C}^\perp) \leq k - a_s(\mathcal{C}) \leq k - a_{p+t+jm}(\mathcal{C}) < k + 1 - a_{p+t+jm}(\mathcal{C})$, and the result follows.
2. Now assume $p + t + jm > s$, i.e., $i - j < a_r(\mathcal{C}^\perp)$. Let $\varepsilon > 0$ with $i - j = a_r(\mathcal{C}^\perp) - \varepsilon$. By definition of r we have
$$\begin{aligned} p + t + jm &= r - im + t + jm \\ &= r - (i - j)m + t \\ &= r - (a_r(\mathcal{C}^\perp) - \varepsilon)m + t \\ &= t + r - m \cdot a_r(\mathcal{C}^\perp) + \varepsilon m \\ &= s + \varepsilon m. \end{aligned}$$
Assume by contradiction $a_r(\mathcal{C}^\perp) = k + 1 - a_{p+t+jm}(\mathcal{C})$, i.e., $a_r(\mathcal{C}^\perp) = k + 1 - a_{s+\varepsilon m}(\mathcal{C})$. Let $\mathcal{A} \in \mathcal{A}_q^D(k, m)$ with $\dim(\mathcal{A} \cap \mathcal{C}) \geq s + \varepsilon m$ and $\dim(\mathcal{A}) = m \cdot a_{s+\varepsilon m}(\mathcal{C}) = m(k + 1 - a_r(\mathcal{C}^\perp))$. By Lemma 1.17 we have
$$\begin{aligned} s + \varepsilon m &\leq \dim(\mathcal{A} \cap \mathcal{C}) \\ &= \dim(\mathcal{A}) + \dim(\mathcal{C}) - \dim(\mathcal{A} + \mathcal{C}) \\ &= m(k + 1 - a_r(\mathcal{C}^\perp)) + t - (km - \dim(\mathcal{A}^\perp \cap \mathcal{C}^\perp)) \\ &= m - m \cdot a_r(\mathcal{C}^\perp) + t + \dim(\mathcal{A}^\perp \cap \mathcal{C}^\perp). \end{aligned}$$
Since $s = t + r - m \cdot a_r(\mathcal{C}^\perp)$, the inequality above can be re-written as $\dim(\mathcal{A}^\perp \cap \mathcal{C}^\perp) \geq r + \varepsilon m - m$. By Theorem 5.30, $\mathcal{A}^\perp \in \mathcal{A}_q^D(k, m)$, and so $m \cdot a_{r+\varepsilon m-m}(\mathcal{C}^\perp) \leq \dim(\mathcal{A}^\perp)$. On the other hand, by Lemma 1.17 we have
$$\dim(\mathcal{A}^\perp) = km - \dim(\mathcal{A}) = km - m(k + 1 - a_r(\mathcal{C}^\perp)) = m(a_r(\mathcal{C}^\perp) - 1).$$

Thus $m \cdot a_{r+\varepsilon m-m}(\mathcal{C}^\perp) \leq \dim(\mathcal{A}^\perp) = m(a_r(\mathcal{C}^\perp) - 1)$, i.e., $a_{r+\varepsilon m-m}(\mathcal{C}^\perp) \leq a_r(\mathcal{C}^\perp) - 1$. Since $\varepsilon > 0$, we have $r + \varepsilon m - m \geq r$. Hence by Theorem 6.31 we have $a_r(\mathcal{C}^\perp) \leq a_{r+\varepsilon m-m}(\mathcal{C}^\perp) \leq a_r(\mathcal{C}^\perp) - 1$, a contradiction. □

Definition 6.37. Let $1 \leq k \leq m$ be integers, and let $\mathcal{C} \subseteq \mathrm{Mat}$ be a Delsarte code of dimension $1 \leq t \leq km$. For any $s \in \mathbb{Z}$, the **s-weight sets** of $\mathcal{C}$ are defined by

$$\begin{aligned} W_s(\mathcal{C}) &:= \{a_{s+im}(\mathcal{C}) : i \in \mathbb{Z},\ 1 \leq s + im \leq t\}, \\ \overline{W}_s(\mathcal{C}) &:= \{k + 1 - a_{s+im}(\mathcal{C}) : i \in \mathbb{Z},\ 1 \leq s + im \leq t\}. \end{aligned}$$

Theorem 6.36 has the following interesting consequence, which is the analogue of Theorem 6.35 for Delsarte codes.

Corollary 6.38. Let $1 \leq k \leq m$ be integers, and let $\mathcal{C} \subseteq \mathrm{Mat}$ be a Delsarte code of dimension $1 \leq t \leq km - 1$. For any integer $1 \leq p \leq m$ we have

$$W_p(\mathcal{C}^\perp) = [k] \setminus \overline{W}_{p+t}(\mathcal{C}).$$

In particular, the Delsarte generalized weights of $\mathcal{C}$ completely determine the Delsarte generalized weights of $\mathcal{C}^\perp$.

Proof. By Theorem 6.36 we have $W_p(\mathcal{C}^\perp) \cap \overline{W}_{p+t}(\mathcal{C}) = \emptyset$, and parts (1), (2) and (3) of Theorem 6.31 imply $W_p(\mathcal{C}^\perp) \cup \overline{W}_{p+t}(\mathcal{C}) \subseteq [k]$. Hence it suffices to show that $|W_p(\mathcal{C}^\perp)| + |\overline{W}_{p+t}(\mathcal{C})| = k$.

By part (4) of Theorem 6.31 the generalized weights $a_{p+im}(\mathcal{C}^\perp)$, for $i \in \mathbb{Z}$ with $1 \leq p + im \leq km - t$, are distinct. Therefore we have

$$|W_p(\mathcal{C}^\perp)| = |\{i \in \mathbb{Z} : \lceil (1-p)/m \rceil \leq i \leq \lfloor (km - t - p)/m \rfloor\}|. \tag{6.1}$$

For the same reason, the generalized weights $a_{p+t+im}(\mathcal{C})$, for $i \in \mathbb{Z}$ with $1 \leq p + t + im \leq t$, are distinct, and so

$$|\overline{W}_{p+t}(\mathcal{C})| = |\{i \in \mathbb{Z} : \lceil (1-p-t)/m \rceil \leq i \leq \lfloor -p/m \rfloor\}|. \tag{6.2}$$

Since $1 \leq p \leq m$, we have $\lceil (1-p)/m \rceil = 0$ and $\lfloor -p/m \rfloor = -1$. Thus equations (6.1) and (6.2) can be written as

$$|W_p(\mathcal{C}^\perp)| = \lfloor (km - t - p)/m \rfloor + 1, \qquad |\overline{W}_{p+t}(\mathcal{C})| = -\lceil (1-p-t)/m \rceil.$$

Therefore it suffices to show

$$\lfloor (km - t - p)/m \rfloor - \lceil (1-p-t)/m \rceil = k - 1. \tag{6.3}$$

Write $t + p = Am + B$ with $0 \leq B \leq m - 1$. If $B = 0$ then $\lfloor (km - t - p)/m \rfloor = k - A$ and $\lceil (1-p-t)/m \rceil = -A + 1$. If $0 < B \leq m - 1$ then $\lfloor (km - t - p)/m \rfloor = k - A - 1$ and $\lceil (1-p-t)/m \rceil = -A$. This shows identity (6.3).

To prove the second part of the statement, observe that by part (4) of Theorem 6.31 the generalized weights of $\mathcal{C}^\perp$ in $W_p(\mathcal{C}^\perp)$ are ordered integers. Hence by the first part of the statement they are determined by the set $\overline{W}_{t+p}(\mathcal{C})$. The result now follows from the fact that any $a_r(\mathcal{C}^\perp)$, $1 \leq r \leq km - t$, belongs to exactly one set $W_p(\mathcal{C}^\perp)$, for some $1 \leq p \leq m$. □

Remark 6.39. Corollary 6.38 gives in particular an explicit method to compute the Delsarte generalized weights of a code $\mathcal{C}^\perp$ starting from the Delsarte generalized weights of $\mathcal{C}$, as we show in the following example.

Example 6.40. Let e.g. $q = 5$ and $k = m = 3$. Let $\mathcal{C} \subseteq \mathrm{Mat}_{3\times 3}(\mathbb{F}_5)$ be the code generated over $\mathbb{F}_5$ by the two matrices

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

It is easy to check that $a_1(\mathcal{C}) = 1$ and $a_2(\mathcal{C}) = 2$. We have $\dim_{\mathbb{F}_q}(\mathcal{C}^\perp) = 9-2 = 7$. We will compute the integers

$$a_1(\mathcal{C}^\perp), \quad a_2(\mathcal{C}^\perp), \quad a_3(\mathcal{C}^\perp), \quad a_4(\mathcal{C}^\perp), \quad a_5(\mathcal{C}^\perp), \quad a_6(\mathcal{C}^\perp), \quad a_7(\mathcal{C}^\perp)$$

employing Corollary 6.38. Start with $p = 1$. We have $W_1(\mathcal{C}^\perp) = \{a_1(\mathcal{C}^\perp), a_4(\mathcal{C}^\perp), a_7(\mathcal{C}^\perp)\}$ and $\overline{W}_3(\mathcal{C}) = \emptyset$. Since $a_1(\mathcal{C}^\perp) < a_4(\mathcal{C}^\perp) < a_7(\mathcal{C}^\perp)$ and $W_1(\mathcal{C}^\perp) = [3] \setminus W_3(\mathcal{C})$, it follows $a_1(\mathcal{C}^\perp) = 1$, $a_4(\mathcal{C}^\perp) = 2$, $a_7(\mathcal{C}^\perp) = 3$. Similarly, $W_2(\mathcal{C}^\perp) = \{a_2(\mathcal{C}^\perp), a_5(\mathcal{C}^\perp)\}$ and $\overline{W}_4(\mathcal{C}) = \{3+1-a_1(\mathcal{C})\} = \{3\}$. It follows $a_2(\mathcal{C}^\perp) = 1$ and $a_5(\mathcal{C}^\perp) = 2$. Finally, $W_3(\mathcal{C}^\perp) = \{a_3(\mathcal{C}^\perp), a_6(\mathcal{C}^\perp)\}$ and $\overline{W}_5(\mathcal{C}) = \{3 + 1 - a_2(\mathcal{C})\} = \{2\}$. Hence $a_3(\mathcal{C}^\perp) = 1$ and $a_6(\mathcal{C}^\perp) = 3$. Summarizing, the Delsarte generalized weights of $\mathcal{C}^\perp$ are the integers

$$a_1(\mathcal{C}^\perp) = 1, \quad a_2(\mathcal{C}^\perp) = 1, \quad a_3(\mathcal{C}^\perp) = 1, \quad a_4(\mathcal{C}^\perp) = 2, \quad a_5(\mathcal{C}^\perp) = 2, \quad a_6(\mathcal{C}^\perp) = 3, \quad a_7(\mathcal{C}^\perp) = 3.$$

Remark 6.41. Combining Theorem 6.28 with the results of Section 5.1 one can see that Corollary 6.38 generalizes the second part of Theorem 6.35.

Remark 6.42. In [74] Oggier and Sboui propose a definition of generalized rank weights for Gabidulin codes which we now briefly describe. Let $C \subseteq \mathbb{F}_{q^m}^k$ be a non-zero Gabidulin code of dimension $1 \leq t \leq k$. Given an integer $1 \leq r \leq t$, the **r-th Oggier-Sboui generalized weight** of C is $m'_r(C) := \min\{\mathrm{maxrk}(D) : D \subseteq C,\ \dim_{\mathbb{F}_{q^m}}(D) = r\}$. Ducoat shows in [25] how the Oggier-Sboui generalized weights relate to the generalized rank weights proposed by Kurihara, Matsumoto and Uyematsu in [57].

One may also define generalized weights for Delsarte codes in analogy with the generalized weights for Gabidulin codes proposed by Oggier and Sboui as follows. Given a Delsarte code $\mathcal{C} \subseteq \mathrm{Mat}$ of dimension $1 \leq t \leq km$ and an integer $1 \leq r \leq t$, define

$$a'_r(\mathcal{C}) := \{\mathrm{maxrk}(\mathcal{D}) : \mathcal{D} \subseteq \mathcal{C},\ \dim_{\mathbb{F}_q}(\mathcal{D}) = r\}.$$

It can be proved that $a'_r(\mathcal{C}) \leq a_r(\mathcal{C})$ for all r, and that equality does not hold in general. Let e.g. $q = 2$, $k = 2$ and $m = 3$. Denote by $\mathcal{C} \subseteq \mathrm{Mat}_{2\times 3}(\mathbb{F}_2)$ the Delsarte code generated by the three $\mathbb{F}_2$-independent matrices

$$A := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad B := \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad C := \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

The 2-dimensional subcode $\mathcal{D} \subseteq \mathcal{C}$ generated by A and C has $\mathrm{maxrk}(\mathcal{D}) = 1$. Hence $a'_2(\mathcal{C}) = 1$. On the other hand, it can be checked that there is no Delsarte optimal anticode $\mathcal{A} \in \mathcal{A}_2^D(2,3)$ with $\dim_{\mathbb{F}_q}(\mathcal{A}) = 3$ and $\dim_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{C}) \geq 2$. It follows $a_2(\mathcal{C}) = 6/3 = 2 \neq a'_2(\mathcal{C})$.

Unfortunately, it is not true in general that the a'_r generalized weights of a Delsarte code determine the a'_r generalized weights of the dual code. Let e.g. $q = 2$, $k = 2$ and $m = 3$. Consider the 2-dimensional Delsarte codes $\mathcal{C}, \mathcal{D} \subseteq \mathrm{Mat}_{2\times 3}(\mathbb{F}_2)$ defined by

$$\mathcal{C} := \langle \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \rangle, \qquad \mathcal{D} := \langle \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \rangle.$$

One can check that $a'_1(\mathcal{C}) = a'_1(\mathcal{D}) = 1$ and $a'_2(\mathcal{C}) = a'_2(\mathcal{D}) = 1$. On the other hand, we have

$$a'_1(\mathcal{C}^\perp) = 1, \quad a'_2(\mathcal{C}^\perp) = 1, \quad a'_3(\mathcal{C}^\perp) = 2, \quad a'_4(\mathcal{C}^\perp) = 2,$$
$$a'_1(\mathcal{D}^\perp) = 1, \quad a'_2(\mathcal{D}^\perp) = 1, \quad a'_3(\mathcal{D}^\perp) = 1, \quad a'_4(\mathcal{D}^\perp) = 2.$$

Thus $\mathcal{C}$ and $\mathcal{D}$ have the same a'_r generalized weights, while $\mathcal{C}^\perp$ and $\mathcal{D}^\perp$ have not. Therefore we do not have an analogue of Corollary 6.38 for the a'_r generalized weights.

6.7 Generalized rank weights for Gabidulin codes and security drops

In [85] Silva and Kschischang propose a rank-metric coding scheme to secure a network communication against an eavesdropper. They also prove that when a Gabidulin code $C \subseteq \mathbb{F}_{q^m}^k$ is employed in their scheme, the information that an eavesdropper can obtain listening at $0 \leq \mu \leq k$ links of the channel is bounded by the quantity

$$\Delta_\mu(C) := \max\{\dim_{\mathbb{F}_q}(V \cap C) : V \in \Lambda_q(k,m),\ \dim_{\mathbb{F}_q}(V) = \mu\}.$$

Clearly, $\Delta_\mu(C) \geq \Delta_{\mu-1}(C)$ for any Gabidulin code C and any integer $1 \leq \mu \leq k$. In analogy with the theory of generalized Hamming weights of [91], we propose the following definition.

Definition 6.43. Let $C \subseteq \mathbb{F}_{q^m}^k$ be a Gabidulin code. An integer $1 \leq \mu \leq k$ is a **worst-case security drop** for C if $\Delta_\mu(C) > \Delta_{\mu-1}(C)$.

We close this chapter with a result that is the analogue for Gabidulin code of [91, Corollary A]. It shows that the generalized rank weights introduced by Kurihara, Matsumoto and Uyematsu in [57] measure the worst-case security drops of a Gabidulin code employed in the scheme of [85].

Theorem 6.44. Let $C \subseteq \mathbb{F}_{q^m}^k$ be a Gabidulin code of dimension $1 \leq t \leq k$ over $\mathbb{F}_q$. Fix an integer $1 \leq \mu \leq k$. The following are equivalent.

1. $\Delta_\mu(C) > \Delta_{\mu-1}(C)$, i.e., μ is a worst-case security drop for C,
2. there exists $1 \leq r \leq t$ with $m_r(C) = \mu$.

Proof. Let us prove (1) $\Rightarrow$ (2). Take $V \in \Lambda_q(k,m)$ with $\dim_{\mathbb{F}_{q^m}}(V) = \mu$ and $\dim_{\mathbb{F}_{q^m}}(V \cap C) = \Delta_\mu(C)$. We have $m_{\Delta_\mu(C)}(C) \leq \mu$. Assume by contradiction $m_{\Delta_\mu(C)}(C) < \mu$. By definition, there exists $U \in \Lambda_q(k,m)$ with $\dim_{\mathbb{F}_{q^m}}(U \cap C) \geq \Delta_\mu(C)$ and $\dim_{\mathbb{F}_{q^m}}(U) < \mu$. Clearly, we can find $H \supseteq U$ with $H \in \Lambda_q(k,m)$ and $\dim_{\mathbb{F}_{q^m}}(H) = \mu - 1$. It follows

$$\Delta_{\mu-1}(C) \geq \dim_{\mathbb{F}_{q^m}}(H \cap C) \geq \dim_{\mathbb{F}_{q^m}}(U \cap C) \geq \Delta_\mu(C),$$

a contradiction. Hence we may take $r = \Delta_\mu(C)$. Now we prove (2) $\Rightarrow$ (1). Let $1 \leq r \leq t$ with $m_r(C) = \mu$. There exists $V \in \Lambda_q(k,m)$ with $\dim_{\mathbb{F}_{q^m}}(V \cap C) \geq r$ and $\dim_{\mathbb{F}_{q^m}}(V) = \mu$. Hence $\Delta_\mu(C) \geq r$. Assume by contradiction $\Delta_\mu(C) = \Delta_{\mu-1}(C)$. Let $U \in \Lambda_q(k,m)$ with $\dim_{\mathbb{F}_{q^m}}(U) = \mu - 1$ and $\dim_{\mathbb{F}_{q^m}}(U \cap C) = \Delta_{\mu-1}(C) = \Delta_\mu(C)$. By definition, $m_{\Delta_\mu(C)}(C) \leq \mu - 1$. Moreover, since $\Delta_\mu(C) \geq r$, by Theorem 6.6 we have $m_{\Delta_\mu(C)}(C) \geq m_r(C)$. It follows $\mu = m_r(C) \leq m_{\Delta_\mu(C)}(C) \leq \mu - 1$, a contradiction. This proves $\Delta_\mu(C) > \Delta_{\mu-1}(C)$. □

Chapter 7

Codes supported on regular lattices

In this last chapter we investigate some connections between coding theory and combinatorics. More precisely, we propose a combinatorial viewpoint on the theory of MacWilliams identities in the general context of additive codes over finite abelian groups. The results presented in this chapter generalize, with different methods, some results obtained by Delsarte for rank-metric codes in [20].

Recall that in coding theory a MacWilliams-type identity expresses a linear transformation between the weight distribution of a code and the weight distribution of the dual code. As mentioned in Section 1.5, MacWilliams identities are named after Jessie MacWilliams, who first discovered relations of this type for linear codes endowed with the Hamming weight. Analogous identities were later established for several classes of codes and weight functions by different authors. In Chapter 5 we discussed in details the MacWilliams identities for rank-metric codes.

In this chapter we propose a combinatorial approach to MacWilliams identities, in the general context of additive codes over finite abelian groups. Following e.g. [10], [43] and [92], an additive code $\mathcal{C} \subseteq G$ is a subgroup of a finite abelian group G, and the dual code $\mathcal{C}^* \subseteq \hat{G}$ is defined to be its character-theoretic annihilator, i.e.,

$$\mathcal{C}^* = \{\chi : G \to \mathbb{C}^*,\ \chi \text{ group homomorphism},\ \chi(g) = 1 \text{ for all } g \in \mathcal{C}\}.$$

In this framework, code and dual code are subsets of different ambient spaces, G and $\hat{G}$, that are not isomorphic in a canonical way in general. As a consequence, the weight distributions of $\mathcal{C}$ and $\mathcal{C}^*$ refer in general to different weight functions, say ω and τ, on G and $\hat{G}$ respectively.

It is known that when ω and τ satisfy a certain property, which we call "compatibility", the ω-distribution of *any* code $\mathcal{C}$ and the τ-distribution of its dual code $\mathcal{C}^*$ determine each other via a linear transformation. The linear relations between the two weight distributions are expressed by some numbers called "Krawtchouk coefficients" (see e.g. [43]). Their existence is guaranteed by the compatibility of the weight functions, but providing an explicit formula for them is difficult in general, even for specific examples.

From the discussion above it appears that two main problems in the area of MacWilliams identities for additive codes over groups are the following: 1) construct families of weight functions that are compatible, and thus give rise to invertible MacWilliams-type identities for additive codes, and 2) provide explicit formulas for the associated Krawtchouk coefficients. In the language of group partitions (see [43] and the following Section 7.1), the two problems above read as follows:

construct families of Fourier-reflexive partitions on finite abelian groups, and explicitly compute the associated Krawtchouk matrices.

Several weight functions that are classically studied in coding theory provide examples of compatible weights, and the Krawtchouk coefficients of the corresponding MacWilliams transformation have been computed by different authors employing ad hoc methods.

Using techniques from lattice theory, in this chapter we introduce a class of weight functions on finite abelian groups that are compatible, and thus automatically yield MacWilliams-type identities for additive codes. Moreover, we study such weight functions employing combinatorial methods. More in detail, we define a regular support to be a function, say σ, over a finite abelian group G that takes values in a graded lattice $\mathcal{L}$ with certain regularity properties. A regular support naturally induces a weight on G via the rank function of $\mathcal{L}$. We then show that a regular support σ on G with values in $\mathcal{L}$ induces a regular support σ^* on the character group $\hat{G}$ with values in the dual lattice $\mathcal{L}^*$. This yields in particular a weight function on $\hat{G}$ via the rank function of $\mathcal{L}^*$. In this framework, we prove that the weight functions on G and $\hat{G}$ induced by σ and σ^*, respectively, are compatible. Moreover, we express the Krawtchouk coefficients of the corresponding MacWilliams transformation in terms of certain combinatorial invariants of the lattice $\mathcal{L}$. Other features of our approach are the following.

1. The most relevant weight functions studied in coding theory (such as the Hamming weight, the rank weight, the Lee weight on $\mathbb{Z}_4$ and the homogeneous weight on certain Frobenius rings) belong, up to equivalence, to the family of weights that we introduce. In all these cases the combinatorial invariants of the underlying lattice are very easy to determine. This allows us to compute the corresponding Krawtchouk coefficients with a simple combinatorial technique, providing new formulas for some of them, or (when the formulas are already known) giving concise proofs for quite sophisticated results. As opposed to other general approaches to MacWilliams identities available in the literature, our method (being more explicit) is "computationally effective", and allows in practice to write down many MacWilliams transformations using a unified combinatorial method.

2. Exploiting the properties of a specific support function, which we call "chain support", we show that every finite abelian group admits a Fourier-reflexive partition (see Section 7.1 for the definition).

3. Using the modularity of certain simple lattices, we show that for every finite abelian group G there exist weight functions $\omega : G \to \mathbb{N}$ and $\tau : \hat{G} \to \mathbb{N}$ which, simultaneously, (a) give rise to MacWilliams identities, (b) endow the underlying finite abelian groups with a metric space structure. Property (b) is particularly interesting for applications in coding theory.

After having studied MacWilliams identities for additive codes, we consider general subsets $\mathcal{C} \subseteq G$ equipped with the weight function ω induced by certain support functions, and establish a Singleton-like bound in this context. The set $\mathcal{C}$ is called optimal if it attains the bound. We show that if $\mathcal{C}$ is an optimal set, then the distance distribution of $\mathcal{C}$ and the weight distribution of any translate of $\mathcal{C}$ can be expressed in terms of the combinatorial invariants of a certain underlying lattice. In the context of rank-metric codes, this extends a result by Delsarte on the distance distribution of MRD codes. We also show that if $\mathcal{C} \subseteq G$ is an optimal subgroup, then the dual subgroup $\mathcal{C}^* \subseteq \hat{G}$ is optimal as well.

Finally, as an application of the regularity of the lattice of subspaces of $\mathbb{F}_q^k$, we give a concise method to enumerate symmetric and skew-symmetric matrices of given size and rank.

The structure of the chapter is as follows. In Section 7.1 we introduce codes, weight functions and partitions of groups. In Section 7.2 we briefly recall some results on finite posets, and introduce regular lattices. We define and study regular supports in Section 7.3. In Section 7.4 we show that regular supports produce compatible pairs of weights, and express the corresponding Krawtchouk coefficients in terms of certain combinatorial invariants of the underlying lattice. In Section 7.5 we apply our approach to several weight functions that are studied in coding theory. Optimal sets are studied in Section 7.6, and enumerative problems of symmetric and skew-symmetric matrices are discussed in Section 7.7.

The results contained in this chapter appear in [79].

7.1 Groups, codes, and compatible weights

Let $(G,+)$ be a group. The **character group** of G, denoted by $(\hat{G},\cdot)$, is the set of group homomorphisms $\chi : G \to \mathbb{C}^*$ endowed with point-wise multiplication, i.e., for $\chi_1, \chi_2 \in \hat{G}$,

$$(\chi_1 \cdot \chi_2)(g) := \chi_1(g)\chi_2(g), \quad \text{for all } g \in G.$$

The neutral element of $(\hat{G},\cdot)$ is the **trivial character** $\varepsilon \equiv 1$ of G. The groups G and $\hat{\hat{G}}$ are canonically isomorphic via the map $\psi : G \to \hat{\hat{G}}$ defined, for $g \in G$, by $\psi(g)(\chi) := \chi(g)$ for all $\chi \in \hat{G}$. It is well-known that when $(G,+)$ is finite and abelian the groups $(G,+)$ and $(\hat{G},\cdot)$ are isomorphic, not canonically in general. In particular, $|G| = |\hat{G}|$. Notice that for all $n \geq 1$ we have $\widehat{G^n} = \hat{G}^n$, where $(\chi_1, ..., \chi_n) \in \widehat{G^n}$ is defined, for all $(g_1, ..., g_n) \in G^n$, by

$$(\chi_1, ..., \chi_n)(g_1, ..., g_n) := \prod_{i=1}^{n} \chi_i(g_i).$$

Definition 7.1. Let G be a finite abelian group. A **code** in G is a subgroup $\mathcal{C} \subseteq G$. The **dual** of $\mathcal{C}$ is the code $\mathcal{C}^* := \{\chi \in \hat{G} : \chi(g) = 1 \text{ for all } g \in \mathcal{C}\} \subseteq \hat{G}$. We say that $\mathcal{C}$ is **trivial** if $\mathcal{C} = \{0\}$ or $\mathcal{C} = G$. The code **generated** by codes $\mathcal{C}, \mathcal{D} \subseteq G$ is the code $\mathcal{C} + \mathcal{D} := \{c + d : c \in \mathcal{C},\ d \in \mathcal{D}\} \subseteq G$.

The following remark summarizes some properties of duality. The proof is left to the reader.

Remark 7.2. Let $\mathcal{C} \subseteq G$ be a code. Then $|\mathcal{C}| \cdot |\mathcal{C}^*| = |G| = |\hat{G}|$. Moreover, identifying G and $\hat{\hat{G}}$ we have $\mathcal{C}^{**} = \mathcal{C}$. Finally, duality and sum of codes relate as follows.

1. Let $\mathcal{C}, \mathcal{D} \subseteq G$ be codes. Then $|\mathcal{C} + \mathcal{D}| = |\mathcal{C}| \cdot |\mathcal{D}| / |\mathcal{C} \cap \mathcal{D}|$.
2. Let $\mathcal{C}_1, ..., \mathcal{C}_t \subseteq G$ be codes, $t \geq 2$. We have $\bigcap_{i=1}^{t} \mathcal{C}_i^* = \left(\sum_{i=1}^{t} \mathcal{C}_i\right)^*$.

Definition 7.3. Let G be a finite abelian group. A **weight** on G is a function $\omega : G \to X$, where X is a finite non-empty set. The **ω-distribution** of a code $\mathcal{C} \subseteq G$ is the collection $\{W_a(\mathcal{C}, \omega) : a \in X\}$, where $W_a(\mathcal{C}, \omega) := |\{g \in \mathcal{C} : \omega(g) = a\}|$ for all $a \in X$.

Let $\omega : G \to X$ and $\tau : \hat{G} \to Y$ be weights. We say that (ω, τ) is a **compatible pair** if for every $g \in G$ and $b \in \tau(\hat{G})$ the complex number

$$\sum_{\substack{\chi \in \hat{G} \\ \tau(\chi) = b}} \chi(g)$$

only depends on $\omega(g)$. If this is the case, then the **Krawtchouk coefficients** associated to (ω, τ) are defined, for every $a \in \omega(G)$ and $b \in \tau(\hat{G})$, by

$$K(\omega,\tau)(a,b) := \sum_{\substack{\chi\in\hat{G}\\ \tau(\chi)=b}} \chi(g),$$

where $g \in G$ is any element with $\omega(g) = a$. When $a \notin \omega(G)$ or $b \notin \tau(\hat{G})$ we put $K(\omega, \tau)(a, b) := 0$.

Remark 7.4. Let $\omega : G \to X$, $\tau : \hat{G} \to Y$ be weights. Identifying G and $\hat{\hat{G}}$ one has $g(\chi) = \chi(g)$ for all $g \in G$ and $\chi \in \hat{G}$. Thus when (τ, ω) is a compatible pair the Krawtchouk coefficients associated to (τ, ω) are given, for every $a \in \tau(\hat{G})$ and $b \in \omega(G)$, by

$$K(\tau,\omega)(a,b) = \sum_{\substack{g\in G\\ \omega(g)=b}} \chi(g),$$

where $\chi \in \hat{G}$ is any character with $\tau(\chi) = a$. Again, if $a \notin \tau(\hat{G})$ or $b \notin \omega(G)$ then we have $K(\tau, \omega)(a, b) = 0$.

Definition 7.5. Let $\omega : G \to X$ be a weight. For all $a \in \omega(G)$ define $P_a := \{g \in G : \omega(g) = a\}$. Then

$$\mathcal{P}(\omega) := \bigsqcup_{a\in\omega(G)} P_a$$

is the **partition** of G induced by ω. We say that weight functions $\omega : G \to X$ and $\omega' : G \to X'$ are **equivalent** if $\mathcal{P}(\omega) = \mathcal{P}(\omega')$, and in this case we write $\omega \sim \omega'$.

Remark 7.6. Let $\omega : G \to X$, $\omega' : G \to X'$, $\tau : \hat{G} \to Y$ and $\tau' : \hat{G} \to Y'$ be weights with $\omega \sim \omega'$ and $\tau \sim \tau'$. There exist bijections $\pi : \omega'(G) \to \omega(G)$ and $\eta : \tau'(\hat{G}) \to \tau(\hat{G})$ such that $\omega = \pi \circ \omega'$ and $\tau = \eta \circ \tau'$. Moreover, it is easy to see that if (ω, τ) is a compatible pair, then (ω', τ') is also a compatible pair, and for all $a \in \omega'(G)$ and $b \in \tau'(\hat{G})$ one has

$$K(\omega',\tau')(a,b) = K(\omega,\tau)(\pi(a),\eta(b)).$$

Therefore the Krawtchouk coefficients associated to (ω', τ') are the same as the Krawtchouk coefficients associated to (ω, τ), up to a suitable permutation. For this reason some authors prefer to directly concentrate on group partitions when studying Krawtchouk coefficients (see e.g. [43]). In coding theory however, given a "numerical" weight function $\omega : G \to X \subseteq \mathbb{N}$, one naturally attempts to define a distance d_ω on G by setting $d_\omega(g, g') := \omega(g - g')$ for all $g, g' \in G$. It is easy to construct groups G and weights $\omega, \omega' : G \to X \subseteq \mathbb{N}$ such that $\omega \sim \omega'$, d_ω is a distance function, but $d_{\omega'}$ is not. This is the reason why in this dissertation we prefer to work with weights rather than with partitions. From the point of view of the study of Krawtchouk coefficients, the partition approach and the weight approach are equivalent.

We now show that compatible pairs of weights produce MacWilliams-type identities. We start recalling from [43] the terminology of group partitions.

Definition 7.7. Let $\mathcal{P} = \bigsqcup_{a=1}^{\ell} P_a$ be a partition of a finite abelian group G. Define an equivalence relation $\equiv$ on $\hat{G}$ by $\chi \equiv \chi'$ if and only if $\sum_{g\in P_a} \chi(g) = \sum_{g\in P_a} \chi'(g)$ for all $a \in \{1, ..., \ell\}$. The equivalence classes of $\equiv$ define a partition of $\hat{G}$ called the **dual partition** of $\mathcal{P}$, denoted by $\hat{\mathcal{P}}$. The partition $\mathcal{P}$ is called **Fourier-reflexive** if $\hat{\hat{\mathcal{P}}} = \mathcal{P}$ when identifying G and $\hat{\hat{G}}$.

We denote by $|\mathcal{P}|$ the cardinality of a partition on a finite abelian group, i.e., the number of equivalence classes induced by $\mathcal{P}$.

Theorem 7.8 (MacWilliams Identities for codes over groups)**.** Let G be a finite abelian group, and let $\omega : G \to X$ and $\tau : \hat{G} \to Y$ be weights. Assume that (ω, τ) is compatible. Then for all codes $\mathcal{C} \subseteq G$ we have

$$W_b(\mathcal{C}^*, \tau) = \frac{1}{|\mathcal{C}|} \sum_{a \in X} K(\omega, \tau)(a, b)\ W_a(\mathcal{C}, \omega).$$

for all $b \in Y$. In particular, the ω-distribution of $\mathcal{C}$ determines the τ-distribution of $\mathcal{C}^*$.

Proof. In the language of [43], we have that $\mathcal{P}(\omega)$ is finer than $\widehat{\mathcal{P}(\tau)}$, the dual of the partition induced by τ on $\hat{G}$. Thus the result follows from [43], Theorem 2.7, along with the observation that follows its proof. □

Remark 7.9. The fact that a pair (ω, τ) is compatible does not imply in general that (τ, ω) is also compatible. The most interesting scenario is when both (ω, τ) and (τ, ω) are compatible, i.e., when ω and τ are **mutually** compatible. In this case, using Theorem 7.8 and the fact that $\mathcal{C}^{**} = \mathcal{C}$, one can easily see that the ω-distribution of a code and the τ-distribution of the dual code determine each other.

Remark 7.6 and Remark 7.9 suggest the following problems about MacWilliams identities over groups. The first two problems have been mentioned in the introduction of the chapter.

(**P1**) Construct weight functions $\omega : G \to X$ and $\tau : \hat{G} \to Y$ such that both (ω, τ) and (τ, ω) are compatible pairs.

(**P2**) Compute the associated Krawtchouk coefficients.

(**P3**) Construct weights ω, τ such that both (ω, τ) and (τ, ω) are compatible, and both d_ω and d_τ are distance functions.

Using tools from lattice theory, in this chapter we construct a family of weight functions ω, τ such that both (ω, τ) and (τ, ω) are compatible pairs. For such weight functions we will also provide a combinatorial description of the corresponding Krawtchouk coefficients in terms of the invariants of an underlying poset with some regularity properties (see Theorem 7.28). It turns out that the most relevant weight functions studied in coding theory belong to the family that we introduce up to equivalence (see Section 7.5). We will also construct, for any finite abelian group G, weight functions $\omega : G \to X \subseteq \mathbb{N}$ and $\tau : \hat{G} \to Y \subseteq \mathbb{N}$ such that (ω, τ) and (τ, ω) are both compatible, and such that d_ω and d_τ are both distance functions (see Example 7.33).

We conclude this section mentioning the product weight and the symmetrized weight induced by a weight function. See also Definition 3.1 and 3.2 of [43].

Definition 7.10. Let $\omega : G \to X$ be a weight, and let $n \geq 1$ be an integer.

1. The **product weight** on G^n associated to ω is the function $\omega^n : G^n \to X^n$ defined, for all $(g_1, ..., g^n)$, by $\omega^n(g_1, ..., g_n) := (\omega(g_1), ..., \omega(g_n))$.
2. Choose an enumeration $X = \{x_0, ..., x_r\}$ and for all $(c_1, ..., c_n) \in X^n$ let $\mathrm{cmp}(c) := (e_0, ..., e_r)$, where $e_i := |\{1 \leq j \leq n : c_j = x_i\}|$ for all $0 \leq i \leq r$. The **symmetrized weight** on G^n associated to ω is the function $\omega^n_{\mathrm{sym}} : G^n \to \{0, ..., n\}^{r+1}$ defined, for all $(g_1, ..., g_n) \in G^n$, by $\omega^n_{\mathrm{sym}}(g_1, ..., g_n) := \mathrm{cmp}(\omega^n(g_1, ..., g_n))$.

Compatibility of pairs is preserved by products and symmetrization, as we now show. The first formula of the following proposition also appears in the proof of [43], Theorem 3.3(a).

Proposition 7.11. Let $\omega : G \to X$ and $\tau : \hat{G} \to Y$ be weights, and let $n \geq 1$ be an integer. Set $r := |X|$ and $s := |Y|$. Assume that (ω, τ) is a compatible pair. Then (ω^n, τ^n) and $(\omega^n_{\mathrm{sym}}, \tau^n_{\mathrm{sym}})$ are compatible pairs. Moreover, for all $a = (a_1, ..., a_n) \in X^n$ and $b = (b_1, ..., b_n) \in Y^n$, and for all $d = (d_0, ..., d_r) \in \{1, ..., n\}^{r+1}$ and $e \in \{1, ..., n\}^{s+1}$ we have:

$$K(\omega^n, \tau^n)(a, b) \;=\; \prod_{j=1}^{n} K(\omega, \tau)(a_j, b_j),$$

$$K(\omega^n_{\mathrm{sym}}, \tau^n_{\mathrm{sym}})(d, e) \;=\; \sum_{\substack{b \in X^n \\ \mathrm{cmp}(b) = e}} \prod_{j=1}^{d_0} K(\omega, \tau)(0, b_j) \prod_{j=d_0+1}^{d_1} K(\omega, \tau)(1, b_j) \;\cdots\; \prod_{j=d_{r-1}+1}^{d_r} K(\omega, \tau)(r, b_j).$$

Proof. Let $(a_1, ..., a_n) \in \omega^n(G^n)$ and $(b_1, ..., b_n) \in \tau^n(\hat{G}^n)$. For any element $(g_1, ..., g_n) \in G^n$ with $\omega^n(g_1, ..., g_n) = (a_1, ..., a_n)$ one has

$$\sum_{\substack{(\chi_1, ..., \chi_n) \in \hat{G}^n \\ \tau^n(\chi_1, ..., \chi_n) = (b_1, ..., b_n)}} (\chi_1, ..., \chi_n)(g_1, ..., g_n) = \prod_{j=1}^{n} K(\omega, \tau)(a_j, b_j). \tag{7.1}$$

This shows that (ω^n, τ^n) is a compatible pair, and proves the first formula in the statement. Now we study the symmetrized weight. Let $(d_0, ..., d_r) \in \omega^n_{\mathrm{sym}}(G^n)$ and $(e_0, ..., e_s) \in \tau^n_{\mathrm{sym}}(\hat{G}^n)$, and let $(g_1, ..., g_n) \in G^n$ with $\omega^n_{\mathrm{sym}}(g_1, ..., g_n) = (d_0, ..., d_r)$. Using (7.1) we compute

$$\sum_{\substack{(\chi_1, ..., \chi_n) \in \hat{G}^n \\ \tau^n_{\mathrm{sym}}(\chi_1, ..., \chi_n) = (e_0, ..., e_s)}} (\chi_1, ..., \chi_n)(g_1, ..., g_n) \;=\; \sum_{\substack{(b_1, ..., b_n) \in X^n \\ \mathrm{cmp}(b_1, ..., b_n) = (e_0, ..., e_s)}} \prod_{j=1}^{n} K(\omega, \tau)(a_j, b_j), \tag{7.2}$$

where $(a_1, ..., a_n) := \omega^n(g_1, ..., g_n)$. Up to a permutation of the entries of $(a_1, ..., a_n)$, without loss of generality we may assume $a_i \leq a_{i+1}$ for all $1 \leq i \leq n-1$. Therefore (7.2) becomes

$$\sum_{\substack{(b_1, ..., b_n) \in X^n \\ \mathrm{cmp}(b_1, ..., b_n) = (e_0, ..., e_s)}} \prod_{j=1}^{d_0} K(\omega, \tau)(0, b_j) \prod_{j=d_0+1}^{d_1} K(\omega, \tau)(1, b_j) \;\cdots\; \prod_{j=d_{r-1}+1}^{d_r} K(\omega, \tau)(r, b_j).$$

The expression above only depends on $(d_0, ..., d_r)$ and $(e_0, ..., e_s)$. This shows that $(\omega^n_{\mathrm{sym}}, \tau^n_{\mathrm{sym}})$ is compatible, and proves the second formula in the statement. □

Proposition 7.11 shows that the computation of the Krawtchouk coefficients of the pairs (ω^n, τ^n) and $(\omega^n_{\mathrm{sym}}, \tau^n_{\mathrm{sym}})$ reduces to the computation of the Krawtchouk coefficients of (ω, τ).

7.2 Regular lattices

In this section we briefly recall some basic notions on posets and lattices, and propose a definition of regular lattice. See Chapter 3 of [87] for a general introduction to posets. In the sequel we only treat finite lattices.

Given a poset $(L, \leq)$ and $S, T \in L$, we write $S < T$ for $S \leq T$ and $S \neq T$. We write $S \lessdot T$ if $S < T$ and there is no $U \in L$ with $S < U < T$. In this case we say that T **covers** S.

Definition 7.12. A **lattice** is a poset $(L, \leq)$ where every $S, T \in L$ have a unique meet and a unique join, denoted by $S \wedge T$ and $S \vee T$, respectively.

Meet and join of a lattice $\mathcal{L} = (L, \leq, \wedge, \vee)$ define two binary, commutative and associative operations $\wedge, \vee : L \times L \to L$. In particular, for any non-empty finite subset $M \subseteq L$, the lattice elements $\bigwedge\{S : S \in M\}$ and $\bigvee\{S : S \in M\}$ are well-defined. When $\mathcal{L}$ is **finite** (i.e., L is finite), we set $0_{\mathcal{L}} := \bigwedge\{S : S \in L\}$ and $1_{\mathcal{L}} := \bigvee\{S : S \in L\}$.

A finite lattice $\mathcal{L}$ is **graded** of **rank** r if all maximal chains in $\mathcal{L}$ have length r. We denote the rank of a graded lattice $\mathcal{L}$ by $\mathrm{rk}(\mathcal{L})$.

Remark 7.13. Let $\mathcal{L} = (L, \leq, \wedge, \vee)$ be a finite graded lattice of rank r. Then there exists a unique function $\rho_{\mathcal{L}} : L \to \{0, ..., r\}$, called the **rank function** of $\mathcal{L}$, with $\rho(0_{\mathcal{L}}) = 0$ and $\rho_{\mathcal{L}}(T) = \rho_{\mathcal{L}}(S) + 1$ whenever $S \lessdot T$ (see [87], page 281). The function $\rho_{\mathcal{L}}$ is monotonic, i.e., $\rho_{\mathcal{L}}(S) \leq \rho_{\mathcal{L}}(T)$ whenever $S \leq T$. Moreover, $\rho_{\mathcal{L}}(L) = \{0, ..., r\}$, and $0_{\mathcal{L}}$ and $1_{\mathcal{L}}$ are the only elements of rank 0 and r, respectively.

The **dual** of a lattice $\mathcal{L} = (L, \leq, \wedge, \vee)$ is the lattice $\mathcal{L}^* = (L, \preceq, \curlywedge, \curlyvee)$, where $S \preceq T$ if and only if $T \leq S$, $\curlywedge := \vee$ and $\curlyvee := \wedge$. If $\mathcal{L}$ is finite (and so $\mathcal{L}^*$ is finite) then $0_{\mathcal{L}^*} = 1_{\mathcal{L}}$ and $1_{\mathcal{L}^*} = 0_{\mathcal{L}}$. Clearly, $\mathcal{L}^{**} = \mathcal{L}$. Notice moreover that $\mathcal{L}$ is graded if and only if $\mathcal{L}$ is graded. If this is the case, then it is easy to see that $\mathrm{rk}(\mathcal{L}) = \mathrm{rk}(\mathcal{L}^*)$ and $\rho_{\mathcal{L}^*}(S) = \mathrm{rk}(\mathcal{L}) - \rho_{\mathcal{L}}(S)$ for all $S \in L$.

Definition 7.14. Let $\mathcal{L} = (L, \leq)$ be a finite poset. The **Möbius function** of $\mathcal{L}$ is the function $\mu_{\mathcal{L}} : \{(S, T) \in L \times L : S \leq T\} \to \mathbb{Z}$ inductively defined by $\mu_{\mathcal{L}}(S, S) = 1$ for all $S \in L$, and

$$\mu_{\mathcal{L}}(S, T) = -\sum_{S \leq U < T} \mu_{\mathcal{L}}(S, U) \quad \text{for all } S, T \in L \text{ with } S < T.$$

Using the fact that a lattice $\mathcal{L}$ and its dual lattice $\mathcal{L}^*$ are anti-isomorphic, one can show that $\mu_{\mathcal{L}^*}(S, T) = \mu_{\mathcal{L}}(T, S)$ for all $S, T \in \mathcal{L}$ (see e.g. [86], Proposition 2.1.10).

Now we introduce a definition of regular lattice inspired by [19].

Definition 7.15. A finite graded lattice $\mathcal{L} = (L, \leq, \wedge, \vee)$ of rank r is **regular** if:

(a) For all $T \in L$ and for all integers $0 \leq s \leq r$,
- the number of $S \in L$ with $\rho_{\mathcal{L}}(S) = s$ and $S \leq T$ only depends on s and $\rho_{\mathcal{L}}(T)$,
- the number of $S \in L$ with $\rho_{\mathcal{L}}(S) = s$ and $T \leq S$ only depends on s and $\rho_{\mathcal{L}}(T)$.

(b) For all $S, T \in L$ with $S \leq T$, $\mu_{\mathcal{L}}(S, T)$ only depends on $\rho_{\mathcal{L}}(S)$ and $\rho_{\mathcal{L}}(T)$.

A similar notion of regularity for semi-lattices was proposed in [19]. The definition of [19] is motivated by coding theory applications via association schemes. Our approach and purposes are different from those of [19].

The main combinatorial invariants of a regular lattice are defined as follows.

Notation 7.16. Let $\mathcal{L} = (L, \leq, \wedge, \vee)$ be a regular lattice of rank r. For all integers $0 \leq s, t \leq r$ we set

$$\mu_{\leq}(s, t) := |\{S \in L : S \leq T,\ \rho_{\mathcal{L}}(S) = s\}| \quad \text{and} \quad \mu_{\geq}(s, t) := |\{S \in L : T \leq S,\ \rho_{\mathcal{L}}(S) = s\}|,$$

where $T \in L$ is any element with $\rho_{\mathcal{L}}(T) = t$. For given integers $0 \leq s \leq t \leq r$ we also define

$$\mu_{\mathcal{L}}(s,t) := \mu_{\mathcal{L}}(S,T),$$

where $S, T \in L$ are any lattice elements with $S \leq T$, $\rho_{\mathcal{L}}(S) = s$, and $\rho_{\mathcal{L}}(T) = t$. For all $s > t$ we set $\mu_{\mathcal{L}}(s,t) := 0$.

The following result easily follows from the definitions and from the properties of the Möbius function. It expresses the parameters of the dual of a regular lattice $\mathcal{L}$ in terms of the parameters of $\mathcal{L}$.

Proposition 7.17. Let $\mathcal{L} = (L, \leq, \wedge, \vee)$ be a regular lattice of rank r. Then $\mathcal{L}^* = (L, \preceq, \curlywedge, \curlyvee)$ is regular of rank r, and for all $0 \leq s, t \leq r$ we have

$$\mu_{\preceq}(s,t) = \mu_{\geq}(r-s, r-t), \qquad \mu_{\succeq}(s,t) = \mu_{\leq}(r-s, r-t), \quad \text{and} \quad \mu_{\mathcal{L}^*}(s,t) = \mu_{\mathcal{L}}(r-t, r-s).$$

We conclude this section mentioning a sufficient condition for lattice regularity that does not involve the Möbius function.

Proposition 7.18. Let $\mathcal{L} = (L, \leq, \wedge, \vee)$ be a finite graded lattice. Assume that for every $S, T \in L$ with $S \leq T$ and for every $\rho_{\mathcal{L}}(S) \leq i \leq \rho_{\mathcal{L}}(T)$ the number $\{U \in L : S \leq U \leq T \text{ and } \rho_{\mathcal{L}}(U) = i\}$ only depends on i, $\rho_{\mathcal{L}}(S)$ and $\rho_{\mathcal{L}}(T)$. Then $\mathcal{L}$ is regular.

Proof. Property (a) of Definition 7.15 is immediate, and property (b) can be proved by induction on $\rho_{\mathcal{L}}(T) - \rho_{\mathcal{L}}(S)$ using the definition of Möbius function. □

7.3 Regular supports and duality

In this section we propose a definition of regular support on a finite abelian group, and establish some preliminaries properties that we will need in the sequel. In particular, we show that a regular support on a finite abelian group G induces a regular support on the character group $\hat{G}$.

Notation 7.19. If G is a group, $\mathcal{L} = (L, \leq)$ is a poset and $\sigma : G \to L$ is any function, then for all $S \in L$ we set $G_\sigma(S) := \{g \in G : \sigma(g) \leq S\}$.

Definition 7.20. Let $(G, +)$ be a finite abelian group, and let $\mathcal{L} = (L, \leq, \wedge, \vee)$ be a regular lattice. A **regular support** on G with values in $\mathcal{L}$ is a function $\sigma : G \to L$ that satisfies the following.

(A) $\sigma(g) = 0_{\mathcal{L}}$ if and only if $g = 0$.
(B) $\sigma(g) = \sigma(-g)$ for all $g \in G$.
(C) $\sigma(g_1 + g_2) \leq \sigma(g_1) \vee \sigma(g_2)$ for all $g_1, g_2 \in G$.
(D) $G_\sigma(S_1 \vee S_2) = G_\sigma(S_1) + G_\sigma(S_2)$ for all $S_1, S_2 \in L$.
(E) For all $S \in L$, $|G_\sigma(S)|$ only depends on $\rho_{\mathcal{L}}(S)$.

Notation 7.21. We denote a regular support on G with values in $\mathcal{L}$ by $\sigma : G \dashrightarrow \mathcal{L}$. Moreover, for all $0 \leq s \leq r$ we set

$$\gamma_\sigma(S) := |G_\sigma(S)|,$$

where $S \in L$ is any element with $\rho_{\mathcal{L}}(S) = s$. Given a lattice element $S \in L$ and a code $\mathcal{C} \subseteq G$, we define $\mathcal{C}_\sigma(S) := G_\sigma(S) \cap \mathcal{C}$.

We now show that the definition of regular lattice behaves well under dualization.

Notation 7.22. Let $\sigma : (G,+) \dashrightarrow \mathcal{L} = (L, \leq, \wedge, \vee)$ be a regular support. Define the function $\sigma^* : \hat{G} \to L$ by

$$\sigma^*(\chi) := \bigvee \{S \in L : \chi \in G_\sigma(S)^*\}$$

for all $\chi \in \hat{G}$. Since $G_\sigma(0_\mathcal{L}) = \{0\}$ by property (A) of Definition 7.20, we have $\chi \in G_\sigma(0_\mathcal{L})^*$ for any $\chi \in \hat{G}$. This shows that $\sigma^*(\chi)$ is well-defined. We regard σ^* as a function on $\hat{G}$ with values in $\mathcal{L}^*$. In particular, according to Notation 7.19, for $S \in L$ we have

$$\hat{G}_{\sigma^*}(S) = \{\chi \in \hat{G} : \sigma^*(\chi) \preceq S\}.$$

Lemma 7.23. Let $\sigma : (G,+) \dashrightarrow \mathcal{L} = (L, \leq, \wedge, \vee)$ be a regular support. Then for all $\chi \in \hat{G}$ we have $\chi \in G_\sigma(\sigma^*(\chi))^*$. Equivalently, $\sigma^*(\chi)$ is the maximum $S \in L$ such that $\chi \in G_\sigma(S)^*$.

Proof. Let $\chi \in \hat{G}$ be any character. As already shown, $\{S \in L : \chi \in G(S)^*\} \neq \emptyset$. Choose an enumeration $\{S \in L : \chi \in G(S)^*\} = \{S_1, S_2, ..., S_t\}$. By property (D) of Definition 7.20 and the associativity of the join we have $G(S_1 \vee S_2 \vee \cdots \vee S_t) = G_\sigma(S_1) + G_\sigma(S_2) + \cdots + G_\sigma(S_t)$. Thus Remark 7.2 implies $G(S_1 \vee S_2 \vee \cdots \vee S_t)^* = G_\sigma(S_1)^* \cap G_\sigma(S_2)^* \cap \cdots \cap G_\sigma(S_t)^*$. Since $\chi \in G_\sigma(S_i)^*$ for all $i \in \{1, ..., t\}$, we have $\chi \in G_\sigma(\sigma^*(\chi))^*$, as claimed. □

The following crucial theorem summarizes the main properties of a regular support. In particular, it shows that a regular support on a group G with values in a lattice $\mathcal{L}$ induces a regular support on the character group $\hat{G}$ with values in the dual lattice $\mathcal{L}^*$.

Theorem 7.24. Let $\sigma : (G,+) \dashrightarrow \mathcal{L} = (L, \leq, \wedge, \vee)$ be regular. The following hold.

1. $G_\sigma(S)^* = \hat{G}_{\sigma^*}(S)$ for all $S \in L$.
2. The map $\chi \mapsto \sigma^*(\chi)$ defines a regular support $\sigma^* : (\hat{G}, \cdot) \dashrightarrow \mathcal{L}^* = (L, \preceq, \curlywedge, \curlyvee)$.
3. $\gamma_{\sigma^*}(s) = |G|/\gamma_\sigma(\mathrm{rk}(\mathcal{L}) - s)$ for all $0 \leq s \leq \mathrm{rk}(\mathcal{L})$.
4. Identifying $\hat{\hat{G}}$ and G we have $\sigma^{**} = \sigma$.

Definition 7.25. The regular support $\sigma^* : (\hat{G}, \cdot) \dashrightarrow \mathcal{L}^*$ defined in part 2 of Theorem 7.24 and Notation 7.22 is called the **dual support** of σ.

Proof of Theorem 7.24. 1. Take any $S \in L$. If $\chi \in G_\sigma(S)^*$ then, by definition, $S \leq \sigma^*(\chi)$, i.e., $\sigma^*(\chi) \preceq S$. This shows $G_\sigma(S)^* \subseteq \hat{G}_{\sigma^*}(S)$. Now assume that $\chi \in \hat{G}_{\sigma^*}(S)$, and let $g \in G_\sigma(S)$. We have $\sigma(g) \leq S \leq \sigma^*(\chi)$, and so $g \in G_\sigma(\sigma^*(\chi))$. Lemma 7.23 implies $\chi(g) = 1$, and so $\hat{G}_{\sigma^*}(S) \subseteq G_\sigma(S)^*$.

2. The lattice $\mathcal{L}^*$ is regular by Proposition 7.17, and the group $(\hat{G}, \cdot)$ is finite and abelian. Let ε be the trivial character of G. By 1 we have $\hat{G}_{\sigma^*}(0_{\mathcal{L}^*}) = G_\sigma(1_\mathcal{L})^* = G^* = \{\varepsilon\}$, and this proves property (A) of Definition 7.20. For $\chi \in \hat{G}$ and $S \in L$ we have $\chi \in G_\sigma(S)^*$ if and only if $1/\chi \in G_\sigma(S)^*$. By definition of dual support, this gives property (B). Now take any $\chi_1, \chi_2 \in \hat{G}$, and let $g \in G_\sigma(\sigma^*(\chi_1)) \cap G_\sigma(\sigma^*(\chi_2))$. Lemma 7.23 implies $\chi_1(g) = \chi_2(g) = 1$, and so $(\chi_1 \cdot \chi_2)(g) = \chi_1(g)\chi_2(g) = 1$. Thus

$$\chi_1 \cdot \chi_2 \in (G_\sigma(\sigma^*(\chi_1)) \cap G_\sigma(\sigma^*(\chi_2)))^* = G_\sigma(\sigma^*(\chi_1) \wedge \sigma^*(\chi_2))^*,$$

where the last equality directly follows from the definition of meet. As a consequence we have $\sigma^*(\chi_2) \wedge \sigma^*(\chi_2) \leq \sigma^*(\chi_1 \cdot \chi_2)$, i.e., $\sigma^*(\chi_1 \cdot \chi_2) \preceq \sigma^*(\chi_1) \curlyvee \sigma^*(\chi_2)$. This establishes property (C). Let $S_1, S_2 \in L$. By definition of meet we have $G_\sigma(S_1 \wedge S_2) = G_\sigma(S_1) \cap G_\sigma(S_2)$. Taking

the duals, by Remark 7.2 we obtain $G_\sigma(S_1 \wedge S_2)^* = G_\sigma(S_1)^* \cdot G_\sigma(S_2)^*$, and part 1 of the statement gives $\hat{G}_{\sigma^*}(S_1 \wedge S_2) = \hat{G}_{\sigma^*}(S_1) \cdot \hat{G}_{\sigma^*}(S_2)$, i.e., $\hat{G}_{\sigma^*}(S_1 \curlyvee S_2) = \hat{G}_{\sigma^*}(S_1) \cdot \hat{G}_{\sigma^*}(S_2)$. This is property (D). Let $S \in L$. By part 1 and Remark 7.2 we have $|\hat{G}_{\sigma^*}(S)| = |G|/|G_\sigma(S)|$. Therefore $|\hat{G}_{\sigma^*}(S)|$ only depends on $\rho_{\mathcal{L}^*}(S) = \mathrm{rk}(\mathcal{L}) - \rho_{\mathcal{L}}(S)$. This is property (E).

3. Let $r := \mathrm{rk}(\mathcal{L}) = \mathrm{rk}(\mathcal{L}^*)$. Take $S \in L$ with $\rho_{\mathcal{L}^*}(S) = s$. Part 1 and Remark 7.2 imply $\hat{G}_{\sigma^*}(S)^* = G_\sigma(S)$. Thus $\gamma_{\sigma^*}(s) = |\hat{G}_{\sigma^*}(S)| = |G|/|\hat{G}_{\sigma^*}(S)^*| = |G|/|G_\sigma(S)| = |G|/\gamma_\sigma(s)$.

4. As before, part 1 and Remark 7.2 give $\hat{G}_{\sigma^*}(S)^* = G_\sigma(S)$ for all $S \in L$. Hence, for all $g \in G$, $\sigma^{**}(g) = \bigvee\{S \in L : g \in \hat{G}_{\sigma^*}(S)^*\} = \bigwedge\{S \in L : g \in G_\sigma(S)\} = \bigwedge\{S \in L : \sigma(g) \leq S\} = \sigma(g)$. This concludes the proof. □

We close this section with an example that shows that every finite abelian group admits a regular support.

Example 7.26 (Chain support)**.** Let $(L, \leq)$ be a finite chain, and let $S_0 < S_1 < \cdots < S_r$ be the elements of L. For all $i, j \in \{0, ..., r\}$ define $S_i \wedge S_j := S_{\min\{i,j\}}$ and $S_i \vee S_j := S_{\max\{i,j\}}$. Then it is easy to see that $\mathcal{L} = (L, \leq, \wedge, \vee)$ is regular lattice of rank r with:

$$\mu_\leq(s,t) = \begin{cases} 1 & \text{if } s \leq t \\ 0 & \text{else} \end{cases} \qquad \mu_\geq(s,t) = \begin{cases} 1 & \text{if } s \geq t \\ 0 & \text{else} \end{cases} \qquad \mu_{\mathcal{L}}(s,t) = \begin{cases} 1 & \text{if } s = t \\ -1 & \text{if } t = s+1 \\ 0 & \text{else} \end{cases}$$

for all $0 \leq s, t \leq r$. Now let $(G, +)$ be a finite abelian group, and let $\mathcal{L} = (L, \subseteq, \wedge, \vee)$ be a chain of subgroups of G, i.e., $\{0\} = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_r = G$, endowed with the structure of regular lattice described above. The **chain support** $\sigma : G \dashrightarrow \mathcal{L}$ is the function $\sigma : G \to L$ defined, for all $g \in G$, by $\sigma(g) := G_i$, where $i = \min\{0 \leq j \leq r : g \in G_j\}$. One can check that σ is a regular support. By definition, $G_\sigma(G_s) = G_s$ for all $0 \leq s \leq r$, and therefore $\gamma_\sigma(s) = |G_s|$ for all s. Moreover, for any $\chi \in \hat{G}$ we have $\sigma^*(\chi) = G_i$, where $i = \max\{0 \leq j \leq r : \chi \in G_j^*\}$.

7.4 Compatible weights from regular supports

A regular support $\sigma : G \dashrightarrow \mathcal{L}$ induces a weight function on the group G via the rank function of the regular lattice $\mathcal{L}$.

Definition 7.27. Let $\sigma : (G, +) \dashrightarrow \mathcal{L}$ be a regular support. The **σ-weight** on $\mathcal{C}$ induced by σ is the function $\omega_\sigma : G \to \{0, ..., \mathrm{rk}(\mathcal{L})\}$ defined by $\omega_\sigma(g) := \rho_{\mathcal{L}}(\sigma(g))$ for all $g \in G$.

Now we state our main result.

Theorem 7.28. Let $\sigma : (G, +) \dashrightarrow \mathcal{L}$ be a regular support, $r = \mathrm{rk}(\mathcal{L})$. The following hold.

1. The pair $(\omega_{\sigma^*}, \omega_\sigma)$ is compatible. Moreover, for all $i \in \omega_{\sigma^*}(\hat{G})$ and $j \in \omega_\sigma(G)$ we have
$$K(\omega_{\sigma^*}, \omega_\sigma)(i,j) \;=\; \sum_{s=0}^{r} \gamma_\sigma(s)\ \mu_{\mathcal{L}}(s,j)\ \mu_\leq(s, r-i)\ \mu_\geq(j,s).$$

2. The pair $(\omega_\sigma, \omega_{\sigma^*})$ is compatible. Moreover, for all $i \in \omega_\sigma(G)$ and $j \in \omega_{\sigma^*}(\hat{G})$ we have
$$K(\omega_\sigma, \omega_{\sigma^*})(i,j) \;=\; |G| \sum_{s=0}^{r} \frac{1}{\gamma_\sigma(r-s)}\ \mu_{\mathcal{L}}(r-j, r-s)\ \mu_\geq(r-s, i)\ \mu_\leq(r-j, r-s).$$

Remark 7.29. Theorem 7.28 shows that a regular support $\sigma : G \dashrightarrow \mathcal{L}$ automatically yields compatible pairs of weights $(\omega_\sigma, \omega_{\sigma^*})$ and $(\omega_{\sigma^*}, \omega_\sigma)$ on G and $\hat{G}$. Moreover, it expresses the associated Krawtchouk coefficients in terms of the combinatorial invariants of the lattice $\mathcal{L}$. This provides an answer to problems (**P1**) and (**P2**) on page 111. As we will see, in many relevant examples such combinatorial invariants are very easy to determine. In those cases Theorem 7.28 gives an effective method to compute the Krawtchouk coefficients.

Proof of Theorem 7.28. Throughout this proof, a sum over an empty set of indices is zero by definition. Let us first show part 1. Part 2 will follow easily. Fix any character $\chi \in \hat{G}$, and let $f, g : L \to \mathbb{C}$ be the complex-valued functions defined by

$$f(T) := \sum_{\substack{g \in G \\ \sigma(g) = T}} \chi(g), \qquad g(T) := \sum_{S \leq T} f(S) \qquad \text{for all } T \in L.$$

By the orthogonality relations of characters (see e.g. [64], Lemma 1.1.32), for all $T \in L$ we have

$$g(T) = \sum_{S \leq T} f(S) = \sum_{g \in G_\sigma(T)} \chi(g) = \begin{cases} \gamma_\sigma(\rho_{\mathcal{L}}(T)) & \text{if } \chi \in G_\sigma(T)^* \\ 0 & \text{if } \chi \notin G_\sigma(T)^*. \end{cases}$$

Therefore applying the Möbius inversion formula ([87], Proposition 3.7.1) to f and g we obtain

$$\begin{aligned} f(T) &= \sum_{\substack{S \leq T \\ \chi \in G_\sigma(S)^*}} \gamma_\sigma(\rho_{\mathcal{L}}(S))\ \mu_{\mathcal{L}}(S,T) = \sum_{s=0}^{r} \sum_{\substack{S \leq T \\ \rho_{\mathcal{L}}(S) = s \\ \chi \in G_\sigma(S)^*}} \gamma_\sigma(s)\ \mu_{\mathcal{L}}(S,T) \\ &= \sum_{s=0}^{r} \sum_{\substack{S \leq T \\ \rho_{\mathcal{L}}(S) = s \\ \chi \in \hat{G}_{\sigma^*}(S)}} \gamma_\sigma(s)\ \mu_{\mathcal{L}}(S,T), \end{aligned}$$

where the last equality follows from part 1 of Theorem 7.24. Thus for any integer $0 \leq j \leq r$ one has

$$\begin{aligned} \sum_{\substack{g \in G \\ \omega_\sigma(g) = j}} \chi(g) &= \sum_{\substack{T \in L \\ \rho_{\mathcal{L}}(T) = j}} f(T) = \sum_{\substack{T \in L \\ \rho_{\mathcal{L}}(T) = j}} \sum_{s=0}^{r} \sum_{\substack{S \leq T \\ \rho_{\mathcal{L}}(S) = s \\ \chi \in \hat{G}_{\sigma^*}(S)}} \gamma_\sigma(s)\ \mu_{\mathcal{L}}(S,T) \\ &= \sum_{s=0}^{r} \gamma_\sigma(s) \sum_{\substack{T \in L \\ \rho_{\mathcal{L}}(T) = j}} \sum_{\substack{S \leq T \\ \rho_{\mathcal{L}}(S) = s \\ \chi \in \hat{G}_{\sigma^*}(S)}} \mu_{\mathcal{L}}(S,T). \end{aligned}$$

By the regularity of $\mathcal{L}$, $\mu_{\mathcal{L}}(S,T) = \mu_{\mathcal{L}}(s,j)$ for all $S, T \in L$ with $S \leq T$, $\rho_{\mathcal{L}}(S) = s$ and $\rho_{\mathcal{L}}(T) = j$. Thus setting $\alpha(s,j,\chi) := |\{(S,T) \in L \times L : \rho_{\mathcal{L}}(S) = s,\ \rho_{\mathcal{L}}(T) = j,\ S \leq T,\ \sigma^*(\chi) \preceq S\}|$ we have

$$\sum_{\substack{g \in G \\ \omega_\sigma(g) = j}} \chi(g) = \sum_{s=0}^{r} \gamma_\sigma(s)\ \mu_{\mathcal{L}}(s,j)\ \alpha(s,j,\chi). \tag{7.3}$$

Now we derive a more convenient expression for $\alpha(s,j,\chi)$. By definition,

$$\alpha(s,j,\chi) = \sum_{\substack{S \in L \\ \rho_{\mathcal{L}}(S) = s \\ \sigma^*(\chi) \preceq S}} |\{T \in L : \rho_{\mathcal{L}}(T) = j,\ S \leq T\}| = \sum_{\substack{S \in L \\ \rho_{\mathcal{L}}(S) = s \\ S \leq \sigma^*(\chi)}} \mu_{\geq}(j,s) = \mu_{\leq}(s, \rho_{\mathcal{L}}(\sigma^*(\chi)))\ \mu_{\geq}(j,s).$$

By the properties of the rank function of the dual lattice (see Section 7.2) and the definition of ω_{σ^*} we have $\rho_{\mathcal{L}}(\sigma^*(\chi)) = r - \rho_{\mathcal{L}^*}(\sigma^*(\chi)) = r - \omega_{\sigma^*}(\chi)$. It follows $\mu_{\leq}(s, \rho_{\mathcal{L}}(\sigma^*(\chi))) = \mu_{\leq}(s, r - \omega_{\sigma^*}(\chi))$, and therefore $\alpha(s, j, \chi) = \mu_{\leq}(s, r - \omega_{\sigma^*}(\chi))\ \mu_{\geq}(j, s)$. Substituting this expression for $\alpha(s, j, \chi)$ into equation (7.3) yields

$$\sum_{\substack{g \in G \\ \omega_\sigma(g) = j}} \chi(g) \ = \ \sum_{s=0}^{r} \gamma_\sigma(s)\ \mu_{\mathcal{L}}(s, j)\ \mu_{\leq}(s, r - \omega_{\sigma^*}(\chi))\ \mu_{\geq}(j, s).$$

By Remark 7.4, this shows part 1.

By Theorem 7.24, σ^* is a regular support, and $\sigma^{**} = \sigma$ when identifying G and $\hat{\hat{G}}$. Thus part 2 follows from part 1 applied to $\sigma^* : \hat{G} \dashrightarrow \mathcal{L}^*$, along with Proposition 7.17. □

Mutually compatible pairs induce Fourier-reflexive partitions in the sense of [43], as the following result shows.

Proposition 7.30. Let $\sigma : G \dashrightarrow \mathcal{L}$ be a regular support. The partitions $\mathcal{P}(\omega_\sigma)$ and $\mathcal{P}(\omega_{\sigma^*})$ are both Fourier-reflexive and mutually dual.

Proof. If $\mathcal{P}$ and $\mathcal{Q}$ are partitions, we write $\mathcal{P} \leq \mathcal{Q}$ if $\mathcal{P}$ is finer than $\mathcal{Q}$. Combining the definition of dual partition with Theorem 7.28 we deduce $\mathcal{P}(\omega_{\sigma^*}) \leq \widehat{\mathcal{P}(\omega_\sigma)}$ and $\mathcal{P}(\omega_\sigma) \leq \widehat{\mathcal{P}(\omega_{\sigma^*})}$. Therefore we have

$$|\mathcal{P}(\omega_{\sigma^*})| \geq |\widehat{\mathcal{P}(\omega_\sigma)}|, \quad |\mathcal{P}(\omega_\sigma)| \geq |\widehat{\mathcal{P}(\omega_{\sigma^*})}|. \tag{7.4}$$

Applying [43, Theorem 3.1] we find

$$|\widehat{\mathcal{P}(\omega_\sigma)}| \geq |\mathcal{P}(\omega_\sigma)|, \quad |\widehat{\mathcal{P}(\omega_{\sigma^*})}| \geq |\mathcal{P}(\omega_{\sigma^*})|. \tag{7.5}$$

Combining the inequalities in (7.4) and (7.5) one easily obtains

$$|\mathcal{P}(\omega_\sigma)| \leq |\widehat{\mathcal{P}(\omega_\sigma)}| \leq |\mathcal{P}(\omega_{\sigma^*})| \leq |\widehat{\mathcal{P}(\omega_{\sigma^*})}| \leq |\mathcal{P}(\omega_\sigma)|.$$

This implies

$$\widehat{\mathcal{P}(\omega_\sigma)} = \mathcal{P}(\omega_{\sigma^*}), \quad \widehat{\mathcal{P}(\omega_{\sigma^*})} = \mathcal{P}(\omega_\sigma), \quad |\widehat{\mathcal{P}(\omega_\sigma)}| = |\mathcal{P}(\omega_\sigma)|, \quad |\widehat{\mathcal{P}(\omega_{\sigma^*})}| = |\mathcal{P}(\omega_{\sigma^*})|.$$

In particular, the partitions $\mathcal{P}(\omega_\sigma)$ and $\mathcal{P}(\omega_{\sigma^*})$ are mutually dual. Moreover, they are both Fourier-reflexive by Theorem 3.1 of [43]. □

Combining Example 7.26, Theorem 7.28, and Proposition 7.30 one immediately obtains the following result.

Corollary 7.31 (Fourier-reflexive partitions via subgroups)**.** Let $(G, +)$ be a finite abelian group, and let $\{0\} = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_r = G$ be a chain of subgroups of G. Then

$$\{0\} \sqcup \bigsqcup_{i=1}^{r} G_i \setminus G_{i-1}$$

is a Fourier-reflexive partition of G of cardinality $r + 1$.

Under certain assumptions on the lattice $\mathcal{L}$, the weight function ω_σ associated to a regular support $\sigma : G \dashrightarrow \mathcal{L}$ induces a distance d_{ω_σ} on G. Recall that a finite lattice $\mathcal{L} = (L, \leq, \wedge, \vee)$ is **modular** if for all $S, T, U \in L$ with $S \leq U$ one has $S \vee (T \wedge U) = (S \vee T) \wedge U$. Clearly, the dual of a modular lattice is modular.

Proposition 7.32. Let $\sigma : (G, +) \dashrightarrow \mathcal{L}$ be a regular support. If $\mathcal{L}$ is modular, then the function $d_{\omega_\sigma} : G \times G \to \mathbb{N}$ defined by $d_{\omega_\sigma}(g, g') := \omega_\sigma(g - g')$ for all $g, g' \in G$ is a distance function.

Proof. Write $d := d_{\omega_\sigma}$. Let $g, g' \in G$. By definition, $d(g, g') = 0$ if and only if $\rho_{\mathcal{L}}(\sigma(g - g')) = 0$. By the properties of $\rho_{\mathcal{L}}$ (Remark 7.13), this happens if and only if $\sigma(g - g') = 0$, i.e., by property (A) of Definition 7.20, if and only if $g = g'$. By property (B) of Definition 7.20 we have $d(g, g') = \omega_\sigma(g - g') = \rho_{\mathcal{L}}(\sigma(g - g')) = \rho_{\mathcal{L}}(\sigma(g' - g)) = \omega_\sigma(g' - g) = d(g', g)$. Now let $h, g, g' \in G$. The rank function of a modular lattice $\mathcal{L} = (L, \leq, \wedge, \vee)$ satisfies $\rho_{\mathcal{L}}(S \vee T) = \rho_{\mathcal{L}}(S) + \rho_{\mathcal{L}}(T) - \rho(S \wedge T)$ for all $S, T \in L$ (see [87], page 287). Thus by property (C) of Definition 7.20 we have

$$d(g, g') = \omega_\sigma(g - g') = \omega_\sigma(g - h - (g' - h)) \leq \rho_{\mathcal{L}}(\sigma(g - h) \vee \sigma(g' - h)) \leq d(g, h) + d(h, g).$$

This concludes the proof. □

Example 7.33 (Chain support, continued)**.** Let $(G, +)$ be a finite abelian group, and let $\mathcal{L}$ be a chain $\{0\} = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_r = G$ of subgroups of G endowed with the lattice structure described in Example 7.26. It is easy to see that $\mathcal{L}$ is modular. Denote by $\sigma : G \dashrightarrow \mathcal{L}$ the associated chain support. By Example 7.26, σ is regular. Thus, by Proposition 7.32, d_{ω_σ} is a distance on G. By Theorem 7.24, σ^* is a regular support. Since $\mathcal{L}$ is modular, $\mathcal{L}^*$ is modular and so, by Proposition 7.32, $d_{\omega_{\sigma^*}}$ is a distance on $\hat{G}$. By Theorem 7.28, $(\omega_\sigma, \omega_{\sigma^*})$ and $(\omega_{\sigma^*}, \omega_\sigma)$ are compatible pairs such that both d_{ω_σ} and $d_{\omega_{\sigma^*}}$ are distance functions. This provides an answer to problem (**P3**) on page 111.

We conclude the example giving a more explicit description of ω_{σ^*}. Let ν be the chain support on the character group $\hat{G}$ associated to the chain $\{1\} = G_r^* \subsetneq G_{r-1}^* \subsetneq \cdots \subsetneq \hat{G}$. We have $\omega_\nu = \omega_{\sigma^*}$. Indeed, as already mentioned in Example 7.26, for a fixed $\chi \in \hat{G}$ we have $\sigma^*(\chi) = G_i$, where $i = \max\{0 \leq j \leq r : \chi \in G_j^*\}$. Thus, by definition, $\omega_{\sigma^*}(\chi) = \rho_{\mathcal{L}^*}(\sigma^*(\chi)) = r - i$. On the other hand,

$$\omega_\nu(\chi) = \min\{0 \leq j \leq r : \chi \in G_{r-j}^*\} = r - \max\{0 \leq j \leq r : \chi \in G_j^*\} = r - i = \omega_{\sigma^*}(\chi),$$

as claimed.

7.5 MacWilliams identities in coding theory

In this section we show that many weight functions traditionally studied in coding theory are induced by suitable regular supports up to equivalence. We also employ Theorem 7.28 to easily compute the corresponding Krawtchouk coefficients with a combinatorial method. Most of such coefficients have been computed by other authors employing ad hoc techniques in the past. Theorem 7.28 provides a general method that applies to different contexts. In Example 7.39 we will also derive new formulas for the Krawtchouk coefficients associated to the homogeneous rings over certain Frobenius rings.

The case of the rank weight (Example 7.37) is particularly interesting, as the standard method to compute the associated Krawtchouk coefficients is quite sophisticated (see [20]). Theorem 7.28 allows to compute them in a simple way. Notice that the results of our Section 5.2 produce a simple proof for the MacWilliams identities for rank-metric codes, but do not directly provide formulas for the Krawtchouk coefficients associated to the rank weight.

Example 7.34 (Additive codes with the Hamming weight)**.** Let $n \geq 1$ be a positive integer, and let $[n] := \{1, ..., n\}$. Then $\mathcal{L} = (2^{[n]}, \subseteq, \cap, \cup)$ is a regular lattice of rank n. The rank function of $\mathcal{L}$

is the cardinality of sets. The parameters of $\mathcal{L}$ are given by

$$\mu_{\subseteq}(s,t) = \binom{t}{s}, \qquad \mu_{\supseteq}(s,t) = \binom{n-t}{s-t}, \qquad \mu_{\mathcal{L}}(s,t) = \begin{cases} (-1)^{t-s} & \text{if } s \leq t \\ 0 & \text{if } s > t \end{cases}$$

for all $0 \leq s,t \leq n$. The formula for $\mu_{\mathcal{L}}(s,t)$ can be easily proved by induction on $t-s$ with the aid of the Binomial Theorem ([87], page 24). See [87], Example 3.8.3 for a different proof using the product of chains. Let $(G,+)$ be a finite abelian group. Define the **Hamming support** $\sigma_{\mathrm{H}} : G^n \to 2^{[n]}$ by $\sigma_{\mathrm{H}}(g_1,...,g_n) := \{i \in [n] : g_i \neq 0\}$ for all $(g_1,...,g_n) \in G^n$. It is a regular support. The weight induced on G^n by the Hamming support is the **Hamming weight** ω_{H}. For $S \subseteq [n]$ and $(\chi_1,...,\chi_n) \in \hat{G}^n$ we have $(\chi_1,...,\chi_n) \in G^n_\sigma(S)^*$ if and only if χ_s is the trivial character of G for all $s \in S$. Therefore $\sigma^*_{\mathrm{H}}(\chi_1,...,\chi_n) = \{i \in [n] : \chi_i \text{ is trivial}\}$. It follows

$$\omega_{\sigma^*_{\mathrm{H}}}(\chi_1,...,\chi_n) = n - |\{i \in [n] : \chi_i \text{ is trivial}\}| = |\{i \in [n] : \chi_i \text{ is not trivial}\}|.$$

Thus in the following we write $\omega_{\sigma^*_{\mathrm{H}}} = \omega_{\mathrm{H}}$. Theorem 7.28 allows to compute the Krawtchouk coefficients for the Hamming weight as

$$K(\omega_{\mathrm{H}},\omega_{\mathrm{H}})(i,j) = \sum_{s=0}^{n} (-1)^{j-s} \, |G|^s \, \binom{n-i}{s}\binom{n-s}{j-s}$$

for all $0 \leq i,j \leq n$. By Theorem 7.8, for every code $\mathcal{C} \subseteq G^n$ and for all $0 \leq j \leq n$ we have

$$W_j(\mathcal{C}^*,\omega_{\mathrm{H}}) = \frac{1}{|\mathcal{C}|} \sum_{i=0}^{n} W_i(\mathcal{C},\omega_{\mathrm{H}}) \sum_{s=0}^{n} (-1)^{j-s} \, |G|^s \, \binom{n-i}{s}\binom{n-s}{j-s}.$$

These are the "MacWilliams identities for the Hamming weight over a group".

Example 7.35 (Linear codes with the Hamming weight)**.** Take $G = \mathbb{F}_q$ in Example 7.34. Define the **orthogonal** of a linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ by $\mathcal{C}^\perp := \{v \in \mathbb{F}_q^n : \langle w,v\rangle = 0 \text{ for all } w \in \mathcal{C}\}$, where $\langle \cdot,\cdot\rangle$ is the standard inner product of $\mathbb{F}_q^n$. One can show that $W_j(\mathcal{C}^\perp,\omega_{\mathrm{H}}) = W_j(\mathcal{C}^*,\omega_{\mathrm{H}})$ for all linear codes $\mathcal{C} \subseteq \mathbb{F}_q^n$. By Example 7.34, for all $0 \leq j \leq n$ we have

$$W_j(\mathcal{C}^\perp,\omega_{\mathrm{H}}) = \frac{1}{|\mathcal{C}|} \sum_{i=0}^{n} W_i(\mathcal{C},\omega_{\mathrm{H}}) \sum_{s=0}^{n} (-1)^{j-s} \, |G|^s \, \binom{n-i}{s}\binom{n-s}{j-s}.$$

These are the "MacWilliams identities for linear codes with the Hamming weight". See for instance Chapter 5 of [68] or Chapter 7 of [51] for equivalent formulations.

Example 7.36 (Exact weight)**.** Let $(G,+)$ be a non-trivial finite abelian group. Let σ denote the chain support on G associated to the chain $\{0\} \subsetneq G$. See Example 7.26. Let $\omega_\sigma : G \to \{0,1\}$ be the induced weight. By the second part of Example 7.33, ω_{σ^*} is the weight on $\hat{G}$ induced by the chain support associated to the chain $\{1\} \subsetneq \hat{G}$. If $n \geq 2$ and $G = \mathbb{F}_2$, then the product weight ω_σ^n is the **exact weight** on $\mathbb{F}_2^n$ (see [68], page 147). For a general G we obtain a weight that partitions the elements of the group G^n according to the positions of their non-zero entries. With the aid of Theorem 7.28 and Example 7.26 one easily computes the Krawtchouk coefficients for $(\omega_\sigma,\omega_{\sigma^*})$ and $(\omega_{\sigma^*},\omega_\sigma)$ as

$$K(\omega_\sigma,\omega_{\sigma^*})(i,j) = K(\omega_{\sigma^*},\omega_\sigma)(i,j) = \begin{cases} 1 & \text{if } j = 0 \\ -1 & \text{if } j = 1 \text{ and } i = 1 \\ |G| - 1 & \text{if } j = 1 \text{ and } i = 0 \end{cases}$$

for all $i,j \in \{0,1\}$. Proposition 7.11 also allows to compute the coefficients for the product and the symmetrized weight.

Example 7.37 (Linear codes with the rank weight)**.** Let $1 \leq k \leq m$ be integers, and let $G := \mathrm{Mat}$ be the vector space of $k \times m$ matrices over $\mathbb{F}_q$. Denote by L the set of all subspaces of $\mathbb{F}_q^k$. Then $\mathcal{L} = (L, \subseteq, \cap, +)$ is a regular lattice of rank k. Notice that the join is the sum of subspaces. The rank function of $\mathcal{L}$ is given by $\rho_{\mathcal{L}}(V) = \dim(V)$ for all $V \subseteq \mathbb{F}_q^k$ (see [87], page 281). The parameters of $\mathcal{L}$ are, for all $0 \leq s, t \leq k$,

$$\mu_{\subseteq}(s,t) = \begin{bmatrix} t \\ s \end{bmatrix}, \qquad \mu_{\supseteq}(s,t) = \begin{bmatrix} k-t \\ s-t \end{bmatrix}, \qquad \mu_{\mathcal{L}}(s,t) = \begin{cases} (-1)^{t-s} q^{\binom{t-s}{2}} & \text{if } s \leq t \\ 0 & \text{if } s > t, \end{cases}$$

where the symbols in squared brackets are the q-ary binomial coefficients (see e.g. [2]). The formula for $\mu_{\mathcal{L}}(s,t)$ can be easily proved by induction on $t-s$ with the aid of the Gaussian Binomial Theorem ([87], equation (1.87) at page 74). An elegant argument that uses the fact that $\mathcal{L}$ is a geometric lattice can be found in [87], Example 3.10.2. Denote by $\mathrm{colsp}(M) \subseteq \mathbb{F}_q^k$ the space generated by the columns of a matrix $M \in \mathrm{Mat}$. Then $\sigma_{\mathrm{rk}} : M \mapsto \mathrm{colsp}(M)$ is a regular support $\sigma_{\mathrm{rk}} : \mathrm{Mat} \dashrightarrow \mathcal{L}$ with $\gamma_\sigma(s) = q^{ms}$ for all $0 \leq s \leq k$ (see Lemma 5.7). Wel call it the **rank support**. Let $\omega_{\mathrm{rk}} := \omega_{\sigma_{\mathrm{rk}}}$ be the **rank weight**, and set $\omega_{\mathrm{rk}}^* := \omega_{\sigma_{\mathrm{rk}}^*}$ for ease of notation. Employing Theorem 7.28, the Krawtchouk coefficients for $(\omega_{\mathrm{rk}}, \omega_{\mathrm{rk}}^*)$ and $(\omega_{\mathrm{rk}}^*, \omega_{\mathrm{rk}})$ can be computed as

$$K(\omega_{\mathrm{rk}}, \omega_{\mathrm{rk}}^*)(i,j) = K(\omega_{\mathrm{rk}}^*, \omega_{\mathrm{rk}})(i,j) = \sum_{s=0}^{k} (-1)^{j-s}\ q^{ms+\binom{j-s}{2}}\ \begin{bmatrix} k-s \\ k-j \end{bmatrix} \begin{bmatrix} k-i \\ s \end{bmatrix} \tag{7.6}$$

for all $0 \leq i, j \leq k$.

Recall that the **trace-product** of matrices $M, N \in \mathrm{Mat}$ is $\langle M, N \rangle := \mathrm{Tr}(MN^t)$, where Tr is the trace of matrices, and the superscript t denotes transposition. The **orthogonal** of a code $\mathcal{C} \subseteq \mathrm{Mat}$ is $\mathcal{C}^\perp := \{M \in \mathrm{Mat} : \langle N, M \rangle = 0 \text{ for all } N \in \mathcal{C}\}$. Notice that in the previous chapters the set $\mathcal{C}^\perp$ was simply called the "dual" of $\mathcal{C}$. Here we prefer to use the word "orthogonal" to emphasize the difference with the character-theoretic notion of duality studied in this chapter.

It is possible to show that if $\mathcal{C} \subseteq \mathrm{Mat}$ is a linear code, then $W_j(\mathcal{C}^\perp, \omega_{\mathrm{rk}}) = W_j(\mathcal{C}^*, \omega_{\mathrm{rk}}^*)$ for all $0 \leq j \leq k$. Thus combining Theorem 7.8 and equation (7.6) we obtain

$$W_j(\mathcal{C}^\perp, \omega_{\mathrm{rk}}) = \frac{1}{|\mathcal{C}|} \sum_{i=0}^{k} W_i(\mathcal{C}, \omega_{\mathrm{rk}}) \sum_{s=0}^{k} (-1)^{j-s}\ q^{ms+\binom{j-s}{2}}\ \begin{bmatrix} k-s \\ k-j \end{bmatrix} \begin{bmatrix} k-i \\ s \end{bmatrix}$$

for all $0 \leq j \leq k$. These are the "MacWilliams identities for linear codes with the rank weight", that we discussed in Chapter 5.

Example 7.38 (Lee weight on $\mathbb{Z}_4$)**.** The **Lee weight** on $\mathbb{Z}_4$ is the function $\omega_{\mathrm{Lee}} : \mathbb{Z}_4 \to \{0,1,2\} \subseteq \mathbb{N}$ defined by $\omega_{\mathrm{Lee}}(0) := 0$, $\omega_{\mathrm{Lee}}(1) = \omega_{\mathrm{Lee}}(3) := 1$ and $\omega_{\mathrm{Lee}}(2) := 2$. See [60] and [47] or Chapter 12 of [51] and the references within. Denote by σ be the chain support on $\mathbb{Z}_4$ associated to the chain $\{0\} \subsetneq \mathbb{Z}_2 \subsetneq \mathbb{Z}_4$. Then $\omega_{\mathrm{Lee}} \sim \omega_\sigma$. Let $\zeta \in \mathbb{C}$ be a primitive fourth root of unity. Define the map $\psi : \mathbb{Z}_4 \to \hat{\mathbb{Z}}_4$ by $\psi(a)(b) := \zeta^{ab}$ for all $a, b \in \mathbb{Z}_4$. Then ψ is a group isomorphism, and it is natural to define the **Lee weight** on $\hat{\mathbb{Z}}_4$ by $\omega_{\mathrm{Lee}}^* := \omega_{\mathrm{Lee}} \circ \psi^{-1}$. A direct computation shows $\omega_\sigma = \omega_{\sigma^*} \circ \psi$, and therefore $\omega_{\mathrm{Lee}}^* = \omega_{\mathrm{Lee}} \circ \psi^{-1} \sim \omega_\sigma \circ \psi^{-1} = \omega_{\sigma^*} \circ \psi \circ \psi^{-1} = \omega_{\sigma^*}$. Thus the Krawtchouk coefficients associated to $(\omega_{\mathrm{Lee}}, \omega_{\mathrm{Lee}}^*)$ are the same as the Krawtchouk coefficients associated to $(\omega_\sigma, \omega_{\sigma^*})$, up to a permutation. They can be explicitly computed combining Example 7.26 and Theorem 7.28 as follows. We write K_{Lee} for $K(\omega_{\mathrm{Lee}}, \omega_{\mathrm{Lee}}^*)$.

$$\begin{array}{lll} K_{\mathrm{Lee}}(0,0) = 1 & K_{\mathrm{Lee}}(0,1) = 2 & K_{\mathrm{Lee}}(0,2) = 1 \\ K_{\mathrm{Lee}}(1,0) = 1 & K_{\mathrm{Lee}}(1,1) = 0 & K_{\mathrm{Lee}}(1,2) = -1 \\ K_{\mathrm{Lee}}(2,0) = 1 & K_{\mathrm{Lee}}(2,1) = -2 & K_{\mathrm{Lee}}(2,2) = 1. \end{array}$$

Proposition 7.11 also allows to compute the Krawtchouk coefficients for the **symmetrized Lee weight** on the product group $\mathbb{Z}_4^n$, for $n \geq 1$.

Example 7.39 (Homogeneous weight on certain Frobenius rings)**.** We denote the socle and the Jacobson radical of a finite (possibly non-commutative) Frobenius ring R by $\mathrm{soc}(R)$ and $\mathrm{rad}(R)$, respectively. See Chapter 6 of [59] for the main properties of Frobenius rings, or [45] and [44] for a more coding-theoretic approach. It is known that $\mathrm{rad}(R)$ is a two-sided ideal, and that $\mathrm{soc}(R) \cong R/\mathrm{rad}(R)$ as rings. Moreover, if R is local, i.e., $\mathrm{rad}(R)$ is the unique maximal left and right ideal of R, then $R/\mathrm{rad}(R)$ is a field, called the **residue field**.

Let $R := R_1 \times R_2 \times \cdots \times R_n$, where each R_i is a finite local Frobenius ring with residue field $R/\mathrm{rad}(R_i) \cong \mathrm{soc}(R_i)$ of order q. Then R is Frobenius with $\mathrm{soc}(R) = \prod_{i=1}^n \mathrm{soc}(R_i)$. The values of the **homogeneous weight** $\omega_{\mathrm{hom}} : R \to \mathbb{R}$ (see [16], [45], and [50]) on R were explicitly computed in [44], Proposition 3.8, as

$$\omega_{\mathrm{hom}}(a) = \begin{cases} 1 - \left(\frac{-1}{q-1}\right)^{\mathrm{wt}(a)} & \text{if } a \in \mathrm{soc}(R) \\ 1 & \text{otherwise,} \end{cases}$$

where $\mathrm{wt}(a) := |\{1 \leq i \leq n : a_i \neq 0\}|$ is the Hamming weight of $a = (a_1, ..., a_n)$.

From now on we assume $q \geq 3$. In particular, we have $\omega_{\mathrm{hom}}(a) = 0$ if and only if $a = 0$. Let $[n+1] := \{1, ..., n+1\}$ and $L := \{S \subseteq [n+1] : n+1 \notin S\} \cup \{[n+1]\}$. Then $\mathcal{L} = (L, \subseteq, \cap, \cup)$ is a regular lattice of rank $n+1$, where the rank function is given by the cardinality of sets. It is easy to see that the parameters of $\mathcal{L}$ are, for all $0 \leq s, t \leq n+1$,

$$\mu_{\subseteq}(s,t) = \begin{cases} \binom{t}{s} & \text{if } s \leq t \leq n \\ \binom{n}{s} & \text{if } s \leq n, t = n+1 \\ 1 & \text{if } s = t = n+1 \\ 0 & \text{if } s > t, \end{cases} \qquad \mu_{\supseteq}(s,t) = \begin{cases} \binom{n-t}{s-t} & \text{if } t \leq s \leq n \\ 1 & \text{if } t \leq s = n+1 \\ 0 & \text{if } s < t, \end{cases}$$

$$\mu_{\mathcal{L}}(s,t) = \begin{cases} (-1)^{t-s} & \text{if } s \leq t \leq n \\ 0 & \text{if } t < s, \text{ or } t = n+1 \text{ and } s < n \\ -1 & \text{if } t = n+1, s = n. \end{cases}$$

The formula for $\mu_{\mathcal{L}}(s,t)$ can be proved by induction on $t - s$ using the Binomial Theorem, as in Example 7.34. Define $\sigma : R \to L$ by $\sigma(a) := [n+1]$ if $a \notin \mathrm{soc}(R)$, and $\sigma(a) := \{1 \leq i \leq n : a_i \neq 0\}$ if $a \in \mathrm{soc}(R)$. One can check that $\sigma : R \dashrightarrow \mathcal{L}$ is a regular support with

$$\gamma_\sigma(s) = \begin{cases} q^s & \text{if } s \leq n \\ |R| & \text{if } s = n+1 \end{cases}$$

for all $0 \leq s \leq n+1$. Moreover, $\omega_\sigma \sim \omega_{\mathrm{hom}}$. By Definition 7.5 and Proposition 7.30, in the language of [43] we have

$$\mathcal{P}(\omega_{\mathrm{hom}}) = \mathcal{P}(\omega_\sigma), \qquad \widehat{\mathcal{P}(\omega_{\mathrm{hom}})} = \mathcal{P}(\omega_{\sigma^*}).$$

Thus the Krawtchouk matrix $\mathbf{K}$ associated to the homogeneous weight partition (see Section 4 of [44]) is given by

$$\mathbf{K}_{ij} := K(\omega_{\sigma^*}, \omega_\sigma)(i,j) \tag{7.7}$$

for all $0 \leq i, j \leq 2$. Notice that $\mathbf{K}$ is defined up to a permutation of rows and columns. With the aid of Theorem 7.28, for $n = 1$ one obtains

$$\mathbf{K} = \begin{bmatrix} 1 & q-1 & |R|-q \\ 1 & q-1 & -q \\ 1 & -1 & 0 \end{bmatrix}.$$

The same matrix appears in [44], and in [11] for $R = \mathbb{Z}_8$. To the extent of our knowledge the general formula that one obtains combining equation (7.7) and Theorem 7.28 is new. Notice moreover that $\mathcal{L}$ is modular, and so Proposition 7.32 shows that ω_σ induces a distance function on R.

For simpler Frobenius rings we can express the homogeneous weight via a suitable chain support on the ring. For example, the homogeneous weight on a finite local Frobenius ring R is equivalent to the chain support associated to the chain $0 \subsetneq \mathrm{soc}(R) \subsetneq R$ (see [9] or [44] for the values of the homogeneous weight defined on these rings).

7.6 Optimality

In this section we study subsets $\mathcal{C} \subseteq G$ that are not necessarily subgroups of G. We consider a slightly more general setting than that we investigated in the previous sections, relaxing the definition of regular support (see the following Notation 7.40). We first establish a Singleton-like bound for subsets $\mathcal{C} \subseteq G$, and call optimal those attaining the bound. We show that if $\mathcal{C}$ is an optimal set, then the distance distribution of $\mathcal{C}$ and the weight distribution of any translate of $\mathcal{C}$ can be expressed in terms of certain combinatorial invariants. In the context of rank-metric codes, this extends a result by Delsarte on the distance distribution of MRD codes. Finally, we show that if $\mathcal{C}$ is an optimal subgroup (i.e. an optimal code), then the dual code $\mathcal{C}^*$ is optimal as well.

Notation 7.40. Throughout this section, $(G, +)$ is a finite abelian group, and $\mathcal{L} = (L, \leq, \wedge, \vee)$ denotes a finite graded lattice of rank r that satisfies property (a) of Definition 7.15. Moreover, $\sigma : G \to L$ is a function that satisfies properties (A), (B), (C) and (E) of Definition 7.20. We denote by $\omega : G \to \{0, ..., r\}$ the function defined by $\omega(g) := \rho_{\mathcal{L}}(\sigma(g))$ for all $g \in G$. We follow the notation of the previous sections, unless specified differently.

In the following we investigate combinatorial properties of subsets $\mathcal{C} \subseteq G$ that are not necessarily subgroups of G.

Definition 7.41. Let $\mathcal{C} \subseteq G$ be any subset with $|\mathcal{C}| \geq 2$. The **minimum weight** and the **minimum distance** of $\mathcal{C}$ are, respectively,

$$w_\omega(\mathcal{C}) := \min\{\omega(g) : g \in \mathcal{C},\ g \neq 0\}, \qquad d_\omega(\mathcal{C}) := \min\{\omega(g - g') : g, g' \in \mathcal{C},\ g \neq g'\}.$$

The **weight** and **distance distributions** of $\mathcal{C}$ are the collections $\{W_i(\mathcal{C}, \omega) : i = 0, ..., r\}$ and $\{D_i(\mathcal{C}, \omega) : i = 0, ..., r\}$ respectively, where

$$W_i(\mathcal{C}, \omega) := |\{g \in \mathcal{C} : \omega(g) = i\}|, \qquad D_i(\mathcal{C}, \omega) := \frac{1}{|\mathcal{C}|}\ |\{(g, g') \in \mathcal{C} \times \mathcal{C} : \omega(g - g') = i\}|$$

for all $i \in \{0, ..., r\}$.

Notice that the map $G \times G \to \{0, ..., r\}$ given by $(g, g') \mapsto \omega(g - g')$ does not need to be a distance function on G.

Remark 7.42. It is easy to check that if $\mathcal{C} \subseteq G$ is a subgroup (i.e., a code), then $w_\omega(\mathcal{C}) = d_\omega(\mathcal{C})$ and $W_i(\mathcal{C}, \omega) = D_i(\mathcal{C}, \omega)$ for all $i = 0, ..., r$.

We start with a Singleton-like bound.

Proposition 7.43. Let $\mathcal{C} \subseteq G$ be a subset with $|\mathcal{C}| \geq 2$. We have $|\mathcal{C}| \leq |G|/\gamma_\sigma(d_\omega(\mathcal{C}) - 1)$.

Proof. Take any $S \in L$ with $\rho_{\mathcal{L}}(S) = d_\omega(\mathcal{C}) - 1$. Such an S always exists by definition of rank of a graded poset. For all $g \in \mathcal{C}$ define

$$\overline{g} := g + G_\sigma(S) = \{g + h : h \in G_\sigma(S)\} \subseteq G.$$

By definition of minimum distance we have $\overline{g} \cap \overline{g'} = \emptyset$ for all $g, g' \in \mathcal{C}$ with $g \neq g'$. Therefore

$$|G| \geq \left| \bigcup_{g \in \mathcal{C}} \overline{g} \right| = \sum_{g \in \mathcal{C}} |\overline{g}| = \sum_{g \in \mathcal{C}} |G_\sigma(S)| = |\mathcal{C}| \cdot \gamma_\sigma(d_\omega(\mathcal{C}) - 1),$$

and the bound follows. □

Definition 7.44. A subset $\mathcal{C} \subseteq G$ is **optimal** if $|\mathcal{C}| \geq 2$ and its parameters attain the bound of Proposition 7.43.

Lemma 7.45. Let $\mathcal{C} \subseteq G$ be an optimal subset with $0 \in \mathcal{C}$. Let $S \in L$ be any lattice element with $s := \rho_{\mathcal{L}}(S) \geq d_\omega(\mathcal{C})$. Then

$$|\mathcal{C}_\sigma(S)| = \frac{|\mathcal{C}|\ \gamma_\sigma(s)}{|G|}.$$

Proof. Let $T \in L$ with $T \leq S$ and $\rho_{\mathcal{L}}(T) = d_\omega(\mathcal{C}) - 1$. Such a T always exists by definition of graded posets. We clearly have $G_\sigma(T) \subseteq G_\sigma(S)$. Define the maps

$$C \xrightarrow{\pi_1} G/G_\sigma(T) \xrightarrow{\pi_2} G/G_\sigma(S)$$

as follows. The function π_1 is the composition of the inclusion $\mathcal{C} \to G$ and the projection on the quotient group $G \to G/G_\sigma(T)$. The map π_2 is given by $g + G_\sigma(T) \mapsto g + G_\sigma(S)$, and it is a well defined group homomorphism, as $G_\sigma(T) \subseteq G_\sigma(S)$.

We claim that π_1 is a bijection. Assume that there exist $g, g' \in \mathcal{C}$ with $\pi_1(g) = \pi_1(g')$, i.e., $g + G_\sigma(T) = g' + G_\sigma(T)$. Then $g - g' \in G_\sigma(T)$ and thus $\omega(g - g') \leq \rho_{\mathcal{L}}(T) = d_\omega(\mathcal{C}) - 1$. It follows $g = g'$, i.e., π_1 is injective. Since $\mathcal{C}$ is optimal, we have $|\mathcal{C}| = |G|/\gamma_\sigma(d_\omega(\mathcal{C}) - 1) = |G|/G_\sigma(T)$, and so π_1 is a bijection, as claimed.

Since both π_1 and π_2 are surjective, the map $\pi := \pi_2 \circ \pi_1$ is surjective as well. Let now $x \in G/G(S)$ be an arbitrary element, and let $h_x \in \mathcal{C}$ with $\pi(h_x) = x$. One can check that the map $\pi^{-1}(0) \to \pi^{-1}(x)$ given by $g \mapsto g + h_x$ is a bijection. Therefore $|\pi^{-1}(0)| = |\pi^{-1}(x)|$ for all $x \in G/G_\sigma(S)$. As a consequence,

$$|\mathcal{C}| = \left| \bigcup_{x \in G/G_\sigma(S)} \pi^{-1}(x) \right| = \sum_{x \in G/G_\sigma(S)} |\pi^{-1}(x)| = \sum_{x \in G/G_\sigma(S)} |\pi^{-1}(0)| = \frac{|G|}{\gamma_\sigma(s)} \cdot |\mathcal{C}_\sigma(S)|,$$

where the last equality follows from the definition of $\mathcal{C}_\sigma(S)$. This shows the expected formula. □

Theorem 7.46. Let $\mathcal{C} \subseteq G$ be an optimal code of minimum distance $d := d_\omega(\mathcal{C})$ with $0 \in \mathcal{C}$. Define the integer matrix P of size $(r - d + 1) \times (r - d + 1)$ by $P_{ij} := \mu_{\leq}(d + i - 1, d + j - 1)$ for all $i, j \in \{1, ..., r - d + 1\}$. Then P is invertible, and the weight distribution of $\mathcal{C}$ is given by

$$W_0(\mathcal{C}, \omega) = 1, \quad W_i(\mathcal{C}, \omega) = 0 \text{ for } 1 \leq i \leq d - 1,$$

$$\begin{pmatrix} W_d(\mathcal{C}, \omega) \\ W_{d+1}(\mathcal{C}, \omega) \\ \vdots \\ W_r(\mathcal{C}, \omega) \end{pmatrix} = P^{-1} \begin{pmatrix} |\mathcal{C}|\ \mu_{\leq}(d, r)\gamma_\sigma(d)/|G| \\ |\mathcal{C}|\ \mu_{\leq}(d + 1, r)\gamma_\sigma(d + 1)/|G| \\ \vdots \\ |\mathcal{C}|\ \mu_{\leq}(r, r)\gamma_\sigma(r)/|G| \end{pmatrix}.$$

In particular, the weight distribution of $\mathcal{C}$ only depends on $|G|$, $d_\omega(\mathcal{C})$, and on the combinatorial invariants of $\mathcal{L}$ and σ.

Proof. Take any $s \in \{d, ..., r\}$, and write $d := d_\omega(\mathcal{C})$. We will count the elements of the set

$$\mathcal{A} := \{(g, S) : g \in \mathcal{C},\ S \in \mathcal{L},\ \rho_{\mathcal{L}}(S) = s,\ \sigma(g) \leq S\}$$

in two different ways. On the one hand, by Lemma 7.45 we have

$$|\mathcal{A}| = \sum_{\substack{S \in L \\ \rho_{\mathcal{L}}(S) = s}} |\mathcal{C}_\sigma(S)| = \mu_{\leq}(s, r)\ \frac{|\mathcal{C}|\ \gamma_\sigma(s)}{|G|}.$$

On the other hand, by definition,

$$|\mathcal{A}| = \sum_{i=d}^{s} \sum_{\substack{g \in \mathcal{C} \\ \omega(g) = i}} |\{S \in L : \sigma(g) \leq S\}| = \sum_{i=d}^{s} W_i(\mathcal{C}, \omega)\ \mu_{\geq}(s, i).$$

Therefore for all $s \in \{d, ..., r\}$ we have

$$\sum_{i=d}^{s} W_i(\mathcal{C}, \sigma)\ \mu_{\geq}(s, i)\ =\ \mu_{\leq}(s, r)\ \frac{|\mathcal{C}|\ \gamma_\sigma(s)}{|G|}.$$

This corresponds to a system of $r - d + 1$ linear equations in the unknowns $W_d(\mathcal{C}, \omega), ..., W_r(\mathcal{C}, \omega)$. The matrix of the system is precisely P, which is invertible because lower triangular with all ones on the diagonal. The result follows. □

Recall that if $\mathcal{C} \subseteq G$ is any subset and $h \in G$, then the **translate** of $\mathcal{C}$ by h is the set $\mathcal{C}_h := \{g - h : g \in \mathcal{C}\}$.

Corollary 7.47. Let $\mathcal{C} \subseteq G$ be an optimal code of minimum distance $d := d_\omega(\mathcal{C})$. Then for all $h \in \mathcal{C}$ we have $W_i(\mathcal{C}_h, \omega) = D_i(\mathcal{C}, \omega)$ for $i \in \{0, ..., r\}$. Moreover, the distance distribution of $\mathcal{C}$ is given by

$$D_0(\mathcal{C}, \omega) = 1, \quad D_i(\mathcal{C}, \omega) = 0 \text{ for } 1 \leq i \leq d - 1,$$

$$\begin{pmatrix} D_d(\mathcal{C}, \omega) \\ D_{d+1}(\mathcal{C}, \omega) \\ \vdots \\ D_r(\mathcal{C}, \omega) \end{pmatrix} = P^{-1} \begin{pmatrix} |\mathcal{C}|\ \mu_{\leq}(d, r)\gamma_\sigma(d)/|G| \\ |\mathcal{C}|\ \mu_{\leq}(d+1, r)\gamma_\sigma(d+1)/|G| \\ \vdots \\ |\mathcal{C}|\ \mu_{\leq}(r, r)\gamma_\sigma(r)/|G| \end{pmatrix},$$

where P is the matrix defined in Theorem 7.46.

Proof. For all integers $i \in \{0, ..., r\}$ one has

$$\begin{aligned} D_i(\mathcal{C}, \omega) &= \frac{1}{|\mathcal{C}|}\ |\{(g, g') \in \mathcal{C} \times \mathcal{C} : \omega(g - g') = i\}| \\ &= \frac{1}{|\mathcal{C}|} \sum_{g' \in \mathcal{C}} |\{g \in \mathcal{C} : \omega(g - g') = i\}| \\ &= \frac{1}{|\mathcal{C}|} \sum_{g' \in \mathcal{C}} |\{g \in \mathcal{C}_{g'} : \omega(g) = i\}| \\ &= \frac{1}{|\mathcal{C}|} \sum_{g' \in \mathcal{C}} W_i(\mathcal{C}_{g'}, \omega). \end{aligned}$$

Let $h \in \mathcal{C}$ be any code element. It is easy to see that the translate $\mathcal{C}_h$ has the same distance distribution as $\mathcal{C}$. In particular, $\mathcal{C}_h$ is optimal. Moreover, since $0 \in \mathcal{C}_h$, its weight distribution is given by Theorem 7.46, and it does not depend in $h \in \mathcal{C}$. Therefore for all $h \in \mathcal{C}$ and $i \in \{0, ..., r\}$ we have

$$D_i(\mathcal{C}, \omega) = \frac{1}{|\mathcal{C}|} \cdot |\mathcal{C}| \cdot W_i(\mathcal{C}_h, \omega) = W_i(\mathcal{C}_h, \omega).$$

This proves the corollary. □

Remark 7.48. In the context of codes endowed with the rank metric, Corollary 7.47 generalizes Theorem 5.6 of [20] on the distance distribution of an MRD code.

We conclude this section showing that if $\mathcal{C}$ is an optimal code (and thus a subgroup of G), and σ also satisfies property (D) of Definition 7.20, then the dual of $\mathcal{C}$ is an optimal code as well.

Lemma 7.49. Let $\mathcal{C} \subseteq G$ be a code, and assume that σ satisfies property (D) of Definition 7.20. Take any $S \in L$, and let $s := \rho_{\mathcal{L}}(S)$. Then

$$|\mathcal{C}_\sigma(S)| = \frac{|\mathcal{C}| \cdot |\mathcal{C}^*_{\sigma^*}(S)|}{\gamma_{\sigma^*}(r-s)}.$$

Proof. By definition, $\mathcal{C}_\sigma(S) = G_\sigma(S) \cap \mathcal{C}$, and Remark 7.2 implies

$$|\mathcal{C}_\sigma(S)| = \frac{|G_\sigma(S)| \cdot |\mathcal{C}|}{|G_\sigma(S) + \mathcal{C}|} = \frac{|G_\sigma(S)| \cdot |\mathcal{C}| \cdot |(G_\sigma(S) + \mathcal{C})^*|}{|G|}. \tag{7.8}$$

Again by Remark 7.2 we have $|(G_\sigma(S) + \mathcal{C})^*| = |G_\sigma(S)^* \cap \mathcal{C}^*| = |\hat{G}_{\sigma^*}(S) \cap \mathcal{C}^*|$, where the last equality follows from Theorem 7.24. Since $\hat{G}_{\sigma^*}(S) \cap \mathcal{C}^* = \mathcal{C}^*_{\sigma^*}(S)$ by definition, equation (7.8) can be written as

$$|\mathcal{C}_\sigma(S)| = \frac{|G_\sigma(S)| \cdot |\mathcal{C}| \cdot |\mathcal{C}^*_{\sigma^*}(S)|}{|G|}.$$

The result now follows from the fact that $|G|/|G_\sigma(S)| = |G|/\gamma_\sigma(s) = \gamma_{\sigma^*}(r-s)$, again by Theorem 7.24. □

Theorem 7.50. Let $\mathcal{C} \subseteq G$ be a non-trivial optimal code, and assume that σ satisfies property (D) of Definition 7.20. Then $d_{\omega_{\sigma^*}}(\mathcal{C}^*) \geq r - d_{\omega_\sigma}(\mathcal{C}) + 2$, and the code $\mathcal{C}^*$ is optimal.

Proof. Let $d := d_{\omega_\sigma}(\mathcal{C})$ and $d^* := d_{\omega_{\sigma^*}}(\mathcal{C}^*)$. Since $\mathcal{C}$ is optimal, we have $|\mathcal{C}| = |G|/\gamma_\sigma(d-1)$. Remark 7.2 and Theorem 7.24 imply

$$|\mathcal{C}^*| = \gamma_\sigma(d-1) = |\hat{G}|/\gamma_{\sigma^*}(r-d+1). \tag{7.9}$$

Let $S \in L$ be any element with $\rho_{\mathcal{L}^*}(S) = r - d + 1$. Then $\rho_{\mathcal{L}}(S) = r - (r-d+1) = d-1$, and so $\mathcal{C}_\sigma(S) = \{0\}$. Lemma 7.49 gives

$$|\mathcal{C}^*_{\sigma^*}(S)| = \frac{|\mathcal{C}_\sigma(S)| \cdot \gamma_{\sigma^*}(r-d+1)}{|\mathcal{C}|} = 1,$$

where the last equality easily follows from equation (7.9) and Remark 7.2. Thus $\mathcal{C}^*_{\sigma^*}(S) = \{0\}$, and so the minimum weight of $\mathcal{C}^*$ satisfies $d^* \geq r - d + 2$. In particular, $\gamma_{\sigma^*}(d^*-1) \geq \gamma_{\sigma^*}(r-d+1)$. Therefore combining Proposition 7.43 applied to $\mathcal{C}^*$ and σ^* with equation (7.9) we obtain

$$\frac{|\hat{G}|}{\gamma_{\sigma^*}(r-d+1)} \geq \frac{|\hat{G}|}{\gamma_{\sigma^*}(d^*-1)} \geq |\mathcal{C}^*| = \frac{|\hat{G}|}{\gamma_{\sigma^*}(r-d+1)}.$$

It follows $|\mathcal{C}^*| = |\hat{G}|/\gamma_{\sigma^*}(d^*-1)$, i.e., $\mathcal{C}^*$ is optimal. □

7.7 Counting symmetric and skew-symmetric matrices

We conclude this chapter mentioning a concise method to compute the number of symmetric and skew-symmetric $k \times k$ matrices of given rank over $\mathbb{F}_q$. Different formulas for the same numbers were given by Carlitz and MacWilliams (see [12], [13], [65]) using sophisticated recursive methods. Our technique is very straightforward, and based on the Möbius inversion formula and the regularity of the lattice of subspaces of $\mathbb{F}_q^k$, which we denote by $\mathcal{L}$ in the sequel. We follow the notation of Example 7.37.

Recall that a $k \times k$ matrix M is **symmetric** if $M_{ij} = M_{ji}$ for all $1 \leq i, j \leq k$ and **skew-symmetric** if $M_{ii} = 0$ and $M_{ij} = -M_{ji}$ for all $1 \leq i, j \leq k$. We denote by Sym and s-Sym the spaces of $k \times k$ symmetric and skew-symmetric matrices over $\mathbb{F}_q$, respectively.

Lemma 7.51. Let $S \subseteq \mathbb{F}_q^k$ be any s-dimensional subspace. Then $\{M \in \text{Sym} : \sigma_{\text{rk}}(M) \subseteq (S)\}$ is a vector space of dimension $s(s+1)/2$ over $\mathbb{F}_q$.

Proof. Define $V := \{x \in \mathbb{F}_q^k : x_i = 0 \text{ for } i > s\} \subseteq \mathbb{F}_q^k$. There exists an $\mathbb{F}_q$-isomorphism $g : \mathbb{F}_q^k \to \mathbb{F}_q^k$ such that $g(S) = V$. Let $G \in \text{GL}_k(\mathbb{F}_q)$ be the matrix associated to g with respect to the canonical basis $\{e_1, ..., e_k\}$ of $\mathbb{F}_q^k$. Since G is invertible, $M \mapsto GMG^t$ is an $\mathbb{F}_q$-linear automorphism of Sym that preserves the rank support of matrices. As a consequence,

$$\dim(\{M \in \text{Sym} : \sigma_{\text{rk}}(M) \subseteq S\}) = \dim(\{M \in \text{Sym} : \sigma_{\text{rk}}(M) \subseteq V\}) = s(s+1)/2,$$

as claimed. □

We can now compute the number of symmetric $k \times k$ matrices over $\mathbb{F}_q$ of rank i as follows. For any subspace $T \subseteq \mathbb{F}_q^k$ define $f(T) := |\{M \in \text{Sym} : \sigma_{\text{rk}}(M) = T\}|$ and $g(T) := \sum_{S \subseteq T} f(S)$. By Lemma 7.51, for all $S \subseteq \mathbb{F}_q^k$ we have $g(S) = q^{s(s+1)}$, where $s := \dim(S)$. Therefore applying the Möbius inversion formula ([87], Proposition 3.7.1) to the functions f and g we obtain, for any given i-dimensional subspace $T \subseteq \mathbb{F}_q^k$,

$$f(T) \;=\; \sum_{S \subseteq T} g(S)\; \mu_{\mathcal{L}}(S,T) \;=\; \sum_{s=0}^{k} \sum_{\substack{S \subseteq T \\ \dim(S)=s}} q^{s(s+1)}\; \mu_{\mathcal{L}}(s,i) \;=\; \sum_{s=0}^{k} q^{\binom{s+1}{2}} \begin{bmatrix} i \\ s \end{bmatrix} (-1)^{i-s} q^{\binom{i-s}{2}}.$$

The expected result is now obtained summing over all the i-dimensional subspaces $T \subseteq \mathbb{F}_q^k$. A similar argument applies to skew-symmetric matrices. The final result is the following.

Proposition 7.52. The number of symmetric and skew-symmetric $k \times k$ matrices over $\mathbb{F}_q$ of rank i is, respectively,

$$\begin{bmatrix} k \\ i \end{bmatrix} \sum_{s=0}^{k} (-1)^{i-s} q^{\binom{s+1}{2}+\binom{i-s}{2}} \begin{bmatrix} i \\ s \end{bmatrix}, \qquad \begin{bmatrix} k \\ i \end{bmatrix} \sum_{s=0}^{k} (-1)^{i-s} q^{\binom{s}{2}+\binom{i-s}{2}} \begin{bmatrix} i \\ s \end{bmatrix}.$$

One can also observe that the spaces of $k \times k$ symmetric and skew-symmetric matrices over $\mathbb{F}_q$ are orthogonal to each other. Therefore the rank distributions of symmetric and skew-symmetric matrices are related by a MacWilliams transformation. More precisely, the following hold.

Corollary 7.53. For all integers $0 \leq j \leq k$ we have

$$W_j(\text{Sym}, \omega_{\text{rk}}) = q^{-\binom{k}{2}} \sum_{i=0}^{k} W_i(\text{s-Sym}, \omega_{\text{rk}}) \sum_{s=0}^{k} (-1)^{j-s}\; q^{ms+\binom{j-s}{2}} \begin{bmatrix} k-s \\ k-j \end{bmatrix} \begin{bmatrix} k-i \\ s \end{bmatrix}.$$

Bibliography

[1] R. Ahlswede, N. Cai, S.-Y.R. Li, R.W. Yeung, *Network information flow*. IEEE Transactions on Information Theory 46 (2000), 4, pp. 1204 – 1216.

[2] G. E. Andrews, *The Theory of Partitions*. Encyclopedia of Mathematics and its Applications, vol. 2, G.C. Rota Editor. Addison-Wesley, 1976.

[3] E. A. Bender, *On Buckhiesters enumeration of $n \times n$ matrices*. Journal of Combinatorial Theory, Series A, 17 (1974), pp. 273 – 274.

[4] A. Beutelspacher, *On t-covers in Finite Projective Spaces*. Journal of Geometry 12 (1979), 1, pp. 10 – 16.

[5] A. Beutelspacher, *Partial Spreads in Finite Projective Spaces and Partial Designs*. Mathematische Zeitschrift 145 (1975), pp. 211 – 230.

[6] A. Beutelspacher, J. Eisfeld, J. Müller, *On Sets of Planes in Projective Spaces Intersecting Mutually in One Point*. Geometriae Dedicata 78 (1999), pp. 143-159.

[7] A. Beutelspacher, U. Rosenbaum, *Projective Geometry: From Foundations to Applications*. Cambridge University Press (1998).

[8] P. G. Buckhiester, *The number of $n \times n$ matrices of rank r and trace α over a finite field*. Duke Mathematical Journal, 39 (1972), pp. 695 – 699.

[9] E. Byrne, *On the weight distribution of codes over finite rings*. Advances in Mathematics of Communications, 5 (2011), pp. 395 –406.

[10] E. Byrne, M. Greferath, M. E. O'Sullivan, *The linear programming bound for codes over finite Frobenius rings*. Designs, Codes and Cryptography, 42 (2007), pp. 289 – 301.

[11] P. Camion, *Codes and association schemes*. In V. S. Pless and W. C. Huffman (editors), Handbook of Coding Theory, Vol. II, pp. 1441 – 1566. Elsevier (1998).

[12] L. Carlitz, *Representations by quadratic forms in a finite field*. Duke Mathematical Journal, 21 (1954), pp. 123 – 137.

[13] L. Carlitz, *Representations by skew forms in a finite field*. Archiv der Mathematik, 5 (1954), pp. 19 – 31.

[14] Cisco Whitepaper 2016, *Visual Networking Index: Global IP Traffic Forecast, 2015 –2020*.

[15] A. Conca, E. De Negri, E. Gorla, *Universal Gröbner bases for maximal minors*. International Mathematics Research Notices, 11 (2015), pp. 3245–3262.

[16] I. Constantinescu, W. Heise, *A metric for codes over residue class rings*. Problems on Informormation Transmission, 33 (1997), pp. 208 –213.

[17] T. M. Cover, J. A. Thomas, *Elements of Information Theory*, second edition. Wiley-Interscience 2006.

[18] J. de la Cruz, E. Gorla, H. Lopez, A. Ravagnani, *Rank distribution of Delsarte codes*. Submitted.

[19] P. Delsarte, *Association schemes and t-designs in regular semilattices*. Journal of Combinatorial Theory, Series A, 2 (1976), 2, pp. 230 – 243.

[20] P. Delsarte, *Bilinear forms over a finite field, with applications to coding theory*. Journal of Combinatorial Theory, Series A, 25 (1978), 3, pp. 226 – 241.

[21] M. Deza, *Une propriété extrémale des plans projectifs finis dans une classe de codes equidistants*. Discrete Mathematics, 6 (1973), pp. 343 – 352.

[22] M. Deza, P. Frankl, *Every large set of equidistant* $(0, +1, -1)$*-vectors forms a sunflower*. Combinatorica, 1 (1981), pp. 225 – 231.

[23] D. A. Drake, J. W. Freeman, *Partial t-spreads and group constructible* (s, r, μ)*-nets*. Journal of Geometry 13 (1979), 2, pp. 210 – 216.

[24] J.-G. Dumas, R. Gow, G. McGuire, J. Sheekey, *Subspaces of matrices with special rank properties*. Linear Algebra and its Applications, 433 (2010), 1, pp. 191 – 202.

[25] J. Ducoat, *Generalized rank weights : a duality statement*. Online preprint: `http://arxiv.org/abs/1306.3899`.

[26] S. El-Zenati, H. Jordon, G. Seelinger, P. Sissokho, L. Spence, *The maximum size of a partial* 3*-spread in a finite vector space over* $GF(2)$. Designs Codes and Cryptography 54 (2010), pp. 101 – 107.

[27] T. Etzion, E. Gorla, A. Ravagnani, E. Wachter-Zeh, *Optimal Ferrers Diagram Rank-Metric Codes*. IEEE Transactions on Information Theory, 64 (2016), n. 4, pp. 1616 – 1630.

[28] T. Etzion, N. Raviv, *Equidistant codes in the Grassmannian*. Discrete Applied Mathematics 186 (2015), pp. 87–97.

[29] T. Etzion, N. Silberstein, *Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams*. IEEE Transactions on Information Theory 55 (2009), 7, pp. 2909 – 2919.

[30] T. Etzion, A. Vardy, *Error-correcting codes in projective space*. IEEE International Symposium on Information Theory 2008, pp. 871 – 875.

[31] T. Etzion, A. Vardy, *Error-Correcting Codes in Projective Space*. IEEE Transactions on Information Theory 57 (2011), 2, pp. 1165 – 1173.

[32] E. Gabidulin *Theory of codes with maximum rank distance*. Problems of Information Transmission, 1 (1985), 2, pp. 1 – 12.

[33] M. Gadouleau, Z. Yan *MacWilliams Identities for the Rank Metric*. ISIT 2007 (Nice, France), pp. 36 – 40.

[34] M. Gadouleau, Z. Yan, *MacWilliams identity for Codes with the Rank Metric*. EURASIP Journal on Wireless Communications and Networking, 2008.

[35] M. Giorgetti, A. Previtali, *Galois invariance, trace codes and subfield subcodes*. Finite Fields and Their Applications, 16 (2010), 2, pp. 96 – 99.

[36] M. Giusti, M. Merle, *Sections des variétés déterminantielles par les plans de coordonnées*. Proc. Int. Conf. on Algebraic Geometry (La Rabida 1981, Spain), Lecture Notes in Mathematics (1982), vol 961, pp. 103–118.

[37] E. Gorla, A. Ravagnani, *Partial Spreads in Random Network Coding*. Finite Fields and Their Applications, 26 (2014), pp. 104 – 115.

[38] E. Gorla, A. Ravagnani, *Subspace codes from Ferrers diagrams*. Journal of Algebra and Its Applications (to appear).

[39] E. Gorla, A. Ravagnani, *Equidistant subspace codes*. Linear Algebra and its Applications, 490 (2016), pp. 48 65.

[40] E. Gorla, F. Manganiello, J. Rosenthal, *An Algebraic Approach for Decoding Spread Codes*. Advances in Mathematics of Communications 6 (2012), 4, pp. 443 – 466.

[41] D. Grant, M. Varanasi, *Duality theory for space-time codes over finite fields*. Advances in Mathematics of Communications, 2 (2005), 1, pp. 35 – 54.

[42] O. Heden, J. Lehmann, E. Năstase, P. Sissokho, *Extremal sizes of subspaces partitions*. Designs Codes and Cryptography 64 (2012), pp. 265 – 274.

[43] H. Gluesing-Luerssen, *Fourier-reflexive partitions and MacWilliams identities for additive codes*. Designs, Codes and Cryptography, 75 (2015), pp. 543 – 563.

[44] H. Gluesing-Luerssen, *Partitions of Frobenius rings induced by the homogeneous weight*. Advances in Mathematics of Communications, 8 (2014), pp. 191 – 207.

[45] M. Greferath, S. Schmidt, *Finite ring combinatorics and MacWilliams' Equivalence Theorem*. Journal of Combinatorial Theory, 92A (2000), pp. 17 – 28.

[46] J. Haglund, *q-rook polynomials and matrices over finite fields*. Advances in Applied Mathematics, 20 (1998), 4, pp. 450 – 487.

[47] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P.Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*. IEEE Transactions on Information Theory, 40 (1994), pp. 301 – 319.

[48] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields* (second edition). Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York (1998).

[49] T. Ho, M. Médard, R. Kötter, D. R. Karger, M. Effros, J. Shi, and B. Leong, *A random linear network coding approach to multicast*. IEEE Transactions on Information Theory, 52 (2006), pp. 4413 – 4430.

[50] T. Honold, I. Landjev, *MacWilliams identities for linear codes over finite Frobenius rings*. In D. Jungnickel and H. Niederreiter, editors, *Proceedings of The Fifth International Conference on Finite Fields and Applications Fq5*, Augsburg, 1999, pp. 276 – 292. Springer 2001.

[51] W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge University Press (2003).

[52] A. J. Klein, J. B. Lewis, A. H. Morales, *Counting matrices over finite fields with support on*

skew Young diagrams and complements of Rothe diagrams. Journal of Algebraic Combinatorics, 39 (2014), 2, pp. 429 – 456.

[53] A. Kohnert, S. Kurz, *Construction of Large Constant Dimension Codes with a Prescribed Minimum Distance*. Mathematical Methods in Computer Science, Lecture Notes in Computer Science (2008), vol. 5393, pp. 31 – 42.

[54] R. Kötter, F. R. Kschischang, *Coding for Errors and Erasures in Random Network Coding*. IEEE Transactions on Information Theory, 54 (2008), 8, pp. 3579 – 3591.

[55] R. Kötter, F. R. Kschischang, D. Silva, *A Rank-Metric Approach to Error Control in Random Network Coding*. IEEE Information Theory Workshop on Information Theory for Wireless Networks (2007).

[56] R. Kötter and M. Médard, *An algebraic approach to network coding*. IEEE/ACM Transactions on Networking, vol. 11 (2003), pp. 782 – 795.

[57] J. Kurihara, R. Matsumoto, T. Uyematsu, *Relative Generalized Rank Weight of Linear Codes and Its Applications to Network Coding*. IEEE Transactions on Information Theory, 61 (2015), 7, pp. 3912 – 3936.

[58] Intel®, *What Happens in an Internet Minute?* `http://www.intel.com/content/www/us/en/communications/internet-minute-infographic.html`

[59] T. Y. Lam, *Lectures on Modules and Rings*. Graduate Text in Mathematics, vol. 189. Springer 1999.

[60] C. Lee, *Some properties of nonbinary error-correcting codes*. IRE Transactions on Information Theory, 4 (1958), 2, pp. 77-82.

[61] J. B. Lewis, R. Liu, G. Panova, A. H. Morales, S. V Sam, Y. X. Zhang, *Matrices with restricted entries and q-analogues of permutations*. Journal of Combinatorics 2 (2012), 3, pp. 355 –396.

[62] S.-Y.R. Li, R.W. Yeung, N. Cai, *Linear network coding*. IEEE Transactions on Information Theory, 49 (2003), 2, pp. 371 – 381.

[63] R. Lidl, H. Niederreiter, *Finite Fields*. Addison-Wesley Publishing Company (1983).

[64] J. H. van Lint, *Introduction to Coding Theory*, third edition. Springer (1999).

[65] F. J. MacWilliams, *Orthogonal matrices over finite fields*. American Mathematical Monthly, 76 (1969), pp. 152 – 164.

[66] R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*. Cambridge University Press (1986).

[67] F. J. MacWilliams, *A Theorem on the Distribution of Weights in a Systematic Code*. Bell System Technical Journal, 42 (1963), 1, pp. 79 – 94.

[68] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North Holland Mathematical Library.

[69] M. Médard, A. Sprintson (eds.), *Network Coding: Fundamentals and Applications*. Elsevier 2012.

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

[71] F. Manganiello, E. Gorla, J. Rosenthal, *Spread Codes and Spread Decoding in Network Coding*. IEEE Proceedings (Toronto 2008), pp. 881 – 885.

[72] C. D. Meyer, *Matrix Analysis and Applied Linear Algebra*. SIAM (2000).

[73] OECD Digital Economy Outlook 2015, available on the website of the European Commission at `http://ec.europa.eu/eurostat/documents/42577/3222224/Digital+economy+outlook+2015/dbdec3c6-ca38-432c-82f2-1e330d9d6a24`.

[74] F. Oggier, A. Sboui, *On the Existence of Generalized Rank Weights*. IEEE International Symposium on Information Theory and its Applications (2012).

[75] L. H. Ozarow, A. D. Wyner, *Wire-tap-channel II*. Bell Labs Technical Journal, 63 (1984), pp. 2135 – 2157.

[76] M. Pedersen, F. Fitzek, T. Larsen, *Implementation and Performance Evaluation of Network Coding for Cooperative Mobile Devices*. IEEE International Conference on Communications (2008).

[77] A. Ravagnani, *Rank-metric codes and their duality theory*. Designs, Codes and Cryptography, 80 (2016), n. 1, pp. 197–216.

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

[79] A. Ravagnani, *Duality of codes supported on regular lattices, with an application to enumerative combinatorics*. Submitted. Online preprint: `http://arxiv.org/abs/1510.02383`.

[80] R. M. Roth, *Maximum-rank array codes and their application to crisscross error correction*. Transactions on Information Theory, 37 (1991), 2, pp. 328 –336.

[81] C. de Seguins Pazzis, *The classification of large spaces of matrices with bounded rank*. Israel Journal of Mathematics, 208 (2015), 1, pp. 219 – 259.

[82] N. Silberstein, A.-L. Trautmann, *New lower bounds for constant dimension codes*. ISIT 2013, pp. 514 – 518.

[83] N. Silberstein, A.-L. Trautmann, *Subspace Codes based on Graph Matchings, Ferrers Diagrams and Pending Blocks* . IEEE Transactions on Information Theory, 61 (2015), 1, pp. 3937 – 3953.

[84] D. Silva, F. R. Kschischang, *On metrics for error correction in network coding*. IEEE Transactions on Information Theory, 55 (2009), 12, pp. 5479 – 5490.

[85] D. Silva, F. R. Kschischang, *Universal Secure Network Coding via Rank-Metric Codes*. IEEE Transactions on Information Theory, 57 (2011), 2, pp. 1124 – 1135.

[86] E. Spiegel, C. J. O'Donnell, *Incidence algebras*. CRC Press (1997).

[87] R. Stanley, *Enumerative combinatorics*. Cambridge University Press 1997.

[88] J.R. Stembridge, *Counting points on varieties over fnite felds related to a conjecture of Kontsevich*. Annals of Combinatorics, 2 (1998), 4, pp. 365 – 385.

[89] P. Torres Compta, F. H. P. Fitzek, D. E. Lucani, *Network coding is the 5G Key Enabling Technology: effects and strategies to manage heterogeneous packet lengths*. Transactions on Emerging Telecommunications Technologies, 26 (2015), 1, pp. 46 – 55.

[90] A-L. Trautmann, Joachim Rosenthal, *New Improvements on the Echelon-Ferrers Construction.* Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems - MTNS 2010, pp. 405 – 408.

[91] V. K. Wei, Generalized Hamming Weights for Linear Codes. IEEE Transactions on Information Theory, 37 (1991), 5, pp. 1412 – 1418.

[92] V. A. Zinoviev, T. Ericson, *Fourier invariant pairs of partitions of finite abelian groups and association schemes.* Problems of Information Transmission, 45 (2009), pp. 221 – 231.