Topics on Reliable and Secure Communication using Rank-Metric and Classical Linear Codes

Martinez Peñas, Umberto

Publication date:
2017

Document Version
Publisher's PDF, also known as Version of record

Link to publication from Aalborg University

Citation for published version (APA):
Martinez Peñas, U. (2017). *Topics on Reliable and Secure Communication using Rank-Metric and Classical Linear Codes*. Aalborg Universitetsforlag.

TOPICS ON RELIABLE AND SECURE COMMUNICATION USING RANK-METRIC AND CLASSICAL LINEAR CODES

BY
UMBERTO MARTÍNEZ-PEÑAS

DISSERTATION SUBMITTED 2017

AALBORG UNIVERSITY
DENMARK

Topics on Reliable and Secure Communication using Rank-Metric and Classical Linear Codes

Ph.D. Dissertation

Umberto Martínez-Peñas

Dissertation submitted September XX, 2017

Dissertation submitted:	September 11, 2017
PhD supervisor:	Prof. Olav Geil Aalborg University
Assistant PhD supervisor:	Assoc. Prof. Diego Ruano Aalborg University
PhD committee:	Adjunct Professor Tom Høholdt (chairman) Aalborg University
	Professor Chiaoping Xing Nanyang Technical University
	Professor Joachim Rosenthal University of Zurich
PhD Series:	Faculty of Engineering and Science, Aalborg University
Department:	Department of Mathematical Sciences

ISSN (online): 2446-1636
ISBN (online): 978-87-7210-063-0

Published by:
Aalborg University Press
Skjernvej 4A, 2nd floor
DK – 9220 Aalborg Ø
Phone: +45 99407140
aauf@forlag.aau.dk
forlag.aau.dk

Printed in Denmark by Rosendahls, 2017

Abstract

Rank-metric codes and code pairs play a central role in reliable and secure communications in different practical settings, such as linear network coding or storage systems with crisscross errors. The behaviour of rank-metric codes is in many cases analogous to that of classical codes, also referred to as Hamming-metric codes. However, there exist numerous cases where rank-metric codes present unexpected properties with no analogy in the Hamming case. In this thesis, we explore the similarities and differences between rank-metric codes and Hamming-metric codes and, from this analysis, we provide new applications in the previously mentioned settings. The results and papers in this thesis fall into three categories:

1. In the first four papers, we study rank-metric nested code pairs and their relative generalized weights. These parameters measure the security performance of the corresponding code pairs in linear network coding and storage systems with crisscross errors.

   We prove that all the well-known bounds for (relative) generalized Hamming weights hold for (relative) generalized rank weights; we establish new characterizations of vector space isometries between code pairs of different lengths preserving rank-metric properties (rank equivalences); we introduce the notion of relative generalized matrix weights, which extend relative generalized rank weights to code pairs that are linear over the base field and which allow us to obtain the first universal secure rank-metric list-decodable nested code pair; we estimate the generalized rank weights of reducible codes and prove that all rank-metric linear codes with optimal generalized rank weights for fixed packet and code sizes are reducible; and finally we provide rank-metric nested code pairs with optimal communication overheads based on previous studies.

2. In the next three papers, we study skew cyclic codes seen as rank-metric codes. We provide bounds on their minimum rank distance analogous to the shift bound and the Hartmann-Tzeng bound; we relate the lattices of skew cyclic codes and vector spaces of roots of skew polyno-

mials in an analogous way to that of classical cyclic codes and classical polynomials; we introduce the notion of rank error-correcting pairs, which give new bounds and decoding algorithms for certain rank-metric codes that include skew cyclic codes; and finally we study when skew cyclic codes of different lengths can be rank equivalent and/or rank degenerate, which has no analogy in the Hamming case.

3. The last two papers form a more miscellaneous collection. In the first of these papers, we study the asymptotic behaviour of sequences of ramp secret sharing schemes, in terms of partial information leakage. This is done by means of the relative generalized Hamming weights of the corresponding code pairs. In the next paper, we study a fundamental algebraic tool for future research on reliable and secure communications: We give a footprint-type bound on the number of common zeros of ideals of polynomials and a given finite collection of their consecutive Hasse derivatives.

The thesis is divided into two parts:

Part I is an introduction to the works included in this thesis. It contains no proofs and is scarce in technical details. It mainly serves as an overview and summary of the main results in the thesis.

Part II collects the papers constituting this thesis in their full form, which have been either peer-reviewed and published, or are currently under review.

Resumé

Rang-metriske koder og kodepar spiller en central rolle for pålidelig og sikker kommunikationer i forskellige praktiske scenarier såsom lineær netværkskodning og distribueret lagring med crisscross-fejl. Rang-metriske koders opførsel er i mange tilfælde analoge med de klassiske koders – også kendt som Hamming-metriske koder. Imidlertid er der talrige tilfælde, hvor rang-metriske koder viser uventede egenskaber uden analogi til Hamming-tilfældet. I denne afhandling udforsker vi ligheder og forskelle mellem rang-metriske koder og Hamming-metriske koder, og vi bruger denne analyse til at give nye anvendelser i de tidligere nævnte scenarier. Resultaterne og artiklerne i denne afhandling falder i tre kategorier:

1. I de første fire artikler studerer vi rang-metriske indlejrede kodepar og deres relative generaliserede vægte. Disse parametre beskriver sikkerheden når kodeparet anvendes i forbindelse med lineær netværkskodning og lagringsystemer med crisscross-fejl. Vi viser, at alle velkendte grænser for (relative) generaliserede Hammingvægte også gælder for (relative) generaliserede rangvægte; vi giver nye karakteriseringer af vektorrumsisomorfier mellem kodepar af forskellige længder, som bevarer rang-metriske egenskaber (rang-ækvivalenser); vi introducerer et koncept, som vi kalder relative generaliserede matrixvægte, hvilket udvider relative generaliserede rangvægte til kodepar, der er lineær over grundlegemet, og gør det muligt at konstruere det første universelle sikre rang-metriske list-decodable indlejrede kodepar; vi evaluerer reducerebare koders generaliserede rangvægte, og vi viser, at alle rang-metriske lineære koder med optimale generaliserede rangvægte nødvendivis er reducerebare, når pakkelængden og kodestørrelsen er faste; og til sidst angiver vi rang-metriske indlejrede kodepar med optimalle kommunikationsoverhead ved hjælp af tidligere resultater.

2. I de næste tre artikler studerer vi skæv-cykliske koder set som rang-metriske koder. Vi giver grænser for deres minimumsrangafstand, som er analoge med shiftsgrænsen og Hartmann-Tzeng grænsen; vi relaterer gitrene af vektorrum dannet af skæv-polynomiumsrødder til skæv-cy-

kliske koder, hvilket svarer til den kendte forbindelse mellem klassiske polynomier og klassiske cykliske koder; vi introducerer et koncept, som vi kalder rangfejlkorrigerende par, hvilket angiver nye grænser og korrigerende algoritmer for visse rang-metriske koder – inklussive skæv-cykliske koder; og til sidst udforsker vi hvornår skæv-cykliske koder med forskellige længder kan være rang-ækvivalente og/eller rang-degenererede, hvilket ikke har nogen analogi til Hammings tilfælde.

3. De sidste to artikler udgør en mere blandet samling. I den første af disse studerer vi de asymptotiske egenskaber for følger af ramp secret sharing schemes i forbindelse med delvis informationsaflytning – dette gøres ved at studere de tilhørende følger af relative generaliserede Hammingsvægte. I den følgende artikel udforsker vi en grundlæggende algebraisk værktøj med henblik på fremtidig forskning i pålidelig og sikker kommunikation: Vi etablerer en slags fodaftryksgrænse for antallet af fælles rødder af polynomier samt en endelig mængde af deres fortløbende Hassesafledte.

Afhandlingen består af to dele:

Del I er en introduktion til afhandlingens arbejder. Denne del indeholder ingen beviser, og alene få resultater præsenteres her. Den tjener som overblik og resumé af de vigtigste resultater i afhandlingen.

Del II består af de artikler, som udgør afhandlingen. De præsenteres i deres fuld form, hvori de er blevet peer-reviewed og publiserede, eller hvori de er under bedømmelse ved tidsskrifter.

Contents

Thesis Details

Thesis Title: Topics on Reliable and Secure Communication using Rank-Metric and Classical Linear Codes

PhD Student: Umberto Martínez-Peñas

PhD Supervisors: Professor Olav Geil, Aalborg University
Associate Professor Diego Ruano, Aalborg University

List of papers:

[A] U. Martínez-Peñas, "On the similarities between generalized rank and Hamming weights and their applications to network coding," *IEEE Transactions on Information Theory* Vol. 62, No. 7, pp. 4081–4095, July 2016.

[B] U. Martínez-Peñas, "Generalized rank weights of reducible codes, optimal cases and related properties," Accepted in *IEEE Transactions on Information Theory*, 13 pages.

Parts of this work appeared in: Proc. 2016 IEEE International Symposium on Information Theory (ISIT), July 2016, pp. 1959–1963.

[C] U. Martínez-Peñas and R. Matsumoto, "Relative generalized matrix weights of matrix codes for universal security on wire-tap networks," Submitted to *IEEE Transactions on Information Theory*, 21 pages.

Parts of this work appeared in: Proc. 54th Annual Allerton Conference on Communication, Control, and Computing, 2016, pp. 800–807.

[D] U. Martínez-Peñas, "Universal secure rank-metric coding schemes with optimal communication overheads," Submitted to *Cryptography and Communications*, 21 pages.

Parts of this work appeared in: Proc. 2017 IEEE International Symposium on Information Theory (ISIT), June 2017, pp. 2761–2765.

[E] U. Martínez-Peñas, “On the roots and minimum rank distance of skew cyclic codes,” *Designs, Codes and Cryptography* Vol. 83, No. 3, pp. 639–660, 2017.

[F] U. Martínez-Peñas and R. Pellikaan, “Rank error-correcting pairs,” *Designs, Codes and Cryptography* Vol. 84, No. 1-2, pp. 261–281, 2017.

[G] U. Martínez-Peñas, “Rank equivalent and rank degenerate skew cyclic codes,” *Advances in Mathematics of Communications* Vol. 11, No. 2, pp. 267–282, 2017.

[H] O. Geil, S. Martin, U. Martínez-Peñas, R. Matsumoto and D. Ruano, “On asymptotically good ramp secret sharing schemes,” Submitted to *IEICE Trans. Fundamentals*, 10 pages.

Parts of this work appeared in: Proc. 9th International Workshop on Coding and Cryptography (WCC), April 2015.

[I] O. Geil and U. Martínez-Peñas, “Bounding the number of common zeros of multivariate polynomials and their consecutive derivatives,” Submitted to *Combinatorics, Probability and Computing*, 26 pages.

Preface

This thesis has been submitted as a collection of papers for assessment in partial fulfillment of the Doctor of Philosophy at the Department of Mathematical Sciences, Aalborg University, Aalborg, Denmark. This PhD has been conducted in the period from September 2014 to August 2017 under the supervision of Professor Olav Geil and Associate Professor Diego Ruano.

This thesis contains two parts. Part I is an extended summary of the contributions obtained in this PhD. Parts of the papers constituting this thesis have been used directly or indirectly in the extended summary. Part II contains the papers in their full form, which have been either peer-reviewed and published, or submitted and under revision at the moment.

Acknowledgement

First of all, I would like to express my most sincere gratitude to my supervisors Professor Olav Geil and Associate Professor Diego Ruano for all their help and support. Olav and Diego introduced me to this field of research and its many ramifications, provided me with invaluable advice and shared with me important ideas in our very fruitful discussions.

I would also like to thank the Department of Mathematical Sciences at Aalborg University, and my colleagues there, for all their help and support.

I would like to express my gratitude to Professor Ryutaroh Matsumoto of Nagoya University and Professor Ruud Pellikaan of Eindhoven University of Technology, who I met during their visits at Aalborg University, and who provided me with invaluable help and deep insight in their fields of research.

I am also grateful to Professor Tom Høholdt of Aalborg University for his continuous help and support.

I am thankful to Professor Daniel Lucani and Professor Muriel Médard for hosting me during my visit at the Massachusetts Institute of Technology.

I wish to express my gratitude to Professor Frank R. Kschischang for his hospitality during my stay at his research group at the University of Toronto. I am especially grateful for our fruitful and revealing discussions.

I also owe thanks to Dr. Relinde Jurrius for inviting me to visit the University of Neuchâtel. I would like to thank her and Dr. Alberto Ravagnani for our very helpful discussions.

Last but not least, I wish to express my deepest gratitude to my family, to my old friends from Spain and to all the new friends I have made during this period, both in Denmark and around the world.

Finally, I gratefully acknowledge the support from The Danish Council for Independent Research for Grant No. DFF-4002-00367 (“How Secret is a Secret?”), which supported my PhD studies, and Grant No. DFF-5137-00076B (“EliteForsk-Rejsestipendium”), which supported, among others, my visits at the Massachusetts Institute of Technology and the University of Toronto.

Umberto Martínez-Peñas
Aalborg University, September 11, 2017

Part I

Introduction

Introduction

Reliability and *security* are desirable in many different communication or storage scenarios. Historically, many of such scenarios were modelled under the *Hamming metric*. Recently, new types of communication channels and storage systems have required other types of metrics. This is the case of the *rank metric*, which is suitable for reliable and secure linear network coding or distributed storage with crisscross errors and erasures, among others.

Since the theory of Hamming-metric codes has been intensively studied throughout the last century, many recent efforts have been made in the literature to obtain similarities between Hamming-metric codes and rank-metric codes.

In this thesis, we further explore such similarities, and we obtain on the way some new results for rank-metric codes that have no analogy in the theory of Hamming-metric codes.

This Introduction serves as an overview of the main results obtained in this thesis, and is organized as follows: The first section collects those results concerning different notions of relative generalized weights and universal security in linear network coding. The second section is devoted to the rank-metric properties of skew cyclic codes and the related theory of rank error-correcting pairs. The third section, which is of a more miscellaneous nature, contains a study of the related problem of secret sharing based on relative generalized Hamming weights, and it concludes with a new footprint-type bound for common zeros of polynomials and some of their consecutive Hasse derivatives.

Throughout this Introduction, we will mark those results taken from each of our papers by its corresponding capital letter, as shown in the section named Thesis Details.

Notation

Fix positive integers m, n and N, a prime power q, and denote by $\mathbb{F}_q$ the finite field with q elements. For a field $\mathbb{F}$, we denote by $\mathbb{F}^{m \times n}$ the vector space of $m \times n$ matrices over $\mathbb{F}$, and by $\mathbb{F}^n$ the vector space of column vectors of length

n over $\mathbb{F}$.

For a basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, we define the *matrix representation map* $M_{\boldsymbol{\alpha}} : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^{m \times n}$ associated to the previous basis by

$$M_{\boldsymbol{\alpha}}(\mathbf{c}) = (c_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n}, \tag{1}$$

where $\mathbf{c}_i = (c_{i,1}, c_{i,2}, \ldots, c_{i,n}) \in \mathbb{F}_q^n$, for $i = 1, 2, \ldots, m$, are the unique vectors in $\mathbb{F}_q^n$ such that $\mathbf{c} = \sum_{i=1}^m \alpha_i \mathbf{c}_i$. The map $M_{\boldsymbol{\alpha}} : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^{m \times n}$ is an $\mathbb{F}_q$-linear vector space isomorphism.

Thus we will usually identify $\mathbb{F}_{q^m}^n$ and $\mathbb{F}_q^{m \times n}$ throughout this Introduction. Moreover, the rank metric in $\mathbb{F}_q^{m \times n}$ can be extended to $\mathbb{F}_{q^m}^n$, via the map $M_{\boldsymbol{\alpha}}$, by defining the rank weight of a vector $\mathbf{c} \in \mathbb{F}_{q^m}^n$ as $\mathrm{wt}_{\mathrm{R}}(\mathbf{c}) = \mathrm{Rk}(M_{\boldsymbol{\alpha}}(\mathbf{c}))$.

In this Introduction, codes will be subsets of either $\mathbb{F}_{q^m}^n$ or $\mathbb{F}_q^{m \times n}$, whose linearity properties are specified in each case, and whose dimensions will be taken over the corresponding field, which will be understood from the context.

Another concept that will be extensively used is that of $\mathbb{F}_{q^m}$-linear Galois closed spaces and Galois closures, introduced in [61]:

Definition 0.1. We say that an $\mathbb{F}_{q^m}$-linear vector space $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$ is Galois closed if

$$\mathcal{V}^q = \{(v_1^q, v_2^q, \ldots, v_n^q) \mid (v_1, v_2, \ldots, v_n) \in \mathcal{V}\} \subseteq \mathcal{V}.$$

We denote by $\Upsilon(\mathbb{F}_{q^m}^n)$ the family of $\mathbb{F}_{q^m}$-linear Galois closed vector spaces in $\mathbb{F}_{q^m}^n$. Given an $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, we define its Galois closure as $\mathcal{C}^* = \sum_{i=0}^{m-1} \mathcal{C}^{q^i}$.

Observe that $\mathcal{C}^*$ is the smallest $\mathbb{F}_{q^m}$-linear Galois closed space containing the $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$.

1 Generalized weights and universal secure linear network coding

In the theory of Hamming-metric codes, the concept of relative generalized Hamming weights [42, 65] has been proven to be crucial to investigate the robustness of secret sharing schemes [7, 57] or codes for wire-tap channels of type II [48] against information leakage [40, 42, 65].

The concept of relative generalized rank weights [39, 45] has shown similar applications in universal secure linear network coding [39, 60]

In this section, we collect our main results concerning different notions of relative generalized weights used to measure universal security in linear network coding. These results are contained in Papers A, B, C and D, and correspond to the first group of results mentioned in the Abstract.

1.1 Preliminaries

In this subsection, we collect the main results in the literature concerning reliable and secure linear network coding.

Consider a network with one source and several sinks, of which we may choose one to focus on. Let n and N be the number of outgoing links from the source and the number of ingoing links to the chosen sink, respectively. Assume that the source wants to transmit a message to the sink. To that end, the source encodes the message into a collection of n packets of length m, seen as a matrix $C \in \mathbb{F}_q^{m \times n}$, being each packet sent through each outgoing link from the source. In this context, *linear network coding* [1, 37, 41] over the finite field $\mathbb{F}_q$ is the process by which relay nodes in the network forward linear combinations of the received packets. According to [37, Def. 1], the sink is expected to receive the matrix

$$Y = CA^T \in \mathbb{F}_q^{m \times N},$$

where $A \in \mathbb{F}_q^{N \times n}$ is called the *transfer matrix* of corresponding source and sink. For robustness and decentralization, it is desirable to choose A at random by choosing the linear combinations randomly at each relay node (*random linear network coding* [31]).

Reliability and *security* in this context was first considered in [10] and [11], respectively. In [60], the authors consider for the first time coding techniques to protect information simultaneously from link errors and link observations, independently and without knowledge of the underlying linear network code. Hence such coding techniques are compatible with random linear network coding.

According to the model in [60], we say that *t errors and ρ erasures* happened if the sink receives

$$Y = CA^T + E \in \mathbb{F}_q^{m \times N},$$

for matrices $E \in \mathbb{F}_q^{m \times N}$ and $A \in \mathbb{F}_q^{N \times n}$, where $t = \mathrm{Rk}(E)$ and $\rho = n - \mathrm{Rk}(A)$, and we say that *$\mu$ observations* happened if the wire-tapper obtains

$$CB^T \in \mathbb{F}_q^{m \times \mu},$$

for a matrix $B \in \mathbb{F}_q^{\mu \times n}$.

The authors in [60] obtained optimal coding techniques when $n \leq m$ by using pairs of $\mathbb{F}_{q^m}$-linear Gabidulin codes in $\mathbb{F}_{q^m}^n$ [21, 55] (one for reliability and one for security) in a concatenated manner. In [39], *nested coset coding schemes* are introduced in this context to apply pairs of codes in an integrated way. The following is [39, Def. 7]:

Definition 0.2. A coset coding scheme over $\mathbb{F}_q$ with message set $\mathcal{S}$ is a family of disjoint nonempty subsets of $\mathbb{F}_q^{m \times n}$, $\mathcal{P}_{\mathcal{S}} = \{\mathcal{C}_{\mathbf{x}}\}_{\mathbf{x} \in \mathcal{S}}$.

For each $\mathbf{x} \in \mathcal{S}$, choose uniformly at random a matrix $C \in \mathcal{C}_{\mathbf{x}}$. Then C is the encoding of $\mathbf{x}$ by the coset coding scheme.

We may use *nested linear code pairs*, introduced in [66, Sec. III.A], to obtain coset coding schemes with linearity properties:

Definition 0.3. A nested $\mathbb{F}_q$-linear code pair is a pair of $\mathbb{F}_q$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$. We may define a coset coding scheme with message set $\mathcal{S} = \mathbb{F}_q^{\ell}$, $\ell = \dim(\mathcal{C}_1 / \mathcal{C}_2)$, based on such a code pair as follows: Choose an $\mathbb{F}_q$-linear subspace $\mathcal{W} \subseteq \mathcal{C}_1$ such that $\mathcal{C}_1 = \mathcal{C}_2 \oplus \mathcal{W}$, define a vector space isomorphism $\psi : \mathbb{F}_q^{\ell} \longrightarrow \mathcal{W}$, and finally define $\mathcal{C}_{\mathbf{x}} = \psi(\mathbf{x}) + \mathcal{C}_2$, for $\mathbf{x} \in \mathbb{F}_q^{\ell}$.

Such coset coding schemes are called $\mathbb{F}_q$-linear nested coset coding schemes [39].

We may define similarly nested $\mathbb{F}_{q^m}$-linear code pairs in $\mathbb{F}_{q^m}^n$, by considering $\mathcal{S} = \mathbb{F}_{q^m}^{\ell}$.

In Paper A, it is shown that this defines a bijection between the family of nested $\mathbb{F}_q$-linear code pairs and the family of coset coding schemes with message set $\mathcal{S} = \mathbb{F}_q^{\ell}$ that are $\mathbb{F}_q$-linear in the following sense:

$$a\mathcal{C}_{\mathbf{x}} + b\mathcal{C}_{\mathbf{y}} \subseteq \mathcal{C}_{a\mathbf{x}+b\mathbf{y}},$$

for all $a, b \in \mathbb{F}_q$ and all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^{\ell}$. Analogously for the $\mathbb{F}_{q^m}$-linear case.

As explained above, we are interested in coset coding schemes that are universally reliable and secure. The following definition is given in a more general form in [60]:

Definition 0.4. Given positive integers t, ρ and μ, we say that a coset coding scheme $\mathcal{P}_{\mathcal{S}}$ is:

1. Universally t-error and ρ-erasure-correcting if, for every $A \in \mathbb{F}_q^{N \times n}$ with $\mathrm{Rk}(A) = n - \rho$, there exists a decoding function $D_A : \mathbb{F}_q^{m \times N} \longrightarrow \mathcal{S}$ such that $D_A(Y) = \mathbf{x}$, for every $\mathbf{x} \in \mathcal{S}$ and every matrix of the form

$$Y = CA^T + E,$$

where $C \in \mathcal{C}_{\mathbf{x}}$ and $E \in \mathbb{F}_q^{m \times N}$ is such that $\mathrm{Rk}(E) \leq t$.

2. Universally secure under μ observations if

$$H(\mathbf{x} | CB^T) = H(\mathbf{x}),$$

for every $B \in \mathbb{F}_q^{\mu \times n}$.

The universal error and erasure-correction capability of coset coding schemes was obtained in terms of the rank metric chronologically in the following works: First in [59, 60] when $\mathcal{C}_2 = \{0\}$, then in [39, Th. 4] for nested $\mathbb{F}_{q^m}$-linear code pairs, and finally in Paper A for general coset coding schemes. To state such result, we need to define the *minimum rank distance* of a coset coding scheme $\mathcal{P}_{\mathcal{S}}$, which is given in Paper A:

$$d_R(\mathcal{P}_{\mathcal{S}}) = \min\{\mathrm{Rk}(C - D) : C \in \mathcal{C}_{\mathbf{x}}, D \in \mathcal{C}_{\mathbf{y}}, \mathbf{x} \neq \mathbf{y}\},$$

where we denote $d_R(\mathcal{C}_1, \mathcal{C}_2) = d_R(\mathcal{P}_{\mathcal{S}})$ for nested coset coding schemes.

Then we may state the following result, which is proven in Paper A in a slightly different form:

Theorem 0.1 ([A]). *For positive integers t and ρ, a coset coding scheme $\mathcal{P}_{\mathcal{S}}$ in $\mathbb{F}_q^{m \times n}$ is universally t-error and ρ-erasure-correcting if, and only if, $2t + \rho < d_R(\mathcal{P}_{\mathcal{S}})$.*

Universal security performance, as in Definition 0.4, is also measured by the minimum rank distance, as proven in [60]. However, the concept of *relative generalized rank weights*, introduced independently in [39, 45] allows us to give a deeper analysis on the information leakage to the wire-tapper:

Definition 0.5. Given nested $\mathbb{F}_{q^m}$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$, we define their r-th relative generalized rank weight as

$$\begin{aligned} d_{R,r}(\mathcal{C}_1, \mathcal{C}_2) = \min\{ & \dim(\mathcal{V}) : \mathcal{V} \in \Upsilon(\mathbb{F}_{q^m}^n), \\ & \dim(\mathcal{C}_1 \cap \mathcal{V}) - \dim(\mathcal{C}_2 \cap \mathcal{V}) \geq r\}, \end{aligned}$$

for $r = 1, 2, \ldots, \dim(\mathcal{C}_1/\mathcal{C}_2)$. For one $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, we define its r-th generalized rank weight as $d_{R,r}(\mathcal{C}) = d_{R,r}(\mathcal{C}, \{\mathbf{0}\})$, for $r = 1, 2, \ldots, \dim(\mathcal{C})$.

It holds that $d_{R,1}(\mathcal{C}_1, \mathcal{C}_2) = d_R(\mathcal{C}_1, \mathcal{C}_2)$ [34, 39, 53]. The following result is proven in [39]:

Theorem 0.2. *Given nested $\mathbb{F}_{q^m}$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$, it holds that $d_{R,r}(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp)$ is the minimum number of links that an adversary needs to wire-tap in order to obtain at least r units of information (number of bits multiplied by $\log_2(q^m)$) of the sent message, for $r = 1, 2, \ldots, \dim(\mathcal{C}_1/\mathcal{C}_2)$.*

In particular, we deduce that the wire-tapper obtains no information about the sent message when listening to less than $d_R(\mathcal{C}_1, \mathcal{C}_2)$ links in the network.

1.2 Equivalences and bounds for generalized rank weights

Theorem 0.1 is one of the main results in Paper A. Other results in that paper, which we summarize in this subsection, establish new connections between relative generalized rank weights and relative generalized Hamming weights.

Mainly, we obtain characterizations of vector space isomorphisms preserving rank-metric properties between $\mathbb{F}_{q^m}$-linear codes. Using such isomorphisms, we are able to define relative generalized rank weights in terms of relative generalized Hamming weights. This will allow us to translate most of the well-known bounds on the latter weights to bounds on the former weights.

We will make use of the following alternative definition of relative generalized rank weights given first in [34] for non-relative weights and extended in Paper A to relative weights:

$$d_{R,r}(\mathcal{C}_1, \mathcal{C}_2) = \min\{\mathrm{wt}_{\mathrm{R}}(\mathcal{D}) : \mathcal{D} \subseteq \mathcal{C}_1, \mathcal{D} \cap \mathcal{C}_2 = \{\mathbf{0}\} \\ \dim(\mathcal{D}) = r\},$$

for $r = 1, 2, \ldots, \dim(\mathcal{C}_1/\mathcal{C}_2)$, where we define $\mathrm{wt}_{\mathrm{R}}(\mathcal{D}) = \dim(\mathcal{D}^*)$, for any $\mathbb{F}_{q^m}$-linear subspace $\mathcal{D} \subseteq \mathbb{F}_{q^m}^n$. It can be proven that $\mathrm{wt}_{\mathrm{R}}(\mathbf{c}) = \mathrm{wt}_{\mathrm{R}}(\langle \mathbf{c} \rangle)$, for every $\mathbf{c} \in \mathbb{F}_{q^m}^n$.

We may now establish the characterizations mentioned above:

Theorem 0.3 ([A]). *Given an $\mathbb{F}_{q^m}$-linear vector space isomorphism $\phi : \mathcal{V} \longrightarrow \mathcal{W}$, where $\mathcal{V} \in \Upsilon(\mathbb{F}_{q^m}^n)$ and $\mathcal{W} \in \Upsilon(\mathbb{F}_{q^m}^{n'})$, the following are equivalent:*

1. *If $\mathbf{c} \in \mathcal{V}$ and $\mathrm{wt}_{\mathrm{R}}(\mathbf{c}) = 1$, then $\mathrm{wt}_{\mathrm{R}}(\phi(\mathbf{c})) = 1$.*

2. *ϕ preserves rank weights, that is, $\mathrm{wt}_{\mathrm{R}}(\phi(\mathbf{c})) = \mathrm{wt}_{\mathrm{R}}(\mathbf{c})$, for all $\mathbf{c} \in \mathcal{V}$.*

3. *For all $\mathbb{F}_{q^m}$-linear subspaces $\mathcal{D} \subseteq \mathcal{V}$, it holds that $\mathrm{wt}_{\mathrm{R}}(\phi(\mathcal{D})) = \mathrm{wt}_{\mathrm{R}}(\mathcal{D})$.*

4. *For all $\mathcal{U} \subseteq \mathcal{V}$ such that $\mathcal{U} \in \Upsilon(\mathbb{F}_{q^m}^n)$, it holds that $\phi(\mathcal{U}) \in \Upsilon(\mathbb{F}_{q^m}^{n'})$.*

5. *There exists $\beta \in \mathbb{F}_{q^m}^*$ and an $\mathbb{F}_{q^m}$-linear vector space isomorphism $\phi' : \mathcal{V} \longrightarrow \mathcal{W}$ such that $\phi'(\mathcal{V}|_{\mathbb{F}_q}) \subseteq \mathcal{W}|_{\mathbb{F}_q}$ and $\phi(\mathbf{c}) = \beta\phi'(\mathbf{c})$, for every $\mathbf{c} \in \mathcal{V}$. Equivalently, there exists a matrix $A \in \mathbb{F}_q^{n \times n'}$ and $\beta \in \mathbb{F}_{q^m}^*$ such that $\phi(\mathbf{c}) = \beta \mathbf{c} A$, for every $\mathbf{c} \in \mathcal{V}$.*

In such case, we will say that ϕ is a rank equivalence.

We recall that the equivalence between Items 2 and 5 in the previous theorem was obtained first in [5, Th. 1] when $\mathcal{V} = \mathcal{W} = \mathbb{F}_{q^m}^n$.

Observe that rank equivalences defined on the appropriate ambient spaces preserve relative generalized rank weights and the full universal security performance of $\mathbb{F}_{q^m}$-linear nested coset coding schemes by [39, Lemma 7].

Since every $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is contained in some $\mathbb{F}_{q^m}$-linear Galois closed space, namely $\mathcal{C}^*$, we may use these spaces as ambient spaces for the rank metric. Hence we may give the following definition:

Definition 0.6 ([A]). We say that two $\mathbb{F}_{q^m}$-linear codes $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ and $\mathcal{C}' \subseteq \mathbb{F}_{q^m}^{n'}$ are rank equivalent if there exists a rank equivalence ϕ between $\mathcal{V}$ and $\mathcal{W}$ such that $\phi(\mathcal{C}) = \mathcal{C}'$, where $\mathcal{C} \subseteq \mathcal{V} \in \Upsilon(\mathbb{F}_{q^m}^n)$ and $\mathcal{C}' \subseteq \mathcal{W} \in \Upsilon(\mathbb{F}_{q^m}^{n'})$.

Before stating our main results, we remark that the previous characterizations also allow us to prove the following: The last generalized rank weight of an $\mathbb{F}_{q^m}$-linear code gives the range of all possible lengths n for which there exists another $\mathbb{F}_{q^m}$-linear code that is rank equivalent to the given one.

Proposition 0.7 ([A]). *Given an $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension k and any positive integer n', there exists an $\mathbb{F}_{q^m}$-linear code $\mathcal{C}' \subseteq \mathbb{F}_{q^m}^{n'}$ that is rank equivalent to $\mathcal{C}$ if, and only if, $n' \geq d_{R,k}(\mathcal{C})$.*

We may now give following interesting connection between relative generalized rank weights and relative generalized Hamming weights, introduced in [42, 65]:

Theorem 0.4 ([A]). *Given nested $\mathbb{F}_{q^m}$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$, it holds that*

$$d_{R,r}(\mathcal{C}_1, \mathcal{C}_2) = \min\{d_{H,r}(\phi(\mathcal{C}_1), \phi(\mathcal{C}_2)) : \phi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n \text{ is a rank equivalence}\},$$

where $d_{H,r}(\mathcal{D}_1, \mathcal{D}_2)$ denotes the r-th relative generalized Hamming weight [42, 65] of nested $\mathbb{F}_{q^m}$-linear codes $\mathcal{D}_2 \subsetneqq \mathcal{D}_1 \subseteq \mathbb{F}_{q^m}^n$, for $r = 1, 2, \ldots, \dim(\mathcal{D}_1/\mathcal{D}_2)$, that is,

$$d_{H,r}(\mathcal{D}_1, \mathcal{D}_2) = \min\{\#I : I \subseteq \{1, 2, \ldots, n\}, \dim(\mathcal{D}_1 \cap \mathcal{V}_I) - \dim(\mathcal{D}_2 \cap \mathcal{V}_I) \geq r\},$$

where $\mathcal{V}_I = \{(c_1, c_2, \ldots, c_n) : c_i = 0, \forall i \notin I\}$, for a subset $I \subseteq \{1, 2, \ldots, n\}$.

This result is used in Paper A to prove the following theorem:

Theorem 0.5 ([A]). *Fix numbers ℓ and $1 \leq r, s \leq \ell$, and functions $f_{r,s}, g_{r,s} : \mathbb{N} \longrightarrow \mathbb{R}$, which may also depend on n, m, ℓ and q. If $g_{r,s}$ is increasing, then every bound of the form*

$$f_{r,s}(d_r(\mathcal{C}_1, \mathcal{C}_2)) \geq g_{r,s}(d_s(\mathcal{C}_1, \mathcal{C}_2))$$

that is valid for relative generalized Hamming weights, for any pair of $\mathbb{F}_{q^m}$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$ with $\dim(\mathcal{C}_1/\mathcal{C}_2) = \ell$, is also valid for relative generalized rank weights.

We now give a list of bounds of this form, most of which are taken from [62]. Among them, only monotonicity [39, Lemma 4] and its refinement [19, Prop. II.3] had been obtained before for (relative) generalized rank weights. Fix positive integers $1 \leq r \leq s \leq \ell$, and denote $d_j = d_{R,j}(\mathcal{C}_1, \mathcal{C}_2)$, for all $j = 1, 2, \ldots, \ell$, for nested $\mathbb{F}_{q^m}$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$ such that $\ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$. The following bounds can be directly translated from relative generalized Hamming weights to relative generalized rank weights:

1. Monotonicity:
$$d_{r+1} \geq d_r + 1,$$
2. Griesmer-type ([62, Bound (14)]):
$$d_r \geq \sum_{i=0}^{r-1} \left\lceil \frac{d_1}{q^{mi}} \right\rceil,$$
3. Griesmer-type ([62, Bound (16)]):
$$d_s \geq d_r + \sum_{i=0}^{s-r} \left\lceil \frac{(q^m - 1)d_r}{(q^{mr} - 1)q^{mi}} \right\rceil,$$
4. [30, Th. 1] or [62, Bound (18)]:
$$(q^{ms} - 1)d_r \leq (q^{ms} - q^{m(s-r)})d_s,$$
5. [30, Cor. 1]:
$$(q^{mr} - 1)d_1 \leq (q^{mr} - q^{m(r-1)})d_r,$$
6. [19, Prop. II.3]:
$$(q^{mr} - 1)d_{r-1} \leq (q^{mr} - q^m)d_r,$$
7. [62, Bound (20)]:
$$d_r \geq n - \left\lfloor \frac{(q^{m(\ell-r)} - 1)(n - d_s)}{q^{m(\ell-s)} - 1} \right\rfloor.$$

1.3 Generalized rank weights of reducible codes

In this subsection, we estimate the generalized rank weights of *reducible codes*, introduced in [23], and show that all $\mathbb{F}_{q^m}$-linear codes with optimal generalized rank weights, for fixed packet and code sizes, must be reducible. These results are obtained in Paper B and have no analogy in the theory of generalized Hamming weights.

Reducible codes were introduced and defined in [23] as follows:

Definition 0.8. Fix positive integers l, k_i and n_i, for $i = 1, 2, \ldots, l$, with $n = n_1 + n_2 + \cdots + n_l$. We say that an $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, of dimension k, is reducible with reduction $\mathcal{R} = (G_{i,j})_{1 \leq i \leq l}^{i \leq j \leq l}$ if it has a generator matrix of the form
$$G = \begin{pmatrix} G_{1,1} & G_{1,2} & G_{1,3} & \ldots & G_{1,l-1} & G_{1,l} \\ 0 & G_{2,2} & G_{2,3} & \ldots & G_{2,l-1} & G_{2,l} \\ 0 & 0 & G_{3,3} & \ldots & G_{3,l-1} & G_{3,l} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & G_{l-1,l-1} & G_{l-1,l} \\ 0 & 0 & 0 & \ldots & 0 & G_{l,l} \end{pmatrix},$$

where $G_{i,j} \in \mathbb{F}_{q^m}^{k_i \times n_j}$, for $i = 1, 2, \ldots, l$ and $j = i, i+1, \ldots, l$.

For a given reduction $\mathcal{R}$ as in the previous definition, we define the main components of the code $\mathcal{C}$ as the $\mathbb{F}_{q^m}$-linear codes $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_l$ with generator matrices $G_{1,1}, G_{2,2}, \ldots, G_{l,l}$, respectively, its row components as the $\mathbb{F}_{q^m}$-linear codes $\mathcal{C}_i^\prime \subseteq \mathbb{F}_{q^m}^n$ with generator matrices

$$G_i^\prime = (0, \ldots, 0, G_{i,i}, G_{i,i+1}, \ldots, G_{i,l}),$$

for $i = 1, 2, \ldots, l$, and its column components as the $\mathbb{F}_{q^m}$-linear codes $\widehat{\mathcal{C}}_j \subseteq \mathbb{F}_{q^m}^{n_j}$ generated by the matrices

$$\widehat{G}_j = (G_{1,j}, G_{2,j}, \ldots, G_{j,j})^T,$$

for $j = 1, 2, \ldots, l$, which need not have full rank.

When choosing $n = lm$ and all codes $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_l \subseteq \mathbb{F}_{q^m}^m$ as Gabidulin codes [21, 55] of the same dimension $k^\prime$, it holds that $k = lk^\prime$ and $d_R(\mathcal{C}) = m - k^\prime + 1$, which is the maximum possible [23]. This is, to the best of our knowledge, the only family of maximum rank distance $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$ whenever $n > m$. This idea can be extended, as we do in Paper B, to obtain maximum rank distance $\mathbb{F}_{q^m}$-linear codes for other families of parameters when $n > m$.

The following lower and upper bounds are given in Paper B and allow us to estimate the generalized rank weights of reducible codes in terms of their components:

Theorem 0.6 ([B]). *Let notation be as in Definition 0.8, and set $d_{R,0}(\mathcal{D}) = 0$ for an $\mathbb{F}_{q^m}$-linear code $\mathcal{D}$. For every $r = 1, 2, \ldots, k$, we have that*

$$\begin{aligned} d_{R,r}(\mathcal{C}) \geq \min\{ & d_{R,r_1}(\mathcal{C}_1) + d_{R,r_2}(\mathcal{C}_2) + \cdots + d_{R,r_l}(\mathcal{C}_l) \\ & : r = r_1 + r_2 + \cdots + r_l, 0 \leq r_i \leq k_i \}, \end{aligned}$$

and

$$\begin{aligned} d_{R,r}(\mathcal{C}) \leq \min\{ & d_{R,r_1}(\mathcal{C}_1^\prime) + d_{R,r_2}(\mathcal{C}_2^\prime) + \cdots + d_{R,r_l}(\mathcal{C}_l^\prime) \\ & : r = r_1 + r_2 + \cdots + r_l, 0 \leq r_i \leq k_i \}. \end{aligned}$$

Moreover, it holds that

$$\begin{aligned} d_{R,r}(\mathcal{C}^\perp) \leq \min\{ & d_{R,\widehat{r}_1}(\widehat{\mathcal{C}}_1^\perp) + d_{R,\widehat{r}_2}(\widehat{\mathcal{C}}_2^\perp) + \cdots + d_{R,\widehat{r}_l}(\widehat{\mathcal{C}}_l^\perp) \\ & : r = \widehat{r}_1 + \widehat{r}_2 + \cdots + \widehat{r}_l, 0 \leq \widehat{r}_j \leq \widehat{k}_j \}, \end{aligned}$$

for $r = 1, 2, \ldots, n - \widehat{k}$, where $\widehat{k}_j = \dim(\widehat{\mathcal{C}}_j^\perp)$, for $j = 1, 2, \ldots, l$, and $\widehat{k} = \widehat{k}_1 + \widehat{k}_2 + \cdots + \widehat{k}_l$.

Observe that the first of these bounds was already given in [23, Lemma 2] for $r = 1$.

On the other hand, if we fix the packet and code sizes, that is, m and $k = \dim(\mathcal{C})$, and we allow n to vary, then all $\mathbb{F}_{q^m}$-linear codes whose generalized rank weights are all optimal must be reducible. To show this, we use the following upper bounds given in Paper A:

Lemma 0.9 ([A]). *Given an $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension k, for each $r = 1, 2, \ldots, k-1$, it holds that*

$$1 \leq d_{R,r+1}(\mathcal{C}) - d_{R,r}(\mathcal{C}) \leq m.$$

As a consequence, for each $r = 1, 2, \ldots, k$, it holds that

$$d_{R,r}(\mathcal{C}) \leq rm.$$

The following result is proven in Paper B:

Theorem 0.7 ([B]). *Throughout the theorem, fix positive integers k and m, and a basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.*

Define the $\mathbb{F}_{q^m}$-linear code $\mathcal{C}_{opt} = \mathcal{C}_1 \times \mathcal{C}_2 \times \cdots \times \mathcal{C}_k \subseteq \mathbb{F}_{q^m}^{km}$, where all $\mathcal{C}_i$ are equal and generated by the vector $(\alpha_1, \alpha_2, \ldots, \alpha_m) \in \mathbb{F}_{q^m}^m$. Then $\dim(\mathcal{C}_{opt}) = k$ and $d_{R,r}(\mathcal{C}_{opt}) = rm$, for $r = 1, 2, \ldots, k$.

Conversely, let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be an $\mathbb{F}_{q^m}$-linear code of dimension k such that $d_{R,r}(\mathcal{C}) = rm$, for every $r = 1, 2, \ldots, k$. Then $\mathcal{C}$ is rank equivalent to the previous code $\mathcal{C}_{opt} \subseteq \mathbb{F}_{q^m}^{km}$. Moreover, the rank equivalence can be explicitly constructed in polynomial time from any basis of $\mathcal{C}$.

Such a decomposition theorem has no analogy in the theory of generalized Hamming weights.

1.4 Relative generalized matrix weights and universal secure rank-metric list-decodable schemes

So far we have studied $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$. In [53], a notion of generalized weights is introduced for $\mathbb{F}_q$-linear codes $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$, called *Delsarte generalized weights*. However, its connection with information leakage was proven in [53] only for $\mathbb{F}_{q^m}$-linear codes.

In this subsection, we introduce a notion of relative generalized weights for nested $\mathbb{F}_q$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$ that measures their universal security performance in terms of worst-case information leakage as in Theorem 0.2. Such relative generalized weights can be defined over any field $\mathbb{F}$, which mathematically plays the role of $\mathbb{F}_q$. In addition, they coincide with Delsarte generalized weights [53] when $\mathbb{F} = \mathbb{F}_q$, $\mathcal{C}_2 = \{0\}$ and $m \neq n$.

The results in this subsection are obtained in Paper C. We start with the main definition:

Definition 0.10 ([C]). Given nested $\mathbb{F}$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$, we define their r-th relative generalized matrix weight as

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) = \min\{ \dim(\mathcal{L}) : \mathcal{L} \subseteq \mathbb{F}^n, \mathbb{F} - \text{linear}, \\ \dim(\mathcal{C}_1 \cap \mathcal{V}_\mathcal{L}) - \dim(\mathcal{C}_2 \cap \mathcal{V}_\mathcal{L}) \geq r\},$$

for $r = 1, 2, \ldots, \dim(\mathcal{C}_1/\mathcal{C}_2)$, where we define

$$\mathcal{V}_\mathcal{L} = \{V \in \mathbb{F}^{m \times n} : \text{Row}(V) \subseteq \mathcal{L}\},$$

for an $\mathbb{F}$-linear subspace $\mathcal{L} \subseteq \mathbb{F}^n$.

For one $\mathbb{F}$-linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$, we define its r-th generalized matrix weight as $d_{M,r}(\mathcal{C}) = d_{M,r}(\mathcal{C}, \{0\})$, for $r = 1, 2, \ldots, \dim(\mathcal{C})$.

In this case, it is proven in Paper C that $d_{M,1}(\mathcal{C}_1, \mathcal{C}_2) = d_R(\mathcal{C}_1, \mathcal{C}_2)$, which extends [53, Th. 30] when both notions of generalized weights coincide.

We may now state a result analogous to Theorem 0.2:

Theorem 0.8 ([C]). *Given nested $\mathbb{F}_q$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$, it holds that $d_{M,r}(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp)$ is the minimum number of links that an adversary needs to wire-tap in order to obtain at least r units of information (number of bits multiplied by $\log_2(q)$) of the sent message.*

In this case, we define the dual of an $\mathbb{F}_q$-linear code $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ as

$$\mathcal{C}^\perp = \{D \in \mathbb{F}_q^{m \times n} : \text{Trace}(CD^T) = 0, \forall C \in \mathcal{C}\}.$$

In particular, as in the $\mathbb{F}_{q^m}$-linear case, we conclude that the wire-tapper obtains no information about the sent message when listening to less than $d_R(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp)$ links in the network.

As expected, it holds that relative generalized matrix weights extend relative generalized rank weights. Moreover, due to the study on duality of rank-metric codes given in [54], this shows that Theorem 0.8 extends Theorem 0.2:

Theorem 0.9 ([C]). *Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be a basis of $\mathbb{F}_{q^m}$ as a vector space over $\mathbb{F}_q$. Given nested $\mathbb{F}_{q^m}$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$, and integers $1 \leq r \leq \dim(\mathcal{C}_1/\mathcal{C}_2)$ (over $\mathbb{F}_{q^m}$) and $0 \leq p \leq m-1$, we have that*

$$d_{R,r}(\mathcal{C}_1, \mathcal{C}_2) = d_{M,rm-p}(M_{\boldsymbol{\alpha}}(\mathcal{C}_1), M_{\boldsymbol{\alpha}}(\mathcal{C}_2)),$$

where $M_{\boldsymbol{\alpha}} : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^{m \times n}$ is as in (1).

The two main applications of these new relative generalized weights are the following, also given in Paper C: First, we obtain universal secure $\mathbb{F}_q$-linear codes for noiseless networks with largest possible message set $\mathcal{S} = \mathbb{F}_q^\ell$

-equivalently, information rate- for a given number of observations μ. To that end, we use the $\mathbb{F}_q$-linear maximum rank distance codes in [16]. This family of optimal universal secure $\mathbb{F}_q$-linear codes for noiseless networks extends those obtained in [60] based on Gabidulin codes [21, 55].

Secondly, we obtain in Paper C the first family of universal secure rank-metric list-decodable ($\mathbb{F}_q$-linear) coset coding schemes. Such schemes are based on a recent construction of rank-metric list-decodable codes by Guruswami et al [27].

We first extend the concept of rank list-decodable codes from [18, Def. 2] to coset coding schemes:

Definition 0.11 ([C]). For positive integers e and L, we say that a coset coding scheme $\mathcal{P}_{\mathcal{S}} = \{\mathcal{C}_{\mathbf{x}}\}_{\mathbf{x}\in\mathcal{S}}$ is rank (e, L)-list-decodable if, for every $Y \in \mathbb{F}_q^{m\times n}$, we have that

$$\#\{\mathbf{x} \in \mathcal{S} : \mathcal{P}_{\mathbf{x}} \cap \mathcal{B}(Y, e) \neq \emptyset\} \leq L,$$

where $\mathcal{B}(Y, e)$ denotes the ball in $\mathbb{F}_q^{m\times n}$ with center Y and rank radius e. The number of list-decodable rank errors is e and the list sizes are said to be polynomial in n if $L = \mathcal{O}(F(n))$, for some polynomial $F(x)$.

We may summarize the mentioned construction as follows:

Theorem 0.10 ([C]). *Assume that n divides m and fix $\varepsilon > 0$ and positive integers s and $0 \leq k_2 < k_1 \leq n$ such that $4sn \leq \varepsilon m$ and $m/n = \mathcal{O}(s/\varepsilon)$. We may explicitly construct nested $\mathbb{F}_q$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m\times n}$ such that:*

1. *$\ell = \dim(\mathcal{C}_1/\mathcal{C}_2) \geq m(k_1 - k_2)(1 - 2\varepsilon)$.*

2. *The corresponding coset coding scheme is universal secure under $\mu \geq k_2$ observations.*

3. *The corresponding coset coding scheme is rank (e, L)-list-decodable for all $e \leq \frac{s}{s+1}(n - k_1)$, with $L \leq q^{\mathcal{O}(s^2/\varepsilon^2)}$, and it admits a list-decoding algorithm that obtains all corresponding uncoded messages with polynomial complexity in n.*

This construction is based on the results in [27], and extends the rank list-decodable codes in [27, Sec. IV], which are obtained by choosing $k_2 = 0$.

To evaluate the near optimality of this construction informally, we may compare it with the optimal universal secure and rank unique-decodable nested $\mathbb{F}_{q^m}$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$, with $n \leq m$, $k_1 = \dim(\mathcal{C}_1)$ and $k_2 = \dim(\mathcal{C}_2)$, obtained in [60], which satisfy that:

1. $\ell = \dim(\mathcal{C}_1/\mathcal{C}_2) = m(k_1 - k_2)$ (here dimensions of $\mathbb{F}_{q^m}$-linear codes are taken over $\mathbb{F}_q$).

2. The corresponding coset coding scheme is universal secure under $\mu = k_2$ observations.

3. The corresponding coset coding scheme is universal e-error-correcting if $e \leq \lfloor \frac{n-k_1}{2} \rfloor$.

When ε is small and s is large, our construction has parameters close to those obtained in [60], and it can list-decode roughly twice as many rank errors as the construction in [60] can unique-decode.

Finally, as a third application, we obtain the following extension of Theorem 0.3:

Theorem 0.11 ([C]). *Let $\phi : \mathcal{V}_{\mathcal{L}} \longrightarrow \mathcal{V}_{\mathcal{K}}$ be an $\mathbb{F}_q$-linear vector space isomorphism, for $\mathbb{F}_q$-linear subspaces $\mathcal{L} \subseteq \mathbb{F}_q^n$ and $\mathcal{K} \subseteq \mathbb{F}_q^{n'}$, and consider the following properties:*

(P 1) There exist full-rank matrices $A \in \mathbb{F}^{m \times m}$ and $B \in \mathbb{F}^{n \times n'}$ such that $\phi(C) = ACB$, for all $C \in \mathcal{V}_{\mathcal{L}}$.

(P 2) A subspace $\mathcal{U} \subseteq \mathcal{V}_{\mathcal{L}}$ is of the form $\mathcal{U} = \mathcal{V}_{\mathcal{J}}$ for an $\mathbb{F}_q$-linear subspace $\mathcal{J} \subseteq \mathbb{F}_q^n$ if, and only if, so is $\phi(\mathcal{U})$.

(P 3) For all $\mathbb{F}_q$-linear subspaces $\mathcal{D} \subseteq \mathcal{V}_{\mathcal{L}}$, it holds that $\mathrm{wt_R}(\phi(\mathcal{D})) = \mathrm{wt_R}(\mathcal{D})$, where

$$\mathrm{wt_R}(\mathcal{D}) = \dim \left(\sum_{D \in \mathcal{D}} \mathrm{Row}(D) \right).$$

(P 4) ϕ is a rank isometry.

Then the following implications hold:

$$(P\ 1) \Longleftrightarrow (P\ 2) \Longleftrightarrow (P\ 3) \Longrightarrow (P\ 4).$$

In addition, $(P\ 3) \Longleftarrow (P\ 4)$ holds when $\mathcal{L} = \mathcal{K} = \mathbb{F}_q^n$ and $m \neq n$.

This result extends not only Theorem 0.3, which extends in turn [5, Th. 1], but also [43, Th. 1] and [44, Prop. 3].

1.5 Universal reliable and secure coset coding schemes with optimal communications overheads

We conclude this study on universal secure linear network coding with an application to secure distributed storage with crisscross errors and erasures.

Consider a distributed storage system where data is encoded into a matrix, where errors may occur along columns (data centers) and/or rows (correlated data among data centers), where several columns may not be available or contacted, and where an eavesdropper obtains information from several columns. These type of errors are called *crisscross errors* and were first studied in [55]. As noticed in that work, this type of reliability and security can be obtained by coset coding schemes that are reliable and secure as in Definition 0.4.

Informally, "rank reliability and security" is stronger than "crisscross reliability and security". Hence we will consider the former type of reliability and security throughout this subsection.

In Paper D, we give a construction of a coset coding scheme that is universal reliable and secure in this context and which has optimal information rate and communication overheads. The ideas behing the modelling of this scenario and the given optimal construction are based on those from *communication efficient secret sharing* [6, 33, 64].

To obtain the mentioned optimal communication overheads, we need to divide packets (*subpacketization*). That is, we will consider matrices in $\mathbb{F}_q^{\alpha m \times n}$ for some positive integer α.

We start by defining communication overheads:

Definition 0.12 ([D]). For a full-rank matrix $A \in \mathbb{F}_q^{d \times n}$ with rows $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_d \in \mathbb{F}_q^n$, we say that certain preprocessing functions $E_{A,i} : \mathbb{F}_q^{\alpha m} \longrightarrow \mathbb{F}_q^{\beta_i m}$, for $i = 1, 2, \ldots, d$, are t-error-correcting with respect to a coset coding scheme $\mathcal{P}_\mathcal{S} = \{\mathcal{C}_X\}_{X \in \mathcal{S}}$, $\mathcal{S} = \mathbb{F}_q^{\alpha m \times \ell}$, if there exists a decoding function $D_A : \prod_{i=1}^d \mathbb{F}_q^{\beta_i m} \longrightarrow \mathbb{F}_q^{\alpha m \times \ell}$ such that

$$D_A \left(\left(E_{A,i} \left(C\mathbf{a}_i^T + \mathbf{e}_i \right) \right)_{i=1}^d \right) = X,$$

for all $C \in \mathcal{C}_X$, all $X \in \mathbb{F}_q^{\alpha m \times \ell}$ and all error matrices $E \in \mathbb{F}_q^{\alpha m \times d}$ of rank at most t with columns $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_d \in \mathbb{F}_q^{\alpha m}$.

We define the communication overhead of the corresponding matrix A and preprocessing functions as

$$\mathrm{CO}(A) = \sum_{i=1}^d \frac{\beta_i}{\alpha} - \ell.$$

Recall from [60, Th. 12] that a general bound on ℓ -equivalently, on the information rate- is the following:

$$\ell \leq n - 2t - \rho - \mu, \tag{2}$$

with parameters as in Definition 0.4. In Paper D we obtain the following lower bound on communication overheads based on its Hamming-analog [33, Th. 1]. Observe that only erasures, and not errors, are considered in communication efficient secret sharing. Thus, the following result is not a trivial rank-analog of [33, Th. 1].

Proposition 0.13 ([D]). *If a coset coding scheme is universally secure under μ observations, then for a full-rank matrix $A \in \mathbb{F}_q^{d \times n}$ and preprocessing functions*

$E_{A,i} : \mathbb{F}_q^{\alpha m} \longrightarrow \mathbb{F}_q^{\beta_i m}$, for $i = 1, 2, \ldots, d$, that are t-error-correcting with respect to such scheme, it holds that:

$$\mathrm{CO}(A) \geq \frac{\ell(2t+\mu)}{d-2t-\mu}. \tag{3}$$

The optimal construction in Paper D is based on the optimal constructions of communication efficient secret sharing schemes in [6, 33]. It can be summarized as follows:

Theorem 0.12 ([D]). *Choose integers k_2, k_1, t_0 and ρ_0 such that $0 \leq k_2 < k_1 \leq n$ and $2t_0 + \rho_0 = n - k_1$, choose any subset $\mathcal{D} \subseteq [n-\rho_0, n]$ such that $n - \rho_0 \in \mathcal{D}$, and denote the elements in $\mathcal{D}$ by $d_h = n - \rho_0 < d_{h-1} < \ldots < d_2 < d_1$.*

Using Gabidulin codes [21, 55] in $\mathbb{F}_{q^m}^n$, we may explicitly construct a coset coding scheme $\mathcal{P}_{\mathcal{S}}$, $\mathcal{S} = \mathbb{F}_q^{\alpha m \times \ell}$, such that $\ell = k_1 - k_2$, it is universally t-error and ρ-erasure-correcting if $2t + \rho \leq n - k_1$, and is universally secure under μ observations if $\mu \leq k_2$. In particular, the scheme is optimal in the sense of (2). Moreover, it holds that

$$\alpha = \mathrm{LCM}\left(d_1 - 2t_0 - k_2, d_2 - 2t_0 - k_2, \ldots, d_h - 2t_0 - k_2\right).$$

In addition, for any $d \in \mathcal{D}$ and any full-rank matrix $A \in \mathbb{F}_q^{d \times n}$, there exist preprocessing functions $E_{A,i} : \mathbb{F}_q^{\alpha m} \longrightarrow \mathbb{F}_q^{\ell \alpha m/(d-2t_0-k_2)}$, for $i = 1, 2, \ldots, d$, which are t_0-error-correcting and satisfying equality in (3), hence having optimal communication overheads for all $d \in \mathcal{D}$.

2 Rank-metric properties of skew cyclic codes

In this section, we collect our main results concerning skew cyclic codes and their rank-metric properties: Structure, minimum rank distance, rank error-correcting algorithms and rank equivalences and degenerateness. These results are contained in Papers E, F and G, and correspond to the second group of results mentioned in the Abstract.

2.1 Preliminaries

Skew cyclic codes play a similar role with respect to the rank metric as that played by cyclic codes with respect to the Hamming metric.

Throughout this section, we will fix positive integers m, n and r such that m divides rn, and we will consider the four finite fields $\mathbb{F}_q$, $\mathbb{F}_{q^r}$, $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^{rn}}$ shown in the following graph, where $\mathbb{F} \longrightarrow \mathbb{F}'$ means that $\mathbb{F}'$ is an extension of $\mathbb{F}$:

$$\begin{tikzcd}
 & \mathbb{F}_q \arrow[dl] \arrow[dr] & \\
\mathbb{F}_{q^m} \arrow[dr] & & \mathbb{F}_{q^r} \arrow[dl] \\
 & \mathbb{F}_{q^{rn}} &
\end{tikzcd}$$

For convenience, we will also denote coordinates from 0 to $n-1$ and consider them as integers modulo n. Moreover, throughout this subsection, we will use the notation $[i] = q^i$, for $i = 0, 1, 2, \ldots$.

The concept of skew cyclic code in $\mathbb{F}_{q^m}^n$ of order r, or q^r-cyclic code, was given first in [21] when $r = 1$ and $m = n$, then extended in [22] to the cases $m \neq n$, and the general definition was first given in [8]:

Definition 0.14. Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be an arbitrary (linear or non-linear) code. We say that it is skew cyclic of order r, or q^r-cyclic if the q^r-shifted vector

$$\sigma_{r,n}(\mathbf{c}) = (c_{n-1}^{[r]}, c_0^{[r]}, c_1^{[r]}, \ldots, c_{n-2}^{[r]}) \tag{4}$$

lies in $\mathcal{C}$, for every $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$.

The main property of $\mathbb{F}_{q^m}$-linear q^r-cyclic codes is that they can be described as left ideals of quotients of *skew polynomial rings*. These rings were first introduced by Ore in [47], where the special case of skew polynomials over finite fields, also named *linearized polynomials*, were studied with more detail in [46].

Formally, a q^r-linearized polynomial (abbreviated as q^r-polynomial) over $\mathbb{F}_{q^m}$ is a polynomial in x of the form

$$F(x) = F_0 x + F_1 x^{[r]} + F_2 x^{[2r]} + \cdots + F_d x^{[dr]},$$

where $F_0, F_1, \ldots, F_d \in \mathbb{F}_{q^m}$, for $i = 0, 1, 2, \ldots, d$. We will denote $\deg_{q^r}(F(x)) = d$ if $F_d \neq 0$, also called *q^r-degree*, and consider the symbolic product $\otimes$ in $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$, defined as follows

$$F(x) \otimes G(x) = F(G(x)),$$

for any $F(x), G(x) \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$. Endowed with this product and usual addition, $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ is a left and right Euclidean domain, that is, left and right Euclidean divisions exist.

The previously mentioned algebraic characterization was obtained independently in [8, Th. 1] and [22, Lemma 3]:

Lemma 0.15. *A code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is $\mathbb{F}_{q^m}$-linear and q^r-cyclic if, and only if, $\mathcal{C}(x)$ is a left ideal in $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$, where*

$$\mathcal{C}(x) = \{c_0 x + c_1 x^{[r]} + \cdots + c_{n-1} x^{[(n-1)r]} + (x^{[rn]} - x) : (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}\}.$$

In the following, we will identify $\mathcal{C}$ with $\mathcal{C}(x)$, and for a q^r-linearized polynomial $F(x) \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$, we will denote by F its residue class modulo $x^{[rn]} - x$.

Skew cyclic codes admit other analogous descriptions as those of cyclic codes. These were proven in [9], in [22] for $r = 1$, and originally in [21] for $r = 1$ and $m = n$:

Theorem 0.13. *There exists a unique q^r-polynomial $G(x) = G_0x + G_1x^{[r]} + \cdots + G_{n-k}x^{[(n-k)r]}$ over $\mathbb{F}_{q^m}$ of q^r-degree $n-k$ that is monic and of minimal q^r-degree among the q^r-polynomials whose residue class modulo $x^{[rn]} - x$ lies in $\mathcal{C}(x)$. It satisfies that $\mathcal{C}(x) = (G)$. There exists another (unique) q^r-polynomial $H(x) = H_0x + H_1x^{[r]} + \cdots + H_kx^{[kr]}$ over $\mathbb{F}_{q^m}$ such that $x^{[rn]} - x = G(x) \otimes H(x) = H(x) \otimes G(x)$. They satisfy:*

1. *A q^r-polynomial F lies in $\mathcal{C}(x)$ if, and only if, $G(x)$ divides $F(x)$ on the right.*

2. *The q^r-polynomials $x \otimes G, x^{[r]} \otimes G, \ldots, x^{[(k-1)r]} \otimes G$ constitute a basis of $\mathcal{C}(x)$.*

3. *The dimension of $\mathcal{C}$ is $k = n - \deg_{q^r}(G(x))$.*

4. *$\mathcal{C}$ has a generator matrix given by*

$$\begin{pmatrix} G_0 & G_1 & \ldots & G_{n-k} & 0 & \ldots & 0 \\ 0 & G_0^{[r]} & \ldots & G_{n-k-1}^{[r]} & G_{n-k}^{[r]} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & G_0^{[(k-1)r]} & G_1^{[(k-1)r]} & \ldots & G_{n-k}^{[(k-1)r]} \end{pmatrix}.$$

5. *A q^r-polynomial F lies in $\mathcal{C}(x)$ if, and only if, $F \otimes H = 0$.*

6. *$\mathcal{C}$ has a parity check matrix (over $\mathbb{F}_{q^m}$) given by*

$$\begin{pmatrix} h_k & h_{k-1} & \ldots & h_0 & 0 & \ldots & 0 \\ 0 & h_k^{[r]} & \ldots & h_1^{[r]} & h_0^{[r]} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & h_k^{[(n-k-1)r]} & h_{k-1}^{[(n-k-1)r]} & \ldots & h_0^{[(n-k-1)r]} \end{pmatrix},$$

   where $h_i = H_i^{[(k-i)r]}$.

7. *$\mathcal{C}^\perp$ is also q^r-cyclic and its generator of minimal q^r-degree is $H^\perp(x) = (h_kx + h_{k-1}x^{[r]} + \cdots + h_0x^{[kr]})/h_0$.*

The q^r-polynomial $G(x)$ will be called the *minimal generator* of $\mathcal{C}(x)$, and $H(x)$ will be called the *minimal check q^r-polynomial* of $\mathcal{C}(x)$.

One of the most well-known families of skew cyclic codes is a subfamily of *generalized Gabidulin codes*. These codes were introduced first in [21] when $r = 1$, and then in general in [38], and are defined as follows. Assume that $n \leq m$ and r and m are coprime, and take a vector $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are linearly independent over $\mathbb{F}_q$, and an integer $1 \leq k \leq n$. We define the (generalized) Gabidulin code of dimension k in $\mathbb{F}_{q^m}^n$ as the $\mathbb{F}_{q^m}$-linear code $\mathrm{Gab}_{k,r}(\boldsymbol{\alpha})$ with generating matrix given by

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \ldots & \alpha_n \\ \alpha_1^{[r]} & \alpha_2^{[r]} & \alpha_3^{[r]} & \ldots & \alpha_n^{[r]} \\ \alpha_1^{[2r]} & \alpha_2^{[2r]} & \alpha_3^{[2r]} & \ldots & \alpha_n^{[2r]} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{[kr]} & \alpha_2^{[kr]} & \alpha_3^{[kr]} & \ldots & \alpha_n^{[kr]} \end{pmatrix}.$$

These codes are maximum rank distance, that is, $d_R(\mathrm{Gab}_{k,r}(\boldsymbol{\alpha})) = n - k + 1$. Moreover, they are q^r-cyclic whenever $m = n$ and $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

2.2 Root spaces and bounds on the minimum rank distance

In this subsection, we establish an anti-isomorphism between the lattice of skew cyclic codes and the lattice of vector spaces of roots of skew polynomials. Then we use the description of skew cyclic codes in terms of roots to obtain lower bounds on their minimum rank distance. These bounds are based on the well-known shift bound and Hartmann-Tzeng bound, and they extend the rank version of the BCH bound given in [12, Prop. 1].

Observe first that a q^r-linearized polynomial $F(x) \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ defines an $\mathbb{F}_{q^r}$-linear map $F : \mathbb{F}_{q^{rn}} \longrightarrow \mathbb{F}_{q^{rn}}$, and in particular its set of roots in $\mathbb{F}_{q^{rn}}$ is an $\mathbb{F}_{q^r}$-linear vector space.

Definition 0.16 ([E]). Given a residue class $F = F(x) + (x^{[rn]} - x)$, we define its root space, denoted as $Z(F)$, as the $\mathbb{F}_{q^r}$-linear vector space of roots in $\mathbb{F}_{q^{rn}}$ of $F(x)$.

Finally, define the map ρ_r between the family of $\mathbb{F}_{q^m}$-linear q^r-cyclic codes in $\mathbb{F}_{q^m}^n$ and the family of q^r-root spaces over $\mathbb{F}_{q^m}$ in $\mathbb{F}_{q^{rn}}$ by $\rho_r(\mathcal{C}) = \mathcal{T}$, where $\mathcal{T} = Z(G)$ and $G(x)$ is the minimal generator of $\mathcal{C}(x)$.

The first main result in Paper E is the following:

Theorem 0.14 ([E]). *The map ρ_r in Definition 0.16 is a lattice anti-isomorphism. More concretely, it is bijective and the following properties hold.*

Let $\mathcal{C}_1(x)$ and $\mathcal{C}_2(x)$ be two q^r-cyclic codes with minimal generators $G_1(x)$ and $G_2(x)$, respectively. Set $\mathcal{T}_1 = Z(G_1)$ and $\mathcal{T}_2 = Z(G_2)$. We have that

1. *$\mathcal{C}_1(x) \cap \mathcal{C}_2(x)$ is the q^r-cyclic code whose minimal generator is given by $M(x) = \mathrm{lcm}(G_1(x), G_2(x))$ (on the right), and $Z(M) = \mathcal{T}_1 + \mathcal{T}_2$.*
2. *$\mathcal{C}_1(x) + \mathcal{C}_2(x)$ is the q^r-cyclic code whose minimal generator is given by $D(x) = \mathrm{gcd}(G_1(x), G_2(x))$ (on the right), and $Z(D) = \mathcal{T}_1 \cap \mathcal{T}_2$.*
3. *$\mathcal{C}_1(x) \subseteq \mathcal{C}_2(x)$ if, and only if, $G_2(x)$ divides $G_1(x)$ on the right, and this holds if, and only if, $\mathcal{T}_2 \subseteq \mathcal{T}_1$.*

Moreover, root spaces also give core information about the corresponding skew cyclic codes:

Theorem 0.15 ([E]). *Let $\mathcal{T} = \rho_r(\mathcal{C})$ as in Definition 0.16, then:*

1. *$G(x) = \prod_{\beta \in \mathcal{T}}(x - \beta)$.*
2. *The dimension of $\mathcal{C}$ over $\mathbb{F}_{q^m}$ is $k = n - \dim_{\mathbb{F}_{q^r}}(\mathcal{T})$.*
3. *For a q^r-polynomial $F(x)$, it holds that $F \in \mathcal{C}(x)$ if, and only if, $F(\beta) = 0$, for all $\beta \in \mathcal{T}$.*
4. *Let $\beta_1, \beta_2, \ldots, \beta_{n-k}$ be a basis of $\mathcal{T}$ over $\mathbb{F}_{q^r}$. Then the matrix*

$$\begin{pmatrix} \beta_1 & \beta_1^{[r]} & \beta_1^{[2r]} & \cdots & \beta_1^{[(n-1)r]} \\ \beta_2 & \beta_2^{[r]} & \beta_2^{[2r]} & \cdots & \beta_2^{[(n-1)r]} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \beta_{n-k} & \beta_{n-k}^{[r]} & \beta_{n-k}^{[2r]} & \cdots & \beta_{n-k}^{[(n-1)r]} \end{pmatrix}$$

   is a parity check matrix of $\mathcal{C}$ over $\mathbb{F}_{q^{rn}}$.

5. *A q^r-polynomial $\widetilde{G}$ generates $\mathcal{C}(x)$ if, and only if, $Z(\widetilde{G}) = \mathcal{T}$, which holds if, and only if, $G(x) = \mathrm{gcd}(\widetilde{G}(x), x^{[rn]} - x)$ (on the right).*

Finally, this root description will allow us in Paper E to give lower bounds on the minimum rank distance of skew cyclic codes analogous to the shift bound [28] and the Hartmann-Tzeng bound [63]. To that end, we need to define independent sequences of $\mathbb{F}_{q^r}$-linear vector subspaces of $\mathbb{F}_{q^{rn}}$ with respect to some $\mathbb{F}_{q^r}$-linear subspace $\mathcal{S} \subseteq \mathbb{F}_{q^{rn}}$.

Definition 0.17 ([E]). Given $\mathbb{F}_{q^r}$-linear subspaces $\mathcal{S}, \mathcal{I}_0, \mathcal{I}_1, \mathcal{I}_2, \ldots \subseteq \mathbb{F}_{q^{rn}}$, we say that the sequence $\mathcal{I}_0, \mathcal{I}_1, \mathcal{I}_2, \ldots$ is independent with respect to $\mathcal{S}$ if the following hold:

1. $\mathcal{I}_0 = \{\mathbf{0}\}$.
2. For $i > 0$, either

(a) $\mathcal{I}_i = \mathcal{I}_j \oplus \langle \beta \rangle$, for some $0 \leq j < i$, $\mathcal{I}_j \subseteq \mathcal{S}$ and $\beta \notin \mathcal{S}$, or

(b) $\mathcal{I}_i = \mathcal{I}_j^{[br]}$, for some $0 \leq j < i$ and some integer $b \geq 0$.

We say that a subspace $\mathcal{I} \subsetneqq \mathbb{F}_{q^{rn}}$ is independent with respect to $\mathcal{S}$ if it is a space in a sequence that is independent with respect to $\mathcal{S}$.

Our rank version of the shift bound [63, Th. 11] is the following:

Theorem 0.16 ([E]). *Let $F \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$ and $\mathcal{S} = Z(F) = \{\beta \in \mathbb{F}_{q^{rn}} : F(\beta) = 0\}$, as in Definition 0.16. If $\mathcal{I} \subsetneqq \mathbb{F}_{q^{rn}}$ is an $\mathbb{F}_{q^r}$-linear subspace independent with respect to $\mathcal{S}$, then*

$$\mathrm{wt_R}(F) \geq \dim_{\mathbb{F}_{q^r}}(\mathcal{I}),$$

where we use the notation

$$\mathrm{wt_R}(F_0 x + F_1 x^{[r]} + \cdots + F_{n-1} x^{[(n-1)r]}) = \mathrm{wt_R}(F_0, F_1, \ldots, F_{n-1}).$$

As in the case of cyclic codes and the Hamming distance, we may derive a rank version of the Hartmann-Tzeng bound [28]:

Corollary 0.18 ([E]). *Take integers $c > 0$, $\delta > 0$ and $s \geq 0$, with $\delta + s \leq \min\{m, n\}$ and $d = \gcd(c, n) < \delta$, and let $\alpha \in \mathbb{F}_{q^{rn}}$ be such that $\mathcal{A} = \{\alpha^{[(i+jc)r]} : 0 \leq i \leq \delta - 2, 0 \leq j \leq s\}$ is a linearly independent (over $\mathbb{F}_{q^r}$) set of vectors, not necessarily pairwise distinct.*

If $F \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$ satisfies that $\mathcal{A} \subseteq \mathcal{T} = Z(F)$, then $\mathrm{wt_R}(F) \geq \delta + s$. In particular, if $\mathcal{C} = \rho_r^{-1}(\mathcal{T})$, with ρ_r as in Definition 0.16, then

$$d_R(\mathcal{C}) \geq \delta + s.$$

Observe that the rank version of the BCH bound given in [12, Prop. 1] is obtained when $s = 0$ and $c = 1$.

2.3 Rank error-correcting pairs

Error-correcting pairs for the Hamming metric were introduced independently by Kötter [36] and Pellikaan [49, 50]. They serve as building blocks to obtain error-correcting algorithms and bounds on the minimum Hamming distance for many families of codes [20, 50, 51].

In this subsection, we will adapt this technique to rank-metric codes, as done in Paper F. We will introduce rank error-correcting pairs for $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$ and for $\mathbb{F}_q$-linear codes in $\mathbb{F}_q^{m \times n}$, and relate both via the map $M_{\boldsymbol{\alpha}}$ from (1). Some skew cyclic codes, including generalized Gabidulin codes, admit rank error-correcting pairs. Thus the results in this subsection enable us to provide new rank error-correcting algorithms for skew cyclic codes.

We also remark here that rank error-correcting pairs of type II (see definitions below) were obtained in the case $m = n$ independently by Alain Couvreur [14].

One of the main ingredients in the Hamming case is the *coordinate-wise* or *Schur product* of codewords in $\mathbb{F}_q^n$. The fact that such product preserves products of polynomials after evaluation makes error-correcting pairs be applicable to many families of codes.

The main dificulty in obtaining rank error-correcting pairs is finding the appropriate products of codewords in $\mathbb{F}_{q^m}^n$ or $\mathbb{F}_q^{m\times n}$. Interestingly, the conventional product of matrices in $\mathbb{F}_q^{m\times n}$ induces a product in $\mathbb{F}_{q^m}^n$ via $M_{\boldsymbol{\alpha}}$ that preserves symbolic products of q-linearized polynomials.

Unfortunately, this product depends on a prefixed basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, which throughout the subsection will be denoted by $\alpha_1, \alpha_2, \ldots, \alpha_m \in \mathbb{F}_{q^m}$.

Definition 0.19 ([F]). Define the product $\star : \mathbb{F}_{q^m}^m \times \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$ as follows. For every $\mathbf{c} \in \mathbb{F}_{q^m}^m$ and every $\mathbf{d} \in \mathbb{F}_{q^m}^n$, let

$$\mathbf{c} \star \mathbf{d} = \sum_{i=1}^{m} c_i \mathbf{d}_i,$$

where $\mathbf{d} = \sum_{i=1}^{m} \alpha_i \mathbf{d}_i$ and $\mathbf{d}_i \in \mathbb{F}_q^n$, for all i, and $\mathbf{c} = (c_1, c_2, \ldots, c_m)$.

The previously mentioned properties can be gathered in the following proposition:

Proposition 0.20 ([F]). *If we denote $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_m)$, then it holds that $\boldsymbol{\alpha}^{[j]} \star \mathbf{c} = \mathbf{c}^{[j]}$, for all $\mathbf{c} \in \mathbb{F}_{q^m}^n$ and all j. In particular,*

$$\mathrm{ev}_{\mathbf{b}}(F(x) \otimes G(x)) = \mathrm{ev}_{\boldsymbol{\alpha}}(F(x)) \star \mathrm{ev}_{\mathbf{b}}(G(x)),$$

for all $\mathbf{b} \in \mathbb{F}_{q^m}^n$ and all $F(x), G(x) \in \mathcal{L}_q\mathbb{F}_{q^m}[x]$, where we use the notation $\mathrm{ev}_{\mathbf{b}}(F(x)) = (F(b_1), F(b_2), \ldots, F(b_n))$. In addition, we have that

$$M_{\boldsymbol{\alpha}}(\mathbf{c} \star \mathbf{d}) = M_{\boldsymbol{\alpha}}(\mathbf{c}) M_{\boldsymbol{\alpha}}(\mathbf{d}),$$

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

We may now define rank error-correcting pairs for $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$ and for $\mathbb{F}_q$-linear codes in $\mathbb{F}_q^{m\times n}$:

Definition 0.21 ([F]). Given $\mathbb{F}_{q^m}$-linear codes $\mathcal{A} \subseteq \mathbb{F}_{q^m}^n$ and $\mathcal{B} \subseteq \mathbb{F}_{q^m}^m$, the pair $(\mathcal{A}, \mathcal{B})$ is called a t-rank error-correcting pair (t-RECP) of type I for $\mathcal{C}$ if the following properties hold:

1. $\mathcal{B} \star \mathcal{A} \subseteq \mathcal{C}^{\perp}$, where $\mathcal{B} \star \mathcal{A}$ denotes the $\mathbb{F}_{q^m}$-linear vector space generated by $\mathbf{b} \star \mathbf{a}$, for $\mathbf{b} \in \mathcal{B}$ and $\mathbf{a} \in \mathcal{A}$.

2. $\dim(\mathcal{A}) > t$.

3. $d_R(\mathcal{B}^\perp) > t$.

4. $d_R(\mathcal{A}) + d_R(\mathcal{C}) > n$.

Definition 0.22 ([F]). Given $\mathbb{F}_q$-linear codes $\mathcal{A} \subseteq \mathbb{F}_q^{m\times n}$ and $\mathcal{B} \subseteq \mathbb{F}_q^{m\times m}$, the pair $(\mathcal{A}, \mathcal{B})$ is called a t-rank error-correcting pair (t-RECP) of type II for $\mathcal{C}$ if the following properties hold:

1. $\mathcal{BA} \subseteq \mathcal{C}^\perp$, where $\mathcal{BA}$ denotes the $\mathbb{F}_q$-linear vector space generated by BA, for $B \in \mathcal{B}$ and $A \in \mathcal{A}$.

2. $\dim(\mathcal{A}) > mt$.

3. $d_R(\mathcal{B}^\perp) > t$.

4. $d_R(\mathcal{A}) + d_R(\mathcal{C}) > n$.

As in the previous section, we define in this context the dual of an $\mathbb{F}_q$-linear code $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ as $\mathcal{C}^\perp = \{D \in \mathbb{F}_q^{m\times n} : \mathrm{Trace}(CD^T) = 0, \forall C \in \mathcal{C}\}$.

As stated in the beginning of this subsection, rank error-correcting pairs of type II were obtained in the case $m = n$ independently by Alain Couvreur [14].

In both cases, these codes induce a rank error-correcting algorithm able to correct t rank errors in polynomial time. We give a sketch of the procedure for RECPs of type I:

Assume that the received codeword is $\mathbf{r} = \mathbf{c} + \mathbf{e}$, with $\mathbf{c} \in \mathcal{C}$, $\mathcal{L} = \mathrm{Row}(M_{\boldsymbol{\alpha}}(\mathbf{e})) \subseteq \mathbb{F}_q^n$ and $\dim(\mathcal{L}) \leq t$. Compute the $\mathbb{F}_{q^m}$-linear vector space

$$\mathcal{K}(\mathbf{r}) = \{\mathbf{a} \in \mathcal{A} : (\mathbf{b} \star \mathbf{a}) \cdot \mathbf{r} = 0, \forall \mathbf{b} \in \mathcal{B}\},$$

which is equal to $\mathcal{K}(\mathbf{e})$ by the first condition of t-RECP. Observe that $\mathcal{K}(\mathbf{r})$ can be described by a system of $\mathcal{O}(n)$ $\mathbb{F}_{q^m}$-linear equations.

By the third condition of t-RECP, it can be shown that $\mathcal{A}(\mathcal{L}) = \mathcal{K}(\mathbf{e}) = \mathcal{K}(\mathbf{r})$, where

$$\mathcal{A}(\mathcal{L}) = \{\mathbf{a} \in \mathcal{A} : \mathrm{Row}(M_{\boldsymbol{\alpha}}(\mathbf{a})) \subseteq \mathcal{L}^\perp\},$$

which was defined in [34].

By the second condition of t-RECP, it can be proven that $\mathcal{A}(\mathcal{L}) = \mathcal{A} \cap \mathcal{V}_{\mathcal{L}}^\perp \neq \{\mathbf{0}\}$, and therefore we may take a nonzero $\mathbf{a} \in \mathcal{A}(\mathcal{L})$. Define $\mathcal{L}' = \mathrm{Row}(M_{\boldsymbol{\alpha}}(\mathbf{a}))^\perp$. Since $\mathbf{a} \in \mathcal{A}(\mathcal{L})$, we have that $\mathcal{L} \subseteq \mathcal{L}'$.

Now, by the fourth condition of t-RECP, we have that

$$\dim(\mathcal{L}') = n - \mathrm{wt_R}(\mathbf{a}) \leq n - d_R(\mathcal{A}) < d_R(\mathcal{C}).$$

Hence we may compute $\mathbf{e}$ or $\mathbf{c}$ by solving a system of $\mathbb{F}_{q^m}$-linear equations using a generator matrix G of $\mathcal{L}'^{\perp}$, or a parity check matrix H of $\mathcal{C}$, respectively. This has complexity $\mathcal{O}(n^3)$ over $\mathbb{F}_{q^m}$.

We have the following connection between both types of RECPs:

Theorem 0.17 ([F]). *Let $\alpha'_1, \alpha'_2, \ldots, \alpha'_m \in \mathbb{F}_{q^m}$ be an orthogonal basis of $\alpha_1, \alpha_2, \ldots, \alpha_m$ over $\mathbb{F}_q$. Take $\mathbb{F}_{q^m}$-linear codes $\mathcal{A}, \mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ and $\mathcal{B} \subseteq \mathbb{F}_{q^m}^m$.*

If $(\mathcal{A}, \mathcal{B})$ is a t-RECP of type I for $\mathcal{C}$ (in the basis $\boldsymbol{\alpha}$), then $(M_{\boldsymbol{\alpha}}(\mathcal{A}), M_{\boldsymbol{\alpha}}(\mathcal{B}))$ is a t-RECP of type II for $M_{\boldsymbol{\alpha}'}(\mathcal{C})$.

As examples, we see that generalized Gabidulin codes admit RECPs of type I:

Proposition 0.23 ([F]). *If $t > 0$, $\mathcal{A} = \mathrm{Gab}_{t+1,r}(\boldsymbol{\alpha}) \subseteq \mathbb{F}_{q^m}^n$, $\mathcal{B} = \mathrm{Gab}_{t,r}(\boldsymbol{\alpha}) \subseteq \mathbb{F}_{q^m}^m$ and $\mathcal{C} = \mathrm{Gab}_{2t,r}(\boldsymbol{\alpha})^{\perp} \subseteq \mathbb{F}_{q^m}^n$, then $(\mathcal{A}, \mathcal{B})$ is a t-RECP of type I for $\mathcal{C}$.*

Some other skew cyclic codes also admit RECPs of type I. Instead of giving these details, we show that the rank Hartmann-Tzeng bound (Corollary 0.18) can be extended to general $\mathbb{F}_q$-linear codes in $\mathbb{F}_q^{m \times n}$ as follows:

Theorem 0.18 ([F]). *Take $\mathbb{F}_q$-linear codes $\mathcal{A}, \mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ and $\mathcal{B} \subseteq \mathbb{F}_q^{m \times m}$, and assume that $\mathcal{B}\mathcal{A} \subseteq \mathcal{C}^{\perp}$. If $d_R(\mathcal{A}^{\perp}) > a > 0$ and $d_R(\mathcal{B}^{\perp}) > b > 0$, then $d_R(\mathcal{C}) \geq a + b$.*

2.4 Rank equivalences between skew cyclic codes

We conclude this section by analysing rank equivalences between skew cyclic codes of different lengths. Observe that cyclic codes and skew cyclic codes of different lengths cannot be equivalent to each other for the Hamming metric, since Hamming-metric equivalences are given by permutations of coordinates after coordinate-wise products with some constant non-zero factors. Therefore the study in this subsection has no analogy for Hamming-metric codes.

Our definition of *rank equivalence* is that of Definition 0.6 and Theorem 0.3. All the results of this subsection (both statements and proofs) make repeated use of that theorem.

Our objective is to find the $\mathbb{F}_{q^m}$-linear skew cyclic code of smallest length that is rank equivalent to a given one. With this motivation, we consider different types of lengths of a given skew cyclic code:

Definition 0.24 ([G]). Given an $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, an element $a \in \mathbb{F}_q^*$ and an integer $r \geq 0$, we define the following numbers:

1. The rank length, $l_R(\mathcal{C})$, as the minimum n' such that $\mathcal{C}$ is rank equivalent to an $\mathbb{F}_{q^m}$-linear code of length n'.

2. The r-th skew length, $l_{Sk,r}(\mathcal{C})$, as the minimum n' such that $\mathcal{C}$ is rank equivalent to an $\mathbb{F}_{q^m}$-linear skew cyclic code of order r and length n', if such a code exists. We define $l_{Sk,r}(\mathcal{C}) = \infty$ otherwise.

3. The (a,r)-shift length, $l_{Sh,a,r}(\mathcal{C})$, as the minimum n' such that $\mathcal{C}$ is rank equivalent to a $\mathbb{F}_{q^m}$-linear code of length n' by a rank equivalence ϕ such that $a(\sigma_{r,n'} \circ \phi) = \phi \circ \sigma_{r,n}$, if such a code exists. We define $l_{Sh,a,r}(\mathcal{C}) = \infty$ otherwise.

4. The period length, $l_P(\mathcal{C})$, as the minimum integer $1 \leq p \leq n$ that generates the ideal modulo n defined as $\{p' : c_{i+p'} = c_i, \forall i, \forall (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}\}$, which necessarily divides n.

The following lemma will be useful, since our given characterizations of rank equivalences in Theorem 0.3 make use of Galois closures as ambient spaces:

Lemma 0.25 ([G]). *If $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$ is $\mathbb{F}_{q^m}$-linear and Galois closed, then it is skew cyclic of some order if, and only if, it is skew cyclic of all orders. Given an $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, if it is skew cyclic of some order, then $\mathcal{C}^*$ is skew cyclic (of all orders).*

We recall from Proposition 0.7 that $l_R(\mathcal{C}) = d_{R,k}(\mathcal{C}) = \dim(\mathcal{C}^*)$, for any $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$. However, it holds that $l_R(\mathcal{C}) \leq l_{Sk,s}(\mathcal{C}) \leq l_{Sh,a,r}(\mathcal{C})$ and $l_{Sh,1,r}(\mathcal{C}) \leq l_P(\mathcal{C})$, where all of these inequalities are strict in many cases, for positive integers s and r, and for $a \in \mathbb{F}_q^*$.

Fortunately, thanks to the previous lemma, we may use the (classical) cyclic structure of skew cyclic Galois closed spaces to decide whether a rank equivalence exists between them:

Theorem 0.19 ([G]). *Let $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$ and $\mathcal{W} \subseteq \mathbb{F}_{q^m}^{n'}$ be $\mathbb{F}_{q^m}$-linear cyclic Galois closed spaces with the same dimension k and check polynomials $h(x)$ and $h'(x)$, respectively. Given $a \in \mathbb{F}_q^*$, an integer $r \geq 0$ and $\beta \in \mathbb{F}_{q^m}^*$ such that $\beta^{[r]} = b\beta$, for some $b \in \mathbb{F}_q^*$, the following are equivalent:*

1. *There exists a rank equivalence $\phi : \mathcal{V} \longrightarrow \mathcal{W}$ such that $a(\sigma_{r,n'} \circ \phi) = \phi \circ \sigma_{r,n}$ and β is as in Theorem 0.3.*

2. *$(ab)^k h'(x) = h(abx)$.*

As a consequence, we may derive the following relations between the previously defined lengths. Here, for $a \in \mathbb{F}_q$, we define the a-order of a polynomial $f(x) \in \mathbb{F}_{q^m}[x]$ as the minimum positive integer e such that $f(x)$ divides $x^e - a^e$ (in $\mathbb{F}_{q^m}[x]$), if one such e exists, and denote it by $\mathrm{ord}_a(f(x))$. If no such e exists, we define $\mathrm{ord}_a(f(x)) = \infty$.

Corollary 0.26 ([G]). *For an integer $s \geq 0$ and an $\mathbb{F}_{q^m}$-linear q^s-cyclic code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, where $h^0(x)$ is the check polynomial of $\mathcal{C}^*$, it holds that*

1. $l_R(\mathcal{C}) = \deg(h^0(x))$.

2. $l_{Sh,1,0}(\mathcal{C}) = l_P(\mathcal{C}) = \operatorname{ord}(h^0(x)) \leq n$.

3. More generally, if $a \in \mathbb{F}_q^*$, then $e = l_{Sh,a,0}(\mathcal{C}) = \operatorname{ord}_a(h^0(x))$.

4. More generally, if $a \in \mathbb{F}_q^*$ and $r \geq 0$, then

$$l_{Sh,a,r}(\mathcal{C}) = \min\{\operatorname{ord}_{ab}(h^0(x)) : b \in \mathbb{F}_q^*, \beta \in \mathbb{F}_{q^m}^*, \beta^{[r]} = b\beta\}.$$

In particular, $l_R(\mathcal{C}) = l_{Sk,s}(\mathcal{C}) = l_{Sh,1,r}(\mathcal{C}) = l_P(\mathcal{C})$ if, and only if, $\deg(h^0(x)) = \operatorname{ord}(h^0(x))$, which holds if, and only if, $h^0(x) = x^e - 1$, for some positive integer e.

Therefore we see that $l_R(\mathcal{C}) < l_{Sh,a,r}(\mathcal{C})$ in many cases, and $l_{Sk,s}(\mathcal{C})$ lies in between. From our work, it is not clear whether we may guarantee that $l_R(\mathcal{C}) = l_{Sk,s}(\mathcal{C})$ or $l_{Sk,s}(\mathcal{C}) = l_{Sh,a,r}(\mathcal{C})$, when $l_R(\mathcal{C}) < l_{Sh,a,r}(\mathcal{C})$. In particular, we cannot guarantee that the smallest length of an $\mathbb{F}_{q^m}$-linear code that is rank equivalent to a given skew cyclic code is attained by a skew cyclic code. Fortunately, we can guarantee that it can be attain by a *pseudo-skew cyclic code* in many cases.

For this purpose, we need some more definitions. Consider the *center* of $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$, denoted by $\mathbb{C}(\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x])$ and defined as the set of q^r-polynomials over $\mathbb{F}_{q^m}$ that commute with every other q^r-polynomial over $\mathbb{F}_{q^m}$. It is well-known that

$$\mathbb{C}(\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]) = \mathcal{L}_{q^l}\mathbb{F}_{q^d}[x],$$

where $l = \operatorname{lcm}(m,r)$ and $d = \gcd(m,r)$. We may now define pseudo-skew cyclic codes, which were introduced in [21] for $r = 1$ and $n = m$, and then independently in [22] for $r = 1$ and in [9] for general parameters:

Definition 0.27. Let $F(x) \in \mathbb{C}(\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x])$ such that $\deg_{q^r}(F(x)) = n$. For an $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, we define $\mathcal{C}_{F(x)}(x)$ as the image of $\mathcal{C}$ in $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(F(x))$ by the $\mathbb{F}_{q^m}$-linear vector space isomorphism $\mathbb{F}_{q^m}^n \longrightarrow \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(F(x))$ given by

$$(c_0, c_1, \ldots, c_{n-1}) \mapsto c_0 x + c_1 x^{[r]} + \cdots + c_{n-1} x^{[(n-1)r]}.$$

Then we say that $\mathcal{C}$ is pseudo-skew cyclic (of order r) if $\mathcal{C}_{F(x)}(x)$ is a left ideal in $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(F(x))$, for some $F(x) \in \mathbb{C}(\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x])$ such that $\deg_{q^r}(F(x)) = n$.

Next, for a positive integer s, we may define a ring automorphism $\theta_s : \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x] \longrightarrow \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ based on the s-th Frobenius map:

$$\theta_s(F_0 x + F_1 x^{[r]} + \cdots + F_d x^{[dr]}) = F_0^{[s]} x + F_1^{[s]} x^{[r]} + \cdots + F_d^{[s]} x^{[dr]},$$

for $F_0, F_1, F_2, \ldots, F_d \in \mathbb{F}_{q^m}$ and a positive integer d. This map induces a ring automorphism of $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$, since $\theta_s(x^{[rn]} - x) = x^{[rn]} - x$. With this tool, we may compute the minimal generator and check q^r-polynomials of the Galois closure of a skew cyclic code in terms of its own minimal generator and check q^r-polynomials:

Proposition 0.28 ([G]). *Take an $\mathbb{F}_{q^m}$-linear q^r-cyclic code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ with minimal generator and check q^r-polynomials $G(x)$ and $H(x)$, respectively. The minimal generator and check q^r-polynomials of $\mathcal{C}^*$ are $G^*(x)$ and $H_0(x)$, respectively, where we define*

$$F^{\perp}(x) = \left(\frac{F_d}{F_0^{[dr]}}\right) x + \left(\frac{F_{d-1}^{[r]}}{F_0^{[dr]}}\right) x^{[r]} + \cdots + \left(\frac{F_0^{[dr]}}{F_0^{[dr]}}\right) x^{[dr]},$$

$$F^{\top}(x) = \left(\frac{F_d}{F_0}\right)^{[(n-d)r]} x + \left(\frac{F_{d-1}}{F_0}\right)^{[(n-d+1)r]} x^{[r]} + \cdots + \left(\frac{F_0}{F_0}\right)^{[nr]} x^{[dr]},$$

$$F^*(x) = \gcd(F(x), \theta_1(F(x)), \ldots, \theta_{m-1}(F(x))),$$

$$F_0(x) = \operatorname{lcm}(F(x)^{\perp}, \theta_1(F(x))^{\perp}, \ldots, \theta_{m-1}(F(x))^{\perp})^{\top},$$

for $F(x) = F_0 x + F_1 x^{[r]} + \cdots + F_d x^{[dr]} \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ such that $F_0 \neq 0$.

Finally, we may state the above mentioned result on attaining the rank length of a skew cyclic code by a pseudo-skew cyclic code:

Theorem 0.20 ([G]). *Take an $\mathbb{F}_{q^m}$-linear q^r-cyclic code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ and assume that $H_0(x)$ is central. Then the map $\phi : \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(H_0(x)) \longrightarrow (G^*(x))/(x^{[rn]} - x)$ given by*

$$\phi(F(x)) = F(x) \otimes G^*(x)$$

is well-defined, maps left ideals to left ideals and constitutes a rank equivalence when seeing its domain and codomain as $\mathbb{F}_{q^m}$-linear Galois closed spaces.

Corollary 0.29 ([G]). *With notation as in the previous theorem, if $H_0(x)$ is central, then the length $l_R(\mathcal{C})$ is attained by an $\mathbb{F}_{q^m}$-linear pseudo-skew cyclic code that is a left ideal in the quotient ring $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(H_0(x))$.*

3 Secret sharing and further tools for raliable and secure communications

In this section, we diverge from the previous studies on rank-metric codes and consider the Hamming-analog of reliable and secure communications. We will first study the partial information leakage, and thus security robustness, of asymptotically good sequences of secret sharing schemes. Secondly, we will give further techniques for bounding zeros of polynomials and some of their consecutive Hasse derivatives. These type of zeros and derivatives have given applications in the theory of locally decodable codes [35] and subspace designs [26].

3.1 Partial information leakage in asymptotically good secret sharing

In this subsection, we will analyse the partial security behaviour of asymptotically good sequences of code-based secret sharing schemes. This study relies on the relative generalized Hamming weights of the underlying linear code pairs. Observe that this problem has no analogy in the theory of reliable and secure communications based on rank-metric codes, since linear codes with optimal rank-metric parameters exist for all possible lengths [16].

Secret sharing was introduced independently by Shamir [57] and Blakley [7]. Informally, it is a method to encode a secret message into n shares in such a way that some sets of shares can recover the secret, whereas other sets give no information about it. As explained in [13] and [40], we may regard secret sharing schemes as coset coding schemes (Definition 0.2), which can also be constructed using nested linear code pairs as in Definition 0.3.

However, we need to slightly modify the definitions in Subsection 1.1. We will always consider $m = 1$, replace $\mathbb{F}_q^{1 \times n}$ by $\mathbb{F}_q^n = \mathbb{F}_q^{n \times 1}$, and we adapt Definition 0.4 to this context as follows. We say that secret sharing scheme has

1. t-privacy if for every subset $I \subseteq \{1, 2, \ldots, n\}$ of size at most t, it holds that
$$H(\mathbf{x}|\mathbf{c}P_I^T) = H(\mathbf{x}),$$
where $P_I \in \mathbb{F}_q^{\#I \times n}$ is the matrix obtained from restricting the $n \times n$ identity matrix to its rows indexed by I.

2. r-reconstruction if for every subset $J \subseteq \{1, 2, \ldots, n\}$ of size at least r, there exists a decoding function $D_J : \mathbb{F}_q^{\#J} \longrightarrow \mathcal{S}$ such that $D_J(\mathbf{y}) = \mathbf{x}$, for every $\mathbf{x} \in \mathcal{S}$ and
$$\mathbf{y} = \mathbf{c}P_J^T,$$
where $\mathbf{c} \in \mathcal{C}_{\mathbf{x}}$.

However, our interest is in studying partial privacy and partial reconstruction of asymptotically good sequences of secret sharing schemes. We may define, as in the previous items, the m-th privacy threshold of the scheme as the maximum positive integer t_m such that from no set of t_m shares one can recover m bits (multiplied by $\log_2(q)$) of information about the secret. Analogously, we define the m-th reconstruction threshold of the scheme as the minimum positive integer r_m such that from any set of r_m shares one can obtain m bits (multiplied by $\log_2(q)$) of information about the secret.

Consider now a sequence of secret sharing schemes built from a sequence of nested linear code pairs $(\mathcal{C}_2(i) \subsetneqq \mathcal{C}_1(i) \subseteq \mathbb{F}_q^{n_i})_{i=1}^{\infty}$, with $n_i \longrightarrow \infty$, $\dim(\mathcal{C}_2(i)) / n_i \longrightarrow R_2$ and $\dim(\mathcal{C}_1(i))/n_i \longrightarrow R_1$, for $i \longrightarrow \infty$. Define $L = R_1 - R_2$, which corresponds to the asymptotic information rate of the sequence, that is, $L = \lim_{i \longrightarrow \infty} \ell_i / n_i$, where $\ell_i = \dim(\mathcal{C}_1(i)/\mathcal{C}_2(i))$, for all i. Next define

$$\Omega^{(1)} = \liminf_{i \to \infty} \frac{t_i}{n_i}, \quad \text{and} \quad \Omega^{(2)} = \limsup_{i \to \infty} \frac{r_i}{n_i}.$$

The sequence of secret sharing schemes is said to be asymptotically good if $\Omega^{(1)} > 0$ and $\Omega^{(2)} < 1$.

Now for fixed $\varepsilon_1, \varepsilon_2 > 0$, we formalize with the following parameters the asymptotic behaviour of the sequence in terms of partial privacy and partial reconstruction:

$$\begin{aligned} \Lambda^{(1)}(\varepsilon_1) \quad &= \quad \sup \Big\{ \liminf_{i \longrightarrow \infty} \frac{t_{m_1(i)}}{n_i} : (m_1(i))_{i=1}^{\infty} \text{ satisfies} \\ & \qquad\qquad 1 \leq m_1(i) \leq \ell_i, \lim_{i \to \infty} (m_1(i)/n_i) = \varepsilon_1 L \Big\}, \\ \Lambda^{(2)}(\varepsilon_2) \quad &= \quad \inf \Big\{ \limsup_{i \longrightarrow \infty} \frac{r_{\ell_i - m_2(i)+1}}{n_i} : (m_2(i))_{i=1}^{\infty} \text{ satisfies} \\ & \qquad\qquad 1 \leq m_2(i) \leq \ell_i, \lim_{i \to \infty} (m_2(i)/n_i) = \varepsilon_2 L \Big\}. \end{aligned}$$

We have the following fundamental bounds on the previous parameters:

$$\Lambda^{(1)}(\varepsilon_1) \leq R_2 + \varepsilon_1 L, \quad \text{and} \quad \Lambda^{(2)}(\varepsilon_2) \geq R_1 - \varepsilon_2 L,$$

and in particular, $\Lambda^{(2)}(\varepsilon_2) - \Lambda^{(1)}(\varepsilon_1) \geq L(1 - \varepsilon_1 - \varepsilon_2)$.

The first main result of this subsection is the following existential result on asymptotically good sequences of secret sharing schemes whose parameters $\Lambda^{(1)}(\varepsilon_1)$ and $\Lambda^{(2)}(\varepsilon_2)$ are arbitrarily close to the optimal values:

Theorem 0.21 ([H]). *For any $0 < R_2 < R_1 < 1$, there exists a sequence of secret sharing schemes with $L = R_1 - R_2$ and having simultaneously $\Lambda^{(1)}(\varepsilon_1)$ arbitrarily close to $R_2 + \varepsilon_1 L$ and $\Lambda^{(2)}(\varepsilon_2)$ arbitrarily close to $R_1 - \varepsilon_2 L$, for all $0 \leq \varepsilon_1, \varepsilon_2 \leq 1$.*

Unfortunately, the proof of this result, which is given in Paper H, is only existential and provides no explicit constructions. To overcome this issue, we propose in Paper H different strategies to obtain asymptotically good sequences of secret sharing schemes with near optimal values of $\Lambda^{(1)}(\varepsilon_1)$ and $\Lambda^{(2)}(\varepsilon_2)$, based on explicit sequences of algebraic geometry codes with good asymptotic parameters. Among these, we will concentrate on those code sequences based on the well-known Garcia-Stichtenoth's second tower of function fields [24]. Their main advantage is that the i-th algebraic geometry code pair in the sequence can be explicitly constructed with complexity $\mathcal{O}({n_i}^3 \log_q^3(n_i))$ over $\mathbb{F}_q$ [58].

We illustrate this idea from Paper H by stating one of its main consequences:

Theorem 0.22 ([H]). *Assume that q is a perfect square. We may construct a sequence of asymptotically good secret sharing schemes such that*

1. *If $1/(\sqrt{q}-1) \leq 1 - R_2$ and $\varepsilon_1 \geq \left(\frac{q}{q-1}\frac{1}{\sqrt{q}-1} - \frac{1}{q-1}(1-R_2)\right)/L$ then $\Lambda^{(1)}(\varepsilon_1) \geq R_2 + \varepsilon_1 L$.*
2. *If $1/(\sqrt{q}-1) \leq R_1$ and $\varepsilon_2 \geq \left(\frac{q}{q-1}\frac{1}{\sqrt{q}-1} - \frac{1}{q-1}R_1\right)/L$ then $\Lambda^{(2)}(\varepsilon_2) \leq R_1 - \varepsilon_2 L$.*

Moreover, the i-th scheme can be explicitly constructed with complexity $\mathcal{O}({n_i}^3 \log_q^3(n_i))$ over $\mathbb{F}_q$.

3.2 A footprint-type bound for consecutive Hasse derivatives of polynomials

In this subsection, we provide a fundamental algebraic tool for upper bounding the number of common zeros over a grid of some polynomials and a finite collection of their consecutive *Hasse derivatives*. These type of zeros and derivatives of polynomials have shown important applications in the theory of *locally decodable codes* [35] and *subspace designs* [26].

Throughout this section we will work over an arbitrary field $\mathbb{F}$ of arbitrary characteristic, and we will use the compact notation $\mathbf{x} = (x_1, x_2, \ldots, x_m)$ and $\mathbf{x}^{\mathbf{i}} = x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m}$, for a set of variables $x_1, x_2, \ldots x_m$ and a multiindex $\mathbf{i} = (i_1, i_2, \ldots, i_m) \in \mathbb{N}^m$. We recall now the definition of Hasse derivative from [29]:

Definition 0.30. Let $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ be a polynomial. Given another family of independent variables $\mathbf{z} = (z_1, z_2, \ldots, z_m)$, the polynomial $F(\mathbf{x}+\mathbf{z})$ can be written uniquely as

$$F(\mathbf{x}+\mathbf{z}) = \sum_{\mathbf{i} \in \mathbb{N}^m} F^{(\mathbf{i})}(\mathbf{x}) \mathbf{z}^{\mathbf{i}},$$

for some polynomials $F^{(\mathbf{i})}(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$, for $\mathbf{i} \in \mathbb{N}^m$. For a given multiindex $\mathbf{i} \in \mathbb{N}^m$, we define the $\mathbf{i}$-th Hasse derivative of $F(\mathbf{x})$ as the polynomial $F^{(\mathbf{i})}(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$.

We next formalize the concept of zero of a polynomial of at least a given *multiplicity* as that of common zero of the given polynomial and a given finite family of its derivatives:

Definition 0.31 ([I]). Let $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ be a polynomial, let $\mathbf{a} \in \mathbb{F}^m$ be an affine point, and let $\mathcal{J} \subseteq \mathbb{N}^m$ be a finite set. We say that $\mathbf{a}$ is a zero of $F(\mathbf{x})$ of multiplicity at least $\mathcal{J}$ if $F^{(\mathbf{i})}(\mathbf{a}) = 0$, for all $\mathbf{i} \in \mathcal{J}$.

We are interested in *consecutive derivatives*, in a coordinate-wise sense, which can be formalized by the concept of *decreasing sets* of multiindices. In the following, $\preceq$ denotes the coordinate-wise ordering in $\mathbb{N}^m$.

Definition 0.32 ([I]). We say that the set $\mathcal{J} \subseteq \mathbb{N}^m$ is decreasing if whenever $\mathbf{i} \in \mathcal{J}$ and $\mathbf{j} \in \mathbb{N}^m$ are such that $\mathbf{j} \preceq \mathbf{i}$, it holds that $\mathbf{j} \in \mathcal{J}$.

From now on, fix a decreasing finite set $\mathcal{J} \subseteq \mathbb{N}^m$, an ideal $I \subseteq \mathbb{F}[\mathbf{x}]$ and finite subsets $\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_m \subseteq \mathbb{F}$. Write $\mathcal{S} = \mathcal{S}_1 \times \mathcal{S}_2 \times \cdots \times \mathcal{S}_m$, and denote by $G_j(x_j) \in \mathbb{F}[x_j]$ the defining polynomial of $\mathcal{S}_j$, that is, $G_j(x_j) = \prod_{s \in \mathcal{S}_j}(x_j - s)$, for $j = 1, 2, \ldots, m$.

Our main result, proven in Paper I, is the following footprint-type bound on the number of zeros of an ideal of polynomials of multiplicity at least $\mathcal{J}$, for some decreasing set $\mathcal{J}$:

Theorem 0.23 ([I]). *For any monomial ordering $\preceq_m$, it holds that*

$$\#\mathcal{V}_{\mathcal{J}}(I) \cdot \#\mathcal{J} \leq \#\Delta_{\preceq_m}(I_{\mathcal{J}}),$$

where we define the ideal

$$I_{\mathcal{J}} = I + \left\langle \left\{ \prod_{j=1}^{m} G_j(x_j)^{r_j} : (r_1, r_2, \ldots, r_m) \notin \mathcal{J} \right\} \right\rangle,$$

we define the set of zeros of multiplicity at least $\mathcal{J}$ of the ideal I in the grid $\mathcal{S} = \mathcal{S}_1 \times \mathcal{S}_2 \times \cdots \times \mathcal{S}_m$ as

$$\mathcal{V}_{\mathcal{J}}(I) = \left\{ \mathbf{a} \in \mathcal{S} : F^{(\mathbf{i})}(\mathbf{a}) = 0, \forall F(\mathbf{x}) \in I, \forall \mathbf{i} \in \mathcal{J} \right\},$$

and where we define the footprint of an ideal $J \subseteq \mathbb{F}[\mathbf{x}]$ as

$$\Delta_{\preceq_m}(J) = \left\{ \mathbf{x}^{\mathbf{i}} : \mathbf{x}^{\mathbf{i}} \notin \langle \mathrm{LM}(J) \rangle \right\},$$

where $\mathrm{LM}(J) = \{\mathrm{LM}(F(\mathbf{x})) : F(\mathbf{x}) \in J\}$ *with respect to the monomial ordering $\preceq_m$.*

The classical footprint bound (see Proposition 8 in [15, Sec. 5.3], and [25, 32]) is a particular case of our bound:

Corollary 0.33. *Setting $\mathcal{J} = \{\mathbf{0}\}$, we obtain that*

$$\#\mathcal{V}(I) \leq \#\Delta\left(I + \langle G_1(x_1), G_2(x_2), \ldots, G_m(x_m) \rangle\right),$$

where $\mathcal{V}(I)$ denotes the set of zeros of the ideal I in $\mathcal{S}$.

The case of zeros of standard multiplicity at least a given positive integer was first obtained as Lemma 2.4 in the extended version of [52], and is also a consequence of our result:

Corollary 0.34. *Given an integer $r \in \mathbb{N}_+$, and setting $\mathcal{J} = \{(i_1, i_2, \ldots, i_m) \in \mathbb{N}^m : \sum_{j=1}^m i_j < r\}$, we obtain that*

$$\#\mathcal{V}_{\geq r}(I) \cdot \binom{m+r-1}{m} \leq \#\Delta \left(I + \left\langle \left\{ \prod_{j=1}^m G_j(x_j)^{r_j} : \sum_{j=1}^m r_j = r \right\} \right\rangle \right),$$

where $\mathcal{V}_{\geq r}(I)$ denotes the set of zeros of multiplicity at least r of the ideal I in $\mathcal{S}$.

Another particular case is obtained by upper bounding each coordinate of the multiindices separately:

Corollary 0.35 ([I]). *Given a multiindex $(r_1, r_2, \ldots, r_m) \in \mathbb{N}_+^m$, and setting $\mathcal{J} = \{(i_1, i_2, \ldots, i_m) \in \mathbb{N}^m : i_j < r_j, j = 1, 2, \ldots, m\}$, we obtain that*

$$\#\mathcal{V}_{\mathcal{J}}(I) \cdot \prod_{j=1}^m r_j \leq \#\Delta \left(I + \langle G_1(x_1)^{r_1}, G_2(x_2)^{r_2}, \ldots, G_m(x_m)^{r_m} \rangle \right).$$

Finally, we observe that some important well-known results in algebraic combinatorics are direct consequences of the footprint bound. In particular, we may obtain extensions of such algebraic combinatoric results to our context. To that end, we define

$$\mathcal{J}_{\mathcal{S}} = \left\{ \mathbf{i} \in \mathbb{N}^m : \mathbf{i} \not\geq (r_1 \#\mathcal{S}_1, r_2 \#\mathcal{S}_2, \ldots, r_m \#\mathcal{S}_m), \forall (r_1, r_2, \ldots, r_m) \notin \mathcal{J} \right\}.$$

The following is an extension of the well-known Alon's combinatorial Nullstellensatz [2, Th. 1.2]. We recall that an extension to standard multiplicities was given in [4, Cor. 3.2], which is also a particular case of the following corollary:

Corollary 0.36 ([I]). *Let $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ be a non-zero polynomial, and let $\mathbf{x}^{\mathbf{i}} = \mathrm{LM}(F(\mathbf{x}))$ for some monomial ordering. If $\mathbf{i} \in \mathcal{J}_{\mathcal{S}}$, then there exist $\mathbf{s} \in \mathcal{S}$ and $\mathbf{j} \in \mathcal{J}$ such that*

$$F^{(\mathbf{j})}(\mathbf{s}) \neq 0.$$

Another important consequence is an extension of the existence and uniqueness of Hermite interpolating polynomials over finite grids:

Corollary 0.37 ([I]). *Given elements $b_{\mathbf{j},\mathbf{a}} \in \mathbb{F}$, where $\mathbf{j} \in \mathcal{J}$ and $\mathbf{a} \in \mathcal{S}$, there exists a unique polynomial of the form*

$$F(\mathbf{x}) = \sum_{\mathbf{i} \in \mathcal{J}_{\mathcal{S}}} F_{\mathbf{i}} \mathbf{x}^{\mathbf{i}} \in \mathbb{F}[\mathbf{x}],$$

where $F_{\mathbf{i}} \in \mathbb{F}$ for all $\mathbf{i} \in \mathcal{J}_{\mathcal{S}}$, such that $F^{(\mathbf{j})}(\mathbf{a}) = b_{\mathbf{j},\mathbf{a}}$, for all $\mathbf{j} \in \mathcal{J}$ and all $\mathbf{a} \in \mathcal{S}$.

Finally, we extend the collection of bounds given by DeMillo and Lipton [17], Zippel [67, Th. 1], [68, Prop. 3], and Alon and Füredi [3, Th. 5]:

Corollary 0.38 ([I]). *For any polynomial* $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$*, if* $\mathbf{x}^{\mathbf{i}} = \mathrm{LM}(F(\mathbf{x})) \in \mathcal{J}_{\mathcal{S}}$*, for some monomial ordering, then it holds that*

$$\#\left(\mathcal{S} \setminus \mathcal{V}_{\mathcal{J}}(F(\mathbf{x}))\right) \#\mathcal{J} \geq \# \left\{ \mathbf{j} \in \mathcal{J}_{\mathcal{S}} : \mathbf{j} \succeq \mathbf{i} \right\}.$$

An interesting explicit bound can be obtained when bounding multi-indices on each coordinate separately. This still gives an extension of the previously mentioned bounds from the literature:

Corollary 0.39 ([I]). *Let* $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ *with* $\mathbf{x}^{\mathbf{i}} = \mathrm{LM}(F(\mathbf{x}))$, $\mathbf{i} = (i_1, i_2, \ldots, i_m)$*, for some monomial ordering. If* $i_j < r_j \#\mathcal{S}_j$*, for* $j = 1, 2, \ldots, m$*, then the number* N *of elements* $\mathbf{s} \in \mathcal{S}$ *such that* $F^{(\mathbf{j})}(\mathbf{s}) \neq 0$*, for some* $\mathbf{j} = (j_1, j_2, \ldots, j_m) \in \mathbb{N}^m$ *with* $j_k < r_k$*, for all* $k = 1, 2, \ldots, m$*, satisfies*

$$N \cdot \prod_{j=1}^{m} r_j \geq \prod_{j=1}^{m} \left(r_j \#\mathcal{S}_j - i_j \right).$$

References

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inform. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[2] N. Alon, "Combinatorial Nullstellensatz," *Combinatorics, Probability and Computing*, vol. 8, no. 1-2, pp. 7–29, 1999.

[3] N. Alon and Z. Füredi, "Covering the cube by affine hyperplanes," *European Journal of Combinatorics*, vol. 14, no. 2, pp. 79–83, 1993.

[4] S. Ball and O. Serra, "Punctured combinatorial Nullstellensätze," *Combinatorica*, vol. 29, no. 5, pp. 511–522, 2009.

[5] T. P. Berger, "Isometries for rank distance and permutation group of Gabidulin codes," *IEEE Trans. Inform. Theory*, vol. 49, no. 11, pp. 3016–3019, 2003.

[6] R. Bitar and S. E. Rouayheb, "Staircase codes for secret sharing with optimal communication and read overheads," in *Proc. 2016 IEEE International Symposium on Information Theory (ISIT)*, 2016, pp. 1396–1400.

[7] G. R. Blakley, "Safeguarding cryptographic keys," *International Workshop on Managing Requirements Knowledge*, vol. 0, p. 313, 1979.

[8] D. Boucher, W. Geiselmann, and F. Ulmer, "Skew-cyclic codes," *Applicable Algebra in Engineering, Communication and Computing*, vol. 18, no. 4, pp. 379–389, 2007.

[9] D. Boucher and F. Ulmer, "Coding with skew polynomial rings," *Journal of Symbolic Computation*, vol. 44, no. 12, pp. 1644–1656, 2009.

[10] N. Cai and R. W. Yeung, "Network coding and error correction," *Proc. 2002 IEEE Inform. Theory Workshop*, pp. 119–122, 2002.

[11] ——, "Secure network coding," in *Proc. 2002 IEEE International Symposium on Information Theory*, p. 323, 2002.

[12] L. Chaussade, P. Loidreau, and F. Ulmer, "Skew codes of prescribed distance or rank," *Designs, Codes and Cryptography*, vol. 50, no. 3, pp. 267–284, 2009.

[13] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan, "Secure computation from random error correcting codes," in *Advances in cryptology—EUROCRYPT 2007*, ser. Lecture Notes in Comput. Sci. Springer Berlin Heidelberg, 2007, vol. 4515, pp. 291–310.

[14] A. Couvreur, "Personal communication," 2015.

[15] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2007.

[16] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *Journal of Combinatorial Theory, Series A*, vol. 25, no. 3, pp. 226–241, 1978.

[17] R. A. Demillo and R. J. Lipton, "A probabilistic remark on algebraic program testing," *Information processing letters*, vol. 7, no. 4, pp. 193–195, 1978.

[18] Y. Ding, "On list-decodability of random rank metric codes and subspace codes," *IEEE Trans. Inform. Theory*, vol. 61, no. 1, pp. 51–59, Jan. 2015.

[19] J. Ducoat, "Generalized rank weights: A duality statement," in *Topics in Finite Fields*, ser. Comtemporary Mathematics, G. L. M. G. Kyureghyan and A. Pott, Eds. American Mathematical Society, 2015, vol. 632, pp. 114–123.

[20] I. Duursma and R. Kötter, "Error-locating pairs for cyclic codes," *IEEE Trans. Inform. Theory*, vol. 40, no. 4, pp. 1108–1121, Jul 1994.

[21] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems Inform. Transmission*, vol. 21, no. 1, pp. 1–12, 1985.

[22] ——, "Rank q-cyclic and pseudo-q-cyclic codes," in *Proc. 2009 IEEE International Symposium on Information Theory*, pp. 2799–2802, 2009.

[23] E. M. Gabidulin, A. V. Ourivski, B. Honary, and B. Ammar, "Reducible rank codes and their applications to cryptography," *IEEE Trans. Inform. Theory*, vol. 49, no. 12, pp. 3289–3293, Dec. 2003.

[24] A. Garcia and H. Stichtenoth, "On the asymptotic behaviour of some towers of function fields over finite fields," *Journal of Number Theory*, vol. 61, no. 2, pp. 248–273, 1996.

[25] O. Geil and T. Høholdt, "Footprints or generalized Bezout's theorem," *IEEE Trans. Inform. Theory*, vol. 46, no. 2, pp. 635–641, 2000.

[26] V. Guruswami and S. Kopparty, "Explicit subspace designs," *Combinatorica*, vol. 36, no. 2, pp. 161–185, Apr 2016.

[27] V. Guruswami, C. Wang, and C. Xing, "Explicit list-decodable rank-metric and subspace codes via subspace designs," *IEEE Trans. Inform. Theory*, vol. 62, no. 5, pp. 2707–2718, May 2016.

[28] C. Hartmann and K. Tzeng, "Generalizations of the BCH bound," *Information and Control*, vol. 20, no. 5, pp. 489–498, 1972.

[29] H. Hasse, "Theorie der höheren differentiale in einem algebraischen funktionenkörper mit vollkommenem konstantenkörper bei beliebiger charakteristik." *Journal für die reine und angewandte Mathematik*, vol. 175, pp. 50–54, 1936.

[30] T. Helleseth, T. Kløve, V. I. Levenshtein, and Ø. Ytrehus, "Bounds on the minimum support weights," *IEEE Trans. Inform. Theory*, vol. 41, no. 2, pp. 432–440, 1995.

[31] T. Ho, M. Médard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inform. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.

[32] T. Høholdt, "On (or in) the Blahut footprint," in *Codes, Curves, and Signals: Common Threads in Communications*, A. Vardy, Ed. Boston, MA: Springer US, 1998, pp. 3–7.

[33] W. Huang, M. Langberg, J. Kliewer, and J. Bruck, "Communication efficient secret sharing," *IEEE Trans. Inform. Theory*, vol. 62, no. 12, pp. 7195–7206, 2016.

[34] R. Jurrius and R. Pellikaan, "On defining generalized rank weights," *Advances in Mathematics of Communications*, vol. 11, no. 1, pp. 225–235, 2017.

[35] S. Kopparty, S. Saraf, and S. Yekhanin, "High-rate codes with sublinear-time decoding," *Journal of the ACM*, vol. 61, no. 5, pp. 28:1–28:20, 2014.

[36] R. Kötter, "A unified description of an error locating procedure for linear codes," *Proc. Algebraic and Combinatorial Coding Theory*, pp. 113–117, 1992, voneshta Voda.

[37] R. Kötter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Networking*, vol. 11, no. 5, pp. 782–795, Oct. 2003.

[38] A. Kshevetskiy and E. M. Gabidulin, "The new construction of rank codes," in *Proc. 2005 IEEE International Symposium on Information Theory*, pp. 2105–2108, Sept 2005.

[39] J. Kurihara, R. Matsumoto, and T. Uyematsu, "Relative generalized rank weight of linear codes and its applications to network coding," *IEEE Trans. Inform. Theory*, vol. 61, no. 7, pp. 3912–3936, Jul. 2015.

[40] J. Kurihara, T. Uyematsu, and R. Matsumoto, "Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized hamming weight," *IEICE Trans. Fundamentals*, vol. E95-A, no. 11, pp. 2067–2075, 2012.

[41] S.-Y. R. Li, R. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inform. Theory*, vol. 49, no. 2, pp. 371–381, Feb. 2003.

[42] Y. Luo, C. Mitrpant, A. J. Han Vinck, and K. Chen, "Some new characters on the wire-tap channel of type II." *IEEE Trans. Inform. Theory*, vol. 51, no. 3, pp. 1222–1229, 2005.

[43] M. Marcus and B. N. Moyls, "Linear transformations on algebras of matrices," *Canad. J. Math.*, vol. 11, pp. 61–66, 1959.

[44] K. Morrison, "Equivalence for rank-metric and matrix codes and automorphism groups of Gabidulin codes," *IEEE Trans. Inform. Theory*, vol. 60, no. 11, pp. 7035–7046, Nov. 2014.

[45] F. E. Oggier and A. Sboui, "On the existence of generalized rank weights," in *Proc. 2012 International Symposium on Information Theory and its Applications*, 2012, pp. 406–410.

[46] O. Ore, "On a special class of polynomials," *Transactions Amererican Mathematical Society*, vol. 35, no. 3, pp. 559–584, 1933.

[47] ——, “Theory of non-commutative polynomials,” *Annals of Mathematics (2)*, vol. 34, no. 3, pp. 480–508, 1933.

[48] L. H. Ozarow and A. D. Wyner, “Wire-tap channel II,” in *Advances in Cryptology: EUROCRYPT 84*, ser. Lecture Notes in Comput. Sci. Springer Berlin Heidelberg, 1985, vol. 209, pp. 33–50.

[49] R. Pellikaan, “On decoding linear codes by error correcting pairs,” *Preprint. Eindhoven University of Technology*, 1988.

[50] ——, “On decoding by error location and dependent sets of error positions,” *Discrete Mathematics*, vol. 106, pp. 369–381, 1992.

[51] ——, “On the existence of error-correcting pairs,” *Journal of Statistical Planning and Inference*, vol. 51, no. 2, pp. 229–242, 1996.

[52] R. Pellikaan and X.-W. Wu, “List decoding of q-ary Reed-Muller codes,” *IEEE Trans. Inform. Theory*, vol. 50, no. 4, pp. 679–682, 2004, extended version: http://www.win.tue.nl/~ruudp/paper/43-exp.pdf.

[53] A. Ravagnani, “Generalized weights: An anticode approach,” *Journal of Pure and Applied Algebra*, vol. 220, no. 5, pp. 1946–1962, 2016.

[54] ——, “Rank-metric codes and their duality theory,” *Designs, Codes and Cryptography*, vol. 80, no. 1, pp. 197–216, 2016.

[55] R. M. Roth, “Maximum-rank array codes and their application to crisscross error correction,” *IEEE Trans. Inform. Theory*, vol. 37, no. 2, pp. 328–336, Mar. 1991.

[56] J. T. Schwartz, “Fast probabilistic algorithms for verification of polynomial identities,” *Journal of the ACM*, vol. 27, no. 4, pp. 701–717, 1980.

[57] A. Shamir, “How to share a secret,” *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[58] K. W. Shum, I. Aleshnikov, P. V. Kumar, H. Stichtenoth, and V. Deolaikar, “A low-complexity algorithm for the construction of algebraic-geometric codes better than the Gilbert-Varshamov bound,” *IEEE Trans. Inform. Theory*, vol. 47, no. 6, pp. 2225–2241, 2001.

[59] D. Silva and F. R. Kschischang, “On metrics for error correction in network coding,” *IEEE Trans. Inform. Theory*, vol. 55, no. 12, pp. 5479–5490, 2009.

[60] ——, “Universal secure network coding via rank-metric codes,” *IEEE Trans. Inform. Theory*, vol. 57, no. 2, pp. 1124–1135, Feb. 2011.

[61] H. Stichtenoth, "On the dimension of subfield subcodes," *IEEE Trans. Inform. Theory*, vol. 36, no. 1, pp. 90–93, Jan. 1990.

[62] M. A. Tsfasman and S. G. Vlăduţ, "Geometric approach to higher weights," *IEEE Trans. Inform. Theory*, vol. 41, no. 6, part 1, pp. 1564–1588, 1995, special issue on algebraic geometry codes.

[63] J. van Lint and R. Wilson, "On the minimum distance of cyclic codes," *IEEE Trans. Inform. Theory*, vol. 32, no. 1, pp. 23–40, Jan 1986.

[64] H. Wang and D. S. Wong, "On secret reconstruction in secret sharing schemes," *IEEE Trans. Inform. Theory*, vol. 54, no. 1, pp. 473–480, 2008.

[65] V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inform. Theory*, vol. 37, no. 5, pp. 1412–1418, 1991.

[66] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Inform. Theory*, vol. 48, no. 6, pp. 1250–1276, Jun. 2002.

[67] R. Zippel, "Probabilistic algorithms for sparse polynomials," in *Proc. International Symposiumon on Symbolic and Algebraic Computation*, ser. EUROSAM '79. London, UK: Springer-Verlag, 1979, pp. 216–226.

[68] ——, "An explicit separation of relativised random and polynomial time and relativised deterministic polynomial time," Ithaca, NY, USA, Tech. Rep., 1989.

Part II

Papers

Paper A

On the Similarities Between Generalized Rank and Hamming Weights and Their Applications to Network Coding

Umberto Martínez-Peñas[1]

The paper has been published in the
IEEE Transactions on Information Theory Vol. 62, No. 7, pp. 4081–4095, July 2016.

[1] Department of Mathematical Sciences, Aalborg University, Aalborg 9220, Denmark

Abstract

Rank weights and generalized rank weights have been proven to characterize error and erasure correction, and information leakage in linear network coding, in the same way as Hamming weights and generalized Hamming weights describe classical error and erasure correction, and information leakage in wire-tap channels of type II and code-based secret sharing. Although many similarities between both cases have been established and proven in the literature, many other known results in the Hamming case, such as bounds or characterizations of weight-preserving maps, have not been translated to the rank case yet, or in some cases have been proven after developing a different machinery. The aim of this paper is to further relate both weights and generalized weights, show that the results and proofs in both cases are usually essentially the same, and see the significance of these similarities in network coding. Some of the new results in the rank case also have new consequences in the Hamming case.

Keywords: Rank weight, generalized rank weight, rank distance, rank-metric codes, network coding, network error correction, secure network coding.

1 Introduction

Linear network coding has been intensively studied during the last decade [1, 4, 15, 18–20, 22, 28, 29, 34, 35]. Consider a network with several sources and several sinks, where each source transmits several packets through the network to multiple sinks. Following [1, 15, 19, 22], "linear network coding" is defined as the process by which, in each node of the network, linear combinations of the received packets are generated (possibly at random [15]) and sent (see [19, Definition 1]). We assume no delays nor cycles.

In this context, errors are considered as erroneous packets that appear on some links, and erasures are considered as the deficiency of the rank of the matrix (called transfer matrix [19, 20, 29]) that describes the received packets as combinations of the ones sent by a given source [20, 29]. In secure network coding, an adversary (or several) may compromise the security of the network by doing the following, among other attacks: introducing t erroneous packets on t different links, modifying the transfer matrix and obtaining information from the sent packets by wiretapping several links [20, 28, 29].

In classical coding for error and erasure correction [16], coding for wire-tap channels of type II [24, 26, 33] and code-based secret sharing [5, 21, 27], the original message is encoded into a vector $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in \mathbb{F}_q^n$, where $\mathbb{F}_q$ is some finite field. Then, errors, erasures and information leakage happen component-wise. This means that some components of $\mathbf{c}$ may be wrong (errors), some components may be erased (erasures), and a wiretapping adversary may obtain some components (information leakage). Using source coding on a network, as in [20, 28], all this is considered to happen on some linear combinations: errors are wrong combinations, erasures are losses of combinations, and information leakage is considered in the form of leaked combinations.

In the classical case, Hamming weights [16] and generalized Hamming weights [33] have been proven to describe error and erasure correction and information leakage on wire-tap channels of type II. On the other hand, in recent years there have been several attempts to find a suitable weight and generalized weight to study linear network coding [18, 20, 25, 28, 34, 35]. Finally, rank weights and generalized rank weights, introduced in [11] and [20, 25], respectively, have been proven to describe exactly the worst case error and erasure correction capability [20, 28, 29], and worst case information leakage on networks [20, 29].

Many similarities between Hamming weights and rank weights have been considered since the paper [11], and for generalized ones since [20, 25]. However, many results on Hamming weights still have no counterpart in the rank case, or require proofs using a different machinery.

The aim of this paper is to give some alternative definitions of rank weights [11] and generalized rank weights [7, 17, 20, 25], and then show that most of the well-known results for Hamming weights, classical error and erasure correction and information leakage, can be directly translated to rank weights, network error and erasure correction and information leakage on networks, once the right definitions and tools are introduced.

After giving some preliminary tools from the literature in Section 2, the new results in this paper are distributed as follows: In Section 3, we gather alternative definitions of rank weights and generalized rank weights from the literature, and propose some new definitions, proving the equivalence between them. In contrast with [7, 17, 25], we also treat relative weights [20]. In Section 4, we study linear equivalences of codes, that is, vector space isomorphisms between codes that preserve rank weights (and generalized rank weights), which allow to say when two codes perform exactly equally in secure network coding. We establish new characterizations of these equivalences that also give a connection with information leakage. We treat for the first time the case of different lengths and obtain the minimum possible lengths of codes, up to these equivalences. In Section 5, we establish a way to derive bounds on generalized rank weights from bounds on generalized Hamming weights, and give a list of some of these bounds. In the rest of the section, we discuss what the Singleton bound in the rank case can be, establishing a new alternative version. In Section 6, we introduce the concept of rank-punctured codes, which plays the same role as classical punctured codes, and which are a main tool for the study of rank weights, erasure correction and information leakage, since punctured codewords are conceptually the same as codewords with erasures. We use this to characterize MRD ranks of codes and introduce the concept of information spaces. Finally, in Section 7, we revisit some of the results regarding error and erasure correction and information leakage on networks. We obtain new relations regarding information leakage and duality, estimate information leakage in terms of dimensions of spaces, and propose a slightly different decoder than that of [20, 28], proving also the characterization of the correction capability of arbitrary (in particular, $\mathbb{F}_q$-linear) coding schemes, which has not been stated nor proven yet.

2 Definitions and preliminaries

Let q be a prime power and m and n, two positive integers. $\mathbb{F}_q$ denotes the finite field with q elements. All vectors are considered to be row vectors, and we use the notation A^T to denote the transpose of a matrix A.

2.1 Linear network coding model

We will consider the network model with errors in [20, 28], where the original message $\mathbf{x} \in \mathbb{F}_{q^m}^k$ (considered as k packets in $\mathbb{F}_{q^m}$) is encoded by a given source into $\mathbf{c} \in \mathbb{F}_{q^m}^n$, whose n components (seen as packets) are sent through a network with n outgoing links from that source node and where a given receiver obtains $\mathbf{y} = \mathbf{c}A^T + \mathbf{e}$, for some transfer matrix $A \in \mathbb{F}_q^{N \times n}$ and some error vector $\mathbf{e} \in \mathbb{F}_{q^m}^N$.

As in [20, 28], when treating error and erasure correction, we will consider multicast networks with one source and several sinks, and no delays nor cycles. In the noiseless case, for treating just information leakage to an adversary, we may assume several sources as long as the packets sent by different sources have no correlations. This allows to treat packets from a different source as errors, which give no extra information to a wiretapping adversary by [20, Proposition 5].

The length of the vector $\mathbf{c}$ is defined as n, and corresponds to the number of outgoing links from the source in the network, while m corresponds to the packet size. Therefore, m and n do not play a symmetric role.

Although it is usual in the literature to only consider the case $n \leq m$, we consider all cases, and we argue as follows (see also [20, Section I.A] for more details): on the one hand, in some Internet protocols, the size of each packet (m) is bounded by some parameters of the protocol, whereas the number of outgoing links (n) is not necessarily bounded. On the other hand, since many computations are carried out over the extension field $\mathbb{F}_{q^m}$, requiring $m \geq n$ may extremely increase the computational complexity of the encoding and decoding.

2.2 Codes and coding schemes

A code in $\mathbb{F}_{q^m}^n$ is just a subset $C \subset \mathbb{F}_{q^m}^n$, whose length is defined as n. We say that C is linear (respectively $\mathbb{F}_q$-linear) if it is an $\mathbb{F}_{q^m}$-linear subspace (respectively $\mathbb{F}_q$-linear). The term arbitrary is used for all codes, including non-linear codes.

Definition A.1 ([20, Definition 7]). A coding scheme (or binning scheme) with message set $\mathcal{S}$ is a family of disjoint nonempty subsets of $\mathbb{F}_{q^m}^n$, $\mathcal{P}_{\mathcal{S}} = \{C_{\mathbf{x}}\}_{\mathbf{x} \in \mathcal{S}}$, together with a probability distribution over each of these sets.

Definition A.2. A coding scheme as in the previous definition is said to be linear if $\mathcal{S} = \mathbb{F}_{q^m}^\ell$, where $0 < \ell \leq n$, and

$$\alpha C_{\mathbf{x}} + \beta C_{\mathbf{y}} \subset C_{\alpha \mathbf{x} + \beta \mathbf{y}},$$

for all $\alpha, \beta \in \mathbb{F}_{q^m}$ and all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_{q^m}^\ell$. Similarly in the $\mathbb{F}_q$-linear case (where $\mathcal{S} = \mathbb{F}_q^\ell$, $0 < \ell \leq mn$).

The encoding in the coding scheme is given in [20, Definition 7] as follows: for each $\mathbf{x} \in \mathcal{S}$, we choose at random (with the chosen distribution) an element $\mathbf{c} \in C_{\mathbf{x}}$. With these definitions, the concept of coding scheme generalizes the concept of code, since a code is a coding scheme where $\# C_{\mathbf{x}} = 1$, for each $\mathbf{x} \in \mathcal{S}$, and thus no probability distribution is required. In the same way, linear and $\mathbb{F}_q$-linear coding schemes generalize linear and $\mathbb{F}_q$-linear codes, respectively.

An equivalent way to describe linear (and $\mathbb{F}_q$-linear) coding schemes is by nested linear code pairs, introduced in [36, Section III.A]. We use the description in [5, Subsection 4.2].

Definition A.3 ([5, 36]). A nested linear code pair is a pair of linear codes $C_2 \subsetneq C_1 \subset \mathbb{F}_{q^m}^n$. Choose a linear space W such that $C_1 = C_2 \oplus W$ (where $\oplus$ represents the direct sum of vector spaces) and an isomorphism $\psi : \mathbb{F}_{q^m}^\ell \longrightarrow W$, where $\ell = \dim(C_1/C_2)$. Then we define the sets $C_{\mathbf{x}} = \psi(\mathbf{x}) + C_2$. They form a linear coding scheme called nested coset coding scheme [20].

If we choose the probability distribution to be uniform, then the encoding can be done as follows: Take uniformly at random $\mathbf{c}' \in C_2$ and define $\mathbf{c} = \psi(\mathbf{x}) + \mathbf{c}'$.

A given code $C \subset \mathbb{F}_{q^m}^n$, seen as a pair $0 \subsetneq C$ is suitable for error correction, but is not suitable for protection against information leakage. Ozarow and Wyner proposed in [26] using the pair $C \subsetneq \mathbb{F}_{q^m}^n$ for protection against information leakage on noiseless channels. The idea of nested linear code pairs was introduced in [36] to protect against both information leakage and noise.

Independently, the same idea was implicitly used by Shamir [27] and Massey [5, Section 3.1] to construct secret sharing schemes, and general nested linear code pairs were first used for this purpose in [5, Section 4.2], where it is claimed in an informal way that they include all possible linear coding schemes. We now state this in a formal way, omitting the proof, which is straightforward. The $\mathbb{F}_q$-linear case is completely analogous.

Proposition A.4. *Given a linear coding scheme $\mathcal{P}_{\mathcal{S}} = \{C_{\mathbf{x}}\}_{\mathbf{x} \in \mathcal{S}}$, define $C_1 = \bigcup_{\mathbf{x} \in \mathcal{S}} C_{\mathbf{x}}$ and $C_2 = C_{\mathbf{0}}$ (recall that $\mathcal{S} = \mathbb{F}_{q^m}^{\ell}$). Then, C_1 and C_2 are linear codes in $\mathbb{F}_{q^m}^n$ and*

1. *$C_2 \subsetneq C_1$.*
2. *The relation given in C_1 by $\mathbf{c} \sim \mathbf{d}$ if, and only if, there exists $\mathbf{x} \in \mathbb{F}_{q^m}^{\ell}$ such that $\mathbf{c}, \mathbf{d} \in C_{\mathbf{x}}$, is an equivalence relation that satisfies the following:*

$$\mathbf{c} \sim \mathbf{d} \quad \Longleftrightarrow \quad \mathbf{c} - \mathbf{d} \in C_2.$$

   In particular, $\mathcal{P}_{\mathcal{S}} = C_1 / C_2$.

3. *The map $\mathbb{F}_{q^m}^{\ell} \longrightarrow \mathcal{P}_{\mathcal{S}} = C_1/C_2 : \mathbf{x} \longmapsto C_{\mathbf{x}}$ is a vector space isomorphism.*

In particular, if we take a subspace $W \subset C_1$ such that $C_1 = C_2 \oplus W$, then we can canonically define an isomorphism $\psi : \mathbb{F}_{q^m}^{\ell} \longrightarrow W$ by $C_{\mathbf{x}} \cap W = \{\psi(\mathbf{x})\}$. Of course, it satisfies that $C_{\mathbf{x}} = \psi(\mathbf{x}) + C_2$.

On the other hand, if $d : \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n \longrightarrow \mathbb{N}$ is the rank (respectively Hamming) distance [11] (respectively [16]), we define the minimum rank (respectively Hamming) distance of the coding scheme $\mathcal{P}_{\mathcal{S}}$ as

$$d(\mathcal{P}_{\mathcal{S}}) = \min\{d(\mathbf{c}_1, \mathbf{c}_2) \mid \mathbf{c}_1 \in C_{\mathbf{x}_1}, \mathbf{c}_2 \in C_{\mathbf{x}_2}, \mathbf{x}_1 \neq \mathbf{x}_2\}. \tag{A.1}$$

For arbitrary codes we obtain the usual definition of minimum distance. For arbitrary coding schemes, it is basically the minimum of the distances between the sets $C_{\mathbf{x}}$, $\mathbf{x} \in \mathcal{S}$.

For a linear coding scheme $\mathcal{P}_{\mathcal{S}}$ and the Hamming distance d, $d(\mathcal{P}_{\mathcal{S}})$ coincides with the minimum coset distance introduced in [9] or the first relative generalized Hamming weight [24]. For a linear coding scheme and the rank distance, it coincides with the first relative generalized rank weight [20].

2.3 Rank weights and rank supports

Now we turn to rank weights. We first observe the following obvious fact from linear algebra.

Lemma A.5. *Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ and $\beta_1, \beta_2, \ldots, \beta_m$ be two bases of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and let $\mathbf{c} \in \mathbb{F}_{q^m}^n$ be a vector. It can be written in a unique way as*

$$\mathbf{c} = \sum_{i=1}^{m} \mathbf{c}_i \alpha_i = \sum_{i=1}^{m} \mathbf{d}_i \beta_i,$$

where $\mathbf{c}_i, \mathbf{d}_i \in \mathbb{F}_q^n$. Moreover,

$$\langle \mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_m \rangle_{\mathbb{F}_q} = \langle \mathbf{d}_1, \mathbf{d}_2 \ldots, \mathbf{d}_m \rangle_{\mathbb{F}_q} \subset \mathbb{F}_q^n.$$

Definition A.6 ([11], [20, Section II.D]). Choose one of such bases $\alpha_1, \alpha_2, \ldots, \alpha_m$, and a vector $\mathbf{c} \in \mathbb{F}_{q^m}^n$. We define the rank support [20] of $\mathbf{c}$ as

$$G(\mathbf{c}) = \langle \mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_m \rangle_{\mathbb{F}_q},$$

where $\mathbf{c} = \sum_{i=1}^{m} \mathbf{c}_i \alpha_i$ and $\mathbf{c}_i \in \mathbb{F}_q^n$. The rank weight of $\mathbf{c}$ [11] is then $\mathrm{wt_R}(\mathbf{c}) = \dim(G(\mathbf{c}))$.

From the previous lemma it follows that $G(\mathbf{c})$ (and $\mathrm{wt_R}(\mathbf{c})$) does not depend on the choice of the basis. However, from now on, we fix one such basis $\alpha_1, \alpha_2, \ldots, \alpha_m$.

Definition A.7 ([17, Definition 1]). For each linear subspace $D \subset \mathbb{F}_{q^m}^n$, we define its rank support as $G(D) = \sum_{\mathbf{d} \in D} G(\mathbf{d})$ and its rank weight as $\mathrm{wt_R}(D) = \dim(G(D))$.

Remark A.8. *We can associate each vector $\mathbf{c} \in \mathbb{F}_{q^m}^n$ with a matrix over $\mathbb{F}_q$, which we denote as follows:*

$$\mu(\mathbf{c}) = \begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,n} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m,1} & c_{m,2} & \cdots & c_{m,n} \end{pmatrix},$$

where $\mathbf{c} = \sum_{i=1}^{m} \alpha_i \mathbf{c}_i$ and $\mathbf{c}_i = (c_{i,1}, c_{i,2}, \ldots, c_{i,n}) \in \mathbb{F}_q^n$. Note that $\alpha_i \mathbf{e}_j$, where $\mathbf{e}_j$ is the canonical basis of $\mathbb{F}_{q^m}^n$, for $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$, is a basis of $\mathbb{F}_{q^m}^n$ over $\mathbb{F}_q$. It follows that $\mu : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^{m \times n}$ is an $\mathbb{F}_q$-linear vector space isomorphism. Moreover, the rank support of $\mathbf{c}$ is the row space of $\mu(\mathbf{c})$, which we denote by $\mathrm{row}(\mu(\mathbf{c}))$*, and the rank weight of $\mathbf{c}$ is the rank of $\mu(\mathbf{c})$, denoted by* $\mathrm{Rk}(\mu(\mathbf{c}))$.

The rank weight of a subspace $D \subset \mathbb{F}_{q^m}^n$ is then the rank of the matrix obtained by appending all rows of all matrices corresponding to the vectors in D. It can be shown [17, Proposition 3 (4)] that we can take the vectors in a basis of D.

Note that $G(\mathbf{c}) = G(\langle \mathbf{c} \rangle)$ and thus $\mathrm{wt_R}(\mathbf{c}) = \mathrm{wt_R}(\langle \mathbf{c} \rangle)$, for every $\mathbf{c} \in \mathbb{F}_{q^m}^n$.

2.4 Trace codes, subfield codes and Galois closures

Now we gather some tools from the literature regarding trace and subfield codes, and Galois closures. More details can be found in [13], [16, Section 3.8], [30, Section II] or [31, Chapter 9]:

Definition A.9. For a vector $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ and any integer $i \geq 0$, we define $\mathbf{x}^{q^i} = (x_1^{q^i}, x_2^{q^i}, \ldots, x_n^{q^i})$. Then we define the trace map on vectors as follows

$$\mathrm{Tr} : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^n : \mathbf{x} \longmapsto \sum_{i=0}^{m-1} \mathbf{x}^{q^i}.$$

For a linear subspace $D \subset \mathbb{F}_{q^m}^n$, we define its Galois closure [30, Definition] as

$$D^* = \sum_{i=0}^{m-1} D^{q^i},$$

its trace code as $\mathrm{Tr}(D) = \{\mathrm{Tr}(\mathbf{d}) \mid \mathbf{d} \in D\}$ and its subfield code as $D|_{\mathbb{F}_q} = D \cap \mathbb{F}_q^n$. We say that D is Galois closed if $D = D^*$. If $D \subset \mathbb{F}_q^n$ and is $\mathbb{F}_q$-linear, we define its extended code as $D \otimes \mathbb{F}_{q^m}$, that is, the code generated over $\mathbb{F}_{q^m}$ by the set D, also denoted as $\langle D \rangle_{\mathbb{F}_{q^m}} \subset \mathbb{F}_{q^m}^n$.

Note that Tr is $\mathbb{F}_q$-linear and D^* is the smallest Galois closed linear code containing D [30]. Moreover, a linear subspace $D \subset \mathbb{F}_{q^m}^n$ is Galois closed if, and only if $D^q \subset D$, which is equivalent to $D^q = D$.

The following proposition easily follows from [30, Lemma 1]. The equivalence between items 1, 2, 4 and 5 were also noticed in [13, 17].

Proposition A.10 ([30]). *For every linear code $C \subset \mathbb{F}_{q^m}^n$ of dimension k, the following are equivalent:*

1. *C is Galois closed.*
2. *C admits a basis of vectors in $\mathbb{F}_q^n$.*
3. *C has a basis consisting of vectors of rank weight 1.*
4. *$C = C|_{\mathbb{F}_q} \otimes \mathbb{F}_{q^m}$.*
5. *$C = \mathrm{Tr}(C) \otimes \mathbb{F}_{q^m}$.*
6. *$\mathrm{Tr}(C) = C|_{\mathbb{F}_q}$.*
7. *$\dim(\mathrm{Tr}(C)) = k$.*
8. *$\dim(C|_{\mathbb{F}_q}) = k$.*

We give a final tool due to Delsarte [6, Theorem 2]:

Lemma A.11 (Delsarte [6]). *For every linear code $C \subset \mathbb{F}_{q^m}^n$, we have that*

$$(C|_{\mathbb{F}_q})^\perp = \mathrm{Tr}(C^\perp), \quad \textit{and} \quad (C^\perp)|_{\mathbb{F}_q} = (\mathrm{Tr}(C))^\perp.$$

3 Equivalent definitions of rank weights and generalized rank weights

In this section we give new equivalent definitions of generalized rank weights [20, 25]. In contrast with [7, 17, 25], we also treat relative weights [20]. Both have been proven to characterize worst-case information leakage and error and erasure correction on networks [20, 25].

3.1 The Hamming case

We briefly recall the definitions of Hamming weights, generalized Hamming weights [33] and their relative versions [24]. Following [33, Section II] (see also [16, Section 7.10]), given a linear subspace $D \subset \mathbb{F}_{q^m}^n$, we define its support as $\mathrm{Supp}(D) = \{i \mid \exists \mathbf{d} \in D, d_i \neq 0\}$ and its Hamming weight as $\mathrm{wt_H}(D) = \#\mathrm{Supp}(D)$. The r-th generalized Hamming weight of a code C [33], and r-th relative generalized Hamming weight of a nested linear code pair $C_2 \subsetneq C_1$ [24] are, respectively,

$$d_{H,r}(C) = \min\{\mathrm{wt_H}(D) \mid D \subset C, \dim(D) = r\}, \tag{A.2}$$

$$\begin{aligned} M_{H,r}(C_1, C_2) = \min\{\mathrm{wt_H}(D) \mid D \subset C_1, \\ D \cap C_2 = 0, \dim(D) = r\}. \end{aligned} \tag{A.3}$$

3.2 Existing equivalent definitions

We briefly review the existing equivalent definitions of generalized rank weights and their relative versions. We attribute the following lemma to a combination of [30] with [20] for $\dim(D) = 1$, and a combination of [30] with [17] for the general case, and show why:

Lemma A.12 ([17, 20, 30]). *For any linear subspace $D \subset \mathbb{F}_{q^m}^n$,*

$$\mathrm{wt_R}(D) = \mathrm{wt_R}(D^*) = \dim(\mathrm{Tr}(D)) = \dim(D^*).$$

Proof. It is immediate that $\dim(D^*) = \dim(\mathrm{Tr}(D^*))$ from Proposition A.10, and moreover it holds that $\mathrm{Tr}(D^*) = \mathrm{Tr}(D)$.

The equality $\mathrm{wt_R}(D) = \dim(D^*)$ is proven in [20, Lemma 11] for $\dim(D) = 1$, hence the result follows immediately in that case.

On the other hand, [17, Theorem 16] states that $G(D) = \mathrm{Tr}(D)$, hence $\mathrm{wt_R}(D) = \dim(\mathrm{Tr}(D))$ and the result follows in the general case. □

Now we define generalized rank weights, introduced in [25] for $n \leq m$, and their relative versions, both introduced in general in [20]:

Definition A.13 ([20, Definition 2]). For a linear code $C \subset \mathbb{F}_{q^m}^n$ and $1 \leq r \leq k = \dim(C)$, we define its r-th generalized rank weight as

$$d_{R,r}(C) = \min\{ \dim V \mid V \subset \mathbb{F}_{q^m}^n, V = V^*, \\ \dim(C \cap V) \geq r\}. \tag{A.4}$$

For a nested linear code pair $C_2 \subsetneq C_1 \subset \mathbb{F}_{q^m}^n$, we define its r-th relative generalized rank weight as

$$M_{R,r}(C_1, C_2) = \min\{ \dim V \mid V \subset \mathbb{F}_{q^m}^n, V = V^*, \\ \dim((C_1 \cap V)/(C_2 \cap V)) \geq r\}. \tag{A.5}$$

Fix a linear code $C \subset \mathbb{F}_{q^m}^n$ and $1 \leq r \leq k = \dim(C)$. We have the following equivalent definitions from the literature:

Lemma A.14 ([17, Corollary 17]). *The r-th generalized rank weight $d_{R,r}(C)$ is equal to*

$$\min\{\mathrm{wt_R}(D) \mid D \subset C, \dim(D) = r\}. \tag{A.6}$$

Lemma A.15 ([7, Proposition II.1]). *If $n \leq m$, the r-th generalized rank weight $d_{R,r}(C)$ is equal to*

$$\min\{\max\{\mathrm{wt_R}(\mathbf{x}) \mid \mathbf{x} \in D^*\} \mid D \subset C, \dim(D) = r\}. \tag{A.7}$$

3.3 New equivalent definitions

In this subsection, we give new equivalent definitions of rank weights, generalized rank weights and their relative versions.

Theorem A.1. *For any linear subspace $D \subset \mathbb{F}_{q^m}^n$, we have that*

$$\mathrm{wt_R}(D) = \min\{\mathrm{wt_H}(\varphi_B(D)) \mid B \subset \mathbb{F}_q^n \textit{ is a basis of } \mathbb{F}_{q^m}^n\},$$

where $\varphi_B : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$ is the linear map defined as $\varphi_B(\mathbf{c}) = \mathbf{x}$, where $\mathbf{c} = \sum_{i=1}^n x_i \mathbf{v}_i$ and $B = \{\mathbf{v}_i\}_{i=1}^n$. In particular, for every vector $\mathbf{c} \in \mathbb{F}_{q^m}^n$, we have that

$$\mathrm{wt_R}(\mathbf{c}) = \min\{\mathrm{wt_H}(\mathbf{x}) \mid \mathbf{c} = \sum_{i=1}^n x_i \mathbf{v}_i, \\ B = \{\mathbf{v}_i\}_{i=1}^n \subset \mathbb{F}_q^n \textit{ is a basis of } \mathbb{F}_{q^m}^n\}.$$

The following inequality is obtained when choosing the basis B as the canonical basis. It also follows easily from the definitions and was first noticed by Gabidulin [11] when $\dim(D) = 1$:

$$\mathrm{wt_R}(D) \leq \mathrm{wt_H}(D). \tag{A.8}$$

Proof of Theorem A.1. We first prove the inequality $\leq$: Let $B = \{\mathbf{v}_i\}_{i=1}^n \subset \mathbb{F}_q^n$ be a basis of $\mathbb{F}_{q^m}^n$. If $\mathbf{c} = \sum_{i=1}^n x_i \mathbf{v}_i$ and $j \geq 0$, then

$$\mathbf{c}^{q^j} = \left(\sum_{i=1}^n x_i \mathbf{v}_i \right)^{q^j} = \sum_{i=1}^n x_i^{q^j} \mathbf{v}_i^{q^j} = \sum_{i=1}^n x_i^{q^j} \mathbf{v}_i,$$

since $\mathbf{v}_i \in \mathbb{F}_q^n$. It follows that $\varphi_B(\mathbf{c}^{q^j}) = \varphi_B(\mathbf{c})^{q^j}$, for all $\mathbf{c} \in \mathbb{F}_{q^m}^n$ and all $j \geq 0$, and therefore,

$$\varphi_B(D^*) = \sum_{j=0}^{m-1} \varphi_B(D^{q^j}) = \sum_{j=0}^{m-1} \varphi_B(D)^{q^j} = \varphi_B(D)^*.$$

Hence, using this and Lemma A.12, we see that

$$\begin{aligned} \mathrm{wt_R}(D) &= \dim(D^*) = \dim(\varphi_B(D^*)) \\ &= \dim(\varphi_B(D)^*) = \mathrm{wt_R}(\varphi_B(D)) \leq \mathrm{wt_H}(\varphi_B(D)), \end{aligned}$$

where the last inequality follows from (A.8).

Now we prove the inequality $\geq$: We will show that we may select an appropriate basis B from the given family such that $\mathrm{wt_R}(D) \geq \mathrm{wt_H}(\varphi_B(D))$.

By Proposition A.10, since D^* is Galois closed, it has a basis $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s$ of vectors in $\mathbb{F}_q^n$. We may extend it to a basis $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ of $\mathbb{F}_q^n$, which is then a basis of $\mathbb{F}_{q^m}^n$ as an $\mathbb{F}_{q^m}$-linear space. Then $\mathrm{Supp}(\varphi_B(D)) \subset \{1, 2, \ldots s\}$, since $\varphi_B(\mathbf{v}_i) = \mathbf{e}_i$, where the vectors $\mathbf{e}_i$ constitute the canonical basis. Therefore, $\mathrm{wt_R}(D) = \dim(D^*) = s \geq \mathrm{wt_H}(\varphi_B(D))$, as desired, and the inequality follows. □

We now give the following new equivalent definitions of generalized rank weights:

Theorem A.2. *For a linear code $C \subset \mathbb{F}_{q^m}^n$ and $1 \leq r \leq k = \dim(C)$, the r-th generalized rank weight of C is equal to:*

$$\begin{aligned} d_{R,r}(C) = \min\{ d_{H,r}(\varphi_B(C)) \mid B \subset \mathbb{F}_q^n \\ \textit{is a basis of } \mathbb{F}_{q^m}^n \} \end{aligned} \tag{A.9}$$

$$= n - \max\{ \dim(L_U^G) \mid U \subset \mathbb{F}_{q^m}^k, \dim(U) = k - r \}, \tag{A.10}$$

where G is a generator matrix of C, φ_B is as in Theorem A.1 and $L_U^G = \{\mathbf{x} \in \mathbb{F}_q^n \mid G\mathbf{x}^T \in U\}$.

Definition (A.10) is an analogous description as that of [14, Lemma 1] for generalized Hamming weights, and is expressed in terms of a generator matrix of the code. We now give new equivalent definitions of relative generalized rank weights. Observe that Definition (A.11) is an extension of Definition (A.6) for relative weights.

Theorem A.3. *For a nested linear code pair $C_2 \subsetneq C_1 \subset \mathbb{F}_{q^m}^n$ and $1 \leq r \leq \ell = \dim(C_1/C_2)$, the r-th relative generalized rank weight of $C_2 \subsetneq C_1$ is equal to:*

$$\begin{aligned} M_{R,r}(C_1, C_2) = \min\{\mathrm{wt_R}(D) \mid D \subset C_1, \\ D \cap C_2 = 0, \dim(D) = r\} \end{aligned} \tag{A.11}$$

$$\begin{aligned} = \min\{M_{H,r}(\varphi_B(C_1), \varphi_B(C_2)) \mid B \subset \mathbb{F}_q^n \\ \text{is a basis of } \mathbb{F}_{q^m}^n\} \end{aligned} \tag{A.12}$$

$$\begin{aligned} = n - \max\{\dim(L_U^G) \mid U \subset \mathbb{F}_{q^m}^{k_1}, \\ \dim(U) = k_1 - r, \dim(U^I) = k_2\}, \end{aligned} \tag{A.13}$$

where φ_B is as in Theorem A.1, G is a generator matrix of C_1, the first k_2 rows of G are a basis of C_2 and U^I is the projection of U onto the first k_2 coordinates.

Now, the last definition is analogous to [37, Lemma 2] for the Haming case. We only prove Theorem A.3, since Theorem A.2 is obtained from it by choosing $C_2 = 0$.

Proof of Theorem A.3. We first prove $(A.5) \geq (A.11)$: Take a V as in (A.5). Since $\dim((C_1 \cap V)/(C_2 \cap V)) \geq r$, we may choose a linear subspace $D \subset C_1 \cap V$ such that $\dim(D) = r$ and $D \cap (C_2 \cap V) = 0$. Hence D is as in (A.11). Moreover, since $D \subset V$, we have that $D^* \subset V^* = V$, hence $\mathrm{wt_R}(D) \leq \dim(V)$ by Lemma A.12, and the inequality follows.

No we prove $(A.5) \leq (A.11)$: Take D as in (A.11), and define $V = D^*$, which is Galois closed. The natural linear map $D \longrightarrow (C_1 \cap V)/(C_2 \cap V)$ is one to one, and hence $\dim((C_1 \cap V)/(C_2 \cap V)) \geq \dim(D) = r$, and V is as in (A.5). Moreover, $\dim(V) = \dim(D^*) = \mathrm{wt_R}(D)$ by Lemma A.12, hence the inequality follows.

Using Theorem A.1 and the expression (A.3), we see that $(A.11) = (A.12)$.

Finally, we prove that $(A.11) = (A.13)$. Fix $U \subset \mathbb{F}_{q^m}^{k_1}$ as in (A.13), and define $V = U^\perp$ and $D = \{\mathbf{v}G \mid \mathbf{v} \in V\}$. It holds that $\dim(D) = r$ and $D \cap C_2 = 0$ since $U^I = \mathbb{F}_{q^m}^{k_2}$. For any $\mathbf{x} \in \mathbb{F}_q^n$, we have that

$$G\mathbf{x}^T \in U \Longleftrightarrow \mathbf{v}G\mathbf{x}^T = \mathbf{0}, \forall \mathbf{v} \in V$$

$$\Longleftrightarrow \mathbf{d} \cdot \mathbf{x} = \mathbf{0}, \forall \mathbf{d} \in D \Longleftrightarrow \mathbf{x} \in D^\perp,$$

and thus $L_U^G = (D^\perp)|_{\mathbb{F}_q}$. Using Lemma A.12 and Delsarte's Lemma A.11,

$$\mathrm{wt_R}(D) = \dim(\mathrm{Tr}(D)) = n - \dim(L_U^G),$$

and we are done. □

4 Equivalences of codes

The purpose of this section is to characterize the $\mathbb{F}_{q^m}$-linear vector space isomorphisms $\phi : V \longrightarrow V'$ that preserve rank weights, where V, V' are Galois closed.

Observe first of all that $\mathrm{wt_R}(V) = \dim(V)$ and $\mathrm{wt_R}(V') = \dim(V')$ by Lemma A.12, hence $\dim(V) = \dim(V')$ is necessary if we want to preserve all possible rank weights.

A first characterization has been given in [3, Theorem 1], for $V = V' = \mathbb{F}_{q^m}^n$. We will see that, due to our new characterizations, equivalent codes are guaranteed to exactly perform in the same way in secure network coding, and not only regarding worst cases (which would be guaranteed just by having the same minimum rank distance). Moreover, in contrast with [3], we consider equivalent codes with different lengths, which allows to consider equivalent codes that can be applied to networks with different number of outgoing links. As a consequence, we will see which is the minimum possible length of a code equivalent to a given one, that is, which is the minimum number of outgoing links that a given code requires.

4.1 New characterizations

Define the sets $\Upsilon(\mathbb{F}_{q^m}^n)$ and $\Lambda(\mathbb{F}_{q^m}^n)$ as the set of Galois closed linear subspaces of $\mathbb{F}_{q^m}^n$ and the set of subspaces of the form $V_I = \{\mathbf{c} \in \mathbb{F}_{q^m}^n \mid c_i = 0, \forall i \notin I\}$, for some $I \subset \mathcal{J} = \{1, 2, \ldots, n\}$, respectively, as in [20]. We will write just Υ and Λ if there is no confusion on the space $\mathbb{F}_{q^m}^n$. For convenience, we also define $L_I = \{\mathbf{c} \in \mathbb{F}_q^n \mid c_i = 0, \text{ if } i \notin I\}$.

The rank weights are defined in terms of the spaces in Υ (see (A.4) or [20]), and the Hamming weights are defined in terms of the spaces in Λ (see [20, 21]). We will use this analogy in the rest of the paper.

We have the following two collections of characterizations of Hamming-weight and rank-weight preserving vector space isomorphisms. To the best of our knowledge, only the equivalence between items 2 and 5 has been noticed in the Hamming case, which is an obvious consequence of MacWilliams extension theorem (see [16, Section 7.9]). We only prove the rank case, that is, Theorem A.5, being the proof of Theorem A.4 analogous.

Theorem A.4. *Given an $\mathbb{F}_{q^m}$-linear vector space isomorphism $\phi : V \longrightarrow V'$, where $V \in \Lambda(\mathbb{F}_{q^m}^n)$ and $V' \in \Lambda(\mathbb{F}_{q^m}^{n'})$, the following are equivalent:*

1. *If $\mathbf{c} \in V$ and $\mathrm{wt_H}(\mathbf{c}) = 1$, then $\mathrm{wt_H}(\phi(\mathbf{c})) = 1$.*

2. *ϕ preserves Hamming weights, that is, $\mathrm{wt_H}(\phi(\mathbf{c})) = \mathrm{wt_H}(\mathbf{c})$, for all $\mathbf{c} \in V$.*

3. *For all linear subspaces $D \subset V$, it holds that $\mathrm{wt_H}(\phi(D)) = \mathrm{wt_H}(D)$.*

4. *For all $U \in \Lambda(\mathbb{F}_{q^m}^n)$, $U \subset V$, it holds that $\phi(U) \in \Lambda(\mathbb{F}_{q^m}^{n'})$.*

5. *ϕ is a monomial map. That is, if $V = V_I$ and $V' = V_J$, with $N = \#I = \#J$, then there exists a bijection $\sigma : I \longrightarrow J$ and elements $\gamma_1, \gamma_2, \ldots, \gamma_N \in \mathbb{F}_{q^m}$ such that $\phi(\mathbf{e}_i) = \gamma_i \mathbf{e}_{\sigma(i)}$, for all $i \in I$.*

In such case, we will say that ϕ is a Hamming-weight preserving transformation or a Hamming equivalence.

Theorem A.5. *Given an $\mathbb{F}_{q^m}$-linear vector space isomorphism $\phi : V \longrightarrow V'$, where $V \in \Upsilon(\mathbb{F}_{q^m}^n)$ and $V' \in \Upsilon(\mathbb{F}_{q^m}^{n'})$, the following are equivalent:*

1. *If $\mathbf{c} \in V$ and $\mathrm{wt_R}(\mathbf{c}) = 1$, then $\mathrm{wt_R}(\phi(\mathbf{c})) = 1$.*

2. *ϕ preserves rank weights, that is, $\mathrm{wt_R}(\phi(\mathbf{c})) = \mathrm{wt_R}(\mathbf{c})$, for all $\mathbf{c} \in V$.*

3. *For all linear subspaces $D \subset V$, it holds that $\mathrm{wt_R}(\phi(D)) = \mathrm{wt_R}(D)$.*

4. *For all $U \in \Upsilon(\mathbb{F}_{q^m}^n)$, $U \subset V$, it holds that $\phi(U) \in \Upsilon(\mathbb{F}_{q^m}^{n'})$.*

5. *There exists $\beta \in \mathbb{F}_{q^m}^* = \mathbb{F}_{q^m} \setminus \{0\}$ and an $\mathbb{F}_{q^m}$-linear vector space isomorphism $\phi' : V \longrightarrow V'$ such that $\phi'(V|_{\mathbb{F}_q}) \subset V'|_{\mathbb{F}_q}$ and $\phi(\mathbf{c}) = \beta\phi'(\mathbf{c})$, for every $\mathbf{c} \in V$. Equivalently, there exists a matrix $A \in \mathbb{F}_q^{n \times n'}$ and $\beta \in \mathbb{F}_{q^m}^*$ such that $\phi(\mathbf{c}) = \beta\mathbf{c}A$, for every $\mathbf{c} \in V$.*

In such case, we will say that ϕ is a rank-weight preserving transformation or a rank-metric equivalence.

Proof. It is obvious that item 2 implies item 1 and item 3 implies item 2.

We now see that item 4 implies item 3. First, the number of sets in the family $\Upsilon(\mathbb{F}_{q^m}^n)$ that are contained in V is the same as the number of sets in the family $\Upsilon(\mathbb{F}_{q^m}^{n'})$ that are contained in V', since $\dim(V) = \dim(V')$. It follows that, given a linear subspace $U \subset V$, $U \in \Upsilon(\mathbb{F}_{q^m}^n)$ if, and only if, $\phi(U) \in \Upsilon(\mathbb{F}_{q^m}^{n'})$. Now given a linear subspace $D \subset V$, since D^* is the smallest set in $\Upsilon(\mathbb{F}_{q^m}^n)$ that contains D, it follows that $\phi(D^*) = \phi(D)^*$. Therefore, $\mathrm{wt_R}(D) = \dim(D^*) = \dim(\phi(D^*)) = \dim(\phi(D)^*) = \mathrm{wt_R}(\phi(D))$ by Lemma A.12.

To prove that item 5 implies item 4, it is enough to show that, for a given subspace $U \subset V$, if $U^q \subset U$, then $\phi(U)^q \subset \phi(U)$. Take bases $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_N\}$ and $B' = \{\mathbf{v}'_1, \mathbf{v}'_2, \ldots, \mathbf{v}'_N\}$ of V and V' in $\mathbb{F}_q^n$, respectively, such that $\phi(\mathbf{v}_i) = \beta\mathbf{v}'_i$. Take $\mathbf{u} \in U$, and write it as $\mathbf{u} = \sum_{i,j} \lambda_{i,j}\alpha_j\mathbf{v}_i$, where $\lambda_{i,j} \in \mathbb{F}_q$. Then $\phi(\mathbf{u})^q = \sum_{i,j} \lambda_{i,j}\beta^q\alpha_j^q\mathbf{v}'_i$. Since $\phi(\mathbf{u}^q) = \sum_{i,j} \lambda_{i,j}\beta\alpha_j^q\mathbf{v}'_i \in \phi(U)$, it follows that $\phi(\mathbf{u})^q \in \phi(U)$.

Finally, we prove that item 1 implies item 5, which is a slight modification of the proof given in [3]. Taking a basis of V in $\mathbb{F}_q^n$ as before, it holds that

$\phi(\mathbf{v}_i) = \beta_i \mathbf{u}_i$, for some $\mathbf{u}_i \in \mathbb{F}_q^n$ and $\beta_i \in \mathbb{F}_{q^m}^*$. Since ϕ is an isomorphism, the vectors $\mathbf{u}_i$ are linearly independent.

Now take $i \neq j$ and assume that $\beta_i \neq a_{i,j}\beta_j$, for every $a_{i,j} \in \mathbb{F}_q$. Then there exists a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ that contains β_i and β_j. Therefore $\phi(\mathbf{v}_i + \mathbf{v}_j) = \beta_i \mathbf{u}_i + \beta_j \mathbf{u}_j$, but $\mathrm{wt_R}(\phi(\mathbf{v}_i + \mathbf{v}_j)) = \mathrm{wt_R}(\mathbf{v}_i + \mathbf{v}_j) = 1$ and also $\mathrm{wt_R}(\beta_i \mathbf{u}_i + \beta_j \mathbf{u}_j) = 2$, since $\mathbf{u}_i$ and $\mathbf{u}_j$ are linearly independent.

We have reached an absurd, so there exists $a_{i,j} \in \mathbb{F}_q^*$ such that $\beta_i = a_{i,j}\beta_j$, for all i, j. Defining $\beta = \beta_1 = a_{1,j}\beta_j$ and $\mathbf{v}_i' = a_{1,i}^{-1}\mathbf{u}_i$, we obtain a description of ϕ as in item 5. □

This motivates the following definition.

Definition A.16. We say that two (arbitrary) codes $C \subset \mathbb{F}_{q^m}^n$ and $C' \subset \mathbb{F}_{q^m}^{n'}$ are rank-metric equivalent if there exists a rank-metric equivalence ϕ between V and V' such that $\phi(C) = C'$, where $C \subset V \in \Upsilon(\mathbb{F}_{q^m}^n)$ and $C' \subset V' \in \Upsilon(\mathbb{F}_{q^m}^{n'})$. Similarly for Hamming equivalent codes.

Remark A.17. *Observe that item 2 states that equivalent codes behave exactly in the same way regarding error and erasure correction, and not just in worst cases, since corresponding codewords have the same rank weight (see [28, Subsection IV.C] for MRD codes, and [20, Theorem 4] and [29, Theorem 2] in general). On the other hand, item 4 states that equivalent linear codes behave exactly in the same way regarding information leakage, and not only in worst cases, since the information leaked by wiretapping links is measured by the dimension of* $C \cap U$*, for some* $U \in \Upsilon$*, as stated in [20, Lemma 7]. The previous theorem thus states that one property is preserved if, and only if, the other is preserved.*

The same holds for the Hamming case, where item 4 states that equivalent codes behave exactly in the same way regarding information leakage in code-based secret sharing [12, 21], and item 2 states that equivalent codes behave exactly in the same way regarding usual error and erasure correction.

Item 1 states that it is only necessary for codes to be equivalent that they behave in the same way regarding "unitary" errors.

Remark A.18. *Observe that, due to the equivalence between items 2 and 3, rank weight preserving transformations preserve not only minimum rank distances and rank weight distributions, but also generalized rank weights and generalized rank weight distributions.*

Remark A.19. *In the Hamming case, if* $\phi : C_1 \longrightarrow C_2$ *is an* $\mathbb{F}_{q^m}$*-linear vector space isomorphism that preserves Hamming weights, for arbitrary linear codes* $C_1 \subset \mathbb{F}_{q^m}^n$ *and* $C_2 \subset \mathbb{F}_{q^m}^{n'}$*, then it can be extended to a Hamming weight preserving isomorphism* $\widetilde{\phi} : V_I \longrightarrow V_J$*, where* $I = \mathrm{Supp}(C_1)$ *and* $J = \mathrm{Supp}(C_2)$*. This is known as MacWilliams extension theorem (see [16, Section 7.9]).*

However, this is not true in the rank case. For a counterexample, see [2, Example 2.9 (c)].

As a consequence, we can now establish the following relations between Hamming and rank weights:

Theorem A.6. *For any linear codes $D, C \subset \mathbb{F}_{q^m}^n$, we have that*

$$\mathrm{wt}_{\mathrm{R}}(D) = \min\{\mathrm{wt}_{\mathrm{H}}(\phi(D)) \mid \phi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n \text{ is a rank-metric equivalence}\},$$

$$d_{R,r}(C) = \min\{d_{H,r}(\phi(C)) \mid \phi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n \text{ is a rank-metric equivalence}\},$$

where $1 \leq r \leq k = \dim(C)$. Moreover, if $n \leq m$, we have that

$$\mathrm{wt}_{\mathrm{H}}(D) = \max\{\mathrm{wt}_{\mathrm{R}}(\phi(D)) \mid \phi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n \text{ is a Hamming equivalence}\},$$

$$d_{H,k}(C) = \max\{d_{R,k}(\phi(C)) \mid \phi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n \text{ is a Hamming equivalence}\}.$$

Proof. The second equality follows from the first one, which we now prove. By Theorem A.5, the map φ_B in Theorem A.1 is a rank-metric equivalence, for any basis $B \subset \mathbb{F}_q^n$ of $\mathbb{F}_{q^m}^n$, since it maps vectors in $\mathbb{F}_q^n$ to vectors in $\mathbb{F}_q^n$. On the other hand, given a rank-metric equivalence $\phi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$, with β and ϕ' as in item 5 in Theorem A.5, define $\mathbf{v}_i = \phi'^{-1}(\mathbf{e}_i)$, where $\mathbf{e}_i$ is the i-th vector in the canonical basis and $B = \{\mathbf{v}_i\}_{i=1}^n$. Hence $\phi' = \varphi_B$ and $\phi = \beta\varphi_B$. Multiplication by β preserves Hamming weights, and hence we see that the first equality follows from Theorem A.1.

The last equality follows from the third one, which we now prove. First, for every Hamming equivalence ϕ, it follows from Theorem A.4 and Equation (A.8) that $\mathrm{wt}_{\mathrm{H}}(D) = \mathrm{wt}_{\mathrm{H}}(\phi(D)) \geq \mathrm{wt}_{\mathrm{R}}(\phi(D))$, and therefore the inequality $\geq$ follows.

To conclude, we need to prove that there exists a Hamming equivalence ϕ such that $\mathrm{wt}_{\mathrm{H}}(D) = \mathrm{wt}_{\mathrm{R}}(\phi(D))$. By taking a suitable Hamming equivalence, we may assume that D has a generator matrix G of the following form: the rows in G (a basis for D) are $\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_r$, and there exist $0 = t_0 < t_1 < t_2 < \ldots < t_r \leq n$ such that, for every $i = 1, 2, \ldots, r$, $g_{i,j} = 1$ if $t_{i-1} < j \leq t_i$, and $g_{i,j} = 0$ if $t_i < j$. Observe that $t_r = \mathrm{wt}_{\mathrm{H}}(D)$.

Finally, choose a basis $\gamma_1, \gamma_2, \ldots, \gamma_m$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and define the Hamming equivalence $\phi(c_1, c_2, \ldots, c_n) = (\gamma_1 c_1, \gamma_2 c_2, \ldots, \gamma_n c_n)$. Then, $\phi(D)$ has a generator matrix whose rows are $\mathbf{h}_i = \phi(\mathbf{g}_i)$, which satisfy that $h_{i,j} = \gamma_j$ if $t_{i-1} < j \leq t_i$, and $h_{i,j} = 0$ if $t_i < j$.

It follows that $G(\phi(D)) = \sum_{i=1}^r G(\mathbf{h}_i) = V_I$, where $I = \{1, 2, \ldots, t_r\}$, and we are done. □

4.2 Rank degenerateness and minimum length

Now we turn to degenerate codes in the rank case, extending the study in [17, Section 6].

Definition A.20. A linear code $C \subset \mathbb{F}_{q^m}^n$ is rank degenerate if it is rank-metric equivalent to a linear code $C' \subset \mathbb{F}_{q^m}^{n'}$ with $n' < n$.

Hamming degenerate codes are defined in the analogous way. As in the Hamming case, rank degenerate codes are identified by looking at their last generalized rank weight. This is the definition of rank degenerate codes used in [17]. However, note that our definition actually states whether a given code does not require the given length, which in network coding means whether a code can be implemented with less outgoing links from the source node.

The next proposition actually gives the whole range of lengths of linear codes rank-metric equivalent to a given one. To prove it, for every $V \in \Upsilon(\mathbb{F}_{q^m}^n)$ and every basis $B \subset \mathbb{F}_q^n$ of V, we define the $\mathbb{F}_{q^m}$-linear map

$$\psi_B : V \longrightarrow \mathbb{F}_{q^m}^{\dim(V)} \tag{A.14}$$

given by $\psi_B(\mathbf{c}) = \mathbf{x}$, if $B = \{\mathbf{v}_i\}_{i=1}^{\dim(V)}$ and $\mathbf{c} = \sum_{i=1}^{\dim(V)} x_i \mathbf{v}_i$. It is a rank-metric equivalence by Theorem A.5.

Proposition A.21. *Given a linear code $C \subset \mathbb{F}_{q^m}^n$ of dimension k and any positive integer n', there exists a linear code $C' \subset \mathbb{F}_{q^m}^{n'}$ that is rank-metric equivalent to C if, and only if, $n' \geq d_{R,k}(C)$.*

Proof. For a given n', assume that there exists a linear code $C' \subset \mathbb{F}_{q^m}^{n'}$ that is rank-metric equivalent to C. Then C' has dimension k and $d_{R,k}(C) = d_{R,k}(C') \leq n'$.

Now fix $n' = d_{R,k}(C) = \dim(C^*)$. Take $V = C^*$ and ψ_B as in (A.14) for some basis $B \subset \mathbb{F}_q^n$ of V. As remarked before, ψ_B is a rank-metric equivalence and thus C is rank-metric equivalent to $C' = \psi_B(C) \subset \mathbb{F}_{q^m}^{n'}$.

Finally, take $n'' \geq n' = d_{R,k}(C)$ and C' as in the previous paragraph. Append $n'' - n' \geq 0$ zeroes to every codeword in C'. The obtained code $C'' \subset \mathbb{F}_{q^m}^{n''}$ is linear and rank-metric equivalent to C', and thus also to C, and we are done. □

Therefore, $d_{R,k}(C)$ gives the minimum possible length (minimum number of outgoing links required by C) of a linear code that is rank equivalent to C. As an immediate consequence, we obtain the following:

Corollary A.22. *A linear code $C \subset \mathbb{F}_{q^m}^n$ of dimension k is rank degenerate if, and only if, $d_{R,k}(C) < n$, or equivalently, $C^* \neq \mathbb{F}_{q^m}^n$.*

On the other hand, we obtain the following result. The first part is [17, Corollary 30].

Proposition A.23. *If $mk < n$, then every linear code $C \subset \mathbb{F}_{q^m}^n$ of dimension k is rank degenerate. On the other hand, if $mk \geq n$, then there exists a linear code $C \subset \mathbb{F}_{q^m}^n$ of dimension k that is not rank degenerate.*

Proof. The first part follows from the previous corollary and the fact that $\dim(C^*) \leq mk$.

Now, if $mk \geq n$, choose $\lambda_{l,j}^{(i)} \in \mathbb{F}_q$, for $1 \leq i \leq k$, $1 \leq j \leq n$ and $1 \leq l \leq m$, such that $\langle \{\mathbf{x}_{l,i}\}_{1 \leq l \leq m}^{1 \leq i \leq k} \rangle = \mathbb{F}_q^n$, where $\mathbf{x}_{l,i} = \sum_{j=1}^n \lambda_{l,j}^{(i)} \mathbf{e}_j$ and $\mathbf{e}_j$ is the canonical basis of $\mathbb{F}_q^n$. This is possible since $mk \geq n$.

On the other hand, define $\mathbf{u}_i = \sum_{l=1}^m \alpha_l \mathbf{x}_{l,i} \in \mathbb{F}_{q^m}^n$, and $C' = \langle \mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k \rangle$. Then, $C'^* = \mathbb{F}_{q^m}^n$ and $\dim(C') \leq k$. Taking $C' \subset C$, with $\dim(C) = k$, we obtain the desired code. □

5 Bounds on generalized rank weights

In this section we establish a method to derive bounds on generalized rank weights from bounds on generalized Hamming weights, and afterwards we discuss what the Singleton bound can be for generalized rank weights. Due to [20, Lemma 7 and Theorem 2], bounds on generalized rank weights directly translate into bounds on worst case information leakage on networks, and therefore are of significant importance.

5.1 Translating bounds on GHWs to bounds on GRWs

Some attempts to give bounds similar to the ones in the Hamming case have been made [7, 20, 25]. In this subsection, we prove that most of the bounds in the Hamming case can be directly translated to the rank case.

Note that, since rank weights are smaller than or equal to Hamming weights (by Equation (A.8)), every bound of the form

$$M \geq g_{s_1,s_2,\ldots,s_N}(d_{s_1}(C), d_{s_2}(C), \ldots, d_{s_N}(C)),$$

that is valid for Hamming weights, where $M > 0$ is a fixed positive real number and $g_{s_1,s_2,\ldots,s_N}$ is increasing in each component, is obviously also valid for rank weights. This is the case of the classical Singleton or Griesmer bounds [16, Section 7.10]. On the other hand, the next result is not straightforward if we do not use (A.9) or (A.12).

Theorem A.7. *Fix numbers k and $1 \leq r, s \leq k$, and functions $f_{r,s}, g_{r,s} : \mathbb{N} \longrightarrow \mathbb{R}$, which may also depend on n, m, k and q. If $g_{r,s}$ is increasing, then every bound of the* *form*

$$f_{r,s}(d_r(C)) \geq g_{r,s}(d_s(C))$$

that is valid for generalized Hamming weights, for any linear code $C \subset \mathbb{F}_{q^m}^n$ *with* $\dim(C) = k$*, is also valid for generalized rank weights. The same holds for relative weights.*

Proof. By Theorem A.2, there exists a basis $B \subset \mathbb{F}_q^n$ of $\mathbb{F}_{q^m}^n$ such that $d_{R,r}(C) = d_{H,r}(\varphi_B(C))$. Therefore,

$$f_{r,s}(d_{R,r}(C)) = f_{r,s}(d_{H,r}(\varphi_B(C)))$$

$$\geq g_{r,s}(d_{H,s}(\varphi_B(C))) \geq g_{r,s}(d_{R,s}(C)),$$

where the last inequality follows again from Theorem A.2. Similarly for relative weights. □

Remark A.24. *The previous theorem is also valid, with the same proof, for the more general bounds*

$$f_{r,s_1,s_2,\ldots,s_N}(d_r(C))$$

$$\geq g_{r,s_1,s_2,\ldots,s_N}(d_{s_1}(C), d_{s_2}(C), \ldots, d_{s_N}(C)),$$

where $g_{r,s_1,s_2,\ldots,s_N}$ *is increasing in each component. However, most of the bounds in the literature are of the form of the previous theorem.*

In [14] and [32, Part I, Section III.A], many of these kind of bounds are given for generalized Hamming weights. One of these (a particular case of [32, Corollary 3.6]) is proven for rank weights in [7, Proposition II.3], using (A.4). Some of these are also valid for relative weights (see [37, Proposition 1 and Proposition 2] or [38]). We next list some of these bounds, where $1 \leq r \leq s \leq k$, and $d_j = d_{R,j}(C)$, for all j. Note that monotonicity is one of these bounds, and therefore it does not need a specific proof. Also recall that linear codes in this paper are $\mathbb{F}_{q^m}$-linear, and hence the field size is q^m, not q.

1. Monotonicity:

$$d_{r+1} \geq d_r + 1,$$

2. Griesmer-type ([32, bound (14)]):

$$d_r \geq \sum_{i=0}^{r-1} \left\lceil \frac{d_1}{q^{mi}} \right\rceil,$$

3. Griesmer-type ([32, bound (16)]):

$$d_s \geq d_r + \sum_{i=0}^{s-r} \left\lceil \frac{(q^m - 1)d_r}{(q^{mr} - 1)q^{mi}} \right\rceil,$$

4. [14, Theorem 1] or [32, bound (18)]:
$$(q^{ms}-1)d_r \leq (q^{ms}-q^{m(s-r)})d_s,$$

5. [14, Corollary 1]:
$$(q^{mr}-1)d_1 \leq (q^{mr}-q^{m(r-1)})d_r,$$

6. [7, Proposition II.3]:
$$(q^{mr}-1)d_{r-1} \leq (q^{mr}-q^{m})d_r,$$

7. [32, bound (20)]:
$$d_r \geq n - \left\lfloor \frac{(q^{m(k-r)}-1)(n-d_s)}{q^{m(k-s)}-1} \right\rfloor.$$

Remark A.25. *A trivial lower bound that is valid for every linear code is $d_{R,r}(C) \geq r$, for all $1 \leq r \leq k$. Observe that a linear code C satisfies that $d_{R,r}(C) = r$, for every $1 \leq r \leq k$ if, and only if, C is Galois closed. This gives another characterization of Galois closed spaces to those in Proposition A.10, in terms of generalized rank weights. In the Hamming case, $d_{H,r}(C) = r$, for every $1 \leq r \leq k$ if, and only if, $C = V_I$, for some $I \subset \{1, 2, \ldots, n\}$.*

5.2 On the Singleton bound

In this subsection, we discuss the possible extensions of the Singleton bound to rank weights. We start by giving a brief overview of the bounds in the literature that resemble the usual Singleton bound, both for a linear code $C \subset \mathbb{F}_{q^m}^n$ and a nested linear code pair $C_2 \subsetneq C_1 \subset \mathbb{F}_{q^m}^n$:

$$d_{R,r}(C) \leq \begin{cases} n-k+r \text{ [20]}, \\ (m-1)k+r \text{ [20]}, \\ \frac{m}{n}(n-k)+1, \text{ if } r=1 \text{ [23]}, \end{cases}$$

$$M_{R,s}(C_1, C_2) \leq \begin{cases} n-k_1+s \text{ [20]}, \\ (m-1)(k_1-k_2)+s \text{ [20]}, \\ \frac{m(n-k_1)}{n-k_2}+1, \text{ if } s=1 \text{ [20]}, \end{cases}$$

where $1 \leq r \leq k = \dim(C)$ and $1 \leq s \leq k_1 - k_2$, $k_1 = \dim(C_1)$ and $k_2 = \dim(C_2)$.

In [8, Proposition 6], a refinement of the classical Singleton bound is given for cyclic codes. By [8, Proposition 5] and duality [7, Theorem], this bound is $d_{R,1}(C) \leq d_{R,k}(C) - k + 1$. Hence this bound is implied by the classical bound and Proposition A.21, or by monotonicity. The description in [8] gives then an alternative description of this bound for cyclic codes.

As a tool for future bounds, we establish the following one. It shows how to obtain bounds for all generalized weights from bounds on the first one or the last one.

Lemma A.26. *For every linear code $C \subset \mathbb{F}_{q^m}^n$, and for every $1 \leq r \leq k-1$, $k = \dim(C)$, it holds that*

$$1 \leq d_{R,r+1}(C) - d_{R,r}(C) \leq m.$$

The same bound applies to relative generalized rank weights.

Proof. It is enough to prove that, if $D \subset D'$ and $\dim(D') = \dim(D) + 1$, then $\mathrm{wt_R}(D') \leq \mathrm{wt_R}(D) + m$. Take $\mathbf{d} \in D'$ such that $D' = D \oplus \langle \mathbf{d} \rangle$. Then $D'^* = D^* + \langle \mathbf{d} \rangle^*$, and the result follows, since $\mathrm{wt_R}(\mathbf{d}) \leq m$. □

Note that this bound implies that an inverse statement to Theorem A.7 is not possible: Take for instance $m = 1$, then we have the bound $d_{R,r+1} = d_{R,r} + 1$, which holds for all linear codes. However, the bound $d_{H,r+1} = d_{H,r} + 1$ does not hold for all linear codes.

The case $r = 1$ of the following bound was established and proven by Loidreau in [23] and for relative weights by Kurihara et al. in [20, Proposition 3]. The general case follows from these and the previous lemma.

Proposition A.27 (Alternative Singleton bound). *If $n > m$, then for every linear code $C \subset \mathbb{F}_{q^m}^n$, and every $1 \leq r \leq k = \dim(C)$,*

$$d_{R,r}(C) \leq \frac{m}{n}(n-k) + m(r-1) + 1.$$

For a code pair $C_2 \subsetneq C_1 \subset \mathbb{F}_{q^m}^n$, with $k_i = \dim(C_i)$, $i = 1, 2$, and every $1 \leq r \leq \dim(C_1/C_2)$,

$$M_{R,r}(C_1, C_2) \leq \frac{m(n-k_1)}{n-k_2} + m(r-1) + 1.$$

Now, for generalized rank weights, it is easy to see that this bound is sharper than the usual Singleton bound if, and only if,

$$r \leq \left\lfloor \frac{n(n-1) - (n-m)k}{n(m-1)} \right\rfloor, \tag{A.15}$$

which is a number in $(1, k]$ if $n \leq mk$ (the case where the code is not necessarily rank degenerate, see Proposition A.23). However, as it is usual and for convenience, we give the following definition:

Definition A.28 ([7, Definition 1]). A linear code $C \subset \mathbb{F}_{q^m}^n$ of dimension k is r-MRD if $d_{R,r}(C) = n - k + r$. We say it is MRD if it is 1-MRD. Similarly for r-MDS and MDS codes, replacing $d_{R,r}$ by $d_{H,r}$ (see [33, Section VI]).

We also obtain the bound $d_{R,r}(C) \leq rm$ from the previous lemma, by induction on r. Therefore, the overview of the Singleton bound becomes now as follows, with notation as above, which improves the bounds in the previous overview:

$$d_{R,r}(C) \leq \begin{cases} n-k+r, \\ rm, \\ \frac{m}{n}(n-k) + m(r-1) + 1, \end{cases}$$

$$M_{R,s}(C_1, C_2) \leq \begin{cases} n-k_1+s, \\ sm, \\ \frac{m(n-k_1)}{n-k_2} + m(s-1) + 1. \end{cases}$$

Remark A.29. *The bound $d_{R,r}(C) \leq rm$ is sharper than the alternative Singleton bound if, and only if, $n \geq mk$. We know that in this case, C is rank degenerate (Proposition A.23). Therefore, for codes that are not rank degenerate, the usual and alternative Singleton bounds are the sharpest ones.*

Remark A.30. *When $n \leq m$ the usual Singleton bound is the sharpest general upper bound on the rank distance, since Gabidulin codes (see [11]) are MRD and may have length n, for all $n \leq m$, and dimension k, for all $1 \leq k \leq n$.*

Since the alternative Singleton bound is sharper for $r = 1$ when $n > m$, it follows immediately that, given $1 \leq k \leq n$, and m, there exists an MRD code over $\mathbb{F}_{q^m}^n$, with length n and dimension k, if and only if, $n \leq m$. This gives a result analogous to the MDS conjecture (see [16, page 265]) for the rank distance – although in this case it is not a conjecture.

Also note that the inequality (A.15) gives a lower bound on the number r such that C is r-MRD.

Remark A.31. *One might ask if a bound of the form $d_{R,r}(C) \leq \frac{m}{n}(n-k) + r$ holds, when $n > m$. However, this is not true even for $r = 2$. Take for example $m = 2$, $n = 4$, $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, and the code $C = \langle (1, \alpha, 0, 0), (0, 0, \alpha, 1) \rangle$, which has dimension $k = 2$. It is easy to see that C^* has dimension 4, since $(1, \alpha, 0, 0), (1, \alpha^q, 0, 0), (0, 0, \alpha, 1)$ and $(0, 0, \alpha^q, 1)$ are linearly independent over $\mathbb{F}_{q^m}$. Thus, for $r = k = 2$,*

$$d_{R,2}(C) = 4, \quad \textit{and} \quad \frac{m}{n}(n-k) + r = \frac{2}{4}(4-2) + 2 = 3.$$

Moreover, we see that $d_{R,2}(C)$ attains the alternative Singleton bound.

We conclude the section with a simple fact that connects r-MRD codes with r-MDS codes, and which follows directly from (A.9).

Proposition A.32. *A linear code $C \subset \mathbb{F}_{q^m}^n$ is r-MRD if, and only if, $\varphi_B(C)$ is r-MDS, for all bases $B \subset \mathbb{F}_q^n$ of $\mathbb{F}_{q^m}^n$.*

Thus, if C is a Gabidulin code [11], it is obviously MDS, but also the codes $\varphi_B(C)$ are MDS. It can also be easily shown that the codes $\varphi_B(C)$ are again Gabidulin codes. Therefore, to prove that they are MRD, it is only necessary to prove that they are MDS.

6 Rank-puncturing and rank-shortening

In this section we discuss what are the operations on rank-metric codes analogous to puncturing and shortening [16, Section 1.5]. The main importance of the concept of puncturing is that a punctured codeword is essentially the same as a codeword with erasures, as in the Hamming case. Recall that the shortened and punctured codes of a given code $C \subset \mathbb{F}_{q^m}^n$ on the coordinates in the set $I \subset \mathcal{J}$ are defined, respectively, as

$$\begin{aligned} C_I =& C \cap V_I = \{\mathbf{c} \in C \mid c_i = 0, \forall i \notin I\}, \\ C^I =& \{(c_i)_{i \in I} \mid \mathbf{c} \in C\}. \end{aligned}$$

6.1 The definitions

For a linear subspace $L \subset \mathbb{F}_q^n$, fix another subspace $L' \subset \mathbb{F}_q^n$ such that $\mathbb{F}_q^n = L' \oplus L^\perp$. Observe that $\dim(L) = n - \dim(L^\perp) = \dim(L')$, which we will use throughout the section. We then define the projection map

$$\pi_{L,L'} : \mathbb{F}_{q^m}^n \longrightarrow V' = L' \otimes \mathbb{F}_{q^m},$$

such that $\pi_{L,L'}(\mathbf{c}) = \mathbf{c}_1$, where $\mathbf{c} = \mathbf{c}_1 + \mathbf{c}_2$, $\mathbf{c}_1 \in V' = L' \otimes \mathbb{F}_{q^m}$ and $\mathbf{c}_2 \in V^\perp = L^\perp \otimes \mathbb{F}_{q^m}$. We then write $C^{L,L'} = \pi_{L,L'}(C)$, for an (arbitrary) code $C \subset \mathbb{F}_{q^m}^n$.

Lemma A.33. *For any two subspaces $L', L'' \subset \mathbb{F}_q^n$ such that $\mathbb{F}_q^n = L' \oplus L^\perp = L'' \oplus L^\perp$, and for any code $C \subset \mathbb{F}_{q^m}^n$, we have that the codes $C^{L,L'}$ and $C^{L,L''}$ are rank-metric equivalent in a canonical way.*

Proof. Define $\phi : V' \longrightarrow V''$ by $\phi(\mathbf{c}) = \pi_{L,L''}(\mathbf{c})$, where $V' = L' \otimes \mathbb{F}_{q^m}$ and $V'' = L'' \otimes \mathbb{F}_{q^m}$.

First we see that ϕ is a vector space isomorphism. Since $\dim(V') = \dim(V'')$, we only need to prove that it is one to one. Assume that $\pi_{L,L''}(\mathbf{c}) = \mathbf{0}$. This means that $\mathbf{c} \in V^\perp$, but also $\mathbf{c} \in V'$ and $V' \cap V^\perp = 0$, hence $\mathbf{c} = \mathbf{0}$.

On the other hand, since $\mathbb{F}_q^n = L'' \oplus L^\perp$, if $\mathbf{c} \in L'$, then $\phi(\mathbf{c}) \in L''$. In other words, $\phi(V'|_{\mathbb{F}_q}) \subset V''|_{\mathbb{F}_q}$. By Theorem A.5, item 5, ϕ is a rank-metric equivalence.

Finally, we see that $\phi(C^{L,L'}) = C^{L,L''}$. If $\mathbf{c}_1 \in C^{L,L'}$, then there exists $\mathbf{c} = \mathbf{c}_1 + \mathbf{c}_2 \in C$, with $\mathbf{c}_2 \in V^\perp$. Write $\mathbf{c} = \widetilde{\mathbf{c}}_1 + \widetilde{\mathbf{c}}_2$, with $\widetilde{\mathbf{c}}_1 \in V''$ and $\widetilde{\mathbf{c}}_2 \in V^\perp$. Then $\mathbf{c}_1 = \widetilde{\mathbf{c}}_1 + (\widetilde{\mathbf{c}}_2 - \mathbf{c}_2)$ and hence $\phi(\mathbf{c}_1) = \widetilde{\mathbf{c}}_1 \in C^{L,L''}$. □

Therefore, the next definition of rank-punctured code is consistent.

Definition A.34. For every $\mathbb{F}_q$-linear space $L \subset \mathbb{F}_q^n$, and every code $C \subset \mathbb{F}_{q^m}^n$, we define its rank-punctured and rank-shortened codes over L as $C^L = C^{L,L'}$ and $C_L = C \cap V$, respectively, for some L' as before, where $V = L \otimes \mathbb{F}_{q^m}$.

Similarly, for a coding scheme $\mathcal{P}_\mathcal{S} = \{C_\mathbf{x}\}_{\mathbf{x} \in \mathcal{S}}$, we can define its rank-punctured and rank-shortened schemes over L as $\mathcal{P}_\mathcal{S}^L = \{C_\mathbf{x}^L\}_{\mathbf{x} \in \mathcal{S}}$ and $\mathcal{P}_{\mathcal{S}L} = \{C_{\mathbf{x}L}\}_{\mathbf{x} \in \mathcal{S}}$, respectively. For a linear coding scheme built from $C_2 \subsetneq C_1 \subset \mathbb{F}_{q^m}^n$, they are the schemes built from $C_2^L \subset C_1^L$ and $C_{2L} \subset C_{1L}$, respectively.

Observe that it is not always true that $C_L \subset C^L$, as opposed to the usual shortening and puncturing. On the other hand, we see that, for every $I \subset \mathcal{J}$, $V_I \in \Upsilon$. Then, it is easy to see that $C^I = C^{L_I}$ and $C_I = C_{L_I}$, regarded as subspaces of V_I. Thus the previous definition extends the usual definition of puncturing and shortening. For brevity, we will use just the words puncturing and shortening for rank-puncturing and rank-shortening, respectively.

Remark A.35. *Note that, given $L \subset \mathbb{F}_q^n$, there may be more than one subspace $L' \subset \mathbb{F}_q^n$ such that $\mathbb{F}_q^n = L' \oplus L^\perp$ (later we will actually see how to obtain them). If $V = L \otimes \mathbb{F}_{q^m}$, then $V^\perp = L^\perp \otimes \mathbb{F}_{q^m}$, and what we are doing is finding a subspace $V' \in \Upsilon$ such that $\mathbb{F}_{q^m}^n = V' \oplus V^\perp$.*

On the other hand, if $V = V_I \in \Lambda$, then $V_I^\perp = V_{\overline{I}}$ and V_I is the unique subspace $V' \in \Lambda$ such that $\mathbb{F}_{q^m}^n = V' \oplus V^\perp$. Therefore, punctured codes in the Hamming case are defined in a unique way, in contrast with the rank case.

Usually, C^I and C_I are considered as subspaces of $\mathbb{F}_{q^m}^{\#I}$. This is obvious since $\mathrm{Supp}(C^I) \subset I$ and V_I is Hamming equivalent to $\mathbb{F}_{q^m}^{\#I}$. For rank-metric codes, we can fix bases B, B' of $L, L' \subset \mathbb{F}_q^n$, respectively, and consider $\psi_B(C_L)$ and $\psi_{B'}(C^L)$, where ψ_B and $\psi_{B'}$ are as in (A.14). That is, we can consider that $C_L, C^L \subset \mathbb{F}_{q^m}^{\dim(L)}$.

6.2 *r*-MRD characterizations

In this subsection, we give characterizations of r-MRD (and r-MDS) codes in terms of dimensions of punctured codes. We start with a tool that generalizes Forney's Lemmas [10, Lemmas 1 and 2] and that is useful to relate dimensions of punctured and shortened codes. Note that [20, Lemma 10] is essentially the second equality in this lemma.

Lemma A.36. *For every linear code $C \subset \mathbb{F}_{q^m}^n$ of dimension k and every subspace $L \subset \mathbb{F}_q^n$, it holds that*

$$\dim(C^L) = \dim(L) - \dim((C^\perp)_L) = k - \dim(C_{L^\perp}).$$

Proof. The second equality is [20, Lemma 10]. Now $\dim(C^L) = \dim(\pi_{L,L'}(C)) = k - \dim(\ker(\pi_{L,L'})) = k - \dim(C_{L^\perp})$. □

We will need the duality theorem for generalized rank weights, which has been established and proven in [7] (we will give a shorter proof in Appendix B):

Theorem A.8 (Duality [7]). *Given a linear code $C \subset \mathbb{F}_{q^m}^n$ of dimension k, write $d_r = d_{R,r}(C)$ for $1 \leq r \leq k$, and $d_s^\perp = d_{R,s}(C^\perp)$, for $1 \leq s \leq n-k$. Then it holds that*

$$\begin{aligned}\{1, 2, \ldots, n\} = &\{d_1, d_2, \ldots, d_k\} \cup \\ &\{n+1-d_1^\perp, n+1-d_2^\perp, \ldots, n+1-d_{n-k}^\perp\},\end{aligned}$$

where the union is disjoint.

Note that, in the next propositions, the equivalence of the two first conditions follows directly from Wei's duality and its corresponding theorem for rank weights, as proven in [32, Proposition 4.1] and [7, Corollary III.3], respectively. The equivalence between item 2 and item 4 for Hamming weights is proven in [16, Theorem 1.4.15], and the case $r = 1$ (C is MDS) is fully proven in [16, Theorem 2.4.3]. It also generalizes [16, Corollary 1.4.14] and [16, Theorem 1.5.7 (ii)].

Proposition A.37. *The following conditions are equivalent for a linear code $C \subset \mathbb{F}_{q^m}^n$ of dimension k, and every $1 \leq r \leq k$:*

1. *The code C is r-MDS.*
2. $d_{H,1}(C^\perp) \geq k - r + 2$.
3. *For all $I \subset \mathcal{J}$ such that $\#I \leq k - r + 1$, we have that* $\dim(C^I) = \#I$.
4. *For all $I \subset \mathcal{J}$ such that $\#I \geq n - k + r - 1$, we have that* $\dim((C^\perp)^I) = n - k$.

Proposition A.38. *The following conditions are equivalent for a linear code $C \subset \mathbb{F}_{q^m}^n$ of dimension k, and every $1 \leq r \leq k$:*

1. *The code C is r-MRD.*
2. $d_{R,1}(C^\perp) \geq k - r + 2$.
3. *For all $L \subset \mathbb{F}_q^n$ such that* $\dim(L) \leq k - r + 1$, *we have that* $\dim(C^L) = \dim(L)$.
4. *For all $L \subset \mathbb{F}_q^n$ such that* $\dim(L) \geq n - k + r - 1$, *we have that* $\dim((C^\perp)^L) = n - k$.

Proof. The equivalence between the first two conditions follows from the duality Theorem A.8, as proven in [7], and the equivalence between the last two conditions follows from Lemma A.36.

Now, we prove that condition 3 implies condition 2. Take $\mathbf{c} \in C^\perp \setminus 0$ and assume that $\mathrm{wt_R}(\mathbf{c}) = \dim(L) \leq k - r + 1$, where $L = (\langle \mathbf{c} \rangle^*)|_{\mathbb{F}_q}$ (recall $\mathrm{wt_R}(\mathbf{c}) = \dim(\langle \mathbf{c} \rangle^*)$ from Lemma A.12). Then by Lemma A.36,

$$\dim(L) = \dim(C^L) = \dim(L) - \dim((C^\perp)_L),$$

and thus $(C^\perp)_L = 0$, but this implies that $\mathbf{c} = \mathbf{0}$, which is a contradiction. Hence $\mathrm{wt_R}(\mathbf{c}) \geq k - r + 2$.

Finally, we prove that condition 2 implies condition 3. Let $L \subset \mathbb{F}_q^n$ be such that $\dim(L) \leq k - r + 1$. Then, by the definition of minimum rank distance (recall (A.4)), we have that $\dim((C^\perp)_L) = 0$, and thus by Lemma A.36,

$$\dim(C^L) = \dim(L) - \dim((C^\perp)_L) = \dim(L).$$

After showing how to compute generator matrices for punctured codes, it can be easily proven that the equivalence between items 2 and 3 generalizes [11, Theorem 1].

Corollary A.39. *The smallest integer r such that C is r-MDS is* $r = k - d_{H,1}(C^\perp) + 2$, *and similarly for rank weights.*

6.3 Information spaces

Next, we define the notion of information space, which plays the same role as information sets in the Hamming case: any original codeword can be recovered from the punctured codeword if (and also only if in the linear case) we puncture on an information space. Therefore, information spaces completely describe the erasure correction capability of a code, and not only worst cases.

Definition A.40. Given a linear code $C \subset \mathbb{F}_{q^m}^n$, we say that a subspace $L \subset \mathbb{F}_q^n$ is an information space for C if $\dim(C^L) = \dim(C)$. Equivalently, if the restriction $\pi_{L,L'} : C \longrightarrow C^L$ is an $\mathbb{F}_{q^m}$-linear vector space isomorphism.

For an (arbitrary) code $C \subset \mathbb{F}_{q^m}^n$, we say that L is an information space for C if $\pi_{L,L'} : C \longrightarrow C^L$ is bijective.

On the other hand, given a code pair $C_2 \subsetneq C_1 \subset \mathbb{F}_{q^m}^n$, we say that L is an information space for C_1, C_2 if $\dim(C_1^L / C_2^L) = \dim(C_1/C_2)$. In general, for an (arbitrary) coding scheme $\mathcal{P}_{\mathcal{S}} = \{C_{\mathbf{x}}\}_{\mathbf{x} \in \mathcal{S}}$, we say that L is an information space for $\mathcal{P}_{\mathcal{S}}$ if $\pi_{L,L'}(C_{\mathbf{x}_1}) \cap \pi_{L,L'}(C_{\mathbf{x}_2}) = \varnothing$, whenever $\mathbf{x}_1 \neq \mathbf{x}_2$.

Observe that a set $I \subset \mathcal{J}$ is an information set for C if, and only if, L_I is an information space for C. Note also that $\pi_{L,L'}$ is always surjective, so it is only necessary to be injective in order to be bijective.

On the other hand, Proposition A.38, item 4, shows threshold values on the dimension of a space to guarantee that it is an information space for a given code, in terms of its minimum rank distance, as in the Hamming case.

Now we characterize MRD codes using information spaces, in the same way as MDS codes are characterized using information sets. Note that the result is a particular case of Proposition A.38, taking $r = 1$. After knowing how to compute generator matrices of punctured codes, it can be shown that this proposition is essentially [11, Theorem 2].

Proposition A.41. *A linear code $C \subset \mathbb{F}_{q^m}^n$ is MRD if, and only if, every $L \subset \mathbb{F}_q^n$, with $\dim(L) = k = \dim(C)$, is an information space for C.*

The following two propositions essentially describe erasure correction on networks. The second one also describes the correction capability of punctured codes. They are analogous to [16, Theorem 1.5.7 (ii)] and [16, Theorem 1.5.1], respectively. The first one also extends [11, Theorem 1] to arbitrary codes.

Proposition A.42. *Given an (arbitrary) code $C \subset \mathbb{F}_{q^m}^n$, if $\rho < d_R(C)$, then every subspace $L \subset \mathbb{F}_q^n$ with $\dim(L) \geq n - \rho$ is an information space for C. If $\rho \geq d_R(C)$, there exists a subspace $L \subset \mathbb{F}_q^n$ with $\dim(L) = n - \rho$ which is not an information space for C.*

Proof. First we prove in the first case that $\pi_{L,L'} : C \longrightarrow C^L$ is injective. Take $\mathbf{c}_1, \mathbf{c}_2 \in C$ such that $\pi_{L,L'}(\mathbf{c}) = \mathbf{0}$, where $\mathbf{c} = \mathbf{c}_1 - \mathbf{c}_2$. Then, $\mathbf{c} \in V^\perp$, $V = L \otimes \mathbb{F}_{q^m}$, and therefore, $\mathrm{wt_R}(\mathbf{c}) \leq \dim(V^\perp) \leq \rho$, which is absurd.

For the second statement, take $\mathbf{c}_1, \mathbf{c}_2$ and $\mathbf{c} = \mathbf{c}_1 - \mathbf{c}_2$ such that $\mathrm{wt_R}(\mathbf{c}) = d_R(C)$, write $D = \langle \mathbf{c} \rangle^* = \langle \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s \rangle$, with $\mathbf{v}_i \in \mathbb{F}_q^n$, and extend this to a basis $B = \{\mathbf{v}_i\}_{i=1}^n$ of $\mathbb{F}_q^n$. Consider $L^\perp = \langle \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_\rho \rangle_{\mathbb{F}_q}$, then $\dim(L) = n - \rho$ and $\pi_{L,L'}(\mathbf{c}_1) = \pi_{L,L'}(\mathbf{c}_2)$. □

Proposition A.43. *Given an (arbitrary) code $C \subset \mathbb{F}_{q^m}^n$ with $\rho < d_R(C)$, every subspace $L \subset \mathbb{F}_q^n$ with $\dim(L) \geq n - \rho$ satisfies that $d_R(C^L) \geq d_R(C) - \rho$. Moreover, there exists a subspace $L \subset \mathbb{F}_q^n$ with $\dim(L) = n - \rho$ such that $d_R(C^L) = d_R(C) - \rho$.*

Proof. With the same notation as in the previous proof, we have that $\mathrm{wt}_{\mathrm{R}}(\pi_{L,L'}(\mathbf{c})) = \dim(\langle\pi_{L,L'}(\mathbf{c})\rangle^*) \geq \dim(\langle\mathbf{c}\rangle^*) - \rho$, and the first statement follows.

Finally, take $\mathbf{c}_1, \mathbf{c}_2$ such that $\mathrm{wt}_{\mathrm{R}}(\mathbf{c}) = d_R(C)$, and write $D = \langle\mathbf{c}\rangle^* = \langle\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s\rangle$, with $\mathbf{v}_i \in \mathbb{F}_q^n$, and extend this to a basis $B = \{\mathbf{v}_i\}_{i=1}^n$ of $\mathbb{F}_q^n$. Consider $L^\perp = \langle\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_\rho\rangle_{\mathbb{F}_q}$ and $L' = \langle\mathbf{v}_{\rho+1}, \mathbf{v}_{\rho+2}, \ldots, \mathbf{v}_n\rangle_{\mathbb{F}_q}$, then $\ker(\pi_{L,L'}) \cap D = L^\perp \otimes \mathbb{F}_{q^m}$, and therefore $\mathrm{wt}_{\mathrm{R}}(\pi_{L,L'}(\mathbf{c})) = \mathrm{wt}_{\mathrm{R}}(\mathbf{c}) - \rho$, and the last statement follows. □

We can extend this to (arbitrary) coding schemes, just by substituting the code C with a coding scheme $\mathcal{P}_{\mathcal{S}} = \{C_{\mathbf{x}}\}_{\mathbf{x}\in\mathcal{S}}$. The proof is the same.

6.4 Computing rank-punctured codes

We conclude the section showing how to compute punctured codes. In the Hamming case, this is obvious, since we only have to project on some of the coordinates. In the rank case, we need to solve some systems of linear equations, which is still an efficient computation.

Proposition A.44. *Given a subspace $L \subset \mathbb{F}_q^n$ and one of its generator matrices A ($L = \mathrm{row}(A)$ and A has full rank [16]), we have that a subspace $L' \subset \mathbb{F}_q^n$ satisfies $\mathbb{F}_q^n = L' \oplus L^\perp$ if, and only if, it has a generator matrix A' such that $A'A^T = I$.*

Proof. First assume that $\mathbb{F}_q^n = L' \oplus L^\perp$ and B is a generator matrix for L'. Take $\mathbf{x}$ such that $\mathbf{x}BA^T = \mathbf{0}$, then $\mathbf{x}B \in L' \cap L^\perp$ and therefore, $\mathbf{x}B = \mathbf{0}$, which implies that $\mathbf{x} = \mathbf{0}$. Hence, BA^T is full rank and there exists an invertible matrix M such that $MBA^T = I$. Taking $A' = MB$ we obtain the desired matrix.

Now assume that L' has a generator matrix A' with $A'A^T = I$. Since $\dim(L') = \dim(L) = n - \dim(L^\perp)$, we need to prove that $L' \cap L^\perp = 0$. Suppose that $\mathbf{x}A' \in L^\perp$, then $\mathbf{x} = \mathbf{x}A'A^T = \mathbf{0}$, and we are done. □

Therefore, to compute subspaces L' with $\mathbb{F}_q^n = L' \oplus L^\perp$, we just need to solve the equations $A\mathbf{a}_i'^T = \mathbf{e}_i^T$, $i = 1, 2, \ldots, \dim(L)$. Different solutions give different spaces.

Note that if A is a generator matrix of $L \subset \mathbb{F}_q^n$ over $\mathbb{F}_q$, then it is a generator matrix of $V = L \otimes \mathbb{F}_{q^m}$ over $\mathbb{F}_{q^m}$.

Lemma A.45. *With the same notation as in the previous proposition, we have that, for every $\mathbf{c} \in \mathbb{F}_{q^m}^n$,*

$$\pi_{L,L'}(\mathbf{c}) = \mathbf{c}A^TA'.$$

And now we give a method to compute the generator matrix of a punctured code C^L, given generator matrices of C and L. The proof is straightforward and follows from the previous lemma.

Proposition A.46. *Let $C \subset \mathbb{F}_{q^m}^n$ be a linear code with generator matrix G, and let $L, L' \subset \mathbb{F}_q^n$ be subspaces with generator matrices A and A', respectively, and such that $A'A^T = I$.*

We have that GA^TA' satisfies that $\mathrm{row}(GA^TA') = C^{L,L'} = C^L$, and thus by deleting linearly dependent rows, we obtain a generator matrix for C^L. Moreover, if L is an information space for C, then GA^TA' is full rank and therefore it is a generator matrix for C^L.

7 Secure network coding

In this section we revisit the description of secure linear network coding in view of the results in the previous sections. Recall from Subsection 2.1 the linear network coding with errors that we are considering, which is the one in [20, 28], and recall from Subsection 2.2 that we assume that the source encodes the original message $\mathbf{x} \in \mathbb{F}_{q^m}^k$ into $\mathbf{c} \in \mathbb{F}_{q^m}^n$ using some coding scheme $\mathcal{P}_{\mathcal{S}} = \{C_{\mathbf{x}}\}_{\mathbf{x} \in \mathcal{S}}$.

As explained in the introduction, we consider an adversary that may compromise the security of the network by doing three things: introducing t erroneous packets on t different links, modifying the transfer matrix A and obtaining information about the original message $\mathbf{x}$ by wiretapping several links.

As in [20, 28], if the receiver obtains the vector $\mathbf{y} = \mathbf{c}A^T + \mathbf{e}$, $t = \mathrm{wt_R}(\mathbf{e})$ and $\rho = n - \mathrm{Rk}(A)$, then we say that t errors and ρ erasures occurred. In Appendix C, we will see how to consider erasures as errors.

7.1 Erasure correction and information leakage revisited

In this subsection we study the problems of erasure correction and information leakage, which are closely related. The amount of leaked information on networks was studied in [20]. We will see how the punctured construction in Section 6 can describe this.

Consider a linear coding scheme built from $C_2 \subsetneq C_1 \subset \mathbb{F}_{q^m}^n$. Denote by S and X the random variables corresponding to the original message and the encoded message by the previous nested coset coding scheme, respectively, and π_I the projection onto the coordinates in $I \subset \mathcal{J}$. It was shown in [12] and [21] that

$$\mathrm{I}(S; \pi_I(X)) = \dim((C_2^\perp)_I / (C_1^\perp)_I) = \dim(C_1^I / C_2^I), \tag{A.16}$$

for every $I \subset \mathcal{J}$, assuming a uniform distribution, where the last equality follows from Lemma A.36, and $\mathrm{I}(X;Y) = H(X) - H(X|Y)$ is the mutual information of the random variables X and Y.

On the other hand, by wiretapping s links in a network, an adversary obtains the variable XB^T, for some matrix $B \in \mathbb{F}_q^{s \times n}$. Assuming uniform distributions, and defining $L = \mathrm{row}(B) \subset \mathbb{F}_q^n$, it is proven in [20, Lemma 7] that

$$\mathrm{I}(S; XB^T) = \dim((C_2^\perp)_L / (C_1^\perp)_L) = \dim(C_1^L / C_2^L), \tag{A.17}$$

where the last equality follows from Lemma A.36.

Therefore, the information leakage is tightly related to the dimension of punctured and shortened codes.

Observe that $\mathrm{I}(S; XB^T) \leq \dim(C_1/C_2)$ and the equality holds if, and only if, L is an information space for C_1, C_2 as in Definition A.40. Remember from Proposition A.42 that if $n - \mathrm{Rk}(B) < d_R(\mathcal{P}_S)$, then $L = \mathrm{row}(B)$ is an information space for $\mathcal{P}_S$. In Appendix A, we show how to efficiently obtain the original message if L is an information space.

Next we give a relation between information leakage and duality, whose philosophy is similar to that of MacWilliams equations, since it means that knowing the information leakage using the code pair $C_2 \subsetneq C_1$ is equivalent to knowing the information leakage using the "dual" code pair $C_1^\perp \subsetneq C_2^\perp$. It is convenient to introduce the definition of access structures:

Definition A.47 ([12]). We define the Hamming access structure of the nested linear code pair $C_2 \subsetneq C_1$ as the collection of the following sets

$$\mathcal{A}(C_1, C_2)_r = \{I \subset \mathcal{J} \mid \dim(C_1^I / C_2^I) = r\},$$

for $0 \leq r \leq \ell = \dim(C_1/C_2)$. Given a set $\mathcal{A} \subset \mathcal{P}(\mathcal{J})$, we define its Hamming dual as $\mathcal{A}^\perp = \{I \subset \mathcal{J} \mid \overline{I} \in \mathcal{A}\}$.

Definition A.48. We define the rank access structure of the nested linear code pair $C_2 \subsetneq C_1$ as the collection of the following linear subspaces of $\mathbb{F}_q^n$

$$\mathcal{B}(C_1, C_2)_r = \{L \subset \mathbb{F}_q^n \mid \dim(C_1^L / C_2^L) = r\},$$

for $0 \leq r \leq \ell = \dim(C_1/C_2)$. Given a set $\mathcal{B} \subset \{L \subset \mathbb{F}_q^n \text{ linear subspace}\}$, we define its rank dual as $\mathcal{B}^\perp = \{L \subset \mathbb{F}_q^n \mid L^\perp \in \mathcal{B}\}$.

We now present the relation with duality, where the Hamming case for $r = 0$ was already proven in [5, Proof of Theorem 1] for the Massey-type scheme [5, Section 3]. The rank case and the general Hamming case are new.

Proposition A.49. *Given a nested linear code pair $C_2 \subsetneq C_1 \subset \mathbb{F}_{q^m}^n$ and $0 \leq r \leq \ell = \dim(C_1/C_2)$, we have that*

$$\mathcal{A}(C_2^\perp, C_1^\perp)_r = \mathcal{A}(C_1, C_2)_{\ell - r}^\perp.$$

Proof. It follows from the following equality, which follows from Lemma A.36,

$$\dim((C_2^{\perp})^I/(C_1^{\perp})^I) + \dim(C_1^{\overline{I}}/C_2^{\overline{I}}) = \ell.$$

Proposition A.50. *Given a nested linear code pair* $C_2 \subsetneq C_1 \subset \mathbb{F}_{q^m}^n$ *and* $0 \leq r \leq \ell = \dim(C_1/C_2)$*, we have that*

$$\mathcal{B}(C_2^{\perp}, C_1^{\perp})_r = \mathcal{B}(C_1, C_2)^{\perp}_{\ell - r}.$$

Proof. Again, it follows from the following equality, which follows from Lemma A.36,

$$\dim((C_2^{\perp})^L/(C_1^{\perp})^L) + \dim(C_1^{L^{\perp}}/C_2^{L^{\perp}}) = \ell.$$

Finally, as consequences of Proposition A.37 and Proposition A.38, we obtain the description of the access structures for MDS and MRD code pairs, respectively. The Hamming case (Corollary A.51) also follows immediately from [12, Section III].

Corollary A.51 ([12, Section III]). *If both* C_1 *and* C_2 *are MDS, then*

$$\dim(C_1^I/C_2^I) = \begin{cases} \ell & , \textit{if } k_1 \leq \#I, \\ \#I - k_2 & , \textit{if } k_2 \leq \#I \leq k_1, \\ 0 & , \textit{if } \#I \leq k_2, \end{cases}$$

for every $I \subset \mathcal{J}$.

Corollary A.52. *If both* C_1 *and* C_2 *are MRD, then*

$$\dim(C_1^L/C_2^L) = \begin{cases} \ell & , \textit{if } k_1 \leq \dim(L), \\ \dim(L) - k_2 & , \textit{if } k_2 \leq \dim(L) \leq k_1, \\ 0 & , \textit{if } \dim(L) \leq k_2, \end{cases}$$

for every linear subspace $L \subset \mathbb{F}_q^n$.

In general, we can compute the information leaked in many cases, but if the involved codes are not MDS (respectively, MRD), then there is always a collection of sets (respectively, subspaces) for which we do not completely know the information leaked. We first establish this fact for the rank case, which follows from Proposition A.38, and give an example in the Hamming case:

Proposition A.53. *Let $C_2 \subsetneq C_1 \subset \mathbb{F}_{q^m}^n$ be a nested linear code pair such that $k_i = \dim(C_i)$, $i = 1, 2$, $\ell = k_1 - k_2$, C_1 is r_1-MRD and $C_2^\perp$ is r_2-MRD, or equivalently, $d_R(C_1^\perp) \geq k_1 - r_1 + 2$ and $d_R(C_2) \geq n - k_2 - r_2 + 2$. If $L \subset \mathbb{F}_q^n$ is a subspace such that $k_2 + r_2 - 1 \leq \dim(L) \leq k_1 - r_1 + 1$, then $\dim(C_1^L / C_2^L) = \dim(L) - k_2$, which only depends on $\dim(L)$ and not on the space L.*

If moreover, $k_2 + r_2 - 1 < k_1 - r_1 + 1$, and taking $s_1 = n - k_1 - d(C_1) + 1$ and $s_2 = k_2 - d(C_2^\perp) + 1$, then for every subspace $L \subset \mathbb{F}_q^n$, it holds that $\dim(C_1^L / C_2^L)$ is

$$\begin{array}{ll} = \ell & , \textit{if } k_1 + s_1 \leq \dim(L), \\ \geq \ell - r_1 + 1 & , \textit{if } k_1 - r_1 + 1 < \dim(L) < k_1 + s_1, \\ = \dim(L) - k_2 & , \textit{if } k_2 + r_2 - 1 \leq \dim(L) \leq k_1 - r_1 + 1, \\ \leq r_2 - 1 & , \textit{if } k_2 - s_2 < \dim(L) < k_2 + r_2 - 1, \\ = 0 & , \textit{if } \dim(L) \leq k_2 - s_2. \end{array}$$

Example A.54. If C_1 and C_2 are algebraic geometric codes constructed from a function field of genus g [32], then we have the Goppa bound [32, Theorem 4.3]: $d_{H,1}(C_i) \geq n - \dim(C_i) + 1 - g$ and $d_{H,1}(C_i^\perp) \geq \dim(C_i) + 1 - g$. It follows from Proposition A.37 that, for the code pair $C_2 \subsetneq C_1$,

$$\dim(C_1^I / C_2^I) \begin{cases} = \ell & , \text{ if } k_1 + g \leq \#I, \\ \geq \ell - g & , \text{ if } k_1 - g < \#I < k_1 + g, \\ = \#I - k_2 & , \text{ if } k_2 + g \leq \#I \leq k_1 - g, \\ \leq g & , \text{ if } k_2 - g < \#I < k_2 + g, \\ = 0 & , \text{ if } \#I \leq k_2 - g. \end{cases}$$

7.2 Error and erasure correction revisited

In this subsection we see how the rank-puncturing can describe error and erasure correction in networks. We will follow a slightly different approach than that of [20, 28].

We will treat the coherent case, that is, the case in which the matrix A is known by the receiver. For simplicity, we will consider the case of one code $C \subset \mathbb{F}_{q^m}^n$, which may be non-linear. At the end we will show how to adapt the results to arbitrary coding schemes. Observe that [20, Theorem 4] only deals with linear (meaning $\mathbb{F}_{q^m}$-linear, as in the rest of the paper) coding schemes.

As we saw in the previous subsection (see also Appendix A), if the sink node receives $\mathbf{y} = \mathbf{c}A^T$ and the number of erasures is less than $d_R(C)$, we can perform erasure correction. For that, we can take a submatrix $\widetilde{A}$ of A which is a generator matrix of $L = \text{row}(A)$, since the other rows in A are redundant. All choices of $\widetilde{A}$ will give the same unique solution.

When there are errors, we would also like to take a submatrix as before and the corresponding subvector of $\mathbf{y}$. However, it is not clear that the decoder in [20, 28] for A and for $\widetilde{A}$ will behave in the same way. We now propose a slightly different approach.

Fix the positive integer N and the matrix $A \in \mathbb{F}_q^{N\times n}$, which are assumed to be known by the receiver.

Definition A.55 ([28, Equations (9), (12)]). For each $\mathbf{c} \in \mathbb{F}_{q^m}^n$ and $\mathbf{y} \in \mathbb{F}_{q^m}^N$, we define the discrepancy between them as

$$\Delta_A(\mathbf{c},\mathbf{y}) = \min\{r \mid \exists \mathbf{z} \in \mathbb{F}_{q^m}^r, D \in \mathbb{F}_q^{N\times r} \\ \text{with } \mathbf{y} = \mathbf{c}A^T + \mathbf{z}D^T\} = \mathrm{wt}_{\mathrm{R}}(\mathbf{y} - \mathbf{c}A^T).$$

Fix nonnegative integers ρ, t, with $\mathrm{Rk}(A) \geq n - \rho$. We will assume that, if $\mathbf{c} \in \mathbb{F}_{q^m}^n$ is sent and $\mathbf{y} \in \mathbb{F}_{q^m}^N$ is received, then $\Delta_A(\mathbf{c},\mathbf{y}) \leq t$, or equivalently, that $\mathbf{y} = \mathbf{c}A^T + \mathbf{e}$, with $\mathrm{wt}_{\mathrm{R}}(\mathbf{e}) \leq t$. Define $L = \mathrm{row}(A)$. We will denote $\widetilde{A} \subset A$ if $\widetilde{A}$ is a submatrix of A that is a generator matrix of L.

Next we recall the decoder in [28] and present a slightly different one.

Definition A.56 ([28, Equation (10)]). We define the decoder

$$\overline{\mathbf{c}} = \mathrm{argmin}_{\mathbf{c}\in C}\Delta_A(\mathbf{c},\mathbf{y}).$$

Definition A.57. For each $\widetilde{A} \subset A$, we define the decoder:

$$\widehat{\mathbf{c}} = \mathrm{argmin}_{\mathbf{c}\in C}\Delta_{\widetilde{A}}(\mathbf{c},\widetilde{\mathbf{y}}),$$

where $\widetilde{\mathbf{y}}$ is the vector obtained from $\mathbf{y}$ taking the coordinates in the same positions as the rows of $\widetilde{A}$.

We will say that one of the previous decoders is infallible [28, Section III.A] if $\widehat{\mathbf{c}} = \mathbf{c}$ (or $\overline{\mathbf{c}} = \mathbf{c}$), when $\mathbf{c}$ is the sent message, for every $\mathbf{c} \in C$.

In [20, 28], sufficient and necessary conditions for the decoder corresponding to A being infallible are given. We will now state that the same conditions are valid for the decoders corresponding to all the submatrices $\widetilde{A}$. In particular, all of them give the correct (and thus, the same) answer.

The main difference is that now the proof only relies on Proposition A.42 and Proposition A.43, where we do not need the machinery developed in [20, 28], in total analogy with the Hamming case, as proven in [16, Theorem 1.5.1], and for the decoding, we do not need all rows in A. Moreover, although it is not difficult to adapt the proof in [20, Theorem 4] for $\mathbb{F}_q$-linear coding schemes, our proof works for any (arbitrary) scheme.

Theorem A.9. *Given an (arbitrary) code $C \subset \mathbb{F}_{q^m}^n$, if $d_R(C) > 2t + \rho$, then the decoders in Definition A.57 are infallible for every $\widetilde{A} \subset A$, and in particular, they all give the same answer. If $d_R(C) \leq 2t + \rho$, then there exists a matrix $A \in \mathbb{F}_q^{N\times n}$ such that for every $\widetilde{A} \subset A$, the decoder in Definition A.57 is not infallible.*

Proof. First, assume $d_R(C) > 2t + \rho$ and fix a matrix $A \in \mathbb{F}_q^{N \times n}$ and $\widetilde{A} \subset A$. Assume also that the sent message is $\mathbf{c} \in C$ and we receive $\mathbf{y} = \mathbf{c}A^T + \mathbf{e}$, with $\mathrm{wt_R}(\mathbf{e}) \leq t$. Define $\widetilde{\mathbf{y}}$ and $\widetilde{\mathbf{e}}$ as the vectors obtained from $\mathbf{y}$ and $\mathbf{e}$, respectively, taking the coordinates in the same positions as the rows in $\widetilde{A}$. Therefore, $\widetilde{\mathbf{y}} = \mathbf{c}\widetilde{A}^T + \widetilde{\mathbf{e}}$.

We have that $\mathrm{Rk}(\widetilde{A}) = \mathrm{Rk}(A)$ and $\mathrm{wt_R}(\widetilde{\mathbf{e}}) \leq \mathrm{wt_R}(\mathbf{e}) \leq t$, and on the other hand,

$$\Delta_{\widetilde{A}}(\mathbf{c}, \widetilde{\mathbf{y}}) = \mathrm{wt_R}(\widetilde{\mathbf{e}}) = \mathrm{wt_R}(\widetilde{\mathbf{e}}A'),$$

where $A'\widetilde{A}^T = I$.

Now, $\mathbf{c}\widetilde{A}^T A' = \pi_{L,L'}(\mathbf{c})$ by Lemma A.45. Since $d_R(C^L) > 2t$ by Proposition A.43, and since L is an information space for C by Proposition A.42, $\mathbf{c}$ is the only vector in C with $d_R(\widetilde{\mathbf{y}}A', \pi_{L,L'}(\mathbf{c})) \leq t$, and we are done.

Finally, if $d_R(C) \leq 2t + \rho$, then take A such that $\dim(L) = n - \rho$ and $d_R(C^L) = d_R(C) - \rho \leq 2t$, which exists by Proposition A.43. Then, take $\widetilde{A} \subset A$ and $\mathbf{c}, \mathbf{c}' \in C$ such that $d_R(\pi_{L,L'}(\mathbf{c}), \pi_{L,L'}(\mathbf{c}')) = d_R(\mathbf{c}\widetilde{A}^T, \mathbf{c}'\widetilde{A}^T) \leq 2t$. There exists $\mathbf{e}, \mathbf{e}' \in \mathbb{F}_{q^m}^N$ such that $\mathrm{wt_R}(\mathbf{e}), \mathrm{wt_R}(\mathbf{e}') \leq t$ and $\mathbf{c}\widetilde{A}^T + \widetilde{\mathbf{e}} = \mathbf{c}'\widetilde{A}^T + \widetilde{\mathbf{e}}'$, and hence the decoder associated with $\widetilde{A}$ gives both $\mathbf{c}$ and $\mathbf{c}'$ as solutions. □

To adapt this to (arbitrary) coding schemes, we just need to replace distances between vectors by distances between cosets

$$d_R(C_{\mathbf{x}}, C_{\mathbf{x}'}) = \min\{d_R(\mathbf{c}, \mathbf{c}') \mid \mathbf{c} \in C_{\mathbf{x}}, \mathbf{c}' \in C_{\mathbf{x}'}\},$$

and the choice of vectors in C by the choice of representatives of a coset $C_{\mathbf{x}}$ in $\mathcal{P}_{\mathcal{S}}$.

A The role of C_1^L/C_2^L in information leakage

In this appendix we explain the role of C_1^L/C_2^L in information leakage beyond the expression (A.17). Let the notation be as in Subsection 7.1.

If the adversary knows the matrix B, then he or she may obtain $\pi_{L,L'}(\mathbf{c}) = \mathbf{c}\widetilde{B}^T\widetilde{B}'$, where $\widetilde{B}$ is a submatrix of B that is a generator matrix of L, and $\widetilde{B}'\widetilde{B}^T = I$. Assuming uniform distributions, it can be shown that the adversary still obtains the same amount of information from $\pi_{L,L'}(\mathbf{c})$:

$$\mathrm{I}(S; XB^T) = \mathrm{I}(S; \pi_{L,L'}(X)) = \dim(C_1^L/C_2^L). \tag{A.18}$$

Actually, we can effectively compute the set of possible sent messages, regardless of the distributions used. If $\psi : \mathbb{F}_{q^m}^{\ell} \longrightarrow W$ is the map in Definition A.3, we can see both ψ and $\pi_{L,L'}$ as maps

$$\mathbb{F}_{q^m}^{\ell} \xrightarrow{\psi} C_1/C_2 \xrightarrow{\pi_{L,L'}} C_1^L/C_2^L,$$

where ψ is an isomorphism and $\pi_{L,L'}$ is surjective. Therefore, knowing $\mathbf{c}' = \pi_{L,L'}(\mathbf{c} + C_2) = \pi_{L,L'}(\psi(\mathbf{x}))$, where $\mathbf{c} = \psi(\mathbf{x})$, we can obtain the set of possible sent messages, which is

$$(\pi_{L,L'} \circ \psi)^{-1}(\mathbf{c}') = \mathbf{x} + \ker(\pi_{L,L'} \circ \psi),$$

regardless of the distribution, and in the case of uniform distributions, dim $(\ker(\pi_{L,L'} \circ\psi)) = \ell - \dim(C_1^L/C_2^L) = H(S) - I(S; \pi_{L,L'}(X)) = H(S|\pi_{L,L'}(X))$.

Moreover, if we know B, we can obtain all vectors in $\mathbf{x} + \ker(\pi_{L,L'} \circ \psi)$ by performing matrix multiplications and solving systems of linear equations.

Assume that G_1, G_2, G' are generator matrices of C_1, C_2, W, respectively, where $C_1 = C_2 \oplus W$, and the first rows of G_1 are the rows in G_2, and the last rows are the rows in G'. Then, for a message $\mathbf{x} \in \mathbb{F}_{q^m}^{\ell}$, the encoding consists in generating uniformly at random a vector $\mathbf{x}_2 \in \mathbb{F}_{q^m}^{k_2}$ and defining $\mathbf{c} = \mathbf{x}_2 G_2 + \mathbf{x}G' = (\mathbf{x}_2, \mathbf{x})G_1$. Therefore, the projections onto the last ℓ coordinates of the solutions of the system $\pi_{L,L'}(\mathbf{c}) = \widetilde{\mathbf{x}}(G_1 \widetilde{B}^T \widetilde{B}')$ will be all the vectors in $\mathbf{x} + \ker(\pi_{L,L'} \circ \psi)$.

If L is an information space for $C_2 \subsetneq C_1$, i.e., $\dim(C_1^L/C_2^L) = \ell$, then all solutions of the previous system coincide in the last ℓ coordinates, which constitute the original message $\mathbf{x} \in \mathbb{F}_{q^m}^{\ell}$.

B Alternative proof of the duality theorem

We will now give a different proof of the duality Theorem A.8 (proven in [7]) that follows from Proposition A.50. Note that a theorem analogous to Wei's duality theorem [33, Theorem 3] has not been given for relative generalized Hamming weights, nor for the rank case. However, Proposition A.50 and its Hamming version work for any nested linear code pair.

We will need the following lemma:

Lemma A.58 ([20, Lemma 4]). *For any linear code $C \subset \mathbb{F}_{q^m}^n$ and any $1 \leq r \leq k$, we have that*

$$d_{R,r}(C) = \min\{j \mid \max\{\dim(C_L) \mid \dim(L) = j\} = r\}.$$

The proof is as follows. By monotonicity and cardinality, it is enough to prove that both sets on the right-hand side are disjoint. Assume that they are not disjoint, then there exist i, j, s such that $d_i = j$ and $d_s^{\perp} = n + 1 - j$. By the previous lemma, the first equality implies that

$$\max\{\dim(C_L) \mid \dim(L) = j\} = i.$$

Now take $C_1 = C$ and $C_2 = 0$ in Proposition A.50. From the fact that $\mathcal{B}(\mathbb{F}_{q^m}^n, C^{\perp})_r = \mathcal{B}(C, 0)_{\ell-r}^{\perp}$ and the previous lemma, the second equality implies that

$$\max\{\dim(C_L) \mid \dim(L) = j - 1\} = s + k - n - 1 + j.$$

Again by the previous lemma, $i > s + k - n - 1 + j$. Now interchanging the role of C and $C^{\perp}$, which also interchanges the roles of i, s; the roles of $j, n + 1 - j$; and the roles of $k, n - k$; we have that $i \leq s + k - n - 1 + j$, which is absurd.

C Seeing errors as erasures

We will show now that erasure correction is equivalent to error correction if the rank support of the error vector is known. This is analogous to the fact that usual erasure correction is equivalent to usual error correction where the positions of the errors (the Hamming support of the error vector) are known. This is a basic fact used in many decoding algorithms for the Hamming distance, which now we hope can be translated to the rank case.

Proposition A.59. *Assume that* $\mathbf{c} \in C$ *and* $\mathbf{y} = \mathbf{c} + \mathbf{e}$, *where* $\mathrm{wt_R}(\mathbf{e}) = t < d_R(C)$ *and* $L = G(\mathbf{e})$. *Then,* $\mathbf{c}$ *is the only vector* $\mathbf{c}' \in C$ *such that* $\mathrm{wt_R}(\mathbf{y} - \mathbf{c}') < d_R(C)$ *and* $L = G(\mathbf{y} - \mathbf{c}')$.

Moreover, if A *is a generator matrix of* $L^{\perp}$, *then* $\mathbf{c}$ *is the unique solution in* C *of the system of equations* $\mathbf{y}A^T = \mathbf{x}A^T$, *where* $\mathbf{x}$ *is the unknown vector.*

Proof. Assume that $\mathbf{y} = \mathbf{c} + \mathbf{e} = \mathbf{c}' + \mathbf{e}'$, where $\mathbf{c}' \in C$ and $G(\mathbf{e}) = G(\mathbf{e}')$. Then $\mathbf{y}A^T = \mathbf{c}A^T = \mathbf{c}'A^T$. Since $\mathrm{Rk}(A) = n - t$ and $t < d_R(C)$, it follows from the previous theorem that $\mathbf{c} = \mathbf{c}'$. □

Acknowledgement

The author wishes to thank Ryutaroh Matsumoto, Relinde Jurrius and Ruud Pellikaan for important comments on their work, during the stay of the last author at Aalborg University, and Olav Geil and Diego Ruano for fruitful discussions and careful reading of the manuscript, including the fact that the duality theorem follows from Proposition A.50. The author also wishes to thank the editor and anonymous reviewers for their very helpful comments. Finally, the author also gratefully acknowledges the support from The Danish Council for Independent Research (Grant No. DFF-4002-00367).

References

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inform. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[2] A. Barra and H. Gluesing-Luerssen, "MacWilliams extension theorems and the local-global property for codes over Frobenius rings," *J. Pure Appl. Algebra*, vol. 219, no. 4, pp. 703–728, 2015.

[3] T. P. Berger, "Isometries for rank distance and permutation group of Gabidulin codes," *IEEE Trans. Inform. Theory*, vol. 49, no. 11, pp. 3016–3019, 2003.

[4] N. Cai and R. W. Yeung, "Network coding and error correction," *Proc. 2002 IEEE Inform. Theory Workshop*, Oct. 2002, pp. 119–122.

[5] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan, "Secure computation from random error correcting codes," in *Advances in cryptology* (Lecture Notes in Comput. Science) Springer, Berlin, 2007, vol. 4515, pp. 291–310.

[6] P. Delsarte, "On subfield subcodes of modified reed-solomon codes (corresp.)," *IEEE Trans. Inform. Theory*, vol. 21, no. 5, pp. 575–576, 1975.

[7] J. Ducoat, "Generalized rank weights: A duality statement," in *Topics in Finite Fields*, ser. Comtemporary Mathematics, G. L. M. G. Kyureghyan and A. Pott, Eds. American Mathematical Society, 2015, vol. 632, pp. 114–123.

[8] J. Ducoat and F. Oggier, "Rank weight hierarchy of some classes of cyclic codes," in *Proc. 2014 IEEE Inform. Theory Workshop*, pp. 142–146, 2014.

[9] I. M. Duursma and S. Park, "Coset bounds for algebraic geometric codes," *Finite Fields Appl.*, vol. 16, no. 1, pp. 36–55, 2010.

[10] G. D. Forney Jr., "Dimension/length profiles and trellis complexity of linear block codes," *IEEE Trans. Inform. Theory*, vol. 40, no. 6, pp. 1741–1752, 1994.

[11] E. Gabidulin, "Theory of codes with maximum rank distance," *Problems Inform. Transmission*, vol. 21, 1985.

[12] O. Geil, S. Martin, R. Matsumoto, D. Ruano, and Y. Luo, "Relative generalized hamming weights of one-point algebraic geometric codes," *IEEE Trans. Inform. Theory*, vol. 60, no. 10, pp. 5938–5949, 2014.

[13] M. Giorgetti and A. Previtali, "Galois invariance, trace codes and subfield subcodes," *Finite Fields Appl.*, vol. 16, no. 2, pp. 96–99, 2010.

[14] T. Helleseth, T. Kløve, V. I. Levenshtein, and Ø. Ytrehus, "Bounds on the minimum support weights," *IEEE Trans. Inform. Theory*, vol. 41, no. 2, pp. 432–440, 1995.

[15] T. Ho, M. Medard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inform. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct 2006.

[16] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.

[17] R. Jurrius and R. Pellikaan, "On defining generalized rank weights," *Advances in Mathematics of Communications*, vol. 11, no. 1, pp. 225–235, 2017.

[18] R. Kötter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inform. Theory*, vol. 54, no. 8, pp. 3579–3591, 2008.

[19] R. Kötter and M. Medard, "An algebraic approach to network coding," *IEEE/ACM Trans. Networking*, vol. 11, no. 5, pp. 782–795, Oct 2003.

[20] J. Kurihara, R. Matsumoto, and T. Uyematsu, "Relative generalized rank weight of linear codes and its applications to network coding," *IEEE Trans. Inform. Theory*, vol. 61, no. 7, pp. 3912–3936, July 2015.

[21] J. Kurihara, T. Uyematsu, and R. Matsumoto, "Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hamming weight," *IEICE Transactions*, vol. E95-A, no. 11, pp. 2067–2075, 2012.

[22] S.-Y. Li, R. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inform. Theory*, vol. 49, no. 2, pp. 371–381, Feb 2003.

[23] P. Loidreau, "Properties of codes in rank metric," in *Proc. 11th International Workshop Algebraic Comb. Coding Theory, Pamporovo, Bulgaria*, Jun 2008, pp. 192–198.

[24] Y. Luo, C. Mitrpant, A. J. H. Vinck, and K. Chen, "Some new characters on the wire-tap channel of type II." *IEEE Trans. Inform. Theory*, vol. 51, no. 3, pp. 1222–1229, 2005.

[25] F. E. Oggier and A. Sboui, "On the existence of generalized rank weights," in *Proc. International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, October 28-31, 2012*, 2012, pp. 406–410.

[26] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," in *Advances in Cryptology: EUROCRYPT 84*, ser. Lecture Notes in Comput. Sci. Springer Berlin Heidelberg, 1985, vol. 209, pp. 33–50.

[27] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[28] D. Silva and F. R. Kschischang, “On metrics for error correction in network coding,” *IEEE Trans. Inform. Theory*, vol. 55, no. 12, pp. 5479–5490, 2009.

[29] ——, “Universal secure network coding via rank-metric codes,” *IEEE Trans. Inform. Theory*, pp. 1124–1135, 2011.

[30] H. Stichtenoth, “On the dimension of subfield subcodes,” *IEEE Trans. Inform. Theory*, vol. 36, no. 1, pp. 90–93, Jan 1990.

[31] ——, *Algebraic function fields and codes*, ser. Graduate Texts in Mathematics. Springer-Verlag Berlin Heidelberg, 2009, vol. 254.

[32] M. A. Tsfasman and S. G. Vlăduţ, “Geometric approach to higher weights,” *IEEE Trans. Inform. Theory*, vol. 41, no. 6, part 1, pp. 1564–1588, 1995, special issue on algebraic geometry codes.

[33] V. K. Wei, “Generalized Hamming weights for linear codes,” *IEEE Trans. Inform. Theory*, vol. 37, no. 5, pp. 1412–1418, 1991.

[34] S. Yang, R. W. Yeung, and Z. Zhang, “Characterization of error correction and detection in a general transmission system,” in *Proc. 2008 IEEE International Symposium on Information Theory (ISIT)*, Toronto, Canada, July 6-11 2008, pp. 812–816.

[35] ——, “Weight properties of network codes,” *European Transactions on Telecommunications*, vol. 19, no. 4, pp. 371 – 383, 2008, invited paper.

[36] R. Zamir, S. Shamai, and U. Erez, “Nested linear/lattice codes for structured multiterminal binning,” *IEEE Trans. Inform. Theory*, vol. 48, no. 6, pp. 1250–1276, Jun 2002.

[37] Z. Zhuang, Y. Luo, and B. Dai, “Code constructions and existence bounds for relative generalized Hamming weight,” *Designs, Codes Cryptography*, vol. 69, no. 3, pp. 275–297, 2013.

[38] Z. Zhuang, Y. Luo, A. H. Vinck, and B. Dai, “Some new bounds on relative generalized Hamming weight,” in *Proc. IEEE 13th International Conference on Communication Technology (ICCT), 2011*. IEEE, 2011, pp. 971–974.

Paper B

Generalized rank weights of reducible codes, optimal cases and related properties

Umberto Martínez-Peñas[1]

The paper has been accepted for publication in the
IEEE Transactions on Information Theory, 13 pages,
and presented at the
IEEE International Symposium on Information Theory, Barcelona, Spain,
July 2016.

[1] Department of Mathematical Sciences, Aalborg University, Aalborg 9220, Denmark

Abstract

Reducible codes for the rank metric were introduced for cryptographic purposes. They have fast encoding and decoding algorithms, include maximum rank distance (MRD) codes and can correct many rank errors beyond half of their minimum rank distance, which makes them suitable for error-correction in network coding. In this paper, we study their security behaviour against information leakage on networks when applied as coset coding schemes, giving the following main results: 1) we give lower and upper bounds on their generalized rank weights (GRWs), which measure worst-case information leakage to the wire-tapper, 2) we find new parameters for which these codes are MRD (meaning that their first GRW is optimal), and use the previous bounds to estimate their higher GRWs, 3) we show that all linear (over the extension field) codes whose GRWs are all optimal for fixed packet and code sizes but varying length are reducible codes up to rank equivalence, and 4) we show that the information leaked to a wire-tapper when using reducible codes is often much less than the worst case given by their (optimal in some cases) GRWs. We conclude with some secondary related properties: Conditions to be rank equivalent to cartesian products of linear codes, conditions to be rank degenerate, duality properties and MRD ranks.

Keywords: Generalized rank weight, rank-metric codes, rank distance, rank equivalent codes, reducible codes, secure network coding.

1 Introduction

Linear network coding was first studied in [1, 14], further formalized in [12], and provides higher throughput than storing and forwarding messages on the network. Two of the *main problems* in this context are error and erasure correction, and security against information leakage to a wire-tapper, which were first studied in [3] and [4], respectively.

Rank-metric codes were found to be universally suitable (meaning independently of the underlying network code) for error and erasure correction in linear network coding in [22], used as forward error-correcting codes, and they were found to be universally suitable against information leakage in [23], used in the form of coset coding. Both constructions can be treated separately and applied together in a concatenated way (see [23, Sec. VII-B]).

On the security side, generalized rank weights (GRWs) of codes that are linear over the extension field were introduced in [13, 18] to measure the worst-case information leakage for a given number of wire-tapped links. Later, GRWs were extended in [21] and [17] to codes that are linear over the base field, where they are called Delsarte generalized weights and generalized matrix weights, respectively. We will use the term GRWs for the latter parameters, which were also found to measure the worst-case information leakage for codes that are linear over the base field [17, Th. 3].

Gabidulin codes [8] constitute a family of maximum rank distance (MRD) codes that cover all cases when the number of outgoing links n is not larger than the packet length m, and all of their GRWs are optimal (meaning largest possible).

Cartesian products of these codes are proposed in [23, Sec. VII.C] for the case $n > m$ both for error correction and security against information leakage. A generalization of these codes, called reducible codes, were introduced earlier in [9] as an alternative to Gabidulin codes [8] to improve the security of rank-based public key cryptosystems [10]. On the error correction side, it was shown in [9] that reducible codes have fast encoding and rank error-correcting algorithms, their minimum rank distance is not worse than that of cartesian products of codes [23, Sec. VII.C], being actually MRD in some cases, and they can correct many rank errors beyond half of their minimum rank distance (even in the MRD cases). Therefore they seem to be the best known codes for error correction in linear network coding when $n > m$.

However, on the security side, only the existence of codes with optimal first GRW (MRD codes) has been studied in the case $n > m$ [17, Sec. IV-B], but no bounds nor estimates of higher GRWs of rank-metric codes or other properties related to their worst-case information leakage are known when $n > m$, except for cyclic codes with minimal GRWs [7].

In this paper, we study the security provided by reducible codes in linear network coding when used for coset coding as in [23] by studying their GRWs and showing their optimality in several cases. In particular, we study for the first time the GRWs of a concrete family of rank-metric codes with $n > m$, which moreover include MRD codes for several parameters.

1.1 Main contributions

Our main contributions are the following:

1. We give lower and upper bounds on GRWs of reducible codes, and exact values for cartesian products, giving a first step in the open problem of estimating or bounding the GRWs of a family of rank-metric codes for $n > m$.

2. We give new families of parameters for which reducible codes are MRD (some were given in [9]), meaning that their first GRW is optimal and thus they are optimal regarding zero information leakage among all linear (over the extension or the base field) codes, by [17, Th. 3]. Using the estimates and exact values of GRWs of these codes in the previous item, we also give a first step in the open problem of finding the GRWs of a family of MRD codes for $n > m$.

3. We show that all linear (over the extension field) codes whose GRWs are all optimal for fixed packet and code sizes, but varying length, lie

in the family of reducible codes from the previous item, up to rank equivalence.

4. Finally, we show that information leakage when using reducible codes is often much less than the worst case given by their GRWs. In particular, they often provide strictly higher security than the known security provided by other MRD codes [17, Sec. IV-B].

1.2 Organization of the paper

After some preliminaries in Section II, the paper is organized as follows: In Section III, we give lower and upper bounds on the GRWs of reducible codes, extending the lower bound on the minimum rank distance given in [9], and see that the given upper bound on the minimum rank distance can be reached by some reduction. In Section IV, we obtain new parameters for which reducible codes are MRD (or close to MRD) and with MRD components, and obtain explicit estimates on their GRWs, including those MRD codes found in [9] and considered for secure network coding in [23]. In Section V, we obtain all linear codes whose GRWs are all optimal, for all fixed packet and code sizes, up to rank equivalence. In Section VI, we see that the actual information leakage occuring when using reducible codes is often much less than the worst case given by their GRWs, providing higher security than other known MRD codes. Finally, in Section VII, we study secondary but related properties: Conditions to be rank equivalent to cartesian products and conditions to be rank degenerate. We study their duality properties and MRD ranks. Finally, we propose alternative constructions to the classical $(\mathbf{u}, \mathbf{u}+\mathbf{v})$ construction.

2 Definitions and preliminaries

2.1 Rank-metric codes

Fix a prime power q and positive integers m and n, and let $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$ denote the finite fields with q and q^m elements, respectively. We may identify vectors in $\mathbb{F}_{q^m}^n$ with $m \times n$ matrices over $\mathbb{F}_q$: Fix a basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. If $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in \mathbb{F}_{q^m}^n$, $c_j = \sum_{i=1}^m \alpha_i c_{i,j}$, and $c_{i,j} \in \mathbb{F}_q$, for $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$, we may identify $\mathbf{c}$ with the matrix

$$M(\mathbf{c}) = \left(c_{i,j}\right)_{1 \leq j \leq n}^{1 \leq i \leq m}. \tag{B.1}$$

The rank weight of a vector $\mathbf{c} \in \mathbb{F}_{q^m}^n$ is defined as the rank of the matrix $M(\mathbf{c})$ and denoted by $\mathrm{wt}_{\mathrm{R}}(\mathbf{c})$. In this paper, a code is a subset of $\mathbb{F}_{q^m}^n$. The term *rank-metric code* is used for codes with the rank metric.

2.2 Universal secure linear network coding

We consider a network with several sources and several sinks as in [1, 14]. In this model, a given source wants to transmit k packets in $\mathbb{F}_q^m$ to one or several sink nodes, and does so by encoding them into a vector, $\mathbf{c} \in \mathbb{F}_{q^m}^n$, which can be seen as n packets in $\mathbb{F}_q^m$ by (B.1), being n the number of outgoing links from the source.

In *linear network coding*, as considered in [1] and [14], the nodes in the network forward linear combinations of received packets (see [12, Definition 1]), achieving higher throughput than just storing and forwarding. This means that a given sink is assumed to receive the vector

$$\mathbf{y} = \mathbf{c}A^T \in \mathbb{F}_{q^m}^N,$$

for some matrix $A \in \mathbb{F}_q^{N \times n}$, called a transfer matrix.

Two of the *main problems* in linear network coding considered in the literature are the following:

1. Error correction [3]: Several packets are injected on some links in the network, hence the sink receives

$$\mathbf{y} = \mathbf{c}A^T + \mathbf{e} \in \mathbb{F}_{q^m}^N,$$

for an error vector $\mathbf{e} \in \mathbb{F}_{q^m}^N$.

2. Information leakage [4]: A wire-tapper listens to $\mu > 0$ links in the network, obtaining

$$\mathbf{z} = \mathbf{c}B^T \in \mathbb{F}_{q^m}^\mu,$$

for a matrix $B \in \mathbb{F}_q^{\mu \times n}$.

In [22], it is proven that rank-metric codes are suitable for error correction when used as forward error-correcting codes, and in [23], it is proven that they are also suitable to protect messages from information leakage when used as coset coding schemes, which were introduced in [25] and [19]. Both coding techniques can be treated separately and applied together in a concatenated way (see [23, Sec. VII-B]).

Moreover, rank-metric codes are *universal* [23] in the sense that they correct a given number of errors and erasures, and protect against a given number of wire-tapped links, independently of the matrices A and B, respectively.

We consider the particular coding schemes in [23, Sec. V-B] with uniform distributions:

Definition B.1 ([23]). Given an $\mathbb{F}_{q^m}$-linear code $C \subsetneq \mathbb{F}_{q^m}^n$ with generator matrix $G \in \mathbb{F}_{q^m}^{k \times n}$, we define its coset coding scheme as follows: For $\mathbf{x} \in \mathbb{F}_{q^m}^k$, its coset encoding is a vector $\mathbf{c} \in \mathbb{F}_{q^m}^n$ chosen uniformly at random and such that $\mathbf{x} = \mathbf{c}G^T$.

This type of encoding has been recently extended to $\mathbb{F}_q$-linear codes in [17, Sec. II-D].

In this paper we will focus on rank-metric codes used for security against information leakage in the form of coset coding.

2.3 Generalized rank weights and information leakage

The information leaked to a wire-tapping adversary when using coset coding schemes was obtained in [23, Lemma 6], then generalized in [13, Lemma 7] to $\mathbb{F}_{q^m}$-linear nested coset coding schemes [26], and in [17, Prop. 4] to $\mathbb{F}_q$-linear coset coding schemes.

We need the concept of Galois closed spaces [24]:

Definition B.2 ([24]). Denote $[i] = q^i$ for an integer $i \geq 0$. If $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is $\mathbb{F}_{q^m}$-linear, we denote

$$\mathcal{C}^{[i]} = \{(c_1^{[i]}, c_2^{[i]}, \ldots, c_n^{[i]}) \mid (c_1, c_2, \ldots, c_n) \in \mathcal{C}\},$$

we define the Galois closure of $\mathcal{C}$ as $\mathcal{C}^* = \sum_{i=0}^{m-1} \mathcal{C}^{[i]}$, and we say that it is Galois closed if $\mathcal{C} = \mathcal{C}^*$.

The next lemma is [23, Lemma 6]. Throughout the paper, $I(X;Y)$ denotes the mutual information of the random variables X and Y, taking logarithms with base q^m.

Lemma B.3 ([23]). *Let S be the uniform random variable in $\mathbb{F}_{q^m}^k$, let X be its coset encoding using an $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ according to Definition B.1, and denote $W = XB^T$, where $B \in \mathbb{F}_q^{\mu \times n}$. Then*

$$I(S;W) = \dim(\mathcal{C} \cap \mathcal{V}), \tag{B.2}$$

where $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$ is the $\mathbb{F}_{q^m}$-linear vector space with generator matrix B.

Since Galois closed spaces in $\mathbb{F}_{q^m}^n$ are those $\mathbb{F}_{q^m}$-linear spaces with a generator matrix over $\mathbb{F}_q$ [24, Lemma 1], the previous lemma motivates the definition of generalized rank weights, introduced independently in [18] for $n \leq m$, and in [13, Def. 2] for the general case:

Definition B.4 ([13]). Given an $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension k, we define its r-th generalized rank weight (GRW), for $1 \leq r \leq k$, as

$$\begin{aligned} d_{R,r}(\mathcal{C}) = \min\{ \dim(\mathcal{V}) \mid \mathcal{V} \subseteq \mathbb{F}_{q^m}^n, \mathbb{F}_{q^m}\text{-linear and} \\ \mathcal{V} = \mathcal{V}^*, \dim(\mathcal{C} \cap \mathcal{V}) \geq r\}. \end{aligned}$$

We also define $d_{R,0}(\mathcal{C}) = 0$ for convenience.

Hence $d_{R,r}(C)$ is the minimum number of links that a wire-tapper needs to listen to in order to obtain at least the amount of information contained in r packets. In other words, $r-1$ packets is the *worst-case information leakage* when at most $d_{R,r}(C)-1$ links are wire-tapped.

The next lemma corresponds to [11, Th. 16, Cor. 17]:

Lemma B.5 ([11]). *Given an $\mathbb{F}_{q^m}$-linear code $C \subseteq \mathbb{F}_{q^m}^n$ of dimension k and $1 \leq r \leq k$, it holds that*

$$d_{R,r}(C) = \min\{\mathrm{wt_R}(D) \mid D \subseteq C, \mathbb{F}_{q^m}\text{-linear and } \dim(D) = r\},$$

where $\mathrm{wt_R}(D) = \dim(D^*)$ *for an $\mathbb{F}_{q^m}$-linear $D \subseteq \mathbb{F}_{q^m}^n$.*

In particular, it is shown in [13, Cor. 1] that $d_{R,1}(C)$ is the minimum rank distance of the code C (also denoted by $d_R(C)$). Thus the minimum rank distance is of particular importance, since it gives the maximum number of wire-tapped links that guarantee zero information leakage, and we may evaluate the code's optimality among all rank-metric codes (linear and non-linear) in this sense using the Singleton bound [5, Th. 6.3]:

$$\#C \leq q^{\max\{m,n\}(\min\{m,n\}-d_R(C)+1)}, \tag{B.3}$$

where $C \subseteq \mathbb{F}_{q^m}^n$ is an arbitrary rank-metric code. Codes attaining this bound are called maximum rank distance (MRD) codes.

2.4 Existing MRD code constructions

We briefly revisit two existing code constructions that have already been considered in the literature:

1. Assume $n \leq m$ and $1 \leq k \leq n$: Take elements $\beta_1, \beta_2, \ldots, \beta_n \in \mathbb{F}_{q^m}$ that are linearly independent over $\mathbb{F}_q$. The $\mathbb{F}_{q^m}$-linear code $C_{Gab} \subseteq \mathbb{F}_{q^m}^n$ generated by the matrix

$$\begin{pmatrix} \beta_1 & \beta_2 & \cdots & \beta_n \\ \beta_1^{[1]} & \beta_2^{[1]} & \cdots & \beta_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1^{[k-1]} & \beta_2^{[k-1]} & \cdots & \beta_n^{[k-1]} \end{pmatrix}$$

has dimension k and minimum rank distance $d_R(C_{Gab}) = n-k+1$, and hence is MRD. These codes are known as Gabidulin codes and were introduced in [8]. Their GRWs were given in [13, Cor. 2]:

$$d_{R,r}(C_{Gab}) = n-k+r.$$

2. Assume $n = lm$ and $k = lk'$, for some positive integers l and $k' \leq m$: The $\mathbb{F}_{q^m}$-linear code $C \subseteq \mathbb{F}_{q^m}^n$ defined as $C = C_1 \times C_2 \times \cdots \times C_l$, where each $C_i \subseteq \mathbb{F}_{q^m}^m$ is a k'-dimensional Gabidulin code, has dimension k and minimum rank distance $d_R(C) = m - k' + 1$, and hence is also MRD. These codes were introduced in [9, Cor. 1] and considered in [23, Sec. VII-C] for secure network coding. In contrast with Gabidulin codes, although a first analysis of these codes is given in [23], their GRWs are still not known. We will find all of them in Section 4.2.

The two previous constructions are particular cases of reducible codes, introduced in [9], which we will study in the rest of the paper.

2.5 Reducible codes and reductions

Consider positive integers $l, n_1, n_2, \ldots, n_l$ and $\mathbb{F}_{q^m}$-linear codes $C_1 \subseteq \mathbb{F}_{q^m}^{n_1}, C_2 \subseteq \mathbb{F}_{q^m}^{n_2}, \ldots, C_l \subseteq \mathbb{F}_{q^m}^{n_l}$ of dimensions $k_1, k_2, \ldots, k_l$, respectively. Consider matrices $G_{i,j} \in \mathbb{F}_{q^m}^{k_i \times n_j}$, for $i = 1, 2, \ldots, l$ and $j = i, i+1, \ldots, l$, where $G_{i,i}$ generates C_i.

Definition B.6 ([9]). We say that an $\mathbb{F}_{q^m}$-linear code $C \subseteq \mathbb{F}_{q^m}^n$ is reducible with reduction $\mathcal{R} = (G_{i,j})_{1 \leq i \leq l}^{i \leq j \leq l}$ if it has a generator matrix of the form

$$G = \begin{pmatrix} G_{1,1} & G_{1,2} & G_{1,3} & \ldots & G_{1,l-1} & G_{1,l} \\ 0 & G_{2,2} & G_{2,3} & \ldots & G_{2,l-1} & G_{2,l} \\ 0 & 0 & G_{3,3} & \ldots & G_{3,l-1} & G_{3,l} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & G_{l-1,l-1} & G_{l-1,l} \\ 0 & 0 & 0 & \ldots & 0 & G_{l,l} \end{pmatrix}.$$

The length of the code C is $n = n_1 + n_2 + \cdots + n_l$ and its dimension is $k = k_1 + k_2 + \cdots + k_l$. C is the cartesian product of the codes $C_1, C_2, \ldots, C_l$ if $G_{i,j} = 0$, for all $j > i$.

Definition B.7. For a given reduction $\mathcal{R}$ as in the previous definition, we define its main components as the codes $C_1, C_2, \ldots, C_l$, its row components as the $\mathbb{F}_{q^m}$-linear codes $C'_i \subseteq \mathbb{F}_{q^m}^n$ with generator matrices

$$G'_i = (0, \ldots, 0, G_{i,i}, G_{i,i+1}, \ldots, G_{i,l}), \tag{B.4}$$

for $i = 1, 2, \ldots, l$, and its column components as the $\mathbb{F}_{q^m}$-linear codes $\widehat{C}_j \subseteq \mathbb{F}_{q^m}^{n_j}$ generated by the matrices

$$\widehat{G}_j = (G_{1,j}, G_{2,j}, \ldots, G_{j,j})^T, \tag{B.5}$$

for $j = 1, 2, \ldots, l$, which need not have full rank.

It holds that $k_i = \dim(C'_i)$, $\widehat{k}_j = \dim(\widehat{C}_j) \geq k_j$, $C = C'_1 \oplus C'_2 \oplus \cdots \oplus C'_l$ and $C \subseteq \widehat{C} = \widehat{C}_1 \times \widehat{C}_2 \times \cdots \times \widehat{C}_l$.

Different reductions always have the same main components if their block sizes are the same. See Appendix A for a discussion on the uniqueness of reductions of a reducible code.

3 Bounds on GRWs of reducible codes and exact values

With notation as in Subsection 2.5, it is proven in [9, Lemma 2] that

$$d_{R,1}(C) \geq \min\{d_{R,1}(C_1), d_{R,1}(C_2), \ldots, d_{R,1}(C_l)\}. \tag{B.6}$$

We now present the main result of this section, which generalizes (B.6) to higher GRWs and also gives upper bounds. As observed below, it gives the exact values for cartesian products.

Theorem B.1. *With notation as in Subsection 2.5, for every $r = 1, 2, \ldots, k$, we have that*

$$\begin{aligned} d_{R,r}(C) \geq \min\{&d_{R,r_1}(C_1) + d_{R,r_2}(C_2) + \cdots + d_{R,r_l}(C_l) \\ &\mid r = r_1 + r_2 + \cdots + r_l, 0 \leq r_i \leq k_i\}, \end{aligned} \tag{B.7}$$

and

$$\begin{aligned} d_{R,r}(C) \leq \min\{&d_{R,r_1}(C'_1) + d_{R,r_2}(C'_2) + \cdots + d_{R,r_l}(C'_l) \\ &\mid r = r_1 + r_2 + \cdots + r_l, 0 \leq r_i \leq k_i\}. \end{aligned} \tag{B.8}$$

The proof can be found at the end of the section. We now elaborate on some particular cases of interest.

First, observe that the bound (B.7) gives the bound (B.6) for the minimum rank distance (the case $r = 1$), and the bound (B.8) gives the following (immediate) upper bound:

$$d_{R,1}(C) \leq \min\{d_{R,1}(C'_1), d_{R,1}(C'_2), \ldots, d_{R,1}(C'_l)\}. \tag{B.9}$$

The previous theorem also gives the following corollary for cartesian products:

Corollary B.8. *If $C = C_1 \times C_2 \times \cdots \times C_l$ and $1 \leq r \leq k$, with notation as before, then*

$$\begin{aligned} d_{R,r}(C) = \min\{&d_{R,r_1}(C_1) + d_{R,r_2}(C_2) + \cdots + d_{R,r_l}(C_l) \\ &\mid r = r_1 + r_2 + \cdots + r_l\}. \end{aligned} \tag{B.10}$$

Now we illustrate Theorem B.1 with the following example that includes the MRD $\mathbb{F}_{q^m}$-linear codes in Subsection 2.4, item 2, for $l = 2$:

Example B.9. With notation as in Theorem B.1, assume that $l = 2$, $n_1, n_2 \leq m$, $k_1 \leq k_2$ and take C_1 and C_2 as MRD codes (the matrix $G_{1,2}$ can be arbitrary). In particular, $d_{R,r_i}(C_i) = n_i - k_i + r_i$ [13] as in Subsection 2.4, $1 \leq r_i \leq k_i$, $i = 1, 2$. We estimate $d_{R,r}(C)$ considering three cases:

1. Assume $1 \leq r \leq k_1$: The bounds (B.7) and (B.8) give
$$\min\{n_1 - k_1, n_2 - k_2\} + r \leq d_{R,r}(C) \leq n_2 - k_2 + r.$$
2. Assume $k_1 < r \leq k_2$ (if $k_1 < k_2$): In this case, in both bounds in Theorem B.1, it is necessary that $r_2 > 0$. Hence, these bounds coincide and give the value $d_{R,r}(C) = n_2 - k_2 + r$.
3. Assume $k_2 < r \leq k$: As in the previous case, now it is necessary that $r_1 > 0$ and $r_2 > 0$, and thus Theorem B.1 gives the value $d_{R,r}(C) = n - k + r$, which is optimal by the Singleton bound [13, Proposition 1].

Finally, it is natural to ask whether different reductions (see Definition B.6) may give different bounds in Theorem B.1. In Appendix A, we show that all reductions have the same main components, thus (B.7) remains unchanged. We now show that (B.9) can always be attained by some particular reduction. Other cases where (B.8) may be attained by some reduction are open.

Proposition B.10. *With notation as in Subsection 2.5, there exists a reduction $\overline{\mathcal{R}} = (\overline{G}_{i,j})_{1 \leq i \leq l}^{i \leq j \leq l}$ of C such that the bound (B.9) is an equality.*

Proof. Assume that the minimum rank distance is attained by $\mathrm{wt_R}(\mathbf{c}) = d_{R,1}(C)$, for $\mathbf{c} \in C$. It holds that $\mathbf{c} = \mathbf{c}'_1 + \mathbf{c}'_2 + \cdots + \mathbf{c}'_l$, with $\mathbf{c}'_i \in C'_i$, and $\mathbf{c}'_i = \mathbf{x}_i G'_{i,i}$ (recall (B.4)), for some $\mathbf{x}_i \in \mathbb{F}_{q^m}^{k_i}$ and all $i = 1, 2, \ldots, l$.

We may assume without loss of generality that $\mathbf{x}_1 \neq \mathbf{0}$. We just need to define $\overline{G}_{i,i} = G_{i,i}$ and choose matrices $A_{1,j} \in \mathbb{F}_{q^m}^{k_1 \times k_j}$ and $\overline{G}_{i,j} \in \mathbb{F}_{q^m}^{k_i \times n_j}$, for $1 \leq i \leq l-1$ and $i+1 \leq j \leq l$, such that the $k \times k$ matrix
$$A = \begin{pmatrix} I & A_{1,2} & A_{1,3} & \ldots & A_{1,l-1} & A_{1,l} \\ 0 & I & 0 & \ldots & 0 & 0 \\ 0 & 0 & I & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & I & 0 \\ 0 & 0 & 0 & \ldots & 0 & I \end{pmatrix}$$
satisfies that $G = A\overline{G}$, where $\overline{G}$ is the generator matrix of C corresponding to $\overline{\mathcal{R}} = (\overline{G}_{i,j})_{1 \leq i \leq l}^{i \leq j \leq l}$, and
$$\mathbf{x}_1 A_{1,j} = -\mathbf{x}_j,$$

for $j = 2, 3, \ldots, l$. It is possible to choose such matrices $A_{1,j}$ because $\mathbf{x}_1 \neq \mathbf{0}$. Then $\mathbf{c} = (\mathbf{x}A)\overline{G}$ lies in the first row component of the reduction $\overline{\mathcal{R}}$ and hence $d_{R,1}(C) = \mathrm{wt_R}(\mathbf{c}) \geq d_{R,1}(\overline{C}'_1)$, implying the result. □

We conclude the section with the proof of Theorem B.1. We need the following lemma:

Lemma B.11. *With notation as in Subsection 2.5, define the sets*

$$A_i = \{0\}^{n_1} \times \cdots \times \{0\}^{n_{i-1}} \times (\mathbb{F}_{q^m}^{n_i} \setminus \{\mathbf{0}\}) \times \mathbb{F}_{q^m}^{n_{i+1}} \times \cdots \times \mathbb{F}_{q^m}^{n_l},$$

for $i = 1, 2, \ldots, l$. For an $\mathbb{F}_{q^m}$-linear vector space $D \subsetneq \mathbb{F}_{q^m}^n$, there exist subspaces $D'_i \subseteq \langle D \cap A_i \rangle$, for i satisfying $D \cap A_i \neq \varnothing$, such that $D = \bigoplus_{D \cap A_i \neq \varnothing} D'_i$ and $D'_i \cap A_j = \varnothing$ for $j > i$.

Proof. We may prove it by induction on the number of indices i such that $D \cap A_i \neq \varnothing$. If such number is 1, the result is trivial by taking $D'_i = D$, since $D = \langle D \cap A_i \rangle$.

Assume that it is larger than 1 and i is the smallest index such that $D \cap A_i \neq \varnothing$. Define $\widetilde{D} = \sum_{j=i+1}^{l} \langle D \cap A_j \rangle \neq \{\mathbf{0}\}$, and let $D'_i \neq \{\mathbf{0}\}$ by one of its complementaries in D. It follows that $D'_i \subseteq \langle D \cap A_i \rangle$ and $D'_i \cap A_j = \varnothing$, for $j > i$.

Now, by induction hypothesis, $\widetilde{D}$ has a decomposition as in the theorem, which together with D'_i gives the desired decomposition of D. □

Proof of Theorem B.1. We first prove (B.7). Take an r-dimensional $\mathbb{F}_{q^m}$-linear subspace $D \subsetneq C$. With notation as in Lemma B.11, define $D_i \subsetneq C_i$ as the projection of D'_i onto the i-th main component, for i such that $D \cap A_i \neq \varnothing$. We see that $\dim(D_i) = \dim(D'_i)$, since $D'_i \subseteq \langle D \cap A_i \rangle$ and $D'_i \cap A_j = \varnothing$ for $j > i$, and by collecting the preimages in D^* by the projection map of bases of D_i^*, for i such that $D \cap A_i \neq \varnothing$, we see that

$$\mathrm{wt_R}(D) \geq \sum_{D \cap A_i \neq \varnothing} \mathrm{wt_R}(D_i),$$

and the result follows by Lemma B.5.

To prove (B.8), take a decomposition $r = r_1 + r_2 + \cdots + r_l$, with $0 \leq r_i \leq k_i$, for $i = 1, 2, \ldots, l$, and take $\mathbb{F}_{q^m}$-linear subspaces $D_i \subseteq C'_i$ with $\dim(D_i) = r_i$ and $\mathrm{wt_R}(D_i) = d_{R,r_i}(C'_i)$. Then define the $\mathbb{F}_{q^m}$-linear subspace $D = D_1 \oplus D_2 \oplus \cdots \oplus D_l \subseteq C$, which satisfies $\dim(D) = r$. By definition, it holds that $D^* = D_1^* + D_2^* + \cdots + D_l^*$. Hence

$$\begin{aligned} \mathrm{wt_R}(D) &\leq \mathrm{wt_R}(D_1) + \mathrm{wt_R}(D_2) + \cdots + \mathrm{wt_R}(D_l) \\ &= d_{R,r_1}(C'_1) + d_{R,r_2}(C'_2) + \cdots + d_{R,r_l}(C'_l), \end{aligned}$$

and the result follows again by Lemma B.5. □

Remark B.12. *Observe that the bound (B.8) is valid with the same proof for a general $\mathbb{F}_{q^m}$-linear code that can be decomposed as a direct sum of $\mathbb{F}_{q^m}$-linear subcodes $C = C'_1 \oplus C'_2 \oplus \cdots \oplus C'_l$.*

Remark B.13. *In the general setting of Theorem B.1, the same result as in Corollary B.8 holds whenever C_i and C'_i are rank equivalent (see Section 5), for each $i = 1, 2, \ldots, l$, since in that case it holds that $d_{R,r}(C_i) = d_{R,r}(C'_i)$ for all $i = 1, 2, \ldots, l$ and all $r = 1, 2, \ldots, k_i$.*

4 MRD reducible codes with MRD main components, and their GRWs

Among all GRWs, the first weight (the minimum rank distance) is of special importance, as explained at the end of Subsection 2.3. Therefore, it is of interest to study the GRWs of a family of MRD codes, that is, codes that are already optimal for the first weight.

In this section, we find new parameters for which reducible codes are MRD or close to MRD when $n > m$, extending the family of MRD codes in [9] (see Subsection 2.4), and then give bounds on their GRWs and exact values in the cartesian product case, using the results in the previous section. Hence we give for the first time estimates and exact values of the GRWs of a family of MRD codes with $n > m$. We will also compare the performance of these codes with those $\mathbb{F}_q$-linear MRD codes obtained by transposing the matrix representations of codewords in a Gabidulin code [17, Sec. IV-B].

4.1 Definition of the codes

Assume $n > m$ and fix an integer $1 \leq k \leq n$. In view of the bound (B.6), we will consider a reducible code $C_{red} \subseteq \mathbb{F}_{q^m}^n$ of dimension k whose main components $C_1, C_2, \ldots, C_l$ (with notation as in Subsection 2.5) have as similar parameters as possible. This will allow to obtain reducible codes with minimum rank distance as large as allowed by (B.3).

First we need the following parameters:

1. There exist unique $l > 0$ and $0 \leq t \leq m - 1$ such that
$$n = lm - t.$$
2. There exist unique $k' > 0$ and $0 \leq s \leq l - 1$ such that
$$k = lk' - s.$$
3. Define then
$$a = \left\lceil \frac{km}{n} \right\rceil - k', \quad \text{and} \quad b = \left\lceil \frac{t}{l} \right\rceil - 1.$$

4. Finally, define
$$t' = l(m-b) - n,$$
which satisfies $0 < t' \leq l$.

We need the next inequalities to define the desired codes:

Lemma B.14. *It holds that $k' \leq m - b$ if $b \geq 0$, and $k' \leq m$ if $b = -1$.*

Proof. For $b = -1$, we have that $t = 0$ and $k = lk' - s \leq n = lm$ implies that $k' \leq m + s/l$. Since $s < l$, the result holds in this case.

Now assume that $b \geq 0$. We have that $k + s \leq n + l$. Writing k and n as above, this inequality reads

$$(lk' - s) + s \leq (lm - t) + l,$$

that is, $lk' + t \leq l(m+1)$ and, dividing by l, it is equivalent to

$$k' + \frac{t}{l} - 1 \leq m.$$

The result follows by the definition of b. □

Finally, we give the construction, distinguishing three cases:

Definition B.15. Define the reducible code $C_{red} \subseteq \mathbb{F}_{q^m}^n$ of dimension k with MRD main components $C_1, C_2, \ldots, C_l$ as follows:

1. If $t = 0$ (i.e. $b = -1$): Choose $C_1, C_2, \ldots, C_l$ such that $l - s$ of them have length m and dimension k', and s of them have length m and dimension $k' - 1$. By (B.6), we have that
$$d_{R,1}(C_{red}) \geq m - k' + 1.$$

2. If $t > 0$ and $t' \leq s$: Choose $C_1, C_2, \ldots, C_l$ such that $l - s$ of them have length $m - b$ and dimension k', $s - t'$ of them have length $m - b$ and dimension $k' - 1$, and t' of them have length $m - b - 1$ and dimension $k' - 1$. By (B.6), we have that
$$d_{R,1}(C_{red}) \geq m - b - k' + 1.$$

3. If $t > 0$ and $t' > s$: Choose $C_1, C_2, \ldots, C_l$ such that $l - t'$ of them have length $m - b$ and dimension k', $t' - s$ of them have length $m - b - 1$ and dimension k', and s of them have length $m - b - 1$ and dimension $k' - 1$. By (B.6), we have that
$$d_{R,1}(C_{red}) \geq m - b - k'.$$

The next theorem is the first main result of this section, and it gives families of parameters m, n and k such that C_{red} is MRD or almost MRD:

Theorem B.2. *Assume that $0 \leq t \leq l$ or $n \geq m^2$. The following holds:*

1. *If $t \leq s$ or $tk' > ms$, then*

$$d_{R,1}(C_{red}) = \left\lfloor \frac{m}{n}(n-k)+1 \right\rfloor,$$

attaining (B.3) if n divides mk.

2. *If $t > s$ and $tk' \leq ms$, then*

$$d_{R,1}(C_{red}) \geq \left\lfloor \frac{m}{n}(n-k) \right\rfloor.$$

Proof. First we see that we only need to assume $0 \leq t \leq l$. Assume that $n \geq m^2$. Since $n = lm - t \geq m^2$ and $t \geq 0$, it holds that $l \geq m$. Therefore $t \leq m-1 \leq l-1$.

Next we observe that

$$\left\lfloor \frac{m}{n}(n-k)+1 \right\rfloor = m - a - k' + 1. \tag{B.11}$$

Before considering the different cases, we will see that $a \geq 0$, and $a = 0$ if and only if $k't \leq sm$.

First it holds that $-1 < km/n - k'$ if and only if

$$(k'-1)n < km.$$

Using that $n = lm - t$ and $k = lk' - s$, and rearranging terms, this inequality reads

$$sm + (k'-1)t < lm + n,$$

which is always true since $s < l$ and $k't \leq k \leq n$. Hence $a \geq 0$. On the other hand, $km/n - k' \leq 0$ if and only if

$$nk' \geq km.$$

Using again that $n = lm - t$ and $k = lk' - s$, and rearranging terms, this inequality reads $k't \leq sm$. This is then the case when $a = 0$.

Now we prove item 1 in the theorem:

Assume first that $t = 0$, then $d_{R,1}(C_{red}) \geq m - k' + 1$ and $a = 0$, hence the result follows in this case by (B.11).

Now assume that $0 < t \leq s$. Then $d_{R,1}(C_{red}) \geq m - k' + 1$ (since $b = 0$) and $k't \leq sm$ holds, since $k' \leq m$. Then $a = 0$ and the result follows in this case by (B.11).

Next assume that $tk' > ms$. Then we know that $a \geq 1$ and

$$\left\lfloor \frac{m}{n}(n-k)+1 \right\rfloor \leq m-k'.$$

Since $b = 0$, we know that $d_{R,1}(C_{red}) \geq m-k'$, hence the result follows in this case by (B.11).

Finally, we prove item 2:

Assume that $t > s$ and $tk' \leq ms$. Then we know that $a = b = 0$ and $d_{R,1}(C_{red}) \geq m-b-k'$. Therefore the result follows also in this case by (B.11) and we are done. □

Remark B.16. *Observe that the MRD reducible codes in Subsection 2.4, item 2, are the subfamily of the codes C_{red} obtained by choosing $t = s = 0$, and hence are particular cases of the codes in the previous theorem.*

Remark B.17. *Observe that the conditions $0 \leq t \leq l$ and $n \geq m^2$ only depend on m and n, but not on k. Hence, for the previous families of values of n and m, we have obtained MRD or almost MRD codes for all dimensions.*

Remark B.18. *In general, the difference $b-a$ will be big if t is much bigger than l. As n grows, the fact $t > l$ happens for fewer values of t. Hence the codes C_{red} are far from optimal when n is small compared to m (still $n > m$) and t is much bigger than l.*

4.2 Estimates and exact values of their GRWs

The next theorem is the second main result in this section, and it gives estimates of the GRWs of the MRD (or almost MRD) reducible codes C_{red} from Theorem B.2, using the lower bound (B.7).

Theorem B.3. *Let the parameters be as in Theorem B.2.*

Assume first that $t \leq s$.

1. *If $1 \leq j \leq l-s$ and $(j-1)k' < r \leq jk'$, or if $l-s < j \leq l-s+t$ and $(j-1)(k'-1)+l-s < r \leq j(k'-1)+l-s$, then*

$$d_{R,r}(C_{red}) \geq j(m-k')+r.$$

2. *If $l-s+t < j \leq l$ and $(j-1)(k'-1)+l-s < r \leq j(k'-1)+l-s$, then*

$$d_{R,r}(C_{red}) \geq j(m-k')+r+(j-l+s-t).$$

Assume now that $t > s$.

1. *If $1 \leq j \leq t-s$ and $(j-1)k' < r \leq jk'$, then*

$$d_{R,r}(C_{red}) \geq j(m-k'-1)+r.$$

2. *If $t - s < j \leq l - s$ and $(j-1)k' < r \leq jk'$, or if $l - s < j \leq l$ and $(j-1)(k'-1) + l - s < r \leq j(k'-1) + l - s$, then*

$$d_{R,r}(C_{red}) \geq j(m - k') + r - t + s.$$

These cases cover all $r = 1, 2, \ldots, k$ and moreover, if C_{red} is the cartesian product of its main components $C_1, C_2, \ldots, C_l$, then all the previous lower bounds are equalities.

Proof. The result follows from Theorem B.1. To see it, we just have to use that $d_{R,r_i}(C_i) = n_i - k_i + r_i$ and see in which way we have to choose $r_i = 0$ or $r_i > 0$ to obtain the minimum in the bound (B.7), for $i = 1, 2, \ldots, l$. This is a straightforward extension of the calculations in Example B.9. □

4.3 Comparison with other MRD codes

In this subsection, we will compare the codes $C_{red} \subseteq \mathbb{F}_{q^m}^n$ from Definition B.15 with the $\mathbb{F}_q$-linear MRD codes $C_{Gab}^T \subseteq \mathbb{F}_{q^m}^n$ obtained by transposing the matrix represenations (see (B.1)) of the codewords in a given $\mathbb{F}_{q^n}$-linear Gabidulin code $C_{Gab} \subseteq \mathbb{F}_{q^n}^m$ (see Subsection 2.4), when $n > m$.

The codes C_{Gab}^T were obtained previously by Delsarte [5, Th. 6] and have been recently considered for universal secure linear network coding in [17, Sec. IV-B].

We next argue the advantages of the codes C_{red} over the codes C_{Gab}^T:

1. *Generalized rank weights*: Although GRWs have recently been extended to $\mathbb{F}_q$-linear codes [17, 21] and its connection to worst-case information leakage has been obtained [17, Th. 3], little is known about them for codes that are not linear over $\mathbb{F}_{q^m}$. In particular, the GRWs of the codes C_{Gab}^T are not known yet, except for their minimum rank distance.

2. *Encoding and decoding complexity*: The complexity of coset encoding and decoding with an $\mathbb{F}_{q^m}$-linear code, as in Definition B.1, is equivalent to the complexity of encoding with one of its generator matrices.

   If k_{red} denotes the dimension of C_{red} over $\mathbb{F}_q$, then the complexity of encoding with a generator matrix coming from one of its reductions is $O(k_{red}m^2)$ operations over $\mathbb{F}_{q^m}$, whereas if k_{Gab} denotes the dimension of C_{Gab} over $\mathbb{F}_q$, then the complexity of encoding with one of its generator matrices is $O(k_{Gab}n^2)$ operations over $\mathbb{F}_{q^n}$. Therefore it is a higher complexity since $n > m$, and the difference between both complexities becomes higher the bigger n is with respect to m.

3. *Possible parameters obtained*: Since the codes C_{Gab}^T are obtained from $\mathbb{F}_{q^n}$-linear codes, their sizes are of the form q^N, where N is some multiple

of n, whereas the sizes of the codes C_{red} are of the form q^M, where M is some multiple of m.

Since we are assuming $n > m$, in a given interval of positive integers, there are more possible parameters attained by the codes C_{red} than by the codes C^T_{Gab}.

4. *Stronger security*: The information leakage for a given number of wire-tapped links when using the codes C_{red} is often much less than the worst case given by their GRWs, as we will see in Section 6. In particular, looking at their first GRW, we will see that more links can be wire-tapped and still guarantee zero information leakage when using C_{red} than when using C^T_{Gab}.

5 All $\mathbb{F}_{q^m}$-linear codes with optimal GRWs for all fixed packet and code sizes

In this section, we obtain all $\mathbb{F}_{q^m}$-linear codes whose GRWs are all optimal for fixed packet and code sizes (m and k, respectively), but varying length, n, up to rank equivalence. These codes are particular cases of the codes C_{red} in the previous section.

Definition B.19. For fixed k and m, and for a basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, define the $\mathbb{F}_{q^m}$-linear code $C_{opt} = C_1 \times C_2 \times \cdots \times C_k \subseteq \mathbb{F}_{q^m}^{km}$, where all C_i are equal and generated by the vector $(\alpha_1, \alpha_2, \ldots, \alpha_m) \in \mathbb{F}_{q^m}^m$.

To claim the above mentioned optimality of these codes, we need the following bounds given in [16, Lemma 6]:

Lemma B.20 ([16]). *Given an $\mathbb{F}_{q^m}$-linear code $C \subseteq \mathbb{F}_{q^m}^n$ of dimension k, for each $r = 1, 2, \ldots, k-1$, it holds that*

$$1 \leq d_{R,r+1}(C) - d_{R,r}(C) \leq m. \tag{B.12}$$

As a consequence, for each $r = 1, 2, \ldots, k$, it holds that

$$d_{R,r}(C) \leq rm. \tag{B.13}$$

Observe that these bounds only depend on the packet and code sizes (m and k, respectively), and they do not depend on the length n.

We first show that the codes C_{opt} attain the previous bounds, and then prove that they are the only ones with this property:

Proposition B.21. *Let $C_{opt} \subseteq \mathbb{F}_{q^m}^{km}$ be the $\mathbb{F}_{q^m}$-linear code in Definition B.19 for given k and m. Then* $\dim(C_{opt}) = k$ *and* $d_{R,r}(C_{opt}) = rm$, *for $r = 1, 2, \ldots, k$.*

Proof. It holds that $d_{R,1}(C_i) = m$, for $i = 1, 2, \ldots, k$, since these codes are one-dimensional Gabidulin codes in $\mathbb{F}_{q^m}^m$ (see Subsection 2.4). Hence, by Corollary B.8, we have that

$$d_{R,k}(C_{opt}) = \sum_{i=1}^{k} d_{R,1}(C_i) = km.$$

By (B.12), it holds that $d_{R,r}(C_{opt}) = rm$, for $r = 1, 2, \ldots, k$. □

We will use the definition of rank equivalences from [16, Def. 8], which are stronger than vector space isomorphisms that preserve rank weights:

Definition B.22 ([16]). If $V \subseteq \mathbb{F}_{q^m}^n$ and $V' \subseteq \mathbb{F}_{q^m}^{n'}$ are $\mathbb{F}_{q^m}$-linear Galois closed spaces, we say that a map $\phi : V \longrightarrow V'$ is a rank equivalence if it is a vector space isomorphism and $\mathrm{wt_R}(\phi(\mathbf{c})) = \mathrm{wt_R}(\mathbf{c})$, for all $\mathbf{c} \in V$.

We say that two codes C and C' are rank equivalent if there exists a rank equivalence between $\mathbb{F}_{q^m}$-linear Galois closed spaces V and V' that contain C and C', respectively, and mapping bijectively C to C'.

Finally, we show that the codes C_{opt} are the only $\mathbb{F}_{q^m}$-linear codes attaining (B.13) for fixed packet and code sizes up to rank equivalence:

Theorem B.4. *Let $C \subseteq \mathbb{F}_{q^m}^n$ be an $\mathbb{F}_{q^m}$-linear code of dimension k such that $d_{R,r}(C) = rm$, for every $r = 1, 2, \ldots, k$.*

Then, for every basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, the code C is rank equivalent to the code $C_{opt} \subseteq \mathbb{F}_{q^m}^{km}$ in Definition B.19. Moreover, the rank equivalence can be explicitly constructed in polynomial time from any basis of C.

We need some preliminary lemmas to prove this result. We start by the following characterization of rank equivalences, which is a particular case of [16, Th. 5]:

Lemma B.23 ([16]). *Let $\phi : V \longrightarrow V'$ be an $\mathbb{F}_{q^m}$-linear vector space isomorphism, where $V \subseteq \mathbb{F}_{q^m}^n$ and $V' \subseteq \mathbb{F}_{q^m}^{n'}$ are $\mathbb{F}_{q^m}$-linear Galois closed spaces.*

It is a rank equivalence if and only if there exist bases $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_t \in \mathbb{F}_q^n$ and $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_t \in \mathbb{F}_q^{n'}$ of V and V', respectively, and a non-zero element $\beta \in \mathbb{F}_{q^m}$, such that $\phi(\mathbf{v}_i) = \beta \mathbf{w}_i$, for $i = 1, 2, \ldots, t$.

We now introduce some notation. For a given vector $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in \mathbb{F}_{q^m}^n$, define $\mathbf{c}^{[i]} = (c_1^{[i]}, c_2^{[i]}, \ldots, c_n^{[i]})$, for all integers $i \geq 0$. Then define the trace map $\mathrm{Tr} : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^n$ of the extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ as follows

$$\mathrm{Tr}(\mathbf{c}) = \mathbf{c} + \mathbf{c}^{[1]} + \mathbf{c}^{[2]} + \cdots + \mathbf{c}^{[m-1]},$$

for all $\mathbf{c} \in \mathbb{F}_{q^m}^n$. We have the following two lemmas:

Lemma B.24. *For a basis $\alpha_1, \alpha_2, \dots, \alpha_m$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, the matrix $A = (\alpha_i^{[j-1]})_{1 \leq i,j \leq m}$ over $\mathbb{F}_{q^m}$ is invertible.*

Proof. Well-known. See for instance [8]. □

Lemma B.25. *For a basis $\alpha_1, \alpha_2, \dots, \alpha_m$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and the matrix $A = (\alpha_i^{[j-1]})_{1 \leq i,j \leq m}$, define*

$$(\beta_1, \beta_2, \dots, \beta_m) = \mathbf{e}_1 A^{-1},$$

where $\mathbf{e}_1 \in \mathbb{F}_{q^m}^m$ is the first vector in the canonical basis. Then $\beta_1, \beta_2, \dots, \beta_m$ is also a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

Moreover, if $B = (\beta_i^{[j-1]})_{1 \leq i,j \leq m}$, then

$$(\alpha_1, \alpha_2, \dots, \alpha_m) = \mathbf{e}_1 B^{-1}.$$

Proof. Write $\boldsymbol{\beta} = (\beta_1, \beta_2, \dots, \beta_m)$. Then $\boldsymbol{\beta} A = \mathbf{e}_1$, which means that $\sum_{i=1}^m \beta_i \alpha_i^{[j-1]} = \delta_{j,1}$, where δ is the Kronecker delta. By raising this equation to the power $[l-1] = q^{l-1}$ and using that $\delta_{j,l}$ is 0 or 1, we see that $\sum_{i=1}^m \beta_i^{[l-1]} \alpha_i^{[j-1]} = \delta_{j,l}$, that is, $\boldsymbol{\beta}^{[l-1]} A = \mathbf{e}_l$, for $l = 1, 2, \dots, m$.

Let $\boldsymbol{\lambda} \in \mathbb{F}_q^m$ be such that $\boldsymbol{\lambda} \cdot \boldsymbol{\beta} = 0$. By raising this equation to the power $[l-1]$, for $l = 1, 2, \dots, m$, we see that $\boldsymbol{\lambda} \cdot \boldsymbol{\beta}^{[l-1]} = 0$ or, equivalently, $\boldsymbol{\lambda} \cdot (\mathbf{e}_l A^{-1}) = 0$, since $\boldsymbol{\lambda} \in \mathbb{F}_q^m$.

Write $\boldsymbol{\mu} = (\mu_1, \mu_2, \dots, \mu_m) = \boldsymbol{\lambda}(A^{-1})^T$. It holds that

$$0 = \boldsymbol{\lambda} \cdot (\mathbf{e}_l A^{-1}) = (\boldsymbol{\lambda}(A^{-1})^T) \cdot \mathbf{e}_l = \boldsymbol{\mu} \cdot \mathbf{e}_l = \mu_l,$$

for $l = 1, 2, \dots, m$. Therefore, $\boldsymbol{\mu} = \mathbf{0}$, thus $\boldsymbol{\lambda} = \mathbf{0}$. Hence the elements $\beta_1, \beta_2, \dots, \beta_m$ are linearly independent over $\mathbb{F}_q$.

Finally, since $\sum_{i=1}^m \beta_i^{[l-1]} \alpha_i^{[j-1]} = \delta_{j,l}$, it holds that $\sum_{i=1}^m \alpha_i \beta_i^{[j-1]} = \delta_{1,j} = \delta_{j,1}$, which means that $(\alpha_1, \alpha_2, \dots, \alpha_m) B = \mathbf{e}_1$, and we are done. □

We may now prove Theorem B.4:

Proof of Theorem B.4. Choose any basis $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_k$ of C. Since $\dim(C^*) = km$ and C^* is generated by the elements $\mathbf{b}_s^{[j-1]}$, for $s = 1, 2, \dots, k$ and $j = 1, 2, \dots, m$, it follows that these elements are linearly independent over $\mathbb{F}_{q^m}$.

Define the vector $\boldsymbol{\beta} = (\beta_1, \beta_2, \dots, \beta_m) = \mathbf{e}_1 A^{-1}$, with notation as in the previous lemma. By that lemma, $\beta_1, \beta_2, \dots, \beta_m$ constitute a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and $(\alpha_1, \alpha_2, \dots, \alpha_m) = \mathbf{e}_1 B^{-1}$.

Consider the vectors $\mathbf{v}_{s,i} = \mathrm{Tr}(\beta_i \mathbf{b}_s) \in \mathbb{F}_q^n$, for $s = 1, 2, \dots, k$ and $i = 1, 2, \dots, m$. Assume that there exist $\lambda_{s,i} \in \mathbb{F}_q$ such that $\sum_{s=1}^k \sum_{i=1}^m \lambda_{s,i} \mathbf{v}_{s,i} = \mathbf{0}$. Then it holds that

$$\sum_{j=1}^m \sum_{s=1}^k \left(\sum_{i=1}^m \lambda_{s,i} \beta_i^{[j-1]} \right) \mathbf{b}_s^{[j-1]} = \mathbf{0}.$$

Hence $\sum_{i=1}^{m} \lambda_{s,i}\beta_i^{[j-1]} = 0$, for $s = 1, 2, \ldots, k$ and $j = 1, 2, \ldots, m$, which implies that $\lambda_{s,i} = 0$, for $s = 1, 2, \ldots, k$ and $i = 1, 2, \ldots, m$.

Therefore, the elements $\mathbf{v}_{s,i}$, for $s = 1, 2, \ldots, k$ and $i = 1, 2, \ldots, m$, constitute a basis of C^* and are vectors in $\mathbb{F}_q^n$. Now define the $\mathbb{F}_{q^m}$-linear vector space isomorphism $\psi : C^* \longrightarrow \mathbb{F}_{q^m}^{km}$ by $\psi(\mathbf{v}_{s,i}) = \mathbf{e}_{(s-1)m+i}$, for $s = 1, 2, \ldots, k$ and $i = 1, 2, \ldots, m$. By Lemma B.23, ψ is a rank equivalence and, moreover,

$$\mathbf{b}_s = \sum_{j=1}^{m} \sum_{i=1}^{m} \alpha_i \beta_i^{[j-1]} \mathbf{b}_s^{[j-1]} = \sum_{i=1}^{m} \alpha_i \mathrm{Tr}(\beta_i \mathbf{b}_s) = \sum_{i=1}^{m} \alpha_i \mathbf{v}_{s,i}.$$

It follows that $\mathbf{v}_s = \psi(\mathbf{b}_s) = \sum_{i=1}^{m} \alpha_i \mathbf{e}_{(s-1)m+i}$, and the vectors $\mathbf{v}_s$, for $s = 1, 2, \ldots, k$, constitute a basis of $\psi(C)$. Finally, this means that $\psi(C) = C_{opt}$ and we are done. □

Remark B.26. *As explained in Subsection 2.2, given an $\mathbb{F}_{q^m}$-linear code $C \subseteq \mathbb{F}_{q^m}^n$ of dimension k, the parameter m represents the packet length, k represents the number of linearly independent packets that we may send using C, or its size, and n represents the number of outgoing links from the source.*

Due to the bounds (B.13), if m and k are fixed and n is not restricted, then the code C_{opt} is the only $\mathbb{F}_{q^m}$-linear code whose GRWs are all optimal, and hence is the only $\mathbb{F}_{q^m}$-linear optimal code regarding information leakage in the network, up to rank equivalence.

Remark B.27. *The codes $C_{opt} \subseteq \mathbb{F}_{q^m}^{km}$ do not only have optimal GRWs, but the difference between two consecutive weights is the largest possible by (B.12):*

$$d_{R,r+1}(C_{opt}) = d_{R,r}(C_{opt}) + m,$$

for $r = 1, 2, \ldots, k-1$. However, for a Gabidulin code C_{Gab} as in Subsection 2.4, the difference between two consecutive weights is the smallest possible by (B.12):

$$d_{R,r+1}(C_{Gab}) = d_{R,r}(C_{Gab}) + 1,$$

for $r = 1, 2, \ldots, k-1$.

Therefore, when using C_{opt}, an adversary that obtains r packets of information, by listening to the smallest possible number of links, needs to listen to at least m more links in order to obtain one more packet of information. However, when using C_{Gab}, the adversary only needs to listen to one more link to obtain one more packet of information.

6 Stronger security of reducible codes

On the error correction side, it is well-known that reducible codes can correct a substantial amount of rank errors beyond half of their minimum rank distance [9, Sec. III.A].

The aim of this section is to show that, on the security side, when using a reducible code C, an eavesdropper may in many cases obtain less than r packets of information even if he or she wire-taps at least $d_{R,r}(C)$ links in the network (see Subsection 2.3).

Setting $r = 1$ and using an MRD reducible code (as in Section 4.1), this means that the eavesdropper obtains no information even when wire-tapping strictly more links than those allowed by other MRD codes ($\mathbb{F}_{q^m}$-linear or $\mathbb{F}_q$-linear), by [17, Th. 3].

The above mentioned stronger security is obtained by upper bounding the dimensions of the code intersected with Galois closed spaces, due to Equation (B.2). We explain this in the remarks at the end of the section.

The following is the main result of this section, where we denote by $\pi_i : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^{n_i}$ the projection map onto the coordinates corresponding to the i-th main component $C_i \subseteq \mathbb{F}_{q^m}^{n_i}$, for $i = 1, 2, \ldots, l$, with notation as in Subsection 2.5.

Theorem B.5. *Let $V \subseteq \mathbb{F}_{q^m}^n$ be an $\mathbb{F}_{q^m}$-linear Galois closed space and assume that, for each $i = 1, 2, \ldots, l$, there exists $0 \leq r_i \leq k_i$ such that $\dim(\pi_i(V)) \leq d_{R,r_i}(C_i)$, with notation as in Subsection 2.5. Then*

$$\dim(C \cap V) \leq \left(\sum_{i=1}^{l} r_i \right) - \#\{ i \mid \dim(\pi_i(V)) < d_{R,r_i}(C_i) \}.$$

In particular, if $\dim(\pi_i(V)) < d_{R,1}(C_i)$, for $i = 1, 2, \ldots, l$, then

$$\dim(C \cap V) = 0.$$

Before proving this theorem, we give two consequences of interest. In the first, we give a sufficient condition for the eavesdropper to obtain less than r packets of information, for a given r, as in the second paragraph of this section:

Corollary B.28. *Let the notation be as in Subsection 2.5, let $1 \leq r \leq k$ and let $V \subseteq \mathbb{F}_{q^m}^n$ be an $\mathbb{F}_{q^m}$-linear Galois closed space. Assume that $r = \sum_{i=1}^{l} r_i$, where $1 \leq r_i \leq k_i$ and $\dim(\pi_i(V)) \leq d_{R,r_i}(C_i)$, for $i = 1, 2, \ldots, l$, and for some j it holds that $\dim(\pi_j(V)) < d_{R,r_j}(C_j)$. Then*

$$\dim(C \cap V) < r.$$

The second consequence is just the previous theorem applied to the codes in Definition B.19:

Corollary B.29. *Let $C_{opt} \subseteq \mathbb{F}_{q^m}^{km}$ be the code in Definition B.19, and let $V \subseteq \mathbb{F}_{q^m}^{km}$ be an $\mathbb{F}_{q^m}$-linear Galois closed space. Then*

$$\dim(C_{opt} \cap V) \leq \#\{ i \mid \pi_i(V) = \mathbb{F}_{q^m}^m \}.$$

Finally, we prove Theorem B.5. We need the following lemma:

Lemma B.30. *Let $V \subseteq \mathbb{F}_{q^m}^n$ be an $\mathbb{F}_{q^m}$-linear Galois closed space, and let the notation be as in Subsection 2.5. It holds that*

$$\dim(C \cap V) \leq \sum_{i=1}^{l} \dim(C_i \cap \pi_i(V)).$$

Proof. Let $D = C \cap V \subseteq C$ and let the notation be as in Lemma B.11. Since $D = \bigoplus_{D \cap A_i \neq \varnothing} D_i'$, we just need to show that $\dim(D_i') \leq \dim(C_i \cap \pi_i(V))$, for i such that $D \cap A_i \neq \varnothing$.

Fix such an index i, and let $\rho_i : D_i' \longrightarrow C_i \cap \pi_i(V)$ be the restriction of π_i to D_i'. It is well-defined since $\pi_i(D_i') \subseteq \pi_i(V)$ by definition of D, and $\pi_i(D_i') \subseteq C_i$ since $D_i' \subseteq \langle C \cap A_i \rangle$.

Finally, we see that ρ_i is one to one since $D_i' \subseteq \langle C \cap A_i \rangle$ and $D_i' \cap A_j = \varnothing$ for $j > i$, and we are done. □

Proof of Theorem B.5. First observe that $\pi_i(V) \subseteq \mathbb{F}_{q^m}^{n_i}$ is again Galois closed, for $i = 1, 2, \ldots, l$. By definition of GRWs, if $\dim(\pi_i(V)) < d_{R,r_i}(C_i)$, then $\dim(C_i \cap \pi_i(V)) < r_i$, for i such that $r_i > 0$. On the other hand, if $\dim(\pi_i(V)) \leq d_{R,r_i}(C_i)$ and $r_i < k_i$, then by monotonicity of GRWs [13, Lemma 4], it holds that $\dim(\pi_i(V)) < d_{R,r_i+1}(C_i)$, which implies that $\dim(C_i \cap \pi_i(V)) < r_i + 1$, that is, $\dim(C_i \cap \pi_i(V)) \leq r_i$. Finally, if $\dim(\pi_i(V)) \leq d_{R,k_i}(C_i)$, then it is trivial that $\dim(C_i \cap \pi_i(V)) \leq \dim(C_i) = k_i$.

The result follows then from the previous lemma. □

Remark B.31. *In the situation of Corollary B.28, if* $\dim(\pi_i(V)) \leq d_{R,r_i}(C_i)$, *for* $i = 1, 2, \ldots, l$ *and with strict inequality for some* j, *then an eavesdropper that obtains* $\mathbf{c}B^T$, *where* B *generates* V, *gains less than* r *packets of information about the original packets by Equation (B.2).*

Observe that the previous condition implies that $\dim(V) < \sum_{i=1}^{l} d_{R,r_i}(C_i)$. *We know from the bound (B.7) that if* $\dim(V) < \sum_{i=1}^{l} d_{R,s_i}(C_i)$ *for all possible decompositions* $r = \sum_{i=1}^{l} s_i$, *then* $\dim(C \cap V) < r$.

However, many $\mathbb{F}_{q^m}$*-linear Galois closed spaces may satisfy* $\dim(\pi_i(V)) < d_{R,r_i}(C_i)$, *for* $i = 1, 2, \ldots, l$, *and a given decomposition* $r = \sum_{i=1}^{l} r_i$, *but may also satisfy* $\dim(V) \geq \sum_{i=1}^{l} d_{R,s_i}(C_i)$ *for some other decomposition* $r = \sum_{i=1}^{l} s_i$.

Take for instance $V = V_1 \times V_2 \times \cdots \times V_l$, *where* $V_i \subseteq \mathbb{F}_{q^m}^{n_i}$ *are* $\mathbb{F}_{q^m}$*-linear Galois closed spaces satisfying* $\dim(V_i) \leq d_{R,r_i}(C_i)$, *for* $i = 1, 2, \ldots, l$ *and with strict inequality for some* j, *but* $\dim(V) = \sum_{i=1}^{l} \dim(V_i) \geq d_{R,r}(C)$.

Remark B.32. *In the particular case of Corollary B.29, to obtain at least* r *packets of information, it must hold that* $\pi_i(V)$ *is the whole space* $\mathbb{F}_{q^m}^{m}$ *for at least* r *indices* i. *Take for instance* $V = V_1 \times V_2 \times \cdots \times V_k$, *where* $V_i \subsetneq \mathbb{F}_{q^m}^{n}$ *satisfies* $\dim(V_i) =$

$m-1$, for $i = 1, 2, \ldots, k$. In that case, $\dim(V) = k(m-1)$, which is usually much bigger than $d_{R,1}(C) = m$. However, the adversary still obtains no information about the original packets.

7 Related properties of reducible codes

In this section, we study some secondary properties of reducible codes that are related to their GRWs.

7.1 Cartesian product conditions

In this subsection, we gather sufficient and necessary conditions for reducible codes to be rank equivalent to cartesian products (see Section 5 for the definition of rank equivalence).

We start by using Galois closures and generalized rank weights to see whether an $\mathbb{F}_{q^m}$-linear code that can be decomposed as a direct sum of smaller codes is rank equivalent to the cartesian product of these codes. It can be seen as a converse statement to Corollary B.8.

Proposition B.33. *Given an $\mathbb{F}_{q^m}$-linear code $C = C'_1 \oplus C'_2 \oplus \cdots \oplus C'_l \subseteq \mathbb{F}_{q^m}^n$, with $k_i = \dim(C'_i)$, for $i = 1, 2, \ldots, l$, and $k = \dim(C)$, we have that $C^* = C'^*_1 + C'^*_2 + \cdots + C'^*_l$ and the following conditions are equivalent:*

1. *C is rank equivalent to a cartesian product $C_1 \times C_2 \times \cdots \times C_l \subseteq \mathbb{F}_{q^m}^n$, where $C_i \subseteq \mathbb{F}_{q^m}^{n_i}$ is rank equivalent to C'_i, and the equivalence map from C to the product is the product of the equivalence maps from C'_i to C_i.*
2. *$C^* = C'^*_1 \oplus C'^*_2 \oplus \cdots \oplus C'^*_l$.*
3. *$d_{R,k}(C) = d_{R,k_1}(C'_1) + d_{R,k_2}(C'_2) + \cdots + d_{R,k_l}(C'_l)$.*
4. *For all $r = 1, 2, \ldots, k$, it holds that*

$$d_{R,r}(C) = \min\{d_{R,r_1}(C'_1) + d_{R,r_2}(C'_2) + \cdots + d_{R,r_l}(C'_l) \\ \mid r = r_1 + r_2 + \cdots + r_l, 0 \leq r_i \leq k_i\}.$$

Proof. It is trivial that item 1 implies item 4 by Corollary B.8. It is also trivial that item 4 implies item 3, and items 2 and 3 are equivalent since $d_{R,k}(C) = \dim(C^*)$ and $d_{R,k_i}(C'_i) = \dim(C'^*_i)$, for $i = 1, 2, \ldots, l$, by Lemma B.5.

Now we prove that item 2 implies item 1. Define $V_i = C'^*_i$, for $i = 1, 2, \ldots, l$, and $V = C^*$. We may assume that C is not rank degenerate, that is, $V = \mathbb{F}_{q^m}^n$. Therefore, $n = \dim(V)$, $n_i = \dim(V_i)$, for $i = 1, 2, \ldots, l$, and $n = n_1 + n_2 + \cdots + n_l$.

On the other hand, define a vector space isomorphisms $\psi_i : V_i \longrightarrow \mathbb{F}_{q^m}^{n_i}$, for $i = 1, 2, \ldots, l$, by sending a basis of V_i of vectors in $\mathbb{F}_q^n$ to the canonical basis of $\mathbb{F}_{q^m}^{n_i}$. It is a rank equivalence by Lemma B.23. Define $C_i = \psi_i(C_i')$. Therefore, C_i and C_i' are rank equivalent by definition.

Finally, define $\psi : V = V_1 \oplus V_2 \oplus \cdots \oplus V_l \longrightarrow \mathbb{F}_{q^m}^n$ by

$$\psi(\mathbf{c}_1 + \mathbf{c}_2 + \cdots + \mathbf{c}_l) = (\psi_1(\mathbf{c}_1), \psi_2(\mathbf{c}_2), \ldots, \psi_l(\mathbf{c}_l)),$$

where $\mathbf{c}_i \in V_i$, for all $i = 1, 2, \ldots, l$. It holds that ψ maps vectors in $\mathbb{F}_q^n$ to vectors in $\mathbb{F}_q^n$ and is a vector space isomorphism. Hence, it is a rank equivalence by Lemma B.23 and verifies the required conditions. □

Corollary B.34. *With notation as in Subsection 2.5, if C_i is rank equivalent to C_i', for all $i = 1, 2, \ldots, l$, then C is rank equivalent to $C_1 \times C_2 \times \cdots \times C_l$.*

Observe that the previous corollary states that Remark B.13 is actually implied by Corollary B.8.

On the other hand, we may use the column components to see wether $C = C_1 \times C_2 \times \cdots \times C_l$ exactly. The proof is straightforward:

Proposition B.35. *With notation as in Subsection 2.5, the following conditions are equivalent:*

1. *$C = C_1 \times C_2 \times \cdots \times C_l$.*
2. *$C = \widehat{C}$.*
3. *$k_i = \widehat{k}_i$, for all $i = 1, 2, \ldots, l$.*
4. *For each $j = 2, 3, \ldots, l$, the rows in $G_{i,j}$, $1 \leq i \leq j-1$, are contained in the main component C_j.*

7.2 Rank degenerate conditions

Recall the definition of rank degenerate codes from [16, Def. 9]:

Definition B.36 ([16]). An $\mathbb{F}_{q^m}$-linear code $C \subseteq \mathbb{F}_{q^m}^n$ of dimension k is rank degenerate if $d_{R,k}(C) < n$.

In network coding, a code is rank degenerate if it can be applied to a network with strictly less outgoing links from the source node (see [11, 16] for more details).

In this subsection, we study sufficient and necessary conditions for reducible codes to be rank degenerate.

Proposition B.37. *With notation as in Subsection 2.5, it holds that:*

1. *If C is rank degenerate, then there exists an $1 \leq i \leq l$ such that C_i is rank degenerate.*
2. *If there exists an $1 \leq j \leq l$ such that $\widehat{C}_j$ is rank degenerate, then C is rank degenerate.*

Proof. We prove each item separately:

1. It follows from
$$d_{R,k}(C) \geq d_{R,k_1}(C_1) + d_{R,k_2}(C_2) + \cdots + d_{R,k_l}(C_l),$$
which follows from Theorem B.1, and the fact that C has length n and C_i has length n_i, for $i = 1, 2, \ldots, l$.
2. We have that $C \subseteq \widehat{C}$. Hence $C^* \subseteq \widehat{C}^*$ and
$$d_{R,k}(C) = \dim(C^*) \leq \dim(\widehat{C}^*) = d_{R,\widehat{k}}(\widehat{C}),$$
by Lemma B.5, and
$$d_{R,\widehat{k}}(\widehat{C}) = d_{R,\widehat{k}_1}(\widehat{C}_1) + d_{R,\widehat{k}_2}(\widehat{C}_2) + \cdots + d_{R,\widehat{k}_l}(\widehat{C}_l),$$
by Corollary B.8, hence the item follows, using now that $\widehat{C}_j$ has length n_j, for $j = 1, 2, \ldots, l$. □

Corollary B.38. *If $C = C_1 \times C_2 \times \cdots \times C_l$, then C is rank degenerate if and only if there exists an $1 \leq i \leq l$ such that C_i is rank degenerate.*

7.3 Duality and bounds on GRWs

With notation as in Subsection 2.5, it is shown in [9] that the dual of the reducible code C has a generator matrix of the form

$$H = \begin{pmatrix} H_{1,1} & 0 & 0 & \ldots & 0 & 0 \\ H_{2,1} & H_{2,2} & 0 & \ldots & 0 & 0 \\ H_{3,1} & H_{3,2} & H_{3,3} & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ H_{l-1,1} & H_{l-1,2} & H_{l-1,3} & \ldots & H_{l-1,l-1} & 0 \\ H_{l,1} & H_{l,2} & H_{l,3} & \ldots & H_{l,l-1} & H_{l,l} \end{pmatrix},$$

where $H_{i,i}$ is a generator matrix of $C_i^\perp$, for $i = 1, 2, \ldots, l$.

We see that reversing the order of the row blocks does not change the code, and reversing the order of the column blocks gives a rank equivalent code. Hence, denoting by $(C^\perp)'_i$ the subcode of $C^\perp$ generated by the matrix

$$H'_i = (H_{i,1}, \ldots, H_{i,i-1}, H_{i,i}, 0, \ldots, 0),$$

for $i = 1, 2, \dots, l$, we may obtain analogous bounds on the generalized rank weights of $C^\perp$ to those in Theorem B.1. We leave the details to the reader.

An upper bound on the GRW of $C^\perp$ using column components of C that follows from Corollary B.8 is the following:

Proposition B.39. *With notation as in Subsection 2.5, it holds that*

$$\begin{aligned} d_{R,r}(C^\perp) \leq \min\{ & d_{R,\widehat{r}_1}(\widehat{C}_1^\perp) + d_{R,\widehat{r}_2}(\widehat{C}_2^\perp) + \cdots + d_{R,\widehat{r}_l}(\widehat{C}_l^\perp) \\ & \mid r = \widehat{r}_1 + \widehat{r}_2 + \cdots + \widehat{r}_l, 0 \leq \widehat{r}_i \leq \widehat{k}_i \}, \end{aligned} \tag{B.14}$$

for $r = 1, 2, \dots, n - \widehat{k}$ (observe that $n - \widehat{k} \leq n - k$).

Proof. It holds that $C \subseteq \widehat{C}$, hence $\widehat{C}^\perp \subseteq C^\perp$, and the result follows then from Corollary B.8 and the fact that $\widehat{C}^\perp = \widehat{C}_1^\perp \times \widehat{C}_2^\perp \times \cdots \times \widehat{C}_l^\perp$. □

In particular, if $\widehat{k} < n$, it holds that

$$d_{R,1}(C^\perp) \leq \min\{d_{R,1}(\widehat{C}_1^\perp), d_{R,1}(\widehat{C}_2^\perp), \dots, d_{R,1}(\widehat{C}_l^\perp)\}. \tag{B.15}$$

7.4 MRD rank

Recall from [13, Prop. 1] the (classical) Singleton bound on GRWs:

$$d_{R,r}(C) \leq n - k + r, \tag{B.16}$$

for any $\mathbb{F}_{q^m}$-linear code $C \subseteq \mathbb{F}_{q^m}^n$, where $k = \dim(C)$ and $1 \leq r \leq k$. By monotonicity of GRWs [13, Lemma 4], if the r-th weight of C attains the Singleton bound, then the s-th weight of C also attains it, for all $s \geq r$. The minimum of such r is called the MRD rank of the code [6, Def. 1]:

Definition B.40 ([6]). For an $\mathbb{F}_{q^m}$-linear code $C \subseteq \mathbb{F}_{q^m}^n$ of dimension k, we define its MRD rank as the minimum positive integer r such that $d_{R,r}(C) = n - k + r$, and denote it by $r(C)$.

If $d_{R,k}(C) < n$, then we define $r(C) = k + 1$.

Observe that the last part of the previous definition is a redefinition of rank degenerate codes. We have the next characterization of $r(C)$ given in [6, Cor. III.3]:

Lemma B.41 ([6]). *For an $\mathbb{F}_{q^m}$-linear code $C \subseteq \mathbb{F}_{q^m}^n$ of dimension k, it holds that*

$$r(C) = k - d_{R,1}(C^\perp) + 2,$$

defining $d_{R,1}(\{\mathbf{0}\}) = n + 1$ for the case $C = \mathbb{F}_{q^m}^n$.

In particular, from the bounds obtained so far, we derive the following result on the MRD rank of a reducible code:

Proposition B.42. *Let the notation be as in Subsection 2.5. It holds that*

$$k - r(C) \geq \min\{k_1 - r(C_1), k_2 - r(C_2), \ldots, k_l - r(C_l)\} \tag{B.17}$$

and

$$k - r(C) \leq \min\{\widehat{k}_1 - r(\widehat{C}_1), \widehat{k}_2 - r(\widehat{C}_2), \ldots, \widehat{k}_l - r(\widehat{C}_l)\}. \tag{B.18}$$

Moreover, denote by $k_{i,j}$ and $r_{i,j}$ the dimension and MRD rank of the $\mathbb{F}_{q^m}$-linear code with parity check matrix $H_{i,j}$, respectively, with notation as in the previous subsection, for $i = 2, 3, \ldots, l$ and $j = 1, 2, \ldots, i-1$. Then

$$\begin{gathered} k - r(C) \leq \min\{k_i - r(C_i) + \sum_{H_{i,j} \neq 0} (k_{i,j} - r_{i,j} + 2) \\ \mid i = 1, 2, \ldots, l\}. \end{gathered} \tag{B.19}$$

Proof. The bound (B.17) follows from the previous lemma and the bound (B.6). The bound (B.18) follows from the previous lemma and the bound (B.15).

Now we prove the bound (B.19). From the previous lemma and the bound (B.9), we obtain that

$$k - r(C) \leq \min\{d_{R,1}((C^\perp)'_1, (C^\perp)'_2, \ldots, (C^\perp)'_l)\},$$

with notation as in the previous subsection. Now, if $d_{i,j}$ denotes the minimum rank distance of the $\mathbb{F}_{q^m}$-linear code with parity check matrix $H_{i,j}$, it follows that

$$d_{R,1}((C^\perp)'_i) \leq d_{R,1}(C_i^\perp) + \sum_{H_{i,j} \neq 0} d_{i,j},$$

and the result follows again from the previous lemma. □

The MRD rank of the code C in Example B.9 was obtained directly using Theorem B.1. However, it could be directly obtained using the previous proposition.

We conclude with the cartesian product case:

Corollary B.43. *With notation as in the previous proposition, if $C = C_1 \times C_2 \times \cdots \times C_l$, it holds that*

$$k - r(C) = \min\{k_1 - r(C_1), k_2 - r(C_2), \ldots, k_l - r(C_l)\},$$

and all the bounds in the previous proposition are equalities.

7.5 Particular constructions

To conclude, in this subsection we briefly recall some constructions of reducible codes in the literature introduced to improve the minimum Hamming distance of cartesian products of codes, and see when they may give improvements for the rank distance.

Recall the well-known $(\mathbf{u}, \mathbf{u} + \mathbf{v})$-construction by Plotkin [20]. Take $\mathbb{F}_{q^m}$-linear codes $C_1, C_2 \subseteq \mathbb{F}_{q^m}^n$, and define the $\mathbb{F}_{q^m}$-linear code $C \subseteq \mathbb{F}_{q^m}^{2n}$ by

$$C = \{(\mathbf{u}, \mathbf{u} + \mathbf{v}) \mid \mathbf{u} \in C_1, \mathbf{v} \in C_2\}.$$

Denoting by $d_H(D)$ the minimum Hamming distance of a code D, it holds that $d_H(C_1 \times C_2) = \min\{d_H(C_1), d_H(C_2)\}$, whereas $d_H(C) = \min\{2d_H(C_1), d_H(C_2)\}$, hence improving the minimum Hamming distance of the cartesian product if $d_H(C_1) < d_H(C_2)$.

Observe that C is reducible. However, its first row component is obviously rank equivalent to its first main component. By Proposition B.33, C and $C_1 \times C_2$ are rank equivalent. Hence the $(\mathbf{u}, \mathbf{u} + \mathbf{v})$-construction gives nothing but cartesian products for the rank metric.

We may apply the same argument for the so-called matrix-product codes [2], which are a generalization of the previous construction. Let the notation be as in Subsection 2.5, fix a non-singular matrix $A \in \mathbb{F}_{q^m}^{l \times l}$ and assume that $N = n_1 = n_2 = \ldots = n_l$. Define the $\mathbb{F}_{q^m}$-linear code $C = (C_1, C_2, \ldots, C_l)A \subseteq \mathbb{F}_{q^m}^n$ with generator matrix

$$G = \begin{pmatrix} a_{1,1}G_1 & a_{1,2}G_1 & \ldots & a_{1,l}G_1 \\ a_{2,1}G_2 & a_{2,2}G_2 & \ldots & a_{2,l}G_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{l,1}G_l & a_{l,2}G_l & \ldots & a_{l,l}G_l \end{pmatrix}.$$

If A is upper triangular, we see that C is a reducible code. Just as before, if $A \in \mathbb{F}_q^{l \times l}$, then C is rank equivalent to $C_1 \times C_2 \times \cdots \times C_l$, and thus this construction gives nothing but cartesian products.

In the following examples we see that, as an alternative, the $(\mathbf{u}, \alpha\mathbf{u} + \mathbf{v})$-construction, for $\alpha \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$, and $(\mathbf{u}, \mathbf{u}^{[i]} + \mathbf{v})$-construction, for $0 < i < m$, may improve the minimum rank distance of the cartesian product.

Example B.44. Consider $\alpha \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$, $n = 3$, $C_1 \subseteq \mathbb{F}_{q^m}^3$ generated by $(1, 0, 0)$ and $C_2 \subseteq \mathbb{F}_{q^m}^3$ generated by $(0, \alpha, \alpha^{[1]})$ and $(0, \alpha^{[1]}, \alpha^{[2]})$. Let C be the $(\mathbf{u}, \alpha\mathbf{u} + \mathbf{v})$-construction of the codes C_1 and C_2.

It holds that $d_{R,1}(C_1 \times C_2) = 1$, whereas $d_{R,1}(C) = 2$.

Example B.45. Consider $\alpha \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$, $n = 3$, $C_1 \subseteq \mathbb{F}_{q^m}^3$ generated by $(\alpha, 0, 0)$ and $C_2 \subseteq \mathbb{F}_{q^m}^3$ generated by $(0, \alpha, \alpha^{[1]})$ and $(0, \alpha^{[1]}, \alpha^{[2]})$. Let C be the $(\mathbf{u}, \mathbf{u}^{[1]} + \mathbf{v})$-construction of the codes C_1 and C_2.

Again, it holds that $d_{R,1}(C_1 \times C_2) = 1$, whereas $d_{R,1}(C) = 2$.

8 Conclusion and open problems

In this paper, we have studied the security performance of reducible codes in network coding when used in the form of coset coding schemes. We have obtained lower bounds on their generalized rank weights (GRWs) that extend the known lower bound on their minimum rank distance [9] and which give exact values for cartesian products, and we have obtained upper bounds that are always reached for the minimum rank distance and some reduction. We have obtained maximum rank distance (MRD) reducible codes with MRD main components for new parameters, extending the families of MRD codes for $n > m$ considered in [9] and [23].

We have obtained all $\mathbb{F}_{q^m}$-linear codes whose GRWs are all optimal, for all fixed packet and code sizes up to rank equivalence. The given code construction is a cartesian product of full-length one-dimensional Gabidulin codes and has the minimum possible length required by the optimality of their GRWs. As we have shown, these codes do not only have optimal GRWs, but the difference between every two consecutive GRWs is the packet lenght, which is optimal, in constrast with Gabidulin codes, for which this difference is the minimum possible. Thus if the length of the code is big enough or not restricted, then the given construction behaves much better than Gabidulin codes in secure network coding.

Afterwards we have shown that, when using reducible codes, a wire-tapping adversary obtains in many cases less information than that described by their GRWs. In particular, when using MRD reducible codes or those with optimal GRWs for fixed packet and code sizes, the eavesdropper obtains no information about the sent packets even when wire-tapping more links than those allowed by other MRD codes.

Finally, we have studied some secondary related properties of reducible codes: Characterizations to be rank equivalent to cartesian products of codes, characterizations to be rank degenerate, bounds on their dual codes, MRD ranks, and alternative constructions to the well-known $(\mathbf{u}, \mathbf{u}+\mathbf{v})$-construction.

To conclude, we list a few open problems of interest regarding the security behaviour of reducible codes:

1. Find other cases when the bounds in Theorem B.1 are equalities, apart from the cases covered in Corollary B.8 and Proposition B.10.

2. Find new parameters for which reducible codes are MRD, or prove the impossibility that a reducible code is MRD for certain parameters.

3. Prove or disprove the optimality of the codes in Section 5 among $\mathbb{F}_q$-linear codes. We remark here that no sharp bounds such as those in

Lemma B.20 are known for general $\mathbb{F}_q$-linear codes, to the best of our knowledge.

A Uniqueness of reductions

In this appendix, we discuss the uniqueness of the main components, row components and column components of a reducible code (see Subsection 2.5). We will show that the main components remain unchanged by changing the reduction or by rank equivalence, hence the bound (B.7) remains unchanged. However, the row components may change by changing the reduction, and the column components may change by a rank equivalence. Hence the bounds (B.8) and (B.14) may change in those cases. See Proposition B.10, for instance.

Fix a reducible code $C \subseteq \mathbb{F}_{q^m}^n$, with notation as in Subsection 2.5.

Proposition B.46. *Given another reduction $\widehat{\mathcal{R}}$ of C with the same row and column block sizes as $\mathcal{R}$, it holds that the main components and column components of $\widehat{\mathcal{R}}$ and $\mathcal{R}$ are the same, respectively.*

Proof. Let $\widehat{\mathcal{R}} = (\widehat{G}_{i,j})_{1\leq i \leq l}^{i\leq j \leq l}$ and let $\widehat{G}$ be the generator matrix of C given by this reduction. Since the matrices $G_{i,i}$ have full rank, there exist matrices $A_{i,j} \in \mathbb{F}_{q^m}^{k_i \times k_j}$, for $i = 1, 2, \ldots, l$ and $j = i, i+1, \ldots, l$, such that the $k \times k$ matrix

$$A = \begin{pmatrix} A_{1,1} & A_{1,2} & A_{1,3} & \ldots & A_{1,l-1} & A_{1,l} \\ 0 & A_{2,2} & A_{2,3} & \ldots & A_{2,l-1} & A_{2,l} \\ 0 & 0 & A_{3,3} & \ldots & A_{3,l-1} & A_{3,l} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & A_{l-1,l-1} & A_{l-1,l} \\ 0 & 0 & 0 & \ldots & 0 & A_{l,l} \end{pmatrix}$$

satisfies that $\widehat{G} = AG$. Then it holds that $\widehat{G}_{i,i} = A_{i,i}G_{i,i}$, for $i = 1, 2, \ldots, l$, and the main components of both reductions coincide. In addition, it holds that

$$\begin{pmatrix} \widehat{G}_{1,j} \\ \widehat{G}_{2,j} \\ \vdots \\ \widehat{G}_{j,j} \end{pmatrix} = \begin{pmatrix} A_{1,1} & A_{1,2} & \ldots & A_{1,j} \\ 0 & A_{2,2} & \ldots & A_{2,j} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & A_{j,j} \end{pmatrix} \begin{pmatrix} G_{1,j} \\ G_{2,j} \\ \vdots \\ G_{j,j} \end{pmatrix},$$

and the column components of both reductions also coincide. □

Proposition B.47. *Assume that the main components of the reduction $\mathcal{R}$ of C are not rank degenerate. Let $\mathcal{R}'$ be a reduction of an $\mathbb{F}_{q^m}$-linear code C' that is rank* *equivalent to C, with the same row and column block sizes as $\mathcal{R}$, and such that the rank equivalence maps the rows of the generator matrix corresponding to $\mathcal{R}$ to the rows of the generator matrix corresponding to $\mathcal{R}'$. Then the main components and row components of $\mathcal{R}'$ and $\mathcal{R}$ are rank equivalent, respectively.*

Proof. Let $\mathcal{R}' = (G'_{i,j})_{1\leq i\leq l}^{i\leq j\leq l}$ and let G' be the generator matrix of C' given by this reduction. By hypothesis and by Lemma B.23, we may assume that the rank equivalence is given by $\phi(\mathbf{c}) = \mathbf{c}A$, for $\mathbf{c} \in \mathbb{F}_{q^m}^n$, for some $n \times n$ matrix

$$A = \begin{pmatrix} A_{1,1} & A_{1,2} & A_{1,3} & \dots & A_{1,l-1} & A_{1,l} \\ A_{2,1} & A_{2,2} & A_{2,3} & \dots & A_{2,l-1} & A_{2,l} \\ A_{3,1} & A_{3,2} & A_{3,3} & \dots & A_{3,l-1} & A_{3,l} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ A_{l-1,1} & A_{l-1,2} & A_{l-1,3} & \dots & A_{l-1,l-1} & A_{l-1,l} \\ A_{l,1} & A_{l,2} & A_{l,3} & \dots & A_{l,l-1} & A_{l,l} \end{pmatrix},$$

with coefficients in $\mathbb{F}_q$, and such that $G' = GA$. Looking at the generator matrices of the last row components of $\mathcal{R}$ and $\mathcal{R}'$, we see that

$$(0, \dots, 0, G'_{l,l}) = (G_{l,l}A_{l,1}, G_{l,l}A_{l,2}, \dots, G_{l,l}A_{l,l}),$$

which implies that $G_{l,l}A_{l,j} = 0$, for $j = 1, 2, \dots, l-1$. This means that the columns of $A_{l,j}$ are in $C_l^{\perp}$. However, since their coefficients lie in $\mathbb{F}_q$, these columns have rank weight equal to 1.

On the other hand, we are assuming that the main components of $\mathcal{R}$ are not rank degenerate, which in particular means that $d_R(C_l^{\perp}) > 1$ (see [11, Def. 26 and Cor. 28]). Therefore, all the columns in $A_{l,j}$ are the zero vector, that is, $A_{l,j} = 0$, for $j = 1, 2, \dots, l-1$.

If we now look at the generator matrices of the $(l-1)$-th row components of $\mathcal{R}$ and $\mathcal{R}'$, we see that

$$(0, \dots, 0, G'_{l-1,l-1}, G'_{l-1,l}) = (G_{l-1,l-1}A_{l-1,1}, \dots$$
$$G_{l-1,l-1}A_{l-1,l-1}, G_{l-1,l-1}A_{l-1,l} + G_{l-1,l}A_{l,l}),$$

which implies that $G_{l-1,l-1}A_{l-1,j} = 0$, for $j = 1, 2, \dots, l-2$. In the same way as before, we see that this implies that $A_{l-1,j} = 0$, for $j = 1, 2, \dots, l-2$.

Continuing iteratively in this way, we see that $A_{i,j} = 0$, for $i > j$. In other words, we have that A is again of the form

$$A = \begin{pmatrix} A_{1,1} & A_{1,2} & A_{1,3} & \dots & A_{1,l-1} & A_{1,l} \\ 0 & A_{2,2} & A_{2,3} & \dots & A_{2,l-1} & A_{2,l} \\ 0 & 0 & A_{3,3} & \dots & A_{3,l-1} & A_{3,l} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & A_{l-1,l-1} & A_{l-1,l} \\ 0 & 0 & 0 & \dots & 0 & A_{l,l} \end{pmatrix}.$$

As in the proof of Proposition B.46, this implies that the main components and row components of $\mathcal{R}$ and $\mathcal{R}'$ are rank equivalent, respectively. □

Acknowledgement

This work was supported by The Danish Council for Independent Research under Grant No. DFF-4002-00367 and Grant No. DFF-5137-00076B (EliteForsk-Rejsestipendium). The author wishes to thank Olav Geil and Diego Ruano for fruitful discussions and comments. He also wishes to thank the editor and anonymous reviewers for their very helpful comments.

References

[1] R. Ahlswede, N. Cai, S. Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inform. Theory*, vol. 46, no. 4, pp. 1204–1216, Sep 2006.

[2] T. D. Blackmore and G. H. Norton, "Matrix-product codes over $\mathbb{F}_q$," *Applicable Algebra in Engineering, Communications and Computing*, vol. 12, pp. 477–500, 2001.

[3] N. Cai and R. W. Yeung, "Network coding and error correction," in *Proc. 2002 IEEE Information Theory Workshop*, 2002, pp. 119–122.

[4] ——, "Secure network coding," in *Proc. 2002 IEEE International Symposium on Information Theory*, 2002, p. 323.

[5] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *Journal of Combinatorial Theory, Series A*, vol. 25, no. 3, pp. 226–241, 1978.

[6] J. Ducoat, "Generalized rank weights: A duality statement," in *Topics in Finite Fields*, ser. Comtemporary Mathematics, G. L. M. G. Kyureghyan and A. Pott, Eds. American Mathematical Society, 2015, vol. 632, pp. 114–123.

[7] J. Ducoat and F. E. Oggier, "Rank weight hierarchy of some classes of cyclic codes," in *IEEE Information Theory Workshop (ITW), 2014*, 2014, pp. 142–146.

[8] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems Inform. Transmission*, vol. 21, no. 1, pp. 1–12, 1985.

[9] E. M. Gabidulin, A. V. Ourivski, B. Honary, and B. Ammar, "Reducible rank codes and their applications to cryptography," *IEEE Trans. Inform. Theory*, vol. 49, no. 12, pp. 3289–3293, 2003.

[10] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov, "Ideals over a non-commutative ring and their application in cryptology," in *Advances in Cryptology — EUROCRYPT '91*, ser. Lecture Notes in Computer Science, D. W. Davies, Ed. Springer Berlin Heidelberg, 1991, vol. 547, pp. 482–489.

[11] R. Jurrius and R. Pellikaan, "On defining generalized rank weights," *Advances in Mathematics of Communications*, vol. 11, no. 1, pp. 225–235, 2017.

[12] R. Kötter and M. Medard, "An algebraic approach to network coding," *IEEE/ACM Trans. Networking*, vol. 11, no. 5, pp. 782–795, Oct 2003.

[13] J. Kurihara, R. Matsumoto, and T. Uyematsu, "Relative generalized rank weight of linear codes and its applications to network coding," *IEEE Trans. Inform. Theory*, vol. 61, no. 7, pp. 3912–3936, 2015.

[14] S.-Y. Li, R. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inform. Theory*, vol. 49, no. 2, pp. 371–381, Feb 2003.

[15] U. Martínez-Peñas, "Generalized rank weights of reducible codes, optimal cases and related properties," in *2016 IEEE International Symposium on Information Theory (ISIT)*, Jul 2016, pp. 1959–1963.

[16] ——, "On the similarities between generalized rank and Hamming weights and their applications to network coding," *IEEE Trans. Inform. Theory*, vol. 62, no. 7, pp. 4081–4095, Jul 2016.

[17] U. Martínez-Peñas and R. Matsumoto, "Unifying notions of generalized weights for universal security on wire-tap networks," in *Proceedings of the 54th Annual Allerton Conference on Communication, Control, and Computing*, 2016. [Online]. Available: https://arxiv.org/abs/1607.01263

[18] F. E. Oggier and A. Sboui, "On the existence of generalized rank weights," in *Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, October 28-31, 2012*, 2012, pp. 406–410.

[19] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," in *Advances in Cryptology: EUROCRYPT 84*, ser. Lecture Notes in Comput. Sci. Springer Berlin Heidelberg, 1985, vol. 209, pp. 33–50.

[20] M. Plotkin, "Binary codes with specified minimum distance," *IRE Trans. Inform. Theory*, vol. 6, no. 4, pp. 445–450, Sep 1960.

[21] A. Ravagnani, "Generalized weights: An anticode approach," *Journal of Pure and Applied Algebra*, vol. 220, no. 5, pp. 1946–1962, 2016.

[22] D. Silva and F. R. Kschischang, "On metrics for error correction in network coding," *IEEE Trans. Inform. Theory*, vol. 55, no. 12, pp. 5479–5490, 2009.

[23] ——, "Universal secure network coding via rank-metric codes," *IEEE Trans. Inform. Theory*, vol. 57, no. 2, pp. 1124–1135, Feb. 2011.

[24] H. Stichtenoth, "On the dimension of subfield subcodes," *IEEE Trans. Inform. Theory*, vol. 36, no. 1, pp. 90–93, 1990.

[25] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[26] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Inform. Theory*, vol. 48, no. 6, pp. 1250–1276, Jun 2002.

Paper C

Relative generalized matrix weights of matrix codes for universal security on wire-tap networks

Umberto Martínez-Peñas[1] and Ryutaroh Matsumoto[2]

The paper has been submitted to the
IEEE Transactions on Information Theory, 21 pages,
and presented at the
54th Annual Allerton Conference on Communication, Control, and
Computing, Monticello, IL, USA, Oct 2016.

[1] Department of Mathematical Sciences, Aalborg University, Aalborg 9220, Denmark

[2] Department of Information and Communication Engineering, Nagoya University, Nagoya, Japan

The layout has been revised.

Abstract

Universal security over a network with linear network coding has been intensively studied. However, previous linear codes and code pairs used for this purpose were linear over a larger field than that used on the network, which restricts the possible packet lengths of optimal universal secure codes, does not allow to apply known list-decodable rank-metric codes and requires performing operations over a large field. In this work, we introduce new parameters (relative generalized matrix weights and relative dimension/rank support profile) for code pairs that are linear over the field used in the network, and show that they measure the universal security performance of these code pairs. For one code and non-square matrices, generalized matrix weights coincide with the existing Delsarte generalized weights, hence we prove the connection between these latter weights and secure network coding, which was left open. As main applications, the proposed new parameters enable us to: 1) Obtain optimal universal secure linear codes on noiseless networks for all possible packet lengths, in particular for packet lengths not considered before, 2) Obtain the first universal secure list-decodable rank-metric code pairs with polynomial-sized lists, based on a recent construction by Guruswami et al, and 3) Obtain new characterizations of security equivalences of linear codes. Finally, we show that our parameters extend relative generalized Hamming weights and relative dimension/length profile, respectively, and relative generalized rank weights and relative dimension/intersection profile, respectively.

Keywords: Network coding, rank weight, relative dimension/rank support profile, relative generalized matrix weight, universal secure network coding.

1 Introduction

Linear network coding was first studied in [1], [23] and [25], and enables us to realize higher throughput than the conventional storing and forwarding. Error correction in this context was first studied in [5], and security, meaning information leakage to an adversary wire-tapping links in the network, was first considered in [6]. In that work, the authors give outer codes with optimal information rate for the given security performance, although using large fields on the network. The field size was later reduced in [15] by reducing the information rate. In addition, the approach in [14] allows us to see secure network coding as a generalization of secret sharing [4, 37], which is a generalization of the wire-tap channel of type II [33].

However, these approaches [6, 14, 15] require knowing and/or modifying the underlying linear network code, which does not allow us to perform, for instance, random linear network coding [21], which achieves capacity in a decentralized manner and is robust to network changes. Later, the use of pairs of linear (block) codes as outer codes was proposed in [39] to protect messages from errors together with information leakage to a wire-tapping adversary (see Remark C.4), depending only on the number of errors and wire-tapped links, respectively, and not depending on the underlying linear network code, which is referred to as *universal security* in [39].

In [39], the encoded message consists of n (number of outgoing links from the source) vectors in $\mathbb{F}_{q^m}$ or $\mathbb{F}_q^m$, called packets, where m is called the packet length and where $\mathbb{F}_q$ is the field used for the underlying linear network code, as opposed to previous works [6, 14, 15], where $m = 1$. The universal performance of the proposed linear codes in [39] is measured by the rank metric [9], and the authors in [39] prove that linear codes in $\mathbb{F}_{q^m}^n$ with optimal rank-metric parameters when $n \leq m$ [17, 36] are also optimal for universal security. This approach was already proposed in [38, 40] for error correction, again not depending on the underlying network code. Later the authors in [20] obtained the first list-decodable rank-metric codes whose list sizes are polynomial in the code length and which are able to list-decode universally on linearly coded networks roughly twice as many errors as optimal rank-metric codes [17, 36] can correct. The rank metric was then generalized in [24] to relative generalized rank weights (RGRWs) and relative dimension/intersection profiles (RDIPs), which were proven in [24] to measure exactly and simultaneously the universal security performance and error-correction capability of pairs of linear codes, in the same way as relative generalized Hamming weights (RGHWs) and relative dimension/length profiles (RDLPs) [26, 42] do on wire-tap channels of type II.

Unfortunately, the codes studied and proposed in [24, 38–40] for universal security are linear over the extension field $\mathbb{F}_{q^m}$. This restricts the possible packet lengths of optimal universal secure codes, requires performing computations over the larger field $\mathbb{F}_{q^m}$ and leaves out important codes, such as the list-decodable rank-metric codes in [20], which are only linear over $\mathbb{F}_q$.

In this work, we introduce new parameters, called relative generalized matrix weights (RGMWs) and relative dimension/rank support profiles (RDRPs), for codes and code pairs that are linear over the smaller field $\mathbb{F}_q$, and prove that they measure their universal security performance in terms of the worst-case information leakage. As main applications, we obtain the first optimal universal secure linear codes on noiseless networks for all possible packet lengths, we obtain the first universal secure list-decodable rank-metric code pairs with polynomial-sized lists, and obtain new characterizations of security equivalences of linear codes.

1.1 Notation

Let q be a prime power and m and n, two positive integers. We denote by $\mathbb{F}_q$ the finite field with q elements, which we will consider to be the field used

Table C.1: New and existing notions of generalized weights

Work	Paremeters	Codes they are used on	Measured security
Def. C.10 & C.11, & Th. C.1	RGMW & RDRP	$\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$, $\mathbb{F}_q$-linear	Universal security on networks
[24, 32]	RGRW & RDIP	$\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$, $\mathbb{F}_{q^m}$-linear	Universal security on networks
[34]	DGW	$\mathcal{C}_2 = \{0\} \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$, $\mathbb{F}_q$-linear	Universal security on networks for $\mathbb{F}_{q^m}$-linear
[26, 42]	RGHW & RDLP	$\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^n$, $\mathbb{F}_q$-linear	Security on wire-tap channels II
[31, 45]	RNGHW	$\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^n$, $\mathbb{F}_q$-linear	Non-universal security on networks

Table C.2: New and existing optimal secure codes for noiseless networks (N = # links, μ = # observations, t = # destinations)

Work	Universality	Field size (q) used over the network	Packet length (m)
Theorem C.2	Yes	Any	Any
[39]	Yes	Any	$m \geq n$ or $n = lm$
[6]	No	$q > \binom{N}{\mu}$	–
[15]	No	$q = \Theta(N^{\mu/2})$	–
[14]	No	$q > \binom{N-1}{\mu-1} + t$ or $q > \binom{2n^3t^2-1}{\mu-1} + t$	–

for the underlying linear network code (see [23, Definition 1]).

Most of our technical results hold for an arbitrary field, which we denote by $\mathbb{F}$ and which mathematically plays the role of $\mathbb{F}_q$. $\mathbb{F}^n$ denotes the vector space of row vectors of length n with components in $\mathbb{F}$, and $\mathbb{F}^{m \times n}$ denotes the vector space of $m \times n$ matrices with components in $\mathbb{F}$. Throughout the paper, a (block) code in $\mathbb{F}^{m \times n}$ (respectively, in $\mathbb{F}^n$) is a subset of $\mathbb{F}^{m \times n}$ (respectively, of $\mathbb{F}^n$), and it is called linear if it is a vector space over $\mathbb{F}$. In all cases, dimensions of vector spaces over $\mathbb{F}$ will be denoted by dim.

Finally, we recall that we may identify $\mathbb{F}_{q^m}^n$ and $\mathbb{F}_q^{m \times n}$ as vector spaces over $\mathbb{F}_q$. Fix a basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ of $\mathbb{F}_{q^m}$ as a vector space over $\mathbb{F}_q$. We define the *matrix representation map* $M_{\boldsymbol{\alpha}} : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^{m \times n}$ associated to the previous basis by

$$M_{\boldsymbol{\alpha}}(\mathbf{c}) = (c_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n}, \tag{C.1}$$

where $\mathbf{c}_i = (c_{i,1}, c_{i,2}, \ldots, c_{i,n}) \in \mathbb{F}_q^n$, for $i = 1, 2, \ldots, m$, are the unique vectors in $\mathbb{F}_q^n$ such that $\mathbf{c} = \sum_{i=1}^m \alpha_i \mathbf{c}_i$. The map $M_{\boldsymbol{\alpha}} : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^{m \times n}$ is an $\mathbb{F}_q$-linear vector space isomorphism.

The works [24, 38–40] consider $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$, which are a subfamily of $\mathbb{F}_q$-linear codes in $\mathbb{F}_q^{m \times n}$ through the map given in (C.1). In this paper, we will consider arbitrary linear (meaning $\mathbb{F}$-linear) codes in $\mathbb{F}^{m \times n}$.

1.2 Our motivations

Our main motivation to study universal secure network coding is to avoid knowing and/or modifying the underlying linear network code, and in particular be able to apply our theory on random linearly coded networks [21], which achieve capacity in a decentralized manner and are robust to network

Table C.3: New and existing characterizations of linear isomorphisms between vector spaces of matrices preserving certain properties

Work	Domain & codomain	Linearity	Properties preserved
Theorem C.4	$\phi : \mathcal{V} \longrightarrow \mathcal{W}, \mathcal{V}, \mathcal{W} \in \mathrm{RS}$	$\mathbb{F}$-linear	Universal security on networks
[28]	$\phi : \mathcal{V} \longrightarrow \mathcal{W}, \mathcal{V}, \mathcal{W} \in \mathrm{RS}$	$\mathbb{F}_{q^m}$-linear	Ranks & universal security on networks
[3]	$\phi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$	$\mathbb{F}_{q^m}$-linear	Ranks
[27, 30]	$\phi : \mathbb{F}^{m \times n} \longrightarrow \mathbb{F}^{m \times n}$	$\mathbb{F}$-linear	Ranks, determinants & eigenvalues
[10]	$\phi : \mathbb{F}^{n \times n} \longrightarrow \mathbb{F}^{n \times n}$	$\mathbb{F}$-linear	Invertible matrices

changes.

Our main motivation to study pairs of linear codes is to be able to protect messages simultaneously from errors, erasures and information leakage to a wire-tapper. See also Section 2 and more concretely, Remark C.4.

Our main motivations to study codes which are linear over the base field $\mathbb{F}_q$ instead of the extension field $\mathbb{F}_{q^m}$ are the following:

1) $\mathbb{F}_q$-linear codes with optimal rank-metric parameters [9], and thus with optimal universal security and error-correction capability, cannot be $\mathbb{F}_{q^m}$-linear for most packet lengths m when $m < n$. In many applications, packet lengths satisfying $m < n$ are required (see the discussion in [24, Subsection I-A], for instance).

2) The only known list-decodable rank-metric codes [20] with polynomial-sized lists are linear over $\mathbb{F}_q$, but not over $\mathbb{F}_{q^m}$. Hence the previous studies on universal security cannot be applied on these codes. In particular, no construction of universal secure list-decodable rank-metric coding schemes with polynomial-sized lists are known.

3) In previous works [38–40], the proposed codes are $\mathbb{F}_{q^m}$-linear and $m \geq n$. In many cases, this requires performing operations over a very large field, instead of the much smaller field $\mathbb{F}_q$.

1.3 Related works and considered open problems

We consider the following four open problems in the literature, which correspond to the main four contributions listed in the following subsection:

1) Several parameters have been introduced to measure the security performance of linear codes and code pairs on different channels, in terms of the worst-case information leakage. The original RGHWs and RDLPs [26, 42] measure security performance over wire-tap channels of type II, and relative network generalized Hamming weigths (RNGHWs) [31, 45] measure security performance over networks depending on the underlying linear network code (non-universal security). Later, RGRWs and RDIPs were introduced in [24, 32] to measure universal security performance of $\mathbb{F}_{q^m}$-linear code pairs $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$. A notion of generalized weight for one $\mathbb{F}_q$-linear code (that is, for an arbitrary $\mathcal{C}_1$ and for $\mathcal{C}_2 = \{0\}$) in $\mathbb{F}_q^{m \times n}$, called Delsarte generalized

weights (DGWs), was introduced in [34], but its connection with universal security was only given for $\mathbb{F}_{q^m}$-linear codes. Thus, no measure of universal security performance for all $\mathbb{F}_q$-linear codes or code pairs is known. See also Table C.1.

2) The first optimal universal secure linear codes for noiseless networks were obtained in [39, Section V], whose information rate attain the information-theoretical limit given in [6]. However, these codes only exist when $m \geq n$. The cartesian products in [39, Subsection VII-C] are also optimal among $\mathbb{F}_q$-linear codes (see Remark C.22), but only exist when m divides n. No optimal universal secure $\mathbb{F}_q$-linear codes for noiseless networks have been obtained for the rest of values of m. See also Table C.2 for an overview of existing optimal constructions, including non-universal codes [6, 14, 15].

3) In [20], the authors introduce the first list-decodable rank-metric codes in $\mathbb{F}_{q^m}^n$ able to list-decode close to the information-theoretical limit and roughly twice as many errors as optimal rank-metric codes [17, 36] are able to correct, in polynomial time and with polynomial-sized lists (on the length n). However, no universal secure coding schemes with such list-decoding capabilities are known. Observe that list-decoding rank errors implies list-decoding errors in linear network coding in a universal manner [38].

4) Several characterizations of maps between vector spaces of matrices preserving certain properties have been given in the literature [3, 10, 27, 28, 30]. The maps considered in [3] are linear over the extension field $\mathbb{F}_{q^m}$ and preserve ranks, and the maps considered in [10, 27, 30] are linear over the base field ($\mathbb{F}_q$ or an arbitrary field) and preserve fundamental properties of matrices, such as ranks, determinants, eigenvalues or invertible matrices. Characterizations of maps preserving universal security performance were first given in [28], although the considered maps were only linear over $\mathbb{F}_{q^m}$. No characterizations of general $\mathbb{F}_q$-linear maps preserving universal security are known. See also Table C.3.

1.4 Our contributions and main results

In the following, we list our four main contributions together with our main result summarizing each of them. Each contribution tackles each open problem listed in the previous subsection, respectively.

1) We introduce new parameters, RGMWs and RDRPs, in Definitions C.10 and C.11, respectively, which measure the universal security performance of $\mathbb{F}_q$-linear code pairs $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$, in terms of the worst-case information leakage. The main result is Theorem C.1 and states the following: The r-th RGMW of the code pair is the minimum number of links that an adversary needs to wire-tap in order to obtain at least r bits of information (multiplied by $\log_2(q)$) about the sent message. The μ-th RDRP of the code pair is the maximum number of bits of information (multiplied by $\log_2(q)$) about the

sent message that can be obtained by wire-tapping μ links of the network.

Since $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$ are also $\mathbb{F}_q$-linear codes in $\mathbb{F}_q^{m \times n}$, RGMWs and RDRPs must coincide with RGRWs and RDIPs [24], respectively, for $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$, which we prove in Theorem C.7.

When $\mathcal{C}_2 = \{0\}$ and $m \neq n$, we will also show in Theorem C.9 that the RGMWs of the pair coincide with their DGWs, given in [34], hence proving the connection between DGWs and universal security for general $\mathbb{F}_q$-linear codes, which was left open.

2) We obtain optimal universal secure $\mathbb{F}_q$-linear codes for noiseless networks for any value of m and n, not only when $m \geq n$ or m divides n, as in previous works [39]. The main result is Theorem C.2, which states the following: Denote by ℓ the number of packets in $\mathbb{F}_q^m$ that the source can transmit and by t the number of links the adversary may wire-tap without obtaining any information about the sent packets. For any m and n, and a fixed value of ℓ (respectively t), we obtain a coding scheme with optimal value of t (respectively ℓ).

3) We obtain the first universal secure list-decodable rank-metric code pairs with polynomial-sized lists. The main result is Theorem C.3, and states the following: Defining ℓ and t as in the previous item, assuming that n divides m, and fixing $1 \leq k_2 < k_2 \leq n$, $\varepsilon > 0$ and a positive integer s such that $4sn \leq \varepsilon m$ and $m/n = \mathcal{O}(s/\varepsilon)$, we obtain an $\mathbb{F}_q$-linear code pair such that $\ell \geq m(k_1 - k_2)(1 - 2\varepsilon)$, $t \geq k_2$ and which can list-decode $\frac{s}{s+1}(n - k_1)$ rank errors in polynomial time, where the list size is $q^{\mathcal{O}(s^2/\varepsilon^2)}$.

4) We obtain characterizations of vector space isomorphisms between certain spaces of matrices over $\mathbb{F}_q$ that preserve universal security performance over networks. The main result is Theorem C.4, which gives several characterizations of $\mathbb{F}_q$-linear vector space isomorphisms $\phi : \mathcal{V} \longrightarrow \mathcal{W}$, where $\mathcal{V}$ and $\mathcal{W}$ are rank support spaces in $\mathbb{F}_q^{m \times n}$ and $\mathbb{F}_q^{m \times n'}$ (see Definition C.7), respectively.

As application, we obtain in Subsection 6.2 ranges of possible parameters m and n that given linear codes and code pairs can be applied to without changing their universal security performance.

1.5 Organization of the paper

First, all of our main results are stated as *Theorems*. After some preliminaries in Section II, we introduce in Section III the new parameters of linear code pairs (RGMWs and RDRPs), give their connection with the rank metric, and prove that they exactly measure the worst-case information leakage universally on networks (Theorem C.1). In Section IV, we give optimal universal secure linear codes for noiseless networks for all possible parameters (Theorem C.2). In Section V, we show how to add universal security to the list-decodable rank-metric codes in [20] (Theorem C.3). In Section VI, we define and give characterizations of security equivalences of linear codes (Theorem C.4), and then obtain ranges of possible parameters of linear codes up to these equivalences. In Section VII, we give upper and lower Singleton-type bounds (Theorems C.5 and C.6) and study when they can be attained, when the dimensions are divisible by m. Finally, in Section VIII, we prove that RGMWs extend RGRWs [24] and RGHWs [26, 42], and we prove that RDRPs extend RDIPs [24] and RDLPs [16, 26] (Theorems C.7 and C.8, respectively). We conclude the section by showing that GMWs coincide with DGWs [34] for non-square matrices, and are strictly larger otherwise (Theorem C.9).

2 Coset coding schemes for universal security in linear network coding

This section serves as a brief summary of the model of linear network coding that we consider (Subsection 2.1), the concept of universal security under this model (Subsection 2.2) and the main definitions concerning coset coding schemes used for this purpose (Subsection 2.3). The section only contains definitions and facts known in the literature, which will be used throughout the paper.

2.1 Linear network coding model

Consider a network with several sources and several sinks. A given source transmits a message $\mathbf{x} \in \mathbb{F}_q^\ell$ through the network to multiple sinks. To that end, that source encodes the message as a collection of n packets of length m, seen as a matrix $C \in \mathbb{F}_q^{m \times n}$, where n is the number of outgoing links from this source. We consider linear network coding on the network, first considered in [1, 25] and formally defined in [23, Definition 1], which allows us to reach higher throughput than just storing and forwarding on the network. This means that a given sink receives a matrix of the form

$$Y = CA^T \in \mathbb{F}_q^{m \times N},$$

where $A \in \mathbb{F}_q^{N \times n}$ is called the transfer matrix corresponding to the considered source and sink, and A^T denotes its transpose. This matrix may be randomly chosen if random linear network coding is applied [21].

2.2 Universal secure communication over networks

In secure and reliable network coding, two of the main problems addressed in the literature are the following:

1. Error and erasure correction [5, 24, 38–40]: An adversary and/or a noisy channel may introduce errors on some links of the network and/or modify the transfer matrix. In this case, the sink receives the matrix

$$Y = CA'^T + E \in \mathbb{F}_q^{m \times N},$$

   where $A' \in \mathbb{F}_q^{N \times n}$ is the modified transfer matrix, and $E \in \mathbb{F}_q^{m \times N}$ is the final error matrix. In this case, we say that $t = \mathrm{Rk}(E)$ errors and $\rho = n - \mathrm{Rk}(A')$ erasures occurred, where Rk denotes the rank of a matrix.

2. Information leakage [6, 14, 15, 24, 39]: A wire-tapping adversary listens to $\mu > 0$ links of the network, obtaining a matrix of the form $CB^T \in \mathbb{F}_q^{m \times \mu}$, for some matrix $B \in \mathbb{F}_q^{\mu \times n}$.

Outer coding in the source node is usually applied to tackle the previous problems, and it is called *universal secure* [39] if it provides reliability and security as in the previous items for fixed numbers of wire-tapped links μ, errors t and erasures ρ, independently of the transfer matrix A used. This implies that no previous knowledge or modification of the transfer matrix is required and random linear network coding [21] may be applied.

2.3 Coset coding schemes for outer codes

Coding techniques for protecting messages simultaneously from errors and information leakage to a wire-tapping adversary were first studied by Wyner in [43]. In [43, p. 1374], the general concept of coset coding scheme, as we will next define, was first introduced for this purpose. We use the formal definition in [24, Definition 7]:

Definition C.1 (Coset coding schemes [24, 43]). A coset coding scheme over the field $\mathbb{F}$ with message set $\mathcal{S}$ is a family of disjoint nonempty subsets of $\mathbb{F}^{m \times n}$, $\mathcal{P}_\mathcal{S} = \{\mathcal{C}_\mathbf{x}\}_{\mathbf{x} \in \mathcal{S}}$.

If $\mathbb{F} = \mathbb{F}_q$, each $\mathbf{x} \in \mathcal{S}$ is encoded by the source by choosing uniformly at random an element $C \in \mathcal{C}_\mathbf{x}$.

Definition C.2 (Linear coset coding schemes [28, Definition 2]). A coset coding scheme as in the previous definition is said to be linear if $\mathcal{S} = \mathbb{F}^\ell$, for some $0 < \ell \leq mn$, and

$$a\mathcal{C}_\mathbf{x} + b\mathcal{C}_\mathbf{y} \subseteq \mathcal{C}_{a\mathbf{x}+b\mathbf{y}},$$

for all $a, b \in \mathbb{F}$ and all $\mathbf{x}, \mathbf{y} \in \mathbb{F}^\ell$.

With these definitions, the concept of coset coding scheme generalizes the concept of (block) code, since a code is a coset coding scheme where $|\mathcal{C}_\mathbf{x}| = 1$, for each $\mathbf{x} \in \mathcal{S}$. In the same way, linear coset coding schemes generalize linear (block) codes.

An equivalent way to describe linear coset coding schemes is by nested linear code pairs, introduced in [44, Section III.A]. We use the description in [7, Subsection 4.2].

Definition C.3 (Nested linear code pairs [7, 44]). A nested linear code pair is a pair of linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$. Choose a vector space $\mathcal{W}$ such that $\mathcal{C}_1 = \mathcal{C}_2 \oplus \mathcal{W}$, where $\oplus$ denotes the direct sum of vector spaces, and a vector space isomorphism $\psi : \mathbb{F}^{\ell} \longrightarrow \mathcal{W}$, where $\ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$. Then we define $\mathcal{C}_{\mathbf{x}} = \psi(\mathbf{x}) + \mathcal{C}_2$, for $\mathbf{x} \in \mathbb{F}^{\ell}$. They form a linear coset coding scheme called nested coset coding scheme [24].

Remark C.4. *As observed in [33] for the wire-tap channel of type II, linear code pairs where $\mathcal{C}_1 = \mathbb{F}^{m \times n}$ are suitable for protecting information from leakage on noiseless channels. Analogously, linear code pairs where $\mathcal{C}_2 = \{0\}$ are suitable for error correction without the presence of eavesdroppers. Observe that these two types of linear code pairs are dual to each other (see Definition C.15 and Appendix A): If $\mathcal{C}_1^{\prime} = \mathcal{C}_2^{\perp}$ and $\mathcal{C}_2^{\prime} = \mathcal{C}_1^{\perp}$, then $\mathcal{C}_1 = \mathbb{F}^{m \times n}$ if, and only if, $\mathcal{C}_2^{\prime} = \{0\}$. To treat both error correction and information leakage, we need general linear coset coding schemes.*

We recall here that the concept of linear coset coding schemes and nested coset coding schemes are exactly the same. An object in the first family uniquely defines an object in the second family and vice-versa. This is formally proven in [28, Proposition 1].

Finally, we recall that the exact universal error and erasure correction capability of a nested coset coding scheme was found, in terms of the rank metric, first in [38, Section IV.C] for the case of one code ($\mathcal{C}_2 = \{0\}$) that is maximum rank distance, then in [39, Theorem 2] for the general case of one linear code (again $\mathcal{C}_2 = \{0\}$), then in [24, Theorem 4] for the case where both codes are linear over an extension field $\mathbb{F}_{q^m}$, and finally in [28, Theorem 9] for arbitrary coset coding schemes (linear over $\mathbb{F}_q$ and non-linear).

3 New parameters of linear coset coding schemes for universal security on networks

This is the main section of the paper, which serves as a basis for the rest of sections. The next sections can be read independently of each other, but all of them build on the results in this section. Here we introduce rank support spaces (Subsection 3.1), which are the main technical building blocks of our theory, then we define of our main parameters and connect them with the rank metric (Subsection 3.2), and we conclude by showing (Theorem C.1) that these parameters measure the worst-case information leakage universally on linearly coded networks (Subsection 3.3).

3.1 Rank supports and rank support spaces

In this subsection, we introduce rank support spaces, which are the mathematical building blocks of our theory. The idea is to attach to each linear code its rank support, given in [22, Definition 1], and based on this rank support, define a vector space of matrices containing the original code that can be seen as its ambient space with respect to the rank metric.

We remark here that the family of rank support spaces can be seen as the family of vector spaces in [35, Notation 25] after transposition of matrices, or the family of vector spaces in [22, Definition 6] taking $\mathcal{C} = \mathbb{F}_q^{m \times n}$. We start with the definitions:

Definition C.5 (Row space and rank). For a matrix $C \in \mathbb{F}^{m \times n}$, we define its row space $\mathrm{Row}(C)$ as the vector space in $\mathbb{F}^n$ generated by its rows. As usual, we define its rank as $\mathrm{Rk}(C) = \dim(\mathrm{Row}(C))$.

Definition C.6 (Rank support and rank weight [22, Definition 1]). Given a vector space $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$, we define its rank support as

$$\mathrm{RSupp}(\mathcal{C}) = \sum_{C \in \mathcal{C}} \mathrm{Row}(C) \subseteq \mathbb{F}^n.$$

We also define the rank weight of the space $\mathcal{C}$ as

$$\mathrm{wt_R}(\mathcal{C}) = \dim(\mathrm{RSupp}(\mathcal{C})).$$

Observe that $\mathrm{RSupp}(\langle\{C\}\rangle) = \mathrm{Row}(C)$ and $\mathrm{wt_R}(\langle\{C\}\rangle) = \mathrm{Rk}(C)$, for every matrix $C \in \mathbb{F}^{m \times n}$, where $\langle \mathcal{A} \rangle$ denotes the vector space generated by a set $\mathcal{A}$ over $\mathbb{F}$.

Definition C.7 (Rank support spaces). Given a vector space $\mathcal{L} \subseteq \mathbb{F}^n$, we define its rank support space $\mathcal{V}_\mathcal{L} \subseteq \mathbb{F}^{m \times n}$ as

$$\mathcal{V}_\mathcal{L} = \{V \in \mathbb{F}^{m \times n} \mid \mathrm{Row}(V) \subseteq \mathcal{L}\}.$$

We denote by $RS(\mathbb{F}^{m \times n})$ the family of rank support spaces in $\mathbb{F}^{m \times n}$.

The following lemma shows that rank support spaces behave as a sort of ambient spaces for linear codes and can be attached bijectively to vector spaces in $\mathbb{F}^n$, which correspond to the rank supports of the original linear codes.

Lemma C.8. *Let $\mathcal{L} \subseteq \mathbb{F}^n$ be a vector space. The following hold:*

1. *$\mathcal{V}_{\mathcal{L}}$ is a vector space and the correspondence $\mathcal{L} \mapsto \mathcal{V}_{\mathcal{L}}$ between subspaces of $\mathbb{F}^n$ and rank support spaces is a bijection with inverse $\mathcal{V}_{\mathcal{L}} \mapsto \mathrm{RSupp}(\mathcal{V}_{\mathcal{L}}) = \mathcal{L}$.*
2. *If $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$ is a vector space and $\mathcal{L} = \mathrm{RSupp}(\mathcal{C})$, then $\mathcal{V}_{\mathcal{L}}$ is the smallest rank support space containing $\mathcal{C}$.*

We conclude the subsection with the following characterizations of rank support spaces, which we will use throughout the paper. In particular, item 2 will be useful to prove Theorem C.4, and item 3 will be useful to prove Theorem C.1.

Proposition C.9. *Fix a set $\mathcal{V} \subseteq \mathbb{F}^{m \times n}$. The following are equivalent:*

1. *$\mathcal{V}$ is a rank support space. That is, there exists a subspace $\mathcal{L} \subseteq \mathbb{F}^n$ such that $\mathcal{V} = \mathcal{V}_{\mathcal{L}}$.*
2. *$\mathcal{V}$ is linear and has a basis of the form $B_{i,j}$, for $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, k$, where there are vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{F}^n$ such that $B_{i,j}$ has the vector $\mathbf{b}_j$ in the i-th row and the rest of its rows are zero vectors.*
3. *There exists a matrix $B \in \mathbb{F}^{\mu \times n}$, for some positive integer μ, such that*

$$\mathcal{V} = \{V \in \mathbb{F}^{m \times n} \mid VB^T = 0\}.$$

In addition, the relation between items 1, 2 and 3 is that $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ are a basis of $\mathcal{L}$, B is a (possibly not full-rank) parity check matrix of $\mathcal{L}$ and $\dim(\mathcal{L}) = n - \mathrm{Rk}(B)$.

In particular, it holds that

$$\dim(\mathcal{V}_{\mathcal{L}}) = m \dim(\mathcal{L}). \tag{C.2}$$

Proof. We prove the following implications:

- 1 $\Longleftrightarrow$ 2: Assume item 1, let $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ be a basis of $\mathcal{L}$, and let $B_{i,j}$ be as in item 2. Then we see that $\mathcal{V} = \langle \{B_{i,j} \mid 1 \leq i \leq m, 1 \leq j \leq k\} \rangle$. The reversed implication follows in the same way by defining $\mathcal{L} = \langle \mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \rangle \subseteq \mathbb{F}^n$.
- 1 $\Longleftrightarrow$ 3: Assume item 1 and let $B \in \mathbb{F}^{\mu \times n}$ be a parity check matrix of $\mathcal{L}$. That is, a generator matrix of the dual $\mathcal{L}^\perp \subseteq \mathbb{F}^n$. Then it holds by definition that $V \in \mathbb{F}^{m \times n}$ has all its rows in $\mathcal{L}$ if, and only if, $VB^T = 0$. Conversely, assuming item 3 and defining $\mathcal{L}$ as the code with parity check matrix B, we see that $\mathcal{V} = \mathcal{V}_{\mathcal{L}}$ by the same argument. Hence the result follows. □

3.2 Definition and basic properties of the new parameters

Definition C.10 (Relative Generalized Matrix Weight). Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$, and $1 \leq r \leq \ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$, we define their r-th relative generalized matrix weight (RGMW) as

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) = \min\{ \dim(\mathcal{L}) \mid \mathcal{L} \subseteq \mathbb{F}^n, \\ \dim(\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}}) - \dim(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}}) \geq r \}.$$

For a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$, and $1 \leq r \leq \dim(\mathcal{C})$, we define its r-th generalized matrix weight (GMW) as

$$d_{M,r}(\mathcal{C}) = d_{M,r}(\mathcal{C}, \{0\}). \tag{C.3}$$

Observe that it holds that

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \geq d_{M,r}(\mathcal{C}_1), \tag{C.4}$$

for all nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$, and all $1 \leq r \leq \ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$.

Definition C.11 (Relative Dimension/Rank support Profile). Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$, and $0 \leq \mu \leq n$, we define their μ-th relative dimension/rank support profile (RDRP) as

$$K_{M,\mu}(\mathcal{C}_1, \mathcal{C}_2) = \max\{ \dim(\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}}) - \dim(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}}) \mid \\ \mathcal{L} \subseteq \mathbb{F}^n, \dim(\mathcal{L}) \leq \mu \}.$$

Now, if $\mathcal{U} \subseteq \mathcal{V} \subseteq \mathbb{F}^{m \times n}$ are vector spaces, the natural linear map $\mathcal{C}_1 \cap \mathcal{U} / \mathcal{C}_2 \cap \mathcal{U} \longrightarrow \mathcal{C}_1 \cap \mathcal{V} / \mathcal{C}_2 \cap \mathcal{V}$ is one to one. Therefore, since we are taking maximums, it holds that

$$K_{M,\mu}(\mathcal{C}_1, \mathcal{C}_2) = \max\{ \dim(\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}}) - \dim(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}}) \mid \\ \mathcal{L} \subseteq \mathbb{F}^n, \dim(\mathcal{L}) = \mu \}.$$

We remark here that some existing notions of relative generalized weights from the literature are particular cases of RGMWs. The corresponding connections are given in Section 8. In particular, GMWs of one linear code coincide with DGWs (introduced in [34]) for non-square matrices.

We next obtain the following characterization of RGMWs that gives an analogous description to the original definition of GHWs by Wei [42]:

Proposition C.12. *Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$, and an integer $1 \leq r \leq \dim(\mathcal{C}_1/\mathcal{C}_2)$, it holds that*

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) = \min\{ \mathrm{wt_R}(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C}_1, \mathcal{D} \cap \mathcal{C}_2 = \{0\}, \\ \dim(\mathcal{D}) = r \}.$$

Proof. Denote by d_r the number on the left-hand side and by d'_r the number on the right-hand side. We prove both inequalities:

$d_r \leq d'_r$: Take a vector space $\mathcal{D} \subseteq \mathcal{C}_1$ such that $\mathcal{D} \cap \mathcal{C}_2 = \{0\}$, $\dim(\mathcal{D}) = r$ and $\mathrm{wt}_{\mathrm{R}}(\mathcal{D}) = d'_r$. Define $\mathcal{L} = \mathrm{RSupp}(\mathcal{D})$.

Since $\mathcal{D} \subseteq \mathcal{V}_{\mathcal{L}}$, we have that $\dim((\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}})/(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}})) \geq \dim((\mathcal{C}_1 \cap \mathcal{D})/(\mathcal{C}_2 \cap \mathcal{D})) = \dim(\mathcal{D}) = r$. Hence

$$d_r \leq \dim(\mathcal{L}) = \mathrm{wt}_{\mathrm{R}}(\mathcal{D}) = d'_r.$$

$d_r \geq d'_r$: Take a vector space $\mathcal{L} \subseteq \mathbb{F}^n$ such that $\dim((\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}})/(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}})) \geq r$ and $\dim(\mathcal{L}) = d_r$.

There exists a vector space $\mathcal{D} \subseteq \mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}}$ with $\mathcal{D} \cap \mathcal{C}_2 = \{0\}$ and $\dim(\mathcal{D}) = r$. We have that $\mathrm{RSupp}(\mathcal{D}) \subseteq \mathcal{L}$, since $\mathcal{D} \subseteq \mathcal{V}_{\mathcal{L}}$, and hence

$$d_r = \dim(\mathcal{L}) \geq \mathrm{wt}_{\mathrm{R}}(\mathcal{D}) \geq d'_r.$$

Thanks to this characterization, we may connect RGMWs with the rank distance [9]. This will be crucial in the next section, where we will use maximum rank distance codes from [9] to obtain optimal universal secure linear codes for noiseless networks. Recall the definition of minimum rank distance of a linear coset coding scheme, which is a particular case of [28, Equation (1)], and which is based on the analogous concept for the Hamming metric given in [13]:

$$d_R(\mathcal{C}_1, \mathcal{C}_2) = \min\{\mathrm{Rk}(C) \mid C \in \mathcal{C}_1, C \notin \mathcal{C}_2\}. \tag{C.5}$$

The following result follows from the previous theorem and the definitions:

Corollary C.13 (Minimum rank distance of linear coset coding schemes). *Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$, it holds that*

$$d_R(\mathcal{C}_1, \mathcal{C}_2) = d_{M,1}(\mathcal{C}_1, \mathcal{C}_2).$$

By Theorem C.9, the previous corollary coincides with item 1 in [34, Theorem 30] when $\mathcal{C}_2 = \{0\}$ and $m \neq n$.

We conclude by showing the connection between RDRPs and RGMWs:

Proposition C.14 (Connection between RDRPs and RGMWs). *Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$ and $1 \leq r \leq \dim(\mathcal{C}_1/\mathcal{C}_2)$, it holds that*

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) = \min\{\mu \mid K_{M,\mu}(\mathcal{C}_1, \mathcal{C}_2) \geq r\}.$$

Proof. It is proven as [24, Proof of Lemma 4]. □

3.3 Measuring information leakage on networks

In this subsection, we show how the introduced parameters (RGMWs and RDRPs) measure the universal security performance of nested linear code pairs.

Assume that a given source wants to convey the message $\mathbf{x} \in \mathbb{F}_q^\ell$, which we assume is a random variable with uniform distribution over $\mathbb{F}_q^\ell$. Following Subsection 2.3, the source encodes $\mathbf{x}$ into a matrix $C \in \mathbb{F}_q^{m \times n}$ using nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$. We also assume that the distributions used in the encoding are all uniform (see Subsection 2.3).

According to the information leakage model in Subsection 2.2, item 2, a wire-tapping adversary obtains $CB^T \in \mathbb{F}_q^{m \times \mu}$, for some matrix $B \in \mathbb{F}_q^{\mu \times n}$.

Recall from [8] the definition of mutual information of two random variables X and Y:

$$I(X;Y) = H(Y) - H(Y \mid X), \tag{C.6}$$

where $H(Y)$ denotes the entropy of Y and $H(Y \mid X)$ denotes the conditional entropy of Y given X, and where we take logarithms with base q (see [8] for more details).

We will need to use the concept of duality with respect to the Hilbert-Schmidt or trace product. In Appendix A, we collect some basic properties of duality of linear codes. We now give the main definitions:

Definition C.15 (Hilbert-Schmidt or trace product). Given matrices $C, D \in \mathbb{F}^{m \times n}$, we define its Hilbert-Schmidt product, or trace product, as

$$\begin{aligned} \langle C, D \rangle &= \mathrm{Trace}(CD^T) \\ &= \sum_{i=1}^{m} \mathbf{c}_i \cdot \mathbf{d}_i = \sum_{i=1}^{m} \sum_{j=1}^{n} c_{i,j} d_{i,j} \in \mathbb{F}, \end{aligned}$$

where $\mathbf{c}_i$ and $\mathbf{d}_i$ are the rows of C and D, respectively, and where $c_{i,j}$ and $d_{i,j}$ are their components, respectively.

Given a vector space $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$, we denote by $\mathcal{C}^\perp$ its dual:

$$\mathcal{C}^\perp = \{ D \in \mathbb{F}^{m \times n} \mid \langle C, D \rangle = 0, \forall C \in \mathcal{C} \}.$$

We first compute the mutual information of the message and the wire-tapper's observation via rank support spaces:

Proposition C.16. *Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$, a matrix $B \in \mathbb{F}_q^{\mu \times n}$, and the uniform random variables $\mathbf{x}$ and CB^T, as in the beginning of this subsection, it holds that*

$$I(\mathbf{x}; CB^T) = \dim(\mathcal{C}_2^\perp \cap \mathcal{V}_\mathcal{L}) - \dim(\mathcal{C}_1^\perp \cap \mathcal{V}_\mathcal{L}), \tag{C.7}$$

where $I(\mathbf{x}; CB^T)$ is as in (C.6), and where $\mathcal{L} = \mathrm{Row}(B)$.

Proof. Define the map $f : \mathbb{F}_q^{m \times n} \longrightarrow \mathbb{F}_q^{m \times \mu}$ given by

$$f(D) = DB^T,$$

for the matrix $B \in \mathbb{F}_q^{\mu \times n}$. Observe that f is a linear map. It follows that

$$\begin{aligned} H(CB^T) = H(f(C)) = \log_q(|f(\mathcal{C}_1)|) = \dim(f(\mathcal{C}_1)) \\ = \dim(\mathcal{C}_1) - \dim(\ker(f) \cap \mathcal{C}_1), \end{aligned}$$

where the last equality is the well-known first isomorphism theorem. On the other hand, we may similarly compute the conditional entropy:

$$\begin{aligned} H(CB^T \mid \mathbf{x}) = H(f(C) \mid \mathbf{x}) = \log_q(|f(\mathcal{C}_2)|) = \dim(f(\mathcal{C}_2)) \\ = \dim(\mathcal{C}_2) - \dim(\ker(f) \cap \mathcal{C}_2). \end{aligned}$$

However, it holds that $\ker(f) = \mathcal{V}_{\mathcal{L}^\perp} \subseteq \mathbb{F}_q^{m \times n}$ by Proposition C.9, since B is a parity check matrix of $\mathcal{L}^\perp$. Therefore

$$\begin{aligned} I(\mathbf{x}; CB^T) = H(CB^T) - H(CB^T \mid \mathbf{x}) \\ = (\dim(\mathcal{C}_1) - \dim(\mathcal{V}_{\mathcal{L}^\perp} \cap \mathcal{C}_1)) - (\dim(\mathcal{C}_2) - \dim(\mathcal{V}_{\mathcal{L}^\perp} \cap \mathcal{C}_2)). \end{aligned}$$

Finally, the result follows by Lemmas C.64 and C.65 in Appendix A. □

The following theorem follows from the previous proposition, Corollary C.13 and the definitions:

Theorem C.1 (Worst-case information leakage). *Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$, and integers $0 \leq \mu \leq n$ and $1 \leq r \leq \dim(\mathcal{C}_1/\mathcal{C}_2)$, it holds that*

1. *$\mu = d_{M,r}(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp)$ is the minimum number of links that an adversary needs to wire-tap in order to obtain at least r units of information (number of bits multiplied by $\log_2(q)$) of the sent message.*
2. *$r = K_{M,\mu}(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp)$ is the maximum information (number of bits multiplied by $\log_2(q)$) about the sent message that can be obtained by wire-tapping at most μ links of the network.*

In particular, $t = d_R(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp) - 1$ is the maximum number of links that an adversary may listen to without obtaining any information about the sent message.

Remark C.17. *Proposition C.16 extends [24, Lemma 7, item 2] from $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$ to $\mathbb{F}_q$-linear codes in $\mathbb{F}_q^{m \times n}$ due to Lemma C.53 in Subsection 8.1. Furthermore, as we will explain in Theorem C.7, our Theorem C.1 extends in the same sense [24, Theorem 2] and [24, Corollary 5].*

Remark C.18. *In Section 8, we will prove that GMWs coincide with DGWs [34] when using one code ($\mathcal{C}_1^\perp = \{0\}$ in Theorem C.1) and non-square matrices. Hence the results in this subsection prove that DGWs measure the worst-case information leakage in these cases, which has not been proven in the literature yet.*

4 Optimal universal secure linear codes for noiseless networks and any packet length

In this section, we obtain linear coset coding schemes built from nested linear code pairs $\mathcal{C} \subsetneqq \mathbb{F}^{m \times n}$, which in this section will refer to those with $\mathcal{C}_2 = \mathcal{C}$ and $\mathcal{C}_1 = \mathbb{F}^{m \times n}$, with optimal universal security performance in the case of finite fields $\mathbb{F} = \mathbb{F}_q$ (Theorem C.2). Recall from Subsection 2.3 that these linear coset coding schemes are suitable for noiseless networks, as noticed in [33] (see also Remark C.4).

In this section, we consider perfect universal secrecy (the adversary obtains no information after wire-tapping a given number of links), thus we make use of the theory in last section concerning the first RGMW. In Section 7, we will consider bounds on the rest of RGMWs, for general code pairs (suitable for noisy networks), and their achievability.

Definition C.19. For a nested linear code pair of the form $\mathcal{C} \subsetneqq \mathbb{F}_q^{m \times n}$, we define its information parameter as $\ell = \dim(\mathbb{F}_q^{m \times n}/\mathcal{C}) = \dim(\mathcal{C}^\perp)$, that is the maximum number of $\log_2(q)$ bits of information that the source can convey, and its security parameter t as the maximum number of links that an adversary may listen to without obtaining any information about the sent message.

Due to Theorem C.1, it holds that $t = d_R(\mathcal{C}^\perp) - 1$. We study two problems:

1. Find a nested linear code pair $\mathcal{C} \subsetneqq \mathbb{F}_q^{m \times n}$ with maximum possible security parameter t when m, n, q and the information parameter ℓ are fixed and given.

2. Find a nested linear code pair $\mathcal{C} \subsetneqq \mathbb{F}_q^{m \times n}$ with maximum possible information parameter ℓ when m, n, q and the security parameter t are fixed and given.

We will deduce bounds on these parameters from the Singleton bound on the dimension of rank-metric codes [9, Theorem 5.4]:

Lemma C.20 ([9, Theorem 5.4]). *For a linear code $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$, it holds that*

$$\dim(\mathcal{C}) \leq \max\{m, n\}(\min\{m, n\} - d_R(\mathcal{C}) + 1). \tag{C.8}$$

As usual in the literature, we say that $\mathcal{C}$ is maximum rank distance (MRD) if equality holds in (C.8).

Thanks to Theorem C.1 and the previous lemma, we may give upper bounds on the attainable parameters in the previous two problems:

Proposition C.21. *Given a nested linear code pair $\mathcal{C} \subsetneqq \mathbb{F}_q^{m \times n}$ with information parameter ℓ and security parameter t, it holds that:*

$$\ell \leq \max\{m,n\}(\min\{m,n\} - t), \tag{C.9}$$

$$t \leq \min\{m,n\} - \left\lceil \frac{\ell}{\max\{m,n\}} \right\rceil. \tag{C.10}$$

In particular, $\ell \leq mn$ and $t \leq \min\{m,n\}$.

Proof. Recall that $\ell = \dim(\mathbb{F}_q^{m \times n} / \mathcal{C}) = \dim(\mathcal{C}^\perp)$ and, due to Theorem C.1, $t = d_R(\mathcal{C}^\perp) - 1$. Hence the result follows from the bound (C.8) for $\mathcal{C}^\perp$. □

On the other hand, the existence of linear codes in $\mathbb{F}_q^{m \times n}$ attaining the Singleton bound on their dimensions, for all possible choices of m, n and minimum rank distance d_R [9, Theorem 6.3], leads to the following existence result on optimal linear coset coding schemes for noiseless networks.

Theorem C.2. *For all choices of positive integers m and n, and all finite fields $\mathbb{F}_q$, the following hold:*

1. *For every positive integer $\ell \leq mn$, there exists a nested linear code pair $\mathcal{C} \subsetneqq \mathbb{F}_q^{m \times n}$ with information parameter ℓ and security parameter $t = \min\{m,n\} - \lceil (\ell / \max\{m,n\}) \rceil$.*
2. *For every positive integer $t \leq \min\{m,n\}$, there exists a nested linear code pair $\mathcal{C} \subsetneqq \mathbb{F}_q^{m \times n}$ with security parameter t and information parameter $\ell = \max\{m,n\}(\min\{m,n\} - t)$.*

Remark C.22. *We remark here that, to the best of our knowledge, only the linear coset coding schemes in item 2 in the previous theorem, for the special case $n \leq m$, have been obtained in the literature. It corresponds to [39, Theorem 7].*

Using cartesian products of MRD codes as in [39, Subsection VII-C], linear coset coding schemes as in item 2 in the previous theorem can be obtained when $n > m$, for the restricted parameters $n = lm$ and $\ell = mlk'$, where l and $k' < m$ are positive integers.

5 Universal secure list-decodable rank-metric linear coset coding schemes

In this section, we will obtain nested linear code pairs $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$ when n divides m that can list-decode rank errors on noisy networks (as opposed to the scenario in last section), whose list sizes are polynomial on the code length n, while being univeral secure under a given number of wire-tapped links. As in last section, we consider perfect universal secrecy, and thus make use of the results in Section 3 concerning the first RGMW of the dual code pair.

We give the construction in Subsection 5.1, together with its parameters (Theorem C.3): information parameter ℓ, security parameter t and number of list-decodable rank errors e. To measure the quality of the proposed code pair, we will compare in Subsection 5.2 their parameters with those obtained when choosing $\mathcal{C}_1$ and $\mathcal{C}_2$ as MRD codes [17, 36], which provide coset coding schemes with both optimal universal security and optimal error-correction capability [39]. We will also show (Subsection 5.3) the near optimality of the obtained construction in terms of the introduced uncertainty on the secret message and the number of list-decodable rank errors.

5.1 The construction and its main properties

We start by extending the definition of rank list-decodable codes from [11, Definition 2] to coset coding schemes:

Definition C.23. For positive integers e and L, we say that a coset coding scheme $\mathcal{P}_{\mathcal{S}} = \{\mathcal{C}_{\mathbf{x}}\}_{\mathbf{x}\in\mathcal{S}}$ over $\mathbb{F}_q$ is rank (e, L)-list-decodable if, for every $Y \in \mathbb{F}_q^{m\times n}$, we have that

$$|\{\mathbf{x} \in \mathcal{S} \mid \mathcal{P}_{\mathbf{x}} \cap \mathcal{B}(Y, e) \neq \emptyset\}| \leq L,$$

where $\mathcal{B}(Y, e)$ denotes the ball in $\mathbb{F}_q^{m\times n}$ with center Y and rank radius e. The number of list-decodable rank errors is e and the list sizes are said to be polynomial in n if $L = \mathcal{O}(F(n))$, for some polynomial $F(x)$.

Remark C.24. *Observe however that, if a coset coding scheme can list-decode e rank errors with polynomial-sized lists of cosets, we still need to decode these cosets to obtain the uncoded secret messages. In general, it is possible that the union of such cosets has exponential size while the scheme can still obtain all the corresponding uncoded messages via an algorithm with polynomial complexity. This is the case in the construction below.*

We now give the above mentioned construction, which exists whenever n divides m. The main objective is to obtain simultaneously large information parameter ℓ, security parameter t and number of list-decodable rank errors e.

Construction C.25. Assume that n divides m and fix $\varepsilon > 0$ and positive integers s and $1 \leq k_2 < k_1 \leq n$ such that $4sn \leq \varepsilon m$ and $m/n = \mathcal{O}(s/\varepsilon)$. In the next subsection, mk_1 and mk_2 will be the dimensions of the MRD linear codes constituting an optimal universal secure nested coset coding scheme, but here they are just fixed parameters.

Fix a basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ of $\mathbb{F}_{q^m}$ as a vector space over $\mathbb{F}_q$, such that $\alpha_1, \alpha_2, \ldots, \alpha_n$ generate $\mathbb{F}_{q^n}$ (recall that $\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^m}$ since n divides m).

Recall that a q-linearized polynomial over $\mathbb{F}_{q^m}$ is a polynomial of the form $F(x) = \sum_{i=0}^{d} F_i x^{q^i}$, where $F_i \in \mathbb{F}_{q^m}$, for some positive integer d. Denote also $\mathrm{ev}_{\boldsymbol{\alpha}}(F(x)) = (F(\alpha_1), F(\alpha_2), \ldots, F(\alpha_n)) \in \mathbb{F}_{q^m}^n$, and finally define the linear codes

$$\mathcal{C}_2 = \{M_{\boldsymbol{\alpha}}(\mathrm{ev}_{\boldsymbol{\alpha}}(F(x))) \mid F_i = 0 \text{ for } i < k_1 - k_2 \text{ and } i \geq k_1\},$$

$$\mathcal{C}_1 = \{M_{\boldsymbol{\alpha}}(\mathrm{ev}_{\boldsymbol{\alpha}}(F(x))) \mid F_i \in \mathcal{H}_i \text{ for } 0 \leq i < k_1 - k_2,$$
$$F_i \in \mathbb{F}_{q^m} \text{ for } k_1 - k_2 \leq i < k_1, F_i = 0 \text{ for } i \geq k_1\},$$

where $M_{\boldsymbol{\alpha}}$ is the map given in (C.1) and $\mathcal{H}_0, \mathcal{H}_1, \ldots, \mathcal{H}_{k_1-k_2-1} \subseteq \mathbb{F}_{q^m}$ are the $\mathbb{F}_q$-linear vector spaces described in [20, Theorem 8]. We recall this description in Appendix B. Observe that these vector spaces depend on ε and s.

Let $\ell = \dim(\mathcal{C}_1/\mathcal{C}_2) = \dim(\mathcal{H}_0 \times \mathcal{H}_1 \times \cdots \times \mathcal{H}_{k_1-k_2-1})$. We now show how $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$ form a coset coding scheme as in Definition C.3. Define the vector space

$$\mathcal{W} = \{M_{\boldsymbol{\alpha}}(\mathrm{ev}_{\boldsymbol{\alpha}}(F(x))) \mid F_i \in \mathcal{H}_i \text{ for } i < k_1 - k_2$$
$$\text{and } F_i = 0 \text{ for } i \geq k_1 - k_2\},$$

which satisfies that $\mathcal{C}_1 = \mathcal{C}_2 \oplus \mathcal{W}$. Now consider the secret space as $\mathcal{H}_0 \times \mathcal{H}_1 \times \cdots \times \mathcal{H}_{k_1-k_2-1} \cong \mathbb{F}_q^{\ell}$, and define the vector space isomorphism $\psi : \mathcal{H}_0 \times \mathcal{H}_1 \times \cdots \times \mathcal{H}_{k_1-k_2-1} \longrightarrow \mathcal{W}$ as follows: For $\mathbf{x} \in \mathcal{H}_0 \times \mathcal{H}_1 \times \cdots \times \mathcal{H}_{k_1-k_2-1}$, take $F(x) = \sum_{i=0}^{k_1-k_2-1} F_i x^{q^i}$ such that $\mathbf{x} = (F_0, F_1, \ldots, F_{k_1-k_2-1})$, and define

$$C = \psi(\mathbf{x}) = M_{\boldsymbol{\alpha}}(\mathrm{ev}_{\boldsymbol{\alpha}}(F(x))).$$

We may now state the main result of this section:

Theorem C.3. *With the same assumptions and notation, the nested coset coding scheme in Construction C.25 satisfies that:*

1. $\ell = \dim(\mathcal{C}_1/\mathcal{C}_2) \geq m(k_1 - k_2)(1 - 2\varepsilon)$.
2. *Its security parameter (Definition C.19) satisfies* $t \geq k_2$.
3. *It is rank* (e, L)*-list-decodable for all* $e \leq \frac{s}{s+1}(n - k_1)$, *with* $L \leq q^{\mathcal{O}(s^2/\varepsilon^2)}$, *and it admits a list-decoding algorithm that obtains all corresponding uncoded messages with polynomial complexity in* n.

We devote the rest of the subsection to prove this theorem. We need to recall some definitions and results from [20]:

Definition C.26 (Subspace designs [20, Definition 3]). Assuming that n divides m and given positive integers r and N, a collection of $\mathbb{F}_q$-linear subspaces $\mathcal{U}_1, \mathcal{U}_2, \ldots, \mathcal{U}_M \subseteq \mathbb{F}_{q^m}$ is called an (r, N, n) $\mathbb{F}_q$-linear subspace design if

$$\sum_{i=1}^{M} \dim(\mathcal{U}_i \cap \mathcal{V}) \leq N,$$

with dimensions taken over $\mathbb{F}_q$, for every $\mathbb{F}_{q^n}$-linear subspace $\mathcal{V} \subseteq \mathbb{F}_{q^m}$ of dimension at most r over $\mathbb{F}_{q^n}$.

The following lemma is part of [20, Theorem 8]:

Lemma C.27 ([20]). *With assumptions and notation as in Construction C.25, the spaces $\mathcal{H}_0, \mathcal{H}_1, \ldots \mathcal{H}_{k_1-k_2-1}$ defined in Appendix B form an $(s, 2(m/n-1)s/\varepsilon, n)$ $\mathbb{F}_q$-linear subspace design.*

Definition C.28 (Periodic subspaces [20, Definition 9]). Given positive integers r, l, k, we say that an affine subspace $\mathcal{H} \subseteq \mathbb{F}_{q^n}^{lk}$ is (r, l, k)-periodic if there exists an $\mathbb{F}_{q^n}$-linear subspace $\mathcal{V} \subseteq \mathbb{F}_{q^n}^{l}$ of dimension at most r over $\mathbb{F}_{q^n}$ such that, for every $j = 2, 3, \ldots, k$ and $\mathbf{a} \in \mathbb{F}_{q^n}^{(j-1)l}$, the affine space

$$\{\pi_{[(j-1)l+1, jl]}(\mathbf{x}) \mid \mathbf{x} \in \mathcal{H}, \pi_{[1,(j-1)l]}(\mathbf{x}) = \mathbf{a}\} \subseteq \mathbb{F}_{q^n}^{l}$$

is contained in $\mathbf{v}_\mathbf{a} + \mathcal{V}$, for a vector $\mathbf{v}_\mathbf{a} \in \mathbb{F}_{q^n}^{l}$ that depends on $\mathbf{a}$. Here, π_J denotes the projection over the coordinates in J, and $[a, b]$ denotes the set of integers i such that $a \leq i \leq b$.

We may now prove our main result:

Proof of Theorem C.3. We prove each item separately:

1) By Lemma C.70 in Appendix B, it holds that $\dim(\mathcal{H}_i) \geq m(1-2\varepsilon)$, for $i = 0, 1, 2, \ldots, k_1 - k_2 - 1$. Therefore

$$\ell = \dim(\mathcal{H}_0 \times \mathcal{H}_1 \times \cdots \times \mathcal{H}_{k_1-k_2-1}) \geq m(k_1-k_2)(1-2\varepsilon).$$

2) By Theorem C.1, the security parameter is $t = d_R(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp) - 1 \geq d_R(\mathcal{C}_2^\perp) - 1$. Since $\mathcal{C}_2$ is MRD, then so is its trace dual [9], which means that $d_R(\mathcal{C}_2^\perp) = k_2 + 1$, and the result follows.

3) As shown in [20, Subsection IV-B], we may perform list-decoding for the Gabidulin code $\mathcal{G}_1 \supseteq \mathcal{C}_1$,

$$\mathcal{G}_1 = \{M_\boldsymbol{\alpha}(\mathrm{ev}_\boldsymbol{\alpha}(F(x))) \mid F_i = 0 \text{ for } i \geq k_1\},$$

and obtain in polynomial time a list containing all possible sent messages that is an $(s-1, m/n, k_1)$-periodic subspace of $\mathbb{F}_{q^n}^{k_1 m/n} \cong \mathbb{F}_{q^m}^{k_1}$ (isomorphic as $\mathbb{F}_{q^n}$-linear vector spaces).

Project this periodic subspace onto the first $k_1 - k_2$ coordinates, which gives a $(s-1, m/n, k_1 - k_2)$-periodic subspace of $\mathbb{F}_{q^m}^{k_1 - k_2}$, and intersect it with $\mathcal{H}_0 \times \mathcal{H}_1 \times \cdots \times \mathcal{H}_{k_1 - k_2 - 1}$. Since $\mathcal{H}_0, \mathcal{H}_1, \ldots \mathcal{H}_{k_1-k_2-1}$ form an $(s, 2(m/n - 1)s/\varepsilon, n)$ $\mathbb{F}_q$-linear subspace design by Lemma C.27, such intersection is an $\mathbb{F}_q$-linear affine space of dimension at most $\mathcal{O}(s^2/\varepsilon^2)$ (recall that $m/n = \mathcal{O}(s/\varepsilon)$) by the definition of subspace designs and periodic subspaces. □

5.2 Comparison with optimal unique-decodable linear coset coding schemes based on MRD codes

In this subsection, we compare the schemes in Construction C.25 with those obtained when using MRD codes [17, 36], whose information parameter ℓ is optimal for given security parameter t and number of unique-decodable rank errors e, due to Theorems 11 and 12 in [39].

Proposition C.29 ([39]). *Assume that $n \leq m$ and $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$ are MRD linear codes of dimensions* $\dim(\mathcal{C}_1) = mk_1$ *and* $\dim(\mathcal{C}_2) = mk_2$ *(recall that, by the Singleton bound (C.8), dimensions of MRD codes are multiple of m when $n \leq m$).*

The linear coset coding scheme (Definition C.3) constructed from this nested linear code pair satisfies that:

1. *Its information parameter is $\ell = m(k_1 - k_2)$.*
2. *Its security parameter is $t = k_2$.*
3. *If the number of rank errors is $e \leq \lfloor \frac{n-k_1}{2} \rfloor$, then rank error-correction can be performed, giving a unique solution.*

Therefore, assuming that n divides m and given MRD linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$ of dimensions $\dim(\mathcal{C}_1) = mk_1$ and $\dim(\mathcal{C}_2) = mk_2$, the linear coset coding scheme in Construction C.25 has at least the same security parameter t as that obtained using $\mathcal{C}_1$ and $\mathcal{C}_2$, an information parameter ℓ that is at least $1 - 2\varepsilon$ times the one obtained using $\mathcal{C}_1$ and $\mathcal{C}_2$, and can list-decode in polynomial time (with list of polynomial size) roughly $n - k_1$ errors, which is twice as many as the rank errors that $\mathcal{C}_1$ and $\mathcal{C}_2$ can correct, due to the previous proposition and Theorem C.3.

5.3 Near optimality of the obtained construction

In this subsection, we will show the near optimality of Construction C.25 in terms of its *introduced uncertainty* $H(C|\mathbf{x})$ compared to the maximum *observed* *information* $H(CB^T)$ by the wire-tapper, and the number of rank errors e that the scheme can list-decode.

Let $\mathbf{x} \in \mathbb{F}_q^\ell$ and $C \in \mathbb{F}_q^{m\times n}$ denote the random variables representing the secret message and the transmitted codeword, respectively, as in Subsection 3.3.

The quantity $H(C|\mathbf{x})$ measures the amount of randomness of C given $\mathbf{x}$ introduced by the corresponding coset coding scheme, and we would like it to be as small as possible since generating randomness is difficult in practice. Observe that $H(C|\mathbf{x}) = \dim(\mathcal{C}_2)$ for nested coset coding schemes. On the other hand, the quantity $H(CB^T)$ measures the amount of observed information by wire-tapping μ links if $B \in \mathbb{F}_q^{\mu\times n}$, which satisfies $H(CB^T) \leq m\mu$, being the inequality usually tight when $I(\mathbf{x}; CB^T) = 0$ or even an equality, as is the case for Gabidulin codes. Thus the following bound is a weaker version of a bound of the form $mt \leq \dim(\mathcal{C}_2)$, which we leave as open problem.

Proposition C.30. *Fix an arbitrary coset coding scheme in $\mathbb{F}_q^{m\times n}$ with message set $\mathcal{S} = \mathbb{F}_q^\ell$, let $\mathbf{x} \in \mathbb{F}_q^\ell$, and let $C \in \mathbb{F}_q^{m\times n}$ be its encoding. It holds that*

$$\max\{H(CB^T) \mid B \in \mathbb{F}_q^{\mu\times n}, I(\mathbf{x}; CB^T) = 0\} \leq H(C|\mathbf{x}).$$

Proof. Fix $B \in \mathbb{F}_q^{\mu\times n}$. The result follows from the following chain of inequalities:

$$\begin{aligned} & I(\mathbf{x}; CB^T) \\ = \; & H(CB^T) - H(CB^T|\mathbf{x}) \\ = \; & H(CB^T) - H(CB^T|C,\mathbf{x}) \\ & + H(CB^T|C,\mathbf{x}) - H(CB^T|\mathbf{x}) \\ = \; & H(CB^T) - H(CB^T|C) \\ & + H(CB^T|C,\mathbf{x}) - H(CB^T|\mathbf{x}) \\ & \text{(since } \mathbf{x} \to C \to CB^T \text{ is a Markov chain [8])} \\ = \; & I(C; CB^T) - I(C; CB^T|\mathbf{x}) \\ \geq \; & H(CB^T) - H(C|\mathbf{x}). \end{aligned}$$

Now consider the coset coding scheme in Construction C.25, and fix $\mu \leq k_2 \leq k_1$. Define the Gabidulin code

$$\mathcal{G}_1 = \{M_{\boldsymbol{\alpha}}(\mathrm{ev}_{\boldsymbol{\alpha}}(F(x))) \mid F_i = 0, i \geq k_1\} \subseteq \mathbb{F}_q^{m\times n},$$

and let G be the uniform random variable on $\mathcal{G}_1$. It holds that

$$\max_{B \in \mathbb{F}_q^{\mu\times n}} H(GB^T) = m\mu, \tag{C.11}$$

since $\mu \leq k_1$. Equation (C.11) together with $\dim(\mathcal{G}_1/\mathcal{C}_1) \leq 2m\varepsilon(k_1 - k_2)$ implies that

$$\max_{B \in \mathbb{F}_q^{\mu \times n}} H(CB^T) \geq m(\mu - 2\varepsilon(k_1 - k_2)).$$

Using that $H(C|\mathbf{x}) = \dim(\mathcal{C}_2) = mk_2$, we see that the bound in the previous proposition is tight for Construction C.25:

$$\begin{aligned} 0 \leq & H(C|\mathbf{x}) - \max\{H(CB^T) \mid B \in \mathbb{F}_q^{\mu \times n}, I(\mathbf{x}; CB^T) = 0\} \\ \leq & m(k_2 - t + 2\varepsilon(k_1 - k_2)) \leq 2\varepsilon m(k_1 - k_2). \end{aligned}$$

Next we show that the rank list-decoding capability cannot be improved for large s and small ε, compared to general nested coset coding schemes. Since rank list-decodable nested coset coding schemes still require decoding each coset, we will consider those such that a complementary space $\mathcal{W}$ as in Definition C.3 is rank list-decodable with polynomial-sized lists after adding an error matrix from the smaller code $\mathcal{C}_2$:

Proposition C.31. *Fix a nested linear code pair $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$ and a subspace $\mathcal{W} \subseteq \mathcal{C}_1$ such that $\mathcal{C}_1 = \mathcal{C}_2 \oplus \mathcal{W}$, and denote by M the maximum rank of a matrix in $\mathcal{C}_2$. If $\mathcal{W}$ is rank $(e + M, L)$-list-decodable with polynomial list sizes L, then*

$$e \leq n - \frac{\dim(\mathcal{C}_1)}{m}.$$

Proof. By [11, Proposition 1], if the linear code $\mathcal{W}$ is rank $(e + M, L)$-list-decodable with polynomial-sized lists L, then

$$e + M \leq n - \dim(\mathcal{W})/m.$$

On the other hand, the maximum rank of codewords in $\mathcal{C}_2$ is at least $\dim(\mathcal{C}_2)/m$ by [35, Proposition 47]. Hence

$$e \leq n - \frac{\dim(\mathcal{W})}{m} - \frac{\dim(\mathcal{C}_2)}{m} = n - \frac{\dim(\mathcal{C}_1)}{m},$$

and we are done. □

For the nested coset coding scheme in Construction C.25, it holds that

$$e = \frac{s}{s+1}(n - k_1), \text{ and}$$

$$n - \frac{\dim(\mathcal{C}_1)}{m} = n - k_1(1 - 2\varepsilon) - 2\varepsilon k_2,$$

which are closer as s becomes larger and ε becomes smaller.

6 Security equivalences of linear coset coding schemes and minimum parameters

In this section, we study when two nested linear code pairs $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$ and $\mathcal{C}'_2 \subsetneqq \mathcal{C}'_1 \subseteq \mathbb{F}^{m' \times n'}$ have the same universal security and/or reliability performance.

First, we define security equivalences and give several characterizations of these in Theorem C.4 (Subsection 6.1), which show that they also preserve error and erasure correction capabilities. As applications, we study ranges and minimum possible parameters m and n for linear codes (Subsection 6.2), and we study when they are degenerate (Subsection 6.3), meaning when they can be applied to networks with strictly smaller length n.

6.1 Security equivalences and rank isometries

In this subsection, we first give in Theorem C.4 the above mentioned characterizations, and we define afterwards security equivalences as maps satisfying one of such characterizations. We continue with Proposition C.37, which shows that security equivalences actually preserve universal security performance as in Subsection 2.2, thus motivating our definition. We conclude by comparing Theorem C.4 with related results from the literature (see also Table C.3).

Due to the importance of the rank metric for error and erasure correction in linear network coding (see Subsection 2.2), and for universal security (by Theorem C.1 and Corollary C.13), we start by considering rank isometries:

Definition C.32 (Rank isometries). We say that a map $\phi : \mathcal{V} \longrightarrow \mathcal{W}$ between vector spaces $\mathcal{V} \subseteq \mathbb{F}^{m \times n}$ and $\mathcal{W} \subseteq \mathbb{F}^{m' \times n'}$ is a rank isometry if it is a vector space isomorphism and $\mathrm{Rk}(\phi(V)) = \mathrm{Rk}(V)$, for all $V \in \mathcal{V}$. In that case, we say that $\mathcal{V}$ and $\mathcal{W}$ are rank isometric.

We have the following result, which was first proven in [27, Theorem 1] for square matrices and the complex field $\mathbb{F} = \mathbb{C}$. In [30, Proposition 3] it is observed that the square condition is not necessary and it may be proven for arbitrary fields:

Proposition C.33 ([27, 30]). *If $\phi : \mathbb{F}^{m \times n} \longrightarrow \mathbb{F}^{m \times n}$ is a rank isometry, then there exist invertible matrices $A \in \mathbb{F}^{m \times m}$ and $B \in \mathbb{F}^{n \times n}$ such that*

1. *$\phi(C) = ACB$, for all $C \in \mathbb{F}^{m \times n}$, or*
2. *$\phi(C) = AC^T B$, for all $C \in \mathbb{F}^{m \times n}$,*

where the latter case can only happen if $m = n$.

We will define security equivalences as certain vector space isomorphisms satisfying one of several equivalent conditions. We first show their equivalence in the following theorem, which is the main result of this section:

Theorem C.4. *Let $\phi : \mathcal{V} \longrightarrow \mathcal{W}$ be a vector space isomorphism between rank support spaces $\mathcal{V} \in RS(\mathbb{F}^{m \times n})$ and $\mathcal{W} \in RS(\mathbb{F}^{m \times n'})$, and consider the following properties:*

(P 1) There exist full-rank matrices $A \in \mathbb{F}^{m \times m}$ and $B \in \mathbb{F}^{n \times n'}$ such that $\phi(C) = ACB$, for all $C \in \mathcal{V}$.

(P 2) A subspace $\mathcal{U} \subseteq \mathcal{V}$ is a rank support space if, and only if, $\phi(\mathcal{U})$ is a rank support space.

(P 3) For all subspaces $\mathcal{D} \subseteq \mathcal{V}$, it holds that $\mathrm{wt_R}(\phi(\mathcal{D})) = \mathrm{wt_R}(\mathcal{D})$.

(P 4) ϕ is a rank isometry.

Then the following implications hold:

$$(P\ 1) \Longleftrightarrow (P\ 2) \Longleftrightarrow (P\ 3) \Longrightarrow (P\ 4).$$

In particular, a security equivalence is a rank isometry and, in the case $\mathcal{V} = \mathcal{W} = \mathbb{F}^{m \times n}$ and $m \neq n$, the reversed implication holds by Proposition C.33.

Proof. See Appendix C. □

Remark C.34. *Unfortunately, the implication $(P\ 3) \Longleftarrow (P\ 4)$ does not always hold. Take for instance $m = n$ and the map $\phi : \mathbb{F}^{m \times m} \longrightarrow \mathbb{F}^{m \times m}$ given by $\phi(C) = C^T$, for all $C \in \mathbb{F}^{m \times m}$.*

Remark C.35. *Observe that, in particular, security equivalences also preserve (relative) generalized matrix weights, (relative) dimension/rank support profiles and distributions of rank weights of vector subspaces, and they are the only rank isometries with these properties.*

Property (P 1) will be useful for technical computations and, in particular, for Proposition C.37 below. As explained in Appendix C, (P 2) allows us to connect (P 1) with (P 3), and (P 3) allows us to connect the first two with the rank metric (P 4), crucial for error and erasure correction as in Subsection 2.2. Finally, Property (P 2) also explains why we will consider security equivalences defined between rank support spaces, and intuitively explains that such spaces behave as ambient spaces in our theory, as mentioned in Subsection 3.1.

Definition C.36 (Security equivalences). We say that a map $\phi : \mathcal{V} \longrightarrow \mathcal{W}$ between rank support spaces $\mathcal{V} \in RS(\mathbb{F}^{m \times n})$ and $\mathcal{W} \in RS(\mathbb{F}^{m \times n'})$ is a security equivalence if it is a vector space isomorphism and satisfies condition (P 1), (P 2) or (P 3) in Theorem C.4.

Two nested linear code pairs $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$ and $\mathcal{C}_2' \subsetneqq \mathcal{C}_1' \subseteq \mathbb{F}^{m \times n'}$ are said to be security equivalent if there exist rank support spaces $\mathcal{V} \in RS(\mathbb{F}^{m \times n})$ and $\mathcal{W} \in RS(\mathbb{F}^{m \times n'})$, containing $\mathcal{C}_1$ and $\mathcal{C}_1'$, respectively, and a security equivalence $\phi : \mathcal{V} \longrightarrow \mathcal{W}$ with $\phi(\mathcal{C}_1) = \mathcal{C}_1'$ and $\phi(\mathcal{C}_2) = \mathcal{C}_2'$.

We now motivate the previous definition with the next proposition, which makes use of Theorem C.4. Observe that Remark C.35 above already shows that security equivalences preserve the worst-case information leakage as described in Theorem C.1. Now, given nested linear code pairs $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$ and $\mathcal{C}_2' \subsetneqq \mathcal{C}_1' \subseteq \mathbb{F}_q^{m \times n'}$, Proposition C.37 below shows that if the dual pairs are security equivalent, then there exists a bijective correspondence between wire-tappers' transfer matrices (matrix B in Subsection 2.2, item 2) that preserves the mutual information with the original sent message. If the original pairs are also security equivalent, we conclude that encoding with $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$ or $\mathcal{C}_2' \subsetneqq \mathcal{C}_1' \subseteq \mathbb{F}_q^{m \times n'}$ yields exactly the same universal error and erasure correction performance, and exactly the same universal security performance over linearly coded networks, as in Subsection 2.2.

Proposition C.37. *Assume that $\mathbb{F} = \mathbb{F}_q$ and the dual pairs of $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$ and $\mathcal{C}_2' \subsetneqq \mathcal{C}_1' \subseteq \mathbb{F}_q^{m \times n'}$ are security equivalent by a security equivalence given by matrices $A \in \mathbb{F}_q^{m \times m}$ and $B \in \mathbb{F}_q^{n \times n'}$ as in item 1 in Theorem C.4. For any matrix $M \in \mathbb{F}_q^{\mu \times n}$, it holds that*

$$I\left(\mathbf{x}; CM^T\right) = I\left(\mathbf{x}; C'(MB)^T\right), \tag{C.12}$$

with notation as in Proposition C.16, where $C \in \mathbb{F}_q^{m \times n}$ and $C' \in \mathbb{F}_q^{m \times n'}$ are the encodings of $\mathbf{x}$ using $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_q^{m \times n}$ and $\mathcal{C}_2' \subsetneqq \mathcal{C}_1' \subseteq \mathbb{F}^{m \times n'}$, respectively.

Furthermore, assuming $n \leq n'$, the correspondence $M \mapsto MB$ is one to one and, for any matrix $N \in \mathbb{F}_q^{\mu \times n'}$, there exists $M \in \mathbb{F}_q^{\mu \times n}$ such that $I\left(\mathbf{x}; C'N^T\right) = I\left(\mathbf{x}; C'(MB)^T\right)$.

Proof. Denote by ϕ the security equivalence. Take a matrix $M \in \mathbb{F}_q^{\mu \times n}$, define $\mathcal{L} = \text{Row}(M) \subseteq \mathbb{F}_q^n$ and $\mathcal{L}' = \text{Row}(MB) \subseteq \mathbb{F}_q^{n'}$. Then $\phi(\mathcal{V}_{\mathcal{L}}) = \mathcal{V}_{\mathcal{L}'}$ and

$$\dim(\phi(\mathcal{C}_1^\perp) \cap \mathcal{V}_{\mathcal{L}'}) = \dim(\phi(\mathcal{C}_1^\perp \cap \mathcal{V}_{\mathcal{L}})) = \dim(\mathcal{C}_1^\perp \cap \mathcal{V}_{\mathcal{L}}),$$

and similarly for $\mathcal{C}_2$. Thus Equation (C.12) follows from Proposition C.16.

Observe that we may assume $n \leq n'$ without loss of generality, since the inverse of a security equivalence is a security equivalence. Thus the injectivity of $M \mapsto MB$ follows from the fact that B has full rank.

Finally, if $N \in \mathbb{F}_q^{\mu \times n'}$, $\mathcal{L} = \mathrm{Row}(N)$ and $\mathcal{K} = \mathrm{Row}(B)$, then $\mathcal{C}_1^\perp \subseteq \mathcal{V}_\mathcal{K}$ and

$$\mathcal{C}_1^\perp \cap \mathcal{V}_\mathcal{L} = \mathcal{C}_1^\perp \cap (\mathcal{V}_\mathcal{L} \cap \mathcal{V}_\mathcal{K}),$$

and similarly for $\mathcal{C}_2^\perp$. Since $\mathcal{V}_\mathcal{L} \cap \mathcal{V}_\mathcal{K} = \mathcal{V}_{\mathcal{L} \cap \mathcal{K}}$ and $\mathcal{L} \cap \mathcal{K} = \mathrm{Row}(MB)$ for a matrix $M \in \mathbb{F}_q^{\mu \times n}$, the last statement follows again from Proposition C.16. □

The topic of vector space isomorphisms $\phi : \mathbb{F}^{m \times n} \longrightarrow \mathbb{F}^{m \times n}$ preserving some specified property has been intensively studied in the literature (see also Table C.3), where the term *Frobenius map* is generally used for maps of the form of those in Proposition C.33.

When $m = n$, it is proven in [10, Theorem 3] that Frobenius maps are characterized by being those preserving invertible matrices and in [27] they are characterized by being those preserving ranks (this is extended to $m \neq n$ in [30, Proposition 3]), those preserving determinants and those preserving eigenvalues.

On the other hand, [3, Theorem 1] shows that $\mathbb{F}_{q^m}$-linear vector space isomorphisms $\phi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$ preserving ranks are given by $\phi(\mathbf{c}) = \beta \mathbf{c} A$, for $\beta \in \mathbb{F}_{q^m} \setminus \{0\}$ and an invertible $A \in \mathbb{F}_q^{n \times n}$. This is extended in [28, Theorem 5] to $\mathbb{F}_{q^m}$-linear vector space isomorphisms whose domain and codomain are $\mathbb{F}_{q^m}$-linear Galois closed spaces in $\mathbb{F}_{q^m}^n$, which correspond to rank support spaces in $\mathbb{F}_q^{m \times n}$ (see Lemma C.53 below).

Therefore, we extend these works in three directions simultaneously: First, we consider the stronger properties (P 1), (P 2) and (P 3) than those considered in [3, 10, 27, 30], which are essentially (P 4). Second, we extend the domains and codomains from $\mathbb{F}^{m \times n}$ to general rank support spaces whose matrices do not necessarily have the same sizes. Finally, in the case $\mathbb{F} = \mathbb{F}_q$, we consider general $\mathbb{F}_q$-linear maps, instead of the particular case of $\mathbb{F}_{q^m}$-linear maps as in [3, 28].

6.2 Minimum parameters of linear codes

As main application of the previous subsection, we study in this subsection the minimum parameters m and n for which there exists a linear code that is security equivalent to a given one. Recall from Subsection 2.1 that m corresponds to the packet length used in the network, and n corresponds to the number of outgoing links from the source.

Both cases of one linear code, that is $\mathcal{C}_2 = \{0\}$ and $\mathcal{C}_1 = \mathbb{F}^{m \times n}$, are covered since they are dual of each other (see also Remark C.4 and Appendix A). Since security equivalences are rank isometries by Theorem C.4, in the first case we find minimum parameters for error and erasure correction, and in the second case we find minimum parameters for universal security on noiseless linearly coded networks.

Proposition C.38. *Fix a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$ of dimension k. There exists a linear code $\mathcal{C}' \subseteq \mathbb{F}^{m \times n'}$ that is security equivalent to $\mathcal{C}$ if, and only if, $n' \geq d_{M,k}(\mathcal{C})$.*

Proof. First, if $\mathcal{C}' \subseteq \mathbb{F}^{m \times n'}$ is security equivalent to $\mathcal{C}$, then $\dim(\mathcal{C}') = k$ and $d_{M,k}(\mathcal{C}) = d_{M,k}(\mathcal{C}') \leq n'$.

On the other hand, assume that $n' \geq d_{M,k}(\mathcal{C})$. Take a subspace $\mathcal{L} \subseteq \mathbb{F}^n$ with $d = \dim(\mathcal{L}) = d_{M,k}(\mathcal{C})$ and $\dim(\mathcal{C} \cap \mathcal{V}_{\mathcal{L}}) \geq k$, which implies that $\mathcal{C} \subseteq \mathcal{V}_{\mathcal{L}}$. Take a generator matrix $A \in \mathbb{F}^{d \times n}$ of $\mathcal{L}$. There exists a full-rank matrix $A' \in \mathbb{F}^{n \times d}$ such that $AA' = I \in \mathbb{F}^{d \times d}$.

The linear map $\phi : \mathcal{V}_{\mathcal{L}} \longrightarrow \mathbb{F}^{m \times d}$, given by $\phi(V) = VA'$, for $V \in \mathcal{V}_{\mathcal{L}}$, is a vector space isomorphism. By dimensions, we just need to see that it is onto. Take $W \in \mathbb{F}^{m \times d}$. It holds that $W = WI = WAA' = \phi(WA)$, and $WA \in \mathcal{V}_{\mathcal{L}}$ by definition.

On the other hand, ϕ is a security equivalence by Theorem C.4. Therefore $\phi(\mathcal{C}) \subseteq \mathbb{F}^{m \times d}$ is security equivalent to $\mathcal{C}$. Finally, we see that appending $n' - d$ zero columns to the matrices in $\phi(\mathcal{C})$ gives a security equivalent code to $\mathcal{C}$ in $\mathbb{F}^{m \times n'}$. □

By transposing matrices, we obtain the following consequence, where we consider linear codes that are rank isometric to a given one. By [28, Theorem 9], such equivalent codes perform equally when used for error and erasure correction, and by Theorem C.1 and Corollary C.13, they perform equally regarding the maximum number of links that an adversary may wire-tap without obtaining any information on noiseless networks.

Corollary C.39. *For a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$, define the transposed linear code*

$$\mathcal{C}^T = \{C^T \mid C \in \mathcal{C}\} \subseteq \mathbb{F}^{n \times m}.$$

If $m' \geq d_{M,k}(\mathcal{C}^T)$, where $k = \dim(\mathcal{C})$, then there exists a linear code $\mathcal{C}' \subseteq \mathbb{F}^{m' \times n}$ that is rank isometric to $\mathcal{C}$.

Proof. It follows from Theorem C.4 and Proposition C.38. □

As a related result, [28, Proposition 3] computes the minimum parameter n for which there exists an $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ that is rank isometric to a given one. In contrast, we consider both parameters m and n, we consider security equivalences for the parameter n, and not only rank isometries, and as the biggest difference with [28], we consider general linear codes, and not only $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$.

6.3 Degenerate codes

In this subsection, we study degenerate codes, which by the study in the previous subsection, can be applied to networks with less outgoing links or, by transposing matrices, with smaller packet length. Degenerateness of codes in the rank metric has been studied in [22, Section 6] and [28, Subsection IV-B], but only for $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$. We extend those studies to general linear codes in $\mathbb{F}^{m \times n}$.

Definition C.40 (Degenerate codes). We say that a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$ is degenerate if it is security equivalent to a linear code $\mathcal{C}' \subseteq \mathbb{F}^{m \times n'}$ with $n' < n$.

The following lemma follows from Proposition C.38:

Lemma C.41. *A linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$ is degenerate if, and only if, $d_{M,k}(\mathcal{C}) < n$, where $k = \dim(\mathcal{C})$.*

Now we may give characterizations in terms of the minimum rank distance of the dual code thanks to Proposition C.66 in Appendix A.

Proposition C.42. *Given a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$, the following hold:*

1. *Assuming $\dim(\mathcal{C}^\perp) \geq m$, $\mathcal{C}$ is degenerate if, and only if, $d_{M,m}(\mathcal{C}^\perp) = 1$.*
2. *If $d_R(\mathcal{C}^\perp) > 1$, then $\mathcal{C}$ is not degenerate.*

Proof. From Proposition C.66, we know that

$$\overline{W}_k(\mathcal{C}) \cup W_0(\mathcal{C}^\perp) = \{1, 2, \ldots, n\},$$

where the sets on the left-hand side are disjoint, and where $k = \dim(\mathcal{C})$. Now, the smallest number in $\overline{W}_k(\mathcal{C})$ is $n + 1 - d_{M,k}(\mathcal{C})$, and the smallest number in $W_0(\mathcal{C}^\perp)$ is $d_{M,m}(\mathcal{C}^\perp)$. Item 1 follows from this and the previous lemma. Item 2 follows from item 1 and Proposition C.44 in Subsection 7.1. □

7 Monotonicity and Singleton-type bounds

In this section, we give upper and lower Singleton-type bounds on RGMWs. We start with the monotonicity of RDRPs and RGMWs (Subsection 7.1), which have their own interest, but which are a crucial tool to prove the main bounds (Theorems C.5 and C.6 in Subsection 7.2). Finally we study linear codes $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$, meaning $\mathcal{C}_1 = \mathcal{C}$ and $\mathcal{C}_2 = \{0\}$, that attain these bounds and whose dimensions are divisible by m (Subsection 7.3).

7.1 Monotonicity of RGMWs and RDRPs

The monotonicity bounds presented in this subsection are crucial tools for Theorems C.5 and C.6, but they also have an interpretation in terms of the worst-case information leakage, due to Theorem C.1: An adversary wire-tapping more links in the network will obtain more information in the worst case, and to obtain more information than the worst case for a given number of links, the adversary needs to wire-tap more links. We also bound the corresponding differences.

Proposition C.43 (Monotonicity of RDRPs). *Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$, and $0 \leq \mu \leq n-1$, it holds that $K_{M,0}(\mathcal{C}_1, \mathcal{C}_2) = 0$, $K_{M,n}(\mathcal{C}_1, \mathcal{C}_2) = \dim(\mathcal{C}_1 / \mathcal{C}_2)$ and*

$$0 \leq K_{M,\mu+1}(\mathcal{C}_1, \mathcal{C}_2) - K_{M,\mu}(\mathcal{C}_1, \mathcal{C}_2) \leq m.$$

Proof. The only property that is not trivial from the definitions is $K_{M,\mu+1}(\mathcal{C}_1, \mathcal{C}_2) - K_{M,\mu}(\mathcal{C}_1, \mathcal{C}_2) \leq m$. Consider $\mathcal{L} \subseteq \mathbb{F}^n$ with $\dim(\mathcal{L}) \leq \mu + 1$ and $\dim(\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}}) - \dim(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}}) = K_{M,\mu+1}(\mathcal{C}_1, \mathcal{C}_2)$.

Take $\mathcal{L}' \subsetneqq \mathcal{L}$ with $\dim(\mathcal{L}') = \dim(\mathcal{L}) - 1$. Using (C.2), a simple computation shows that

$$\dim(\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}'}) + m \geq \dim(\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}}).$$

Since $\dim(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}'}) \leq \dim(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}})$, it holds that

$$\begin{aligned} &\dim(\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}'}) - \dim(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}'}) + m \\ &\geq \dim(\mathcal{C}_1 \cap \mathcal{V}_{\mathcal{L}}) - \dim(\mathcal{C}_2 \cap \mathcal{V}_{\mathcal{L}}), \end{aligned}$$

and the result follows. □

Proposition C.44 (Monotonicity of RGMWs). *Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$ with $\ell = \dim(\mathcal{C}_1 / \mathcal{C}_2)$, it holds that*

$$0 \leq d_{M,r+1}(\mathcal{C}_1, \mathcal{C}_2) - d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \leq \min\{m, n\},$$

for $1 \leq r \leq \ell - 1$, and

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) + 1 \leq d_{M,r+m}(\mathcal{C}_1, \mathcal{C}_2),$$

for $1 \leq r \leq \ell - m$.

Proof. The first inequality in the first equation is obvious. We now prove the second inequality. By Proposition C.12, there exists a subspace $\mathcal{D} \subseteq \mathcal{C}_1$ with $\mathcal{D} \cap \mathcal{C}_2 = \{0\}$, $\dim(\mathcal{D}) = r$ and $\mathrm{wt_R}(\mathcal{D}) = d_{M,r}(\mathcal{C}_1, \mathcal{C}_2)$. Now take $D \in \mathcal{C}_1$ not contained in $\mathcal{D} \oplus \mathcal{C}_2$, and consider $\mathcal{D}' = \mathcal{D} \oplus \langle \{D\} \rangle$. We see from the definitions that $\mathrm{RSupp}(\mathcal{D}') \subseteq \mathrm{RSupp}(\mathcal{D}) + \mathrm{Row}(D)$, and hence

$$\mathrm{wt_R}(\mathcal{D}') \leq \mathrm{wt_R}(\mathcal{D}) + \mathrm{Rk}(D) \leq d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) + \min\{m, n\}.$$

Therefore it follows that $d_{M,r+1}(\mathcal{C}_1, \mathcal{C}_2) \leq d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) + \min\{m, n\}$.

The last inequality follows from Proposition C.14 and Proposition C.43. □

Due to Theorem C.9, the first and third inequalities in the previous proposition coincide with items 3 and 4 in [34, Theorem 30] when $\mathcal{C}_2 = \{0\}$ and $m \neq n$.

7.2 Upper and lower Singleton-type bounds

Due to Theorem C.1, it is desirable to obtain nested linear code pairs with large RGMWs. The following result gives a fundamental upper bound on them, whose achievability for one linear code ($\mathcal{C}_2 = \{0\}$) is studied in the next subsection.

Theorem C.5 (Upper Singleton-type bound). *Given nested linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1 \subseteq \mathbb{F}^{m \times n}$ and $1 \leq r \leq \ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$, it holds that*

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \leq n - \left\lceil \frac{\ell - r + 1}{m} \right\rceil + 1. \tag{C.13}$$

In particular, it follows that

$$\dim(\mathcal{C}_1/\mathcal{C}_2) \leq \max\{m, n\}(\min\{m, n\} - d_R(\mathcal{C}_1, \mathcal{C}_2) + 1),$$

which extends (C.8) to nested linear code pairs.

Proof. First of all, we have that $d_{M,\ell}(\mathcal{C}_1, \mathcal{C}_2) \leq n$ by definition. Therefore the case $r = \ell$ follows.

For the general case, we will prove that $md_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \leq mn - \ell + r + m - 1$. Assume that $1 \leq r \leq \ell - hm$, where the integer $h \geq 0$ is the maximum possible. That is, $r + (h+1)m > \ell$. Using Proposition C.44, we obtain

$$md_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \leq md_{M,r+hm}(\mathcal{C}_1, \mathcal{C}_2) - hm$$

$$\leq md_{M,\ell}(\mathcal{C}_1, \mathcal{C}_2) - hm \leq mn - \ell + r + m - 1,$$

where the last inequality follows from $md_{M,\ell}(\mathcal{C}_1, \mathcal{C}_2) \leq mn$ and $r + (h+1)m - 1 \geq \ell$.

Finally, the last bound is obtained by setting $r = 1$ and using Corollary C.13 for the given nested linear code pair and the pair obtained by transposing matrices. □

Due to Theorem C.9, the previous theorem coincides with item 5 in [34, Theorem 30] when $\mathcal{C}_2 = \{0\}$ and $m \neq n$.

Remark C.45. *In view of [24, Proposition 1] or [26, Equation (24)], it is natural to wonder whether a sharper bound of the form*

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \leq n - \left\lceil \frac{\dim(\mathcal{C}_1) - r + 1}{m} \right\rceil + 1$$

holds. However, this is not the case in general, as the following example shows.

Example C.46. Consider $m = 2$, the canonical basis $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ of $\mathbb{F}^n$, and the linear codes $\mathcal{C}_1 = \mathbb{F}^{2\times n}$ and

$$\mathcal{C}_2 = \left\langle \left(\begin{array}{c} \mathbf{e}_1 \\ \mathbf{0} \end{array} \right), \left(\begin{array}{c} \mathbf{e}_2 \\ \mathbf{0} \end{array} \right), \ldots, \left(\begin{array}{c} \mathbf{e}_n \\ \mathbf{0} \end{array} \right) \right\rangle.$$

Observe that $\ell = \dim(\mathcal{C}_1/\mathcal{C}_2) = n$. A bound as in the previous remark would imply that $d_{M,n}(\mathcal{C}_1, \mathcal{C}_2) \leq \lceil n/2 \rceil$. However, a direct inspection shows that $d_{M,n}(\mathcal{C}_1, \mathcal{C}_2) = n$, since all vectors $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ must lie in the row space of any $\mathcal{D}$ with $\mathcal{C}_1 = \mathcal{C}_2 \oplus \mathcal{D}$.

On the other hand, we have the following lower bound:

Theorem C.6 (Lower Singleton-type bound). *Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^{m\times n}$ and $1 \leq r \leq \dim(\mathcal{C}_1/\mathcal{C}_2)$, it holds that $md_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \geq r$, which implies that*

$$d_{M,r}(\mathcal{C}_1, \mathcal{C}_2) \geq \left\lceil \frac{r}{m} \right\rceil. \tag{C.14}$$

Proof. Take a subspace $\mathcal{D} \subseteq \mathbb{F}^{m\times n}$ and define $\mathcal{L} = \mathrm{RSupp}(\mathcal{D})$. We have that $\mathcal{D} \subseteq \mathcal{V}_{\mathcal{L}}$. Using (C.2), we see that

$$m\mathrm{wt}_{\mathrm{R}}(\mathcal{D}) = m \dim(\mathcal{L}) = \dim(\mathcal{V}_{\mathcal{L}}) \geq \dim(\mathcal{D}).$$

The result follows from this and Proposition C.12. □

Due to Theorem C.9, the previous theorem coincides with item 6 in [34, Theorem 30] when $\mathcal{C}_2 = \{0\}$ and $m \neq n$.

7.3 Linear codes attaining the bounds and whose dimensions are divisible by the packet length

In this subsection, we study the achievability of the bounds (C.13) and (C.14) for one linear code whose dimension is divisible by the packet length m. As we will show in Subsection 8.3, DGWs [34] of one linear code coincide with its GMWs when $m \neq n$. Thus the two propositions below coincide with Corollaries 31 and 32 in [34] when $m \neq n$.

Recall from (C.8) that, if a linear code is MRD and $n \leq m$, then its dimension is divisible by m. In the next proposition, we show that GMWs of MRD linear codes for $n \leq m$ are all given by m, n and $\dim(\mathcal{C})$, and all attain the upper Singleton-type bound (C.13):

Proposition C.47. *Let $\mathcal{C} \subseteq \mathbb{F}^{m\times n}$ be a linear code with $\dim(\mathcal{C}) = mk$. The following are equivalent if $n \leq m$:*

1. *$\mathcal{C}$ is maximum rank distance (MRD).*

2. *$d_R(\mathcal{C}) = n - k + 1$.*

3. $d_{M,r}(\mathcal{C}) = n - k + \left\lfloor \frac{r-1}{m} \right\rfloor + 1$, *for all* $1 \leq r \leq mk$.

Proof. Item 1 and item 2 are equivalent by definition, and item 3 implies item 2 by choosing $r = 1$.

Now assume item 2 and let $1 \leq r \leq mk$. Let $r = hm + s$, with $h \geq 0$ and $0 \leq s < m$. We need to distinguish the cases $s > 0$ and $s = 0$. We prove only the first case, being the second analogous. By Proposition C.44, we have that

$$d_{M,r}(\mathcal{C}) \geq h + d_{M,s}(\mathcal{C}) \geq h + d_R(\mathcal{C}) = n - k + h + 1.$$

On the other hand, $\lceil (mk - r + 1)/m \rceil = k - h$, and therefore the bound (C.13) implies that

$$d_{M,r}(\mathcal{C}) \leq n - k + h + 1,$$

and hence $d_{M,r}(\mathcal{C}) = n - k + \lfloor (r-1)/m \rfloor + 1$ since $\lfloor (r-1)/m \rfloor = h$, and item 3 follows. □

Regarding the lower Singleton-type bound, we show in the next proposition that rank support spaces are also characterized by having the minimum possible GMWs in view of (C.14):

Proposition C.48. *Let* $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$ *be a linear code with* $\dim(\mathcal{C}) = mk$. *The following are equivalent:*

1. *$\mathcal{C}$ is a rank support space. That is, there exists a subspace $\mathcal{L} \subseteq \mathbb{F}^n$ such that $\mathcal{C} = \mathcal{V}_{\mathcal{L}}$.*
2. $d_{M,km}(\mathcal{C}) = k$.
3. $d_{M,r}(\mathcal{C}) = \lceil r/m \rceil$, *for all* $1 \leq r \leq mk$.

Proof. Assume that $\mathcal{C} = \mathcal{V}_{\mathcal{L}}$, as in item 1. By taking a sequence of subspaces

$$\{\mathbf{0}\} \subsetneqq \mathcal{L}_1 \subsetneqq \mathcal{L}_2 \subsetneqq \ldots \subsetneqq \mathcal{L}_k = \mathcal{L},$$

we see that $d_{M,rm-p}(\mathcal{C}) \leq \dim(\mathcal{L}_r) = r$, for $1 \leq r \leq k$ and $0 \leq p \leq m-1$, since $\dim(\mathcal{C} \cap \mathcal{V}_{\mathcal{L}_r}) = \dim(\mathcal{V}_{\mathcal{L}_r}) = mr \geq mr - p$. Hence item 3 follows.

Item 3 implies item 2 by taking $r = km$.

Finally, assume item 2. Take a subspace $\mathcal{L} \subseteq \mathbb{F}^n$ such that $\dim(\mathcal{L}) = d_{M,km}(\mathcal{C}) = k$ and $\dim(\mathcal{C} \cap \mathcal{V}_{\mathcal{L}}) \geq mk$. By definition and by (C.2), it holds that $\dim(\mathcal{C} \cap \mathcal{V}_{\mathcal{L}}) \geq mk = \dim(\mathcal{V}_{\mathcal{L}})$, which implies that $\mathcal{C} \cap \mathcal{V}_{\mathcal{L}} = \mathcal{V}_{\mathcal{L}}$, or in other words, $\mathcal{V}_{\mathcal{L}} \subseteq \mathcal{C}$. Since $\dim(\mathcal{C}) = mk = \dim(\mathcal{V}_{\mathcal{L}})$, we see that $\mathcal{V}_{\mathcal{L}} = \mathcal{C}$ and item 1 follows. □

8 Relation with other existing notions of generalized weights

In this section, we study the relation between RGMWs and RDRPs and other notions of generalized weights (see Table C.1). We first show that RGMWs and RDRPs extend RGRWs and RDIPs [24, 32] (Theorem C.7 in Subsection 8.1), respectively, then we show that they extend RGHWs and RDLPs [16, 26, 42] (Theorem C.8 in Subsection 8.2), respectively, and we conclude by showing that GMWs coincide with DGWs [34] for one linear code, meaning $\mathcal{C}_1 = \mathcal{C}$ arbitrary and $\mathcal{C}_2 = \{0\}$, when $m \neq n$, and are strictly larger when $m = n$ (Theorem C.9 in Subsection 8.3).

8.1 RGMWs extend relative generalized rank weights

In this subsection, we prove that RGMWs and RDRPs extend RGRWs and RDIPs [24, 32], respectively.

Definition C.49 (Galois closed spaces [41]). We say that an $\mathbb{F}_{q^m}$-linear vector space $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$ is Galois closed if

$$\mathcal{V}^q = \{(v_1^q, v_2^q, \ldots, v_n^q) \mid (v_1, v_2, \ldots, v_n) \in \mathcal{V}\} \subseteq \mathcal{V}.$$

We denote by $\Upsilon(\mathbb{F}_{q^m}^n)$ the family of $\mathbb{F}_{q^m}$-linear Galois closed vector spaces in $\mathbb{F}_{q^m}^n$.

RGRWs and RDIPs are then defined in [24] as follows:

Definition C.50 (Relative Generalized Rank Weigths [24, Definition 2]). Given nested $\mathbb{F}_{q^m}$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$, and $1 \leq r \leq \ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$ (over $\mathbb{F}_{q^m}$), we define their r-th relative generalized rank weight (RGRW) as

$$\begin{aligned} d_{R,r}(\mathcal{C}_1, \mathcal{C}_2) = \min\{ & \dim(\mathcal{V}) \mid \mathcal{V} \in \Upsilon(\mathbb{F}_{q^m}^n), \\ & \dim(\mathcal{C}_1 \cap \mathcal{V}) - \dim(\mathcal{C}_2 \cap \mathcal{V}) \geq r\}, \end{aligned}$$

where dimensions are taken over $\mathbb{F}_{q^m}$.

Definition C.51 (Relative Dimension/Intersection Profile [24, Definition 1]). Given nested $\mathbb{F}_{q^m}$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$, and $0 \leq \mu \leq n$, we define their μ-th relative dimension/intersection profile (RDIP) as

$$\begin{aligned} K_{R,\mu}(\mathcal{C}_1, \mathcal{C}_2) = \max\{ & \dim(\mathcal{C}_1 \cap \mathcal{V}) - \dim(\mathcal{C}_2 \cap \mathcal{V}) \mid \\ & \mathcal{V} \in \Upsilon(\mathbb{F}_{q^m}^n), \dim(\mathcal{V}) \leq \mu\}, \end{aligned}$$

where dimensions are taken over $\mathbb{F}_{q^m}$.

The following is the main result of the subsection, which shows that Theorem C.1 extends the study on worst-case information leakage on $\mathbb{F}_q$-linearly coded networks in [24] (see its Theorem 2 and Corollary 5) from $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$ to general $\mathbb{F}_q$-linear codes in $\mathbb{F}_q^{m \times n}$, when considering uniform probability distributions.

Theorem C.7. *Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be a basis of $\mathbb{F}_{q^m}$ as a vector space over $\mathbb{F}_q$. Given nested $\mathbb{F}_{q^m}$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$, and integers $1 \leq r \leq \ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$ (over $\mathbb{F}_{q^m}$), $0 \leq p \leq m-1$ and $0 \leq \mu \leq n$, we have that*

$$d_{R,r}(\mathcal{C}_1, \mathcal{C}_2) = d_{M,rm-p}(M_{\boldsymbol{\alpha}}(\mathcal{C}_1), M_{\boldsymbol{\alpha}}(\mathcal{C}_2)),$$

$$mK_{R,\mu}(\mathcal{C}_1, \mathcal{C}_2) = K_{M,\mu}(M_{\boldsymbol{\alpha}}(\mathcal{C}_1), M_{\boldsymbol{\alpha}}(\mathcal{C}_2)),$$

where $M_{\boldsymbol{\alpha}} : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^{m \times n}$ is as in (C.1).

The theorem follows from the next two lemmas, where we take the first one from [41]:

Lemma C.52 ([41, Lemma 1]). *An $\mathbb{F}_{q^m}$-linear vector space $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$ is Galois closed if, and only if, it has a basis of vectors in $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_{q^m}$.*

Lemma C.53. *Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be a basis of $\mathbb{F}_{q^m}$ as a vector space over $\mathbb{F}_q$, and let $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$ be an arbitrary set. The following are equivalent:*

1. *$\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$ is an $\mathbb{F}_{q^m}$-linear Galois closed vector space. That is, $\mathcal{V} \in \Upsilon(\mathbb{F}_{q^m}^n)$.*
2. *$M_{\boldsymbol{\alpha}}(\mathcal{V}) \subseteq \mathbb{F}_q^{m \times n}$ is a rank support space. That is, $M_{\boldsymbol{\alpha}}(\mathcal{V}) \in RS(\mathbb{F}_q^{m \times n})$.*

Moreover, if $M_{\boldsymbol{\alpha}}(\mathcal{V}) = \mathcal{V}_{\mathcal{L}}$ for a subspace $\mathcal{L} \subseteq \mathbb{F}_q^n$, then

$$\dim(\mathcal{V}) = \dim(\mathcal{L}),$$

where $\dim(\mathcal{V})$ is taken over $\mathbb{F}_{q^m}$ and $\dim(\mathcal{L})$ over $\mathbb{F}_q$.

Proof. We first observe the following. For an arbitrary set $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$, the previous lemma states that $\mathcal{V}$ is an $\mathbb{F}_{q^m}$-linear Galois closed vector space if, and only if, $\mathcal{V}$ is $\mathbb{F}_q$-linear and it has a basis over $\mathbb{F}_q$ of the form $\mathbf{v}_{i,j} = \alpha_i \mathbf{b}_j$, for $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, k$, where $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{F}_q^n$. By considering $B_{i,j} = M_{\boldsymbol{\alpha}}(\mathbf{v}_{i,j}) \in \mathbb{F}_q^{m \times n}$, we see that this condition is equivalent to item 2 in Proposition C.9, and we are done. □

Remark C.54. *The results in this subsection can be extended to Galois extensions of fields $\mathbb{F} \subseteq \widetilde{\mathbb{F}}$ of finite degree m. For that purpose, we only need to define Galois closed spaces as those $\widetilde{\mathbb{F}}$-linear subspaces $\mathcal{V} \subseteq \widetilde{\mathbb{F}}^n$ that are closed under the action of every field morphism in the Galois group of the extension $\mathbb{F} \subseteq \widetilde{\mathbb{F}}$. The rest of definitions and results in this subsection can be directly translated word by word to this case, except for Lemma C.52, which would be replaced by [18, Theorem 1].*

Thus the results in this subsection can be applied to generalizations of rank-metric codes such as those in [2].

8.2 RGMWs extend relative generalized Hamming weights

In this subsection, we show that RGMWs and RDRPs also extend RGHWs and RDLPs [16, 26, 42], respectively. We start with the definitions of Hamming supports and Hamming support spaces:

Definition C.55 (Hamming supports). Given a vector space $\mathcal{C} \subseteq \mathbb{F}^n$, we define its Hamming support as

$$\begin{aligned}\mathrm{HSupp}(\mathcal{C}) = \{i \in \{1, 2, \ldots, n\} \mid \\ \exists (c_1, c_2, \ldots, c_n) \in \mathcal{C}, c_i \neq 0\}.\end{aligned}$$

We also define the Hamming weight of the space $\mathcal{C}$ as

$$\mathrm{wt_H}(\mathcal{C}) = |\mathrm{HSupp}(\mathcal{C})|.$$

Finally, for a vector $\mathbf{c} \in \mathbb{F}^n$, we define its Hamming support as $\mathrm{HSupp}(\mathbf{c}) = \mathrm{HSupp}(\langle \{\mathbf{c}\} \rangle)$, and its Hamming weight as $\mathrm{wt_H}(\mathbf{c}) = \mathrm{wt_H}(\langle \{\mathbf{c}\} \rangle)$.

Definition C.56 (Hamming support spaces). Given a subset $I \subseteq \{1, 2, \ldots, n\}$, we define its Hamming support space as the vector space in $\mathbb{F}^n$ given by

$$\mathcal{L}_I = \{(c_1, c_2, \ldots, c_n) \in \mathbb{F}^n \mid c_i = 0, \forall i \notin I\}.$$

We may now define RGHWs and RDLPs:

Definition C.57 (Relative Generalized Hamming Weigths [26, Section III]). Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^n$, and $1 \leq r \leq \ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$, we define their r-th relative generalized Hamming weight (RGHW) as

$$\begin{aligned}d_{H,r}(\mathcal{C}_1, \mathcal{C}_2) = \min\{|I| \mid I \subseteq \{1, 2, \ldots, n\}, \\ \dim(\mathcal{C}_1 \cap \mathcal{L}_I) - \dim(\mathcal{C}_2 \cap \mathcal{L}_I) \geq r\}.\end{aligned}$$

As in Proposition C.12, it holds that

$$\begin{aligned}d_{H,r}(\mathcal{C}_1, \mathcal{C}_2) = \min\{\mathrm{wt_H}(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C}_1, \mathcal{D} \cap \mathcal{C}_2 = \{0\}, \\ \dim(\mathcal{D}) = r\}.\end{aligned}$$

Given a linear code $\mathcal{C} \subseteq \mathbb{F}^n$, we see that its r-th GHW [42, Section II] is $d_{H,r}(\mathcal{C}) = d_{H,r}(\mathcal{C}, \{\mathbf{0}\})$, for $1 \leq r \leq \dim(\mathcal{C})$.

Definition C.58 (Relative Dimension/Length Profile [16, 26]). Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^n$, and $0 \leq \mu \leq n$, we define their μ-th relative dimension/length profile (RDLP) as

$$\begin{aligned}K_{H,\mu}(\mathcal{C}_1, \mathcal{C}_2) = \max\{\dim(\mathcal{C}_1 \cap \mathcal{L}_I) - \dim(\mathcal{C}_2 \cap \mathcal{L}_I) \mid \\ I \subseteq \{1, 2, \ldots, n\}, |I| \leq \mu\}.\end{aligned}$$

To prove our results, we need to see vectors in $\mathbb{F}^n$ as matrices in $\mathbb{F}^{n\times n}$. To that end, we introduce the diagonal matrix representation map $\Delta : \mathbb{F}^n \longrightarrow \mathbb{F}^{n\times n}$ given by

$$\Delta(\mathbf{c}) = \operatorname{diag}(\mathbf{c}) = (c_i \delta_{i,j})_{1\leq i\leq n, 1\leq j\leq n}, \tag{C.15}$$

where $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in \mathbb{F}^n$ and $\delta_{i,j}$ represents the Kronecker delta. In other words, $\Delta(\mathbf{c})$ is the diagonal matrix whose diagonal vector is $\mathbf{c}$.

The map $\Delta : \mathbb{F}^n \longrightarrow \mathbb{F}^{n\times n}$ is linear, one to one and, for any vector space $\mathcal{D} \subseteq \mathbb{F}^n$, it holds that

$$\mathrm{wt}_{\mathrm{R}}(\Delta(\mathcal{D})) = \mathrm{wt}_{\mathrm{H}}(\mathcal{D}).$$

We may now give the main result of this subsection:

Theorem C.8. *Given nested linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}^n$, and integers $1 \leq r \leq \ell = \dim(\mathcal{C}_1/\mathcal{C}_2)$, and $0 \leq \mu \leq n$, we have that*

$$d_{H,r}(\mathcal{C}_1, \mathcal{C}_2) = d_{M,r}(\Delta(\mathcal{C}_1), \Delta(\mathcal{C}_2)),$$

$$K_{H,\mu}(\mathcal{C}_1, \mathcal{C}_2) = K_{M,\mu}(\Delta(\mathcal{C}_1), \Delta(\mathcal{C}_2)).$$

Proof. We prove the first equality, being the second analogous. Denote by d_r the number on the left-hand side and by d'_r the number on the right-hand side, and prove both inequalities:

$d_r \leq d'_r$: Take a vector space $\mathcal{L} \subseteq \mathbb{F}^n$ such that $\dim(\mathcal{L}) = d'_r$ and $\dim((\Delta(\mathcal{C}_1) \cap \mathcal{V}_{\mathcal{L}})/(\Delta(\mathcal{C}_2) \cap \mathcal{V}_{\mathcal{L}})) \geq r$. It holds that $\mathcal{V}_{\mathcal{L}} \cap \Delta(\mathbb{F}^n) = \Delta(\mathcal{L}_I)$, for some subset $I \subseteq \{1, 2, \ldots, n\}$. We have that $\dim((\mathcal{C}_1 \cap \mathcal{L}_I)/(\mathcal{C}_2 \cap \mathcal{L}_I)) \geq r$ and

$$d_r \leq |I| = \mathrm{wt}_{\mathrm{R}}(\Delta(\mathcal{L}_I)) \leq \mathrm{wt}_{\mathrm{R}}(\mathcal{V}_{\mathcal{L}}) = \dim(\mathcal{L}) = d'_r.$$

$d_r \geq d'_r$: Take a subset $I \subseteq \{1, 2, \ldots, n\}$ such that $|I| = d_r$ and $\dim((\mathcal{C}_1 \cap \mathcal{L}_I)/(\mathcal{C}_2 \cap \mathcal{L}_I)) \geq r$. Now it holds that $\Delta(\mathcal{L}_I) = \mathcal{V}_{\mathcal{L}_I} \cap \Delta(\mathbb{F}^n)$. Therefore $\dim((\Delta(\mathcal{C}_1) \cap \mathcal{V}_{\mathcal{L}_I})/(\Delta(\mathcal{C}_2) \cap \mathcal{V}_{\mathcal{L}_I})) \geq r$ and

$$d'_r \leq \dim(\mathcal{L}_I) = |I| = d_r.$$

8.3 Relation with Delsarte generalized weights

A notion of generalized weights, called Delsarte generalized weights (DGWs), for a linear code, which in this section means $\mathcal{C}_1 = \mathcal{C}$ arbitrary and $\mathcal{C}_2 = \{0\}$ has already been proposed in [34] as an algebraic invariant of the code. We will prove that GMWs are strictly larger than DGWs when $m = n$, and we will prove that both coincide in the other cases.

These weights are defined in terms of optimal anticodes for the rank metric:

Definition C.59 (Maximum rank distance). For a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$, we define its maximum rank distance as

$$\mathrm{MaxRk}(\mathcal{C}) = \max\{\mathrm{Rk}(\mathrm{C}) \mid C \in \mathcal{C}, C \neq 0\}.$$

The following bound is given in [35, Proposition 47]:

$$\dim(\mathcal{C}) \leq m\mathrm{MaxRk}(\mathcal{C}). \tag{C.16}$$

This leads to the definition of rank-metric optimal anticodes:

Definition C.60 (Optimal anticodes [34, Definition 22]). We say that a linear code $\mathcal{V} \subseteq \mathbb{F}^{m \times n}$ is a (rank-metric) optimal anticode if equality in (C.16) holds.

We will denote by $A(\mathbb{F}^{m \times n})$ the family of linear optimal anticodes in $\mathbb{F}^{m \times n}$.

In view of this, DGWs are defined in [34] as follows:

Definition C.61 (Delsarte generalized weights [34, Definition 23]). For a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$ and an integer $1 \leq r \leq \dim(\mathcal{C})$, we define its r-th Delsarte generalized weight (DGW) as

$$\begin{aligned} d_{D,r}(\mathcal{C}) = m^{-1} \min\{ \dim(\mathcal{V}) \mid \mathcal{V} \in A(\mathbb{F}^{m \times n}),\\ \dim(\mathcal{C} \cap \mathcal{V}) \geq r\}. \end{aligned}$$

Observe that $d_{D,r}(\mathcal{C})$ is an integer since the dimension of optimal anticodes is a multiple of m by definition.

Before giving the main result, we need the following proposition:

Proposition C.62. *If a set $\mathcal{V} \subseteq \mathbb{F}^{m \times n}$ is a rank support space, then it is a (rank-metric) optimal anticode. In other words, $RS(\mathbb{F}^{m \times n}) \subseteq A(\mathbb{F}^{m \times n})$. The reversed inclusion also holds if $m \neq n$.*

Proof. We first prove that $RS(\mathbb{F}^{m \times n}) \subseteq A(\mathbb{F}^{m \times n})$. Let $\mathcal{V} \in RS(\mathbb{F}^{m \times n})$ and let $B_{i,j}$, $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, k$, be a basis of $\mathcal{V}$ as in Proposition C.9, item 2. For any $V = \sum_{i=1}^{m} \sum_{j=1}^{k} \lambda_{i,j} B_{i,j} \in \mathcal{V}$, with $\lambda_{i,j} \in \mathbb{F}$, it holds that

$$\mathrm{Rk}(V) \leq \dim(\langle \mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \rangle) = k,$$

where $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ are as in Proposition C.9, item 2. Therefore $\dim(\mathcal{V}) = mk \geq m\mathrm{MaxRk}(\mathcal{V})$ and $\mathcal{V}$ is an optimal anticode.

We now prove that $A(\mathbb{F}^{m \times n}) \subseteq RS(\mathbb{F}^{m \times n})$ when $m \neq n$. Let $\mathcal{V} \in A(\mathbb{F}^{m \times n})$. By [34, Theorem 26], there exist full-rank matrices $A \in \mathbb{F}_q^{m \times m}$ and $B \in \mathbb{F}_q^{n \times n}$ such that $\mathcal{V} = \{ACB \in \mathbb{F}_q^{m \times n} \mid C \in \mathcal{V}_{\mathcal{L}}\}$, where $\mathcal{L} = \mathbb{F}_q^k \times \{0\}^{n-k}$ for some positive integer k. By Proposition C.9, $\mathcal{V}$ is a rank support space and we are done. □

In [34, Theorem 18] it is proven that $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$ is an $\mathbb{F}_{q^m}$-linear Galois closed vector space if, and only if, it is an $\mathbb{F}_{q^m}$-linear vector space satisfying equality in (C.16). Hence due to Lemma C.53, the previous proposition strengthens [34, Theorem 18] when $m \neq n$ by showing that the $\mathbb{F}_{q^m}$-linearity of $\mathcal{V}$ may be weakened to $\mathbb{F}_q$-linearity. Moreover, our result holds for any field $\mathbb{F} \neq \mathbb{F}_q$.

The main result of this subsection is the next theorem, which follows from the previous proposition and the corresponding definitions:

Theorem C.9. *For a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$ and an integer $1 \leq r \leq \dim(\mathcal{C})$, we have that*

$$d_{D,r}(\mathcal{C}) \leq d_{M,r}(\mathcal{C}) \text{ if } m = n, \text{ and}$$
$$d_{D,r}(\mathcal{C}) = d_{M,r}(\mathcal{C}) \text{ if } m \neq n.$$

Due to Theorem C.1, when considering universal security on linearly coded networks it is desirable to obtain linear codes $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ with large GMWs. Therefore, linear codes with large DGWs serve this purpose, but linear codes with low DGWs may still have large GMWs when $m = n$.

The next example shows that not all linear optimal anticodes are rank support spaces when $m = n$, that is, $RS(\mathbb{F}^{n \times n}) \subsetneqq A(\mathbb{F}^{n \times n})$, for any n and any field $\mathbb{F}$. As a consequence, in some cases GMWs are strictly larger than DGWs. To that end, we will use the characterization of rank support spaces as matrix modules from Appendix D.

Example C.63. Consider $m = n = 2$ and the linear code

$$\mathcal{C} = \left\langle \left(\begin{array}{cc} 1 & 0 \\ 0 & 0 \end{array} \right), \left(\begin{array}{cc} 0 & 1 \\ 0 & 0 \end{array} \right) \right\rangle \subseteq \mathbb{F}^{2 \times 2}.$$

It holds that $\dim(\mathcal{C}) = 2$, $m = 2$ and $\mathrm{MaxRk}(\mathcal{C}) = 1$. Therefore $\mathcal{C}$ is an optimal anticode. However, it is not a matrix module, and therefore it is not a rank support space (see Appendix D), since

$$\left(\begin{array}{cc} 0 & 0 \\ 1 & 0 \end{array} \right) \left(\begin{array}{cc} 1 & 0 \\ 0 & 0 \end{array} \right) = \left(\begin{array}{cc} 0 & 0 \\ 1 & 0 \end{array} \right) \notin \mathcal{C}.$$

In other words, $RS(\mathbb{F}^{2 \times 2}) \subsetneqq A(\mathbb{F}^{2 \times 2})$.

On the one hand, we have that $d_{D,1}(\mathcal{C}) = d_{D,2}(\mathcal{C}) = 1$, by [34, Corollary 32], or just by inspection.

On the other hand, it is easy to check that $d_{M,1}(\mathcal{C}) = 1$, and since $\mathrm{RSupp}(\mathcal{C}) = \mathbb{F}^2$, it holds that $d_{M,2}(\mathcal{C}) = 2$. Therefore $d_{M,2}(\mathcal{C}) > d_{D,2}(\mathcal{C})$.

Observe that we may trivially extend this example to any value of $m = n$, and it holds for an arbitrary field $\mathbb{F}$.

9 Conclusion and open problems

In this work, we have extended the study of universal security provided by $\mathbb{F}_{q^m}$-linear nested coset coding schemes from [24, 39] to that provided by $\mathbb{F}_q$-linear schemes, where $\mathbb{F}_q$ is the field used on the network and m is the packet length.

Thanks to this study, we have completed the list of parameters ℓ, t, m and n for which we can obtain optimal universal secure $\mathbb{F}_q$-linear codes for noiseless networks from [39], and we have added *near optimal* universal security to the rank list-decodable codes from [20], providing the first universal secure linear coset coding schemes able to list-decode in polynomial time roughly twice the rank errors that optimal universal secure schemes can unique-decode, with almost the same secret message size ℓ and security parameter t.

Motivated by our study, we defined a family of security equivalences between linear coset coding schemes and gave mathematical characterizations of such equivalences, which allowed us to obtain, in terms of the last generalized matrix weight, ranges of parameters m and n of networks on which a linear code can be applied with the same security performance.

Finally, we give the following list of open problems:

1) Obtain optimal universal secure and error-correcting linear coset coding schemes for noisy networks for all possible parameters ℓ, t, m, n, and number of rank errors.

2) Extend the concept of universal *strong security* from [24, Definition 6] to general $\mathbb{F}_q$-linear coset coding schemes, and provide optimal universal strong secure schemes as those in [24, Section V] for all possible parameters ℓ, t, m and n, for either noiseless or noisy networks.

3) Subsection 5.3 implies that ℓ is close to but smaller than $n-t-e$, where e is the number of list-decodable rank errors with polynomial list sizes L. We conjecture, but leave as open problem, that a bound similar to $\ell \leq n-t-e$ holds in general.

4) Study the sharpness of the bounds given in Theorem C.6.

A Duality theory

In this appendix, we collect technical results concerning trace duality of linear codes in $\mathbb{F}^{m\times n}$ used throughout the paper. Some of the results are taken or expanded from the literature, and some are new. Recall first the definition of trace product and dual of a linear code in $\mathbb{F}^{m\times n}$ (Definition C.15).

First, since the trace product in $\mathbb{F}^{m\times n}$ coincides with the usual inner product in $\mathbb{F}^{mn}$, it holds that

$$\dim(\mathcal{C}^\perp) = mn - \dim(\mathcal{C}), \quad \mathcal{C} \subseteq \mathcal{D} \Longleftrightarrow \mathcal{D}^\perp \subseteq \mathcal{C}^\perp,$$

$$\mathcal{C}^{\perp\perp} = \mathcal{C}, \quad (\mathcal{C} + \mathcal{D})^{\perp} = \mathcal{C}^{\perp} \cap \mathcal{D}^{\perp}, \quad (\mathcal{C} \cap \mathcal{D})^{\perp} = \mathcal{C}^{\perp} + \mathcal{D}^{\perp},$$

for linear codes $\mathcal{C}, \mathcal{D} \subseteq \mathbb{F}^{m \times n}$. We have the following:

Lemma C.64 ([35, Lemma 27]). *If $\mathcal{V} \in RS(\mathbb{F}^{m \times n})$, then $\mathcal{V}^{\perp} \in RS(\mathbb{F}^{m \times n})$. More concretely, for any subspace $\mathcal{L} \subseteq \mathbb{F}^n$, it holds that*

$$(\mathcal{V}_{\mathcal{L}})^{\perp} = \mathcal{V}_{(\mathcal{L}^{\perp})}.$$

Lemma C.65 (Forney's duality [16]). *Given vector spaces $\mathcal{C}, \mathcal{V} \subseteq \mathbb{F}^{m \times n}$, it holds that*

$$\dim(\mathcal{V}) - \dim((\mathcal{C}^{\perp}) \cap \mathcal{V}) = \dim(\mathcal{C}) - \dim(\mathcal{C} \cap (\mathcal{V}^{\perp})).$$

We now show that all GMWs of a linear code determine uniquely those of the corresponding dual code. Since GMWs and DGWs [34] coincide when $\mathbb{F} = \mathbb{F}_q$ and $m \neq n$ by Theorem C.9, the next result coincides with [34, Corollary 38] in such cases:

Proposition C.66. *Given a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$ with $k = \dim(\mathcal{C})$, and given an integer $p \in \mathbb{Z}$, define*

$$\begin{aligned} W_p(\mathcal{C}) =& \{d_{M,p+rm}(\mathcal{C}) \mid r \in \mathbb{Z}, 1 \leq p + rm \leq k\}, \\ \overline{W}_p(\mathcal{C}) =& \{n + 1 - d_{M,p+rm}(\mathcal{C}) \mid r \in \mathbb{Z}, 1 \leq p + rm \leq k\}. \end{aligned}$$

Then it holds that

$$\{1, 2, \ldots, n\} = W_p(\mathcal{C}^{\perp}) \cup \overline{W}_{p+k}(\mathcal{C}),$$

where the union is disjoint.

The proof of this proposition can be translated word by word from the proof of [34, Corollary 38] using the monotonicity properties from Proposition C.44. However, [34, Corollary 38] relies on [34, Theorem 37], and therefore we need to extend such result to the cases $\mathbb{F} \neq \mathbb{F}_q$ or $m = n$. The following lemma constitutes such extension:

Lemma C.67. *Given a linear code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$ with $k = \dim(\mathcal{C})$, and given $1 \leq r \leq k$ and $1 \leq s \leq mn - k$, it holds that*

$$d_{M,s}(\mathcal{C}^{\perp}) \neq n + 1 - d_{M,r}(\mathcal{C})$$

if $r = p + k + r'm$ and $s = p + s'm$, for some integers $p, r', s' \in \mathbb{Z}$.

Proof. Assume that equality holds for a pair of such r and s. Denote $\mathcal{C}_{\mathcal{L}} = \mathcal{C} \cap \mathcal{V}_{\mathcal{L}}$, for a linear subspace $\mathcal{L} \subseteq \mathbb{F}^n$, and rewrite Proposition C.14 as follows:

$$\begin{aligned} d_{M,r}(\mathcal{C}) = \min\{\mu \mid \max\{ \dim(\mathcal{C}_{\mathcal{L}}) \mid \mathcal{L} \subseteq \mathbb{F}^n, \\ \dim(\mathcal{L}) = \mu\} \geq r\}. \end{aligned} \tag{C.17}$$

Write $d_{M,r}(\mathcal{C}) = \mu$. Then Equation (C.17) implies that

$$\max\{\dim(\mathcal{C}_{\mathcal{L}}) \mid \mathcal{L} \subseteq \mathbb{F}^n, \dim(\mathcal{L}) = \mu\} \geq r, \tag{C.18}$$

and μ is the minimum integer with such property. Now write $d_{M,s}(\mathcal{C}^\perp) = \nu = n + 1 - \mu$. In the same way, Equation (C.17) implies that

$$\max\{\dim((\mathcal{C}^\perp)_{\mathcal{L}}) \mid \mathcal{L} \subseteq \mathbb{F}^n, \dim(\mathcal{L}) = \nu\} \geq s.$$

On the other hand, given a subspace $\mathcal{L} \subseteq \mathbb{F}^n$ with $\dim(\mathcal{L}) = \nu$, we have that

$$\dim(\mathcal{C}_{\mathcal{L}^\perp}) = \dim(\mathcal{C} \cap (\mathcal{V}_{\mathcal{L}})^\perp) = k - m\nu + \dim((\mathcal{C}^\perp)_{\mathcal{L}}),$$

where the first equality follows from Lemma C.64, and the second equality follows from Lemma C.65 and Equation (C.2). Therefore, it holds that

$$\begin{aligned} &\max\{\dim(\mathcal{C}_{\mathcal{L}}) \mid \mathcal{L} \subseteq \mathbb{F}^n, \dim(\mathcal{L}) = \mu - 1\} \\ &\geq k - m\nu + s = k - mn - m + m\mu + s. \end{aligned} \tag{C.19}$$

From the fact that μ is the minimum integer satisfying Equation (C.18), and from Equation (C.19), we conclude that

$$k - mn - m + m\mu + s < r.$$

Now if we interchange the roles of $\mathcal{C}$ and $\mathcal{C}^\perp$, and the roles of r and s, then we automatically interchange the roles of μ and $n + 1 - \mu$, and the roles of k and $mn - k$. Therefore, we may also conclude that

$$k - mn + m\mu + s > r.$$

Using the expressions $r = p + k + r'm$ and $s = p + s'm$, and dividing everything by m, the previous two inequalities are, respectively

$$s' - n - 1 + \mu < r', \quad \text{and} \quad s' - n + \mu > r',$$

which contradict each other. Hence the lemma follows. □

Observe that the duality theorem for GRWs [12] is a direct consequence of Theorem C.7 and Proposition C.66:

Corollary C.68 ([12]). *Given an $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension k over $\mathbb{F}_{q^m}$, denote $d_r = d_{R,r}(\mathcal{C})$ and $d_s^\perp = d_{R,s}(\mathcal{C}^\perp)$, for $1 \leq r \leq k$ and $1 \leq s \leq n - k$. Then*

$$\begin{aligned} \{1, 2, \ldots, n\} = \{d_1, d_2, \ldots, d_k\} \\ \cup \{n + 1 - d_1^\perp, n + 1 - d_2^\perp, \ldots, n + 1 - d_{n-k}^\perp\}, \end{aligned}$$

where the union is disjoint.

Finally, we show that the duality theorem for GHWs [42] is a consequence of Theorem C.8 and Proposition C.66:

Corollary C.69 ([42]). *Given a linear code $\mathcal{C} \subseteq \mathbb{F}^n$ of dimension k, denote $d_r = d_{H,r}(\mathcal{C})$ and $d_s^\perp = d_{H,s}(\mathcal{C}^\perp)$, for $1 \leq r \leq k$ and $1 \leq s \leq n-k$. Then*

$$\{1,2,\ldots,n\} = \{d_1, d_2, \ldots, d_k\}$$

$$\cup \{n+1-d_1^\perp, n+1-d_2^\perp, \ldots, n+1-d_{n-k}^\perp\},$$

where the union is disjoint.

Proof. We will use the notation in Proposition C.66 during the whole proof. First of all, by Theorem C.8 it holds that $W_p(\Delta(\mathcal{C})) = \{d_{H,p}(\mathcal{C})\}$ if $1 \leq p \bmod n \leq k$ and $W_p(\Delta(\mathcal{C})) = \varnothing$ if $k+1 \leq p \bmod n \leq n-1$ or $p \bmod n = 0$. Therefore

$$\bigcup_{p=1}^{n} W_{p-k}(\Delta(\mathcal{C})) = \{d_1, d_2, \ldots, d_k\}.$$

On the other hand, from Proposition C.66 it follows that

$$\left(\bigcup_{p=1}^{n} W_{p-k}(\Delta(\mathcal{C})) \right) \cup \left(\bigcap_{p=1}^{n} \overline{W}_p(\Delta(\mathcal{C})^\perp) \right) = \{1,2,\ldots,n\},$$

where the union is disjoint. Hence we only need to show that $n+1-d_s^\perp \in \overline{W}_p(\Delta(\mathcal{C})^\perp)$, for $p = 1,2,\ldots,n$ and $s = 1,2,\ldots,n-k$.

Denote by $\mathcal{D}_n \subseteq \mathbb{F}^{n \times n}$ the vector space of matrices with zero components in their diagonals. It holds that $\Delta(\mathcal{C})^\perp = \Delta(\mathcal{C}^\perp) \oplus \mathcal{D}_n$.

Fix $1 \leq s \leq n-k$ and denote $d = d_{H,s}(\mathcal{C}^\perp)$. First, consider a subspace $\mathcal{D} \subseteq \mathcal{C}^\perp$ with $\mathrm{wt_H}(\mathcal{D}) = d$ and $\dim(\mathcal{D}) = s$, and define $\mathcal{D}' \subseteq \Delta(\mathcal{C})^\perp$ as the direct sum of $\Delta(\mathcal{D})$ and all matrices in $\mathcal{D}_n$ with columns in the Hamming support of $\mathcal{D}$. Since $\dim(\mathcal{D}') = d(n-1)+s$ and $\mathrm{wt_R}(\mathcal{D}') = d$, by Proposition C.12 it follows that

$$d_{M,d(n-1)+s}(\Delta(\mathcal{C})^\perp) \leq d. \tag{C.20}$$

On the other hand, assume that $d_{M,(d-1)(n-1)+s}(\Delta(\mathcal{C})^\perp) = d' < d$. Let $\mathcal{E} \subseteq \Delta(\mathcal{C})^\perp$ be such that $\mathrm{wt_R}(\mathcal{E}) = d'$ and $\dim(\mathcal{E}) = (d-1)(n-1)+s$. Denote by $\mathcal{E}_D$ the vector space of matrices obtained by replacing the elements outside the diagonal of those matrices in $\mathcal{E}$ by zero. If $\mathcal{L} = \mathrm{RSupp}(\mathcal{E}) \subseteq \mathbb{F}^n$, we claim that

$$\dim(\mathcal{E} \cap \mathcal{D}_n) \leq n\mathrm{wt_R}(\mathcal{E}) - \mathrm{wt_H}(\mathcal{L}). \tag{C.21}$$

It is sufficient to show that $\dim(\mathcal{V}_\mathcal{L} \cap \mathcal{D}_n) = n\dim(\mathcal{L}) - \mathrm{wt_H}(\mathcal{L})$. Denote by $\mathcal{V}_{\mathcal{L}D}$ the vector space of matrices obtained by replacing the elements outside the diagonal of those matrices in $\mathcal{V}_\mathcal{L}$ by zero. Then, by Proposition

C.9, $\dim(\mathcal{V}_{\mathcal{L}D}) = \mathrm{wt}_{\mathrm{H}}(\mathcal{L})$, and $\dim(\mathcal{V}_{\mathcal{L}} \cap \mathcal{D}_n) = \dim(\mathcal{V}_{\mathcal{L}}) - \dim(\mathcal{V}_{\mathcal{L}D}) = n\dim(\mathcal{L}) - \mathrm{wt}_{\mathrm{H}}(\mathcal{L})$.

By monotonicity (Proposition C.44), we have that $d' = d - 1$, and thus $\dim(\mathcal{E}) = d'(n-1) + s$. Therefore, by (C.21), $\dim(\Delta^{-1}(\mathcal{E}_D)) = \dim(\mathcal{E}_D) = \dim(\mathcal{E}) - \dim(\mathcal{E} \cap \mathcal{D}_n) \geq s + \mathrm{wt}_{\mathrm{H}}(\mathcal{L}) - d'$. Choose indices $i_1, i_2, \ldots, i_{\mathrm{wt}_{\mathrm{H}}(\mathcal{L})-d'}$ from $\mathrm{HSupp}(\Delta^{-1}(\mathcal{E}_D))$, and define

$$\mathcal{W} = \{\mathbf{c} \in \Delta^{-1}(\mathcal{E}_D) \mid c_{i_j} = 0, 1 \leq j \leq \mathrm{wt}_{\mathrm{H}}(\mathcal{L}) - d'\}.$$

Then $\mathcal{W} \subseteq \mathcal{C}^{\perp}$, $\dim(\mathcal{W}) \geq s$, and $\mathrm{wt}_{\mathrm{H}}(\mathcal{W}) \leq \mathrm{wt}_{\mathrm{H}}(\Delta^{-1}(\mathcal{E}_D)) - \mathrm{wt}_{\mathrm{H}}(\mathcal{L}) + d' \leq d'$, which implies $d_{H,s}(\mathcal{C}^{\perp}) = d' < d$, which is a contradiction. Hence

$$d_{M,(d-1)(n-1)+s}(\Delta(\mathcal{C})^{\perp}) \geq d. \tag{C.22}$$

Combining Equation (C.20) and Equation (C.22), we conclude that

$$d_{M,(d-1)(n-1)+s+j}(\Delta(\mathcal{C})^{\perp}) = d,$$

for $j = 0, 1, 2, \ldots, n-1$, which implies that $n + 1 - d_s^{\perp} \in \overline{W}_p(\Delta(\mathcal{C})^{\perp})$, for $p = 1, 2, \ldots, n$, and we are done. □

B Construction of explicit subspace designs

In this appendix, we recall how to construct the subspace design formed by $\mathcal{H}_0, \mathcal{H}_1, \mathcal{H}_2, \ldots \subseteq \mathbb{F}_{q^m}$ in Section 5. This construction is given in [20], based on a construction in [19], and is explicit in the sense that it can be constructed using an algorithm of polynomial complexity on q.

Fix $\varepsilon > 0$ and a positive integer s such that $4sn \leq \varepsilon m$, and assume that n divides m. Let $d_1 = q^{m/n-1}, d_2 = q^{m/n-2}, \ldots, d_{m/n} = 1$ and let $\gamma_1, \gamma_2, \ldots, \gamma_{m/n}$ be distinct non-zero elements of $\mathbb{F}_{q^n}$. Define

$$f_i(x_1, x_2 \ldots, x_{m/n}) = \sum_{j=1}^{m/n} \gamma_j^i x_j^{d_j},$$

for $i = 1, 2, \ldots, s$, and let $\mathcal{S} \subseteq \mathbb{F}_{q^n}^{m/n}$ be the set of common zeros of $f_1, f_2, \ldots, f_s$, which is an $\mathbb{F}_q$-linear vector space. We may assume that $\mathcal{S} \subseteq \mathbb{F}_{q^m}$ by an $\mathbb{F}_{q^n}$-linear vector space isomorphism $\mathbb{F}_{q^n}^{m/n} \cong \mathbb{F}_{q^m}$ (any isomorphism works).

Let β be a primitive element of $\mathbb{F}_{q^n}$. For $\alpha \in \mathbb{F}_{q^{n\lfloor \frac{\varepsilon m}{2ns} \rfloor}}$, let

$$\mathcal{S}_\alpha = \left\{ \alpha^{q^j} \beta^i \mid 0 \leq j < \left\lfloor \frac{\varepsilon m}{2ns} \right\rfloor, 0 \leq i < 2s \right\}.$$

The algorithm in [19, Subsection 4.3] gives in polynomial time over q a set $\mathcal{F} \subseteq \mathbb{F}_{q^{n\lfloor \frac{\varepsilon m}{2ns} \rfloor}}$ of size $q^{\Omega(\frac{\varepsilon m}{ns})}$ such that:

1. $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^{n\lfloor \frac{\varepsilon m}{2ns} \rfloor}}$, for all $\alpha \in \mathcal{F}$,
2. $\mathcal{S}_\alpha \cap \mathcal{S}_\beta = \varnothing$, for all distinct $\alpha, \beta \in \mathcal{F}$, and
3. $|\mathcal{S}_\alpha| = 2s\lfloor \frac{\varepsilon m}{2ns} \rfloor$, for all $\alpha \in \mathcal{F}$.

Define the $\mathbb{F}_{q^n}$-linear vector space $\mathcal{V}_\alpha \subseteq \mathbb{F}_{q^n}^{m/n}$ as

$$\begin{aligned}\mathcal{V}_\alpha = \{(a_0, a_1, \ldots, a_{m/n-1}) \in \mathbb{F}_{q^n}^{m/n} \mid \\ \sum_{i=0}^{m/n-1} a_i(\alpha\beta^j)^i = 0 \mid 0 \leq j < 2s\},\end{aligned}$$

for every $\alpha \in \mathcal{F}$, where we may consider $\mathcal{V}_\alpha \subseteq \mathbb{F}_{q^m}$ as before.

Finally, the $\mathbb{F}_q$-linear vector spaces $\mathcal{H}_0, \mathcal{H}_1, \mathcal{H}_2, \ldots \subseteq \mathbb{F}_{q^m}$ in Section 5 are defined as $\mathcal{H}_i = \mathcal{S} \cap \mathcal{V}_{\alpha_i}$, for distinct $\alpha_i \in \mathcal{F}$.

The constructions of $\mathcal{F}$ and $\mathcal{V}_\alpha$ appeared first in [19, Subsection 4.2] and $\mathcal{S}$ appeared first in [20, Corollary 6].

We conclude the appendix by computing the dimensions of the vector spaces $\mathcal{H}_0, \mathcal{H}_1, \mathcal{H}_2, \ldots \subseteq \mathbb{F}_{q^m}$, which is done in the proof of [20, Theorem 8]:

Lemma C.70 ([20]). *The vector spaces $\mathcal{H}_0, \mathcal{H}_1, \mathcal{H}_2, \ldots \subseteq \mathbb{F}_{q^m}$ have dimension at least $m(1-2\varepsilon)$ over $\mathbb{F}_q$.*

C Proof of Theorem C.4

In this appendix, we give the proof of Theorem C.4.

First we prove (P 1) $\Longrightarrow$ (P 2): It follows immediately from the characterization of rank support spaces in Proposition C.9, item 3.

Now we prove (P 2) $\Longrightarrow$ (P 3): Let $\mathcal{L} = \mathrm{RSupp}(\mathcal{D}) \subseteq \mathbb{F}^n$ and $\mathcal{L}' = \mathrm{RSupp}(\phi(\mathcal{D})) \subseteq \mathbb{F}^{n'}$. It holds that $\mathcal{V}_{\mathcal{L}} \subseteq \mathcal{V}$ and $\mathcal{V}_{\mathcal{L}'} \subseteq \mathcal{W}$, and they are the smallest rank support spaces in $\mathcal{V}$ and $\mathcal{W}$ containing $\mathcal{D}$ and $\phi(\mathcal{D})$, respectively, by Lemma C.8. Since ϕ preserves rank support spaces and their inclusions, we conclude that $\phi(\mathcal{V}_{\mathcal{L}}) = \mathcal{V}_{\mathcal{L}'}$, which implies that $\dim(\mathcal{L}) = \dim(\mathcal{L}')$ by (C.2), and (P 3) follows.

Next we prove (P 2) $\Longleftarrow$ (P 3): Assume that $\mathcal{U} \subseteq \mathcal{V}$ is a rank support space. This means that $m\mathrm{wt}_{\mathrm{R}}(\mathcal{U}) = \dim(\mathcal{U})$ by (C.2). Since ϕ satisfies (P 3) and is a vector space isomorphism, we conclude that $m\mathrm{wt}_{\mathrm{R}}(\phi(\mathcal{U})) = \dim(\phi(\mathcal{U}))$, and thus $\phi(\mathcal{U})$ is a rank support space also by (C.2). Similarly we may prove that, if $\phi(\mathcal{U})$ is a rank support space, then $\mathcal{U}$ is a rank support space.

Now we prove (P 3) $\Longrightarrow$ (P 4): Trivial from the fact that $\mathrm{wt}_{\mathrm{R}}(\langle\{C\}\rangle) = \mathrm{Rk}(C)$, for all $C \in \mathcal{V}$.

Finally we prove (P 1) $\Longleftarrow$ (P 2): Denote $\dim(\mathcal{V}) = \dim(\mathcal{W}) = mk$ and consider bases of $\mathcal{V}$ and $\mathcal{W}$ as in Proposition C.9, item 2. By defining vector space isomorphisms $\mathbb{F}^{m\times k} \longrightarrow \mathcal{V}$ and $\mathcal{W} \longrightarrow \mathbb{F}^{m\times k}$, sending such bases to the canonical basis of $\mathbb{F}^{m\times k}$, we see that we only need to prove the result for the particular case $\mathcal{V} = \mathcal{W} = \mathbb{F}^{m\times n}$.

Denote by $E_{i,j} \in \mathbb{F}^{m\times n}$ the matrices in the canonical basis, for $1 \leq i \leq m$, $1 \leq j \leq n$, that is, $E_{i,j}$ has 1 in its (i,j)-th component, and zeroes in its other components.

Consider the rank support space $\mathcal{U}_j = \langle E_{1,j}, E_{2,j}, \ldots, E_{m,j} \rangle \subseteq \mathbb{F}^{m\times n}$, for $1 \leq j \leq n$. Since $\phi(\mathcal{U}_j)$ is a rank support space, it has a basis $B_{i,j}$, $i = 1, 2, \ldots, m$, as in Proposition C.9, item 2, for a vector $\mathbf{b}_j \in \mathbb{F}^n$. This means that

$$\phi(E_{i,j}) = \sum_{s=1}^{m} a_{s,i}^{(j)} B_{s,j},$$

for some $a_{s,i}^{(j)} \in \mathbb{F}$, for all $s, i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$. If we define the matrix $A^{(j)} \in \mathbb{F}^{m\times m}$ whose (s,i)-th component is $a_{s,i}^{(j)}$, and $B \in \mathbb{F}^{n\times n}$ whose j-th row is $\mathbf{b}_j$, then a simple calculation shows that

$$\phi(E_{i,j}) = A^{(j)} E_{i,j} B,$$

and the matrices $A^{(j)}$ and B are invertible. If we prove that there exist non-zero $\lambda_j \in \mathbb{F}$ with $A^{(j)} = \lambda_j A^{(1)}$, for $j = 2, 3, \ldots, n$, then we are done, since we can take the vectors $\lambda_j \mathbf{b}_j$ instead of $\mathbf{b}_j$, define $A = A^{(1)}$, and then it holds that

$$\phi(E_{i,j}) = A E_{i,j} B,$$

for all $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$, implying (P 1).

To this end, we first denote by $\mathbf{a}_i^{(j)} \in \mathbb{F}^m$ the i-th column in $A^{(j)}$ (written as a row vector). Observe that we have already proven that ϕ preserves ranks. Hence $\mathrm{Rk}(\phi(E_{i,j} + E_{i,1})) = 1$, which means that $\mathrm{Rk}(A^{(j)} E_{i,j} + A^{(1)} E_{i,1}) = 1$, which implies that there exist $\lambda_{i,j} \in \mathbb{F}$ with

$$\mathbf{a}_i^{(j)} = \lambda_{i,j} \mathbf{a}_i^{(1)}.$$

On the other hand, a matrix calculation shows that

$$\begin{aligned}\phi\left(\sum_{i=1}^{m}\sum_{j=1}^{n} E_{i,j}\right) &= \left(\sum_{i=1}^{m} \mathbf{a}_i^{(1)}, \sum_{i=1}^{m} \mathbf{a}_i^{(2)}, \ldots, \sum_{i=1}^{m} \mathbf{a}_i^{(n)}\right) B \\ &= \left(\sum_{i=1}^{m} \mathbf{a}_i^{(1)}, \sum_{i=1}^{m} \lambda_{i,2} \mathbf{a}_i^{(1)}, \ldots, \sum_{i=1}^{m} \lambda_{i,n} \mathbf{a}_i^{(1)}\right) B.\end{aligned}$$

Since $\mathrm{Rk}(\sum_{i=1}^{m} \sum_{j=1}^{n} E_{i,j}) = 1$ and the vectors $\mathbf{a}_i^{(1)}$, $1 \leq i \leq m$, are linearly independent, we conclude that $\lambda_{i,j}$ depends only on j and not on i, and we are done.

D Matrix modules

Rank support spaces can also be seen as left submodules of the left module $\mathbb{F}^{m \times n}$ over the (non-commutative) ring $\mathbb{F}^{m \times m}$. This has been used in Example C.63. Since we think this result is of interest by itself, we include the characterization in this appendix.

Definition C.71 (Matrix modules). We say that a set $\mathcal{V} \subseteq \mathbb{F}^{m \times n}$ is a matrix module if

1. $V + W \in \mathcal{V}$, for every $V, W \in \mathcal{V}$, and
2. $MV \in \mathcal{V}$, for every $M \in \mathbb{F}^{m \times m}$ and every $V \in \mathcal{V}$.

Proposition C.72. *A set $\mathcal{V} \subseteq \mathbb{F}^{m \times n}$ is a rank support space if, and only if, it is a matrix module.*

Proof. Assume that $\mathcal{V}$ is a rank support space. Using the characterization in Proposition C.9, item 3, it is trivial to see that $\mathcal{V}$ is a matrix module.

Assume now that $\mathcal{V}$ is a matrix module. It holds that $\mathcal{V}$ is a vector space. Let $\mathcal{L} = \mathrm{RSupp}(\mathcal{V})$, and take $\mathbf{v} \in \mathcal{L}$. There exist $V_1, V_2, \ldots, V_s \in \mathcal{V}$ and $\mathbf{v}_j \in \mathrm{Row}(V_j)$, for $j = 1, 2, \ldots, s$, such that $\mathbf{v} = \sum_{j=1}^{s} \mathbf{v}_j$.

For fixed $1 \leq i \leq m$ and $1 \leq j \leq s$, it is well-known that there exists $M_{i,j} \in \mathbb{F}^{m \times m}$ such that $M_{i,j} V_j$ has $\mathbf{v}_j$ as its i-th row and the rest of its rows are zero vectors. Since $\mathcal{V}$ is closed under sums of matrices, we conclude that $\mathcal{V}_{\mathcal{L}} \subseteq \mathcal{V}$ and therefore both are equal. □

Acknowledgment

The work of U. Martínez-Peñas was supported by The Danish Council for Independent Research under Grant No. DFF-4002-00367 and Grant No. DFF-5137-00076B ("EliteForsk-Rejsestipendium"). The work of R. Matsumoto was supported by the Japan Society for the Promotion of Science under Grant No. 26289116. The authors wish to thank Alberto Ravagnani for clarifying the relation between GMWs and DGWs. The first author is also thankful for the support and guidance of his advisors Olav Geil and Diego Ruano. At the time of submission, the first author was visiting the Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto. He greatly appreciates the support and hospitality of Frank R. Kschischang. Finally, the authors also wish to thank the editor and anonymous reviewers for their very helpful comments.

References

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inform. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[2] D. Augot, P. Loidreau, and G. Robert, "Rank metric and gabidulin codes in characteristic zero," in *Proc. 2013 IEEE International Symposium on Information Theory*, July 2013, pp. 509–513.

[3] T. P. Berger, "Isometries for rank distance and permutation group of Gabidulin codes," *IEEE Trans. Inform. Theory*, vol. 49, no. 11, pp. 3016–3019, 2003.

[4] G. R. Blakley, "Safeguarding cryptographic keys," *International Workshop on Managing Requirements Knowledge*, vol. 0, p. 313, 1979.

[5] N. Cai and R. W. Yeung, "Network coding and error correction," *Proc. 2002 IEEE Inform. Theory Workshop*, pp. 119–122, 2002.

[6] ——, "Secure network coding," in *Proc. 2002 IEEE International Symposium on Information Theory*, 2002, p. 323.

[7] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan, "Secure computation from random error correcting codes," in *Advances in cryptology—EUROCRYPT 2007*, ser. Lecture Notes in Comput. Sci. Springer Berlin Heidelberg, 2007, vol. 4515, pp. 291–310.

[8] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley-Interscience, 2006.

[9] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *Journal of Combinatorial Theory, Series A*, vol. 25, no. 3, pp. 226–241, 1978.

[10] J. Dieudonné, "Sur une généralisation du groupe orthogonal à quatre variables," *Archiv der Mathematik*, vol. 1, no. 4, pp. 282–287, 1948.

[11] Y. Ding, "On list-decodability of random rank metric codes and subspace codes," *IEEE Trans. Inform. Theory*, vol. 61, no. 1, pp. 51–59, Jan. 2015.

[12] J. Ducoat, "Generalized rank weights: A duality statement," in *Topics in Finite Fields*, ser. Comtemporary Mathematics, G. L. M. G. Kyureghyan and A. Pott, Eds. American Mathematical Society, 2015, vol. 632, pp. 114–123.

[13] I. M. Duursma and S. Park, "Coset bounds for algebraic geometric codes," *Finite Fields Appl.*, vol. 16, no. 1, pp. 36–55, 2010.

[14] S. El Rouayheb, E. Soljanin, and A. Sprintson, “Secure network coding for wiretap networks of type II,” *IEEE Trans. Inform. Theory*, vol. 58, no. 3, pp. 1361–1371, Mar. 2012.

[15] J. Feldman, T. Malkin, R. Servedio, and C. Stein, “On the capacity of secure network coding,” in *Proc. 42nd Annual Allerton Conference on Communication, Control, and Computing*, 2004.

[16] G. D. Forney Jr., “Dimension/length profiles and trellis complexity of linear block codes,” *IEEE Trans. Inform. Theory*, vol. 40, no. 6, pp. 1741–1752, 1994.

[17] E. M. Gabidulin, “Theory of codes with maximum rank distance,” *Problems Inform. Transmission*, vol. 21, no. 1, pp. 1–12, 1985.

[18] M. Giorgetti and A. Previtali, “Galois invariance, trace codes and subfield subcodes,” *Finite Fields Appl.*, vol. 16, no. 2, pp. 96–99, 2010.

[19] V. Guruswami and S. Kopparty, “Explicit subspace designs,” *Combinatorica*, vol. 36, no. 2, pp. 161–185, Apr 2016.

[20] V. Guruswami, C. Wang, and C. Xing, “Explicit list-decodable rank-metric and subspace codes via subspace designs,” *IEEE Trans. Inform. Theory*, vol. 62, no. 5, pp. 2707–2718, May 2016.

[21] T. Ho, M. Médard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, “A random linear network coding approach to multicast,” *IEEE Trans. Inform. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.

[22] R. Jurrius and R. Pellikaan, “On defining generalized rank weights,” *Advances in Mathematics of Communications*, vol. 11, no. 1, pp. 225–235, 2017.

[23] R. Kötter and M. Médard, “An algebraic approach to network coding,” *IEEE/ACM Trans. Networking*, vol. 11, no. 5, pp. 782–795, Oct. 2003.

[24] J. Kurihara, R. Matsumoto, and T. Uyematsu, “Relative generalized rank weight of linear codes and its applications to network coding,” *IEEE Trans. Inform. Theory*, vol. 61, no. 7, pp. 3912–3936, Jul. 2015.

[25] S.-Y. R. Li, R. Yeung, and N. Cai, “Linear network coding,” *IEEE Trans. Inform. Theory*, vol. 49, no. 2, pp. 371–381, Feb. 2003.

[26] Y. Luo, C. Mitrpant, A. J. Han Vinck, and K. Chen, “Some new characters on the wire-tap channel of type II.” *IEEE Trans. Inform. Theory*, vol. 51, no. 3, pp. 1222–1229, 2005.

[27] M. Marcus and B. N. Moyls, "Linear transformations on algebras of matrices," *Canad. J. Math.*, vol. 11, pp. 61–66, 1959.

[28] U. Martínez-Peñas, "On the similarities between generalized rank and Hamming weights and their applications to network coding," *IEEE Trans. Inform. Theory*, vol. 62, no. 7, pp. 4081–4095, 2016.

[29] U. Martínez-Peñas and R. Matsumoto, "Unifying notions of generalized weights for universal security on wire-tap networks," in *Proc. 54th Annual Allerton Conference on Communication, Control, and Computing*, 2016, pp. 800–807.

[30] K. Morrison, "Equivalence for rank-metric and matrix codes and automorphism groups of Gabidulin codes," *IEEE Trans. Inform. Theory*, vol. 60, no. 11, pp. 7035–7046, Nov. 2014.

[31] C. K. Ngai, R. W. Yeung, and Z. Zhang, "Network generalized Hamming weight," *IEEE Trans. Inform. Theory*, vol. 57, no. 2, pp. 1136–1143, Feb 2011.

[32] F. E. Oggier and A. Sboui, "On the existence of generalized rank weights," in *Proc. 2012 International Symposium on Information Theory and its Applications*, 2012, pp. 406–410.

[33] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," in *Advances in Cryptology: EUROCRYPT 84*, ser. Lecture Notes in Comput. Sci. Springer Berlin Heidelberg, 1985, vol. 209, pp. 33–50.

[34] A. Ravagnani, "Generalized weights: An anticode approach," *Journal of Pure and Applied Algebra*, vol. 220, no. 5, pp. 1946–1962, 2016.

[35] ——, "Rank-metric codes and their duality theory," *Designs, Codes and Cryptography*, vol. 80, no. 1, pp. 197–216, 2016.

[36] R. M. Roth, "Maximum-rank array codes and their application to crisscross error correction," *IEEE Trans. Inform. Theory*, vol. 37, no. 2, pp. 328–336, Mar. 1991.

[37] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[38] D. Silva and F. R. Kschischang, "On metrics for error correction in network coding," *IEEE Trans. Inform. Theory*, vol. 55, no. 12, pp. 5479–5490, 2009.

[39] ——, "Universal secure network coding via rank-metric codes," *IEEE Trans. Inform. Theory*, vol. 57, no. 2, pp. 1124–1135, Feb. 2011.

[40] D. Silva, F. R. Kschischang, and R. Kötter, “A rank-metric approach to error control in random network coding,” *IEEE Trans. Inform. Theory*, vol. 54, no. 9, pp. 3951–3967, Sept 2008.

[41] H. Stichtenoth, “On the dimension of subfield subcodes,” *IEEE Trans. Inform. Theory*, vol. 36, no. 1, pp. 90–93, Jan. 1990.

[42] V. K. Wei, “Generalized Hamming weights for linear codes,” *IEEE Trans. Inform. Theory*, vol. 37, no. 5, pp. 1412–1418, 1991.

[43] A. D. Wyner, “The wire-tap channel,” *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[44] R. Zamir, S. Shamai, and U. Erez, “Nested linear/lattice codes for structured multiterminal binning,” *IEEE Trans. Inform. Theory*, vol. 48, no. 6, pp. 1250–1276, Jun. 2002.

[45] Z. Zhang and B. Zhuang, “An application of the relative network generalized hamming weight to erroneous wiretap networks,” in *2009 IEEE Inform. Theory Workshop*, Oct 2009, pp. 70–74.

Paper D

Universal secure rank-metric coding schemes with optimal communication overheads

Umberto Martínez-Peñas[1]

The paper has been submitted to
Cryptography and Communications, 21 pages,
and presented at the
IEEE International Symposium on Information Theory, Aachen, Germany,
June 2017.

[1] Department of Mathematical Sciences, Aalborg University, Aalborg 9220, Denmark

Abstract

We study the problem of reducing the communication overhead from a noisy wire-tap channel or storage system where data is encoded as a matrix, when more columns (or their linear combinations) are available. We present its applications to reducing communication overheads in universal secure linear network coding and secure distributed storage with crisscross errors and erasures and in the presence of a wire-tapper. Our main contribution is a method to transform coding schemes based on linear rank-metric codes, with certain properties, to schemes with lower communication overheads. By applying this method to pairs of Gabidulin codes, we obtain coding schemes with optimal information rate with respect to their security and rank error correction capability, and with universally optimal communication overheads, when $n \leq m$, being n and m the number of columns and number of rows, respectively. Moreover, our method can be applied to other families of maximum rank distance codes when $n > m$. The downside of the method is generally expanding the packet length, but some practical instances come at no cost.

Keywords: Communication overheads, crisscross error-correction, decoding bandwidth, information-theoretical security, rank-metric codes.

MSC: 94A60, 94A62, 94B99.

1 Introduction

Universal secure linear network coding with errors and erasures was first studied in [22], where rank-metric coding schemes were proposed to protect messages sent over a linearly coded network from link errors, erasures and information leakage to a wire-tapper. Similarly, rank-metric codes have been applied to storage systems where data is stored as a matrix and where errors and erasures affect several rows and/or columns, also called crisscross errors and erasures [21]. These errors and erasures have been recently motivated by correlated and mixed failures in distributed storage systems where data is stored in several data centers (columns), which in turn store several blocks of data (rows). See [14].

In this paper, we study how to reduce the communication overhead from such a noisy wire-tap channel or storage system to the receiver, when more columns, or their linear combinations, are available: Less ingoing links to the receiver fail in the network case, or more data centers are available and contacted in the distributed storage case. As it has been noticed in secret sharing in the literature [2, 13, 24], which corresponds to Hamming-metric erasure-correction and security, if more pieces of data (columns in our case) are available, they can be preprocessed via subpacketization so that the overall transmitted information from the channel or storage system to the receiver is reduced.

A similar concept of subpacketization has been recently developed for Reed-Solomon codes in [10]. In another direction, coding schemes recovering part of the encoded data (a node in a storage system, for instance), with respect to the Hamming metric, have already been studied, giving rise to *regenerating codes* [5, 6, 20], which reduce communication bandwidth, and *locally repairable codes* [9, 12, 23], which reduce the number of contacted nodes. The latter codes have been recently extended to the rank metric in [14]. In contrast, our aim is to recover the whole uncoded data while reducing the communication bandwidth, as in [2, 13, 24], but with respect to the rank metric and, as a consequence, with respect to the crisscross metric.

We illustrate and motivate the problem with a pair of examples. The details of the constructions will be given in Subsection 5.1.

Example D.1. Consider a linearly coded network, as in [22, Sec. VII-A], over a finite field of size $q = 256$ (8-bit symbols), with packet length $m = 2048$, number of outgoing links from the source $n = 40$, at least $N \geq n$ ingoing links to the sink, and where $\mu \leq 8$ links may be wire-tapped and $\rho \leq 16$ ingoing links to the sink may fail.

In [22, Th. 11], a coding scheme is given with optimal information rate 16/40, able to correct the given number of erasures and secure under the given number of observations over such network, independently of its inner code (*universally*). The overall communication overhead from the last ingoing links to the sink is of 8 packets: The source wants to transmit 16 uncoded packets and the sink receives 24 encoded packets.

Thanks to Theorem D.2 and dividing each packet into 32 subpackets of length 64 each, we will obtain a coding scheme with the same parameters, but such that the overall communication overhead at the ingoing links to the sink is of 4 packets (the minimum possible) if none of them fail (only 20 packets are received by the sink).

Example D.2. Let again $n = 40$ and $m = 2048$, and consider a distributed storage system where data is stored as an $m \times n$ matrix over the same finite field ($q = 256$), where each column corresponds to a data center that stores n symbols over $\mathbb{F}_q$, that is, 40 8-bit symbols. Assume that ρ data centers may fail or not be available, errors occur along t rows and/or columns due to certain correlations, and a wire-tapper eavesdrops μ data centers. Assume also that $\rho + 2t \leq 16$ and $\mu \leq 8$.

As in the previous example, the use of a pair of maximum rank distance codes allows to obtain the desired reliability and security while achieving the optimal information rate 16/40 (see [21]), with a communication overhead of 8 packets from the contacted data centers to the receiver. Again, in this work we obtain a coding scheme with the same parameters but where the communication overhead is reduced to 4 packets (the minimum possible) if no errors occur and all data centers are available and contacted.

The paper is organized as follows: In Section 2, we establish the information-theoretical setting, defining coherent linearized noisy wire-tap channels, which we take from [22], and we establish a method of subpacketization that allows to use linear codes over the extension field. In Section 3, we define communication overheads for these linearized channels and give lower bounds on these parameters similar to those in [13]. In Section 4, we give the main contribution of this paper, which is a general method to transform coding schemes based on pairs of linear rank-metric codes, with certain properties, into coding schemes with lower communication overheads. In Section 5, we apply Gabidulin codes [8, 21] to obtain coding schemes with optimal information rates and communication overheads for $n \leq m$, which can be seen as a rank-metric analog of the constructions in [2, 13]. However, our method allows us to correct errors, and not only erasures as in the secret sharing case [2, 13], and can be applied to other families of maximum rank distance codes, such as those in [7] for $n > m$. Finally, in Section 6, we discuss the applications in universal secure linear network coding and secure distributed storage with crisscross errors and erasures.

Notation

Throughout the paper, we fix a prime power q and positive integers m, n, N, α, ℓ, t, ρ and μ. We denote by $\mathbb{F}_q$ the finite field with q elements, $\mathbb{F}_q^n$ denotes the set of row vectors of length n over $\mathbb{F}_q$, and $\mathbb{F}_q^{m \times n}$ denotes the set of $m \times n$ matrices over $\mathbb{F}_q$. In this paper, a code is a subset of either $\mathbb{F}_q^n$ or $\mathbb{F}_q^{m \times n}$, whose linearity properties are specified in each case. For an $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, we will denote by $\mathcal{C}^\perp$ its dual code with respect to the usual $\mathbb{F}_{q^m}$-bilinear inner product. We also use the notation $[n] = \{1, 2, \ldots, n\}$ and $[m, n] = \{m, m+1, \ldots, n\}$ whenever $m \leq n$, and we denote by $H(X)$, $H(X \mid Y)$ and $I(X; Y)$ the entropy, conditional entropy and mutual information of the random variables X and Y, respectively (see [3]), where logarithms will always be taken with base q.

2 Information-theoretical setting and preliminaries

2.1 Coherent linearized channels and coset coding schemes

We will consider the secret message S to be a uniform random variable in $\mathcal{S} = \mathbb{F}_q^{\alpha m \times \ell}$, and we will consider noisy wire-tap channels (which can also be thought of as distributed storage systems) as given in [22]:

Definition D.3 (Coherent linearized channel [22]). We define a coherent linearized noisy wire-tap channel with t errors, ρ erasures with erasure matrix $A \in \mathbb{F}_q^{N \times n}$ of rank at least $n - \rho$, and μ observations as a channel with input a variable $X \in \mathcal{X} = \mathbb{F}_q^{\alpha m \times n}$, output to the receiver $Y \in \mathcal{Y} = \mathbb{F}_q^{\alpha m \times N}$, and output to the eavesdropper $W \in \mathcal{W} = \mathbb{F}_q^{\alpha m \times \mu}$, together with a conditional probability distribution $P(Y, W|X)$ such that

$$\begin{aligned} \mathcal{Y}_X = \{Y \in \mathbb{F}_q^{\alpha m \times N} \, | Y = XA^T + E, \\ E \in \mathbb{F}_q^{\alpha m \times N}, \mathrm{Rk}(E) \leq t\}, \\ \mathcal{W}_X = \{W \in \mathbb{F}_q^{\alpha m \times \mu} \, | W = XB^T, B \in \mathbb{F}_q^{\mu \times n}\}, \end{aligned}$$

where $\mathcal{Y}_X = \{Y \in \mathcal{Y} \mid P(Y|X) > 0\}$ and $\mathcal{W}_X = \{W \in \mathcal{W} \mid P(W|X) > 0\}$, for a given $X \in \mathcal{X}$.

In [22], it is shown that a linearly coded network over $\mathbb{F}_q$ with link errors, erasures and information leakage, and where the last coding coefficients are known to the receiver, can be modelled as a coherent linearized noisy wire-tap channel. We will focus on this scenario and discuss how to translate the results to the distributed storage scenario with crisscross errors and erasures in Subsection 6.2, since the latter can be seen as a simpler case.

As encoders, we consider coset coding schemes as in [16, Def. 7], which are a particular case of those in [22].

Definition D.4 (Coset coding schemes [16]). A coset coding scheme over the field $\mathbb{F}_q$ with secret message set $\mathcal{S} = \mathbb{F}_q^{\alpha m \times \ell}$ and coded message set $\mathcal{X} = \mathbb{F}_q^{\alpha m \times n}$ is a randomized function

$$F : \mathbb{F}_q^{\alpha m \times \ell} \longrightarrow \mathbb{F}_q^{\alpha m \times n},$$

where, for every $S \in \mathbb{F}_q^{\alpha m \times \ell}$, $C = F(S)$ is the uniform random variable over a set $\mathcal{C}_S \subseteq \mathbb{F}_q^{\alpha m \times n}$. To allow correct decoding, we also assume that $\mathcal{C}_S \cap \mathcal{C}_T = \varnothing$ if $S \neq T$. Finally, we define the information rate of the scheme as

$$R = \frac{\log_q(\#\mathcal{S})}{\log_q(\#\mathcal{X})} = \frac{\alpha m \ell}{\alpha m n} = \frac{\ell}{n}. \tag{D.1}$$

In linear network coding, universal reliability and security means correcting a number of link errors and erasures and being secure under a number of link observations, independently of the network inner code. This leads in [22] to the following definition:

Definition D.5 (Universal schemes [22]). We say that the coset coding scheme $F : \mathbb{F}_q^{\alpha m \times \ell} \longrightarrow \mathbb{F}_q^{\alpha m \times n}$ is:

1. Universally t-error and ρ-erasure-correcting if, for every coherent linearized channel with t errors, ρ erasures and erasure matrix $A \in \mathbb{F}_q^{N \times n}$, there exists a decoding function $D_A : \mathcal{Y} \longrightarrow \mathcal{S}$ such that
$$D_A(Y) = S,$$
for all $Y \in \bigcup_{X \in \mathcal{C}_S} \mathcal{Y}_X$ and all $S \in \mathcal{S}$.

2. Universally secure under μ observations if, for every coherent linearized channel with μ observations, it holds that
$$H(S|W) = H(S),$$
or equivalently $I(S;W) = 0$, for all $W \in \bigcup_{X \in \mathcal{C}_S} \mathcal{W}_X$ and all $S \in \mathcal{S}$.

2.2 Using linear codes over the extension field

In what follows, we will make use of codes that are linear over the extension field $\mathbb{F}_{q^m}$. To that end, we need to see how to identify matrices in $\mathbb{F}_q^{\alpha m \times n}$ with matrices in $\mathbb{F}_{q^m}^{\alpha \times n}$:

Definition D.6. Fix a basis $\gamma_1, \gamma_2, \ldots, \gamma_m$ of $\mathbb{F}_{q^m}$ as a vector space over $\mathbb{F}_q$, and define the map
$$\varphi_n : \mathbb{F}_{q^m}^{\alpha \times n} \longrightarrow \mathbb{F}_q^{\alpha m \times n} \tag{D.2}$$
as follows: Given a matrix $C \in \mathbb{F}_{q^m}^{\alpha \times n}$ with entries $c_{i,j} \in \mathbb{F}_{q^m}$, for $i = 1, 2, \ldots, \alpha$ and $j = 1, 2, \ldots, n$, we define $\varphi_n(C)$ as the unique $\alpha m \times n$ matrix with coefficients $d_{l,j} \in \mathbb{F}_q$, for $l = 1, 2, \ldots, \alpha m$ and $j = 1, 2, \ldots, n$, such that
$$c_{i,j} = \sum_{u=1}^{m} d_{(i-1)m+u,j} \gamma_u,$$
for $i = 1, 2, \ldots, \alpha$ and $j = 1, 2, \ldots, n$. Finally, we define the rank over $\mathbb{F}_q$ of a matrix $E \in \mathbb{F}_{q^m}^{\alpha \times n}$ as the rank over $\mathbb{F}_q$ of the matrix $\varphi_n(E) \in \mathbb{F}_q^{\alpha m \times n}$, and we denote it by $\mathrm{Rk}_q(E)$.

The key result is that the effect of coherent linearized noisy wire-tap channels in Definition D.3 remains unchanged by the map φ_n, as we will now see:

Lemma D.7. *Let $C \in \mathbb{F}_{q^m}^{\alpha \times n}$, $A \in \mathbb{F}_q^{N \times n}$ and $E \in \mathbb{F}_{q^m}^{\alpha \times N}$. It holds that*
$$\varphi_N \left(CA^T + E \right) = \varphi_n(C) A^T + \varphi_N(E),$$
and $\mathrm{Rk}_q(E) = \mathrm{Rk}(\varphi_N(E))$ *by definition.*

Proof. The additive property of φ_n is clear from the definition, so we may assume that $E = 0$. Denote the entries of C and $\varphi_n(C)$ as in Definition D.6, and let $a_{v,j}$, $\widetilde{c}_{i,j}$ and $\widetilde{d}_{l,j}$ be the entries of A, CA^T and $\varphi_N\left(CA^T\right)$, respectively, for $v = 1,2,\ldots,N$, $i = 1,2,\ldots,\alpha$, $l = 1,2,\ldots,\alpha m$ and $j = 1,2,\ldots,n$. It holds that

$$\widetilde{c}_{i,j} = \sum_{v=1}^{n} c_{i,v}a_{j,v} = \sum_{v=1}^{n}\left(\sum_{u=1}^{m} d_{(i-1)m+u,v}\gamma_u\right)a_{j,v}$$
$$= \sum_{u=1}^{m}\left(\sum_{v=1}^{n} d_{(i-1)m+u,v}a_{j,v}\right)\gamma_u,$$

but it also holds that

$$\widetilde{c}_{i,j} = \sum_{u=1}^{m} \widetilde{d}_{(i-1)m+u,j}\gamma_u,$$

for $i = 1,2,\ldots,\alpha$ and $j = 1,2,\ldots,n$. Since $\gamma_1,\gamma_2,\ldots,\gamma_m$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and $\sum_{v=1}^{n} d_{(i-1)m+u,v}a_{j,v} \in \mathbb{F}_q$, for $i = 1,2,\ldots,\alpha$, and $j = 1,2,\ldots,n$, we conclude that

$$\widetilde{d}_{(i-1)m+u,j} = \sum_{v=1}^{n} d_{(i-1)m+u,v}a_{j,v},$$

for $i = 1,2,\ldots,\alpha$, $u = 1,2,\ldots,m$ and $j = 1,2,\ldots,n$, which means that $\varphi_N\left(CA^T\right) = \varphi_n(C)A^T$, and the result follows. □

Hence we may identify the sets $\mathbb{F}_q^{\alpha m\times n}$ and $\mathbb{F}_{q^m}^{\alpha\times n}$, seen as $\mathbb{F}_q$-linear vector spaces together with the metric given by the rank and the function Rk_q, respectively. We will do this repeatedly throughout the paper.

To conclude the section, we recall the construction of coset coding schemes in [16, Def. 4] based on pairs of $\mathbb{F}_{q^m}$-linear codes with $\alpha = 1$ (no subpacketization).

Definition D.8 (Nested coset coding schemes [16]). A nested coset coding scheme (with $\alpha = 1$) is a coset coding scheme such that $\mathcal{C}_S = \varphi(S) + \mathcal{C}_2$, where $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$ are $\mathbb{F}_{q^m}$-linear codes and $\varphi : \mathbb{F}_{q^m}^{\ell} \longrightarrow \mathcal{W}$ is a vector space isomorphism over $\mathbb{F}_{q^m}$, for an $\mathbb{F}_{q^m}$-linear space $\mathcal{W} \subseteq \mathbb{F}_{q^m}^n$ such that $\mathcal{C}_1 = \mathcal{C}_2 \oplus \mathcal{W}$, where $\oplus$ denotes the direct sum of vector spaces.

To measure the reliability and security of these coding schemes, we need the concept of *relative minimum rank distance*, which is a particular case of [16, Def. 2]:

Definition D.9 (Relative minimum rank distance [16]). Given $\mathbb{F}_{q^m}$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$, we define their relative minimum rank distance as

$$d_R\left(\mathcal{C}_1,\mathcal{C}_2\right) = \min\left\{\mathrm{Rk}_q(\mathbf{e}) \mid \mathbf{e} \in \mathcal{C}_1, \mathbf{e} \notin \mathcal{C}_2\right\}.$$

The minimum rank distance of a single code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is defined as $d_R(\mathcal{C}) = d_R(\mathcal{C},\{\mathbf{0}\})$.

The next result, which follows directly from [16, Cor. 5 and Th. 4], gives the mentioned reliability and security performance of nested coset coding schemes. Recall that we denote by $\mathcal{C}^\perp$ the dual of an $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ with respect to the usual $\mathbb{F}_{q^m}$-bilinear inner product in $\mathbb{F}_{q^m}^n$.

Lemma D.10 ([16]). *Given $\mathbb{F}_{q^m}$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$, the nested coset coding scheme in Definition D.8 is universally t-error and ρ-erasure-correcting if, and only if, $2t + \rho < d_R(\mathcal{C}_1, \mathcal{C}_2)$, and is universally secure under μ observations if, and only if, $\mu < d_R\left(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp\right)$.*

Observe that $d_R(\mathcal{C}_1) \leq d_R(\mathcal{C}_1, \mathcal{C}_2)$ and $d_R\left(\mathcal{C}_2^\perp\right) \leq d_R\left(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp\right)$, hence the minimum rank distances of $\mathcal{C}_1$ and $\mathcal{C}_2^\perp$ give sufficient conditions on the number of correctable errors and erasures and on the number of links that may be wire-tapped without information leakage, respectively.

3 Communication overheads in coherent linearized channels

In this section we formalize how, as in communication efficient secret sharing [2, 13, 24], if a coset coding scheme is able to correct t errors and ρ erasures, but $d > n - \rho$ pieces of information are available (the rank of A is at least d), then we may reduce the communication overhead from the channel to the receiver by making use of the additional $d - n + \rho > 0$ linearly independent rows of A. Observe that only erasures, and not errors, are considered in the Hamming analog described in [2, 13, 24].

Let $F : \mathbb{F}_q^{\alpha m \times \ell} \longrightarrow \mathbb{F}_q^{\alpha m \times n}$ be a coset coding scheme, let $A \in \mathbb{F}_q^{d \times n}$ be of rank d (if $A \in \mathbb{F}_q^{N \times n}$ has rank $d < N$, we may delete or ignore linearly dependent rows), let $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_d \in \mathbb{F}_q^n$ be its rows, and let $E_{A,i} : \mathbb{F}_q^{\alpha m} \longrightarrow \mathbb{F}_q^{\beta_i m}$ be preprocessing functions, where $1 \leq \beta_i \leq \alpha$, for $i = 1, 2, \ldots, d$. We define their correction capability with respect to F as follows:

Definition D.11. For a full-rank matrix $A \in \mathbb{F}_q^{d \times n}$, the preprocessing functions $E_{A,i} : \mathbb{F}_q^{\alpha m} \longrightarrow \mathbb{F}_q^{\beta_i m}$, for $i = 1, 2, \ldots, d$, are t-error-correcting with respect to the coset coding scheme $F : \mathbb{F}_q^{\alpha m \times \ell} \longrightarrow \mathbb{F}_q^{\alpha m \times n}$ if there exists a decoding function $D_A : \prod_{i=1}^d \mathbb{F}_q^{\beta_i m} \longrightarrow \mathbb{F}_q^{\alpha m \times \ell}$ such that

$$D_A\left(\left(E_{A,i}\left(C\mathbf{a}_i^T + \mathbf{e}_i\right)\right)_{i=1}^d\right) = S, \tag{D.3}$$

for all $C \in \mathcal{C}_S$, all $S \in \mathbb{F}_q^{\alpha m \times \ell}$ and all error matrices $E \in \mathbb{F}_q^{\alpha m \times d}$ of rank at most t with columns $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_d \in \mathbb{F}_q^{\alpha m}$.

We define then the decoding bandwidth and communication overhead as q-analogs of those in [13, Def. 2]:

Definition D.12 (Decoding bandwidth and communication overhead). For a full-rank matrix $A \in \mathbb{F}_q^{d \times n}$ and functions $E_{A,i} : \mathbb{F}_q^{\alpha m} \longrightarrow \mathbb{F}_q^{\beta_i m}$, for $i = 1, 2, \ldots, d$, we define their decoding bandwidth and communication overhead, respectively, as

$$\mathrm{DB}(A) = \frac{\sum_{i=1}^{d} \beta_i m}{\alpha m} = \sum_{i=1}^{d} \frac{\beta_i}{\alpha} \quad \text{and} \quad \mathrm{CO}(A) = \sum_{i=1}^{d} \frac{\beta_i}{\alpha} - \ell.$$

Thus, if a *packet* is a vector in $\mathbb{F}_q^{\alpha m}$, then the decoding bandwidth is the amount (which need not be an integer due to the subpacketization) of packets that the receiver obtains, or needs to obtain, from the channel, and the communication overhead is the difference with respect to the original number of uncoded packets.

Observe that, fixing n and ℓ (thus the information rate), we may only focus on communication overheads, since both behave equally.

To measure the quality of a coset coding scheme, we need the following two bounds. The first is given in [22, Th. 12] and can be seen as a q-analog of the bound in [13, Prop. 1], although considering also errors and not only erasures:

Proposition D.13 ([22]). *If the coset coding scheme $F : \mathbb{F}_q^{\alpha m \times \ell} \longrightarrow \mathbb{F}_q^{\alpha m \times n}$ is universally t-error and ρ-erasure-correcting, and universally secure under μ observations, then*

$$\ell \leq n - 2t - \rho - \mu. \tag{D.4}$$

Next we give a q-analog of the bound in [13, Th. 1], again adding the effect of errors, which was not considered in [13]:

Proposition D.14. *If the coset coding scheme $F : \mathbb{F}_q^{\alpha m \times \ell} \longrightarrow \mathbb{F}_q^{\alpha m \times n}$ is universally secure under μ observations, then for a full-rank matrix $A \in \mathbb{F}_q^{d \times n}$ and preprocessing functions $E_{A,i} : \mathbb{F}_q^{\alpha m} \longrightarrow \mathbb{F}_q^{\beta_i m}$, for $i = 1, 2, \ldots, d$, that are t-error-correcting with respect to F, it holds that:*

$$\mathrm{CO}(A) \geq \frac{\ell(2t + \mu)}{d - 2t - \mu}, \tag{D.5}$$

Proof. We may assume without loss of generality that $\beta_1 \leq \beta_2 \leq \ldots \leq \beta_d$ as in the proof of [13, Th. 1].

First, we prove that the preprocessing functions $E_{A,i} : \mathbb{F}_q^{\alpha m} \longrightarrow \mathbb{F}_q^{\beta_i m}$, for $i = 1, 2, \ldots, d - 2t$ are 0-error-correcting with respect to $F : \mathbb{F}_q^{\alpha m \times \ell} \longrightarrow \mathbb{F}_q^{\alpha m \times n}$.

If they were not, then there would exist $C_1 \in \mathcal{C}_{S_1}$ and $C_2 \in \mathcal{C}_{S_2}$, with $S_1 \neq S_2$, such that

$$\left(E_{A,i} \left(C_1 \mathbf{a}_i^T \right) \right)_{i=1}^{d-2t} = \left(E_{A,i} \left(C_2 \mathbf{a}_i^T \right) \right)_{i=1}^{d-2t} .$$

On the other hand, there exist $\mathbf{e}_i \in \mathbb{F}_q^{\alpha m}$ such that $C_1 \mathbf{a}_i^T + \mathbf{e}_i = C_2 \mathbf{a}_i^T$, for $i = d-2t+1, d-2t+2, \ldots, d-t$, and $C_1 \mathbf{a}_i^T = C_2 \mathbf{a}_i^T + \mathbf{e}_i$, for $i = d-t+1, d-t+2, \ldots, d$. Thus we see that the preprocessing functions $E_{A,i} : \mathbb{F}_q^{\alpha m} \longrightarrow \mathbb{F}_q^{\beta_i m}$, for $i = 1, 2, \ldots, d$, cannot be t-error-correcting with respect to F, which is a contradiction.

Next, defining $f_i = E_{A,i} \left(C \mathbf{a}_i^T \right)$, where $C = F(S)$, for $i = 1, 2, \ldots, d-2t$ and $S \in \mathbb{F}_q^{\alpha m \times \ell}$, we may prove exactly as in the proof of [13, Th. 1] that

$$\sum_{i=1}^{d-2t} \frac{\beta_i}{\alpha} \geq \frac{\ell(d-2t)}{d-2t-\mu}, \tag{D.6}$$

and also

$$\frac{\beta_{d-2t-\mu}}{\alpha} \geq \frac{\ell}{d-2t-\mu}. \tag{D.7}$$

Now using that $\beta_{d-2t-\mu} \leq \beta_{d-2t-\mu+1} \leq \ldots \leq \beta_d$, and combining Equations (D.6) and (D.7), we conclude that

$$\begin{aligned} \mathrm{DB}(A) &= \left(\sum_{i=1}^{d-2t} \frac{\beta_i}{\alpha} \right) + \left(\sum_{i=d-2t+1}^{d} \frac{\beta_i}{\alpha} \right) \\ &\geq \frac{\ell(d-2t)}{d-2t-\mu} + 2t \frac{\ell}{d-2t-\mu} = \frac{\ell d}{d-2t-\mu}, \end{aligned}$$

and the bound on $\mathrm{CO}(A)$ follows by substracting ℓ to this inequality. □

4 A general construction based on linear rank-metric codes

In this section, given a nested coset coding scheme (Definition D.8) able to correct t_0 errors and ρ_0 erasures, for fixed positive integers t_0 and ρ_0, and given an arbitrary set $\mathcal{D} \subseteq [n-\rho_0, n]$ such that $n - \rho_0 \in \mathcal{D}$ (in particular for $\mathcal{D} = [n-\rho_0, n]$), we construct a coset coding scheme able to correct t_0 errors and any $n-d$ erasures with lower communication overheads than the original scheme, for all $d \in \mathcal{D}$. Moreover, both the original scheme and the modified one are universally secure under the same number of observations. The downside of the method is multiplying the packet length of the original coset coding scheme by a parameter α, depending on the involved codes, to achieve the desired subpacketization. The main result of the section is the following:

Theorem D.1. *Take $\mathbb{F}_{q^m}$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$, a positive integer ρ_0 such that $\rho_0 < d_R(\mathcal{C}_1, \mathcal{C}_2)$, and choose any subset $\mathcal{D} \subseteq [n - \rho_0, n]$ such that $n - \rho_0 \in \mathcal{D}$. Denote $\mathcal{D} = \{d_1, d_2, \ldots, d_h\}$, where $d_h = n - \rho_0 < d_{h-1} < \ldots < d_2 < d_1$, and assume that there exists a sequence of nested $\mathbb{F}_{q^m}$-linear codes*

$$\mathcal{C}_1 = \mathcal{C}^{(h)} \subsetneqq \mathcal{C}^{(h-1)} \subsetneqq \ldots \subsetneqq \mathcal{C}^{(2)} \subsetneqq \mathcal{C}^{(1)} \subseteq \mathbb{F}_{q^m}^n$$

such that

$$d_R\left(\mathcal{C}^{(j)}, \mathcal{C}_2\right) \geq n - d_j + 1,$$

for $j = 1, 2, \ldots, h$. Define then $k_1 = \dim(\mathcal{C}_1)$, $k_2 = \dim(\mathcal{C}_2)$, $\ell = k_1 - k_2$, $\alpha_j = k^{(j)} - k_2$ for $j = 1, 2, \ldots, h$, and

$$\alpha = \mathrm{LCM}(\alpha_1, \alpha_2, \ldots, \alpha_h).$$

There exists a coset coding scheme $F : \mathbb{F}_{q^m}^{\alpha \times \ell} \longrightarrow \mathbb{F}_{q^m}^{\alpha \times n}$ that is universally t-error and ρ-erasure-correcting if $2t + \rho < d_R(\mathcal{C}_1, \mathcal{C}_2)$, and is universally secure under μ observations if $\mu < d_R\left(\mathcal{C}_2^{\perp}, \mathcal{C}^{(1)\perp}\right)$.

In addition, for any $d \in \mathcal{D}$ and any full-rank matrix $A \in \mathbb{F}_q^{d \times n}$, there exist preprocessing functions $E_{A,i} : \mathbb{F}_q^{\alpha m} \longrightarrow \mathbb{F}_q^{\beta_i m}$, for $i = 1, 2, \ldots, d$, which are t-error-correcting with respect to F, whenever $2t < d_R\left(\mathcal{C}^{(j)}, \mathcal{C}_2\right) - n + d$, and such that

$$\mathrm{CO}(A) = \frac{\ell\left(d - k^{(j)} + k_2\right)}{k^{(j)} - k_2},$$

where $k^{(j)} = \dim\left(\mathcal{C}^{(j)}\right)$, for j such that $d = d_j$.

4.1 Description of the construction for Theorem D.1

Let the notation be as in Theorem D.1 and take a generator matrix $G_2 \in \mathbb{F}_{q^m}^{k_2 \times n}$ of $\mathcal{C}_2$ and a generator matrix $G_1 \in \mathbb{F}_{q^m}^{k_1 \times n}$ of $\mathcal{C}_1$ of the form

$$G_1 = \left(\begin{array}{c} G_2 \\ G_c \end{array} \right) \in \mathbb{F}_{q^m}^{k_1 \times n},$$

for some matrix $G_c \in \mathbb{F}_{q^m}^{\ell \times n}$. Decreasingly in $j = h-1, h-2, \ldots, 2, 1$, take a generator matrix $G^{(j)} \in \mathbb{F}_{q^m}^{k^{(j)} \times n}$ of $\mathcal{C}^{(j)}$ of the form

$$G^{(j)} = \left(\begin{array}{c} G^{(j+1)} \\ G_c^{(j+1)} \end{array} \right) \in \mathbb{F}_{q^m}^{k^{(j)} \times n},$$

for some matrix $G_c^{(j+1)} \in \mathbb{F}_{q^m}^{\left(k^{(j)}-k^{(j+1)}\right)\times n}$. Next define the following positive integers, which are analogous to the integers defined in [13, Eq. (11)]:

$$p_j = \begin{cases} \frac{\ell\alpha}{\alpha_1} & \text{if } j = 1, \\ \frac{\ell\alpha}{\alpha_j} - \frac{\ell\alpha}{\alpha_{j-1}} & \text{if } 1 < j \leq h. \end{cases}$$

Let $S \in \mathbb{F}_{q^m}^{\alpha\times\ell}$ be the secret message and generate uniformly at random a matrix $R \in \mathbb{F}_{q^m}^{\alpha\times k_2}$. Divide S and R as follows:

$$S = \begin{pmatrix} S_1 \\ S_2 \\ \vdots \\ S_h \end{pmatrix}, \quad R = \begin{pmatrix} R_1 \\ R_2 \\ \vdots \\ R_h \end{pmatrix},$$

where

$$S_j \in \mathbb{F}_{q^m}^{p_j\times\ell} \text{ and } R_j \in \mathbb{F}_{q^m}^{p_j\times k_2},$$

for $j = 1, 2, \ldots, h$. Next, we define the matrices

$$\begin{array}{rcccccccl} M_1 & = & (R_1 & S_1 & D_{1,1} & D_{1,2} & \ldots & D_{1,h-1}), \\ M_2 & = & (R_2 & S_2 & D_{2,1} & D_{2,2} & \ldots & 0), \\ M_3 & = & (R_3 & S_3 & D_{3,1} & D_{3,2} & \ldots & 0), \\ \vdots & & & \vdots & & & & \vdots \\ M_{h-1} & = & (R_{h-1} & S_{h-1} & D_{h-1,1} & 0 & \ldots & 0), \\ M_h & = & (R_h & S_h & 0 & 0 & \ldots & 0), \end{array}$$

where $M_u \in \mathbb{F}_{q^m}^{p_u\times k^{(1)}}$, and where the matrices $D_{u,v} \in \mathbb{F}_{q^m}^{p_u\times(\alpha_{h-v}-\alpha_{h-v+1})}$ are defined iteratively as follows: For $v = 1, 2, \ldots, h-1$, the components of the v-th column block

$$\begin{pmatrix} D_{1,v} \\ D_{2,v} \\ \vdots \\ D_{h-v,v} \end{pmatrix} \in \mathbb{F}_{q^m}^{\ell\alpha/\alpha_{h-v}\times(\alpha_{h-v}-\alpha_{h-v+1})},$$

are the components (after some fixed rearrangement) of

$$(S_{h-v+1}|D_{h-v+1,1}|D_{h-v+1,2}|\ldots|D_{h-v+1,v-1}),$$

whose size is $p_{h-v+1} \times \alpha_{h-v+1}$ (observe that $p_{j+1}\alpha_{j+1} = (\alpha_j - \alpha_{j+1})\ell\alpha/\alpha_j$). For convenience, we define the matrices

$$M_j' = \begin{pmatrix} M_1 \\ M_2 \\ \vdots \\ M_j \end{pmatrix} \in \mathbb{F}_{q^m}^{\ell\alpha/\alpha_j\times k^{(1)}}, \tag{D.8}$$

for $j = 1, 2, \ldots, h$.

Finally, we define the coset coding scheme $F : \mathbb{F}_{q^m}^{\alpha \times \ell} \longrightarrow \mathbb{F}_{q^m}^{\alpha \times n}$ by

$$C = F(S) = M'_h G^{(1)} \in \mathbb{F}_{q^m}^{\alpha \times n}. \tag{D.9}$$

To conclude, we define $E_{A,i} : \mathbb{F}_{q^m}^{\alpha} \longrightarrow \mathbb{F}_{q^m}^{\ell\alpha/\alpha_j}$ as follows. For $j = 1, 2, \ldots, h$, for $i = 1, 2, \ldots, d_j$, and for a full-rank matrix $A \in \mathbb{F}_q^{d_j \times n}$, we define $E_{A,i}(\mathbf{y}_i) \in \mathbb{F}_{q^m}^{\ell\alpha/\alpha_j}$ by restricting $\mathbf{y}_i \in \mathbb{F}_{q^m}^{\alpha}$ to its first $\ell\alpha/\alpha_j$ rows.

4.2 Proof of Theorem D.1

Let the notation be as in Theorem D.1 and as in the previous subsection. We prove each statement in Theorem D.1 separately:

1) The coset coding scheme is universally t-error and ρ-erasure-correcting if $2t + \rho < d_R(\mathcal{C}_1, \mathcal{C}_2)$*:* Take $A \in \mathbb{F}_q^{N \times n}$ of rank at least $n - \rho$ and an error matrix $E \in \mathbb{F}_{q^m}^{\alpha \times N}$ such that $\mathrm{Rk}_q(E) \leq t$. Divide E in the same way as S and R, that is,

$$E = \begin{pmatrix} E_1 \\ E_2 \\ \vdots \\ E_h \end{pmatrix} \in \mathbb{F}_{q^m}^{\alpha \times N},$$

where $E_j \in \mathbb{F}_{q^m}^{p_j \times N}$, and observe that $\mathrm{Rk}_q(E_j) \leq \mathrm{Rk}_q(E) \leq t$, for $j = 1, 2, \ldots, h$. From

$$(S_h | R_h | 0) G^{(1)} A^T + E_h = (S_h | R_h) G_1 A^T + E_h$$

we obtain S_h by Lemma D.10, since $\mathrm{Rk}_q(E_h) \leq t$ and $2t + \rho < d_R(\mathcal{C}_1, \mathcal{C}_2)$. By definition, we have obtained $D_{u,1}$, for $u = 1, 2, \ldots h - 1$. Hence substracting $D_{h-1,1} G_c^{(h)} A^T$ from $(S_{h-1} | R_{h-1} | D_{h-1,1} |\, 0) G^{(1)} A^T + E_{h-1}$, we may obtain $(S_{h-1} | R_{h-1}) G_1 A^T + E_{h-1}$, and thus we obtain S_{h-1} again by Lemma D.10. Now, we have also obtained $D_{u,2}$, for $u = 1, 2, \ldots, h-2$. Proceeding iteratively in the same way, we see that we may obtain all the matrices S_j, for $j = 1, 2, \ldots, h$, and thus we obtain the whole message S.

2) The coset coding scheme is universally secure under any $\mu < d_R\left(\mathcal{C}_2^{\perp}, \mathcal{C}_1^{\perp}\right)$ *observations:* We first need the following preliminary lemma, which follows from [18, Th. 3]:

Lemma D.15. *Let* $B \in \mathbb{F}_q^{\mu \times n}$ *and let* $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$ *be* $\mathbb{F}_{q^m}$*-linear codes. If* $\mathrm{Rk}(B) < d_R\left(\mathcal{C}_2^{\perp}, \mathcal{C}_1^{\perp}\right)$*, then*

$$\mathcal{C}_2 B^T = \mathcal{C}_1 B^T,$$

where $\mathcal{C} B^T = \left\{ \mathbf{c} B^T \mid \mathbf{c} \in \mathcal{C} \right\} \subseteq \mathbb{F}_{q^m}^{\mu}$*, for a code* $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$*.*

Proof. See Appendix A. □

Take $B \in \mathbb{F}_q^{\mu \times n}$, and assume that the eavesdropper obtains

$$W = CB^T = M_h' G^{(1)} B^T \in \mathbb{F}_{q^m}^{\alpha \times \mu}.$$

The random variable W has support inside the $\mathbb{F}_{q^m}$-linear vector space

$$\mathcal{C}_{B,\alpha}^{(1)} = \left\{ MG^{(1)} B^T \mid M \in \mathbb{F}_{q^m}^{\alpha \times k^{(1)}} \right\} \subseteq \mathbb{F}_{q^m}^{\alpha \times \mu}.$$

Recall from [3, Th. 2.6.4] that, if a random variable X has support in the set $\mathcal{X}$, then $H(X) \leq \log_q(\#\mathcal{X})$. Hence

$$H(W) \leq \log_q \left(\#\mathcal{C}_{B,\alpha}^{(1)} \right) = m \dim \left(\mathcal{C}_{B,\alpha}^{(1)} \right) = \alpha m \dim \left(\mathcal{C}^{(1)} B^T \right),$$

where dimensions are taken over $\mathbb{F}_{q^m}$. On the other hand, using the analogous notation $\mathcal{C}_{2B,\alpha}$ for $\mathcal{C}_2$ instead of $\mathcal{C}^{(1)}$, it holds that

$$H(W \mid S) = \log_q \left(\#\mathcal{C}_{2B,\alpha} \right) = m \dim \left(\mathcal{C}_{2B,\alpha} \right) = \alpha m \dim \left(\mathcal{C}_2 B^T \right),$$

since, given a value of S, the variable W is a uniform random variable over an $\mathbb{F}_{q^m}$-linear affine space obtained by translating the vector space $\mathcal{C}_{2B,\alpha}$. Hence we obtain that

$$\begin{aligned} 0 \leq I(S;W) &= H(W) - H(W \mid S) \\ &\leq \alpha m \left(\dim \left(\mathcal{C}^{(1)} B^T \right) - \dim \left(\mathcal{C}_2 B^T \right) \right) = 0, \end{aligned}$$

where the last equality follows from Lemma D.15. Thus $I(S;W) = 0$ and we are done.

3) The preprocessing functions are t-error-correcting for any $2t < d_R \left(\mathcal{C}^{(j)}, \mathcal{C}_2 \right) - n + d$, *where* $d = d_j$*:* Fix $d \in \mathcal{D}$ and a full-rank matrix $A \in \mathbb{F}_q^{d \times n}$, and let $E_{A,i} : \mathbb{F}_{q^m}^{\alpha} \longrightarrow \mathbb{F}_{q^m}^{\ell \alpha / \alpha_j}$ be preprocessing functions as in the previous subsection, for $i = 1, 2, \ldots, d$, and where j is such that $d = d_j$.

Let $E \in \mathbb{F}_{q^m}^{\alpha \times d}$ be an error matrix such that $\mathrm{Rk}_q(E) \leq t$, and let $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_d \in \mathbb{F}_{q^m}^{\alpha}$ be its columns. By definition, $E_{A,i} \left(C\mathbf{a}_i^T + \mathbf{e}_i \right)$ is the i-th column of

$$M_j' G^{(1)} A^T + E_j' \in \mathbb{F}_{q^m}^{\ell \alpha / \alpha_j \times d},$$

for $i = 1, 2, \ldots, d$, and a submatrix $E_j' \in \mathbb{F}_{q^m}^{\ell \alpha / \alpha_j \times d}$ of E, which thus satisfies that $\mathrm{Rk}_q(E_j') \leq \mathrm{Rk}_q(E) \leq t$. Therefore, we may obtain the matrix M_j' as in item 1, since $2t + n - d < d_R(\mathcal{C}^{(j)}, \mathcal{C}_2)$. By definition, the matrices $S_1, S_2, \ldots, S_j$ are contained in M_j'. Moreover, the matrices $D_{1,h-j}, D_{2,h-j}, \ldots, D_{j,h-j}$ are also contained in M'_j, and from them we obtain by definition S_{j+1} and $D_{j+1,1}$, $D_{j+1,2}, \ldots, D_{j+1,h-j-1}$. Now, the matrices $D_{1,h-j-1}, D_{2,h-j-1}, \ldots, D_{j,h-j-1}$ are contained in M'_j and we also have $D_{j+1,h-j-1}$, hence we may obtain by definition S_{j+2} and $D_{j+2,1}, D_{j+2,2}, \ldots, D_{j+2,h-j-2}$. Continuing iteratively in this way, we may obtain all $S_1, S_2, \ldots, S_h$ and hence the message S.

Finally, we have that

$$\mathrm{CO}(A) = \sum_{i=1}^{d} \frac{\beta_i}{\alpha} - \ell = \sum_{i=1}^{d} \frac{\ell\alpha}{\alpha_j \alpha} - \ell$$

$$= \frac{\ell d}{\alpha_j} - \ell = \frac{\ell(d-\alpha_j)}{\alpha_j} = \frac{\ell\left(d - k^{(j)} + k_2\right)}{k^{(j)} - k_2}.$$

5 MRD codes and coset coding schemes with optimal communication overheads

In this section, we apply Theorem D.1 to pairs of Gabidulin codes [8, 21] and their cartesian products [7]. The first family yields optimal coset coding schemes when $n \leq m$ in the sense of (D.4) and (D.5), and the second family constitutes a family of maximum rank distance (MRD) codes when $n > m$ [7, Cor. 1].

We recall the definition of MRD codes for convenience of the reader. The Singleton bound for an arbitrary (linear or not) code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ was first given in [4, Th. 6.3]:

$$\#\mathcal{C} \leq q^{\max\{m,n\}(\min\{m,n\} - d_R(\mathcal{C}) + 1)}. \tag{D.10}$$

We then say that $\mathcal{C}$ is MRD if equality holds in (D.10). In another direction, a Singleton bound on the relative minimum rank distance of a pair of $\mathbb{F}_{q^m}$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$ was first given in [16, Prop. 3]:

$$d_R(\mathcal{C}_1, \mathcal{C}_2) \leq \min\left\{ n - \dim(\mathcal{C}_1), \frac{m(n - \dim(\mathcal{C}_1))}{n - \dim(\mathcal{C}_2)} \right\} + 1. \tag{D.11}$$

Thus if $\mathcal{C}_1$ is MRD and $n \leq m$, then equality is satisfied in (D.11).

5.1 Coset coding schemes based on Gabidulin codes

In this subsection we will make use of Gabidulin codes, which were introduced independently in [8, Sec. 4] and [21, Sec. III]. Throughout this subsection, we will assume that $n \leq m$.

Definition D.16 ([8, 21]). Fix a basis $\gamma_1, \gamma_2, \ldots, \gamma_m$ of $\mathbb{F}_{q^m}$ as a vector space over $\mathbb{F}_q$, and let $0 \leq k \leq n$. The Gabidulin code of dimension k and length n

over $\mathbb{F}_{q^m}$, constructed from the previous basis, is the $\mathbb{F}_{q^m}$-linear code $\mathcal{G}_k \subseteq \mathbb{F}_{q^m}^n$ with parity-check matrix given by

$$\begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \cdots & \gamma_n \\ \gamma_1^q & \gamma_2^q & \gamma_3^q & \cdots & \gamma_n^q \\ \gamma_1^{q^2} & \gamma_2^{q^2} & \gamma_3^{q^2} & \cdots & \gamma_n^{q^2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \gamma_1^{q^{n-k-1}} & \gamma_2^{q^{n-k-1}} & \gamma_3^{q^{n-k-1}} & \cdots & \gamma_n^{q^{n-k-1}} \end{pmatrix} \in \mathbb{F}_{q^m}^{(n-k)\times n}.$$

It was proven in [8, Th. 6] and [21, Th. 2] that the code $\mathcal{G}_k \subseteq \mathbb{F}_{q^m}^n$ satisfies

$$\dim(\mathcal{G}_k) = k, \quad \text{and} \quad d_R(\mathcal{G}_k) = n - k + 1, \tag{D.12}$$

constituting thus a family of MRD codes covering all parameters when $n \leq m$. Moreover it is clear from the definition that, for a fixed basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, they form a nested sequence of codes:

$$\{\mathbf{0}\} = \mathcal{G}_0 \subsetneqq \mathcal{G}_1 \subsetneqq \mathcal{G}_2 \subsetneqq \ldots \subsetneqq \mathcal{G}_{n-1} \subsetneqq \mathcal{G}_n = \mathbb{F}_{q^m}^n. \tag{D.13}$$

Thus the next theorem follows directly from Theorem D.1:

Theorem D.2. *Choose integers k_2, k_1, t_0 and ρ_0 such that $0 \leq k_2 < k_1 \leq n$ and $2t_0 + \rho_0 = n - k_1$, and choose any subset $\mathcal{D} \subseteq [n - \rho_0, n]$ such that $n - \rho_0 \in \mathcal{D}$.*

Now, fix a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, let $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$ be $\mathbb{F}_{q^m}$-linear Gabidulin codes of dimensions k_2 and k_1 (that is, $\mathcal{G}_{k_2}$ and $\mathcal{G}_{k_1}$), respectively, and denote the elements in $\mathcal{D}$ by $d_h = n - \rho_0 < d_{h-1} < \ldots < d_2 < d_1$.

The coset coding scheme $F : \mathbb{F}_{q^m}^{\alpha \times \ell} \longrightarrow \mathbb{F}_{q^m}^{\alpha \times n}$ in Theorem D.1 based on this pair of codes and the subsequence of (D.13) given by the Gabidulin codes $\mathcal{C}^{(j)} = \mathcal{G}_{d_j - 2t_0}$, that is, $k^{(j)} = d_j - 2t_0$, for $j = 1, 2, \ldots, h$, satisfies $\ell = k_1 - k_2$, is universally t-error and ρ-erasure-correcting if $2t + \rho \leq n - k_1$, and is universally secure under μ observations if $\mu \leq k_2$. In particular, the scheme is optimal in the sense of (D.4). Moreover, it holds that

$$\alpha = \text{LCM}\left(d_1 - 2t_0 - k_2, d_2 - 2t_0 - k_2, \ldots, d_h - 2t_0 - k_2\right).$$

In addition, for any $d \in \mathcal{D}$ and any full-rank matrix $A \in \mathbb{F}_q^{d \times n}$, there exist preprocessing functions $E_{A,i} : \mathbb{F}_q^{\alpha m} \longrightarrow \mathbb{F}_q^{\ell \alpha m/(d - 2t_0 - k_2)}$, for $i = 1, 2, \ldots, d$, which are t_0-error-correcting and satisfying equality in (D.5), hence having optimal communication overheads for all $d \in \mathcal{D}$.

Observe that the packet length m of the original Gabidulin codes is multiplied by α, which depends only on the maximum number of observations, the number of correctable errors and the set of possible erasures $\mathcal{D}$.

However, there are instances as Example D.1 where, due to a particular subpacketization, we need not expand the packet length, hence we obtain a strict improvement on the communication overheads at no cost on the rest of the parameters.

We now give the details of Example D.1 and Example D.2, which share the same construction: With the given parameters, the construction in [22, Th. 11] gives $\ell = 16$ by choosing $k_1 = 24$ and $k_2 = 8$. However, decomposing the packet length as $\alpha m = 2048$, with $m = 64$ and $\alpha = 32$, we may choose $\mathcal{D} = \{24, 40\}$, $k^{(1)} = 40$, $k_1 = 24$ and $k_2 = 8$, thus $\alpha_1 = 32$, $\alpha_2 = 16$, and $\alpha = 32$, and the example follows.

5.2 Coset coding schemes based on MRD cartesian products

In this subsection, we will make use of cartesian products of Gabidulin codes, which yield again MRD codes, but in the case $n > m$, in contrast with plain Gabidulin codes as in the previous subsection. To the best of our knowledge, this is the only known family of MRD $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$ when $n > m$.

Throughout this subsection, we will assume that $n = lm$, for some positive integer l. Take another integer $1 \leq k \leq m$, and consider the cartesian product

$$\mathcal{C} = \mathcal{G}_k^l \subseteq \mathbb{F}_{q^m}^n,$$

where $\mathcal{G}_k \subseteq \mathbb{F}_{q^m}^m$ is a Gabidulin code as in Definition D.16. It is proven in [7, Cor. 1] that

$$\dim(\mathcal{C}) = lk, \quad \text{and} \quad d_R(\mathcal{C}) = m - k + 1, \tag{D.14}$$

and therefore $\mathcal{C}$ is MRD. Since the codes $\mathcal{G}_k$ can be taken in a nested sequence for a fixed basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, as in Equation (D.13), the next result also follows directly from Theorem D.1:

Theorem D.3. *Choose integers k_1, k_2, t_0 and ρ_0 such that $0 \leq k_2 < k_1 \leq m$ and $2t_0 + \rho_0 = m - k_1$, and choose any subset $\mathcal{D} \subseteq [n - \rho_0, n]$ with elements $d_h = n - \rho_0 < d_{h-1} < \ldots < d_2 < d_1$.*

Define $k^{(j)} = d_j - (l-1)m - 2t_0$ and the $\mathbb{F}_{q^m}$-linear codes

$$\mathcal{C}_2 = \mathcal{G}_{k_2}^l \subsetneqq \mathcal{C}^{(j)} = \mathcal{G}_{k^{(j)}}^l \subseteq \mathbb{F}_{q^m}^n,$$

for $j = 1, 2, \ldots, h$, and observe that $k^{(h)} = k_1$, hence $\mathcal{C}^{(h)} = \mathcal{C}_1 = \mathcal{G}_{k_1}^l$.

The coset coding scheme $F : \mathbb{F}_{q^m}^{\alpha \times \ell} \longrightarrow \mathbb{F}_{q^m}^{\alpha \times n}$ in Theorem D.1 based on these codes satisfies $\ell = l(k_1 - k_2)$, is universally t-error and ρ-erasure-correcting if $2t + \rho \leq m - k_1$, and is universally secure under μ observations if $\mu \leq k_2$. Moreover, it holds that

$$\alpha = \mathrm{LCM}\left\{ l(d_j - 2t_0 - k_2) - (l-1)n \mid j = 1, 2, \ldots, h \right\}.$$

In addition, for any $d \in \mathcal{D}$ and any full-rank matrix $A \in \mathbb{F}_q^{d \times n}$, there exist preprocessing functions $E_{A,i} : \mathbb{F}_q^{\alpha m} \longrightarrow \mathbb{F}_q^{\ell \alpha m / (l(d-2t_0-k_2)-(l-1)n)}$, for $i = 1, 2, \ldots, d$, which are t_0-error-correcting and such that

$$\mathrm{CO}(A) = \frac{\ell \left(l(2t_0 + k_2) + (l-1)(n-d) \right)}{l(d - 2t_0 - k_2) - (l-1)n}.$$

Observe that the particular case $l = 1$ corresponds to the particular case $n = m$ in Theorem D.2.

6 Applications

6.1 Universal secure linear network coding

Consider a network with n outgoing links from a source and N ingoing links to a sink, and where the source wants to transmit ℓ packets, encoded into n packets (all of the same length), to the sink. Linear network coding, introduced in [1, 15, 17], consists in sending linear combinations over $\mathbb{F}_q$ of the received packets at each node of the network, which increases throughput with respect to storing and forwarding.

In this scenario, link errors and erasures expand through the network and an eavesdropper may obtain linear combinations of the sent packets. Thus if the coefficients of the final linear combinations are known to the receiver, then a linearly coded network, with link errors, erasures and observations, can be modelled as a coherent linearized noisy wire-tap channel [22], as in Definition D.3.

Assume that the packet length is at least n, and fix positive integers t, ρ and μ with $2t + \rho + \mu < n$ and $\rho \leq N$. In [22, Th. 11] a construction (pairs of Gabidulin codes) is given such that $\ell = n - 2t - \rho - \mu$, which is optimal due to (D.4).

However, assuming that q is big enough and the erasure matrix $A \in \mathbb{F}_q^{N \times n}$ (see Definition D.3) is taken at random as in [11], then it will be full-rank with high probability and ρ can be thought of as a number of erased ingoing links to the sink, due to noise, link failure or the action of the adversary.

Theorem D.2 gives an alternative construction to [22, Th. 11] with optimal $\ell = n - 2t - \rho - \mu$, where if more than $n - \rho$ ingoing links to the sink are available, the sink can contact the corresponding nodes after exchanging feedback on the number of available nodes, and reduce the communication overhead (hence the amount of packets received by the sink) to its optimal value in view of (D.5).

6.2 Secure distributed storage with crisscross errors and erasures

Errors and erasures occurring along several rows and/or columns of a matrix over $\mathbb{F}_q$ are called *crisscross errors and erasures* in the literature, and can happen in memory chips and magnetic tapes, for instance (see [21]). Recently, crisscross error and erasure-correction has gained attention in the context of distributed storage where data is stored in several data centers (columns), which in turn store several blocks of data (rows), where mixed and/or correlated failures may occur (see [14]).

In this work, we consider a storage system where data is stored as an $\alpha m \times n$ matrix over $\mathbb{F}_q$, where columns are thought of as data centers that are contacted to obtain information from, and rows are blocks of data expanding across the different data centers and sharing correlated errors. More formally, we consider column erasures (equivalently, data centers being available and contacted) together with crisscross errors and where an eavesdropper may listen to a number of columns (data centers).

We formalize crisscross error-correction in the following definitions, which we take from [21, Sec. I]:

Definition D.17 (Crisscross weights [21]). A cover of a matrix $E \in \mathbb{F}_q^{\alpha m \times n}$ is a pair of sets $X \subseteq [\alpha m]$ and $Y \subseteq [n]$ such that if $e_{i,j} \neq 0$, then $i \in X$ or $j \in Y$. We then define the crisscross weight of E as

$$\mathrm{wt}_c(E) = \min \{\#X + \#Y \mid (X, Y) \subseteq [\alpha m] \times [n] \text{ is a cover of } E\}. \qquad \text{(D.15)}$$

We may then formalize crisscross error and erasure-correction, together with security, as follows:

Definition D.18. For a subset $I \subseteq [n]$, define the matrix $P_I \in \mathbb{F}_q^{\#I \times n}$ as that constituted by the rows of the $n \times n$ identity matrix indexed by I. We say that the coset coding scheme $F : \mathbb{F}_q^{\alpha m \times \ell} \longrightarrow \mathbb{F}_q^{\alpha m \times n}$ is:

1. Crisscross t-error and ρ-erasure-correcting if, for every $I \subseteq [n]$ with $\#I = n - \rho$, there exist a decoding function $D_I : \mathbb{F}_q^{\alpha m \times (n-\rho)} \longrightarrow \mathbb{F}_q^{\alpha m \times \ell}$ such that
$$D_I \left(C P_I^T + E \right) = S,$$
for all $C \in \mathcal{C}_S$, all $E \in \mathbb{F}_q^{\alpha m \times (n-\rho)}$ with $\mathrm{wt}_c(E) \leq t$, and all $S \in \mathbb{F}_q^{\alpha m \times \ell}$.

2. Secure under μ column-observations if
$$H(W \mid S) = H(S),$$
for any matrix $W \in \mathbb{F}_q^{\alpha m \times \mu}$ constituted by μ columns of $C = F(S)$, for all $S \in \mathbb{F}_q^{\alpha m \times \ell}$.

In this scenario, pieces of data correspond to columns, instead of linear combinations of columns, hence we will consider preprocessing functions $E_{I,i} : \mathbb{F}_q^{\alpha m} \longrightarrow \mathbb{F}_q^{\beta_i m}$ depending on a subset of columns $I \subseteq [n]$, where $i \in I$. Hence we may formalize the crisscross error-correction capability of preprocessing functions as follows:

Definition D.19. For a subset $I \subseteq [n]$ with $d = \#I$, the preprocessing functions $E_{I,i} : \mathbb{F}_q^{\alpha m} \longrightarrow \mathbb{F}_q^{\beta_i m}$, for $i = 1, 2, \ldots, d$, are t-crisscross error-correcting with respect to F if there exists a decoding function $D_I : \prod_{i=1}^{d} \mathbb{F}_q^{\beta_i m} \longrightarrow \mathbb{F}_q^{\alpha m \times \ell}$ such that

$$D_I \left(\left(E_{I,i} \left(\mathbf{c}_i + \mathbf{e}_i \right) \right)_{i=1}^{d} \right) = S, \tag{D.16}$$

where $C \in \mathcal{C}_S$ and $\mathbf{c}_i$ denotes the i-th column of C, for $i = 1, 2, \ldots, d$, for all $S \in \mathbb{F}_q^{\alpha m \times \ell}$ and all error matrices $E \in \mathbb{F}_q^{\alpha m \times d}$ of crisscross weight at most t with columns $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_d \in \mathbb{F}_q^{\alpha m}$.

The decoding bandwidth and communication overhead of such functions are defined as in Definition D.12.

We now see that the bounds (D.4) and (D.5) also hold in this context:

Proposition D.20. *If the coset coding scheme $F : \mathbb{F}_q^{\alpha m \times \ell} \longrightarrow \mathbb{F}_q^{\alpha m \times n}$ is crisscross t-error and ρ-erasure-correcting, and secure under μ column-observations, then*

$$\ell \leq n - 2t - \rho - \mu. \tag{D.17}$$

Moreover, for a subset $I \subseteq [n]$ with $d = \#I$ and preprocessing functions $E_{I,i} : \mathbb{F}_q^{\alpha m} \longrightarrow \mathbb{F}_q^{\beta_i m}$, for $i = 1, 2, \ldots, d$, that are t-crisscross error-correcting with respect to F, it holds that:

$$\mathrm{CO}(I) \geq \frac{\ell(2t + \mu)}{d - 2t - \mu}, \tag{D.18}$$

Proof. Define $\rho' = \rho + 2t$. We will prove that F is ρ'-crisscross erasure-correcting. If it is not, then there exists a subset $I \subseteq [n]$ with $\#I = n - \rho'$, and there exist $C_1 \in \mathcal{C}_{S_1}$ and $C_2 \in \mathcal{C}_{S_2}$, where $S_1 \neq S_2$, such that

$$C_1 P_I^T = C_2 P_I^T.$$

Next take a set of the form $I_1 = I \cup J_1 \cup J_2$, where $\#I_1 = n - \rho$ and $t = \#J_1 = \#J_2$ (recall that $n - \rho = n - \rho' + 2t$). There exist matrices $E_1, E_2 \in \mathbb{F}_q^{\alpha m \times (n - \rho)}$ of crisscross weight at most t such that

$$C_1 P_{I_1}^T + E_1 = C_2 P_{I_1}^T + E_2.$$

Hence F cannot be crisscross t-error and ρ-erasure-correcting, and we reach a contradiction. Now, this implies that F is a classical secret sharing scheme with alphabet $\mathbb{F}_q^{\alpha m}$, reconstruction ρ' and privacy μ. Thus it follows directly from [13, Th. 1] that

$$\ell \leq n - \rho' - \mu = n - \rho - 2t - \mu,$$

and we are done.

Finally, the bound (D.18) can be proven in the same way as the bound (D.5). □

To conclude, we observe that a coset coding scheme, together with preprocessing functions, which are universally (rank) error and erasure-correcting and universally secure in the sense of Definitions D.5 and D.11 are also crisscross erasure and error-correcting and secure under a given number of column observations in the sense of Definitions D.18 and D.19, with exactly the same parameters. Thus all constructions in this paper can be directly translated into the context of this subsection.

For illustration purposes, we show how to translate Theorem D.2 to this context, thus obtaining coset coding schemes which are optimal in the sense of (D.17) and (D.18) for all parameters, whenever $n \leq m$.

Corollary D.21. *Assume $n \leq m$, choose integers k_2, k_1, t_0 and ρ_0 such that $0 \leq k_2 < k_1 \leq n$ and $2t_0 + \rho_0 = n - k_1$, and choose any subset $\mathcal{D} \subseteq [n - \rho_0, n]$ with elements $d_h = n - \rho_0 < d_{h-1} < \ldots < d_2 < d_1$.*

The coset coding scheme $F : \mathbb{F}_{q^m}^{\alpha \times \ell} \longrightarrow \mathbb{F}_{q^m}^{\alpha \times n}$ in Theorem D.2 with these parameters satisfies $\ell = k_1 - k_2$, is crisscross t-error and ρ-erasure-correcting if $2t + \rho \leq n - k_1$, and is secure under μ column-observations if $\mu \leq k_2$. In particular, the scheme is optimal in the sense of (D.17). Moreover, it holds that

$$\alpha = \mathrm{LCM}\left(d_1 - 2t_0 - k_2, d_2 - 2t_0 - k_2, \ldots, d_h - 2t_0 - k_2\right).$$

In addition, for any $d \in \mathcal{D}$ and any subset $I \subseteq [n]$ with $d = \#I$, there exist preprocessing functions $E_{I,i} : \mathbb{F}_q^{\alpha m} \longrightarrow \mathbb{F}_q^{\ell \alpha m/(d - 2t_0 - k_2)}$, for $i = 1, 2, \ldots, d$, which are t_0-crisscross error-correcting and satisfying equality in (D.18), hence having optimal communication overheads for all $d \in \mathcal{D}$.

Observe that optimal crisscross error and erasure-correcting coding schemes can also be obtained by using maximum distance separable (MDS) codes in $\mathbb{F}_q^{\alpha m \times n}$, by identifying this vector space with $\mathbb{F}_q^{\alpha m n}$, as noticed in [21]. However, such constructions may require extremely large finite fields, for instance $q > \alpha m n$ for Reed-Solomon codes, whereas rank-metric codes allow to obtain optimal coding schemes with the only constraint $n \leq m$, being q unrestricted, allowing in particular using binary fields ($q = 2$).

7 Conclusion and open problems

In this paper, we have studied the problem of reducing the communication overhead on a noisy wire-tap channel or storage system where data is encoded as a matrix. The method developed in Section 4 allows to reduce the communication overhead, when more columns are available, at the cost of expanding the packet length (number of rows). However, in the optimal case of pairs of Gabidulin codes (Section 5), strict improvements on the communication overheads are possible at no cost on the rest of the parameters, as shown in Example D.1 for practical instances in the applications. We leave as open problem to study when the packet length need not be expanded. Another interesting open problem is to extend our method to codes that are linear over the base field $\mathbb{F}_q$, instead of the extension field $\mathbb{F}_{q^m}$. This would allow to use all possible MRD codes [4].

A Proof of Lemma D.15

Fix $\mathbb{F}_{q^m}$-linear codes $\mathcal{C}_2 \subsetneqq \mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$ and a matrix $B \in \mathbb{F}_q^{\mu \times n}$ in the rest of the appendix.

We start with an auxiliary result, which is a particular case of [18, Th. 3]:

Lemma D.22 ([18]). *It holds that*

$$d_R(\mathcal{C}_1, \mathcal{C}_2) = \min\{\mathrm{Rk}(A) \mid A \in \mathbb{F}_q^{\nu \times n}, \nu \in \mathbb{N}, \textit{ and } \\ \dim\left(\mathcal{C}_1 \cap \mathrm{Row}(A) / \mathcal{C}_2 \cap \mathrm{Row}(A)\right) \geq 1\},$$

where $\mathrm{Row}(A) \subseteq \mathbb{F}_{q^m}^n$ *denotes the* $\mathbb{F}_{q^m}$*-linear vector space generated by the rows of the matrix* $A \in \mathbb{F}_q^{\nu \times n}$.

Given an $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, consider the map $\mathcal{C} \longrightarrow \mathcal{C}B^T$ defined by $\mathbf{c} \mapsto \mathbf{c}B^T$, for $\mathbf{c} \in \mathcal{C}$. It is surjective and its kernel is $\mathcal{C} \cap \left(\mathcal{V}^\perp\right)$, where $\mathcal{V} = \mathrm{Row}(B)$. Therefore

$$\dim(\mathcal{C}) = \dim\left(\mathcal{C}B^T\right) + \dim\left(\mathcal{C} \cap \left(\mathcal{V}^\perp\right)\right).$$

Using this equation and computing dimensions, it follows that

$$\dim\left(\mathcal{C}_1 B^T / \mathcal{C}_2 B^T\right) = \dim\left(\mathcal{C}_2^\perp \cap \mathcal{V} / \mathcal{C}_1^\perp \cap \mathcal{V}\right). \tag{D.19}$$

Now, using that $\mathrm{Rk}(B) < d_R\left(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp\right)$ and the previous lemma, it holds that $\mathcal{C}_2^\perp \cap \mathcal{V} = \mathcal{C}_1^\perp \cap \mathcal{V}$. Hence the result follows by (D.19).

Acknowledgement

The author gratefully acknowledges the support from The Danish Council for Independent Research (Grant No. DFF-4002-00367 and Grant No. DFF-5137-00076B "EliteForsk-Rejsestipendium"), and is thankful for the guidance of his advisors Olav Geil and Diego Ruano. This manuscript was written in part when the author was visiting the University of Toronto. He greatly appreciates the support and hospitality of Frank R. Kschischang, and is thankful for valuable discussions on this work.

References

[1] R. Ahlswede, N. Cai, S. Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inform. Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.

[2] R. Bitar and S. E. Rouayheb, "Staircase codes for secret sharing with optimal communication and read overheads," in *Proc. 2016 IEEE International Symposium on Information Theory (ISIT)*, 2016, pp. 1396–1400.

[3] T. M. Cover and J. A. Thomas, *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing), 2nd Edition*. Wiley-Interscience, 2006.

[4] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *Journal of Combinatorial Theory, Series A*, vol. 25, no. 3, pp. 226–241, 1978.

[5] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," *IEEE Trans. Inform. Theory*, vol. 56, no. 9, pp. 4539–4551, 2010.

[6] A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "A survey on network codes for distributed storage," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 476–489, 2011.

[7] E. M. Gabidulin, A. V. Ourivski, B. Honary, and B. Ammar, "Reducible rank codes and their applications to cryptography," *IEEE Trans. Inform. Theory*, vol. 49, no. 12, pp. 3289–3293, 2003.

[8] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Probl. Inf. Transm.*, vol. 21, no. 1, pp. 1–12, 1985.

[9] P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin, "On the locality of codeword symbols," *IEEE Trans. Inform. Theory*, vol. 58, no. 11, pp. 6925–6934, 2012.

[10] V. Guruswami and M. Wootters, "Repairing Reed-Solomon codes," in *Proc. 48th Annual ACM Symposium on Theory of Computing*. ACM, 2016, pp. 216–226.

[11] T. Ho, M. Medard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inform. Theory*, vol. 52, no. 10, pp. 4413–4430, 2006.

[12] C. Huang, M. Chen, and J. Li, "Pyramid codes: Flexible schemes to trade space for access efficiency in reliable data storage systems," in *Sixth IEEE International Symposium on Network Computing and Applications (NCA 2007)*, 2007, pp. 79–86.

[13] W. Huang, M. Langberg, J. Kliewer, and J. Bruck, "Communication efficient secret sharing," *IEEE Trans. Inform. Theory*, vol. 62, no. 12, pp. 7195–7206, 2016.

[14] S. Kadhe, S. E. Rouayheb, I. Duursma, and A. Sprintson, "Rank-metric codes with local recoverability," in *Proc. 54th Annual Allerton Conference on Communication, Control, and Computing*, 2016.

[15] R. Kötter and M. Medard, "An algebraic approach to network coding," *IEEE/ACM Trans. Networking*, vol. 11, no. 5, pp. 782–795, Oct 2003.

[16] J. Kurihara, R. Matsumoto, and T. Uyematsu, "Relative generalized rank weight of linear codes and its applications to network coding," *IEEE Trans. Inform. Theory*, vol. 61, no. 7, pp. 3912–3936, 2015.

[17] S. Y. Li, R. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inform. Theory*, vol. 49, no. 2, pp. 371–381, 2003.

[18] U. Martínez-Peñas, "On the similarities between generalized rank and Hamming weights and their applications to network coding," *IEEE Trans. Inform. Theory*, vol. 62, no. 7, pp. 4081–4095, 2016.

[19] ——, "Universal secure rank-metric coding schemes with optimal communication overheads," in *Proc. 2017 IEEE International Symposium on Information Theory (ISIT)*, Jun 2017.

[20] K. V. Rashmi, N. B. Shah, and P. V. Kumar, "Optimal exact-regenerating codes for distributed storage at the msr and mbr points via a product-matrix construction," *IEEE Trans. Inform. Theory*, vol. 57, no. 8, pp. 5227–5239, 2011.

[21] R. M. Roth, "Maximum-rank array codes and their application to criss-cross error correction," *IEEE Trans. Inform. Theory*, vol. 37, no. 2, pp. 328–336, 1991.

[22] D. Silva and F. R. Kschischang, “Universal secure network coding via rank-metric codes,” *IEEE Trans. Inform. Theory*, vol. 57, no. 2, pp. 1124–1135, 2011.

[23] I. Tamo and A. Barg, “A family of optimal locally recoverable codes,” *IEEE Trans. Inform. Theory*, vol. 60, no. 8, pp. 4661–4676, 2014.

[24] H. Wang and D. S. Wong, “On secret reconstruction in secret sharing schemes,” *IEEE Trans. Inform. Theory*, vol. 54, no. 1, pp. 473–480, 2008.

Paper E

On the roots and minimum rank distance of skew cyclic codes

Umberto Martínez-Peñas[1]

The paper has been published in
Designs, Codes and Cryptography Vol. 83, No. 3, pp. 639–660, 2017.

[1] Department of Mathematical Sciences, Aalborg University, Aalborg 9220, Denmark

Abstract

Skew cyclic codes play the same role as cyclic codes in the theory of error-correcting codes for the rank metric. In this paper, we give descriptions of these codes by root spaces, cyclotomic spaces and idempotent generators. We prove that the lattice of skew cyclic codes is anti-isomorphic to the lattice of root spaces, study these two lattices and extend the rank-BCH bound on their minimum rank distance to rank-metric versions of the van Lint-Wilson's shift and Hartmann-Tzeng bounds. Finally, we study skew cyclic codes which are linear over the base field, proving that these codes include all Hamming-metric cyclic codes, giving then a new relation between these codes and rank-metric skew cyclic codes.

Keywords: Cyclic codes, finite rings, Hamming distance, linearized polynomial rings, rank distance, skew cyclic codes.

MSC: 15A03, 15B33, 94B15.

1 Introduction

Cyclic codes play a very important role in the theory of error-correcting codes in the Hamming metric. On the other hand, error-correcting codes in the rank metric [7] have been proven to be crucial in applications to network coding (see [18]). Only a few families of rank-metric codes are known (for instance [7, 12]) and only for a restricted choice of parameters. Therefore it is of interest to study new and different families of codes with good rank-metric parameters, simple algebraic descriptions and fast encoding and decoding algorithms.

Usual cyclic codes have been considered for the rank metric in [5, 19] and a new construction, the so-called rank q-cyclic codes, was introduced in [7] for square matrices and has been generalized in [8] for other lengths. Independently, this notion has been generalized to skew or q^r-cyclic codes in the work by Ulmer et al. in [1–3], where r may be different from 1.

Some Gabidulin codes consisting of square matrices are q-cyclic (see [7, 8]), which implies that the family of q-cyclic codes includes some maximum rank distance (MRD) codes. In [7], in [8] and in [1–3], it is also shown (in increasing order of generality) that these codes can be represented as left ideals in a quotient ring of linearized polynomials. Therefore, this construction of rank-metric codes seems to be the appropriate extension of cyclic codes to the rank metric.

In this paper, we focus on two objectives: First, studying the minimum rank distance of skew cyclic codes by giving new lower bounds and by relating it with the Hamming metric. Secondly, studying and relating the lattices of skew cyclic codes and root spaces, which in particular allows to easily construct skew cyclic codes and compare the sharpness of the obtained bounds.

After some preliminaries in Section 2, the results are organized as follows: In Section 3, we give descriptions of skew cyclic codes by root spaces and cyclotomic spaces. In Section 4, we prove that the lattices of skew cyclic codes and root spaces are anti-isomorphic (isomorphic with the orders reversed), and study these lattices. In Section 5, we give bounds on their minimum rank distance, extending the rank-BCH bound obtained in [3] to rank-metric versions of the Hartmann-Tzeng bound [10] and the van Lint-Wilson shift bound [21]. Finally, in Section 6, we study skew cyclic codes that are linear over the base field, proving that classical cyclic codes equipped with the Hamming metric are a particular case of skew cyclic codes equipped with the rank metric, giving then new relations between both.

2 Definitions and preliminaries

2.1 Finite field extensions used in this work

Fix from now on a prime power q and positive integers m, n and r, and assume that m divides rn. We will consider the four finite fields $\mathbb{F}_q$, $\mathbb{F}_{q^r}$, $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^{rn}}$ shown in the following graph, where $\mathbb{F} \longrightarrow \mathbb{F}'$ means that $\mathbb{F}'$ is an extension of $\mathbb{F}$:

$$\begin{tikzcd}
 & \mathbb{F}_q \arrow[dl] \arrow[dr] & \\
\mathbb{F}_{q^m} \arrow[dr] & & \mathbb{F}_{q^r} \arrow[dl] \\
 & \mathbb{F}_{q^{rn}} &
\end{tikzcd}$$

Dimensions of vector spaces over a field $\mathbb{F}$ will be denoted by $\dim_{\mathbb{F}}$, or just dim if the field is clear from the context. For a field extension $\mathbb{F} \subseteq \mathbb{F}'$ and a subset $A \subseteq \mathbb{F}'^n$, we denote by $\langle A \rangle_{\mathbb{F}}$ the $\mathbb{F}$-linear vector space in $\mathbb{F}'^n$ generated by A.

2.2 Rank-metric codes and generalized Gabidulin codes

For convenience, all coordinates from 0 to $n-1$ or $m-1$ will be considered as integers modulo n or m, respectively. Given $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_{q^m}^n$, its rank weight [7] is defined as $\mathrm{wt_R}(\mathbf{c}) = \dim_{\mathbb{F}_q}(\langle c_0, c_1, \ldots, c_{n-1} \rangle_{\mathbb{F}_q})$. Equivalently, if $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and $\mathbf{c} = \sum_{i=0}^{m-1} \alpha_i \mathbf{c}_i$, where $\mathbf{c}_i \in \mathbb{F}_q^n$, then $\mathrm{wt_R}(\mathbf{c}) = \dim_{\mathbb{F}_q}(\langle \mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{m-1} \rangle_{\mathbb{F}_q})$.

For an $\mathbb{F}_{q^m}$-linear code $C \subseteq \mathbb{F}_{q^m}^n$, its minimum rank distance is $d_R(C) = \min\{\mathrm{wt_R}(\mathbf{c}) \mid \mathbf{c} \in C \setminus \{\mathbf{0}\}\}$. We have the Singleton bound [7] $d_R(C) \leq n - \dim(C) + 1$, and we say that C is maximum rank distance (MRD) if equality holds.

Sometimes we will use a normal basis, that is, a basis of $\mathbb{F}_{q^m}$ (or $\mathbb{F}_{q^n}$) over $\mathbb{F}_q$ of the form $\alpha, \alpha^{[1]}, \alpha^{[2]}, \ldots, \alpha^{[m-1]}$ (or $\alpha^{[n-1]}$), for some $\alpha \in \mathbb{F}_{q^m}$, where we use the notation $[i] = q^i$. Normal bases exist for all values of m (or n). See for instance, [13, Theorem 3.73].

We will consider the following family of MRD codes, usually called Gabidulin codes. They were originally defined in [7] for $r = 1$, and generalized for any r in [12]. Assume that $n \leq m$ and r and m are coprime, and take a vector $\boldsymbol{\beta} = (\beta_0, \beta_1, \ldots, \beta_{n-1}) \in \mathbb{F}_{q^m}^n$, where $\beta_0, \beta_1, \ldots, \beta_{n-1}$ are linearly independent over $\mathbb{F}_q$, and an integer $1 \leq k \leq n$. We define the (generalized) Gabidulin code of dimension k in $\mathbb{F}_{q^m}^n$ as the $\mathbb{F}_{q^m}$-linear code $\mathrm{Gab}_{k,r}(\boldsymbol{\beta})$ with parity check matrix given by

$$\mathcal{H}_{k,r}(\boldsymbol{\beta}) = \begin{pmatrix} \beta_0 & \beta_1 & \beta_2 & \cdots & \beta_{n-1} \\ \beta_0^{[r]} & \beta_1^{[r]} & \beta_2^{[r]} & \cdots & \beta_{n-1}^{[r]} \\ \beta_0^{[2r]} & \beta_1^{[2r]} & \beta_2^{[2r]} & \cdots & \beta_{n-1}^{[2r]} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \beta_0^{[(n-k-1)r]} & \beta_1^{[(n-k-1)r]} & \beta_2^{[(n-k-1)r]} & \cdots & \beta_{n-1}^{[(n-k-1)r]} \end{pmatrix}.$$

2.3 Linearized polynomials

Denote by $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ the set of q^r-linearized polynomials (abbreviated as q^r-polynomials) over $\mathbb{F}_{q^m}$ (see [7, 15, 16] or [13, Chapter 3]), that is, the polynomials in x of the form

$$F(x) = F_0 x + F_1 x^{[r]} + F_2 x^{[2r]} + \cdots + F_d x^{[dr]},$$

where $F_0, F_1, \ldots, F_d \in \mathbb{F}_{q^m}$, for $i = 0, 1, 2, \ldots, d$. We will denote $\deg_{q^r}(F(x)) = d$ if $F_d \neq 0$ and consider the symbolic product $\otimes$ in $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$, defined as follows

$$F(x) \otimes G(x) = F(G(x)),$$

for any $F(x), G(x) \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ (see [7, 13, 15, 16]). This product is distributive with respect to usual addition, associative, non-commutative and x is a left and right unit. Endowed with it and usual addition, $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ is a left and right Euclidean domain, that is, left and right Euclidean divisions exist (see [15, 16]). The term "product" will mean "symbolic product", and we will use the term "conventional" for the usual product.

2.4 Skew cyclic codes: Generator and check polynomials

Definition E.1 ([1–3, 7, 8]). Let $C \subseteq \mathbb{F}_{q^m}^n$ be an arbitrary (linear or non-linear) code. We say that it is skew cyclic or q^r-cyclic if the q^r-shifted vector

$$\sigma_{r,n}(\mathbf{c}) = (c_{n-1}^{[r]}, c_0^{[r]}, c_1^{[r]}, \ldots, c_{n-2}^{[r]}) \tag{E.1}$$

lies in C, for every $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$.

Observe that we may assume that $1 \leq r \leq m$. Moreover, by taking $r = m$, we recover the definition of cyclic codes.

Since m divides rn, $x^{[rn]} - x$ commutes with every q^r-polynomial in $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ and we may consider the quotient ring $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$, isomorphic as $\mathbb{F}_{q^m}$-linear vector space to $\mathbb{F}_{q^m}^n$ by the map $\gamma_r : \mathbb{F}_{q^m}^n \longrightarrow \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$, where

$$\gamma_r(F_0, F_1, \ldots, F_{n-1}) = F_0 x + F_1 x^{[r]} + F_2 x^{[2r]} + \cdots + F_{n-1} x^{[(n-1)r]}. \tag{E.2}$$

In the rest of the paper, given $F(x) \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$, we will use the notation F for the class of $F(x)$ modulo $x^{[rn]} - x$, that is, for the element $F = F(x) + (x^{[rn]} - x) \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$.

For $C \subseteq \mathbb{F}_{q^m}^n$, we define $C(x) = \gamma_r(C)$, that is, the image of C by the map γ_r. The following characterization is obtained independently in [1, Theorem 1] and [8, Lemma 3]:

Lemma E.2 ([1, 8]). *A code $C \subseteq \mathbb{F}_{q^m}^n$ is $\mathbb{F}_{q^m}$-linear and q^r-cyclic if, and only if, $C(x)$ is a left ideal in $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$.*

Remark E.3. *In [1–3], and in [8] for $r = 1$, left ideals in the rings $\mathcal{L}_{q^r}\mathbb{F}_q[x]/(L(x))$ are also considered, where $L(x)$ commutes with every other q^r-polynomial in $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$. We will call these codes pseudo-q^r-cyclic codes. The results in this paper concerning q^r-root spaces and left ideals in $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$ may be directly generalized to left ideals in $\mathcal{L}_{q^r}\mathbb{F}_q[x]/(L(x))$, if $L(x)$ has simple roots and if we replace $\mathbb{F}_{q^{rn}}$ by the splitting field of $L(x)$. The results are written for $L(x) = x^{[rn]} - x$ for simplicity.*

From now on, we will fix a left ideal $C(x)$. The following theorem summarizes the main properties of the generator and check polynomials of C. These were proven in [2], in [8] for $r = 1$, and originally in [7] for $r = 1$ and $m = n$:

Theorem E.1 (Generator and check polynomials [2, 7, 8]). *There exists a unique q^r-polynomial $G(x) = G_0 x + G_1 x^{[r]} + \cdots + G_{n-k} x^{[(n-k)r]}$ over $\mathbb{F}_{q^m}$ of degree $q^{(n-k)r}$ that is monic and of minimal degree among the q^r-polynomials whose residue class modulo $x^{[rn]} - x$ lies in $C(x)$. It satisfies that $C(x) = (G)$. There exists another (unique) q^r-polynomial $H(x) = H_0 x + H_1 x^{[r]} + \cdots + H_k x^{[kr]}$ over $\mathbb{F}_{q^m}$ such that $x^{[rn]} - x = G(x) \otimes H(x) = H(x) \otimes G(x)$. They satisfy:*

1. *A q^r-polynomial F lies in $C(x)$ if, and only if, $G(x)$ divides $F(x)$ on the right (in the ring $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$).*

2. *The q^r-polynomials $x \otimes G, x^{[r]} \otimes G, \ldots, x^{[(k-1)r]} \otimes G$ constitute a basis (over $\mathbb{F}_{q^m}$) of $C(x)$.*

3. *The dimension of C (over $\mathbb{F}_{q^m}$) is $k = n - \deg_{q^r}(G(x))$.*

4. *C has a generator matrix (over $\mathbb{F}_{q^m}$) given by*

$$\mathcal{G} = \begin{pmatrix} G_0 & G_1 & \ldots & G_{n-k} & 0 & \ldots & 0 \\ 0 & G_0^{[r]} & \ldots & G_{n-k-1}^{[r]} & G_{n-k}^{[r]} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & G_0^{[(k-1)r]} & G_1^{[(k-1)r]} & \ldots & G_{n-k}^{[(k-1)r]} \end{pmatrix}.$$

Moreover, if C has another generator matrix $\mathcal{G}'$ with the same form, for the values G'_i, $i = 0, 1, 2, \ldots, n-k$, then $G'_i = G'_{n-k} G_i$, for all i.

5. *A q^r-polynomial F lies in $C(x)$ if, and only if, $F \otimes H = 0$.*

6. *C has a parity check matrix (over $\mathbb{F}_{q^m}$) given by*

$$\mathcal{H} = \begin{pmatrix} h_k & h_{k-1} & \ldots & h_0 & 0 & \ldots & 0 \\ 0 & h_k^{[r]} & \ldots & h_1^{[r]} & h_0^{[r]} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & h_k^{[(n-k-1)r]} & h_{k-1}^{[(n-k-1)r]} & \ldots & h_0^{[(n-k-1)r]} \end{pmatrix},$$

where $h_i = H_i^{[(k-i)r]}$.

7. *$C^\perp$ is also q^r-cyclic and its generator of minimal degree is $H^\perp(x) = (h_k x + h_{k-1} x^{[r]} + \cdots + h_0 x^{[kr]})/h_0$.*

The q^r-polynomial $G(x)$ will be called the minimal generator of $C(x)$, and $H(x)$ will be called the minimal check q^r-polynomial of $C(x)$.

2.5 The assumptions on the lengths of skew cyclic codes

To conclude, we see that restricting to the case where m divides rn does not leave any q^r-cyclic code out of study. Assume that N is a positive integer, and take an arbitrary q^r-cyclic code $C \subseteq \mathbb{F}_{q^m}^N$. Define $n = \text{lcm}(m, N)$, which satisfies that $n = sm = tN$ for positive integers s and t, and define $\psi : \mathbb{F}_{q^m}^N \longrightarrow \mathbb{F}_{q^m}^n$ by

$$\psi(c_0, c_1, \ldots, c_{N-1}) = (c_0, c_1, \ldots, c_{N-1}; c_0, c_1, \ldots, c_{N-1}; \ldots; c_0, c_1, \ldots, c_{N-1}),$$

where we repeat the vector $(c_0, c_1, \ldots, c_{N-1})$ t times. It holds that ψ is $\mathbb{F}_{q^m}$-linear, one to one and $\text{wt}_R(\mathbf{c}) = \text{wt}_R(\psi(\mathbf{c}))$, for all $\mathbf{c} \in \mathbb{F}_{q^m}^N$. Moreover, if we define $\sigma_{r,n}$ and $\sigma_{r,N}$ as in Definition E.1, then $\psi(\sigma_{r,N}(\mathbf{c})) = \sigma_{r,n}(\psi(\mathbf{c}))$, for all $\mathbf{c} \in \mathbb{F}_{q^m}^N$, and therefore, $C \subseteq \mathbb{F}_{q^m}^N$ is q^r-cyclic if, and only if, so is $\psi(C)$. The same holds for $\mathbb{F}_q$-linearity and $\mathbb{F}_{q^m}$-linearity. To sum up, every q^r-cyclic code can be seen as a code in $\mathbb{F}_{q^m}^n$, where m divides rn.

3 Root spaces and cyclotomic spaces

In this section we will describe left ideals in $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$ in terms of q^r-root spaces and q^r-cyclotomic spaces, which are a subfamily of the former one and will which allow to easily construct skew cyclic codes. As in the classical theory of cyclic codes, we will see that the lattice of q^r-cyclic codes is anti-isomorphic (isomorphic with the orders reversed) to the lattice of q^r-root spaces. In Section 5 we will use this q^r-root space description of q^r-cyclic codes to extend the rank-BCH bound in [3, Proposition 1] to more general bounds on the minimum rank distance of q^r-cyclic codes.

3.1 The root space associated to a skew cyclic code

A q^r-polynomial $F(x)$ over $\mathbb{F}_{q^m}$ defines an $\mathbb{F}_{q^r}$-linear map $F : \mathbb{F}_{q^{rn}} \longrightarrow \mathbb{F}_{q^{rn}}$, and in particular its set of roots or zeroes in $\mathbb{F}_{q^{rn}}$ is an $\mathbb{F}_{q^r}$-linear vector space.

Definition E.4 (Root spaces). An $\mathbb{F}_{q^r}$-linear subspace of $\mathbb{F}_{q^{rn}}$ will be called a q^r-root space over $\mathbb{F}_{q^m}$ if it is the space of roots in $\mathbb{F}_{q^{rn}}$ of some $F(x) \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$.

On the other hand, for a residue class $F = F(x) + (x^{[rn]} - x)$, we define its root space, denoted as $Z(F)$, as the root space in $\mathbb{F}_{q^{rn}}$ of $F(x)$.

Finally, define the map ρ_r between the family of $\mathbb{F}_{q^m}$-linear q^r-cyclic codes in $\mathbb{F}_{q^m}^n$ and the family of q^r-root spaces over $\mathbb{F}_{q^m}$ in $\mathbb{F}_{q^{rn}}$ by $\rho_r(C) = T$, where $T = Z(G)$ and $G(x)$ is the minimal generator of $C(x)$.

Observe that the second definition is consistent, since if $F_1 = F_2$, then $F_1(x) - F_2(x)$ is divisible on the right by $x^{[rn]} - x$, and hence $F_1(x)$ and $F_2(x)$ have the same roots in $\mathbb{F}_{q^{rn}}$. The following lemma is a particular case of [13, Theorem 3.50]:

Lemma E.5 ([13]). *Given $F(x) \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$, assume that the set of its roots T lie in $\mathbb{F}_{q^{rn}}$ and all roots are simple. Then*

$$deg_{q^r}(F(x)) = \dim_{\mathbb{F}_{q^r}}(T).$$

The following theorem gathers the basic relations between C and $\rho_r(C)$:

Theorem E.2. *Let $T = \rho_r(C)$ as in Definition E.4, then:*

1. *$G(x) = \prod_{\beta \in T}(x - \beta)$.*
2. *The dimension of C over $\mathbb{F}_{q^m}$ is $k = n - \dim_{\mathbb{F}_{q^r}}(T)$.*
3. *For a q^r-polynomial $F(x)$, it holds that $F \in C(x)$ if, and only if, $F(\beta) = 0$, for all $\beta \in T$.*

4. *Let $\beta_1, \beta_2, \ldots, \beta_{n-k}$ be a basis of T over $\mathbb{F}_{q^r}$. Then the matrix*

$$\mathcal{M}(\boldsymbol{\beta}) = \begin{pmatrix} \beta_1 & \beta_1^{[r]} & \beta_1^{[2r]} & \ldots & \beta_1^{[(n-1)r]} \\ \beta_2 & \beta_2^{[r]} & \beta_2^{[2r]} & \ldots & \beta_2^{[(n-1)r]} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \beta_{n-k} & \beta_{n-k}^{[r]} & \beta_{n-k}^{[2r]} & \ldots & \beta_{n-k}^{[(n-1)r]} \end{pmatrix}$$

is a parity check matrix of C over $\mathbb{F}_{q^{rn}}$.

5. *A q^r-polynomial $\widetilde{G}$ generates $C(x)$ if, and only if, $Z(\widetilde{G}) = T$, which holds if, and only if, $G(x) = \gcd(\widetilde{G}(x), x^{[rn]} - x)$ (on the right).*

Proof. First, since $G(x)$ divides $x^{[rn]} - x$ symbolically on the right, it also divides it conventionally. Therefore, $G(x)$ has simple roots because $x^{[rn]} - x$ has simple roots, and item 1 follows.

Since the roots of $G(x)$ are simple, item 2 follows directly from the previous lemma and Theorem E.1.

Next, if $F \in (G)$, then $G(x)$ divides $F(x)$ on the right and therefore $T \subseteq Z(F)$. On the other hand, assume that $F(\beta) = 0$, for all $\beta \in T$. By the Euclidean division, we have that $F(x) = Q(x) \otimes G(x) + R(x)$, with $\deg(R(x)) < \deg(G(x))$, but then $R(\beta) = 0$, for all $\beta \in T$, and hence $R(x) = 0$. We conclude that $F \in (G)$ and item 3 follows. Item 4 follows immediately from item 3.

Finally, assume that $\widetilde{G}$ generates $C(x)$. Since G divides $\widetilde{G}$ and $\widetilde{G}$ divides G on the right, we have that $Z(\widetilde{G}) = T$. Now assume that $Z(\widetilde{G}) = T$ and define $D(x) = \gcd(\widetilde{G}(x), x^{[rn]} - x)$. We have that $D(x) = A(x) \otimes \widetilde{G}(x) + B(x) \otimes (x^{[rn]} - x)$, for some q^r-polynomials $A(x)$ and $B(x)$. It follows that $T \subseteq Z(D)$, and since $D(x)$ divides $\widetilde{G}(x)$, it holds that $T = Z(D)$. Finally, since $D(x)$ divides $x^{[rn]} - x$, every root of $D(x)$ lies in $\mathbb{F}_{q^{rn}}$ and is simple, which implies that $D(x) = G(x)$. Now assume that $G(x) = \gcd(\widetilde{G}(x), x^{[rn]} - x)$, then $G(x) = A(x) \otimes \widetilde{G}(x) + B(x) \otimes (x^{[rn]} - x)$, for some q^r-polynomials $A(x)$ and $B(x)$. Therefore, $G \in (\widetilde{G})$, and since $G(x)$ divides $\widetilde{G}(x)$, it holds that $(G) = (\widetilde{G})$, and item 5 follows. □

On the other hand, we have the following equivalent conditions on inclusions of q^r-cyclic codes and q^r-root spaces.

Corollary E.6. *Let $C_1(x) = (G_1)$ and $C_2(x) = (G_2)$ be two q^r-cyclic codes with $T_1 = Z(G_1)$ and $T_2 = Z(G_2)$, where $G_1(x)$ and $G_2(x)$ are the minimal generators of $C_1(x)$ and $C_2(x)$, respectively. Then $C_1(x) \subseteq C_2(x)$ if, and only if, $G_2(x)$ divides $G_1(x)$ on the right, and this holds if, and only if, $T_2 \subseteq T_1$.*

Proof. The first equivalence is clear from Theorem E.1. Now, if $G_2(x)$ divides $G_1(x)$ on the right, then it is obvious that $T_2 \subseteq T_1$.

Finally, assume that $T_2 \subseteq T_1$, and perform the Euclidean division to obtain $G_1(x) = Q(x) \otimes G_2(x) + R(x)$, with $\deg(R(x)) < \deg(G_2(x))$. We have that $R(\beta) = 0$, for every $\beta \in T_2$, and by the previous theorem, $R \in (G_2)$. However, $G_2(x)$ is the minimal generator of $C_2(x)$, so it follows that $R(x) = 0$, that is, $G_2(x)$ divides $G_1(x)$ on the right. □

The previous corollary and Theorem E.2 imply that the map ρ_r is bijective:

Corollary E.7. *The map ρ_r in Definition E.4 is bijective.*

Proof. We first see that it is onto. Take $T = Z(F)$ a q^r-root space over $\mathbb{F}_{q^m}$ in $\mathbb{F}_{q^{rn}}$. By item 5 in Theorem E.2, it holds that $Z(G) = T$ if $G(x)$ is the minimal generator of $C(x) = (F)$. Therefore, $T = \rho_r(C)$. On the other hand, ρ_r is one to one by the previous corollary. □

In the next section we will see that the family of q^r-root spaces over $\mathbb{F}_{q^m}$ in $\mathbb{F}_{q^{rn}}$ is a lattice with sums and additions of vector spaces, and therefore Corollary E.6 together with the previous corollary mean that the map ρ_r is an anti-isomorphism of lattices (an isomorphism with the orders reversed).

On the other hand, Theorem E.2 gives the following criterion to say whether an $\mathbb{F}_{q^r}$-linear subspace $T \subseteq \mathbb{F}_{q^{rn}}$ is a q^r-root space, in terms of q^r-cyclic codes:

Corollary E.8. *Let $T \subseteq \mathbb{F}_{q^{rn}}$ be $\mathbb{F}_{q^r}$-linear, take one of its bases $\beta_1, \beta_2, \ldots, \beta_{n-k}$ over $\mathbb{F}_{q^r}$, and define $\mathcal{M}(\boldsymbol{\beta})$ as in Theorem E.2. Consider $\widetilde{C} \subseteq \mathbb{F}_{q^{rn}}^n$, the $\mathbb{F}_{q^{rn}}$-linear code with $\mathcal{M}(\boldsymbol{\beta})$ as parity check matrix. Then T is a q^r-root space over $\mathbb{F}_{q^m}$ if, and only if,*

$$\dim_{\mathbb{F}_{q^m}}(\widetilde{C} \cap \mathbb{F}_{q^m}^n) = \dim_{\mathbb{F}_{q^{rn}}}(\widetilde{C}), \tag{E.3}$$

which holds if, and only if, $\widetilde{C}$ has a basis of vectors in $\mathbb{F}_{q^m}^n$.

Proof. Assume first that $T = Z(F)$, for some q^r-polynomial $F(x)$ over $\mathbb{F}_{q^m}$, and define $C(x) = (F)$. By items 4 and 5 in Theorem E.2, $C = \widetilde{C} \cap \mathbb{F}_{q^m}^n$, and by item 2 in the same theorem, $\dim_{\mathbb{F}_{q^m}}(C) = k = \dim_{\mathbb{F}_{q^{rn}}}(\widetilde{C})$.

Assume now that $\dim_{\mathbb{F}_{q^m}}(C) = \dim_{\mathbb{F}_{q^{rn}}}(\widetilde{C})$, where $C = \widetilde{C} \cap \mathbb{F}_{q^m}^n$. Since $\widetilde{C}$ is q^r-cyclic, it follows that C is also q^r-cyclic. By definition, $T \subseteq Z(G)$, for the minimal generator $G(x)$ of $C(x)$. Now, $\dim_{\mathbb{F}_{q^m}}(C) = k$ by hypothesis, and hence $\dim_{\mathbb{F}_{q^r}}(Z(G)) = n - k$ by item 2 in Theorem E.2. Also by hypothesis, $\dim_{\mathbb{F}_{q^r}}(T) = n - k$, so it holds that $T = Z(G)$. □

Observe that condition (E.3) means that $\widetilde{C}$ is Galois closed over $\mathbb{F}_{q^m}$. See [14, 20] for more details on Galois closed vector spaces. The following example shows how to use this result to see whether a given vector space is a q^r-root space.

Example E.9. Assume that $n = 2m$ and $r = 1$, and take a normal basis $\alpha, \alpha^{[1]}, \ldots, \alpha^{[n-1]} \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Consider the ($\mathbb{F}_q$-linear) vector subspaces $T_1, T_2 \subseteq \mathbb{F}_{q^n}$ generated by α and $\alpha, \alpha^{[m]}$, respectively. Define also the codes $\widetilde{C}_1, \widetilde{C}_2 \subseteq \mathbb{F}_{q^n}^n$ with parity check matrices $\mathcal{M}(\alpha)$ and $\mathcal{M}(\alpha, \alpha^{[m]})$, respectively, and define $D_i = (\widetilde{C}_i \cap \mathbb{F}_{q^m}^n)^{\perp}$, $i = 1, 2$. They satisfy $D_i = \mathrm{Tr}(\widetilde{C}_i^{\perp})$, $i = 1, 2$, by Delsarte's theorem [4, Theorem 2], where Tr denotes the trace of the extension $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$, that is, $\mathrm{Tr}(x) = x + x^{[m]}$.

We will see that T_1 is not a q-root space over $\mathbb{F}_{q^m}$, whereas T_2 is. Moreover, we will see that $D_1 = D_2$, which has dimension 2 over $\mathbb{F}_{q^m}$ and which shows that condition (E.3) in the previous corollary is satisfied for T_2 but not for T_1.

Since $\dim(T_1) = 1$, if it were a q-root space, then there would exist $b \in \mathbb{F}_{q^m}$ with $F(\alpha) = 0$, where $F(x) = x^{[1]} - bx$ by Corollary E.7. Since $x^{[m]} \otimes F(x) = F(x) \otimes x^{[m]}$, it holds that $F(\alpha^{[m]}) = 0$. This would imply that $\alpha, \alpha^{[m]} \in T_1$ and $\dim(T_1) = 1$, which is absurd.

On the other hand, we see that $D_1 \subseteq D_2$. Define the vectors $\boldsymbol{\alpha} = (\alpha, \alpha^{[1]}, \ldots, \alpha^{[n-1]}) \in \mathbb{F}_{q^n}^n$, $\mathbf{v}_0 = \mathrm{Tr}(\alpha\boldsymbol{\alpha}) = \alpha\boldsymbol{\alpha} + \alpha^{[m]}\boldsymbol{\alpha}^{[m]}$ and $\mathbf{v}_1 = \mathrm{Tr}(\alpha^{[1]}\boldsymbol{\alpha}) = \alpha^{[1]}\boldsymbol{\alpha} + \alpha^{[1+m]}\boldsymbol{\alpha}^{[m]}$, which belong to D_1 and also to $\widetilde{C}_2^{\perp}$. Moreover, we see that they are linearly independent over $\mathbb{F}_{q^n}$ and, therefore, they constitute a basis of $\widetilde{C}_2^{\perp}$. This means that $D_1 = D_2$ and $\dim_{\mathbb{F}_{q^m}}(D_2) = \dim_{\mathbb{F}_{q^n}}(\widetilde{C}_2^{\perp}) = 2$.

In conclusion, condition (E.3) is satisfied for T_2 but not for T_1. By the previous corollary, it holds that T_2 is a q-root space over $\mathbb{F}_{q^m}$, and we have seen that T_1 is not a q-root space over $\mathbb{F}_{q^m}$.

3.2 Cyclotomic spaces

Now we turn to a special subclass of q^r-root spaces in $\mathbb{F}_{q^{rn}}$, namely the class of q^r-cyclotomic spaces. These spaces will play the same role as cyclotomic sets in the classical theory of cyclic codes (see [11, Theorem 4.4.2] and [11, Theorem 4.4.3]), that is, they generate the lattice of q^r-root spaces, and are key concepts to easily construct skew cyclic codes.

For this we need the concept of minimal q^r-polynomial of an element $\beta \in \mathbb{F}_{q^{rn}}$ over $\mathbb{F}_{q^m}$. The following lemma and definition constitute an extension of [13, Theorem 3.68] and the discussion prior to it:

Lemma E.10. *For any β in an extension field of $\mathbb{F}_{q^{\mathrm{lcm}(r,m)}}$, there exists a unique monic q^r-polynomial $F(x) \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ of minimal degree such that $F(\beta) = 0$. Moreover, if $L(\beta) = 0$ for another q^r-polynomial $L(x)$ over $\mathbb{F}_{q^m}$, then $F(x)$ divides $L(x)$ both conventionally and symbolically on the right.*

Proof. If $\beta \in \mathbb{F}_{q^{rt}}$, $t > 0$, then the polynomial $\widetilde{F}(x) = x^{[rt]} - x$ lies in $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ and $\widetilde{F}(\beta) = 0$. Therefore there exists an $F(x) \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ monic and of minimal degree such that $F(\beta) = 0$. Let $L(x) \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ be such that

$L(\beta) = 0$, and perform the Euclidean division to obtain $L(x) = Q(x) \otimes F(x) + R(x)$, with $\deg(R(x)) < \deg(F(x))$. Then $R(\beta) = 0$, and since $F(x)$ is of minimal degree, we have that $R(x) = 0$, and therefore $F(x)$ divides $L(x)$ both conventionally and symbolically on the right. This also proves that $F(x)$ is unique and we are done. □

Definition E.11. For β in an extension field of $\mathbb{F}_{q^{\mathrm{lcm}(r,m)}}$, the q^r-polynomial $F(x)$ in the previous lemma is called the minimal q^r-polynomial of β over $\mathbb{F}_{q^m}$.

Now we may define q^r-cyclotomic spaces in $\mathbb{F}_{q^{rn}}$:

Definition E.12 (Cyclotomic spaces). Given $\beta \in \mathbb{F}_{q^{rn}}$, we define its q^r-cyclotomic space over $\mathbb{F}_{q^m}$ as the $\mathbb{F}_{q^r}$-linear vector space $C_{q^r}(\beta)$ of roots of the minimal q^r-polynomial of β over $\mathbb{F}_{q^m}$.

Example E.13. Let the notation and assumptions be as in Example E.9. Since the basis $\alpha^{[b]}, (\alpha^{[b]})^{[1]}, \ldots, (\alpha^{[b]})^{[n-1]}$ is also normal, in Example E.9 we have proven that $C_q(\alpha^{[b]}) = \langle \alpha^{[b]}, \alpha^{[b+m]} \rangle$.

In general, for $r = 1$ and $n = sm$, we have the following result:

Proposition E.14. *If $\alpha, \alpha^{[1]}, \ldots, \alpha^{[n-1]}$ is a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, then it holds that $C_q(\alpha^{[b]}) = \langle \alpha^{[b]}, \alpha^{[b+m]}, \ldots, \alpha^{[b+(s-1)m]} \rangle$, for every integer $b \geq 0$.*

Proof. We may assume that $b = 0$ without loss of generality. First of all, for every $F(x) \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$, we see that $x^{[m]} \otimes F(x) = F(x) \otimes x^{[m]}$ and, therefore $F(\beta) = 0$ implies that $F(\beta^{[m]}) = 0$, for any $\beta \in \mathbb{F}_{q^n}$. This means that $\langle \alpha, \alpha^{[m]}, \ldots, \alpha^{[(s-1)m]} \rangle \subseteq C_q(\alpha)$.

The reversed inclusion is proven using Corollary E.8 as in Example E.9. To that end, we need to define the vectors $\mathbf{v}_i = \mathrm{Tr}(\alpha^{[i]}\boldsymbol{\alpha}) = \sum_{j=0}^{s-1} \alpha^{[i+jm]}\boldsymbol{\alpha}^{[jm]} \in \mathbb{F}_{q^m}^n$, for $i = 0, 1, 2, \ldots, s-1$, where $\boldsymbol{\alpha} = (\alpha, \alpha^{[1]}, \ldots, \alpha^{[n-1]}) \in \mathbb{F}_{q^n}^n$. The vectors $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{s-1}$ are linearly independent over $\mathbb{F}_{q^m}$, since so are the vectors $\boldsymbol{\alpha}$, $\boldsymbol{\alpha}^{[m]}, \ldots, \boldsymbol{\alpha}^{[(s-1)m]}$ and the following matrix is non-singular:

$$\begin{pmatrix} \alpha & \alpha^{[m]} & \alpha^{[2m]} & \ldots & \alpha^{[(s-1)m]} \\ \alpha^{[1]} & \alpha^{[1+m]} & \alpha^{[1+2m]} & \ldots & \alpha^{[1+(s-1)m]} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^{[s-1]} & \alpha^{[s-1+m]} & \alpha^{[s-1+2m]} & \ldots & \alpha^{[s-1+(s-1)m]} \end{pmatrix}.$$

□

Next we see that every q^r-root space is a sum of q^r-cyclotomic spaces. Since in the next section we will see that sums and intersections of q^r-root spaces are again q^r-root spaces, this means that the subclass of q^r-cyclotomic spaces generates the lattice of q^r-root spaces:

Proposition E.15. *Given a q^r-root space $T \subseteq \mathbb{F}_{q^{rn}}$ over $\mathbb{F}_{q^m}$, there exist $\beta_1, \beta_2, \ldots, \beta_u \in T$ such that $T = C_{q^r}(\beta_1) + C_{q^r}(\beta_2) + \cdots + C_{q^r}(\beta_u)$. Moreover, if the q^r-cyclotomic spaces $C_{q^r}(\beta_i)$ over $\mathbb{F}_{q^m}$ are minimal and T is not a sum of a strict subset of them, then the sum is direct.*

Proof. Take $L(x) \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ such that $T = Z(L)$. For every $\beta \in T$, if $F(x)$ is its minimal q^r-polynomial over $\mathbb{F}_{q^m}$, then by Lemma E.10, $F(x)$ divides $L(x)$ and, therefore, $C_{q^r}(\beta) = Z(F) \subseteq Z(L) = T$. This means that $T = \sum_{\beta \in T} C_{q^r}(\beta)$. Since the sum is finite, the result follows.

Finally, assume that the $C_{q^r}(\beta_i)$ are minimal and T is not a sum of a strict subset of them. If there exists $\beta \in C_{q^r}(\beta_i) \cap (\sum_{j \neq i} C_{q^r}(\beta_j))$ that is not zero, then by minimality of $C_{q^r}(\beta_i)$, we have that $C_{q^r}(\beta) = C_{q^r}(\beta_i)$, and therefore $C_{q^r}(\beta_i) \subseteq \sum_{j \neq i} C_{q^r}(\beta_j)$. However, this means that T is the sum of the spaces $C_{q^r}(\beta_j)$, with $j \neq i$, which contradicts the assumptions. □

4 The lattices of q^r-cyclic codes and q^r-root spaces

It is straightforward to see that sums and intersections of q^r-cyclic codes are again q^r-cyclic. In this section we will see that the same holds for q^r-root spaces. By Corollary E.6, both lattices are anti-isomorphic. We will also prove this directly by showing that intersections of q^r-cyclic codes correspond to sums of q^r-root spaces and viceversa. We will also study the concept of q^r-cyclic complementary of a q^r-cyclic code, rank equivalences and lattice morphisms.

4.1 The lattice anti-isomorphism

Theorem E.3. *Let $C_1(x)$ and $C_2(x)$ be two q^r-cyclic codes with minimal generators $G_1(x)$ and $G_2(x)$, respectively. Set $T_1 = Z(G_1)$ and $T_2 = Z(G_2)$. We have that*

1. *$C_1(x) \cap C_2(x)$ is the q^r-cyclic code whose minimal generator is given by $M(x) = \mathrm{lcm}(G_1(x), G_2(x))$ (on the right), and $Z(M) = T_1 + T_2$.*

2. *$C_1(x) + C_2(x)$ is the q^r-cyclic code whose minimal generator is given by $D(x) = \gcd(G_1(x), G_2(x))$ (on the right), and $Z(D) = T_1 \cap T_2$.*

In particular, sums and intersections of q^r-root spaces are again q^r-root spaces, and they form a lattice anti-isomorphic to the lattice of q^r-cyclic codes by the map ρ_r in Definition E.4. Moreover, the lattice of q^r-root spaces is generated by the subclass of q^r-cyclotomic spaces.

Proof. Define $M(x)$ as the minimal generator of $C_1(x) \cap C_2(x)$. We have that $G_1(x)$ and $G_2(x)$ both divide $M(x)$ on the right by Theorem E.1, item 1, since $M \in (G_1)$ and $M \in (G_2)$. Now, if $F \in C_1(x) \cap C_2(x)$, then $M(x)$ divides $F(x)$

on the right for the same reason. In conclusion, $M(x)$ is the least common multiple on the right of $G_1(x)$ and $G_2(x)$.

On the other hand, define $D(x)$ as the greatest common divisor of $G_1(x)$ and $G_2(x)$ on the right. By the Euclidean algorithm, we may find a Bézout's identity on the right $D(x) = Q_1(x) \otimes G_1(x) + Q_2(x) \otimes G_2(x)$. This implies that $(D) \subseteq C_1(x) + C_2(x)$. Moreover, by definition $D(x)$ divides both $G_1(x)$ and $G_2(x)$ on the right, and therefore $C_1(x) + C_2(x) \subseteq (D)$, and hence they are equal.

To see that $D(x)$ is the minimal generator, take $F \in (D)$, then $F(x) = Q(x) \otimes D(x) + P(x) \otimes (x^{[rn]} - x)$. But since $D(x)$ divides both $G_1(x)$ and $G_2(x)$, and these divide $x^{[rn]} - x$, then $D(x)$ divides $x^{[rn]} - x$ and hence, it divides $F(x)$.

Finally, we see that $T_1 \cup T_2 \subseteq Z(M)$ by Theorem E.2, item 3, since $M \in C_1(x) \cap C_2(x)$. Therefore, $T_1 + T_2 \subseteq Z(M)$. On the other hand, since $D \in C_1(x) + C_2(x)$, we see that $T_1 \cap T_2 \subseteq Z(D)$ also by Theorem E.2, item 3. By the same theorem, we have that

$$\dim(T_1 + T_2) + \dim(T_1 \cap T_2) = \dim(T_1) + \dim(T_2) = (n - \dim(C_1)) + (n - \dim(C_2))$$

$$= (n - \dim(C_1 \cap C_2)) + (n - \dim(C_1 + C_2)) = \dim(Z(M)) + \dim(Z(D)).$$

Hence, $Z(M) = T_1 + T_2$ and $Z(D) = T_1 \cap T_2$ and we are done.

The last statement of the theorem follows from Proposition E.15. □

4.2 Skew cyclic complementaries and idempotent generators

The existence and/or uniqueness of complementaries is an important property of lattices. In the theory of classical cyclic codes, every cyclic code has a unique complementary cyclic code when the length and q are coprime [11, Exercise 243]. In this case, every cyclic code also has an idempotent generator [11, Theorem 4.3.2], which describes very easily the complementary cyclic code (see [11, Theorem 4.4.6]).

In this subsection we investigate the existence and uniqueness of q^r-cyclic complementaries and idempotent generators of q^r-cyclic codes, and relate both.

Observe that, by the fact that the map ρ_r in Definition E.2 is a lattice anti-isomorphism, two q^r-cyclic codes are complementary if, and only if, their corresponding q^r-root spaces are complementary.

Proposition E.16. *Given q^r-cyclic codes $C_1(x)$ and $C_2(x)$ with minimal generators $G_1(x)$ and $G_2(x)$, we have that they are complementary, that is, $\mathbb{F}_{q^m}^n = C_1 \oplus C_2$ if, and only if, $G_1(x)$ and $G_2(x)$ are coprime (on the right) and $\deg_{q^r}(G_1(x)) + \deg_{q^r}(G_2(x)) = n$.*

Proof. By Theorem E.3, the condition $C_1(x) + C_2(x) = \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$ is equivalent to $D(x) = x$, which means that $G_1(x)$ and $G_2(x)$ are coprime. By Theorem E.1, if C_1 and C_2 are complementary, then

$$\deg_{q^r}(G_1(x)) + \deg_{q^r}(G_2(x)) = n - \dim(C_1) + n - \dim(C_2)$$

$$= n - (\dim(C_1) + \dim(C_2) - \dim(C_1 + C_2)) = n - \dim(C_1 \cap C_2) = n.$$

Conversely, if $D(x) = x$ and $\deg_{q^r}(G_1(x)) + \deg_{q^r}(G_2(x)) = n$, then $C_1 + C_2 = \mathbb{F}_{q^m}^n$ by Theorem E.3 and $\dim(C_1 \cap C_2) = 0$ by Theorem E.1 as before, and the theorem follows. □

In [9, Theorem 6], the existence of an idempotent generator is proven when n is coprime with q and also with the order of the automorphism $\alpha \mapsto \alpha^{[r]}$. We next prove the existence in other cases (see Example E.19 below), and give other properties.

Theorem E.4. *Let $C(x)$ be a left ideal with minimal generator $G(x)$ and check q^r-polynomial $H(x)$. The following holds*

1. *An element $E \in C(x)$ is idempotent (that is, $E \otimes E = E$) and generates $C(x)$ if, and only if, it is a unit on the right in this ideal.*
2. *Given a q^r-polynomial $F(x)$ and an idempotent generator E of $C(x)$, it holds that $F \in C(x)$ if, and only if, $F = F \otimes E$. In particular, $x - E(x)$ is a check polynomial for $C(x)$.*
3. *For any idempotent generator E of $C(x)$, the q^r-polynomial $x - E$ is also idempotent and $(x - E)$ is a complementary for $C(x)$.*
4. *Assume that G and H are coprime on both sides. That is, we may obtain Bézout identities on both sides*

$$x = G \otimes G_1 + H \otimes H_1 = G_2 \otimes G + H_2 \otimes H,$$

in the ring $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$. Let $E = x - H_2 \otimes H$ and $E' = x - H \otimes H_1$. It holds that $E = E'$, and it is an idempotent generator for $C(x)$.

Proof. Items 1 and 2 are proven as in the classical case (see [11, Section 4.3]). For item 3, we have that $(x - E) + (E)$ is the whole quotient ring. On the other hand, take $F \in (x - E) \cap (E)$. By item 1, E and $x - E$ are units on the right in the ideals that they generate. Therefore, $F = F \otimes E$ and $F = F \otimes (x - E) = F - F \otimes E = F - F = 0$. It follows that $(x - E) \cap (E) = \{0\}$, and item 3 is proven.

We now prove item 4. We have that $E = G_2 \otimes G$, $E' = G \otimes G_1$ and $G \otimes H = H \otimes G = 0$ by Theorem E.1. Therefore $E' = E \otimes E' = E$, and it is idempotent. On the other hand, $E \in (G)$ and $G = G \otimes E' \in (E')$, and therefore $C(x) = (G) = (E)$. □

From the previous theorem and proposition, we deduce the following for a left ideal $C(x)$ with minimal generator $G(x)$ and check q^r-polynomial $H(x)$:

Corollary E.17. *The q^r-cyclic codes (G) and (H) are complementary if, and only if, $G(x)$ and $H(x)$ are coprime. In that case, if E is the idempotent described in item 4 in the previous theorem, then $(x - E) = (H)$.*

Remark E.18. *Recall from Theorem E.2, item 5, that in particular, the minimal generator of a left ideal can be efficiently obtained from the idempotent generator.*

Example E.19. Let $q = 2$, $n = m = 3$ and $r = 1$, consider the primitive element $\alpha \in \mathbb{F}_{2^3}$ such that $\alpha^3 + \alpha + 1 = 0$, and the q-polynomials $G(x) = x^{[2]} + \alpha^4 x^{[1]} + \alpha^6 x$ and $H(x) = x^{[1]} + \alpha x$, as in [8, Example 2]. By Euclidean division on both sides, we find that

$$x = x \otimes G(x) + (x^{[1]} + \alpha x) \otimes H(x) = G(x) \otimes x + H(x) \otimes (x^{[1]} + \alpha x).$$

Then $E = E' = G$. In this case the idempotent generator coincides with the minimal generator. Observe also that here the order of the automorphism $\alpha \mapsto \alpha^{[1]}$ is 3, and hence is not coprime with n. Therefore, Theorem E.4 covers other cases than [9, Theorem 6].

On the other hand, we see that the q-polynomial $x - E = x^{[2]} + \alpha^4 x^{[1]} + \alpha^2 x = (x^{[1]} + \alpha x) \otimes H(x)$ is an idempotent generator of (H), which is a complementary for $C(x)$, as stated in the previous corollary.

4.3 Rank equivalences and lattice automorphisms

To conclude the section, we study rank equivalences and automorphisms of lattices of the family of q^r-cyclic codes. A rank equivalence $\varphi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$ is an $\mathbb{F}_{q^m}$-linear vector space isomorphism with $\mathrm{wt_R}(\varphi(\mathbf{c})) = \mathrm{wt_R}(\mathbf{c})$ (see [14] for more details on rank equivalences). For convenience, we define the rank weight of $F \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$ as

$$\mathrm{wt_R}(F) = \mathrm{wt_R}(F_0, F_1, \ldots, F_{n-1}) = \mathrm{wt_R}(\gamma_r^{-1}(F)), \tag{E.4}$$

where γ_r is as in (E.2). Since the map ρ_r in Definition E.2 is a lattice anti-isomorphism by Theorem E.3, every automorphism of the lattice of $\mathbb{F}_{q^m}$-linear q^r-cyclic codes induces an automorphism of the lattice of q^r-root spaces over $\mathbb{F}_{q^m}$. In particular, every ring automorphism of $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$ induces such a lattice automorphism.

We study the following class of ring automorphisms:

Definition E.20. For every $a = 0, 1, 2, \ldots, rn - 1$, we define the morphism $\varphi_a : \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x) \longrightarrow \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$ by $\varphi_a(F) = x^{[rn-a]} \otimes F \otimes x^{[a]}$.

We observe that this map is well-defined and corresponds to rising to the power q^{rn-a} in $\mathbb{F}_{q^m}^n$ (and φ_0 is the identity). That is, if $F = F_0x + F_1x^{[r]} + \cdots + F_{n-1}x^{[(n-1)r]}$, then

$$x^{[rn-a]} \otimes F \otimes x^{[a]} = F_0^{[rn-a]}x + F_1^{[rn-a]}x^{[r]} + \cdots + F_{n-1}^{[rn-a]}x^{[(n-1)r]}.$$

We gather the main properties of the maps φ_a in the next proposition:

Proposition E.21. *For every $a, a' = 0, 1, 2, \ldots, rn-1$, the map φ_a satisfies:*

1. *φ_a is a ring isomorphism. Viewed as map $\varphi_a : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$, it is $\mathbb{F}_q$-linear and $\mathbb{F}_{q^m}$-semilinear.*
2. *$\varphi_a = \varphi_{a'}$ if, and only if, a and a' are congruent modulo m.*
3. *$\varphi_0 = \mathrm{Id}$ and $\varphi_a \circ \varphi_{a'} = \varphi_{a'} \circ \varphi_a = \varphi_{a+a'}$. In particular, $\varphi_a \circ \varphi_{n-a} = \varphi_{n-a} \circ \varphi_a = \mathrm{Id}$.*
4. *For every q^r-polynomial $F(x)$, it holds that $\mathrm{wt_R}(F) = \mathrm{wt_R}(\varphi_a(F))$ (see (E.4)), that is, φ_a is a rank equivalence.*
5. *φ_a maps left ideals to left ideals and, in general, maps q^r-cyclic codes to q^r-cyclic codes.*
6. *φ_a maps idempotents to idempotents.*

Proof. The first three items are straightforward calculations. The last two items follow from these first three items.

Finally, if $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_{q^m}^n$, then the dimension of the vector space generated by $c_0, c_1, \ldots, c_{n-1}$ in $\mathbb{F}_{q^m}$ is the same as the dimension (over $\mathbb{F}_q$) of the vector space generated by $c_0^q, c_1^q, \ldots, c_{n-1}^q$, since rising to the power q is an $\mathbb{F}_q$-linear automorphism of $\mathbb{F}_{q^m}$. Therefore, $\mathrm{wt_R}(c_0, c_1, \ldots, c_{n-1}) = \mathrm{wt_R}(c_0^q, c_1^q, \ldots, c_{n-1}^q)$.

Since φ_a corresponds to rising to the power q^{rn-a}, we see that it also preserves rank weights, and item 4 follows. □

Remark E.22. *By item 6 in the previous proposition and Theorem E.2, item 5, we may obtain the minimal generator of a q^r-cyclic code equivalent to a given one if we know the minimal generator or an idempotent of this latter code.*

On the other hand, these are the only maps coming from ring automorphisms of $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$ having the following reasonable properties: they commute with the q^r-shifting operators (E.1), are $\mathbb{F}_q$-linear and leave the field $\mathbb{F}_{q^m}$ invariant ($\mathbb{F}_{q^m}$ is a subring of $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$ by considering any $\alpha \in \mathbb{F}_{q^m}$ as the polynomial αx).

Proposition E.23. *For $a = 0, 1, 2, \ldots, rn-1$, if we view φ_a as a map $\varphi_a : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$, then it holds that*

$$\sigma_{r,n} \circ \varphi_a = \varphi_a \circ \sigma_{r,n},$$

where $\sigma_{r,n}$ is as in (E.1). Moreover, if φ is an $\mathbb{F}_q$-linear ring automorphism of $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$ satisfying this condition and leaving $\mathbb{F}_{q^m}$ invariant, then $\varphi = \varphi_a$ for some $a = 0, 1, 2, \ldots, rn-1$.

Proof. The fact that a ring automorphism φ commutes with $\sigma_{r,n}$ is equivalent to the condition

$$\varphi(x^{[1]} \otimes F) = x^{[1]} \otimes \varphi(F), \tag{E.5}$$

for all $F \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$, which is satisfied if $\varphi = \varphi_a$.

On the other hand, since $\varphi(\alpha x + \beta x) = \varphi(\alpha x) + \varphi(\beta x)$ and $\varphi(\alpha x \otimes \beta x) = \varphi(\alpha x) \otimes \varphi(\beta x)$, for all $\alpha, \beta \in \mathbb{F}_{q^m}$, we have that φ is an automorphism of the field $\mathbb{F}_{q^m}$ when restricted to constant polynomials αx.

Moreover, if $\alpha \in \mathbb{F}_q$, by $\mathbb{F}_q$-linearity it holds that $\varphi(\alpha x) = \alpha x \otimes \varphi(x) = \alpha x$. Hence $\mathbb{F}_q$ is fixed by the automorphism induced by φ in $\mathbb{F}_{q^m}$. Therefore, there exists an $a = 0, 1, 2, \ldots, m-1$ such that $\varphi(\alpha x) = \alpha^{[nr-a]} x$, for all $\alpha \in \mathbb{F}_{q^m}$. This together with (E.5) means that $\varphi = \varphi_a$ and we are done. □

Finally, we see that the lattice automorphism induced by φ_a in the lattice of q^r-spaces over $\mathbb{F}_{q^m}$ corresponds to the one induced by the field automorphism of $\mathbb{F}_{q^{rn}}$ given by $\beta \mapsto \beta^{[a]}$. In particular, by item 2 in Proposition E.21, two of these automorphisms of the lattice of q^r-root spaces over $\mathbb{F}_{q^m}$, for a and a', respectively, are equal if, and only if, a and a' are congruent modulo m. In short:

Proposition E.24. *For all $a = 0, 1, 2, \ldots, nr-1$ and all $F \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$, it holds that $Z(\varphi_a(F)) = Z(F)^{[a]}$. In particular, $Z(F)^{[a]} = Z(F)^{[a']}$ if a and a' are congruent modulo m.*

5 Bounds on the minimum rank distance

In this section we will give lower bounds on the minimum rank distance of q^r-cyclic codes. The simplest bound on the minimum Hamming distance of classical cyclic codes is the BCH bound, which has been adapted to a bound on the minimum rank distance of q^r-cyclic codes in [3, Proposition 1]. In this section, we will give two extensions of this bound analogous to the Hartmann-Tzeng bound [10] in the form of [21, Theorem 2], and another one analogous to the bound in [21, Theorem 11], also known as the shift bound.

5.1 The rank-shift and rank-Hartmann-Tzeng bounds

We start by giving the definition of independent sequence of $\mathbb{F}_{q^r}$-linear vector subspaces of $\mathbb{F}_{q^{rn}}$ with respect to some $\mathbb{F}_{q^r}$-linear subspace $S \subseteq \mathbb{F}_{q^{rn}}$.

Definition E.25. Given $\mathbb{F}_{q^r}$-linear subspaces $S, I_0, I_1, I_2, \ldots \subseteq \mathbb{F}_{q^{rn}}$, we say that the sequence $I_0, I_1, I_2, \ldots$ is independent with respect to S if the following hold:

1. $I_0 = \{\mathbf{0}\}$.
2. For $i > 0$, either
   (a) $I_i = I_j \oplus \langle \beta \rangle$, for some $0 \leq j < i$, $I_j \subseteq S$ and $\beta \notin S$, or
   (b) $I_i = I_j^{[br]}$, for some $0 \leq j < i$ and some integer $b \geq 0$.

We say that a subspace $I \subseteq \mathbb{F}_{q^{rn}}$ is independent with respect to S if it is a space in a sequence that is independent with respect to S.

The van Lint-Wilson or shift bound [21, Theorem 11] for the rank metric becomes then as follows. Observe that it is a bound on the rank weight (see (E.4)) of a given q^r-polynomial in $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$ in terms of its roots.

Theorem E.5 (Rank-shift bound). *Let $F \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$ and $S = Z(F)$ $= \{\beta \in \mathbb{F}_{q^{rn}} \mid F(\beta) = 0\}$, as in Definition E.4. If $I \subseteq \mathbb{F}_{q^{rn}}$ is an $\mathbb{F}_{q^r}$-linear subspace independent with respect to S, then*

$$\mathrm{wt_R}(F) \geq \dim_{\mathbb{F}_{q^r}}(I),$$

where $\mathrm{wt_R}(F)$ *is as in (E.4).*

Proof. Define the vector $\mathbf{F} = (F_0, F_1, \ldots, F_{n-1}) \in \mathbb{F}_{q^m}^n$ if $F = F_0 x + F_1 x^{[r]} + \cdots + F_{n-1} x^{[(n-1)r]}$ (recall (E.2)). Now write $\mathbf{F} = \sum_{i=0}^{m-1} \alpha_i \mathbf{F}_i$, where $\mathbf{F}_i \in \mathbb{F}_q^n$, for $i = 0, 1, \ldots, m-1$ and $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Define $w = \mathrm{wt_R}(F)$, and recall from Subsection 2.2 that $w = \dim_{\mathbb{F}_q}(\langle \mathbf{F}_0, \mathbf{F}_1, \ldots, \mathbf{F}_{m-1} \rangle_{\mathbb{F}_q})$.

Let A be a $w \times n$ matrix over $\mathbb{F}_q$ whose rows generate the vector space $\langle \mathbf{F}_0, \mathbf{F}_1, \ldots, \mathbf{F}_{m-1} \rangle_{\mathbb{F}_q}$. Since A is full-rank, there exists a $w \times n$ matrix A' over $\mathbb{F}_q$ such that $AA'^T = I$. On the other hand, by definition of A, there exist $\mathbf{x}_i \in \mathbb{F}_q^w$ with $\mathbf{F}_i = \mathbf{x}_i A$, for $i = 0, 1, \ldots, m-1$. It follows that

$$\mathbf{F}(A'^T A) = \sum_{i=0}^{m-1} \alpha_i \mathbf{x}_i A (A'^T A) = \sum_{i=0}^{m-1} \alpha_i \mathbf{x}_i (AA'^T) A = \sum_{i=0}^{m-1} \alpha_i \mathbf{x}_i A = \mathbf{F}.$$

On the other hand, for an $\mathbb{F}_{q^r}$-linear subspace $J \subseteq \mathbb{F}_{q^{rn}}$, define the $\mathbb{F}_{q^{rn}}$-linear subspace of $\mathbb{F}_{q^{rn}}^w$ given by

$$V(J) = \langle \{(\beta, \beta^{[r]}, \beta^{[2r]}, \ldots, \beta^{[(n-1)r]}) A^T \mid \beta \in J\} \rangle_{\mathbb{F}_{q^{rn}}} \subseteq \mathbb{F}_{q^{rn}}^w.$$

We will prove that $\dim_{\mathbb{F}_{q^{rn}}}(V(I)) = \dim_{\mathbb{F}_{q^r}}(I)$, and hence it will follow that $w \geq \dim_{\mathbb{F}_{q^r}}(I)$.

By definition, there exists a sequence $I_0, I_1, I_2, \ldots \subseteq \mathbb{F}_{q^{rn}}$ of $\mathbb{F}_{q^r}$-linear subspaces that is independent with respect to S and $I = I_i$, for some i. We will prove by induction on i that $\dim_{\mathbb{F}_{q^{rn}}}(V(I_i)) = \dim_{\mathbb{F}_{q^r}}(I_i)$.

For $i = 0$, we have that $I_0 = \{0\}$ and $V(I_0) = \{\mathbf{0}\}$, and the statement is true.

Fix $i > 0$ and assume that it is true for all $0 \leq j < i$. The space I_i may be obtained in two different ways, according to Definition E.25:

First, assume that $I_i = I_j \oplus \langle \beta \rangle$, with $0 \leq j < i$, $I_j \subseteq S$ and $\beta \notin S$. Therefore, $\dim_{\mathbb{F}_{q^r}}(I_i) = \dim_{\mathbb{F}_{q^r}}(I_j) + 1$. It follows that $\dim_{\mathbb{F}_{q^{rn}}}(V(I_i)) \leq \dim_{\mathbb{F}_{q^{rn}}}(V(I_j)) + 1$. Assume that $\dim_{\mathbb{F}_{q^{rn}}}(V(I_i)) = \dim_{\mathbb{F}_{q^{rn}}}(V(I_j))$. This means that

$$(\beta, \beta^{[r]}, \beta^{[2r]}, \ldots, \beta^{[(n-1)r]})A^T \in V(I_j).$$

On the other hand, for every $\gamma \in S$, it holds that

$$0 = F(\gamma) = \mathbf{F}(\gamma, \gamma^{[r]}, \ldots, \gamma^{[(n-1)r]})^T = (\mathbf{F}A'^T)(A(\gamma, \gamma^{[r]}, \ldots, \gamma^{[(n-1)r]})^T).$$

Since $(\beta, \beta^{[r]}, \beta^{[2r]}, \ldots, \beta^{[(n-1)r]})A^T$ is a linear combination (over $\mathbb{F}_{q^{rn}}$) of vectors in $V(I_j)$, it follows that

$$0 = (\mathbf{F}A'^T)(A(\beta, \beta^{[r]}, \ldots, \beta^{[(n-1)r]})^T) = \mathbf{F}(\beta, \beta^{[r]}, \ldots, \beta^{[(n-1)r]})^T = F(\beta),$$

which means that $\beta \in S$, a contradiction. Thus $\dim_{\mathbb{F}_{q^{rn}}}(V(I_i)) = \dim_{\mathbb{F}_{q^{rn}}}(V(I_j))$ $+1$ and the result holds in this case.

Now assume that $I_i = I_j^{[br]}$, for some integer $b \geq 0$ and $0 \leq j < i$. Since rising to the power q^r in $\mathbb{F}_{q^{rn}}$ is an $\mathbb{F}_{q^r}$-linear vector space automorphism, we have that $\dim_{\mathbb{F}_{q^r}}(I_i) = \dim_{\mathbb{F}_{q^r}}(I_j)$. On the other hand, rising to the power q^r in $\mathbb{F}_{q^{rn}}^w$ is an $\mathbb{F}_{q^{rn}}$-semilinear vector space automorphism, which also preserve dimensions over $\mathbb{F}_{q^{rn}}$. Since $V(I_i) = V(I_j)^{[br]}$, we have that $\dim_{\mathbb{F}_{q^{rn}}}(V(I_i)) = \dim_{\mathbb{F}_{q^{rn}}}(V(I_j))$ and the result holds also in this case. □

Future research on other possible generalizations of the rank-BCH bound could be trying to obtain rank versions of the bounds in [6, 17], to cite some. We next give a toy example to illustrate the previous bound:

Example E.26. Let $r = 1$, $n = m = 2$. Take a vector $\mathbf{F} = (F_0, F_1) \in \mathbb{F}_{q^2}^2$. We next see that the previous bound gives the exact value of $\mathrm{wt_R}(\mathbf{F})$. Observe that $\mathrm{wt_R}(\gamma \mathbf{F}) = \mathrm{wt_R}(\mathbf{F})$, for all non-zero $\gamma \in \mathbb{F}_{q^2}$, and hence we may assume $\mathbf{F} = (1, \alpha)$ for some $\alpha \in \mathbb{F}_{q^2}$. Let $S = Z(F) \subseteq \mathbb{F}_{q^2}$, for $F(x) = x^{[1]} + \alpha x$, and distinguish two cases:

1. $\mathrm{wt_R}(\mathbf{F}) = 1$, that is, $\alpha \in \mathbb{F}_q$: We have that $S = \{\mathbf{0}\}$ if $\alpha = 0$, and $S = \langle \beta \rangle$, for some non-zero $\beta \in \mathbb{F}_{q^2}$ if $\alpha \neq 0$. We may start constructing an independent sequence by $I_1 = \langle \gamma \rangle$, for some $\gamma \in \mathbb{F}_{q^2} \setminus S$. We see that these (and $I_0 = \{0\}$) are all subspaces independent with respect to S, and hence we may only construct an independent space of dimension 1.

2. $\mathrm{wt_R}(\mathbf{F}) = 2$, that is, $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$: In this case, $S = \langle \beta \rangle$, for some $\beta \in \mathbb{F}_{q^2}$. Then β and β^q are linearly independent over $\mathbb{F}_q$ since $\beta^q + \alpha\beta = 0$ and $\alpha \notin \mathbb{F}_q$.

   Define $I_1 = \langle \beta^q \rangle$, then $I_2 = I_1^q = \langle \beta \rangle$ and finally $I_3 = I_2 \oplus \langle \beta^q \rangle = \langle \beta, \beta^q \rangle$. It holds that $\dim(I_3) = 2$, hence the previous bound is an equality: $2 = \mathrm{wt_R}(\mathbf{F}) \geq \dim(I_3) = 2$.

As a consequence of the previous theorem, we may give the following bound, analogous to the Hartmann-Tzeng bound as it appears in [21, Theorem 2]:

Corollary E.27 (Rank-HT bound). *Take integers $c > 0$, $\delta > 0$ and $s \geq 0$, with $\delta + s \leq \min\{m, n\}$ and $d = \gcd(c, n) < \delta$, and let $\alpha \in \mathbb{F}_{q^{rn}}$ be such that $A = \{\alpha^{[(i+jc)r]} \mid 0 \leq i \leq \delta - 2, 0 \leq j \leq s\}$ is a linearly independent (over $\mathbb{F}_{q^r}$) set of vectors, not necessarily pairwise distinct.*

If $F \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$ satisfies that $A \subseteq T = Z(F)$, then $\mathrm{wt_R}(F) \geq \delta + s$ (recall (E.4)). In particular, if $C = \rho_r^{-1}(T)$, with ρ_r as in Definition E.4, then

$$d_R(C) \geq \delta + s.$$

Proof. First, since $\delta + s \leq n$, we have that $ds < \delta s \leq n$, and n/d is the order of c modulo n. Hence, the elements jcr, for $j = 0, 1, 2, \ldots, s$, are all distinct modulo rn.

On the other hand, we may assume that A is maximal with the given structure. That is, there exists $0 \leq i \leq \delta - 2$ with $\alpha^{[(i+(s+1)c)r]} \notin T$ and there exists $0 \leq j \leq s$ such that $\alpha^{[(\delta-1+jc)r]} \notin T$. From the proof, we will see that we may assume for simplicity that $j = 0$, and by repeatedly raising to the power q^r, we will also see that we may assume that $i = \delta - 2$.

We will now define a suitable sequence $I_0, I_1, I_2, \ldots \subseteq \mathbb{F}_{q^{rn}}$ of $\mathbb{F}_{q^r}$-linear spaces independent with respect to $S = T$, and with $\dim_{\mathbb{F}_{q^r}}(I_i) \geq \delta + s$ for some $i \geq 0$. We start by $I_0 = \{\mathbf{0}\}$, and $I_{2i+1} = I_{2i} \oplus \langle \alpha^{[(\delta-2+(s+1)c)r]} \rangle$ and $I_{2i+2} = I_{2i+1}^{[(n-c)r]}$, for $i = 0, 1, 2, \ldots, s$.

We see by induction that $J_1 = I_{2s+2}$ is generated by the set

$$\{\alpha^{[(\delta-2+jc)r]} \mid 0 \leq j \leq s\}.$$

Next, define $J_{2i+1} = J_{2i} \oplus \langle \alpha^{[(\delta-1)r]} \rangle$ and $J_{2i} = J_{2i-1}^{[(n-1)r]}$, for $i = 1, 2, \ldots, \delta - 1$.

Finally, again by induction we see that $J_{2\delta-1}$ is generated by the set

$$\{\alpha^{[ir]} \mid 0 \leq i \leq \delta - 1\} \cup \{\alpha^{[jcr]} \mid 1 \leq j \leq s\}, \tag{E.6}$$

whose elements are all distinct by the first two paragraphs in the proof: First, these two sets are disjoint. If $\alpha^{[jcr]} = \alpha^{[ir]}$, for some $1 \leq i \leq \delta - 1$ and $1 \leq j \leq s$, then by considering $jc, jc+1, \ldots, jc+\delta-2$, we see that $\alpha^{[(\delta-1)r]} \in T$, a contradiction. Now, if two elements in the set on the left are equal, then we see again that $\alpha^{[(\delta-1)r]} \in T$. Finally, if two elements in the set on the right are equal, we may now see that $\alpha^{[(\delta-2+(s+1)c)r]} \in T$, which is again a contradiction.

Since there are $\delta + s$ elements in the set (E.6) and they are linearly independent by hypothesis, the result follows from the previous theorem. □

By taking $s = 0$ and $c = 1$, we see that the rank version of the BCH bound obtained in [3, Proposition 1] is a corollary of the previous bound:

Corollary E.28 (Rank-BCH bound [3, Proposition 1]). *Take an integer $\delta > 0$, with $\delta \leq \min\{m, n\}$, and let $\alpha \in \mathbb{F}_{q^{rn}}$ be such that $\alpha, \alpha^{[r]}, \alpha^{[2r]}, \ldots, \alpha^{[(\delta-2)r]}$ are linearly independent over $\mathbb{F}_{q^r}$.*

If $F \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$ satisfies that $T = Z(F)$ contains the previous elements, then $\mathrm{wt_R}(F) \geq \delta$ (recall (E.4)). In particular, if $C = \rho_r^{-1}(T)$, with ρ_r as in Definition E.4, then

$$d_R(C) \geq \delta.$$

Thanks to the lattice study of the previous two sections and, in particular, thanks to Proposition E.14, we can see that it is not difficult to find examples where the rank-HT bound beats the rank-BCH bound, as in the classical case:

Example E.29. Consider $r = 1$, $n = 2m$ and $m = 31$, and take a normal basis $\alpha, \alpha^{[1]}, \ldots, \alpha^{[61]}$ of $\mathbb{F}_{q^{62}}$ over $\mathbb{F}_q$. Take $c = 5$, $\delta = 4$ and $s = 3$, and the q-root space

$$T = (C_q(\alpha) \oplus C_q(\alpha^{[1]}) \oplus C_q(\alpha^{[2]})) \oplus (C_q(\alpha^{[5]}) \oplus C_q(\alpha^{[6]}) \oplus C_q(\alpha^{[7]}))$$

$$\oplus (C_q(\alpha^{[10]}) \oplus C_q(\alpha^{[11]}) \oplus C_q(\alpha^{[12]})) \oplus (C_q(\alpha^{[15]}) \oplus C_q(\alpha^{[16]}) \oplus C_q(\alpha^{[17]})).$$

By Proposition E.14, we have that $C_q(\alpha^{[i]})$ has $\{\alpha^{[i]}, \alpha^{[31+i]}\}$ as a basis, and hence has dimension 2. Therefore, the code $C = \rho_r^{-1}(T)$ has dimension $62 - 24 = 38$. The rank-BCH bound states that $d_R(C) \geq 4$, whereas the rank-HT bound improves it giving $d_R(C) \geq 7$.

5.2 Rank-BCH codes from normal bases are generalized Gabidulin codes

As a consequence of the bound in Corollary E.28, a family of q^r-cyclic codes with a designed minimum rank distance is defined in [3, Section 3], in analogy with classical BCH codes. By means of difference equations and Casoratian determinants, rank-BCH codes are defined in [3] as q^r-cyclic codes with prescribed minimum rank distance and generator polynomial of minimal degree.

We will give an alternative description in terms of q^r-cyclotomic spaces, which will allow us to prove that, when $m = n$ and r and n are coprime, rank-BCH codes from normal bases are generalized Gabidulin codes, as in Subsection 2.2, which are MRD.

Definition E.30. Given $1 \leq \delta \leq m$, we say that the q^r-cyclic code $C(x)$ over $\mathbb{F}_{q^m}$ is a rank-BCH code of designed minimum rank distance δ if the corresponding q^r-root space T over $\mathbb{F}_{q^m}$ (see Definition E.4) is

$$T = C_{q^r}(\alpha) + C_{q^r}(\alpha^{[r]}) + C_{q^r}(\alpha^{[2r]}) + \cdots + C_{q^r}(\alpha^{[(\delta-2)r]}),$$

where $\alpha \in \mathbb{F}_{q^{rn}}$ and $\alpha, \alpha^{[r]}, \alpha^{[2r]}, \ldots, \alpha^{[(\delta-2)r]}$ are linearly independent over $\mathbb{F}_{q^r}$.

The following result follows immediately from Corollary E.28:

Proposition E.31. *The rank-BCH code $C(x)$ in the previous definition satisfies that*

$$d_R(C) \geq \delta.$$

If $m = n$ and r and n are coprime, the Gabidulin codes $\mathrm{Gab}_{k,r}(\boldsymbol{\beta})$ defined using a normal basis (see Subsection 2.2) are rank-BCH codes also using normal bases, and viceversa, and all of them are MRD codes. Hence the family of rank-BCH codes include MRD codes. We will use [12, Lemma 2], which is the following:

Lemma E.32 ([12, Lemma 2]). *If r and n are coprime and $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{F}_{q^n}$ are linearly independent over $\mathbb{F}_q$, then they are also linearly independent over $\mathbb{F}_{q^r}$, considered as elements in $\mathbb{F}_{q^{rn}}$.*

Theorem E.6. *Assume $m = n$ and r and n are coprime. Take a normal basis $\alpha, \alpha^{[1]}, \ldots, \alpha^{[n-1]} \in \mathbb{F}_{q^n} = \mathbb{F}_{q^m}$ and $1 \leq \delta \leq n$. Then the corresponding rank-BCH code $C(x)$, as in Definition E.30, is the generalized Gabidulin code $\mathrm{Gab}_{k,r}(\boldsymbol{\alpha})$ (see Subsection 2.2), where $\boldsymbol{\alpha} = (\alpha, \alpha^{[r]}, \ldots, \alpha^{[(n-1)r]})$ and $k = n - \delta + 1$.*

Proof. Since $m = n$, we have that $\alpha \in \mathbb{F}_{q^m}$, and hence $C_{q^r}(\alpha^{[i]}) = \langle \alpha^{[i]} \rangle_{\mathbb{F}_{q^r}}$, for all $i = 0, 1, 2, \ldots, n-1$. Therefore, the q^r-root space T corresponding to

$C(x)$ is $T = \langle \alpha, \alpha^{[r]}, \ldots, \alpha^{[(\delta-2)r]} \rangle_{\mathbb{F}_{q^r}}$, whose dimension over $\mathbb{F}_{q^r}$ is $\delta - 1$ by the previous lemma.

Hence, by item 4 in Theorem E.2, the matrix $\mathcal{M}(\alpha, \alpha^{[r]}, \ldots, \alpha^{[(\delta-2)r]})$ is a parity check matrix of C over $\mathbb{F}_{q^m}$. However, this is also the parity check matrix of the above mentioned Gabidulin code of dimension k, $\mathcal{H}_{k,r}(\boldsymbol{\alpha})$, if $k = n - \delta + 1$ (see Subsection 2.2). Therefore both are equal and the theorem follows. □

6 General $\mathbb{F}_q$-linear skew cyclic codes: Connecting Hamming-metric cyclic codes and rank-metric skew cyclic codes

To conclude, we will give some first steps in the general study of $\mathbb{F}_q$-linear q^r-cyclic codes in $\mathbb{F}_{q^m}^n$.

Its main interest for our purposes is that they include both the family of skew cyclic codes in the rank metric, which are the main topic of this paper, and the classical family of cyclic codes in the Hamming metric, as we will prove in the first subsection.

Moreover, as we will see in the second subsection, some $\mathbb{F}_{q^m}$-linear q^r-cyclic codes in the rank metric with $m = n$ actually are obtained from cyclic codes in the Hamming metric via $\mathbb{F}_q$-linear q^r-cyclic codes, which will allow us to compare their parameters and give a negative criterion of MRD skew cyclic codes in terms of MDS cyclic codes.

6.1 Hamming-metric cyclic codes are rank-metric skew cyclic codes

Assume in this subsection that $m = n$, fix a basis $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and define the map $E : \mathbb{F}_q^n \longrightarrow \mathbb{F}_{q^n}^n$ by

$$E(c_0, c_1, \ldots, c_{n-1}) = (c_0\alpha_0, c_1\alpha_1, \ldots, c_{n-1}\alpha_{n-1}). \tag{E.7}$$

This map is one to one, $\mathbb{F}_q$-linear and $\mathrm{wt_H}(\mathbf{c}) = \mathrm{wt_R}(E(\mathbf{c}))$, where $\mathrm{wt_H}(\mathbf{c})$ denotes the Hamming weight of the vector $\mathbf{c}$. Therefore, the codes $C \subseteq \mathbb{F}_q^n$ and $E(C) \subseteq \mathbb{F}_{q^n}^n$ behave equally, where we consider the Hamming metric for C and the rank metric for $E(C)$.

Assume also in this subsection that n and r are coprime and $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ satisfies that $\alpha_i = \alpha^{[ir]}$, for $i = 0, 1, 2, \ldots, n-1$, where $\alpha, \alpha^{[1]}, \ldots, \alpha^{[n-1]}$ is a normal basis. In this case, classical cyclic codes correspond to q^r-cyclic codes.

Theorem E.7. *With the assumptions as in the previous paragraph, an arbitrary (linear or non-linear) code $C \subseteq \mathbb{F}_q^n$ is cyclic if, and only if, the code $E(C) \subseteq \mathbb{F}_{q^n}^n$ is q^r-cyclic.*

Moreover, C is $\mathbb{F}_q$-linear if, and only if, so is $E(C)$, and the Hamming-metric behaviour of C is the same as the rank-metric behaviour of $E(C)$, since $\mathrm{wt_H}(\mathbf{c}) = \mathrm{wt_R}(E(\mathbf{c}))$, *for all* $\mathbf{c} \in \mathbb{F}_q^n$.

Proof. Let $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$ and $E(\mathbf{c}) = (d_0, d_1, \ldots, d_{n-1}) \in E(C)$. Then

$$E(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) = (c_{n-1}\alpha, c_0\alpha^{[r]}, \ldots, c_{n-2}\alpha^{[(n-1)r]})$$

$$= ((c_{n-1}\alpha^{[(n-1)r]})^{q^r}, (c_0\alpha)^{q^r}, \ldots, (c_{n-2}\alpha^{[(n-2)r]})^{q^r}) = (d_{n-1}^{q^r}, d_0^{q^r}, \ldots, d_{n-2}^{q^r}),$$

and the result follows, since the linearity claim is trivial from the linearity of E. □

6.2 MRD skew cyclic codes and MDS cyclic codes

We will now relate MRD $\mathbb{F}_{q^n}$-linear q^r-cyclic codes in $\mathbb{F}_{q^n}^n$ with classical MDS $\mathbb{F}_q$-linear cyclic codes in $\mathbb{F}_q^n$. We first need some properties of $\mathbb{F}_q$-linear q^r-cyclic codes. The following lemma is proven in the same way as Lemma E.2:

Lemma E.33. *A code $C \subseteq \mathbb{F}_{q^m}^n$ is $\mathbb{F}_q$-linear and q^r-cyclic if, and only if, $C(x)$ satisfies that $G - H \in C(x)$ and $F \otimes G \in C(x)$, for all $F(x) \in \mathcal{L}_{q^r}\mathbb{F}_q[x]$ and all $G, H \in C(x)$.*

Definition E.34. A subset $C(x) \subseteq \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$ satisfying the conditions in the previous lemma is called an $\mathbb{F}_q$-left ideal.

By Theorem E.7 and Lemma E.33, classical cyclic codes for the Hamming metric can be seen as $\mathbb{F}_q$-left ideals in $\mathcal{L}_{q^r}\mathbb{F}_{q^n}[x]/(x^{[rn]} - x)$ for the rank metric, provided that n and r are coprime.

We observe that $\mathbb{F}_q$-left ideals are finitely generated. That is, every $\mathbb{F}_q$-left ideal is of the form $C(x) = (G_1, G_2, \ldots, G_t)_{\mathbb{F}_q}$, where we define

$$(G_1, G_2, \ldots, G_t)_{\mathbb{F}_q} = \left\{ \sum_{i=1}^{t} Q_i \otimes G_i \mid Q_i(x) \in \mathcal{L}_{q^r}\mathbb{F}_q[x] \right\}.$$

However, not all $\mathbb{F}_q$-left ideals are principal, that is, of the form $(G)_{\mathbb{F}_q}$, for some $G(x) \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$. The following proposition relates the dimension of an $\mathbb{F}_q$-left ideal and its number of generators. We also describe generators of the vector space C over $\mathbb{F}_q$ as in Theorem E.1:

Proposition E.35. *Let $C(x)$ be an $\mathbb{F}_q$-left ideal with $C(x) = (G_1, G_2, \ldots, G_t)_{\mathbb{F}_q}$. It holds that:*

1. *$C(x)$ is generated by $x^{[j]} \otimes G_i$ as an $\mathbb{F}_q$-linear vector space, for $j = 0, 1, \ldots, n-1$ and $i = 1, 2, \ldots, t$. In particular, a basis of C over $\mathbb{F}_q$ may be obtained from the set of vectors*
$$(G_{i,n-j}^{[jr]}, G_{i,n-j+1}^{[jr]}, \ldots, G_{i,n-j-1}^{[jr]}),$$
for the previous i and j, where $G_i(x) = G_{i,0}x + G_{i,1}x^{[r]} + \cdots + G_{i,n-1}x^{[n-1]}$.
2. *The dimension of C (over $\mathbb{F}_q$) satisfies $\dim(C(x)) \leq tn$.*
3. *There exist $F_1, F_2, \ldots, F_{mn} \in C(x)$ such that $C(x) = (F_1, F_2, \ldots, F_{mn})_{\mathbb{F}_q}$.*

Proof. The first item follows from the fact that $x^{[j]} \otimes G_j$ corresponds to the vector $(G_{i,n-j}^{[jr]}, G_{i,n-j+1}^{[jr]}, \ldots, G_{i,n-j-1}^{[jr]})$. The second item follows from this first item, and the third item follows from the fact that $\dim(C) \leq mn$. □

Now we see that classical cyclic codes actually correspond to principal $\mathbb{F}_q$-left ideals. For that purpose, let the assumptions be as in Theorem E.7 and define the operators $L, E : \mathbb{F}_q[x]/(x^n - 1) \longrightarrow \mathcal{L}_{q^r}\mathbb{F}_{q^n}[x]/(x^{[rn]} - x)$ as

$$L(f_0 + f_1x + \cdots + f_{n-1}x^{n-1}) = f_0x + f_1x^{[r]} + \cdots + f_{n-1}x^{[(n-1)r]}, \text{ and}$$

$$E(g_0 + g_1x + \cdots + g_{n-1}x^{n-1}) = g_0\alpha x + g_1\alpha^{[r]}x^{[r]} + \cdots + g_{n-1}\alpha^{[(n-1)r]}x^{[(n-1)r]},$$

where $f_i, g_i \in \mathbb{F}_q$, for $i = 0, 1, \ldots, n-1$.

Proposition E.36. *With the assumptions as in Theorem E.7, for all $f(x), g(x) \in \mathbb{F}_q[x]\ /(x^n - 1)$, it holds that*

$$L(f(x)) \otimes E(g(x)) = E(f(x)g(x)). \tag{E.8}$$

In particular, if $[g(x)]$ denotes the ideal in $\mathbb{F}_q[x]/(x^n - 1)$ generated by $g(x)$, then

$$E([g(x)]) = (E(g(x)))_{\mathbb{F}_q}. \tag{E.9}$$

This means that, if $C \subseteq \mathbb{F}_q^n$ is cyclic, then $E(C)(x)$ is a principal $\mathbb{F}_q$-left ideal generated by $E(g(x))$ if $g(x)$ generates the ideal in $\mathbb{F}_q[x]/(x^n - 1)$ corresponding to C.

Proof. If $f(x) = f_0 + f_1x + \cdots + f_{n-1}x^{n-1}$ and $g(x) = g_0 + g_1x + \cdots + g_{n-1}x^{n-1}$, then

$$L(f(x)) \otimes E(g(x)) = \sum_{i=0}^{n-1} \left(\sum_{j=0}^{n-1} f_{i-j}g_j(\alpha^{[jr]})^{[(i-j)r]} \right) x^{[ir]}$$

$$= \sum_{i=0}^{n-1} \left(\sum_{j=0}^{n-1} f_{i-j}g_j \right) \alpha^{[ir]}x^{[ir]} = E(f(x)g(x)),$$

and Equation (E.8) follows. The second part (E.9) follows immediately from (E.8). □

On the other hand, if $C(x) = (G_1, G_2, \ldots, G_t)_{\mathbb{F}_q}$, then the $\mathbb{F}_{q^m}$-linear code generated by $C(x)$ is

$$C(x)_{\mathbb{F}_{q^m}} = (G_1, G_2, \ldots, G_t) = (D),$$

where D is the greatest common divisor of $G_1, G_2, \ldots, G_t$ in the quotient ring $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$. Therefore, $d_R(C(x)) \geq d_R((D))$, and the q^r-root space $T = Z(D) = Z(G_1) \cap Z(G_2) \cap \ldots \cap Z(G_t)$ may be used to give bounds on the minimum rank distance of $C(x)$, using for example the bounds in Section 5.

Now we come to the main result in this subsection, where we see that the $\mathbb{F}_{q^n}$-linear code generated by a classical cyclic code is again principal, with the same minimal generator and corresponding dimension, but its minimum rank distance is lower than the minimum Hamming distance of the original cyclic code. In particular, this gives a negative criterion for MRD skew cyclic codes in terms of MDS cyclic codes.

Theorem E.8. *With the assumptions as in Theorem E.7, if $g(x) \in \mathbb{F}_q[x]/(x^n - 1)$ is the minimal generator of the $\mathbb{F}_q$-linear cyclic code $C \subsetneq \mathbb{F}_q^n$ and $\widehat{C} = \langle E(C) \rangle_{\mathbb{F}_{q^n}}$, then $\widehat{C}$ is the $\mathbb{F}_{q^n}$-linear q^r-cyclic code corresponding to*

$$\widehat{C}(x) = (E(g(x))).$$

Moreover, $E(g(x))$ is the minimal generator of $\widehat{C}(x)$, and:

1. $d_R(\widehat{C}) \leq d_H(C)$, $\dim_{\mathbb{F}_{q^n}}(\widehat{C}) = \dim_{\mathbb{F}_q}(C)$.

2. *If $\widehat{C}$ is MRD, then C is MDS.*

Proof. It is well-known that the shifted vectors in $\mathbb{F}_q^n$,

$$(g_0, g_1, \ldots, g_{n-k}, 0, \ldots, 0), (0, g_0, g_1, \ldots, g_{n-k}, 0, \ldots, 0), \ldots,$$
$$(0, \ldots, 0, g_0, g_1, \ldots, g_{n-k})$$

constitute a basis of C, where $g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$ and $g_{n-k} \neq 0$. By Proposition E.35 and Proposition E.36, the q^r-shifted vectors in $\mathbb{F}_{q^n}^n$,

$$(g_0\alpha, g_1\alpha^{[r]}, \ldots, g_{n-k}\alpha^{[(n-k)r]}, 0, \ldots, 0),$$
$$(0, g_0\alpha^{[r]}, g_1\alpha^{[2r]}, \ldots, g_{n-k}\alpha^{[(n-k+1)r]}, 0, \ldots, 0), \ldots$$
$$(0, \ldots, 0, g_0\alpha^{[(n-k-1)r]}, g_1\alpha^{[(n-k)r]}, \ldots, g_{n-k}\alpha^{[(n-1)r]})$$

generate $\widehat{C}$ as an $\mathbb{F}_{q^n}$-linear vector space. Since $g_{n-k} \neq 0$, it follows that these vectors are linearly independent over $\mathbb{F}_{q^n}$. Hence the result follows from Theorem E.1 and the fact that $d_H(C) = d_R(E(C)) \geq d_R(\langle E(C) \rangle_{\mathbb{F}_{q^n}}) = d_R(\widehat{C})$. □

Example E.37. Consider the repetition cyclic code $C \subseteq \mathbb{F}_q^n$ generated by $(1,1,\ldots,1)$ and assume $r = 1$. Then $E(C)$ is the $\mathbb{F}_q$-linear code generated by $(\alpha, \alpha^{[1]}, \ldots, \alpha^{[n-1]})$, and hence the $\mathbb{F}_{q^n}$-linear code generated by $E(C)$ is $\widehat{C}$, also generated by the same vector.

It holds that $\dim_{\mathbb{F}_q}(C) = 1$, $d_H(C) = n$ and C is MDS. On the other hand, $\dim_{\mathbb{F}_{q^n}}(\widehat{C}) = 1$, $d_R(\widehat{C}) = n$ and $\widehat{C}$ is MRD.

Example E.38. Assume that $r = 1$ and n is even, and consider the cyclic code $C \subseteq \mathbb{F}_q^n$ generated by $(1,0,1,0,\ldots,0)$ and $(0,1,0,1,\ldots,1)$. Then $\widehat{C}$ is the $\mathbb{F}_{q^n}$-linear code generated by $(\alpha, 0, \alpha^{[2]}, 0, \ldots, 0)$ and $(0, \alpha^{[1]}, 0, \alpha^{[3]}, \ldots, \alpha^{[n-1]})$.

It holds that $\dim_{\mathbb{F}_q}(C) = 2$, $d_H(C) = n/2$. On the other hand, $\dim_{\mathbb{F}_{q^n}}(\widehat{C})$ $= 2$, $d_R(\widehat{C}) = n/2$. Hence both have the same parameters and none reach the Singleton bounds for the corresponding metrics. Moreover, the minimal generator of C is $g(x) = 1 + x^2 + x^4 + \cdots + x^{n-2}$, whereas the minimal generator of $\widehat{C}$ is $E(g(x)) = \alpha x + \alpha^{[2]} x^{[2]} + \alpha^{[4]} x^{[4]} + \cdots + \alpha^{[n-2]} x^{[n-2]}$.

Acknowledgement

The author wishes to thank the anonymous reviewers for their very helpful comments and suggestions. The author also wishes to thank Olav Geil, Ruud Pellikaan and Diego Ruano for fruitful discussions and careful reading of the manuscript. Finally, the author gratefully acknowledges the support from The Danish Council for Independent Research (Grant No. DFF-4002-00367).

References

[1] D. Boucher, W. Geiselmann, and F. Ulmer, "Skew-cyclic codes," *Applicable Algebra in Engineering, Communication and Computing*, vol. 18, no. 4, pp. 379–389, 2007.

[2] D. Boucher and F. Ulmer, "Coding with skew polynomial rings," *Journal of Symbolic Computation*, vol. 44, no. 12, pp. 1644 – 1656, 2009, gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics.

[3] L. Chaussade, P. Loidreau, and F. Ulmer, "Skew codes of prescribed distance or rank," *Designs, Codes and Cryptography*, vol. 50, no. 3, pp. 267–284, 2009.

[4] P. Delsarte, "On subfield subcodes of modified reed-solomon codes (corresp.)," *IEEE Transactions Information Theory*, vol. 21, no. 5, pp. 575–576, Sep. 2006.

[5] J. Ducoat and F. Oggier, "Rank weight hierarchy of some classes of cyclic codes," in *Information Theory Workshop (ITW), 2014 IEEE*, Nov 2014, pp. 142–146.

[6] I. M. Duursma and R. Pellikaan, "A symmetric Roos bound for linear codes," *Journal of Combinatorial Theory, Series A*, vol. 113, no. 8, pp. 1677 – 1688, 2006, special Issue in Honor of Jacobus H. van Lint.

[7] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems Informormation Transmission*, vol. 21, 1985.

[8] ——, "Rank q-cyclic and pseudo-q-cyclic codes," in *IEEE International Symposium on Information Theory, 2009. ISIT 2009.*, June 2009, pp. 2799–2802.

[9] F. Gursoy, I. Siap, and B. Yildiz, "Construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$," *Advances in Mathematics of Communications*, vol. 8, no. 3, pp. 313–322, 2014.

[10] C. Hartmann and K. Tzeng, "Generalizations of the BCH bound," *Information and Control*, vol. 20, no. 5, pp. 489 – 498, 1972.

[11] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.

[12] A. Kshevetskiy and E. M. Gabidulin, "The new construction of rank codes," in *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.*, Sept 2005, pp. 2105–2108.

[13] R. Lidl and H. Niederreiter, *Finite Fields*. Amsterdam: Encyclopedia of Mathematics and its Applications. Addison-Wesley, 1983, vol. 20.

[14] U. Martínez-Peñas, "On the similarities between generalized rank and Hamming weights and their applications to network coding," *IEEE Trans. Inform. Theory*, vol. 62, no. 7, pp. 4081–4095, 2016.

[15] O. Ore, "On a special class of polynomials," *Trans. Amer. Math. Soc.*, vol. 35, no. 3, pp. 559–584, 1933.

[16] ——, "Theory of non-commutative polynomials," *Ann. of Math. (2)*, vol. 34, no. 3, pp. 480–508, 1933.

[17] R. Pellikaan, "The shift bound for cyclic, Reed-Muller and geometric Goppa codes," in *Arithmetic, Geometry and Coding Theory*, vol. 4. Luminy, 1996, pp. 155–174.

[18] D. Silva and F. R. Kschischang, "On metrics for error correction in network coding," *IEEE Trans. Inform. Theory*, vol. 55, no. 12, pp. 5479–5490, 2009.

[19] U. Sripati and B. S. Rajan, “On the rank distance of cyclic codes,” in *Information Theory, 2003. Proceedings. IEEE International Symposium on*, June 2003, pp. 72–.

[20] H. Stichtenoth, “On the dimension of subfield subcodes,” *IEEE Transactions Information Theory*, vol. 36, no. 1, pp. 90–93, Jan 1990.

[21] J. van Lint and R. Wilson, “On the minimum distance of cyclic codes,” *IEEE Transactions on Information Theory*, vol. 32, no. 1, pp. 23–40, Jan 1986.

Paper F

Rank error-correcting pairs

Umberto Martínez-Peñas[1] and Ruud Pellikaan[2]

The paper has been published in
Designs, Codes and Cryptography Vol. 84, No. 1-2, pp. 261–281, 2017.

[1] Department of Mathematical Sciences, Aalborg University, Aalborg 9220, Denmark

[2] Department of Mathematics and Computing Science, Eindhoven University of Technology, The Netherlands

The layout has been revised.

Abstract

Error-correcting pairs were introduced as a general method of decoding linear codes with respect to the Hamming metric using coordinatewise products of vectors, and are used for many well-known families of codes. In this paper, we define new types of vector products, extending the coordinatewise product, some of which preserve symbolic products of linearized polynomials after evaluation and some of which coincide with usual products of matrices. Then we define rank error-correcting pairs for codes that are linear over the extension field and for codes that are linear over the base field, and relate both types. Bounds on the minimum rank distance of codes and MRD conditions are given. Finally we show that some well-known families of rank-metric codes admit rank error-correcting pairs, and show that the given algorithm generalizes the classical algorithm using error-correcting pairs for the Hamming metric.

Keywords: Decoding, error-correcting pairs, linearized polynomials, rank metric, vector products.

MSC: 15B33, 94B35, 94B65.

1 Introduction

Error-correcting pairs were introduced independently by Pellikaan in [19, 20] and by Kötter in [13]. These are pairs of linear codes satisfying some conditions with respect to the coordinatewise product and a given linear code, for which they define an error-correcting algorithm with respect to the Hamming metric in polynomial time.

Linear codes with an error-correcting pair include many well-known families, such as (generalized) Reed-Solomon codes, many cyclic codes (such as BCH codes), Goppa codes and algebraic geometry codes (see [6, 20, 21]).

Error-correcting codes with respect to the rank metric [8] have recently gained considerable attention due to their applications in network coding [25]. In the rank metric, maximum rank distance (MRD) Gabidulin codes, as defined in [8, 14], have been widely used, and decoding algorithms using linearized polynomials are given in [8, 14, 16]. A related construction, the so-called q-cyclic or skew cyclic codes, were introduced by Gabidulin in [8] for square matrices and generalized independently by himself in [9] and by Ulmer et al. in [1].

However, more general methods of decoding with respect to the rank metric are lacking, specially for codes that are linear over the base field instead of the extension field.

The contributions of this paper are organized as follows. In Section 3, we introduce some families of vector products that coincide with usual products of matrices for some sizes. One of these products preserves symbolic products of linearized polynomials after evaluation and is the unique product with this property for some particular sizes. In Section 4, we introduce the concept of rank error-correcting pair and give efficient decoding algorithms based on them. Subsection 4.1 treats linear codes over the extension field, and Subsection 4.2 treats linear codes over the base field. In Section 5, we prove that the latter type of rank error-correcting pairs generalize the former type. In Section 6, we derive bounds on the minimum rank distance and give MRD conditions based on rank error-correcting pairs. Finally, in Section 7, we study some families of codes that admit rank error-correcting pairs, showing that the given algorithm generalizes the classical algorithm using error-correcting pairs for the Hamming metric.

2 Preliminaries

2.1 Notation

Fix a prime power q and positive integers m and n, and fix from now on a basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ of $\mathbb{F}_{q^m}$ as a vector space over $\mathbb{F}_q$. $\mathbb{F}_{q^m}^n$ denotes the $\mathbb{F}_{q^m}$-linear vector space of row vectors over $\mathbb{F}_{q^m}$ with n components, and $\mathbb{F}_q^{m \times n}$ denotes the $\mathbb{F}_q$-linear vector space of $m \times n$ matrices over $\mathbb{F}_q$.

We will also use the following notation. Given a subset $\mathcal{A} \subseteq \mathbb{F}_{q^m}^n$, we denote by $\langle \mathcal{A} \rangle_{\mathbb{F}_q}$ and $\langle \mathcal{A} \rangle_{\mathbb{F}_{q^m}}$ the $\mathbb{F}_q$-linear and $\mathbb{F}_{q^m}$-linear vector spaces generated by $\mathcal{A}$, respectively. For an $\mathbb{F}_{q^m}$-linear (respectively $\mathbb{F}_q$-linear) code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ (respectively $\mathcal{C} \subseteq \mathbb{F}_q^n$), we denote its dimension over $\mathbb{F}_{q^m}$ (respectively over $\mathbb{F}_q$) by $\dim(\mathcal{C})$. If $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ or $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ is $\mathbb{F}_q$-linear, we denote its dimension over $\mathbb{F}_q$ by $\dim_{\mathbb{F}_q}(\mathcal{C})$.

2.2 Rank-metric codes

In the literature, it is usual to consider two types of rank-metric codes: $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$, and $\mathbb{F}_q$-linear codes in $\mathbb{F}_q^{m \times n}$.

We will use the following classical matrix representation of vectors in $\mathbb{F}_{q^m}^n$ to connect both types of codes. Let $\mathbf{c} \in \mathbb{F}_{q^m}^n$, there exist unique $\mathbf{c}_i \in \mathbb{F}_q^n$, for $i = 1, 2, \ldots, m$, such that $\mathbf{c} = \sum_{i=1}^m \alpha_i \mathbf{c}_i$. Let $\mathbf{c}_i = (c_{i,1}, c_{i,2}, \ldots, c_{i,n})$ or, equivalently, $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ and $c_j = \sum_{i=1}^m \alpha_i c_{i,j}$. Then we define the $m \times n$ matrix, with coefficients in $\mathbb{F}_q$,

$$M(\mathbf{c}) = (c_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n}. \tag{F.1}$$

The map $M : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^{m \times n}$ is an $\mathbb{F}_q$-linear vector space isomorphism. Unless it is necessary, we will not write subscripts for M regarding the values m, n, or the basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ (which of course change the map M).

By definition [8], the rank weight of $\mathbf{c}$ is $\mathrm{wt_R}(\mathbf{c}) = \mathrm{Rk}(M(\mathbf{c}))$, the rank of the matrix $M(\mathbf{c})$, for every $\mathbf{c} \in \mathbb{F}_{q^m}^n$. We also define the rank support of $\mathbf{c}$ as the row space of the matrix $M(\mathbf{c})$, that is, $\mathrm{RSupp}(\mathbf{c}) = \mathrm{Row}(M(\mathbf{c})) \subseteq \mathbb{F}_q^n$. We may identify any non-linear or $\mathbb{F}_q$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ with $M(\mathcal{C}) \subseteq \mathbb{F}_q^{m\times n}$ and write $d_R(\mathcal{C}) = d_R(M(\mathcal{C}))$ for their minimum rank distance [8].

2.3 Hamming-metric codes as rank-metric codes

We briefly discuss how to see Hamming-metric codes as rank-metric codes. We define the map $D : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^{n\times n}$ as follows. For every vector $\mathbf{c} \in \mathbb{F}_q^n$, define the matrix

$$D(\mathbf{c}) = \mathrm{diag}(\mathbf{c}) = (c_i\delta_{i,j})_{1\leq i\leq n, 1\leq j\leq n}, \tag{F.2}$$

that is, the diagonal $n \times n$ matrix with coefficients in $\mathbb{F}_q$ whose diagonal vector is $\mathbf{c}$. The map D is $\mathbb{F}_q$-linear and one to one. Moreover, the Hamming weight of a vector $\mathbf{c} \in \mathbb{F}_q^n$ is $\mathrm{wt}_{\mathrm{H}}(\mathbf{c}) = \mathrm{Rk}(D(\mathbf{c}))$.

This gives a way to represent error-correcting codes $\mathcal{C} \subseteq \mathbb{F}_q^n$ in the Hamming metric as error-correcting codes $D(\mathcal{C}) \subseteq \mathbb{F}_q^{n\times n}$ in the rank metric, where the Hamming weight distribution of $\mathcal{C}$ corresponds bijectively to the rank weight distribution of $D(\mathcal{C})$. In particular, the minimum Hamming distance of $\mathcal{C}$ satisfies $d_H(\mathcal{C}) = d_R(D(\mathcal{C}))$.

On the other hand, let $\phi : \mathcal{C}_1 \longrightarrow \mathcal{C}_2$ be an $\mathbb{F}_q$-linear Hamming-metric equivalence between $\mathbb{F}_q$-linear codes $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^n$. It is well-known that ϕ is a monomial map, that is, there exist $a_1, a_2, \ldots, a_n \in \mathbb{F}_q^*$ and a permutation σ with $\phi(\mathbf{c}) = (a_1c_{\sigma(1)}, a_2c_{\sigma(2)}, \ldots, a_nc_{\sigma(n)})$, for all $\mathbf{c} \in \mathcal{C}_1$. We may trivially extend this map to a rank-metric equivalence $\phi' : D(\mathcal{C}_1) \longrightarrow D(\mathcal{C}_2)$ by the same formula. Hence Hamming-metric equivalent codes correspond to rank-metric equivalent codes.

2.4 Error-correcting pairs for the Hamming metric

We conclude by defining error-correcting pairs (ECPs) for the Hamming metric, introduced independently by Pellikaan in [19, 20] and by Kötter in [13]. Define the coordinatewise product $*$ of vectors in $\mathbb{F}_q^n$ by

$$\mathbf{a} * \mathbf{b} = (a_1b_1, a_2b_2, \ldots, a_nb_n),$$

for all $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$. For two linear subspaces $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q^n$, we define the linear subspace $\mathcal{A} * \mathcal{B} = \langle \{\mathbf{a} * \mathbf{b} \mid \mathbf{a} \in \mathcal{A}, \mathbf{b} \in \mathcal{B}\} \rangle \subseteq \mathbb{F}_q^n$.

Definition F.1. Let $\mathcal{A}, \mathcal{B}, \mathcal{C} \subseteq \mathbb{F}_q^n$ be linear codes and t a positive integer. The pair $(\mathcal{A}, \mathcal{B})$ is called a t-error-correcting pair (t-ECP) for $\mathcal{C}$ if the following properties hold:

1. $\mathcal{A} * \mathcal{B} \subseteq \mathcal{C}^\perp$.

2. $\dim(\mathcal{A}) > t$.

3. $d_H(\mathcal{B}^\perp) > t$.

4. $d_H(\mathcal{A}) + d_H(\mathcal{C}) > n$.

In [19, 20] it is shown that, if $\mathcal{C}$ has a t-ECP, then it has a decoding algorithm with complexity $O(n^3)$ that can correct up to t errors in the Hamming metric (and therefore, $d_H(\mathcal{C}) \geq 2t+1$). This algorithm is analogous to the ones that we will describe in Subsections 4.1 and 4.2. Actually, as we will see in Subsection 7.1, the algorithm presented in Subsection 4.2 extends the classical algorithm for Hamming-metric codes.

3 Vector products for the rank metric

In this section, we define and give the basic properties of a family of products of vectors in $\mathbb{F}_{q^m}^n$, which will play the same role as the coordinatewise product $*$ for vectors in $\mathbb{F}_q^n$.

Definition F.2. We first define the product $\star : \mathbb{F}_{q^m}^m \times \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$ in the following way. For every $\mathbf{c} \in \mathbb{F}_{q^m}^m$ and every $\mathbf{d} \in \mathbb{F}_{q^m}^n$, we define

$$\mathbf{c} \star \mathbf{d} = \sum_{i=1}^m c_i \mathbf{d}_i,$$

where $\mathbf{d} = \sum_{i=1}^m \alpha_i \mathbf{d}_i$ and $\mathbf{d}_i \in \mathbb{F}_q^n$, for all $i = 1, 2, \ldots, m$, and $\mathbf{c} = (c_1, c_2, \ldots, c_m)$. Note that the second argument of $\star$ and its codomain are the same, whereas its first argument is different if $m \neq n$.

On the other hand, given a map $\varphi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^m$, we define the product $\star_\varphi : \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$ in the following way. For every $\mathbf{c}, \mathbf{d} \in \mathbb{F}_{q^m}^n$, we define

$$\mathbf{c} \star_\varphi \mathbf{d} = \varphi(\mathbf{c}) \star \mathbf{d} = \sum_{i=1}^m \varphi(\mathbf{c})_i \mathbf{d}_i,$$

where $\mathbf{d} = \sum_{i=1}^m \alpha_i \mathbf{d}_i$ and $\mathbf{d}_i \in \mathbb{F}_q^n$, for all $i = 1, 2, \ldots, m$, and $\varphi(\mathbf{c}) = (\varphi(\mathbf{c})_1, \varphi(\mathbf{c})_2, \ldots, \varphi(\mathbf{c})_m)$.

Remark F.3. *The following basic properties of the previous products hold:*

1. *The product $\star$ depends on the choice of the basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q^n$, whereas the coordinatewise product $*$ does not.*

2. *The product $\star$ is $\mathbb{F}_{q^m}$-linear in the first component and $\mathbb{F}_q$-linear in the second component.*

3. *If φ is $\mathbb{F}_q$-linear, then the product $\star_\varphi$ is $\mathbb{F}_q$-bilinear.*
4. *On the other hand, if φ is $\mathbb{F}_{q^m}$-linear, then the product $\star_\varphi$ is $\mathbb{F}_{q^m}$-linear in the first component and $\mathbb{F}_q$-linear in the second component.*

It is of interest to see if two maps give the same product:

Lemma F.4. *Given maps $\varphi, \psi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^m$, it holds that $\star_\varphi = \star_\psi$ if, and only if, $\varphi = \psi$.*

Proof. Fix i and take $\mathbf{d} \in \mathbb{F}_{q^m}^n$ such that $\mathbf{d}_i = \mathbf{e}_1$, the first vector in the canonical basis of $\mathbb{F}_q^n$ and $\mathbf{d}_j = \mathbf{0}$, for $j \neq i$. Since $\mathbf{c} \star_\varphi \mathbf{d} = \mathbf{c} \star_\psi \mathbf{d}$, it follows that $\varphi(\mathbf{c})_i = \psi(\mathbf{c})_i$. This is valid for an arbitrary i, hence $\varphi(\mathbf{c}) = \psi(\mathbf{c})$, for any $\mathbf{c} \in \mathbb{F}_{q^m}^n$, which implies that $\varphi = \psi$. The reverse implication is trivial. □

One of the most important properties of the coordinatewise product $*$ is that it preserves multiplications of polynomials after evaluation. We will define below a natural product that will preserve symbolic multiplications of linearized polynomials after evaluation.

Definition F.5 (q-linearized polynomials). A q-linearized polynomial over $\mathbb{F}_{q^m}$ is a polynomial of the form

$$F = a_0 x + a_1 x^{[1]} + \cdots + a_d x^{[d]},$$

where $a_0, a_1, \ldots, a_d \in \mathbb{F}_{q^m}$ and $[i] = q^i$, for all $i \geq 0$. We denote by $\mathcal{L}_q\mathbb{F}_{q^m}[x]$ the set of q-linearized polynomials over $\mathbb{F}_{q^m}$.

These polynomials induce $\mathbb{F}_q$-linear maps in any extension field of $\mathbb{F}_{q^m}$.

Definition F.6 (Evaluation map). For a vector $\mathbf{b} = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_{q^m}^n$, we will define the evaluation map

$$\mathrm{ev}_{\mathbf{b}} : \mathcal{L}_q\mathbb{F}_{q^m}[x] \longrightarrow \mathbb{F}_{q^m}^n$$

by $\mathrm{ev}_{\mathbf{b}}(F) = (F(b_1), F(b_2), \ldots, F(b_n))$, for all $F \in \mathcal{L}_q\mathbb{F}_{q^m}[x]$.

We start by the following interpolation lemma.

Lemma F.7. *If $n \leq m$, and $\mathbf{c} \in \mathbb{F}_{q^m}^n$, there exists a unique q-linearized polynomial $F \in \mathcal{L}_q\mathbb{F}_{q^m}[x]$ of degree strictly less than $q^n = [n]$ such that $F(\alpha_i) = c_i$, for all $i = 1, 2, \ldots, n$.*

Proof. Consider the evaluation map $\mathrm{ev}_{\boldsymbol{\alpha}} : \mathcal{L}_q\mathbb{F}_{q^m}[x] \longrightarrow \mathbb{F}_{q^m}^n$ for the vector $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Since it is $\mathbb{F}_{q^m}$-linear and the $\mathbb{F}_{q^m}$-linear space of q-linearized polynomials of degree less than $[n]$ has dimension n, it is enough to prove that, if $F(\alpha_i) = 0$, for $i = 1, 2, \ldots, n$, then $F = 0$.

By the linearity of F, we have that $F(\sum_i \lambda_i \alpha_i) = \sum_i \lambda_i F(\alpha_i) = 0$, for every $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{F}_q$. Therefore, F has q^n different roots and degree strictly less than q^n, hence $F = 0$, and we are done. □

Now we may define the desired products:

Definition F.8. If $n \leq m$, we denote by $F_{\mathbf{c}}$ the q-linearized polynomial of degree less than $[n]$ corresponding to $\mathbf{c} \in \mathbb{F}_{q^m}^n$.

For $\mathbf{c} \in \mathbb{F}_{q^m}^n$ and $n \leq m$, we define the vector $\varphi_n(\mathbf{c}) \in \mathbb{F}_{q^m}^m$ as $\varphi_n(\mathbf{c})_i = F_{\mathbf{c}}(\alpha_i)$, for $i = 1, 2, \ldots, m$. If $n \geq m$, we define $\varphi_n(\mathbf{c}) = (c_1, c_2, \ldots, c_m)$.

Finally, we will define the product $\star = \star_{\varphi_n} : \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$ (see Definition F.2).

Note that if $m = n$, both definitions of φ_n lead to $\varphi_n(\mathbf{c}) = \mathbf{c}$. Also note that φ_n depends on the basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ for $n < m$, while it does not for $n \geq m$.

When $m = n$, the product $\star$ in the previous definition coincides with the product $\star$ in Definition F.2, whereas if $m \neq n$, then there is no confusion between these products, since the first argument is different. Hence the meaning of $\star$ is clear from the context.

In the following remark we show how to perform interpolation using symbolic multiplications of linearized polynomials. Recall that the symbolic multiplication of two linearized polynomials $F, G \in \mathcal{L}_q\mathbb{F}_{q^m}[x]$ is defined as their composition $F \circ G$, which lies in $\mathcal{L}_q\mathbb{F}_{q^m}[x]$.

Remark F.9. *Interpolation as presented in Lemma F.7 can be performed as follows. First, we see that the map $\mathbf{c} \in \mathbb{F}_{q^m}^n \mapsto F_{\mathbf{c}}$ is $\mathbb{F}_{q^m}$-linear. Therefore,*

$$F_{\mathbf{c}} = \sum_{i=1}^{n} c_i F_{\mathbf{e}_i},$$

where $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ and $\mathbf{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ is the i-th vector in the canonical basis of $\mathbb{F}_{q^m}^n$ over $\mathbb{F}_{q^m}$, for $i = 1, 2, \ldots, n$. On the other hand, it holds that

$$F_{\mathbf{e}_i} = \frac{G_i}{G_i(\alpha_i)}, \quad \textit{where} \quad G_i = \prod_{\beta \in \langle \alpha_j | j \neq i \rangle} (x - \beta),$$

for $i = 1, 2, \ldots, n$. The polynomial $G_i / G_i(\alpha_i)$ in this expression is well-defined since α_i does not belong to the $\mathbb{F}_q$-linear vector space generated by the elements α_j, for $j \neq i$, and the expression in the numerator is a q-linearized polynomial by [15, Theorem 3.52] and has degree less than q^n. However, the complexity of constructing G_i in this way is of $O(q^{n-1})$ conventional multiplications. The following expression shows how to compute G_i with $O(n-1)$ symbolic multiplications:

$$G_i = L_{i,n} \circ L_{i,n-1} \circ \cdots \circ \widehat{L}_{i,i} \circ \cdots \circ L_{i,2} \circ L_{i,1},$$

where $L_{i,1} = x^{[1]} - (\alpha_1^{[1]} / \alpha_1)x$ and, for $j = 2, 3, \ldots, n$,

$$L_{i,j} = x^{[1]} - (\widetilde{L}_{i,j}(\alpha_j)^{[1]} / \widetilde{L}_{i,j}(\alpha_j))x$$

and $\widetilde{L}_{i,j} = L_{i,j-1} \circ \cdots \circ \widehat{L}_{i,i} \circ \cdots \circ L_{i,2} \circ L_{i,1}$. The notation $\widehat{L}_{i,i}$ means that the polynomial $L_{i,i}$ is omitted.

Next we see the linearity properties of the maps φ_n and hence of the product $\star$.

Lemma F.10. *For any values of m and n, the map $\varphi_n : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^m$ is $\mathbb{F}_{q^m}$-linear.*

Proof. For $n \geq m$, it is clear. For $n \leq m$, it is enough to note that $F_{\gamma\mathbf{c}+\delta\mathbf{d}} = \gamma F_{\mathbf{c}} + \delta F_{\mathbf{d}}$ as in the remark above, for all $\gamma, \delta \in \mathbb{F}_{q^m}$ and all $\mathbf{c}, \mathbf{d} \in \mathbb{F}_{q^m}^n$. □

The interesting property of the product $\star$ is that it preserves symbolic multiplications of linearized polynomials, as we will see now, and in the case $n \leq m$, it is the unique product with this property.

From now on, we denote $\boldsymbol{\alpha}_n = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ if $n \leq m$, and we complete the vector with other elements if $n > m$, $\boldsymbol{\alpha}_n = (\alpha_1, \alpha_2, \ldots, \alpha_m, \gamma_1, \gamma_2, \ldots, \gamma_n)$. We will also denote $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_m)$. Observe that $\varphi_n(\boldsymbol{\alpha}_n) = \boldsymbol{\alpha}$ in all cases, and moreover, $\varphi_n(\boldsymbol{\alpha}_n^{[j]}) = \boldsymbol{\alpha}^{[j]}$, if $j < n$.

Proposition F.11. *The following properties hold:*

1. *$\boldsymbol{\alpha}^{[j]} \star \mathbf{c} = \mathbf{c}^{[j]}$, for all $\mathbf{c} \in \mathbb{F}_{q^m}^n$ and all j. In particular,*
$$\mathrm{ev}_{\mathbf{b}}(F \circ G) = \mathrm{ev}_{\boldsymbol{\alpha}}(F) \star \mathrm{ev}_{\mathbf{b}}(G),$$
for all $\mathbf{b} \in \mathbb{F}_{q^m}^n$ and all $F, G \in \mathcal{L}_q\mathbb{F}_{q^m}[x]$.

2. *$\boldsymbol{\alpha}_n^{[j]} \star \mathbf{c} = \mathbf{c}^{[j]}$, for all $\mathbf{c} \in \mathbb{F}_{q^m}^n$ and all $j < n$. In particular,*
$$\mathrm{ev}_{\mathbf{b}}(F \circ G) = \mathrm{ev}_{\boldsymbol{\alpha}_n}(F) \star \mathrm{ev}_{\mathbf{b}}(G),$$
for all $\mathbf{b} \in \mathbb{F}_{q^m}^n$ and all $F, G \in \mathcal{L}_q\mathbb{F}_{q^m}[x]$, where F has degree strictly less than $[n]$.

3. *If $n \leq m$, then $\star$ is associative, that is, $\mathbf{a} \star (\mathbf{b} \star \mathbf{c}) = (\mathbf{a} \star \mathbf{b}) \star \mathbf{c}$, for all $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{F}_{q^m}^n$.*

Moreover, if $n \leq m$, and if $\odot$ is another product that satisfies item 2 for $\mathbf{b} = \boldsymbol{\alpha}_n$ (or item 1 for $\mathbf{b} = \boldsymbol{\alpha}$), then $\odot = \star$. In particular, by Lemma F.4, if $\star_\varphi$ satisfies this property, then $\varphi = \varphi_n$.

Proof. 1. The first part follows from the following chain of equalities:

$$\boldsymbol{\alpha}^{[j]} \star \mathbf{c} = \sum_{i=1}^{m} \alpha_i^{[j]} \mathbf{c}_i = \left(\sum_{i=1}^{m} \alpha_i \mathbf{c}_i \right)^{[j]} = \mathbf{c}^{[j]},$$

where $\mathbf{c} = \sum_{i=1}^{m} \alpha_i \mathbf{c}_i$ and $\mathbf{c}_i \in \mathbb{F}_q^n$, for all $i = 1, 2, \ldots, m$. The second part follows from the first part, since $\boldsymbol{\alpha}^{[j]} = \mathrm{ev}_{\boldsymbol{\alpha}}(x^{[j]})$ and therefore,

$$\mathrm{ev}_{\boldsymbol{\alpha}}(x^{[j]}) \star \mathrm{ev}_{\mathbf{b}}(G) = \mathrm{ev}_{\mathbf{b}}(G)^{[j]} = \mathrm{ev}_{\mathbf{b}}(G^{[j]}) = \mathrm{ev}_{\mathbf{b}}(x^{[j]} \circ G).$$

Hence the item follows since $\star$ is $\mathbb{F}_{q^m}$-linear in the first component, by Remark F.3 and Lemma F.10.

2. It follows from item 1, since $\varphi_n(\boldsymbol{\alpha}_n^{[j]}) = \boldsymbol{\alpha}^{[j]}$, if $j < n$.

3. It follows from item 2, since $\mathrm{ev}_{\boldsymbol{\alpha}_n}$ is surjective (by Lemma F.7) and symbolic multiplication of linearized polynomials is associative. □

If $n \leq m$, the last part of the proposition follows from the fact that $\mathrm{ev}_{\boldsymbol{\alpha}_n}$ (or $\mathrm{ev}_{\boldsymbol{\alpha}}$) is surjective, which follows from Lemma F.7.

We will now give a matrix representation of the products $\star_\varphi$, and show that the product $\star$ actually extends the product $*$. For that purpose, we define the "extension" map $E : \mathbb{F}_q^n \longrightarrow \mathbb{F}_{q^n}^n$ by $E = M^{-1} \circ D$ (recall Subsection 2.2 and Subsection 2.3), which is $\mathbb{F}_q$-linear and one to one. In other words,

$$E(\mathbf{c}) = (\alpha_1 c_1, \alpha_2 c_2, \ldots, \alpha_n c_n), \tag{F.3}$$

for all $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in \mathbb{F}_q^n$, which satisfies that $\mathrm{wt_R}(E(\mathbf{c})) = \mathrm{wt_H}(\mathbf{c})$. We gather in the next proposition the relations between the products $\star_\varphi$ and $*$, and the maps M, D and E. The proof is straightforward.

Proposition F.12. *For all values of m and n, all maps $\varphi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^m$ and all vectors $\mathbf{c}' \in \mathbb{F}_{q^m}^m$ and $\mathbf{c}, \mathbf{d} \in \mathbb{F}_{q^m}^n$, we have that*

$$M(\mathbf{c}' \star \mathbf{d}) = M(\mathbf{c}')M(\mathbf{d}) \quad \textit{and} \quad M(\mathbf{c} \star_\varphi \mathbf{d}) = M(\varphi(\mathbf{c}))M(\mathbf{d}).$$

On the other hand, if $m = n$ and $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$, then

$$D(\mathbf{a} * \mathbf{b}) = D(\mathbf{a})D(\mathbf{b}) \quad \textit{and} \quad E(\mathbf{a} * \mathbf{b}) = E(\mathbf{a}) \star E(\mathbf{b}).$$

Hence, the product $\star : \mathbb{F}_{q^m}^m \times \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$ is just the usual product of $m \times m$ matrices with $m \times n$ matrices over $\mathbb{F}_q$, whereas the products $\star_\varphi$ are also products of matrices after expanding the $m \times n$ matrix in the first argument to an $m \times m$ matrix over $\mathbb{F}_q$.

4 Rank error-correcting pairs

We will define in this section error-correcting pairs (ECPs) for the rank metric, using the products $\star$ and $\star_\varphi$ (recall Definition F.2 and Definition F.8).

However, which inner product to use for defining orthogonality and duality in $\mathbb{F}_{q^m}^n$, or in $\mathbb{F}_q^{m\times n}$, is not clear. First of all, we will always use the standard ($\mathbb{F}_q$-bilinear) inner product $\cdot$ in $\mathbb{F}_q^n$. On the other hand, we will first present ECPs in $\mathbb{F}_{q^m}^n$ that use the ($\mathbb{F}_{q^m}$-bilinear) "extension" inner product,

$$\mathbf{c}\cdot\mathbf{d} = c_1d_1 + c_2d_2 + \cdots + c_nd_n \in \mathbb{F}_{q^m}, \tag{F.4}$$

for all $\mathbf{c} = (c_1, c_2, \ldots, c_n), \mathbf{d} = (d_1, d_2, \ldots, d_n) \in \mathbb{F}_{q^m}^n$, and afterwards we will use the ($\mathbb{F}_q$-bilinear) "base" (or "trace") inner product in $\mathbb{F}_q^{m\times n}$,

$$\langle C, D\rangle = \mathbf{c}_1\cdot\mathbf{d}_1 + \mathbf{c}_2\cdot\mathbf{d}_2 + \cdots + \mathbf{c}_m\cdot\mathbf{d}_m = \mathrm{Tr}(CD^T) = \sum_{i,j} c_{i,j}d_{i,j} \in \mathbb{F}_q, \tag{F.5}$$

for $C, D \in \mathbb{F}_q^{m\times n}$,where $\mathbf{c}_i, \mathbf{d}_i \in \mathbb{F}_q^n$, for $i = 1, 2, \ldots, m$, are the rows of C and D, respectively, and $c_{i,j}, d_{i,j} \in \mathbb{F}_q$ are the entries of C and D, respectively. Tr denotes the usual trace of a square matrix.

Whereas the product $\cdot$ is the standard $\mathbb{F}_{q^m}$-bilinear product in $\mathbb{F}_{q^m}^n$, the product $\langle,\rangle$ corresponds to the standard $\mathbb{F}_q$-bilinear product in $\mathbb{F}_q^{mn} \cong \mathbb{F}_q^{m\times n}$. A duality theory for the product $\langle,\rangle$ and $\mathbb{F}_q$-linear rank-metric codes is developed originally in [4] and further in [22], where it is also shown that duals of $\mathbb{F}_{q^m}$-linear codes with respect to the "extension" inner product are equivalent to duals with respect to the "base" inner product (see [22, Theorem 21]). We will come back to this in Section 5, where we will relate both kinds of error-correcting pairs.

Now we will give some relations between the product $\star$ and the previous inner products that we will use later. If $\mathbf{c}, \mathbf{d} \in \mathbb{F}_{q^m}^n$, $\mathbf{d} = \sum_{i=1}^m \alpha_i \mathbf{d}_i$ and $\mathbf{d}_i \in \mathbb{F}_q^n$, for all $i = 1, 2, \ldots, m$, then we define

$$\mathbf{c}(\mathbf{d}) = (\mathbf{c}\cdot\mathbf{d}_1, \mathbf{c}\cdot\mathbf{d}_2, \ldots, \mathbf{c}\cdot\mathbf{d}_m) \in \mathbb{F}_{q^m}^m. \tag{F.6}$$

Lemma F.13. *Given $\mathbf{c}, \mathbf{d} \in \mathbb{F}_{q^m}^n$ and $\mathbf{a}, \mathbf{b} \in \mathbb{F}_{q^m}^m$, and given $C, D \in \mathbb{F}_q^{m\times n}$ and $A, B \in \mathbb{F}_q^{m\times m}$, the following properties hold:*

1. *$M(\mathbf{c}(\mathbf{d})) = M(\mathbf{c})M(\mathbf{d})^T$.*
2. *$\langle B, A^T\rangle = \langle B^T, A\rangle$.*
3. *$(\mathbf{b}\star\mathbf{c})\cdot\mathbf{d} = \mathbf{b}\cdot\mathbf{d}(\mathbf{c})$.*
4. *$\langle BC, D\rangle = \langle B, DC^T\rangle = \langle B^T, CD^T\rangle = \langle B^TD, C\rangle$.*
5. *$\mathbf{c}(\mathbf{d}) = \mathbf{0}$ if, and only if, $\mathbf{d}(\mathbf{c}) = \mathbf{0}$ if, and only if, $\mathrm{RSupp}(\mathbf{c}) \subseteq \mathrm{RSupp}(\mathbf{d})^\perp$.*
6. *$CD^T = 0$ if, and only if, $DC^T = 0$ if, and only if, $\mathrm{Row}(C) \subseteq \mathrm{Row}(D)^\perp$.*

Proof. They are straightforward computations. For item 1, observe that

$$\mathbf{c}(\mathbf{d}) = (\mathbf{c}\cdot\mathbf{d}_1, \mathbf{c}\cdot\mathbf{d}_2, \ldots, \mathbf{c}\cdot\mathbf{d}_m) = \sum_{i=1}^{m} \alpha_i(\mathbf{c}_i\cdot\mathbf{d}_1, \mathbf{c}_i\cdot\mathbf{d}_2, \ldots, \mathbf{c}_i\cdot\mathbf{d}_m).$$

Hence

$$M(\mathbf{c}(\mathbf{d}))_{i,k} = \mathbf{c}_i\cdot\mathbf{d}_k = \sum_{j=1}^{n} c_{i,j}d_{k,j} = \sum_{j=1}^{n} M(\mathbf{c})_{i,j}M(\mathbf{d})^T_{j,k}.$$

Therefore, $M(\mathbf{c}(\mathbf{d})) = M(\mathbf{c})M(\mathbf{d})^T$.

For item 3,

$$(\mathbf{b}\star\mathbf{c})\cdot\mathbf{d} = \left(\sum_{i=1}^{m} b_i\mathbf{c}_i\right)\cdot\mathbf{d} = \sum_{i=1}^{m} b_i(\mathbf{c}_i\cdot\mathbf{d}) = \mathbf{b}\cdot\mathbf{d}(\mathbf{c}).$$

The first equivalence in item 5 follows from item 1. Now, the second equivalence follows from the following chain of equivalences:

$$\mathbf{c}(\mathbf{d}) = \mathbf{0} \iff \mathbf{c}_k\cdot\mathbf{d}_i = 0, \forall i,k \iff \mathrm{RSupp}(\mathbf{c}) \subseteq \mathrm{RSupp}(\mathbf{d})^{\perp}.$$

4.1 Using the extension inner product

Denote by $\mathcal{D}^{\perp}$ the dual of an $\mathbb{F}_{q^m}$-linear code $\mathcal{D} \subseteq \mathbb{F}_{q^m}^n$ with respect to the extension product $\cdot$. Fix $\mathbb{F}_{q^m}$-linear codes $\mathcal{A}, \mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ and $\mathcal{B} \subseteq \mathbb{F}_{q^m}^m$ such that $\mathcal{B}\star\mathcal{A} \subseteq \mathcal{C}^{\perp}$, where $\mathcal{B}\star\mathcal{A}$ is defined as

$$\mathcal{B}\star\mathcal{A} = \langle\{\mathbf{b}\star\mathbf{a} \mid \mathbf{a}\in\mathcal{A}, \mathbf{b}\in\mathcal{B}\}\rangle_{\mathbb{F}_{q^m}}. \tag{F.7}$$

In many cases, $\mathcal{B} = \varphi(\mathcal{B}')$, where $\varphi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^m$ and $\mathcal{B}' \subseteq \mathbb{F}_{q^m}^n$ are both $\mathbb{F}_{q^m}$-linear. In that case, we denote $\mathcal{B}' \star_{\varphi} \mathcal{A} = \varphi(\mathcal{B}')\star\mathcal{A}$.

Observe that, since $\mathcal{B}$ is $\mathbb{F}_{q^m}$-linear and $\star$ is $\mathbb{F}_{q^m}$-linear in the first component, it holds that $\langle\{\mathbf{b}\star\mathbf{a} \mid \mathbf{a}\in\mathcal{A}, \mathbf{b}\in\mathcal{B}\}\rangle_{\mathbb{F}_{q^m}} = \langle\{\mathbf{b}\star\mathbf{a} \mid \mathbf{a}\in\mathcal{A}, \mathbf{b}\in\mathcal{B}\}\rangle_{\mathbb{F}_q}$.

We next compute generators of this space:

Proposition F.14. *If* $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_r$ *generate* $\mathcal{A}$ *and* $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_s$ *generate* $\mathcal{B}$*, as* $\mathbb{F}_{q^m}$*-linear vector spaces, then the vectors*

$$\mathbf{b}_i \star (\alpha_l \mathbf{a}_j),$$

for $1 \le i \le s$*,* $1 \le j \le r$ *and* $1 \le l \le m$*, generate* $\mathcal{B}\star\mathcal{A}$ *as an* $\mathbb{F}_{q^m}$*-linear space.*

In the case $\mathcal{B} = \varphi(\mathcal{B}')$ and $\mathbf{b}'_1, \mathbf{b}'_2, \ldots, \mathbf{b}'_s$ generate $\mathcal{B}'$ as an $\mathbb{F}_{q^m}$-linear space, then the elements $\mathbf{b}'_i \star_{\varphi} (\alpha_l\mathbf{a}_j)$ generate $\mathcal{B}' \star_{\varphi} \mathcal{A}$ as an $\mathbb{F}_{q^m}$-linear space.

Regarding the dimension of $\mathcal{B}\star\mathcal{A}$ (or $\mathcal{B}\star_{\varphi}\mathcal{A}$), that is, how many of the elements $\mathbf{b}_i \star (\alpha_l \mathbf{a}_j)$ are linearly independent, the next example shows that any number may be possible in the case $n \le m$, where the previous proposition says that an upper bound in the general case is $\min\{\dim(\mathcal{A})\dim(\mathcal{B})m, n\}$:

Example F.15. Assume that $n \leq m$, fix $1 \leq t \leq n$, and define $\mathbf{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$ and $\mathbf{b} = \mathbf{a} + \mathbf{a}^{[1]} + \cdots + \mathbf{a}^{[t-1]} \in \mathbb{F}_{q^m}^n$. Let $\gamma \in \mathbb{F}_{q^m}$ be such that $\gamma, \gamma^{[1]}, \ldots, \gamma^{[t-1]}$ are pairwise distinct, and write $\gamma_i = \gamma^{[i]}$, for $i = 0, 1, \ldots, t-1$. Let $\mathcal{A}$ and $\mathcal{B}$ be the $\mathbb{F}_{q^m}$-linear vector spaces generated by $\mathbf{a}$ and $\mathbf{b}$, respectively. By Proposition F.11, item 2, we have that

$$\mathbf{b} \star (\gamma^j \mathbf{a}) = \sum_{i=0}^{t-1} \mathbf{a}^{[i]} \star (\gamma^j \mathbf{a}) = \gamma_0^j \mathbf{a} + \gamma_1^j \mathbf{a}^{[1]} + \cdots + \gamma_{t-1}^j \mathbf{a}^{[t-1]} \in \mathcal{B} \star \mathcal{A},$$

for $j = 0, 1, 2, \ldots, t-1$, and these elements are linearly independent over $\mathbb{F}_{q^m}$, since the coefficients γ_i^j of the vectors $\mathbf{a}^{[i]}$ form a Vandermonde matrix. Furthermore, $\mathcal{B} \star \mathcal{A}$ is contained in the subspace generated by $\mathbf{a}, \mathbf{a}^{[1]}, \ldots, \mathbf{a}^{[t-1]}$, hence they are equal. Therefore, $\dim(\mathcal{A}) = \dim(\mathcal{B}) = 1$, whereas $\dim(\mathcal{B} \star \mathcal{A}) = t$.

Let $\mathbf{d} \in \mathbb{F}_{q^m}^n$ and define

$$\mathcal{K}(\mathbf{d}) = \{\mathbf{a} \in \mathcal{A} \mid (\mathbf{b} \star \mathbf{a}) \cdot \mathbf{d} = 0, \forall \mathbf{b} \in \mathcal{B}\}.$$

Then $\mathcal{K}(\mathbf{d})$ is $\mathbb{F}_q$-linear and the condition defining it may be verified just on a basis of $\mathcal{B}$ as $\mathbb{F}_{q^m}$-linear vector space. Observe that (precomputing the values $\varphi(\mathbf{b}')$, where the vectors $\mathbf{b}'$ are in a basis of $\mathcal{B}'$, in the case $\mathcal{B} = \varphi(\mathcal{B}')$), we can efficiently verify whether $\mathbf{a} \in \mathcal{K}(\mathbf{d})$. On the other hand, if $\mathcal{L} \subseteq \mathbb{F}_q^n$ is a linear subspace, define

$$\mathcal{A}(\mathcal{L}) = \{\mathbf{a} \in \mathcal{A} \mid \mathrm{RSupp}(\mathbf{a}) \subseteq \mathcal{L}^\perp\},$$

as in [11, 12]. We briefly connect this definition with the so-called rank-shortened codes in [18, Definition 6], where $\mathcal{A}_{\mathcal{L}^\perp} = \mathcal{A} \cap \mathcal{V}_{\mathcal{L}}^\perp$ and $\mathcal{V}_{\mathcal{L}} = \mathcal{L} \otimes \mathbb{F}_{q^m}$ is defined as the $\mathbb{F}_{q^m}$-linear vector space in $\mathbb{F}_{q^m}^n$ generated by $\mathcal{L}$:

Lemma F.16. *It holds that $\mathcal{A}(\mathcal{L}) = \mathcal{A}_{\mathcal{L}^\perp}$. In particular, it is an $\mathbb{F}_{q^m}$-linear space.*

Proof. Fix a basis $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_w$ of $\mathcal{L}$, and take $\mathbf{a} = \sum_{i=1}^m \alpha_i \mathbf{a}_i \in \mathcal{A}$, where $\mathbf{a}_i \in \mathbb{F}_q^n$, for $i = 1, 2, \ldots, m$. The result follows from the following chain of equivalent conditions

$$\mathrm{RSupp}(\mathbf{a}) \in \mathcal{L}^\perp \iff \mathbf{a}_i \in \mathcal{L}^\perp, \forall i \iff$$

$$\mathbf{a}_i \cdot \mathbf{v}_j = 0, \forall i, j \iff \mathbf{a} \cdot \mathbf{v}_j = 0, \forall j \iff \mathbf{a} \in \mathcal{V}_{\mathcal{L}}^\perp.$$

The following properties are the basic tools for the decoding algorithm of error correcting pairs:

Proposition F.17. *Let $\mathbf{r} = \mathbf{c} + \mathbf{e}$, where $\mathbf{c} \in \mathcal{C}$ and $\mathrm{wt}_{\mathrm{R}}(\mathbf{e}) \leq t$. Define also $\mathcal{L} = \mathrm{RSupp}(\mathbf{e}) \subseteq \mathbb{F}_q^n$. The following properties hold:*

1. *$\mathcal{K}(\mathbf{r}) = \mathcal{K}(\mathbf{e})$.*
2. *$\mathcal{A}(\mathcal{L}) \subseteq \mathcal{K}(\mathbf{e})$.*
3. *If $t < d_R(\mathcal{B}^\perp)$, then $\mathcal{A}(\mathcal{L}) = \mathcal{K}(\mathbf{e})$. In this case, $\mathcal{K}(\mathbf{e})$ is $\mathbb{F}_{q^m}$-linear.*

Proof. 1. It follows from $\mathcal{B} \star \mathcal{A} \subseteq \mathcal{C}^\perp$.

2. Let $\mathbf{a} \in \mathcal{A}(\mathcal{L})$. It follows from the definitions (recall (F.6)) or Lemma F.13 that $\mathbf{e}(\mathbf{a}) = \mathbf{0}$. Hence, by that lemma, $(\mathbf{b} \star \mathbf{a}) \cdot \mathbf{e} = \mathbf{b} \cdot \mathbf{e}(\mathbf{a}) = 0$, for all $\mathbf{b} \in \mathcal{B}$. Thus $\mathbf{a} \in \mathcal{K}(\mathbf{e})$.

3. By the previous item, we only need to prove that $\mathcal{K}(\mathbf{e}) \subseteq \mathcal{A}(\mathcal{L})$.

   Let $\mathbf{a} \in \mathcal{K}(\mathbf{e})$. It follows from Lemma F.13 that $\mathbf{e}(\mathbf{a}) \in \mathcal{B}^\perp$. Moreover, since $M(\mathbf{e}(\mathbf{a})) = M(\mathbf{e})M(\mathbf{a})^T$ by the same lemma, it holds that $\mathrm{wt}_\mathrm{R}(\mathbf{e}(\mathbf{a})) \leq \mathrm{wt}_\mathrm{R}(\mathbf{e}) \leq t$.

   Let $\mathbf{a} = \sum_{i=1}^m \alpha_i \mathbf{a}_i$, with $\mathbf{a}_i \in \mathbb{F}_q^n$, for $i = 1, 2, \ldots, m$. Since $t < d_R(\mathcal{B}^\perp)$, it follows that $\mathbf{e}(\mathbf{a}) = \mathbf{0}$ or, in other words, $\mathbf{a}_i \cdot \mathbf{e} = 0$, which implies that $\mathbf{a}_i \in \mathcal{L}^\perp$, for all $i = 1, 2, \ldots, m$, and therefore, $\mathrm{RSupp}(\mathbf{a}) \subseteq \mathcal{L}^\perp$.

We now come to the definition of t-rank error-correcting pairs of type I, where we use the extension inner product $\cdot$.

Definition F.18. Given the $\mathbb{F}_{q^m}$-linear codes $\mathcal{A}, \mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ and $\mathcal{B} \subseteq \mathbb{F}_{q^m}^m$, the pair $(\mathcal{A}, \mathcal{B})$ is called a t-rank error-correcting pair (t-RECP) of type I for $\mathcal{C}$ if the following properties hold:

1. $\mathcal{B} \star \mathcal{A} \subseteq \mathcal{C}^\perp$.
2. $\dim(\mathcal{A}) > t$.
3. $d_R(\mathcal{B}^\perp) > t$.
4. $d_R(\mathcal{A}) + d_R(\mathcal{C}) > n$.

If $\mathcal{B} = \varphi(\mathcal{B}')$, where φ and $\mathcal{B}' \subseteq \mathbb{F}_{q^m}^n$ are $\mathbb{F}_{q^m}$-linear, we say that $(\mathcal{A}, \mathcal{B}')$ is a t-RECP of type I for φ and $\mathcal{C}$, and if $\varphi = \varphi_n$, we will call it simply a t-RECP of type I for $\mathcal{C}$.

In order to describe a decoding algorithm for $\mathcal{C}$ using $(\mathcal{A}, \mathcal{B})$, we will need [18, Proposition 17], slightly modified (the proof is the same), which basically states that error correction is equivalent to erasure correction if the rank support of the error is known:

Lemma F.19 ([18]). *Assume that $\mathbf{c} \in \mathcal{C}$ and $\mathbf{r} = \mathbf{c} + \mathbf{e}$, where $\mathrm{RSupp}(\mathbf{e}) \subseteq \mathcal{L}$ and $\dim(\mathcal{L}) < d_R(\mathcal{C})$. Then, $\mathbf{c}$ is the only vector in $\mathcal{C}$ such that $\mathrm{RSupp}(\mathbf{r} - \mathbf{c}) \subseteq \mathcal{L}$.*

Moreover, if G is a generator matrix of $\mathcal{L}^\perp$, then $\mathbf{c}$ is the unique solution in $\mathcal{C}$ of the system of equations $\mathbf{r}G^T = \mathbf{x}G^T$, where $\mathbf{x}$ is the unknown vector. And if H is a parity check matrix for $\mathcal{C}$ over $\mathbb{F}_{q^m}$, then $\mathbf{e}$ is the unique solution to the system $\mathbf{r}H^T = \mathbf{x}H^T$ with $\mathrm{RSupp}(\mathbf{x}) \subseteq \mathcal{L}$.

Now we present, in the proof of the following theorem, a decoding algorithm for $\mathcal{C}$ using $(\mathcal{A}, \mathcal{B})$.

Theorem F.1. *If $(\mathcal{A}, \mathcal{B})$ is a t-RECP of type I for $\mathcal{C}$, then $\mathcal{C}$ verifies that $d_R(\mathcal{C}) \geq 2t + 1$ and admits a decoding algorithm able to correct errors $\mathbf{e} \in \mathbb{F}_{q^m}^n$ with $\mathrm{wt_R}(\mathbf{e}) \leq t$ of complexity $O(n^3)$ over the field $\mathbb{F}_{q^m}$.*

Proof. We will explicitly describe the decoding algorithm. As a consequence, we will derive that $d_R(\mathcal{C}) \geq 2t + 1$. Assume that the received codeword is $\mathbf{r} = \mathbf{c} + \mathbf{e}$, with $\mathbf{c} \in \mathcal{C}$, $\mathrm{RSupp}(\mathbf{e}) = \mathcal{L}$ and $\dim(\mathcal{L}) \leq t$.

Compute the space $\mathcal{K}(\mathbf{r})$, which is equal to $\mathcal{K}(\mathbf{e})$ by the first condition of t-RECP and Proposition F.17, item 1. Observe that $\mathcal{K}(\mathbf{r})$ can be described by a system of $O(n)$ linear equations by Proposition F.14.

By the third condition of t-RECP and Proposition F.17, we have that $\mathcal{A}(\mathcal{L}) = \mathcal{K}(\mathbf{e}) = \mathcal{K}(\mathbf{r})$. Therefore, we have computed the space $\mathcal{A}(\mathcal{L})$.

By the second condition of t-RECP and Lemma F.16, we have that $\mathcal{A}(\mathcal{L}) = \mathcal{A} \cap \mathcal{V}_{\mathcal{L}}^\perp \neq 0$, where $\mathcal{V}_{\mathcal{L}} = \mathcal{L} \otimes \mathbb{F}_{q^m}$, and therefore we may take a nonzero $\mathbf{a} \in \mathcal{A}(\mathcal{L})$. Define $\mathcal{L}' = \mathrm{RSupp}(\mathbf{a})^\perp$. Since $\mathbf{a} \in \mathcal{A}(\mathcal{L})$, we have that $\mathcal{L} \subseteq \mathcal{L}'$.

Now, by the fourth condition of t-RECP, we have that

$$\dim(\mathcal{L}') = n - \mathrm{wt_R}(\mathbf{a}) \leq n - d_R(\mathcal{A}) < d_R(\mathcal{C}).$$

Hence, by Lemma F.19, we may compute $\mathbf{e}$ or $\mathbf{c}$ by solving a system of linear equations using a generator matrix G of $\mathcal{L}'^\perp$, or a parity check matrix H of $\mathcal{C}$, respectively. This has complexity $O(n^3)$ over $\mathbb{F}_{q^m}$.

Finally, assume that $d_R(\mathcal{C}) \leq 2t$ and take two different vectors $\mathbf{c}, \mathbf{c}' \in \mathcal{C}$ and $\mathbf{e}, \mathbf{e}' \in \mathbb{F}_{q^m}^n$ such that $\mathbf{r} = \mathbf{c} + \mathbf{e} = \mathbf{c}' + \mathbf{e}'$ and $\mathrm{wt_R}(\mathbf{e}), \mathrm{wt_R}(\mathbf{e}') \leq t$. The previous algorithm gives as output both vectors $\mathbf{e}$ and $\mathbf{e}'$, but the output is unique, hence $\mathbf{e} = \mathbf{e}'$. This implies that $\mathbf{c} = \mathbf{c}'$, contradicting the hypothesis. Therefore, $d_R(\mathcal{C}) \geq 2t + 1$. □

If $m = n$, then the order of complexity over $\mathbb{F}_q$ increases, although it still is polynomial in n. On the other hand, if m is considerably smaller than n, then the complexity is $O(n^3)$ also over $\mathbb{F}_q$.

Gabidulin codes [8] have decoding algorithms of cubic complexity (see for instance [8]), and an algorithm of quadratic complexity was obtained in [16]. As we will see in Section 7, the previous decoding algorithm may be applied to a wider variety of rank-metric codes.

Remark F.20. *Observe that, from the proof of the previous theorem, if the pair $(\mathcal{A},\mathcal{B})$ satisfies the first three properties in Definition F.18, then we may use it to find a subspace $\mathcal{L}' \subseteq \mathbb{F}_q^n$ that contains the rank support of the error vector.*

Therefore, we say in this case that $(\mathcal{A},\mathcal{B})$ is a t-rank error-locating pair of type I for $\mathcal{C}$.

4.2 Using the base inner product

Now we turn to the case where we use the base inner product $\langle , \rangle$. We will denote by $\mathcal{D}^*$ the dual of an $\mathbb{F}_q$-linear code $\mathcal{D} \subseteq \mathbb{F}_q^{m\times n}$ with respect to $\langle , \rangle$.

We will use the same notation as in the previous subsection, although now $\mathcal{A},\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ and $\mathcal{B} \subseteq \mathbb{F}_q^{m\times m}$ are $\mathbb{F}_q$-linear, and $\mathcal{B}\mathcal{A} \subseteq \mathcal{C}^*$, where

$$\mathcal{B}\mathcal{A} = \langle \{BA \mid A \in \mathcal{A}, B \in \mathcal{B}\}\rangle_{\mathbb{F}_q}. \tag{F.8}$$

Observe that $M(\mathcal{B}' \star \mathcal{A}') = M(\mathcal{B}')M(\mathcal{A}')$, if $\mathcal{A}',\mathcal{B}' \subseteq \mathbb{F}_{q^m}^n$ are $\mathbb{F}_q$-linear vector spaces, by Proposition F.12. Generators of the space (F.8) are now simpler to compute:

Proposition F.21. *If $A_1, A_2, \ldots, A_r$ generate $\mathcal{A}$ and $B_1, B_2, \ldots, B_s$ generate $\mathcal{B}$, as $\mathbb{F}_q$-linear vector spaces, then the matrices*

$$B_iA_j,$$

for $1 \leq i \leq s$ and $1 \leq j \leq r$, generate $\mathcal{B}\mathcal{A}$ as an $\mathbb{F}_q$-linear vector space.

Let $D \in \mathbb{F}_q^{m\times n}$ and define

$$\mathcal{K}(D) = \{A \in \mathcal{A} \mid \langle BA, D\rangle = 0, \forall B \in \mathcal{B}\}.$$

Then $\mathcal{K}(D)$ is again $\mathbb{F}_q$-linear and the condition may be verified just on a basis of $\mathcal{B}$ as $\mathbb{F}_q$-linear vector space. On the other hand, if $\mathcal{L} \subseteq \mathbb{F}_q^n$ is a linear subspace, we define in the same way

$$\mathcal{A}(\mathcal{L}) = \{A \in \mathcal{A} \mid \mathrm{Row}(A) \subseteq \mathcal{L}^\perp\},$$

which is $\mathbb{F}_q$-linear (recall that we use the classical product $\cdot$ in $\mathbb{F}_q^n$), since we still have that $M^{-1}(\mathcal{A}(\mathcal{L})) = M^{-1}(\mathcal{A}) \cap \mathcal{V}_\mathcal{L}^\perp$, $\mathcal{V}_\mathcal{L} = \mathcal{L} \otimes \mathbb{F}_{q^m}$.

The following properties still hold:

Proposition F.22. *Let $R = C + E$, where $C \in \mathcal{C}$ and $\mathrm{Rk}(E) \leq t$. Define also $\mathcal{L} = \mathrm{Row}(E) \subseteq \mathbb{F}_q^n$. Then*

1. *$\mathcal{K}(R) = \mathcal{K}(E)$.*
2. *$\mathcal{A}(\mathcal{L}) \subseteq \mathcal{K}(E)$.*

3. *If $t < d_R(\mathcal{B}^*)$, then $\mathcal{A}(\mathcal{L}) = \mathcal{K}(E)$.*

Proof.

1. It also follows from $\mathcal{B}\mathcal{A} \subseteq \mathcal{C}^*$.
2. Take $A \in \mathcal{A}(\mathcal{L})$. Hence by definition or Lemma F.13, it holds that $EA^T = 0$, since $\mathrm{Row}(E) = \mathcal{L}$ and $\mathrm{Row}(A) \subseteq \mathcal{L}^\perp$. Therefore, for every $B \in \mathcal{B}$, we have that
$$\langle BA, E\rangle = \langle B, EA^T\rangle = 0,$$
by Lemma F.13. Then item 2 follows.
3. By the previous item, we only need to prove that $\mathcal{K}(E) \subseteq \mathcal{A}(\mathcal{L})$.
Let $A \in \mathcal{K}(E)$. It follows from Lemma F.13 that $EA^T \in B^*$. Moreover, it holds that $\mathrm{Rk}(EA^T) \leq \mathrm{Rk}(E) \leq t$. Since $t < d_R(\mathcal{B}^*)$, it follows that $EA^T = 0$, which implies that $\mathrm{Row}(A) \in \mathcal{L}^\perp$.

We now define t-rank error-correcting pairs of type II, where we use the base product $\langle , \rangle$, in contrast with the t-RECP of last subsection.

Definition F.23. Given the $\mathbb{F}_q$-linear codes $\mathcal{A}, \mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ and $\mathcal{B} \subseteq \mathbb{F}_q^{m\times m}$, the pair $(\mathcal{A}, \mathcal{B})$ is called a t-rank error-correcting pair (t-RECP) of type II for $\mathcal{C}$ if the following properties hold:

1. $\mathcal{B}\mathcal{A} \subseteq \mathcal{C}^*$.
2. $\dim_{\mathbb{F}_q}(\mathcal{A}) > mt$.
3. $d_R(\mathcal{B}^*) > t$.
4. $d_R(\mathcal{A}) + d_R(\mathcal{C}) > n$.

The same decoding algorithm, with the corresponding modifications, works in this case with polynomial complexity:

Theorem F.2. *If $(\mathcal{A}, \mathcal{B})$ is a t-RECP of type II for $\mathcal{C}$, then $\mathcal{C}$ satisfies that $d_R(\mathcal{C}) \geq 2t + 1$ and admits a decoding algorithm able to correct errors $E \in \mathbb{F}_q^{m\times n}$ with* $\mathrm{Rk}(E) \leq t$ *with polynomial complexity in (m, n) over the field $\mathbb{F}_q$.*

Proof. The proof is the same as in Theorem F.1, with the corresponding modifications. Note that in this case, if $\mathcal{L} = \mathrm{Row}(E)$ and $\mathcal{V}_\mathcal{L} = \mathcal{L} \otimes \mathbb{F}_{q^m}$, then $\dim_{\mathbb{F}_q}(\mathcal{V}_\mathcal{L}) = m \dim(\mathcal{L}) \leq mt$. On the other hand, $M^{-1}(\mathcal{A}(\mathcal{L})) = M^{-1}(\mathcal{A}) \cap \mathcal{V}_\mathcal{L}$, as in the previous subsection. Hence the condition $\dim_{\mathbb{F}_q}(\mathcal{A}) > mt$ ensures that $\mathcal{A}(\mathcal{L}) \neq 0$. □

Remark F.24. *As in Remark F.20, if the pair $(\mathcal{A}, \mathcal{B})$ satisfies the first three properties in Definition F.23, then we may use it to find a subspace $\mathcal{L}' \subseteq \mathbb{F}_q^n$ that contains the rank support of the error vector. We say in this case that $(\mathcal{A}, \mathcal{B})$ is a t-rank error-locating pair of type II for $\mathcal{C}$.*

5 The connection between the two types of RECPs

So far we have three types of error-correcting pairs: classical ECPs for linear codes in $\mathbb{F}_q^n$ that correct errors in the Hamming metric, ECPs for $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$ (RECPs of type I), and ECPs for general $\mathbb{F}_q$-linear codes in $\mathbb{F}_{q^m}^n$ or $\mathbb{F}_q^{m \times n}$ (RECPs of type II), where the two latter types correct errors in the rank metric. In this section we will see that RECPs of type II generalize RECPs of type I. In Section 7 we will see that, in some way, RECPs of type II also generalize ECPs for the Hamming metric.

We will need the following:

Definition F.25. Given the basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, we say that it is orthogonal (or dual) to another basis $\alpha'_1, \alpha'_2, \ldots, \alpha'_m$ if

$$\mathrm{Tr}(\alpha_i \alpha'_j) = \delta_{i,j},$$

for all $i, j = 1, 2, \ldots, m$. Here, Tr denotes the trace of the extension $\mathbb{F}_q \subsetneq \mathbb{F}_{q^m}$.

It is well-known that, for a given basis $\alpha_1, \alpha_2, \ldots, \alpha_m$, there exists a unique orthogonal basis (see for instance the discussion after [15, Definition 2.50]). We will denote it as in the previous definition: $\alpha'_1, \alpha'_2, \ldots, \alpha'_m$. In particular, the dual basis of $\alpha'_1, \alpha'_2, \ldots, \alpha'_m$ is $\alpha_1, \alpha_2, \ldots, \alpha_m$.

Now denote by $M_\alpha, M_{\alpha'} : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^{m \times n}$ the matrix representation maps (recall (F.1)) associated to the previous bases, respectively. The following lemma is [22, Theorem 21]:

Lemma F.26 ([22]). *Given an $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, it holds that*

$$M_{\alpha'}(\mathcal{C}^\perp) = M_\alpha(\mathcal{C})^*.$$

On the other hand, we have the following:

Lemma F.27. *For every $\mathbb{F}_{q^m}$-linear code $\mathcal{D} \subseteq \mathbb{F}_{q^m}^n$, it holds that*

$$d_R(\mathcal{D}^\perp) = d_R(M_\alpha(\mathcal{D})^*) = d_R(M_{\alpha'}(\mathcal{D})^*).$$

Proof. It follows from the fact that $d_R(\mathcal{D}^\perp) = d_R(M_{\alpha'}(\mathcal{D}^\perp)) = d_R(M_\alpha(\mathcal{D})^*)$, and analogously interchanging the roles of α and α'. □

Therefore, we may now prove that RECPs of type II generalize RECPs of type I:

Theorem F.3. *Take $\mathbb{F}_{q^m}$-linear codes $\mathcal{A}, \mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ and $\mathcal{B} \subseteq \mathbb{F}_{q^m}^m$. If $(\mathcal{A}, \mathcal{B})$ is a t-RECP of type I for $\mathcal{C}$ (in the basis α), then $(M_\alpha(\mathcal{A}), M_\alpha(\mathcal{B}))$ is a t-RECP of type II for $M_{\alpha'}(\mathcal{C})$.*

Proof. Using Lemma F.26 and Proposition F.12, we obtain that

$$M_\alpha(\mathcal{B})M_\alpha(\mathcal{A}) = M_\alpha(\mathcal{B} \star \mathcal{A}) \subseteq M_\alpha(\mathcal{C}^\perp) = M_{\alpha'}(\mathcal{C})^*,$$

and the first condition is satisfied.

The second condition follows from the fact that $\dim_{\mathbb{F}_q}(\mathcal{A}) = m \dim_{\mathbb{F}_{q^m}}(\mathcal{A})$, and M_α is an $\mathbb{F}_q$-linear vector space isomorphism.

Finally, the third condition follows from Lemma F.27 and the fourth condition remains unchanged. Hence the result follows. □

Observe that in the same way, t-rank error-locating pairs of type II generalize t-rank error-locating pairs of type I.

6 MRD codes and bounds on the minimum rank distance

In this section we will give bounds on the minimum rank distance of codes that follow from the properties of rank error-correcting pairs, in a similar way to the bounds in [21]. We will also see that, in some cases, MRD conditions on two of the codes imply that the third is also MRD.

We will fix $\mathbb{F}_q$-linear codes $\mathcal{A}, \mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ and $\mathcal{B} \subseteq \mathbb{F}_q^{m \times m}$. Due to Lemmas F.26 and F.27, and Proposition F.12, the results in this section may be directly translated into results where we consider the "extension" inner product $\cdot$ and $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$.

We will make use of the following consequence of the Singleton bound:

Lemma F.28. *For every $\mathbb{F}_q$-linear code $\mathcal{D} \subseteq \mathbb{F}_q^{m \times n}$ it holds that*

$$d_R(\mathcal{D}) + d_R(\mathcal{D}^*) \leq n + 2.$$

Proof. The Singleton bound implies that

$$\dim_{\mathbb{F}_q}(\mathcal{D})/m \leq n - d_R(\mathcal{D}) + 1, \quad \text{and} \quad \dim_{\mathbb{F}_q}(\mathcal{D}^*)/m \leq n - d_R(\mathcal{D}^*) + 1.$$

Adding both inequalities up and using that $\dim_{\mathbb{F}_q}(\mathcal{D}) + \dim_{\mathbb{F}_q}(\mathcal{D}^*) = mn$, the result follows. □

Proposition F.29. *Assume that $\mathcal{B}\mathcal{A} \subseteq \mathcal{C}^*$. If $d_R(\mathcal{A}^*) > a > 0$ and $d_R(\mathcal{B}^*) > b > 0$, then $d_R(\mathcal{C}) \geq a + b$.*

Proof. Take $C \in \mathcal{C}$ and $A \in \mathcal{A}$, and define $\mathcal{L} = \mathrm{Row}(C) \subseteq \mathbb{F}_q^n$. By Lemma F.13, we have that

$$0 = \langle BA, C \rangle = \langle B^T, AC^T \rangle,$$

for all $B \in \mathcal{B}$ and all $A \in \mathcal{A}$, which means that the $\mathbb{F}_q$-linear space $\mathcal{A}(C) = \{AC^T \mid A \in \mathcal{A}\} \subseteq (\mathcal{B}^T)^*$, and hence $d_R(\mathcal{A}(C)) > b$.

Let G be a $t \times n$ generator matrix over $\mathbb{F}_q$ of $\mathcal{L}$ (where $t = \mathrm{Rk}(C)$). Taking a subset of rows of C that generate $\mathcal{L}$, we see that $\mathcal{A}(C)$ is $\mathbb{F}_q$-linearly isomorphic and rank-metric equivalent to $\mathcal{A}_1 = \{AG^T \mid A \in \mathcal{A}\} \subseteq \mathbb{F}_q^{m \times t}$. Take $D \in \mathcal{A}_1^*$. For every $A \in \mathcal{A}$, it holds that

$$\langle A, DG \rangle = \langle AG^T, D \rangle = 0,$$

by Lemma F.13. Therefore, $DG \in \mathcal{A}^*$. Moreover, $\mathrm{Rk}(D) = \mathrm{Rk}(DG)$ since G is full rank, and hence $\mathrm{Rk}(D) > a$. Therefore, $d_R(\mathcal{A}_1^*) > a$. Together with $d_R(\mathcal{A}_1) > b$ and the previous lemma, we obtain that

$$a + 1 + b + 1 \leq d_R(\mathcal{A}_1) + d_R(\mathcal{A}_1^*) \leq t + 2,$$

that is, $t \geq a + b$, and the result follows. □

We obtain the following corollary on MRD codes:

Corollary F.30. *Assume that $n \leq m$ (otherwise, take transposed matrices), $d_R(\mathcal{A}) = n - t$, $\dim_{\mathbb{F}_q}(\mathcal{A}) = m(t+1)$, $d_R(\mathcal{B}) = m - t + 1$ and $\dim_{\mathbb{F}_q}(\mathcal{B}) = mt$. Then, for all $\mathcal{D} \subseteq (\mathcal{B}\mathcal{A})^*$, it holds that $d_R(\mathcal{D}) \geq 2t + 1$ and $(\mathcal{A}, \mathcal{B})$ is a t-RECP of type II for $\mathcal{D}$.*

Proof. $\mathcal{A}$ and $\mathcal{B}$ are MRD codes, since their minimum rank distance attains the Singleton bound. By [4, Theorem 5.5] (see also [22, Corollary 41]), $\mathcal{A}^*$ and $\mathcal{B}^*$ are also MRD, which implies that

$$d_R(\mathcal{A}^*) > t + 1, \quad \text{and} \quad d_R(\mathcal{B}^*) > t.$$

By the previous proposition, it holds that $d_R(\mathcal{D}) \geq 2t + 1$. We see that the properties of RECPs of type II are satisfied, and the result follows. □

Now we obtain bounds on $d_R(\mathcal{A})$ from bounds on $d_R(\mathcal{B}^*)$ and $d_R(\mathcal{C}^*)$:

Proposition F.31. *Assume that $\mathcal{B}\mathcal{A} \subseteq \mathcal{C}^*$. If $d_R(\mathcal{B}^*) > b > 0$ and $d_R(\mathcal{C}^*) > c > 0$, then $d_R(\mathcal{A}) \geq b + c$.*

Proof. The proof is analogous to the proof of Proposition F.29. In this case, we fix $A \in \mathcal{A}$, with $\mathcal{L} = \mathrm{Row}(A)$, $t = \mathrm{Rk}(A)$, and consider $A(\mathcal{C}) = \{AC^T \mid C \in \mathcal{C}\}$. The rest of the proof follows the same lines, interchanging the roles of $\mathcal{A}$ and $\mathcal{C}$, and using the fact that $\langle BA, C \rangle = \langle B^T C, A \rangle$, from Lemma F.13, and $d_R(\mathcal{B}^*) = d_R((\mathcal{B}^T)^*)$. □

Again, we may give the following corollary on MRD codes:

Corollary F.32. *Assume that $\mathcal{B}\mathcal{A} \subseteq \mathcal{C}^*$ and $n \leq m$. If $d_R(\mathcal{C}) = 2t + 1$, $\dim_{\mathbb{F}_q}(\mathcal{C}) = m(n - 2t)$ and $(\mathcal{A}, \mathcal{B})$ is a t-RECP of type II for $\mathcal{C}$, then $d_R(\mathcal{A}) \geq n - t$ and $mt < \dim_{\mathbb{F}_q}(\mathcal{A}) \leq m(t+1)$. If $\dim_{\mathbb{F}_q}(\mathcal{A})$ is a multiple of m (in particular, if $M^{-1}(\mathcal{A})$ is $\mathbb{F}_{q^m}$-linear), then $\mathcal{A}$ is MRD.*

Proof. By the properties of RECPs of type II, we have that $d_R(\mathcal{B}^*) > t$, and since $\mathcal{C}$ is MRD, then $\mathcal{C}^*$ is also MRD and we have that $d_R(\mathcal{C}^*) = n - 2t + 1$. Therefore, $d_R(\mathcal{A}) \geq n - t$ by the previous proposition. By the properties of RECPs of type II, $\dim_{\mathbb{F}_q}(\mathcal{A}) > mt$, and we are done. The last statement follows from the Singleton bound for $\mathcal{A}$. □

We now turn to a bound analogous to [21, Proposition 3.1]. The BCH bound on the minimum Hamming distance of cyclic codes is generalized by the Hartmann-Tzeng bounds [10] and further generalized by the Roos bound [23, 24]. The next proposition is the rank-metric equivalent of the Roos bound [23, 24] for the Hamming metric, as mentioned in [7, Proposition 5].

Proposition F.33. *Assume the following properties for $a, b > 0$:*

$$(1)\ \mathcal{B}\mathcal{A} \subseteq \mathcal{C}^*, \quad (2)\ \dim_{\mathbb{F}_q}(\mathcal{A}) > ma, \quad (3)\ d_R(\mathcal{B}^*) > b,$$

$$(4)\ d_R(\mathcal{A}) + a + b > n, \quad \textit{and} \quad (5)\ d_R(\mathcal{A}^*) > 1.$$

Then it holds that $d_R(\mathcal{C}) > a + b$.

Proof. Take $C \in \mathcal{C}$ and let $\mathcal{L} = \mathrm{Row}(C) \subseteq \mathbb{F}_q^n$ and $t = \mathrm{Rk}(C)$. Conditions (1), (3) and (5) imply that $t > b$ by Proposition F.29.

Assume that $b < t \leq a + b$. Take linear subspaces $\mathcal{L}_-, \mathcal{L}_+, \mathcal{U} \subseteq \mathbb{F}_q^n$ such that $\mathcal{L}_- \subseteq \mathcal{L} \subseteq \mathcal{L}_+$, $\mathcal{L}_+ = \mathcal{U} \oplus \mathcal{L}_-$, $b = \dim(\mathcal{L}_-)$ and $a + b = \dim(\mathcal{L}_+)$. Since $m \dim(\mathcal{U}) = ma < \dim_{\mathbb{F}_q}(\mathcal{A})$ by condition (2), we have that $\mathcal{A}(\mathcal{U}) \neq 0$, and therefore there exists a non-zero $A \in \mathcal{A}$ with $\mathrm{Row}(A) \subseteq \mathcal{U}^\perp$.

It holds that every row in C is in $\mathcal{L}_+$. Since the rows in A are in $\mathcal{U}^\perp$, it holds that $AC^T = AN^T$, where N is obtained from C by substituting every row by its projection from $\mathcal{U} \oplus \mathcal{L}_-$ to $\mathcal{L}_-$.

Therefore $\mathrm{Rk}(AC^T) \leq \mathrm{Rk}(N) \leq \dim(\mathcal{L}_-) = b$, but $AC^T \in (\mathcal{B}^T)^*$ by condition (1) and Lemma F.13, and hence $AC^T = 0$ by condition (3). This means that $\mathrm{Row}(A) \subseteq \mathcal{L}_-^\perp \cap \mathcal{U}^\perp = \mathcal{L}_+^\perp$. Thus, $\mathrm{Rk}(A) \leq n - a - b < d_R(\mathcal{A})$, which is absurd by condition (4), since $A \neq 0$. We conclude that $t > a + b$ and we are done. □

Taking $a = b = t$ for some $t > 0$, where a and b are as in the previous proof, we obtain the following particular case:

Corollary F.34. *For all $\mathbb{F}_q$-linear codes $\mathcal{D} \subseteq (\mathcal{B}\mathcal{A})^*$ such that* $\dim_{\mathbb{F}_q}(\mathcal{A}) > mt$, *$d_R(\mathcal{B}^*) > t$, $d_R(\mathcal{A}) > n - 2t$ and $d_R(\mathcal{A}^*) > 1$, it holds that $d_R(\mathcal{D}) \geq 2t + 1$ and $(\mathcal{A}, \mathcal{B})$ is a t-RECP of type II for $\mathcal{D}$.*

Observe that the previous result states that, if some conditions on $\mathcal{A}$ and $\mathcal{B}$ hold, then they form a t-RECP of type II for all $\mathbb{F}_q$-linear codes contained in $(\mathcal{B}\mathcal{A})^*$. That is, we have found a t-rank error-correcting algorithm for all $\mathbb{F}_q$-linear subcodes of $(\mathcal{B}\mathcal{A})^*$.

7 Some codes with a t-RECP

In this section, we study families of codes that admit a t-RECP of some type.

7.1 Hamming-metric codes with ECPs

Take $\mathbb{F}_q$-linear codes $\mathcal{A}, \mathcal{B}, \mathcal{C} \subseteq \mathbb{F}_q^n$ such that $(\mathcal{A}, \mathcal{B})$ is a t-ECP for $\mathcal{C}$ in the Hamming metric. We will see that the algorithm presented in Theorem F.2 is actually an extension of the decoding algorithm in the Hamming metric using t-ECPs [19, 20]. We observe the following (recall the definition of D in (F.2)):

Remark F.35. *For all* $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$*, it holds that*

$$\mathbf{a} \cdot \mathbf{b} = \langle D(\mathbf{a}), D(\mathbf{b}) \rangle.$$

Moreover, it holds that

$$D(\mathcal{B})D(\mathcal{A}) \subseteq D(\mathcal{C})^*.$$

Therefore, from the previous remark and the properties of D, the $\mathbb{F}_q$-linear codes $D(\mathcal{A}), D(\mathcal{B}), D(\mathcal{C}) \subseteq \mathbb{F}_q^{n \times n}$ satisfy the following conditions:

1. $D(\mathcal{B})D(\mathcal{A}) \subseteq D(\mathcal{C})^*$.
2. $\dim_{\mathbb{F}_q}(D(\mathcal{A})) > t$.
3. $d_R(D(\mathcal{B})^*) = 1$.
4. $d_R(D(\mathcal{A})) + d_R(D(\mathcal{C})) > n$.

That is, $(D(\mathcal{A}), D(\mathcal{B}))$ satisfy the same conditions as t-RECPs of type II for $D(\mathcal{C})$, except that conditions 2 and 3 are weakened. However, the previous conditions are enough to correct any error $D(\mathbf{e}) \in \mathbb{F}_q^{n \times n}$, where $\mathbf{e} \in \mathbb{F}_q^n$ and $\mathrm{wt_H}(\mathbf{e}) \leq t$,

Assume the received vector is $R = D(\mathbf{c}) + D(\mathbf{e})$, with $\mathbf{c} \in \mathcal{C}$ and $\mathrm{wt_H}(\mathbf{e}) \leq t$. Correcting the diagonal of $R = D(\mathbf{c}) + D(\mathbf{e})$ for the Hamming metric is the same as correcting the matrix $R = D(\mathbf{c}) + D(\mathbf{e})$ itself for the rank metric. We will next show that the algorithm in Theorem F.2 is exactly the same as the algorithm for ECPs in the Hamming metric.

Define $I \subseteq \{1, 2, \ldots, n\}$ as the Hamming support of $\mathbf{e} = (e_1, e_2, \ldots, e_n) \in \mathbb{F}_q^n$, that is, $I = \mathrm{HSupp}(\mathbf{e}) = \{i \in \{1, 2, \ldots, n\} \mid e_i \neq 0\}$, and define

$$\mathcal{K}_H(\mathbf{e}) = \{\mathbf{a} \in \mathcal{A} \mid (\mathbf{b} * \mathbf{a}) \cdot \mathbf{e} = 0, \forall \mathbf{b} \in \mathcal{B}\}, \text{ and}$$

$$\mathcal{A}(I) = \{\mathbf{a} \in \mathcal{A} \mid \mathrm{HSupp}(\mathbf{a}) \subseteq I^c\},$$

where I^c denotes the complementary of I. It holds that $\mathrm{Row}(D(\mathbf{e})) = \mathcal{L}_I \subseteq \mathbb{F}_q^n$, the space generated by the vectors $\mathbf{e}_i$ in the canonical basis, for $i \in I$. Therefore, by Remark F.35, the properties of D, Proposition F.12 and the fact that $\mathcal{L}_I^\perp = \mathcal{L}_{I^c}$, it holds that

$$\mathcal{K}(R) = \mathcal{K}(D(\mathbf{e})) = D(\mathcal{K}_H(\mathbf{e})) \quad \text{and} \quad (D(\mathcal{A}))(\mathcal{L}_I) = D(\mathcal{A}(I)).$$

Moreover, since $\mathcal{A}(I) = \mathcal{K}_H(\mathbf{e})$ by the properties of ECPs in the Hamming metric, we also have that

$$\mathcal{K}(R) = D(\mathcal{K}_H(\mathbf{e})) = D(\mathcal{A}(I)) = (D(\mathcal{A}))(\mathcal{L}_I).$$

Hence, computing $\mathcal{K}(R)$ implies computing $(D(\mathcal{A}))(\mathcal{L}_I)$. Finally, since $\mathcal{A}(I) \neq 0$ by the properties of ECPs, we have that $(D(\mathcal{A}))(\mathcal{L}_I) \neq 0$. The rest of the algorithm goes in the same way as in Theorem F.2. That is, the decoding algorithm in Theorem F.2 actually extends the decoding algorithm given by ECPs in the Hamming metric.

7.2 Gabidulin codes

Gabidulin codes, introduced in [8], are a well-known family of MRD $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$, when $n \leq m$. In [14], a generalization of these codes is given, also formed by MRD codes.

Fix $n \leq m$. They can be defined as follows. For each $\mathbf{b} = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_{q^m}^n$, where $b_1, b_2, \ldots, b_n$ are linearly independent over $\mathbb{F}_q$, each $k = 1, 2, \ldots, n$ and each integer r such that r and m are coprime, we define the (generalized) Gabidulin code of dimension k in $\mathbb{F}_{q^m}^n$ as

$$\mathrm{Gab}_{k,m,n}(r, \mathbf{b}) = \{(F(b_1), F(b_2), \ldots, F(b_n)) \mid F \in \mathcal{L}_{q,r,k}\mathbb{F}_{q^m}[x]\},$$

where $\mathcal{L}_{q,r,k}\mathbb{F}_{q^m}[x]$ denotes the $\mathbb{F}_{q^m}$-linear vector space of q-linearized polynomials of the form

$$F(x) = a_0 x + a_1 x^{[r]} + a_2 x^{[2r]} + a_3 x^{[3r]} + \cdots + a_{k-1} x^{[(k-1)r]},$$

for some $a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^m}$. Observe that classical Gabidulin codes as defined in [8] are obtained by setting $r = 1$. Also observe that, for any invertible matrix $P \in \mathbb{F}_q^{n \times n}$, it holds that

$$\mathrm{Gab}_{k,m,n}(r, \mathbf{b})P = \mathrm{Gab}_{k,m,n}(r, \mathbf{b}P),$$

and hence $\mathbb{F}_{q^m}$-linearly rank-metric equivalent codes to Gabidulin codes are again Gabidulin codes.

The following lemma follows from Proposition F.11:

Lemma F.36. *For every positive integers k, l with $k + l - 1 \leq n$, it holds that*

$$\mathrm{Gab}_{k,m,m}(r, \boldsymbol{\alpha}) \star \mathrm{Gab}_{l,m,n}(r, \mathbf{b}) = \mathrm{Gab}_{k+l-1,m,n}(r, \mathbf{b}).$$

In the case $r = 1$, it holds that

$$\mathrm{Gab}_{k,m,n}(1, \boldsymbol{\alpha}_n) \star \mathrm{Gab}_{l,m,n}(1, \mathbf{b}) = \mathrm{Gab}_{k+l-1,m,n}(1, \mathbf{b}).$$

On the other hand, for $r = 1$ and the maps φ_n, the following lemma follows from the definitions:

Lemma F.37. *It holds that*

$$\varphi_n(\mathrm{Gab}_{k,m,n}(1, \boldsymbol{\alpha}_n)) = \mathrm{Gab}_{k,m,m}(1, \boldsymbol{\alpha}).$$

With these two lemmas, we can prove that Gabidulin codes have t-RECP of type I. Recall from [14] that

$$\mathrm{Gab}_{k,m,n}(r, \mathbf{b})^{\perp} = \mathrm{Gab}_{n-k,m,n}(r, \mathbf{b}'),$$

for some $\mathbf{b}' \in \mathbb{F}_{q^m}^n$ that can be computed from $\mathbf{b}$.

Theorem F.4. *If $t > 0$, $\mathcal{A} = \mathrm{Gab}_{t+1,m,n}(r, \mathbf{b})$, $\mathcal{B} = \mathrm{Gab}_{t,m,m}(r, \boldsymbol{\alpha})$ and $\mathcal{C} = \mathrm{Gab}_{2t,m,n}(r, \mathbf{b})^{\perp}$, then $(\mathcal{A}, \mathcal{B})$ is a t-RECP of type I for $\mathcal{C}$. In the case $r = 1$, we may take $\mathcal{B} = \mathrm{Gab}_{t,m,n}(r, \boldsymbol{\alpha}_n)$.*

Proof. The first condition follows from Lemma F.36. On the other hand, $\dim_{\mathbb{F}_{q^m}}(\mathcal{A}) = t + 1$, so the second condition follows. The third condition is trivial, and for the case $r = 1$ and $\mathcal{B} = \mathrm{Gab}_{t,m,n}(1, \boldsymbol{\alpha}_n)$ it follows from Lemma F.37. Finally, the fourth condition follows from the following computation:

$$d_R(\mathcal{A}) + d_R(\mathcal{C}) = n - t + 2t + 1 = n + t + 1,$$

and the theorem follows. □

We see that $d_R(\mathcal{A}) = n - t > n - 2t$. Hence, the pair $(M_\alpha(\mathcal{A}), M_\alpha(\mathcal{B}))$, with notation as in Section 5, can be used by Corollary F.34 to efficiently correct any error of rank at most t for every $\mathbb{F}_q$-linear subcode of a (generalized) Gabidulin code. Such efficient decoding algorithms seem not to have been obtained yet.

Corollary F.38. *Let $t, \mathcal{A}, \mathcal{B}$ and $\mathcal{C}$ be as in the previous theorem. Then, for every $\mathbb{F}_q$-linear subcode $\mathcal{D} \subseteq \mathcal{C}$, the pair $(M_\alpha(\mathcal{A}), M_\alpha(\mathcal{B}))$ is a t-RECP of type II for $M_{\alpha'}(\mathcal{D})$.*

Proof. It follows from the previous theorem, Theorem F.3 and Corollary F.34. □

On the other hand, decoding algorithms for generalized Gabidulin codes with $r \neq 1$ seem to have been obtained only in [14], also of cubic complexity.

7.3 Skew cyclic codes

Skew cyclic codes (or q^r-cyclic codes) play the same role as cyclic codes in the theory of error-correcting codes for the rank metric. They were originally introduced in [8] for $r = 1$ and $m = n$, and further generalized in [9] for $r = 1$ and any m and n, and for any r in the work by Ulmer et al. [1, 2]. In this subsection we will only treat the case $r = 1$.

Assume that $n = sm$ is a multiple of m. We will see in this subsection that, in that case, some $\mathbb{F}_{q^m}$-linear q-cyclic codes have rank error-locating pairs of type I, in analogy to the ideas in [6]. We say that an $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is q-cyclic if the q-shifted vector

$$(c_{n-1}^q, c_0^q, c_1^q, \ldots, c_{n-2}^q)$$

lies in $\mathcal{C}$, for every $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$. As in [17], we say that an $\mathbb{F}_q$-linear subspace $\mathcal{T} \subseteq \mathbb{F}_{q^n}$ is a q-root space (over $\mathbb{F}_{q^m}$) if it is the root space in $\mathbb{F}_{q^n}$ of a q-linearized polynomial in $\mathcal{L}_q\mathbb{F}_{q^m}[x]$.

By [17, Theorem 3], $\mathbb{F}_{q^m}$-linear q-cyclic codes are codes in $\mathbb{F}_{q^m}^n$ with a parity check matrix over $\mathbb{F}_{q^n}$ of the form

$$\mathcal{M}(\beta_1, \beta_2, \ldots, \beta_{n-k}) = \begin{pmatrix} \beta_1 & \beta_1^{[1]} & \beta_1^{[2]} & \cdots & \beta_1^{[n-1]} \\ \beta_2 & \beta_2^{[1]} & \beta_2^{[2]} & \cdots & \beta_2^{[n-1]} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \beta_{n-k} & \beta_{n-k}^{[1]} & \beta_{n-k}^{[2]} & \cdots & \beta_{n-k}^{[n-1]} \end{pmatrix},$$

where $\beta_1, \beta_2, \ldots, \beta_{n-k}$ is a basis of $\mathcal{T}$ over $\mathbb{F}_q$, for some q-root space $\mathcal{T}$. Moreover by [17, Corollary 2], $\mathbb{F}_{q^m}$-linear q-cyclic codes are in bijection with q-root spaces over $\mathbb{F}_{q^m}$.

The next bound, which is given in [17, Corollary 4], is an extension of the rank-metric version of the BCH bound (by setting $w = 0$ and $c = 1$) found in [2, Proposition 1]:

Lemma F.39 (Rank-HT bound [17]). *Let $c > 0$, $\delta > 0$ and $w \geq 0$ be integers with $\delta + w \leq \min\{m, n\}$ and $d = \gcd(c, n) < \delta$, and $\alpha \in \mathbb{F}_{q^n}$ be such that the set $\mathcal{A} = \{\alpha^{[i+jc]} \mid 0 \leq i \leq \delta - 2, 0 \leq j \leq w\}$ is a linearly independent set of vectors.*

If $\mathcal{C}$ is the $\mathbb{F}_{q^m}$-linear q-cyclic code corresponding to the q-root space $\mathcal{T}$ and $\mathcal{A} \subseteq \mathcal{T}$, then $d_R(\mathcal{C}) \geq \delta + w$.

To use it, we need to deal with normal bases. First, it is well-known [15] that the orthogonal (or dual) basis of a normal basis $\alpha, \alpha^{[1]}, \ldots, \alpha^{[n-1]} \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is again a normal basis $\beta, \beta^{[1]}, \ldots, \beta^{[n-1]} \in \mathbb{F}_{q^n}$. Define $\boldsymbol{\alpha} = (\alpha, \alpha^{[1]}, \ldots, \alpha^{[n-1]})$ and $\boldsymbol{\beta} = (\beta, \beta^{[1]}, \ldots, \beta^{[n-1]})$. Then it holds that

$$\boldsymbol{\alpha}^{[i]} \cdot \boldsymbol{\beta}^{[j]} = \mathrm{Tr}(\alpha^{[i]}\beta^{[j]}) = \delta_{i,j}$$

by definition. On the other hand, for a subset $I \subseteq \{1, 2, \ldots, n\}$, define the matrix

$$\mathcal{M}_{\boldsymbol{\alpha}}(I) = \mathcal{M}(\alpha^{[i]} \mid i \in I),$$

and similarly for $\boldsymbol{\beta}$.

Define the $\mathbb{F}_{q^m}$-linear codes $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_{q^m}^n$ as the subfield subcodes of the codes in $\mathbb{F}_{q^n}^n$ with generator matrices $\mathcal{M}_{\boldsymbol{\alpha}}(I)$ and $\mathcal{M}_{\boldsymbol{\alpha}}(J)$, for some subsets $I, J \subseteq \{1, 2, \ldots, n\}$, respectively.

In order to obtain q-cyclic codes, we will assume that the space generated by $\{\alpha^{[i]} \mid i \in I\}$ is a q-root space, and similarly for J. Due to the cyclotomic space description of q-root spaces in [17, Proposition 2], this holds if the following condition holds: if $i \in I$, then $i + m \in I$ (modulo n), and similarly for J.

Define the $\mathbb{F}_{q^m}$-linear q-cyclic code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ with parity check matrix $\mathcal{M}_{\boldsymbol{\alpha}}(I + J)$. Observe that $I + J$ also gives a q-root space by the previous paragraph. We have the following lemmas:

Lemma F.40. *$\mathcal{A}$ and $\mathcal{B}$ are the q-cyclic codes with parity check matrices $\mathcal{M}_{\boldsymbol{\beta}}(I^c)$ and $\mathcal{M}_{\boldsymbol{\beta}}(J^c)$ over $\mathbb{F}_{q^n}$, respectively.*

Proof. We prove it for $\mathcal{A}$. Define $\widetilde{\mathcal{A}}$ as the $\mathbb{F}_{q^n}$-linear code in $\mathbb{F}_{q^n}^n$ with generator matrix $\mathcal{M}_{\boldsymbol{\alpha}}(I)$. It is enough to prove that $\mathcal{M}_{\boldsymbol{\beta}}(I^c)$ is a parity check matrix for $\widetilde{\mathcal{A}}$.

However, since $\boldsymbol{\alpha}^{[i]} \cdot \boldsymbol{\beta}^{[j]} = 0$, for every $i \in I$ and $j \notin I$, it holds that $\mathcal{M}_{\boldsymbol{\alpha}}(I)\mathcal{M}_{\boldsymbol{\beta}}(I^c)^T = 0$. On the other hand, these two matrices are full rank and the number of rows in $\mathcal{M}_{\boldsymbol{\alpha}}(I)$ together with the number of rows in $\mathcal{M}_{\boldsymbol{\beta}}(I^c)$ is $\#I + \#(I^c) = n$, and the result follows. □

Lemma F.41. *It holds that $\mathcal{B} \star \mathcal{A} \subseteq \mathcal{C}^\perp$.*

Proof. By Proposition F.11, item 2, we see that $\mathcal{B} \star \mathcal{A}$ is contained in the $\mathbb{F}_{q^n}$-linear code with generator matrix $\mathcal{M}_{\boldsymbol{\alpha}}(I + J)$. Denote such code by $\mathcal{D}$, that is, $\mathcal{B} \star \mathcal{A} \subseteq \mathcal{D}$ and $\mathcal{D} \subseteq \mathbb{F}_{q^n}^n$.

By definition, $\mathcal{C} = \mathcal{D}^\perp \cap \mathbb{F}_{q^m}^n$, and by [17, Corollary 3], $\mathcal{D}$ is Galois closed over $\mathbb{F}_{q^m}$, which means that $\mathcal{D}^\perp \cap \mathbb{F}_{q^m}^n = (\mathcal{D} \cap \mathbb{F}_{q^m}^n)^\perp$ by [18, Proposition 2] and Delsarte's theorem [5, Theorem 2]. Hence

$$\mathcal{B} \star \mathcal{A} \subseteq \mathcal{D} \cap \mathbb{F}_{q^m}^n = (\mathcal{D}^\perp \cap \mathbb{F}_{q^m}^n)^\perp = \mathcal{C}^\perp.$$

We may now prove that $(\mathcal{A}, \mathcal{B})$ is a t-rank error-locating pair of type I (see Remark F.20) for $\mathcal{C}$, and with some stronger hypotheses, it is also a t-rank error-correcting pair for $\mathcal{C}$.

Theorem F.5. *Fix a positive integer t and assume that $\#I > t$ and J contains $\delta - 1$ consecutive elements, for some $\delta > t$. Then $(\mathcal{A}, \mathcal{B})$ is a t-rank error-locating pair for $\mathcal{C}$. If moreover, $d_R(\mathcal{A}) + d_R(\mathcal{C}) > n$, then $(\mathcal{A}, \mathcal{B})$ is a t-rank error-correcting pair of type I for $\mathcal{C}$.*

Proof. From the previous lemma, we have that $\mathcal{B} \star \mathcal{A} \subseteq \mathcal{C}^\perp$. On the other hand, $\mathcal{A}$ satisfies that $\dim(\mathcal{A}) = \#I > t$, and $\mathcal{B}$ satisfies that $d_R(\mathcal{B}^\perp) \geq \delta > t$ by Lemma F.39. Then $(\mathcal{A}, \mathcal{B})$ is a t-rank error-locating pair of type I for $\mathcal{C}$. □

Observe that we may obtain the bound $d_R(\mathcal{C}) \geq \delta + w$ by Proposition F.29 assuming that I contains the elements ic, for $0 \leq i \leq w$. This means that, for q-cyclic codes constructed with a normal basis, the rank-HT bound found in [17, Corollary 4] is implied by Proposition F.29, as in the classical case. Further cases are left open.

Acknowledgement

Rank error-correcting pairs of type II have been obtained in the case $m = n$ independently by Alain Couvreur [3]. The authors wish to thank him for this communication and for useful discussions and comments.

The authors wish to thank the anonymous reviewers for their helpful comments and also gratefully acknowledge the support from The Danish Council for Independent Research (Grant No. DFF-4002-00367). This paper was started during the visit of the second author to Aalborg University, Denmark, which was supported by the previous grant.

References

[1] D. Boucher, W. Geiselmann, and F. Ulmer, “Skew-cyclic codes,” *Applicable Algebra in Engineering, Communication and Computing*, vol. 18, no. 4, pp. 379–389, 2007.

[2] L. Chaussade, P. Loidreau, and F. Ulmer, “Skew codes of prescribed distance or rank,” *Designs, Codes and Cryptography*, vol. 50, no. 3, pp. 267–284, 2009.

[3] A. Couvreur, “Personal communication,” 2015.

[4] P. Delsarte, “Bilinear forms over a finite field, with applications to coding theory,” *Journal of Combinatorial Theory, Series A*, vol. 25, no. 3, pp. 226 – 241, 1978.

[5] ——, “On subfield subcodes of modified reed-solomon codes (corresp.),” *IEEE Transactions Information Theory*, vol. 21, no. 5, pp. 575–576, Sep. 2006.

[6] I. Duursma and R. Kötter, "Error-locating pairs for cyclic codes," *IEEE Transactions on Information Theory*, vol. 40, no. 4, pp. 1108–1121, 1994.

[7] I. Duursma and R. Pellikaan, "A symmetric Roos bound for linear codes," *Journal of Combinatorial Theory, Series A*, vol. 113, no. 8, pp. 1677–1688, 2006.

[8] E. Gabidulin, "Theory of codes with maximum rank distance," *Problems Information Transmission*, vol. 21, 1985.

[9] ——, "Rank q-cyclic and pseudo-q-cyclic codes," in *IEEE International Symposium on Information Theory, 2009. ISIT 2009*, 2009, pp. 2799–2802.

[10] C. Hartmann and K. Tzeng, "Generalizations of the BCH bound," *Information and Control*, vol. 20, no. 5, pp. 489 – 498, 1972.

[11] R. Jurrius and R. Pellikaan, "The extended and generalized rank weight enumerator," 2014, aCA 2014, Applications of Computer Algebra, 9 July 2014, Fordham University, New York, Computer Algebra in Coding Theory and Cryptography.

[12] R. Jurrius and R. Pellikaan, "On defining generalized rank weights," *Advances in Mathematics of Communications*, vol. 11, no. 1, pp. 225–235, 2017.

[13] R. Kötter, "A unified description of an error locating procedure for linear codes," *Proceedings of Algebraic and Combinatorial Coding Theory*, pp. 113 – 117, 1992, voneshta Voda.

[14] A. Kshevetskiy and E. Gabidulin, "The new construction of rank codes," in *IEEE International Symposium on Information Theory, 2005. ISIT 2005*, 2005, pp. 2105–2108.

[15] R. Lidl and H. Niederreiter, *Finite Fields.* Amsterdam: Encyclopedia of Mathematics and its Applications. Addison-Wesley, 1983, vol. 20.

[16] P. Loidreau, "A Welch–Berlekamp like algorithm for decoding Gabidulin codes," in *Coding and Cryptography*, ser. Lecture Notes in Computer Science, y. Ytrehus, Ed. Springer Berlin Heidelberg, 2006, vol. 3969, pp. 36–45.

[17] U. Martínez-Peñas, "On the roots and minimum rank distance of skew cyclic codes," *Designs, Codes and Cryptography*, vol. 83, no. 3, pp. 639–660, 2017.

[18] U. Martínez-Peñas, "On the similarities between generalized rank and Hamming weights and their applications to network coding," *IEEE Trans. Inform. Theory*, vol. 62, no. 7, pp. 4081–4095, 2016.

[19] R. Pellikaan, “On decoding linear codes by error correcting pairs,” *Preprint. Eindhoven University of Technology*, 1988.

[20] ——, “On decoding by error location and dependent sets of error positions,” *Discrete Mathematics*, vol. 106, pp. 369–381, 1992.

[21] ——, “On the existence of error-correcting pairs,” *Journal of Statistical Planning and Inference*, vol. 51, no. 2, pp. 229 – 242, 1996, shanghai Conference Issue on Designs, Codes, and Finite Geometries, Part I.

[22] ——, “Rank-metric codes and their duality theory,” *Designs, Codes and Cryptography*, vol. 80, no. 1, pp. 197–216, 2016.

[23] C. Roos, “A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound,” *Journal Combinatorial Theory (Series A)*, vol. 33, pp. 229–232, 1982.

[24] ——, “A new lower bound for the minimum distance of a cyclic code,” *IEEE Transactions Information Theory*, vol. IT-29, pp. 330–332, 1982.

[25] D. Silva and F. Kschischang, “On metrics for error correction in network coding,” *IEEE Transactions Information Theory*, vol. 55, no. 12, pp. 5479–5490, 2009.

Paper G

Rank equivalent and rank degenerate skew cyclic codes

Umberto Martínez-Peñas[1]

The paper has been published in
Advances in Mathematics of Communications Vol. 11, No. 2, pp. 267–282, 2017,
and presented at the
Workshop on Mathematics in Communications, Santander, Spain, July 2016.

[1] Department of Mathematical Sciences, Aalborg University, Aalborg 9220, Denmark

Abstract

Two skew cyclic codes can be equivalent for the Hamming metric only if they have the same length, and only the zero code is degenerate. The situation is completely different for the rank metric. We study rank equivalences between skew cyclic codes of different lengths and, with the aim of finding the skew cyclic code of smallest length that is rank equivalent to a given one, we define different types of length for a given skew cyclic code, relate them and compute them in most cases. We give different characterizations of rank degenerate skew cyclic codes using conventional polynomials and linearized polynomials. Some known results on the rank weight hierarchy of cyclic codes for some lengths are obtained as particular cases and extended to all lengths and to all skew cyclic codes. Finally, we prove that the smallest length of a linear code that is rank equivalent to a given skew cyclic code can be attained by a pseudo-skew cyclic code.

Keywords: Cyclic codes, finite rings, linearized polynomial rings, rank degenerate, rank distance, rank equivalence, skew cyclic codes.

MSC: 15B33, 94B15, 94B65.

1 Introduction

Codes in the rank metric have numerous applications such as network coding [8, 11, 14]. Among these codes, cyclic codes and skew cyclic codes have been considered in [1, 2, 4–6, 10], since they have simple algebraic descriptions and fast encoding and decoding algorithms.

In the network coding model of [8, 11, 14], the length of a rank-metric code corresponds to the number of outgoing links from the source. Whereas it is obvious how to increase the length of a code and preserve at the same time its rank-metric properties, just by appending zeroes, it is not obvious whether a rank-metric code can be shortened (which would mean that it is degenerate) nor how. On the other hand, skew cyclic codes of smaller length have faster encoding and decoding algorithms.

In contrast with the Hamming-metric case, skew cyclic codes may be rank equivalent and have different lengths. The aim of this paper is to study rank equivalences between skew cyclic codes and in which way they can be rank degenerate.

Both problems have direct consequences on the generalized rank weights [8] of skew cyclic codes, which measure the information leakage by wiretapping links in the network, following the model of [8, 11, 14]. In particular, from our study we will obtain as particular cases the main results in [4], which we also extend to all parameters and all skew cyclic codes.

After some preliminaries in Section 2, the results in this paper are as follows: in Section 3, we define different types of length for skew cyclic codes, regarding the rank metric, and establish some inequalities between them. In Section 4, we use the polynomial description of the Galois closure of skew cyclic codes to compute most of the lengths defined in the previous section. In Section 5, we treat cyclic codes and relate their polynomial description to that of their Galois closures (by means of generator and check polynomials, idempotent generators and root sets), giving at the end several characterizations of rank degenerate cyclic codes and obtaining the results in [4] as particular cases. In Section 6, we proceed as in the previous section, but for general skew cyclic codes, using their linearized-polynomial description. Finally in Section 7, we see that, although the linear code of minimum length that is rank equivalent to a given skew cyclic code need not be skew cyclic, it may be chosen as pseudo-skew cyclic in many cases.

2 Definitions and preliminaries

Fix a prime power q and positive integers m and n, and let $\mathbb{F}_{q^s}$ denote the finite field with q^s elements for a positive integer s. A code $C \subseteq \mathbb{F}_{q^m}^n$ will be called linear if it is $\mathbb{F}_{q^m}$-linear. In general, linearity will mean $\mathbb{F}_{q^m}$-linearity. The number n is called the length of the code C.

We will denote the coordinate indices in $\mathbb{F}_{q^m}^n$ from 0 to $n-1$, and consider them as integers modulo n. Given a vector $\mathbf{c} \in \mathbb{F}_{q^m}^n$, we define its rank weight [5] as the dimension of the $\mathbb{F}_q$-linear vector space generated by its components. We denote it by $\mathrm{wt_R}(\mathbf{c})$.

Define the shifting operator $s_n : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$ as

$$s_n(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0, \ldots, c_{n-2}),$$

for every $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_{q^m}^n$. For any integer $r \geq 0$, define also the r-th Frobenius and q^r-shifting operators as $\theta_r, \sigma_{r,n} : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$, respectively, where θ_r acts by raising every component of a vector to the power q^r and $\sigma_{r,n} = \theta_r \circ s_n$.

Definition G.1. A code $C \subseteq \mathbb{F}_{q^m}^n$ is cyclic if $s_n(C) \subseteq C$, is q^r-cyclic (or skew cyclic of order r) if $\sigma_{r,n}(C) \subseteq C$, and is Galois closed (over $\mathbb{F}_q$) if $\theta_1(C) \subseteq C$.

Observe that cyclic codes are q^0-cyclic (or q^m-cyclic), that is, they are also skew cyclic. Skew cyclic codes were introduced in [5] for $r = 1$ and $n = m$, and then independently in [6] for $r = 1$ and in [1] for general parameters.

Denote $[i] = q^i$, for any integer $i \geq 0$. Following [15], for a given linear code $C \subseteq \mathbb{F}_{q^m}^n$, we define its Galois closure as $C^* = \sum_{i=0}^{m-1} C^{[i]}$, which is the smallest linear Galois closed space containing C, and we also define $C^0 = \bigcap_{i=0}^{m-1} C^{[i]}$, which is the biggest linear Galois closed space contained in C.

Recall from [15, Lemma 2] that $(C^\perp)^* = (C^0)^\perp$ and $(C^\perp)^0 = (C^*)^\perp$.

On the other hand, if $V \subseteq \mathbb{F}_{q^m}^n$ and $V' \subseteq \mathbb{F}_{q^m}^{n'}$ are linear Galois closed spaces, we say that a map $\phi : V \longrightarrow V'$ is a rank equivalence if it is a vector space isomorphism and $\mathrm{wt_R}(\phi(\mathbf{c})) = \mathrm{wt_R}(\mathbf{c})$, for all $\mathbf{c} \in V$. We say that two codes C and C' are rank equivalent if there exists a rank equivalence between linear Galois closed spaces V and V' that contain C and C', respectively. This definition of rank equivalent linear codes was introduced in [11, Definition 8].

By [11, Theorem 5], rank equivalent codes not only perform exactly in the same way regarding rank error and erasure correction, but also information leakage on networks (see [11, Remark 2]). Moreover, rank equivalences can be easily described, as the following lemma states, which is a particular case of [11, Theorem 5]:

Lemma G.2 ([11]). *A vector space isomorphism $\phi : V \longrightarrow V'$ between linear Galois closed spaces is a rank equivalence if, and only if, there exist $\beta \in \mathbb{F}_{q^m}^*$ and an $n \times n'$ matrix A over $\mathbb{F}_q$ that maps bijectively V to V' and such that*

$$\phi(\mathbf{c}) = \beta \mathbf{c} A,$$

for all $\mathbf{c} \in V$.

As in [11, Definition 9], we say that a linear code $C \subseteq \mathbb{F}_{q^m}^n$ is rank degenerate if it is rank equivalent to a linear code with smaller length.

3 Lengths and Galois closures

Following the model in [8, 11, 14], given a linear code $C \subseteq \mathbb{F}_{q^m}^n$, the length n represents the number of outgoing links of a network where C is implemented, whereas m represents the packet length. If C is rank equivalent to a code with length $n' \neq n$, then it may be implemented as a linear code in a network with n' outgoing links and with exactly the same performance [11]. However we may want to implement C as a skew cyclic code, and hence we need it to be rank equivalent to a skew cyclic code of length n'.

On the other hand, we may always increase their lengths preserving their rank-metric properties just by appending zeroes. This motivates the following definitions:

Definition G.3. Given a linear code $C \subseteq \mathbb{F}_{q^m}^n$, an element $a \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ and an integer $r \geq 0$, we define the following numbers:

1. The rank length, $l_R(C)$, as the minimum n' such that C is rank equivalent to a linear code of length n'.

2. The r-th skew length, $l_{Sk,r}(C)$, as the minimum n' such that C is rank equivalent to a linear skew cyclic code of order r and length n', if such a code exists. We define $l_{Sk,r}(C) = \infty$ otherwise.

3. The (a, r)-shift length, $l_{Sh,a,r}(C)$, as the minimum n' such that C is rank equivalent to a linear code of length n' by a rank equivalence ϕ such that $a(\sigma_{r,n'} \circ \phi) = \phi \circ \sigma_{r,n}$, if such a code exists. We define $l_{Sh,a,r}(C) = \infty$ otherwise.

4. The period length, $l_P(C)$, as the minimum integer $1 \leq p \leq n$ that generates the ideal modulo n defined as $\{p' \mid c_{i+p'} = c_i, \forall i, \forall (c_0, c_1, \ldots, c_{n-1}) \in C\}$, which necessarily divides n.

We also say that an integer $1 \leq p \leq n$ is an a-period of C if $c_{i+p} = ac_i$, for all $i = 0, 1, 2 \ldots, n-1$ and all $(c_0, c_1, \ldots, c_{n-1}) \in C$.

Remark G.4. *In the definition of $l_{Sh,a,r}(C)$, the rank equivalence ϕ that commutes with the q^r-shifting operators is supposed to be defined between linear Galois closed spaces that are cyclic, in order to make sense (see Lemma G.6 below).*

Remark G.5. *Assume that V and V' are linear cyclic Galois closed spaces. If a rank equivalence $\phi : V \longrightarrow V'$ satisfies that $a(\sigma_{r,n'} \circ \phi) = \phi \circ \sigma_{r,n}$, for some $r \geq 0$ and $a \in \mathbb{F}_q^*$, then*

$$\phi(\sigma_{s,n}(\mathbf{c})) = \beta(\sigma_{s,n}(\mathbf{c}))A = \beta^{1-[s-r]}(\beta\sigma_{r,n}(\mathbf{c})A)^{[s-r]} = \beta^{1-[s-r]}(\phi(\sigma_{r,n}(\mathbf{c})))^{[s-r]}$$

$$= \beta^{1-[s-r]}(a\sigma_{r,n'}(\phi(\mathbf{c})))^{[s-r]} = (\beta^{1-[s-r]}a)\sigma_{s,n'}(\phi(\mathbf{c})),$$

for all $\mathbf{c} \in V$, where A and β are as in Lemma G.2.

Hence, ϕ sends q^s-cyclic codes to q^s-cyclic codes, for any $s \geq 0$.

We have the following on the skew cyclic structure of linear Galois closed spaces:

Lemma G.6. *If $V \subseteq \mathbb{F}_{q^m}^n$ is linear and Galois closed, then it is skew cyclic of some order if, and only if, it is skew cyclic of all orders. Given a linear code $C \subseteq \mathbb{F}_{q^m}^n$, if it is skew cyclic of some order, then C^* and C^0 are skew cyclic (of all orders).*

Proof. Since $\theta_1(V) \subseteq V$, it holds that $\theta_r(V) = V$, for all $r \geq 0$. Hence, if we fix two integers $r, s \geq 0$, we have that $\sigma_{r,n}(V) \subseteq V$ if, and only if, $\sigma_{s,n}(V) \subseteq V$, and the first statement follows.

For the second statement, assume that C is q^r-cyclic. It holds that

$$\sigma_{r,n}(C^*) = \sum_{i=0}^{m-1} \sigma_{r,n}(C^{[i]}) = \sum_{i=0}^{m-1} \sigma_{r,n}(C)^{[i]} \subseteq \sum_{i=0}^{m-1} C^{[i]} = C^*,$$

and similarly for C^0, and we are done. □

By [11, Proposition 3], it follows that $l_R(C)$ is equal to the k-th generalized rank weight of C [8, Definition 2], for $k = \dim(C)$, which is the dimension of C^*:

$$l_R(C) = d_{R,k}(C) = \dim(C^*). \tag{G.1}$$

We may establish now the following relations between the different types of lengths:

Proposition G.7. *For any integers $r, s \geq 0$, a linear q^s-cyclic code $C \subseteq \mathbb{F}_{q^m}^n$ and an element $a \in \mathbb{F}_q^*$, it holds that*

1. $l_R(C) \leq l_{Sk,s}(C) \leq l_{Sh,a,r}(C)$.
2. $l_{Sh,1,r}(C) \leq l_P(C)$.
3. $l_R(C) = l_R(C^*)$, $l_{Sh,a,r}(C) = l_{Sh,a,r}(C^*)$ *and* $l_P(C) = l_P(C^*)$.
4. $l_{Sk,r}(C) \geq l_{Sk,r}(C^*) = l_R(C)$.

Proof. In item 1, the first inequality is trivial and the second one follows from Remark G.5.

To prove item 2, we see that puncturing in the first $l_P(C)$ coordinates gives a rank equivalence from C^* to a linear Galois closed subspace of $\mathbb{F}_{q^m}^{l_P(C)}$ that commutes with $\sigma_{r,n}$, and the inequality follows.

We now prove item 3. First, $l_R(C) = \dim(C^*) = \dim(C^{**}) = l_R(C^*)$ by (G.1). Now, if ϕ is a rank equivalence between C and a skew cyclic code C' such that $a(\sigma_{r,n'} \circ \phi) = \phi \circ \sigma_{r,n}$, then ϕ preserves Galois closures, and hence C^* is rank equivalent to C'^* by ϕ. It follows that $l_{Sh,a,r}(C) \geq l_{Sh,a,r}(C^*)$, being the reversed inequality obvious. On the other hand, it follows from the definitions that $l_P(C) = l_P(C^*)$.

Finally, item 4 is proven in the same way as the fact that $l_{Sh,a,r}(C) \geq l_{Sh,a,r}(C^*)$. The fact that $l_{Sk,r}(C^*) = l_R(C^*)$ follows from the definitions. □

Corollary G.8. *For any linear skew cyclic code $C \subseteq \mathbb{F}_{q^m}^n$ and any $i = R$, (Sk, r), (Sh, a, r), P, we have the following Singleton-type bounds:*

$$d_R(C) \leq l_i(C) - k + 1,$$

where d_R denotes the minimum rank distance.

Proof. The case $i = R$ follows from the classical Singleton bound [5] and the fact that there exists a linear code of length $l_R(C)$ that is rank equivalent to C. The rest of the bounds follow from this case and the previous proposition. □

4 Using the conventional-polynomial representation of Galois closures

It is well-known [7, Chapter 4] that a linear cyclic code $C \subseteq \mathbb{F}_{q^m}^n$ can be represented as an ideal $C(x)$ in the quotient ring $\mathbb{F}_{q^m}[x]/(x^n - 1)$, and it has unique polynomials $g(x), h(x) \in \mathbb{F}_{q^m}[x]$, called generator and check polynomials, respectively, such that $g(x)$ is monic and of minimal degree among those with residue class in $C(x)$, and $g(x)h(x) = x^n - 1$. Moreover, $g(x)$ generates $C(x)$.

There are two more descriptions of linear cyclic codes. If $g(x)$ and $h(x)$ are coprime (which holds if q and n are coprime), then there exists a unique idempotent polynomial $e(x) \in C(x)$ (that is, $e(x)^2 = e(x)$ in $\mathbb{F}_{q^m}[x]/(x^n - 1)$) that generates $C(x)$ [7, Theorem 4.3.2].

On the other hand, for a given polynomial $f(x) \in \mathbb{F}_{q^m}[x]$, let $Z(f(x))$ denote the set of its roots in its splitting field. If q and n are coprime, then we may associate C with the root set $Z(g(x))$. This gives a bijective correspondence between linear cyclic codes in $\mathbb{F}_{q^m}^n$ and root sets of divisors of $x^n - 1$ [7, Section 4.4].

In this section we will focus on this conventional-polynomial representation of linear cyclic codes (in contrast with the linearized-polynomial representation in the following sections), which may be used for the Galois closure of any linear skew cyclic code by Lemma G.6.

Observe that the r-th Frobenius map θ_r induces a ring automorphism $\theta_r : \mathbb{F}_{q^m}[x] \longrightarrow \mathbb{F}_{q^m}[x]$ given by

$$\theta_r(f_0 + f_1 x + \cdots + f_d x^d) = f_0^{[r]} + f_1^{[r]} x + \cdots + f_d^{[r]} x^d, \qquad \text{(G.2)}$$

for all $f_0 + f_1 x + \cdots + f_d x^d \in \mathbb{F}_{q^m}[x]$. Since $\theta_r(x^n - 1) = x^n - 1$, it induces a ring automorphism of the quotient ring $\mathbb{F}_{q^m}[x]/(x^n - 1)$.

Recall from [7, Exercise 243] that, again if $g(x)$ and $h(x)$ are coprime, then there exists a unique linear cyclic code C^c such that $C \oplus C^c = \mathbb{F}_{q^m}^n$, called the cyclic complementary code of C. Its generator and check polynomials are $h(x)$ and $g(x)$, respectively, its idempotent generator is $1 - e(x)$ and its root set is $Z(h(x)) = Z(x^n - 1) \setminus Z(g(x))$.

We have the following expected characterizations:

Lemma G.9. *Given a linear cyclic code $C \subseteq \mathbb{F}_{q^m}^n$ as in the beginning of this section, the following are equivalent:*

1. *C is Galois closed.*
2. *$g(x) \in \mathbb{F}_q[x]$.*
3. *$h(x) \in \mathbb{F}_q[x]$.*
4. *(If $g(x)$ and $h(x)$ are coprime) $e(x) \in \mathbb{F}_q[x]$.*

5. *(If q and n are coprime) $Z(g(x))^q = Z(g(x))$.*

6. *(If $g(x)$ and $h(x)$ are coprime) C^c is Galois closed.*

Proof. It is enough to note the following:

1. $\theta_1(C)$ has $\theta_1(g(x))$ as generator polynomial, since it generates $\theta_1(C)(x)$ and θ_1 preserves monic polynomials and degrees. Hence the equivalence between items 1 and 2 follows.

2. $\theta_1(C)$ has $\theta_1(h(x))$ as check polynomial, by the fact that $x^n - 1 = \theta_1(x^n - 1) = \theta_1(g(x))\theta_1(h(x))$ and the previous item in this proof. Hence the equivalence between items 1 and 3 follows.

3. If $g(x)$ and $h(x)$ are coprime, then $\theta_1(C)$ has $\theta_1(e(x))$ as idempotent generator, since $\theta_1(e(x))$ is again idempotent, generates $\theta_1(C)(x)$ and the idempotent generator is unique [7, Theorem 4.3.2]. Hence the equivalence between items 1 and 4 follows.

4. If q and n are coprime, then $\theta_1(C)$ corresponds to the root set $Z(g(x))^q$, since $Z(\theta_1(g(x))) = Z(g(x))^q$. Hence the equivalence between items 1 and 5 follows.

Finally, the equivalence between items 1 and 6 follows from the fact that $h(x)$ and $g(x)$ are the generator and check polynomials of C^c, respectively. □

We now characterize rank equivalences that commute with the q^r-shifting operators in terms of generator matrices. For a matrix X over $\mathbb{F}_{q^m}$ with n columns, we define $\sigma_{r,n}(X)$ as the matrix such that its i-th row is the q^r-shifted i-th row of X.

Recall from [15, Lemma 1] that linear Galois closed spaces are those with a basis of vectors in $\mathbb{F}_q^n$, that is, a generator matrix with coefficients in $\mathbb{F}_q$.

Proposition G.10. *For linear cyclic Galois closed spaces $V \subseteq \mathbb{F}_{q^m}^n$ and $V' \subseteq \mathbb{F}_{q^m}^{n'}$, and a rank equivalence $\phi : V \longrightarrow V'$, where we define β and A as in Lemma G.2, the following are equivalent for a given $a \in \mathbb{F}_q^*$ and $r \geq 0$:*

1. *$a(\sigma_{r,n'} \circ \phi) = \phi \circ \sigma_{r,n}$.*

2. *If G is a generator matrix of V, then $\sigma_{r,n}(G)A = a\beta^{[r]-1}\theta_r(G)s_{n'}(A)$.*

In particular, choosing G with coefficients in $\mathbb{F}_q$, the second item reads $s_n(G)A = a\beta^{[r]-1}Gs_{n'}(A)$. Therefore, if any of the previous items hold, then $\beta^{[r]-1} = b \in \mathbb{F}_q^*$.

On the other hand, the check polynomials of V and V' can be easily used to see whether there exists such a rank equivalence between them, which is the first main result of this section:

Theorem G.1. *Let $V \subseteq \mathbb{F}_{q^m}^n$ and $V' \subseteq \mathbb{F}_{q^m}^{n'}$ be linear cyclic Galois closed spaces with the same dimension k and check polynomials $h(x)$ and $h'(x)$, respectively. Given $a \in \mathbb{F}_q^*$, an integer $r \geq 0$ and $\beta \in \mathbb{F}_{q^m}^*$ such that $\beta^{[r]} = b\beta$, for some $b \in \mathbb{F}_q^*$, the following are equivalent:*

1. *There exists a rank equivalence $\phi : V \longrightarrow V'$ such that $a(\sigma_{r,n'} \circ \phi) = \phi \circ \sigma_{r,n}$ and β is as in Lemma G.2.*

2. *$(ab)^k h'(x) = h(abx)$.*

Proof. We first prove that item 1 implies item 2. Let $h(x) = h_0 + h_1 x + \cdots + h_k x^k$. Assume that there exists a rank equivalence $\phi : V \longrightarrow V'$ satisfying item 1. Let $g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$ be the generator polynomial of V, and let $\mathbf{g} = (g_0, g_1, \ldots, g_{n-k}, 0, \ldots, 0) \in \mathbb{F}_q^n$. Define $f(x) = f_0 + f_1 x + \cdots + f_{n-1} x^{n-1} \in \mathbb{F}_{q^m}[x]$ such that $\mathbf{f} = (f_0, f_1, \ldots, f_{n-1}) = \phi(\mathbf{g})$. By Lemma G.2, we have that $f(x) = \beta \widetilde{f}(x)$, for some $\widetilde{f}(x) \in \mathbb{F}_q[x]$.

It holds that $a^i \sigma_{r,n'}^i(\mathbf{f}) = \phi(\sigma_{r,n}^i(\mathbf{g}))$, for $i = 0, 1, 2, \ldots, k$. In polynomial representation, we have that $\sigma_{r,n}^i(\mathbf{g})$ corresponds to $x^i g(x)$, and $x^k g(x) = \sum_{i=0}^{k-1} -h_i x^i g(x)$. On the other hand, $\sigma_{r,n'}^i(\mathbf{f})$ corresponds to $x^i \theta_r^i(f(x)) = x^i \beta^{[ir]} \widetilde{f}(x) = x^i b^i \beta \widetilde{f}(x)$. Hence $x^k a^k b^k \widetilde{f}(x) = \sum_{i=0}^{k-1} -h_i a^i b^i x^i \widetilde{f}(x)$. In other words, $h(abx)\widetilde{f}(x) = 0$.

On the other hand, the vectors $\sigma_{r,n'}^i(\mathbf{f}) = a^{-i}\phi(\sigma_{r,n}^i(\mathbf{g}))$, $i = 0, 1, \ldots, k-1$, constitute a basis of V', which implies that $\widetilde{f}(x), x\widetilde{f}(x), \ldots, x^{k-1}\widetilde{f}(x)$ constitute a basis of $V'(x)$. Hence, $\widetilde{f}(x)$ generates the ideal $V'(x)$. Since $h(abx)\widetilde{f}(x) = 0$, we conclude by degrees that $h(abx) = (ab)^k h'(x)$, and we are done.

Now we prove that item 2 implies item 1. Let $\mathbf{g}' = (g_0', g_1', \ldots, g_{n'-k}', 0, \ldots, 0) \in \mathbb{F}_{q^m}^{n'}$ by such that $g'(x) = g_0' + g_1' x + \cdots + g_{n'-k}' x^{n'-k}$ is the generator polynomial of V'. We just need to define ϕ by the formula

$$\phi(\sigma_{r,n}^i(\mathbf{g})) = a^i \sigma_{r,n'}^i(\beta \mathbf{g}') = (a^i b^i)\beta \sigma_{r,n'}^i(\mathbf{g}'), \tag{G.3}$$

for $i = 0, 1, 2, \ldots, k-1$, which defines a rank equivalence between V and V' by Lemma G.2, and see that this formula also holds for $i = k$. If that happens, then the equality $a(\sigma_{r,n'} \circ \phi) = \phi \circ \sigma_{r,n}$ holds on a basis of V and then it holds on all V.

To see that Equation (G.3) also holds for $i = k$, we may argue as in the converse implication by using again that $(ab)^k h'(x) = h(abx)$. □

On the other hand, given a polynomial $f(x) \in \mathbb{F}_{q^m}[x]$, we define its order as the minimum positive integer e such that $f(x)$ divides $x^e - 1$ (in $\mathbb{F}_{q^m}[x]$), and denote it by $\mathrm{ord}(f(x))$. In general, for $a \in \mathbb{F}_q$, we define the a-order of $f(x)$ as the minimum positive integer e such that $f(x)$ divides $x^e - a^e$ (in

$\mathbb{F}_{q^m}[x]$), if one such e exists, and denote it by $\mathrm{ord}_a(f(x))$. If no such e exists, we define $\mathrm{ord}_a(f(x)) = \infty$.

We may now prove the second main result of this section:

Theorem G.2. *For an integer $s \geq 0$ and a linear q^s-cyclic code $C \subseteq \mathbb{F}_{q^m}^n$, where $h^0(x)$ is the check polynomial of C^*, it holds that*

1. $l_R(C) = \deg(h^0(x))$.
2. $l_{Sh,1,0}(C) = l_P(C) = \mathrm{ord}(h^0(x)) \leq n$.
3. *More generally, if $a \in \mathbb{F}_q^*$, then $e = l_{Sh,a,0}(C) = \mathrm{ord}_a(h^0(x))$ and e is an a^e-period of C.*
4. *More generally, if $a \in \mathbb{F}_q^*$ and $r \geq 0$, then*

$$l_{Sh,a,r}(C) = \min\{\mathrm{ord}_{ab}(h^0(x)) \mid b \in \mathbb{F}_q^*, \beta \in \mathbb{F}_{q^m}^*, \beta^{[r]} = b\beta\}.$$

In particular, $l_R(C) = l_{Sk,s}(C) = l_{Sh,1,r}(C) = l_P(C)$ if, and only if, $\deg(h^0(x)) = \mathrm{ord}(h^0(x))$, which holds if, and only if, $h^0(x) = x^e - 1$, for some positive integer e.

Proof. First of all, we have seen that $l_R(C) = \dim(C^*)$, and this dimension is $\deg(h^0(x))$. Hence item 1 follows.

Now, the equality $l_{Sh,1,0}(C) = \mathrm{ord}(h^0(x))$ in item 2 follows from item 3 by choosing $a = 1$, and it is straightforward to see that $\mathrm{ord}(h^0(x))$ is equal to $l_P(C)$.

Item 3 follows now from item 4, since $\beta^{[0]} = \beta$, for all $\beta \in \mathbb{F}_{q^m}$. Moreover, since $x^e f(x) = a^e f(x)$, for all $f(x) \in C(x)$, we see that e is an a^e-period of C.

Next we prove item 4. Assume that there exists a rank equivalence $\phi : C^* \longrightarrow V'$, where V' is a linear cyclic Galois closed space of length e and $a(\sigma_{r,n'} \circ \phi) = \phi \circ \sigma_{r,n}$. By the previous theorem, the check polynomial of V' is $(ab)^{-k} h^0(abx)$, $k = \dim(C^*)$, with notation as in the previous theorem. Hence, we see that $h^0(x)$ divides $x^e - (ab)^e$, since $h^0(abx)$ divides $x^e - 1$.

Conversely, if $h^0(x)$ divides $x^e - (ab)^e$, we may define the linear cyclic Galois closed space $V' \subseteq \mathbb{F}_{q^m}^e$ with check polynomial $h'(x) = (ab)^{-k} h^0(abx)$, which divides $x^e - 1$. Then there exists a rank equivalence $\phi : C^* \longrightarrow V'$ as before by the previous theorem.

Therefore, choosing the elements b and β that minimize the number e, we see that $l_{Sh,a,r}(C) = \mathrm{ord}_{ab}(h^0(x))$, and item 4 follows.

Finally, by Proposition G.7, we conclude that $l_R(C) = l_{Sk,s}(C) = l_{Sh,1,r}(C) = l_P(C)$ if, and only if, $\deg(h^0(x)) = \mathrm{ord}(h^0(x))$. It is straightforward to see that this is equivalent to $h^0(x) = x^e - 1$, $e = \mathrm{ord}(h^0(x))$. □

In the next sections we will give results on C in terms of its structure, and relate it to the structure of C^* and C^0.

5 Cyclic codes, conventional polynomials and root sets

Given a polynomial $f(x) \in \mathbb{F}_{q^m}[x]$, we define the following polynomials, where divisibility is considered in $\mathbb{F}_{q^m}[x]$:

$$f^*(x) = \gcd(f(x), \theta_1(f(x)), \ldots, \theta_{m-1}(f(x))), \tag{G.4}$$

$$f^0(x) = \mathrm{lcm}(f(x), \theta_1(f(x)), \ldots, \theta_{m-1}(f(x))), \tag{G.5}$$

$$f^{\perp}(x) = x^{\deg(f(x))} f(x^{-1}) / f(0), \tag{G.6}$$

assuming $f(0) \neq 0$ in the last equation. We have the following:

Lemma G.11. *For any polynomial $f(x) \in \mathbb{F}_{q^m}[x]$, it holds that $f^*(x), f^0(x) \in \mathbb{F}_q[x]$.*

Proof. Since θ_1 leaves the set $\{f(x), \theta_1(f(x)), \ldots, \theta_{m-1}(f(x))\}$ invariant and is a ring automorphism, it holds that $\theta_1(f^*(x)) = f^*(x)$ and $\theta_1(f^0(x)) = f^0(x)$, which mean that both lie in $\mathbb{F}_q[x]$. □

Now fix a linear cyclic code $C \subseteq \mathbb{F}_{q^m}^n$, whose generator and check polynomials are $g(x)$ and $h(x)$, respectively. It is well-known that $h^{\perp}(x)$ and $g^{\perp}(x)$ are the generator and check polynomials of $C^{\perp}$, respectively [7, Theorem 4.2.7]. The following proposition explains the previous notation:

Proposition G.12. *The generator and check polynomials of C^* are $g^*(x)$ and $h^0(x)$, respectively, and the generator and check polynomials of C^0 are $g^0(x)$ and $h^*(x)$, respectively. In particular,*

$$(g^*)^{\perp}(x) = (g^{\perp})^*(x), \quad (g^0)^{\perp}(x) = (g^{\perp})^0(x),$$

$$(h^*)^{\perp}(x) = (h^{\perp})^*(x), \quad \textit{and} \quad (h^0)^{\perp}(x) = (h^{\perp})^0(x).$$

Proof. Taking ideals, it holds that $C(x) = \sum_{i=0}^{m-1} C^{[i]}(x)$, and $C^{[i]}$ has $\theta_i(g(x))$ as generator polynomial. It is well-known that the generator polynomial of the sum of cyclic codes is the greatest common divisor of their generator polynomials [7, Theorem 4.3.7].

Hence the polynomial $g^*(x)$ is the generator polynomial of C^*. Similarly $g^0(x)$ is the generator polynomial of C^0, using now that the generator polynomial of the intersection of cyclic codes is the least common multiple of their generator polynomials [7, Theorem 4.3.7].

On the other hand, we have that $\theta_i(g(x))\theta_i(h(x)) = \theta_i(x^n - 1) = x^n - 1$, for $i = 0, 1, 2, \ldots, m-1$. Hence the greatest common divisor of the polynomials $\theta_i(g(x))$ and the least common multiple of the polynomials $\theta_i(h(x))$

satisfy the same. That is, $g^*(x)h^0(x) = x^n - 1$, and $h^0(x)$ is the check polynomial of C^*. Similarly for C^0.

Finally, since $g^\perp(x)$ is the check polynomial of $C^\perp$, it follows that $(g^\perp)^*(x)$ is the check polynomial of $(C^\perp)^0$. On the other hand, since $g^*(x)$ is the generator polynomial of C^*, it holds that $(g^*)^\perp(x)$ is the check polynomial of $(C^*)^\perp$. Since $(C^\perp)^0 = (C^*)^\perp$, it follows that $(g^*)^\perp(x) = (g^\perp)^*(x)$. The remaining equalities are proven in the same way. □

On the other hand, we have the following relations of idempotent generators and cyclic complementaries.

Proposition G.13. *Assume that $g(x)$ and $h(x)$ are coprime and $e(x)$ is the idempotent generator of C. Then C^* and C^0 have $1 - \prod_{i=0}^{m-1}(1 - \theta_i(e(x)))$ and $\prod_{i=0}^{m-1} \theta_i(e(x))$ as idempotent generators, respectively. Moreover it holds that*

$$(C^c)^* = (C^0)^c \quad \textit{and} \quad (C^c)^0 = (C^*)^c.$$

Proof. First, the idempotent generator of the intersection of cyclic codes is the product of their idempotent generators [7, Theorem 4.3.7], hence $\prod_{i=0}^{m-1} \theta_i(e(x))$ is the idempotent generator of C^0.

On the other hand, C^c has $h(x)$ as generator polynomial, thus $(C^c)^*$ has $h^*(x)$ as generator polynomial by the previous proposition. Moreover, C^0 has $h^*(x)$ as check polynomial, also by the previous proposition. Therefore $(C^c)^* = (C^0)^c$. Similarly we may prove that $(C^c)^0 = (C^*)^c$.

Finally, It holds that $\prod_{i=0}^{m-1}(1 - \theta_i(e(x)))$ is the idempotent generator of $(C^c)^0$ by the first part of this proof. Using that $(C^c)^0 = (C^*)^c$, we see that $1 - \prod_{i=0}^{m-1}(1 - \theta_i(e(x)))$ is the idempotent generator of C^*. □

We will now relate C, C^* and C^0 by means of the defining root set of C. We will relate $l_R(C^\perp)$ with the parameter $\eta_q(C)$ introduced in [4], which will allow us to easily derive the main results in that paper.

If q and n are coprime, let $m' \geq m$ be such that $\mathbb{F}_{q^{m'}}$ is the splitting field of $g(x)$. Let $\alpha_1, \alpha_2, \ldots, \alpha_{n-k} \in \mathbb{F}_{q^{m'}}$ be the simple roots of $g(x)$, and assume that they are ordered in the following way: there exist $1 = m_0 < m_1 < m_2 < \ldots < m_t = n - k + 1$ such that $\alpha_{m_i}, \alpha_{m_i+1}, \ldots, \alpha_{m_{i+1}-1}$ are roots of the minimal polynomial $\mu_i(x) \in \mathbb{F}_q[x]$ of α_{m_i} over $\mathbb{F}_q$, for $i = 0, 1, \ldots, t-1$.

Definition G.14 ([4, Definition 3, Definition 4]). With notation as in the previous paragraph, we define

$$\mu_q(g(x)) = \prod_{i=0}^{t-1} \mu_r(x) \in \mathbb{F}_q[x] \quad \text{and} \quad \eta_q(C) = \deg(\mu_q(g(x))).$$

We have the following relations, which in particular compute the root sets corresponding to C^* and C^0:

Proposition G.15. *If q and n are coprime, then*

1. $\mu_q(g(x)) = g^0(x)$.
2. $Z(g^0(x)) = \bigcup_{i=0}^{m-1} Z(g(x))^{[i]}$ *and* $Z(g^*(x)) = \bigcap_{i=0}^{m-1} Z(g(x))^{[i]}$.
3. $\eta_q(C) = \deg(g^0(x)) = \dim((C^\perp)^*)$ *and* $\deg(g^*(x)) = \dim((C^\perp)^0)$.

Analogous identities hold replacing $g(x)$, $g^*(x)$ and $g^0(x)$ by $h(x)$, $h^*(x)$ and $h^0(x)$, respectively.

Proof. First, $g(x)$ divides $\mu_q(g(x))$ in $\mathbb{F}_{q^{m'}}[x]$ by looking at their roots. By the same argument as in Lemma G.9, we see that $g(x)$ divides $\mu_q(g(x))$ in $\mathbb{F}_{q^m}[x]$.

Fix a positive integer r. Since θ_r is a ring isomorphism, we see that $\theta_r(g(x))$ also divides $\theta_r(\mu_q(g(x))) = \mu_q(g(x))$ in $\mathbb{F}_{q^m}[x]$. Hence $\mu_q(g(x))$ is divisible by the least common multiple of the polynomials $\theta_r(g(x))$, $r = 0, 1, 2, \ldots, m-1$.

Finally, since the Galois group of the extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^{m'}}$ is constituted by the maps θ_r, we see that the previous least common multiple vanishes at the roots of the polynomials $\mu_i(x)$, for $i = 0, 1, \ldots, t-1$. Hence it holds that $\mu_q(g(x)) = \mathrm{lcm}(g(x), \theta_1(g(x)), \ldots, \theta_{m-1}(g(x))) = g^0(x)$ and item 1 follows.

By the same discussion, since $Z(\theta_i(g(x))) = Z(g(x))^{[i]}$, we have that $Z(g^0(x)) = \bigcup_{i=0}^{m-1} Z(g(x))^{[i]}$. On the other hand, denoting $Z = Z(x^n - 1)$ and using that $g^*(x)h^0(x) = g(x)h(x) = x^n - 1$, we have that $Z(g^*(x))$ is equal to:

$$Z \setminus Z(h^0(x)) = Z \setminus \left(\bigcup_{i=0}^{m-1} Z(h(x))^{[i]} \right) = \bigcap_{i=0}^{m-1} (Z \setminus Z(h(x)))^{[i]} = \bigcap_{i=0}^{m-1} Z(g(x))^{[i]},$$

and item 2 follows. Item 3 follows from item 1 and Proposition G.12. □

Remark G.16. *Hence $C^\perp$ is rank degenerate if, and only if, $\eta_q(C) < n$, which by the duality theorem for generalized rank weights [3, Theorem] is equivalent to $d_R(C) = 1$ (see [3] for more details). Hence [4, Proposition 2] and [4, Proposition 3] follow. We have actually proven that*

$$\eta_q(C) = l_R(C^\perp), \tag{G.7}$$

which combined with the same duality theorem also implies [4, Proposition 5]. Moreover, together with Corollary G.8 we obtain [4, Proposition 6].

We may now state the main result of this section, which computes lengths of cyclic codes in terms of their intrinsic structure:

Theorem G.3. *It holds that*

$$l_R(C) = n - \deg(\gcd(g(x), \theta_1(g(x)), \ldots, \theta_{m-1}(g(x))))$$

$$= \deg(\mathrm{lcm}(h(x), \theta_1(h(x)), \ldots, \theta_{m-1}(h(x)))),$$

and if q and n are coprime, then

$$l_R(C) = \eta_q(C^\perp) = n - \# \left(\bigcap_{i=0}^{m-1} Z(g(x))^{[i]} \right) = \# \left(\bigcup_{i=0}^{m-1} Z(h(x))^{[i]} \right).$$

On the other hand, for $a \in \mathbb{F}_q^*$, it holds that

$$l_{Sh,a,0}(C) = \mathrm{ord}_a(h^0(x)) = \mathrm{ord}_a(h(x)) = \mathrm{ord}_a(\mu_q(h(x)))$$

$$= \min\{e \mid \alpha^e = a^e, \forall \alpha \in Z(h(x))\}.$$

Proof. The first two equalities follow from Theorem G.2, item 1, and Proposition G.12. If q and n are coprime, then the next three equalities follow from the same results as before together with Proposition G.15 and Equation (G.7). Finally, the last four equalities follow from the same results as before together with Theorem G.2, items 2 and 3. □

The following characterizations of rank degenerate cyclic codes follow:

Corollary G.17. *The following conditions are equivalent:*

1. *C is rank degenerate. That is, $l_R(C) < n$.*
2. $\gcd(g(x), \theta_1(g(x)), \ldots, \theta_{m-1}(g(x))) \neq 1$.
3. $\mathrm{lcm}(h(x), \theta_1(h(x)), \ldots, \theta_{m-1}(h(x))) \neq x^n - 1$.
4. *(If $g(x)$ and $h(x)$ are coprime) $\prod_{i=0}^{m-1}(1 - \theta_i(e(x)))) = 0$ in $\mathbb{F}_{q^m}[x]/(x^n - 1)$, where $e(x)$ is the idempotent generator of C.*
5. *(If q and n are coprime) $\eta_q(C^\perp) < n$.*
6. *(If q and n are coprime) $\bigcap_{i=0}^{m-1} Z(g(x))^{[i]} \neq \emptyset$.*
7. *(If q and n are coprime) $\bigcup_{i=0}^{m-1} Z(h(x))^{[i]} \subsetneq Z(x^n - 1)$.*

6 Skew cyclic codes, linearized polynomials and root spaces

In this section we will fix a positive integer r and assume that m divides rn, and will use the linearized-polynomial description of skew cyclic codes given in [1, 5, 6, 10] to give similar characterizations of lengths and rank degenerateness as in the previous section for general skew cyclic codes. By the discussion after [10, Subsection 2.5], assuming that m divides rn does not leave any skew cyclic code out of study regarding the lengths $l_i(C)$.

Denote by $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ the ring of q^r-linearized polynomials over $\mathbb{F}_{q^m}$ (see [5, 12, 13] or [9, Chapter 3]), that is, polynomials of the form

$$F(x) = F_0 x + F_1 x^{[r]} + F_2 x^{[2r]} + \cdots + F_d x^{[dr]},$$

where $F_0, F_1, F_2, \ldots, F_d \in \mathbb{F}_{q^m}[x]$, and where we consider composition of maps $\otimes$ as product. We also define the q^r-degree of $F(x)$ as $\deg_{q^r}(F(x)) = d$ if $F_d \neq 0$.

Recall that q^r-linearized polynomials over $\mathbb{F}_{q^m}$ define $\mathbb{F}_{q^r}$-linear maps between field extensions of $\mathbb{F}_{q^r}$ and their compositions as such define again q^r-linearized polynomials over $\mathbb{F}_{q^m}$. This ring constitutes an Euclidean domain on the right and on the left [5, 12, 13], but we will always consider divisibility on the right. We will also use the term “conventional” to refer to the usual product and divisibility of polynomials.

Since m divides rn, $x^{[rn]} - x$ commutes with every other q^r-linearized polynomial over $\mathbb{F}_{q^m}$ and the left ideal $(x^{[rn]} - x)$ is two-sided. Thus, we may consider the ring $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$, which is isomorphic to $\mathbb{F}_{q^m}^n$ as a vector space.

Linear q^r-cyclic codes correspond to left ideals in $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$ [1, 5, 6]. Fix one $C \subseteq \mathbb{F}_{q^m}^n$. It has unique generator polynomial $G(x)$ and check polynomial $H(x)$ with the same properties as in the usual case [1, 6, 10]: $G(x)$ is of minimal degree and monic, and $x^{[rn]} - x = G(x) \otimes H(x) = H(x) \otimes G(x)$.

For a given $F(x) \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$, we will also write $F = F(x) + (x^{[rn]} - x)$, the residue class of $F(x)$ modulo $x^{[rn]} - x$. Recall that, since q^r-linearized polynomials induce $\mathbb{F}_{q^r}$-linear maps, their root sets are $\mathbb{F}_{q^r}$-linear vector spaces. We may denote by $Z(F)$ the $\mathbb{F}_{q^r}$-linear space of zeroes in $\mathbb{F}_{q^{rn}}$ of $F(x) \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$. This definition is consistent, since two q^r-polynomials $F_1(x)$ and $F_2(x)$ have the same roots in $\mathbb{F}_{q^r}$ if $F_1(x) - F_2(x) \in (x^{[rn]} - x)$.

On the other hand, the s-th Frobenius map θ_s defines also a ring automorphism $\theta_s : \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x] \longrightarrow \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ using the same formula as in the conventional case (G.2) and induces a ring automorphism of $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$, since $\theta_r(x^{[rn]} - x) = x^{[rn]} - x$.

In this section we will consider the q^r-cyclic structure of linear Galois closed spaces. However, describing generator and check polynomials of $C^\perp$, C^* and C^0 is not as straightforward as in the conventional case. Given a q^r-polynomial $F(x) = F_0 x + F_1 x^{[r]} + \cdots + F_d x^{[rd]} \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ that divides $x^{[rn]} - x$, with $F_d \neq 0$, we define:

$$F^\perp(x) = \left(\frac{F_d}{F_0^{[dr]}} \right) x + \left(\frac{F_{d-1}^{[r]}}{F_0^{[dr]}} \right) x^{[r]} + \cdots + \left(\frac{F_0^{[dr]}}{F_0^{[dr]}} \right) x^{[dr]}, \tag{G.8}$$

$$F^\top(x) = \left(\frac{F_d}{F_0} \right)^{[(n-d)r]} x + \left(\frac{F_{d-1}}{F_0} \right)^{[(n-d+1)r]} x^{[r]} + \cdots + \left(\frac{F_0}{F_0} \right)^{[nr]} x^{[dr]}, \tag{G.9}$$

$$F^*(x) = \gcd(F(x), \theta_1(F(x)), \ldots, \theta_{m-1}(F(x))), \tag{G.10}$$

$$F^0(x) = \operatorname{lcm}(F(x), \theta_1(F(x)), \ldots, \theta_{m-1}(F(x))), \tag{G.11}$$

$$F_*(x) = \gcd(F(x)^\perp, \theta_1(F(x))^\perp, \ldots, \theta_{m-1}(F(x))^\perp)^\top, \tag{G.12}$$

$$F_0(x) = \operatorname{lcm}(F(x)^\perp, \theta_1(F(x))^\perp, \ldots, \theta_{m-1}(F(x))^\perp)^\top. \tag{G.13}$$

As in the previous section, we have the following:

Lemma G.18. *For any q^r-polynomial $F(x) \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$, it holds that $F^*(x)$, $F^0(x)$, $F_*(x)$, $F_0(x) \in \mathcal{L}_{q^r}\mathbb{F}_q[x]$.*

Proof. Since θ_1 leaves the set $\{F(x), \theta_1(F(x)), \ldots, \theta_{m-1}(F(x))\}$ invariant and is a ring automorphism, it holds that $\theta_1(F^*(x)) = F^*(x)$ and $\theta_1(F^0(x)) = F^0(x)$. Observing that $\theta_1(F^\perp(x)) = \theta_1(F(x))^\perp$ and $\theta_1(F^\top(x)) = \theta_1(F(x))^\top$, we see that $\theta_1(F_*(x)) = F_*(x)$ and $\theta_1(F_0(x)) = F_0(x)$. Hence the result follows. □

Before going on, we will establish a result analogous to Proposition G.9. In the linearized case, if $G(x)$ and $H(x)$ are coprime on both sides, then there exist an idempotent generator $E(x)$ of C by [10, Theorem 4], and the linear skew cyclic code with generator and check polynomials $H(x)$ and $G(x)$, respectively, is a complementary space of C by [10, Corollary 4]. We denote it by C^c. It also has an idempotent generator given by $x - E(x)$ [10, Corollary 4].

Proposition G.19. *The following are equivalent:*

1. *C is Galois closed.*

2. *$G(x) \in \mathcal{L}_{q^r}\mathbb{F}_q[x]$.*

3. *$H(x) \in \mathcal{L}_{q^r}\mathbb{F}_q[x]$.*

4. *$Z(G) \subseteq \mathbb{F}_{q^{rn}}$ is an ($\mathbb{F}_{q^r}$-linear) Galois closed space over $\mathbb{F}_q$. That is, $Z(G)^q = Z(G)$ (also called q-modulus in [9, Chapter 3]).*

5. *(If $G(x)$ and $H(x)$ are coprime on both sides) $E(x) \in \mathbb{F}_q[x]$.*

6. *(If $G(x)$ and $H(x)$ are coprime on both sides) C^c is Galois closed.*

Proof. Analogous to that of Proposition G.9. □

It is proven in [2, 5, 6] that $H^\perp(x)$ is the generator polynomial of $C^\perp$. We now find its check polynomial:

Lemma G.20. *The check polynomial of $C^\perp$ is $G^\top(x)$.*

Proof. Let $\widetilde{G}(x) = \widetilde{G}_0 x + \widetilde{G}_1 x^{[r]} + \cdots + \widetilde{G}_{n-k} x^{[(n-k)r]}$ be the check polynomial of $C^\perp$. It is shown in [2] that $C^\perp$ has a parity check matrix of the form

$$\begin{pmatrix} G_0 & G_1 & \ldots & G_{n-k} & 0 & \ldots & 0 \\ 0 & G_0^{[r]} & \ldots & G_{n-k-1}^{[r]} & G_{n-k}^{[r]} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & G_0^{[(k-1)r]} & G_1^{[(k-1)r]} & \ldots & G_{n-k}^{[(k-1)r]} \end{pmatrix}.$$

By [10, Theorem 1, items 4 and 6], there is a unique parity check matrix of that form and hence it holds that $\widetilde{G}_i^{[(n-k+i)r]} = G_{n-k-i}/G_0$. Raising this equality to the power $[(k+i)r]$ we obtain $\widetilde{G}_i = \widetilde{G}_i^{[nr]} = (G_{n-k-i}/G_0)^{[(k+i)r]}$, for $i = 0, 1, 2, \ldots, n-k$, since m divides rn, and we are done. □

On the other hand, we have the following:

Lemma G.21. *For a q^r-polynomial $F(x) = F_0 x + F_1 x^{[r]} + \cdots + F_d x^{[rd]} \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ that divides $x^{[rn]} - x$, with $F_d \neq 0$, it holds that*

$$F^{\perp\top}(x) = F^{\top\perp}(x) = F(x)/F_d,$$

$$(F_*)^\perp(x) = (F^\perp)^*(x) \quad \textit{and} \quad (F_0)^\perp(x) = (F^\perp)^0(x),$$

and analogously replacing $\perp$ by $\top$ in the last two equalities.

Proof. The first two equalities are straightforward computations. For the last two equalities, it is enough to observe again that $\theta_i(F^\perp(x)) = \theta_i(F(x))^\perp$ and use the previous two equalities. Analogously replacing $\perp$ by $\top$. □

We will need the following result, which is [10, Theorem 3]:

Lemma G.22 ([10, Theorem 3]). *Assume that $C_1, C_2 \subseteq \mathbb{F}_{q^m}^n$ are linear q^r-cyclic codes with generator polynomials $G_1(x)$ and $G_2(x)$, respectively. Then*

1. *$C_1 \cap C_2$ is the q^r-cyclic code with generator polynomial given by $M(x) = \operatorname{lcm}(G_1(x), G_2(x))$ and $Z(M) = Z(G_1) + Z(G_2)$.*

2. *$C_1 + C_2$ is the q^r-cyclic code with generator polynomial given by $D(x) = \gcd(G_1(x), G_2(x))$ and $Z(D) = Z(G_1) \cap Z(G_2)$.*

Finally, we may compute the generator and check polynomials of C^* and C^0, seen as q^r-cyclic codes:

Proposition G.23. *The generator and check polynomials of C^* are $G^*(x)$ and $H_0(x)$, respectively, and the generator and check poylnomials of C^0 are $G^0(x)$ and $H_*(x)$, respectively.*

Proof. By the previous lemma, if $C_1, C_2 \subsetneq \mathbb{F}_{q^m}^n$ are q^r-cyclic codes with generator polynomials $G_1(x), G_2(x)$, respectively, and check polynomials $H_1(x), H_2(x)$, respectively, it holds that $C_1 + C_2$ and $(C_1 + C_2)^\perp = C_1^\perp \cap C_2^\perp$ have generator polynomials $\gcd(G_1(x), G_2(x))$ and $\mathrm{lcm}(H_1^\perp(x), H_2^\perp(x))$ (on the right), respectively. By the previous lemma and Lemma G.20, the check polynomial of $C_1 + C_2$ is then $\mathrm{lcm}(H_1^\perp(x), H_2^\perp(x))^\top$.

We obtain the result for C^* by applying this iteratedly to C, $\theta_1(C)$, $\theta_2(C)$, $\ldots$, $\theta_{m-1}(C)$, observing that the generator and check polynomials of $\theta_i(C)$ are $\theta_i(G(x))$ and $\theta_i(H(x))$, respectively, for $i = 0, 1, 2, \ldots, m-1$. Similarly for C^0. □

We know from Lemma G.6 that C^* and C^0 are skew cyclic of all orders. In the previous sections we used their cyclic (or q^0-cyclic) nature and their conventional generator and check polynomials. We may relate them with the generator and check polynomials obtained in the previous proposition.

For that purpose, we define the operator $L : \mathbb{F}_{q^m}[x] \longrightarrow \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ by

$$L(f_0 + f_1 x + \cdots + f_d x^d) = f_0 x + f_1 x^{[r]} + \cdots + f_d x^{[rd]}. \tag{G.14}$$

Proposition G.24. *Let the notation be as in the previous proposition, and let $g^*(x)$, $g^0(x)$ be the generator (conventional) polynomials of C^* and C^0, respectively, and let $h^0(x)$ and $h^*(x)$ be their check (conventional) polynomials, respectively. Then*

$$G^*(x) = L(g^*(x)), \quad H_0(x) = L(h^0(x)),$$

$$G^0(x) = L(g^0(x)), \quad \textit{and} \quad H_*(x) = L(h^*(x)).$$

Proof. It follows from the uniqueness of the generator and parity check matrices for cyclic and q^r-cyclic codes given by their generator and check polynomials. See [7, Theorem 4.2.1 and Theorem 4.2.7] for the cyclic case, and [2] and [10, Theorem 1] for the q^r-cyclic case. □

On the other hand, we have the following relations between the root spaces of the generator and check polynomials of C, C^* and C^0, as in Proposition G.15.

Proposition G.25. *It holds that*

1. $Z(G^*) = \bigcap_{i=0}^{m-1} Z(G)^{[i]}$ *and* $Z(G^0) = \sum_{i=0}^{m-1} Z(G)^{[i]}$.
2. $\dim_{\mathbb{F}_{q^r}}(Z(H_*)) = \dim_{\mathbb{F}_{q^r}}(\bigcap_{i=0}^{m-1} Z(H^\perp)^{[i]})$.
3. $\dim_{\mathbb{F}_{q^r}}(Z(H_0)) = \dim_{\mathbb{F}_{q^r}}(\sum_{i=0}^{m-1} Z(H^\perp)^{[i]})$.

Proof. The first item follows from Lemma G.22 and the fact that $Z(\theta_i(G)) = Z(G)^{[i]}$, for $i = 0, 1, 2, \ldots, m-1$.

On the other hand, since $H_*(x)$ divides $x^{[rn]} - x$ on the right, it also divides it conventionally, and hence it has simple roots. Hence it holds that $\dim_{\mathbb{F}_{q^r}}(Z(H_*)) = \deg_{q^r}(H_*(x))$ and similarly for $(H_*)^\perp(x)$. Thus

$$\dim_{\mathbb{F}_{q^r}}(Z(H_*)) = \deg_{q^r}(H_*(x)) = \deg_{q^r}((H_*)^\perp(x)) = \dim_{\mathbb{F}_{q^r}}(Z((H_*)^\perp)).$$

Again by Lemma G.22 and Lemma G.21, we have that

$$Z((H_*)^\perp) = \bigcap_{i=0}^{m-1} Z(H^\perp)^{[i]},$$

using again the fact that $Z(\theta_i(H^\perp)) = Z(H^\perp)^{[i]}$, for $i = 0, 1, 2, \ldots, m-1$. Therefore item 2 follows. Item 3 is proven in a similar way. □

We may now state a similar result to Theorem G.3:

Theorem G.4. *It holds that*

$$\begin{aligned} l_R(C) &= n - \deg_{q^r}(\mathrm{gcd}(G(x), \theta_1(G(x)), \ldots, \theta_{m-1}(G(x)))) \\ &= \deg_{q^r}(\mathrm{lcm}(H^\perp(x), \theta_1(H^\perp(x)), \ldots, \theta_{m-1}(H^\perp(x)))) \\ &= n - \dim_{\mathbb{F}_{q^r}}\left(\bigcap_{i=0}^{m-1} Z(G)^{[i]}\right) = \dim_{\mathbb{F}_{q^r}}\left(\sum_{i=0}^{m-1} Z(H^\perp)^{[i]}\right). \end{aligned}$$

Proof. The first two equalities follow from Theorem G.2, item 1, and Proposition G.24. The next two equalities follow from the previous proposition and the fact that $\dim_{\mathbb{F}_{q^r}}(Z(G^*)) = \deg_{q^r}(G^*(x))$ and $\dim_{\mathbb{F}_{q^r}}(Z(H_0)) = \deg_{q^r}(H_0(x))$, since they have simple roots. □

We obtain the following characterizations of rank degenerate skew cyclic codes:

Corollary G.26. *The following conditions are equivalent:*

1. *C is rank degenerate. That is, $l_R(C) < n$.*

2. $\gcd(G(x), \theta_1(G(x)), \ldots, \theta_{m-1}(G(x))) \neq x$.
3. $\operatorname{lcm}(H^{\perp}(x), \theta_1(H^{\perp}(x)), \ldots, \theta_{m-1}(H^{\perp}(x))) \neq x^{[rn]} - x$.
4. $\bigcap_{i=0}^{m-1} Z(G)^{[i]} \neq \{\mathbf{0}\}$.
5. $\sum_{i=0}^{m-1} Z(H^{\perp})^{[i]} \neq \mathbb{F}_{q^{rn}}$.

7 Attaining the rank length by pseudo-skew cyclic codes

So far we have tried to find the linear skew cyclic code of smallest length that is rank equivalent to a given one C. We have given upper bounds on that length and seen that a general lower bound is $l_R(C)$, although it is not clear that this length can be attained by a linear skew cyclic code that is rank equivalent to C.

In this section, we will see that the length $l_R(C)$ can in many cases be attained by some linear pseudo-skew cyclic code. As skew cyclic codes, pseudo-skew cyclic codes were introduced in [5] for $r = 1$ and $n = m$, and then independently in [6] for $r = 1$ and in [2] for general parameters.

Definition G.27. Let $f(x) \in \mathbb{F}_{q^m}[x]$ be of degree n. For a linear code $C \subseteq \mathbb{F}_{q^m}^n$, we define $C_{f(x)}(x)$ as the image of C in $\mathbb{F}_{q^m}[x]/(f(x))$ by the linear vector space isomorphism $\mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}[x]/(f(x))$ given by

$$(c_0, c_1, \ldots, c_{n-1}) \mapsto c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}.$$

Then we say that C is pseudo-cyclic if $C_{f(x)}(x)$ is an ideal in $\mathbb{F}_{q^m}[x]/(f(x))$, for some $f(x) \in \mathbb{F}_{q^m}[x]$ of degree n.

Fix now a linear cyclic code $C \subseteq \mathbb{F}_{q^m}^n$, and let the notation be as in Section 5.

Theorem G.5. *The map $\phi : \mathbb{F}_{q^m}[x]/(h^0(x)) \longrightarrow (g^*(x))/(x^n - 1)$ given by*

$$\phi(f(x)) = f(x) g^*(x)$$

is well-defined, maps ideals to ideals and constitutes a rank equivalence when seeing its domain and codomain as linear Galois closed spaces.

Proof. First of all, it is well-defined since $h^0(x) g^*(x) = x^n - 1$. It is linear since it preserves additions and $\phi(p(x) f(x)) = p(x)\phi(f(x))$, for all $p(x), f(x) \in \mathbb{F}_{q^m}[x]$. For the same reason it maps ideals to ideals.

On the other hand, if $f(x) g^*(x) = 0$ in the quotient $(g^*(x))/(x^n - 1)$, then $f(x) g^*(x) = p(x)(x^n - 1)$ for some polynomial $p(x) \in \mathbb{F}_{q^m}[x]$, which implies that $f(x) = p(x)h^0(x)$. Therefore, ϕ is one to one. Since it is obviously onto, we conclude that it is a vector space isomorphism.

Finally, since $g^*(x) \in \mathbb{F}_q[x]$, we see that ϕ maps polynomials of degree less that k with coefficients in $\mathbb{F}_q$ to polynomials with coefficients in $\mathbb{F}_q$, and hence it is a rank equivalence by Lemma G.2. □

Corollary G.28. *The length $l_R(C)$ is attained by a linear pseudo-cyclic code that is an ideal in the quotient ring $\mathbb{F}_{q^m}[x]/(h^0(x))$.*

We now treat the skew cyclic case. We consider the the center of $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$, denoted by $\mathbb{C}(\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x])$ and defined as the set of q^r-polynomials over $\mathbb{F}_{q^m}$ that commute with every other q^r-polynomial over $\mathbb{F}_{q^m}$. It is well-known that

$$\mathbb{C}(\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]) = \mathcal{L}_{q^l}\mathbb{F}_{q^d}[x],$$

where $l = \text{lcm}(m, r)$ and $d = \text{gcd}(m, r)$.

Definition G.29. Let $F(x) \in \mathbb{C}(\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x])$ such that $\deg_{q^r}(F(x)) = n$. For a linear code $C \subseteq \mathbb{F}_{q^m}^n$, we define $C_{F(x)}(x)$ as the image of C in $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(F(x))$ by the linear vector space isomorphism $\mathbb{F}_{q^m}^n \longrightarrow \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(F(x))$ given by

$$(c_0, c_1, \ldots, c_{n-1}) \mapsto c_0x + c_1x^{[r]} + \cdots + c_{n-1}x^{[(n-1)r]}.$$

Then we say that C is pseudo-skew cyclic (of order r) if $C_{F(x)}(x)$ is a left ideal in $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(F(x))$, for some $F(x) \in \mathbb{C}(\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x])$ such that $\deg_{q^r}(F(x)) = n$.

Fix now a linear q^r-cyclic code $C \subsetneq \mathbb{F}_{q^m}^n$, and let the notation be as in Section 6. We have the following result, whose proof is analogous to that of Theorem G.5.

Theorem G.6. *Assume that $H_0(x)$ is central. Then the map $\phi : \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(H_0(x)) \longrightarrow (G^*(x))/(x^{[rn]} - x)$ given by*

$$\phi(F(x)) = F(x) \otimes G^*(x)$$

is well-defined, maps left ideals to left ideals and constitutes a rank equivalence when seeing its domain and codomain as linear Galois closed spaces.

Corollary G.30. *If $H_0(x)$ is central, then the length $l_R(C)$ is attained by a linear pseudo-skew cyclic code that is a left ideal in the quotient ring $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(H_0(x))$.*

Acknowledgement

The author wishes to thank Olav Geil and Diego Ruano for fruitful discussions and careful reading of the manuscript. The author also gratefully acknowledges the support from The Danish Council for Independent Research (Grant No. DFF-4002-00367).

References

[1] D. Boucher, W. Geiselmann, and F. Ulmer, “Skew-cyclic codes,” *Applicable Algebra in Engineering, Communication and Computing*, vol. 18, no. 4, pp. 379–389, 2007.

[2] D. Boucher and F. Ulmer, “Coding with skew polynomial rings,” *Journal of Symbolic Computation*, vol. 44, no. 12, pp. 1644 – 1656, 2009, gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics.

[3] J. Ducoat, “Generalized rank weights: A duality statement,” in *Topics in Finite Fields*, ser. Comtemporary Mathematics, G. L. M. G. Kyureghyan and A. Pott, Eds. American Mathematical Society, 2015, vol. 632, pp. 114–123.

[4] J. Ducoat and F. Oggier, “Rank weight hierarchy of some classes of cyclic codes,” in *Information Theory Workshop (ITW), 2014 IEEE*, Nov 2014, pp. 142–146.

[5] E. M. Gabidulin, “Theory of codes with maximum rank distance,” *Problems Informormation Transmission*, vol. 21, 1985.

[6] ——, “Rank q-cyclic and pseudo-q-cyclic codes,” in *IEEE International Symposium on Information Theory, 2009. ISIT 2009.*, June 2009, pp. 2799–2802.

[7] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.

[8] J. Kurihara, R. Matsumoto, and T. Uyematsu, “Relative generalized rank weight of linear codes and its applications to network coding,” *IEEE Trans. Inform. Theory*, vol. 61, no. 7, pp. 3912–3936, Jul. 2015.

[9] R. Lidl and H. Niederreiter, *Finite Fields*. Amsterdam: Encyclopedia of Mathematics and its Applications. Addison-Wesley, 1983, vol. 20.

[10] U. Martínez-Peñas, “On the roots and minimum rank distance of skew cyclic codes,” *Designs, Codes and Cryptography*, vol. 83, no. 3, pp. 639–660, 2017.

[11] U. Martínez-Peñas, “On the similarities between generalized rank and Hamming weights and their applications to network coding,” *IEEE Trans. Inform. Theory*, vol. 62, no. 7, pp. 4081–4095, 2016.

[12] O. Ore, “On a special class of polynomials,” *Trans. Amer. Math. Soc.*, vol. 35, no. 3, pp. 559–584, 1933.

[13] ——, “Theory of non-commutative polynomials,” *Ann. of Math. (2)*, vol. 34, no. 3, pp. 480–508, 1933.

[14] D. Silva and F. R. Kschischang, “On metrics for error correction in network coding,” *IEEE Trans. Inform. Theory*, vol. 55, no. 12, pp. 5479–5490, 2009.

[15] H. Stichtenoth, “On the dimension of subfield subcodes,” *IEEE Transactions Information Theory*, vol. 36, no. 1, pp. 90–93, Jan 1990.

Paper H

On asymptotically good ramp secret sharing schemes

Olav Geil[1], Stefano Martin[1], Umberto Martínez-Peñas[1], Ryutaroh Matsumoto[2] and Diego Ruano[1]

The paper has been submitted to the
IEICE Trans. Fundamentals, 10 pages,
and presented at the
9th International Workshop on Coding and Cryptography, Paris, France,
April 2015.

[1] Department of Mathematical Sciences, Aalborg University, Aalborg 9220, Denmark

[2] Department of Information and Communication Engineering, Nagoya University, Nagoya, Japan

Abstract

Asymptotically good sequences of linear ramp secret sharing schemes have been intensively studied by Cramer et al. in terms of sequences of pairs of nested algebraic geometric codes [4–8, 10]. In those works the focus is on full privacy and full reconstruction. In this paper we analyze additional parameters describing the asymptotic behavior of partial information leakage and possibly also partial reconstruction giving a more complete picture of the access structure for sequences of linear ramp secret sharing schemes. Our study involves a detailed treatment of the (relative) generalized Hamming weights of the considered codes.

Keywords: Algebraic geometric codes, generalized Hamming weights, relative generalized Hamming weights, secret sharing.

1 Introduction

A secret sharing scheme [2, 3, 23, 29] is a cryptographic method to encode a secret $\mathbf{s}$ into multiple shares $c_1, \ldots, c_n$ so that only from specified subsets of the shares one can recover $\mathbf{s}$. Often it is assumed that n participants each receive a share, no two different participants receiving the same. The secret and the share vector $\mathbf{c} = (c_1, \ldots, c_n)$ corresponding to it are assumed to be taken at random with some given distributions (usually uniform), and the recovery capability of a set of shares is measured from an information-theoretical point of view [29]. The term ramp secret sharing scheme [3, 7, 29] is used for those schemes where some sets of shares partially determine the secret, but not completely. This allows the shares to be of smaller size than the secret.

In this paper, we concentrate on linear ramp secret sharing schemes with uniform distribution on the secret and uniform distribution on the share vector conditioned to the secret, which is widely considered in the literature (see, for instance, [6, 7, 12, 17]). Here, the secret is a vector $\mathbf{s} \in \mathbb{F}_q^\ell$ (for some finite field $\mathbb{F}_q$), and we assume that the shares are elements $c_1, \ldots, c_n \in \mathbb{F}_q$. The term linear means that a linear combination of share vectors is a share vector of the corresponding linear combination of secrets. In [7, Sec. 4.2] it was shown that such schemes are equivalent to the following construction based on two nested linear codes $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ with $\dim C_1 - \dim C_2 = \ell$. Writing $k_2 = \dim C_2$ and $k_1 = \dim C_1$ (and consequently $\ell = k_1 - k_2$) let $\{\mathbf{b}_1, \ldots, \mathbf{b}_{k_2}\}$ be a basis for C_2 and extend it to a basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_{k_1}\}$ for C_1. A secret $\mathbf{s} = (s_1, \ldots, s_\ell)$ is encoded by first choosing at random coefficients $a_1, \ldots, a_{k_2} \in \mathbb{F}_q$ and then letting the share vector be

$$\mathbf{c} = a_1\mathbf{b}_1 + \cdots + a_{k_2}\mathbf{b}_{k_2} + s_1\mathbf{b}_{k_2+1} + \cdots + s_\ell\mathbf{b}_{k_1}. \tag{H.1}$$

Define a q-bit of information to be $\log_2(q)$ bits of information. Then, for the schemes that we consider, the mutual information between the secret and a set of shares is an integer between 0 and ℓ if measured in q-bits [17, Proof of Th. 4]. Therefore, for each $m = 1, \ldots, \ell$, we may define the following threshold values [12, Def. 2]:

- The m-th privacy threshold of the scheme is the maximum integer t_m such that from no set of t_m shares one can recover m q-bits of information about the secret. That is, $t_m = \max\{\#J \mid J \subseteq \{1, \ldots, n\}, I(J) < m\}$, where $I(J) = I\big(s_1, \ldots, s_\ell \,;\, (c_i \mid i \in J)\big)$. Here, c_i is the i-th component of $\mathbf{c}$ in (H.1), and $I(;)$ is the mutual information taking logarithms in base q.
- The m-th reconstruction threshold of the scheme is the minimum integer r_m such that from any set of r_m shares one can obtain m q-bits of information about $\mathbf{s}$. That is, $r_m = \min\{\#J \mid J \subseteq \{1, \ldots, n\}, I(J) \geq m\}$.

The numbers $t = t_1$ and $r = r_\ell$ have been intensively studied in the literature, e.g. [3, 7, 29], where they are called privacy and reconstruction threshold, respectively. Clearly t is the greatest number such that no set of t shares holds any information on the secret and r is the smallest number such that from any set of r shares one can reconstruct the information in full. In a series of papers the asymptotic behavior of such parameters has been investigated [4–8, 10] in terms of corresponding infinite sequences of nested code pairs of increasing length. Observe here that the above problem cannot be investigated when we consider secret sharing schemes constructed from univariate polynomials over a finite field [21, 23, 30, 32]. Because in the asymptotic problem considered in [4–8, 10] the number of participants grows beyond the share size, while the construction with univariate polynomials requires the number of participants to be at most the share size.

In the present paper we take a particular interest in sequences of nested code pairs $(C_2(i) \subsetneq C_1(i) \subset \mathbb{F}_q^{n_i})_{i=1}^{\infty}$ with n_i and with $\ell_i = \dim C_1(i) - \dim C_2(i)$ satisfying

$$\lim_{i \to \infty} n_i = \infty, \quad \text{and} \quad \liminf_{i \to \infty} (\ell_i / n_i) = L \tag{H.2}$$

for some fixed $0 < L < 1$, see [4–8, 10]. The reason for us to require (H.2) is to obtain a constant information rate. For instance if the schemes are to be used in connection with distributed storage as mentioned in [29] then a memory of size $1/L$ times the information size is enough. As in the above listed papers the focus in on full privacy and full reconstruction, what is studied there is

$$\liminf_{i \to \infty} \frac{t}{n_i} = \Omega^{(1)} \quad \text{and} \quad \limsup_{i \to \infty} \frac{r}{n_i} = \Omega^{(2)}. \tag{H.3}$$

Here, t and r are the privacy and reconstruction thresholds for the schemes based on $C_2(i) \subsetneq C_1(i) \subset \mathbb{F}_q^{n_i}$, and thereby are functions in i. For any chosen value of L and corresponding feasible $\Omega^{(1)}$ it is desirable to have the threshold gap $\Omega^{(2)} - \Omega^{(1)}$ as small as possible. One way of achieving this [4–8, 10] is to base the secret sharing schemes on sequences of nested code pairs related to an optimal tower of function fields and to require $\lim_{i\to\infty}(\dim C_1(i)/n_i) = R_1$ and $\lim_{i\to\infty}(\dim C_2(i)/n_i) = R_2$ for some fixed rates $R_1 > R_2$. Using the Goppa bound [15] one then obtains good parameters $L = R_1 - R_2$, $\Omega^{(2)}$ and $\Omega^{(1)}$. For future reference we formalize the concept of asymptotic goodness in a definition, where for completeness we also include the case $L = 0$, although we do not study this case in the present paper.

Definition H.1. Let $0 < R_2 \leq R_1 < 1$ and consider a sequence of nested codes $(C_2(i) \subsetneq C_1(i) \subset \mathbb{F}_q^{n_i})_{i=1}^{\infty}$ with $n_i \to \infty$, $\dim C_2(i)/n_i \to R_2$ and $\dim C_1(i)/n_i \to R_1$ for $i \to \infty$. The corresponding sequence of linear ramp secret sharing schemes is said to be asymptotically good if the parameters from (H.3) satisfy $0 < \Omega^{(1)}$ and $\Omega^{(2)} < 1$.

The purpose of the present paper is to provide additional information on the access structure of sequences of linear ramp secret sharing schemes by studying partial information leakage and partial reconstruction parameters. More precisely, given a sequence of linear ramp secret sharing schemes and any fixed numbers $0 \leq \varepsilon_1, \varepsilon_2 \leq 1$ we study the asymptotic parameters

$$\begin{aligned}
\Lambda^{(1)}(\varepsilon_1) &= \sup\big\{ \liminf_{i\to\infty} \frac{t_{m_1(i)}}{n_i} \mid (m_1(i))_{i=1}^{\infty} \text{ satisfies} \\
&\qquad 1 \leq m_1(i) \leq \ell_i, \lim_{i\to\infty}(m_1(i)/n_i) = \varepsilon_1 L\big\}, \\
\Lambda^{(2)}(\varepsilon_2) &= \inf\big\{ \limsup_{i\to\infty} \frac{r_{\ell_i - m_2(i)+1}}{n_i} \mid (m_2(i))_{i=1}^{\infty} \text{ satisfies} \\
&\qquad 1 \leq m_2(i) \leq \ell_i, \lim_{i\to\infty}(m_2(i)/n_i) = \varepsilon_2 L\big\}.
\end{aligned}$$

Such parameters tell us that asymptotically no fraction less than $\Lambda^{(1)}(\varepsilon_1)$ of the shares holds more information on the secret than a fraction ε_1. Similarly, from any fraction greater than $\Lambda^{(2)}(\varepsilon_2)$ of the shares one can gain information on the secret corresponding to a fraction $1 - \varepsilon_2$ or more. Of particular interest is $\Lambda^{(1)}(0)$ which ensures almost full privacy. It is a surprising fact that for secret sharing schemes based on algebraic geometric codes this number can be significantly larger than $\Omega^{(1)}$, meaning that such schemes are more secure than anticipated (see Section 3 and Theorem H.12). The situation is similar with regards to reconstruction. In another direction, for fixed values of L and corresponding feasible $\Lambda^{(1)}(\varepsilon_1)$ we determine for the general class of ramp secret sharing schemes the smallest value $\Lambda^{(2)}(\varepsilon_2)$ such that a sequence of codes with these parameters exists. This bound – which can be seen as an asymptotic Singleton bound for linear ramp secret sharing schemes – is then by a non-constructive proof shown to be achievable, but unfortunately, we obtain no information regarding $\Omega^{(1)}$ and $\Omega^{(2)}$ for those sequences.

Sequences of linear ramp secret sharing schemes based on algebraic geometric codes defined from optimal towers of function fields are interesting for the following three reasons. Firstly, for such sequences the parameters L, $\Omega^{(1)}$ and $\Omega^{(2)}$ are simultaneously good. Also $\Lambda^{(1)}(\varepsilon_1)$ and $\Lambda^{(2)}(\varepsilon_2)$ are good, although they do not always reach the Singleton bound. Secondly, such sequences are constructible if q is a perfect square and are semi-constructible if not. Finally, as demonstrated in [4–8, 10] examples of such sequences are important in connection with secure multiparty computation due to nice properties on the componentwise product of share vectors.

Our analysis of the asymptotic secret sharing parameters is based on the material in [12, 17] which translates information-theoretical properties of a ramp secret sharing scheme based on nested linear codes $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ into coding-theoretical properties of the nested codes. In particular, bounding generalized Hamming weights [28] of C_1 and $C_2^\perp$ and relative generalized Hamming weights [18] of the pairs $C_2 \subsetneq C_1$ and $C_1^\perp \subsetneq C_2^\perp$ implies bounds on the privacy and reconstruction numbers t_i and r_i.

We describe the relations between our study and the previous similar researches [21, 30, 32]. In [30], Yamamoto treated the case where real-valued coding and leakage rates are treated in asymptotic setting with two or three shares. Our study lets the number of shares grow to the infinity, and the asymptotic problem studied in this paper is therefore different from [30] where the number of shares is limited to two or three. [21] considered the ramp (non-perfect) secret sharing with general access structures. They clarified lower bounds on the share sizes, but did not provide an explicit construction except simple extension of Shamir's scheme. [32] treated the case where $t_m + 1 = r_m$, $m = 1, \ldots, \ell$ of the proposed scheme, and proposed an optimal scheme that minimizes the ratio of share sizes to secret size. The underlying assumption in [32] was that both share sizes and secret size can be made arbitrarily large to decrease the above mentioned ratio, because their proposed construction [32, Section 5] used their previous research [31] that used a univariate polynomial construction over finite fields, in which the number of shares cannot be larger than the size of the finite field used in construction. On the other hand, in this study we always considered a fixed size q of shares, in the same way as [4–8, 10], and therefore our study cannot be directly compared with [32].

The paper is organized as follows. In Section 2 we give the Singleton bound for linear ramp secret sharing schemes. Using the material from 1 we then show that for arbitrary L, sequences of schemes exist such that for arbitrary $\varepsilon_1, \varepsilon_2$ one gets arbitrarily close to the Singleton bound for $\Lambda^{(1)}(\varepsilon_1)$ and $\Lambda^{(2)}(\varepsilon_2)$. In Section 3 we then discuss how to obtain sequences of ramp secret sharing schemes with good values of L, $\Omega^{(1)}$ and $\Omega^{(2)}$ from optimal towers of function fields. As a preparation step to treat later in the paper $\Lambda^{(1)}(\varepsilon_1)$ and $\Lambda^{(2)}(\varepsilon_2)$ for these sequences of schemes we next study relative generalized Hamming weights of algebraic geometric codes in Section 4 and derive asymptotic consequences in Section 5. Then finally in Section 6 we collect our findings into information on $\Omega^{(1)}$, $\Omega^{(2)}$, $\Lambda^{(1)}(\varepsilon_1)$ and $\Lambda^{(2)}(\varepsilon_2)$ for sequences of ramp secret sharing schemes based on algebraic geometric codes coming from optimal towers of function fields. Due to lack of space, the authors must assume readers' familiarity with algebraic geometry codes. because a short readable review on algebraic geometry codes seems impossible. Readers are referred to [15] and [25] for background knowledge. on algebraic geometry codes.

2 The Singleton bound

The code parameters governing the privacy and reconstruction numbers t_m and r_m of linear ramp secret sharing schemes are the relative generalized Hamming weights [18] which we now define together with the generalized Hamming weights [28].

Definition H.2. Consider $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ and let $\ell = k_1 - k_2$ where $k_1 = \dim C_1$ and $k_2 = \dim C_2$. For $m = 1, \ldots, \ell$ the m-th relative generalized Hamming weight (RGHW) is:

$$\begin{aligned} M_m(C_1, C_2) &= \min\{\#\mathrm{Supp}(D) \mid D \subset C_1 \text{ is a linear space} \\ &\qquad \text{with } \dim(D) = m \text{ and } D \cap C_2 = \{\mathbf{0}\}\}, \end{aligned}$$

where $\mathrm{Supp}(D) = \{i \in \{1, 2, \ldots, n\} \mid \exists \mathbf{d} \in D, d_i \neq 0\}$. For $m = 1, 2, \ldots, k_1$, the m-th generalized Hamming weight (GHW) of C_1 is defined as $d_m(C_1) = M_m(C_1, \{\mathbf{0}\})$.

Clearly, the RGHWs can be lower bounded by the GHWs of the same index, and as the latter are often easier to estimate we shall also take an interest in them. The following theorem, which is [12, Th. 3], gives a characterization of the threshold numbers t_m and r_m in terms of the RGHWs of the pairs $C_2 \subsetneq C_1$ and $C_1^\perp \subsetneq C_2^\perp$, where $C^\perp$ denotes the dual of the linear code C.

Theorem H.1. *Consider a linear ramp secret sharing scheme based on codes $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$. Then for $m = 1, 2, \ldots, \ell$,*

$$\begin{aligned} t_m &= M_m(C_2^\perp, C_1^\perp) - 1, \text{ and} \\ r_m &= n - M_{\ell-m+1}(C_1, C_2) + 1. \end{aligned}$$

Observe, that as a consequence we obtain $t_m \geq d(C_2^\perp) - 1$ and $r_m \leq n - d_{\ell-m+1}(C_1) + 1$. Given a sequence of linear ramp secret sharing schemes satisfying (H.2), numbers $0 \leq \varepsilon_1, \varepsilon_2 \leq 1$ and any two sequences $(m_1(i))_{i=1}^{\infty}$ and $(m_2(i))_{i=1}^{\infty}$ with $\lim_{i\to\infty}(m_1(i)/n_i) \to \varepsilon_1 L$ and $\lim_{i\to\infty}(m_2(i)/n_i) \to \varepsilon_2 L$ we then obtain

$$\begin{aligned}
\Omega^{(1)} &= \liminf_{i\to\infty} \frac{M_1(C_2^{\perp}, C_1^{\perp})}{n_i} \geq \liminf_{i\to\infty} \frac{d(C_2^{\perp})}{n_i} && \text{(H.4)} \\
\Omega^{(2)} &= 1 - \liminf_{i\to\infty} \frac{M_1(C_1, C_2)}{n_i} \\
&\leq 1 - \liminf_{i\to\infty} \frac{d(C_1)}{n_i} && \text{(H.5)} \\
\Lambda^{(1)}(\varepsilon_1) &\geq \liminf_{i\to\infty} \frac{M_{m_1(i)}(C_2^{\perp}, C_1^{\perp})}{n_i} && \text{(H.6)} \\
&\geq \liminf_{i\to\infty} \frac{d_{m_1(i)}(C_2^{\perp})}{n_i} && \text{(H.7)} \\
\Lambda^{(2)}(\varepsilon_2) &\leq 1 - \liminf_{i\to\infty} \frac{M_{m_2(i)}(C_1, C_2)}{n_i} && \text{(H.8)} \\
&\leq 1 - \liminf_{i\to\infty} \frac{d_{m_2(i)}(C_1)}{n_i} && \text{(H.9)}
\end{aligned}$$

To study the optimality of linear ramp secret sharing schemes we recall the Singleton bound [18, Section IV] for a linear code pair $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ and its dual pair $C_1^{\perp} \subsetneq C_2^{\perp} \subset \mathbb{F}_q^n$: for each $m = 1, 2, \ldots, \ell$,

$$M_m(C_1, C_2) \leq n - k_1 + m, \quad \text{and} \quad M_m(C_2^{\perp}, C_1^{\perp}) \leq k_2 + m. \qquad \text{(H.10)}$$

From these bounds and Theorem H.1, it follows that $r_m \geq k_2 + m$ and $t_m \leq k_2 + m - 1$, and as a consequence

$$\Omega^{(2)} - \Omega^{(1)} \geq L \qquad \text{(H.11)}$$

and

$$\Lambda^{(2)}(\varepsilon_2) - \Lambda^{(1)}(\varepsilon_1) \geq L(1 - \varepsilon_1 - \varepsilon_2). \qquad \text{(H.12)}$$

There exist choices of $\Omega^{(1)} < \Omega^{(2)}$ such that (H.11) is not nearly tight, meaning that L cannot be close to $\Omega^{(2)} - \Omega^{(1)}$ [4, Th. 3.26, Th. 4.6]. It is therefore surprising that for any fixed value of $\Lambda^{(1)}(0) < \Lambda^{(2)}(0)$ there exist sequences of linear ramp secret sharing schemes with L arbitrarily close to $\Lambda^{(2)}(0) - \Lambda^{(1)}(0)$. Even more, by the strict monotonicity of RGHWs [18, Pro. 2], for such schemes $L(1 - \varepsilon_1 - \varepsilon_2)$ becomes arbitrarily close to $\Lambda^{(2)}(\varepsilon_2) - \Lambda^{(1)}(\varepsilon_1)$ for all $0 \leq \epsilon_1, \epsilon_2 \leq 1$. Our proof is non-constructive, as might be expected, and it unfortunately does not reveal any non-trivial information on the corresponding values of $\Omega^{(1)}$ and $\Omega^{(2)}$. We leave it for further research to determine simultaneous information on these parameters, and in particular to decide if the sequences fulfill the requirements in Definition H.1 for being asymptotically good. In 1 we prove the following result:

Theorem H.2. *For* $0 \leq R_2 < R_1 \leq 1$, $0 \leq \delta \leq 1$, $0 \leq \delta^\perp \leq 1$, $0 < \tau \leq \min\{\delta, R_1 - R_2\}$ *and* $0 < \tau^\perp \leq \min\{\delta^\perp, R_1 - R_2\}$*, if*

$$R_1 + \delta < 1 + \tau \ \textit{and}\ \ (1 - R_2) + \delta^\perp < 1 + \tau^\perp, \tag{H.13}$$

then for any prime power q *there exists an infinite sequence of nested linear code pairs* $C_2(i) \subsetneq C_1(i) \subset \mathbb{F}_q^{n_i}$*, where* $n_i \to \infty$ *for* $i \to \infty$*, and where*

$$\lim_{i\to\infty} \frac{\dim(C_1(i))}{n_i} = R_1,$$

$$\lim_{i\to\infty} \frac{\dim(C_2(i))}{n_i} = R_2,$$

$$\liminf_{i\to\infty} \frac{M_{\lceil n_i \tau \rceil}(C_1(i), C_2(i))}{n_i} \geq \delta, \textit{ and}$$

$$\liminf_{i\to\infty} \frac{M_{\lceil n_i \tau^\perp \rceil}(C_2(i)^\perp, C_1(i)^\perp)}{n_i} \geq \delta^\perp.$$

As a corollary we see that the difference in (H.12) can become arbitrarily close to zero.

Corollary H.3. *For any* $0 < R_2 < R_1 < 1$ *there exists a sequence of linear ramp secret sharing schemes satisfying (H.2) with* $L = R_1 - R_2$ *and having simultaneous* $\Lambda^{(1)}(\varepsilon_1)$ *arbitrarily close to* $R_2 + \varepsilon_1 L$ *and* $\Lambda^{(2)}$ *arbitrarily close to* $R_1 - \varepsilon_2 L$ *for all* $0 \leq \varepsilon_1, \varepsilon_2 \leq 1$.

Proof. As noted prior to Theorem H.2 by the strict monotonicity of the RGHWs it is enough to prove $L = R_1 - R_2$ and that $\Lambda^{(1)}(0)$ can be arbitrarily close to R_2 simultaneously with $\Lambda^{(2)}(0)$ being arbitrarily close to R_1. We start by proving a result which at a first glance seems weaker – but from which the above will follow. Let $0 < \varepsilon \leq \min\{R_1/L, (1 - R_2)/L\}$ and choose arbitrarily small $\mu > 0$. In Theorem H.2 choose $\tau = \tau^\perp = \varepsilon L$, $\delta = 1 - R_1 + \varepsilon L - \mu$ and $\delta^\perp = R_2 + \varepsilon L - \mu$. By inspection all the conditions of the theorem are satisfied and therefore by (H.6) and (H.8) for any ε in the considered interval there exists a sequence of linear ramp secret sharing schemes satisfying (H.2) such that $\Lambda^{(1)}(\varepsilon)$ is arbitrarily close to $R_2 + \varepsilon L$ simultaneously with $\Lambda^{(2)}(\varepsilon)$ being arbitrarily close to $R_1 - \varepsilon L$. The theorem finally follows by considering a sequence of numbers $(\varepsilon(i))_{i=1}^\infty$ between 0 and $\min\{R_1/L, (1 - R_2)/L\}$ and with $\lim_{i\to\infty} \varepsilon(i) = 0$. For each $\varepsilon(i)$ we have a sequence $\mathcal{S}(i)$ of secret sharing schemes as described above. Now build a new sequence of schemes in which the i-th scheme is the i-th scheme from the sequence $\mathcal{S}(i)$. The resulting scheme satisfies the requirement mentioned at the beginning of the proof. □

3 Asymptotically good sequences of schemes from algebraic geometric codes

In the remaining part of the paper we concentrate on ramp secret sharing schemes defined from pairs of nested algebraic geometric codes. In the present section we collect known information to describe what is possible concerning the parameters L, $\Omega^{(1)}$ and $\Omega^{(2)}$. In subsequent sections we then derive information on $\Lambda^{(1)}(\varepsilon_1)$ and $\Lambda^{(2)}(\varepsilon_2)$.

Let $\mathcal{F}$ be an algebraic function field over $\mathbb{F}_q$ of transcendence degree one. In the rest of the paper we consider divisors $D = P_1 + \cdots + P_n$ and G with disjoint supports, where the places P_i are rational and pairwise distinct. For any divisor E, we define the Riemann-Roch space $\mathcal{L}(E)$ of functions $f \in \mathcal{F}$ such that the divisor $(f) + E$ is effective (see also [15, Def. 2.36]). We denote by $C_{\mathcal{L}}(D, G)$ the evaluation code of length n obtained by evaluating functions $f \in \mathcal{L}(G)$ in the places P_i. An algebraic geometric code is a code of the form $C_{\mathcal{L}}(D, G)$ or $C_{\mathcal{L}}(D, G)^{\perp}$. We call the first primary algebraic geometric codes and the latter dual. The well-known Goppa bound [15, Th. 2.65] gives information on the relation between dimension and minimum distance for primary or dual codes.

Theorem H.3. *Let C be an algebraic geometric code of dimension k defined from a function field of genus g. Then the minimum distance satisfies $d(C) \geq n - k + 1 - g$.*

Given a function field $\mathcal{F}$, we shall write $N(\mathcal{F})$ for its number of rational places and $g(\mathcal{F})$ for its genus. For asymptotic purposes, we will make use of Ihara's constant [16]

$$A(q) = \limsup_{g(\mathcal{F}) \to \infty} \frac{N(\mathcal{F})}{g(\mathcal{F})},$$

where the limit is taken over all function fields over $\mathbb{F}_q$ of genus $g(\mathcal{F}) > 0$. The Drinfeld-Vlăduţ bound [27] states that

$$A(q) \leq \sqrt{q} - 1. \tag{H.14}$$

As is well-known $A(q)$ is always strictly positive and equality in (H.14) holds if q is a perfect square [16]. See [1] for the status on what is known about $A(q)$ for q being a non-square. For convenience, we give the following definition:

Definition H.4. A tower of function fields $(\mathcal{F}_i)_{i=1}^{\infty}$ over $\mathbb{F}_q$ is optimal if $N(\mathcal{F}_i) \to \infty$ and $N(\mathcal{F}_i)/g(\mathcal{F}_i) \to A(q)$ for $i \to \infty$. On the other hand, $(C_i)_{i=1}^{\infty}$ is an optimal sequence of one-point algebraic geometric codes defined from $\mathcal{F}_i$ if $n_i/N(\mathcal{F}_i) \to 1$ for $i \to \infty$, where n_i is the length of C_i.

The above together with (H.4) and (H.5) immediately combine into the following result concerning the existence of asymptotically good sequences of ramp secret sharing schemes.

Theorem H.4. *Let $(C_2(i) \subsetneq C_1(i) \subset \mathbb{F}_q^{n_i})_{i=1}^{\infty}$ be a sequence of nested algebraic geometric codes defined from an optimal tower of function fields and satisfying $n_i = N(\mathcal{F}_i) - 1$, $\dim C_1(i)/n_i \to R_1$ and $\dim C_2(i)/n_i \to R_2$ for some $0 < R_2 \leq R_1 < 1$. Then the corresponding sequence of linear ramp secret sharing schemes (see Section 1) satisfies $\Omega^{(1)} \geq R_2 - \frac{1}{A(q)}$ and $\Omega^{(2)} \leq R_1 + \frac{1}{A(q)}$.*

In particular we obtain asymptotically good ramp secret sharing schemes (Definition H.1) if $\frac{1}{A(q)} < R_2 \leq R_1 < 1 - \frac{1}{A(q)}$. If moreover $R_2 < R_1$ then also the crucial requirement (H.2) is satisfied. Observe that due to the assumption $n_i = N(\mathcal{F}_i) - 1$ we may choose the codes in Theorem H.4 as one-point codes, meaning that without loss of generality we may consider codes of the form $C_2(i) = C_{\mathcal{L}}(D, \mu_2(i)Q)$ and $C_1(i) = C_{\mathcal{L}}(D, \mu_1(i)Q)$, where D is the sum of n_i distinct rational places in $\mathcal{F}_i$ and Q is another rational place in the same function field.

4 RGHWs and GHWs of algebraic geometric codes

In this section, we give non-asymptotic analysis that are necessary in Sections 5 and 6 to treat the parameters $\Lambda^{(1)}(\varepsilon_1)$ and $\Lambda^{(2)}(\varepsilon_2)$ of the sequences of algebraic geometric schemes discussed in the previous section. The next theorem combines [15, Th. 2.65], [26, Th. 4.3, Cor. 4.2] and [28, Th. 1]. The first part which is a generalization of Theorem H.3 is known as the Goppa bound for GHWs.

Theorem H.5. *Let C be an algebraic geometric code of dimension k defined from a function field of genus g. Then $d_m(C) \geq n - k + m - g$, for $1 \leq m \leq g$, and $d_m(C) = n - k + m$, for $g + 1 \leq m \leq k$.*

For algebraic geometric codes $C_2 \subsetneq C_1$, the above theorem exactly gives $d_m(C_1)$ and $M_m(C_1, C_2)$ when $g < m$. In Proposition H.6 and Proposition H.7 below, we will improve it in the case $m \leq g$ for one-point codes. From now on we will concentrate on one-point algebraic geometric codes. That is, codes $C_{\mathcal{L}}(D, G)$ or $C_{\mathcal{L}}(D, G)^{\perp}$, where $G = \mu Q$, Q is a rational place and $\mu \geq -1$. Writing ν_Q for the valuation at Q, the Weierstrass semigroup corresponding to Q is

$$H(Q) = -\nu_Q \left(\bigcup_{\mu=0}^{\infty} \mathcal{L}(\mu Q) \right) = \{\mu \in \mathbb{N}_0 \mid \mathcal{L}(\mu Q) \neq \mathcal{L}((\mu - 1)Q)\}.$$

As is well-known, the number of missing positive numbers in $H(Q)$ equals the genus g of the function field. The conductor c is by definition the smallest element in $H(Q)$ such that all integers greater than or equal to that number belong to the set. The following lemma is well-known [15, Th. 2.65]:

Lemma H.5. *For $\mu \geq -1$, $k = \dim C_{\mathcal{L}}(D, \mu Q)$ satisfies:*

- *$k \geq \mu + 1 - g$ if $\mu \leq 2g - 2$,*
- *$k = \mu + 1 - g$ if $2g - 2 < \mu < n$, and*
- *$k \leq \mu + 1 - g$ if $n \leq \mu$.*

If $\mu = n + 2g - 1$, then $C_{\mathcal{L}}(D, \mu Q) = \mathbb{F}_q^n$.

From [12, Th. 19, 20] we have the following result.

Theorem H.6. *Let $C_1 = C_{\mathcal{L}}(D, \mu_1 Q)$ and $C_2 = C_{\mathcal{L}}(D, \mu_2 Q)$, with $-1 \leq \mu_2 < \mu_1$. Write $k_1 = \dim C_1$, $k_2 = \dim C_2$ and $\ell = k_1 - k_2$. If $1 \leq m \leq \ell$, then*

1. *$M_m(C_1, C_2) \geq n - \mu_1 + \min\{\#\{\alpha \in \cup_{s=1}^{m-1}(i_s + H(Q)) \mid \alpha \notin H(Q)\} \mid -(\mu_1 - \mu_2) + 1 \leq i_1 < \ldots < i_{m-1} \leq -1\}$.*
2. *$M_m(C_2^\perp, C_1^\perp) \geq \min\{\#\{\alpha \in \cup_{s=1}^{m}(i_s + (\mu_1 - H(Q))) \mid \alpha \in H(Q)\} \mid -(\mu_1 - \mu_2) + 1 \leq i_1 < \ldots < i_m \leq 0\}$.*

Choosing $C_2 = \{\mathbf{0}\}$ in item 1, we obtain a bound on the GHWs of C_1. Similarly, choosing $C_1 = \mathbb{F}_q^n$ in item 2, we get a bound on the GHWs of $C_2^\perp$.

Proposition H.6. *For $0 \leq \gamma \leq c$, let $h_\gamma = \#\left(H(Q) \cap (0, \gamma]\right)$ and let $\mu \geq -1$ and $k = \dim C_{\mathcal{L}}(D, \mu Q)$. If $\mu < n$ and $1 \leq m \leq \min\{k, g\}$, then*

$$d_m(C_{\mathcal{L}}(D, \mu Q)) \geq n - k + 2m - c + h_{c-m} \geq n - k + 2m - c.$$

Proof. We will apply item 1 in Theorem H.6 for $\mu_1 = \mu$ and $\mu_2 = -1$. Consider numbers $-\mu \leq i_1 < \cdots < i_{m-1} \leq -1$. We have $[c - m + 1, c] \setminus H(Q) \subset [\max\{0, c + i_1\}, c] \setminus H(Q) \subset \{\alpha \in \cup_{s=1}^{m-1}(i_s + H(Q)) \mid \alpha \notin H(Q)\} \cap [0, \infty)$, where the first inclusion comes from $i_1 \leq -m + 1$. Now the number of elements in $[c - m + 1, c] \cap H(Q)$ is at most $(c - g) - h_{c-m}$, and we have that $\#\left(\{\alpha \in \cup_{s=1}^{m-1}(i_s + H(Q)) \mid \alpha \notin H(Q)\} \cap [0, \infty)\right) \geq m - (c - g) + h_{c-m}$. On the other hand, we have that $\{i_1, \ldots, i_{m-1}\} \subset \{\alpha \in \cup_{s=1}^{m-1}(i_s + H(Q)) \mid \alpha \notin H(Q)\} \cap (-\infty, 0)$. Thus, from Theorem H.6, we obtain $d_m(C_{\mathcal{L}}(D, \mu Q)) \geq (n - \mu) + (m - 1) + (m - c + g + h_{c-m})$. Since $k \geq \mu - g + 1$ by Lemma H.5, the result follows. □

Proposition H.7. *For $\gamma \geq 1$, let $h'_\gamma = \#([\gamma, \infty) \setminus H(Q))$ and let $\mu > 2g - 2$ and $k = \dim C_{\mathcal{L}}(D, \mu Q)^\perp$. If $1 \leq m \leq \min\{k, g\}$, then*

$$d_m(C_{\mathcal{L}}(D, \mu Q)^\perp) \geq n - k + 2m - c + h'_{\mu-c+m} \geq n - k + 2m - c.$$

Proof. We will apply item 2 in Theorem H.6 for $\mu_1 = n + 2g - 1$ and $\mu_2 = \mu$ to prove that $M_m(C_2^\perp, C_1^\perp) \geq k_2 + 2m - c + h'_{\mu_2-c+m}$, where $k_2 = \dim C_2$. Consider numbers $-(\mu_1 - \mu_2) + 1 \leq i_1 < \cdots < i_m \leq 0$. First, $(i_m + \mu_1 - H(Q)) \cap [0, \mu_2]$ contains the set $[0, \mu_1 - c - (\mu_1 - \mu_2) + m] = [0, \mu_2 - c + m]$, since $i_m \geq -(\mu_1 - \mu_2) + m$ and $\mu_1 - c - (\mu_1 - \mu_2) + m \leq \mu_2$. Here, we used the assumption $m \leq g$ and the fact that $g \leq c$. Thus, $\#\left((i_m + \mu_1 - H(Q)) \cap H(Q) \cap [0, \mu_2]\right)$ is greater than or equal to $(\mu_2 - c + m + 1) - (g - h'_{\mu_2-c+m})$. On the other hand, $\{\mu_1 + i_1, \ldots, \mu_1 + i_m\}$ is contained in $\{\alpha \in \cup_{s=1}^m (i_s + (\mu_1 - H(Q))) \mid \alpha \in H(Q)\}$, which are m elements in the range $(\mu_2, \mu_1]$. Thus, from the previous theorem we obtain $M_m(C_2^\perp, C_1^\perp) \geq (\mu_2 - c + m + 1 - g + h_{\mu_2-c+m}) + m$. Since $k_2 \leq \mu_2 - g + 1$ and $C_1 = \mathbb{F}_q^n$ by Lemma H.5, the result follows. □

5 Asymptotic analysis for algebraic geometric codes

As a preparation step to treat the parameters $\Lambda^{(1)}(\varepsilon_1)$ and $\Lambda^{(2)}(\varepsilon_2)$ of sequences of schemes based on algebraic geometric codes, in this section we derive asymptotic consequences of the non-asymptotic results derived in the previous section. We start our investigations by commenting on [26, Th. 5.9], which if true would imply that the codes in Theorem H.4 would attain the Singleton bound (H.12) in all cases $\frac{1}{q} < R_2 < R_1 < 1 - \frac{1}{q}$ and for all $0 \leq \varepsilon_1, \varepsilon_2 \leq 1$. Below we reformulate [26, Th. 5.9] with the needed modification which ensures that the Singleton bound is reached when $1/A(q) < \rho$, in contrast to $0 \leq \rho$, as it appears in [26]. We also adapt the formulation to better fit our purposes of constructing asymptotically good sequences of secret sharing schemes. We include the proof from [26] to explain why this modification is needed.

Theorem H.7. *Let $(\mathcal{F}_i)_{i=1}^\infty$ be an optimal tower of function fields over $\mathbb{F}_q$. Consider R, ρ with $0 \leq \rho \leq R \leq 1$. Let $(C_i)_{i=1}^\infty$ be an optimal sequence of one-point algebraic geometric codes defined from $(\mathcal{F}_i)_{i=1}^\infty$ such that $\dim C_i / n_i \to R$. For all sequences of positive integers $(m_i)_{i=1}^\infty$ with $m_i/n_i \to \rho$, it holds that $\delta = \liminf_{i\to\infty} d_{m_i}(C_i)/n_i \geq 1 - R + \rho - \frac{1}{A(q)}$ and, if $1/A(q) < \rho$, then $\delta = 1 - R + \rho$.*

Proof. The first bound on δ is an easy consequence of the Goppa bound (the first part of Theorem H.5). Now assume $1/A(q) < \rho$. By assumption, for i large enough we have $m_i > g(\mathcal{F}_i)$, which by the last part of Theorem H.5 implies that $d_{m_i}(C_i) = n_i - \dim C_i + m_i$. Dividing by n_i and taking the limit, we obtain the result. □

The theorem states that the Singleton bound (H.10) can be asymptotically reached when $1/A(q) < \rho$, which implies $1/(\sqrt{q} - 1) < \rho$ by (H.14). However, this leaves the cases $1/A(q) \geq \rho$ undecided. In the following, we shall concentrate on finding asymptotic results for the cases $1/A(q) \geq \rho$. We will need [26, Cor. 3.6] and Wei's duality theorem [28, Th. 3], which we now recall in this order:

Lemma H.8. *For every linear code $C \subset \mathbb{F}_q^n$ we have that*

$$d_m(C) \geq d_1(C)\frac{q^m - 1}{q^m - q^{m-1}}, \quad m = 1, \ldots, \dim C.$$

Lemma H.9. *Let $C \subset \mathbb{F}_q^n$ be a linear code,* $\dim C = k$. *Write $d_r = d_r(C)$, $d_s^\perp = d_s(C^\perp)$ for $1 \leq r \leq k$, $1 \leq s \leq n-k$. Then,*

$$\{1, \ldots, n\} = \{d_1, \ldots, d_k\} \cup \{n+1-d_{n-k}^\perp, \ldots, n+1-d_1^\perp\}.$$

Our first result is a strict improvement to Theorem H.7.

Theorem H.8. *Let $(\mathcal{F}_i)_{i=1}^\infty$ be an optimal tower of function fields over $\mathbb{F}_q$. Consider R, ρ with $1/A(q) \leq R \leq 1$ and $\frac{q}{q-1}\frac{1}{A(q)} - \frac{1}{q-1}R \leq \rho \leq R$. Let $(C_i)_{i=1}^\infty$ be an optimal sequence of one-point algebraic geometric codes defined from $(\mathcal{F}_i)_{i=1}^\infty$ such that* $\dim C_i/n_i \rightarrow R$. *There exists a sequence of positive integers $(m_i)_{i=1}^\infty$ such that $m_i/n_i \rightarrow \rho$ and $d_{m_i}(C_i)/n_i \rightarrow \delta = 1 - R + \rho$.*

Proof. In this proof we use the notation $k_i = \dim C_i$. Let $f : \mathbb{N} \rightarrow \mathbb{N}$ be a function such that $f(i) \rightarrow \infty$ and $f(i)/n_i \rightarrow 0$, as $i \rightarrow \infty$. Now fix i. The Goppa bound (Theorem H.5) together with Lemma H.8 tell us that

$$d_{f(i)}(C_i^\perp) \geq \frac{q^{f(i)} - 1}{q^{f(i)} - q^{f(i)-1}}(k_i - g(\mathcal{F}_i)).$$

Write $h(i)$ for the right-hand side, that is, $d_{f(i)}(C_i^\perp) \geq \lceil h(i) \rceil$. Observe that $h(i) > 0$, since asymptotically $k_i > g(\mathcal{F}_i)$. If we write $d_s^\perp = d_s(C_i^\perp)$ for $1 \leq s \leq n_i - k_i$, we have that $n_i + 1 - \lceil h(i) \rceil \geq n_i + 1 - d_{f(i)}^\perp$. From this inequality and the monotonicity of GHWs, it follows that the sets

$$\{n_i + 1 - \lceil h(i) \rceil, n_i + 2 - \lceil h(i) \rceil, \ldots, n_i\} \text{ and}$$

$$\{n_i + 1 - d_{n_i - k_i}^\perp, n_i + 1 - d_{n_i - k_i - 1}^\perp, \ldots, n_i + 1 - d_{f(i)+1}^\perp\}$$

are disjoint. Therefore, from Lemma H.9 it follows that

$$d_{k_i - \lceil h(i) \rceil + f(i)}(C_i) \geq n_i + 1 - \lceil h(i) \rceil. \tag{H.15}$$

Now take a sequence of positive integers $(m_i)_{i=1}^\infty$ such that

$$k_i - \lceil h(i) \rceil + f(i) \leq m_i \leq k_i \tag{H.16}$$

(observe that the left-hand side is smaller than k_i for large i). From (H.15), (H.16) and the monotonicity of GHWs we get

$$\begin{aligned} d_{m_i}(C_i) &\geq d_{k_i-\lceil h(i)\rceil+f(i)}(C_i)+m_i-k_i+\lceil h(i)\rceil-f(i) \\ &\geq n_i-k_i+m_i-f(i)+1. \end{aligned} \tag{H.17}$$

□

Dividing by n_i and letting $i \to \infty$, (H.16) and (H.17) become

$$\frac{q}{q-1}\frac{1}{A(q)}-\frac{1}{q-1}R \leq \rho \leq R,$$

$$\delta = \lim_{i\to\infty}\frac{d_{m_i}(C_i)}{n_i} = 1-R+\rho.$$

We have the following result for lower values of ρ.

Theorem H.9. *Let $(\mathcal{F}_i)_{i=1}^{\infty}$ be an optimal tower of function fields over $\mathbb{F}_q$. Consider R,ρ with $0 \leq \rho \leq R \leq 1$. Let $(C_i)_{i=1}^{\infty}$ be an optimal sequence of one-point algebraic geometric codes defined from $(\mathcal{F}_i)_{i=1}^{\infty}$ such that* $\dim C_i/n_i \to R$*. For all sequences of positive integers $(m_i)_{i=1}^{\infty}$ with $m_i/n_i \to \rho$, the number $\delta = \liminf_{i\to\infty} d_{m_i}(C_i)/n_i$ satisfies*

$$\delta \geq \frac{q}{q-1}\left(1-R-\frac{1}{A(q)}\right)+\rho.$$

Proof. Let $0 < \varepsilon < 1$ be an arbitrary fixed number. From the Goppa bound (Theorem H.5) and Lemma H.8 we obtain that

$$\frac{d_{\lceil \varepsilon m_i\rceil}(C_i)}{n_i} \geq \frac{q^{\varepsilon m_i}-1}{q^{\varepsilon m_i}-q^{\varepsilon m_i-1}}\left(1-\frac{\dim C_i}{n_i}-\frac{g_i}{n_i}\right).$$

Using again the monotonicity of GHWs we obtain that

$$\frac{d_{m_i}(C_i)}{n_i} \geq \frac{q^{\varepsilon m_i}-1}{q^{\varepsilon m_i}-q^{\varepsilon m_i-1}}\left(1-\frac{\dim C_i}{n_i}-\frac{g_i}{n_i}\right)+\frac{m_i(1-\varepsilon)}{n_i}.$$

□

Now, letting $i \to \infty$ first and then $\varepsilon \to 0$, we obtain

$$\delta = \liminf_{i\to\infty}\frac{d_{m_i}(C_i)}{n_i} \geq \frac{q}{q-1}\left(1-R-\frac{1}{A(q)}\right)+\rho.$$

In the following, we concentrate on Garcia and Stichtenoth's second tower [11] of function fields $(\mathcal{F}_i)_{i=1}^{\infty}$ over $\mathbb{F}_q$ where q is an arbitrary perfect square. From [22] we have a complete description of the corresponding Weierstrass semigroups and [24] gives an efficient method for constructing the corresponding optimal sequences of one-point algebraic geometric codes. We will apply the two new bounds on GHWs given in Proposition H.6 and Proposition H.7 to this tower. In the rest of this section, q is always a perfect square and by $(\mathcal{F}_i)_{i=1}^{\infty}$ we mean Garcia and Stichtenoth's second tower [11]. We will need the following properties of each $\mathcal{F}_i$ ([11, 22]): its number of rational places satisfies $N(\mathcal{F}_i) > q^{\frac{i-1}{2}}(q - \sqrt{q})$, its genus is given by

$$g(\mathcal{F}_i) = \begin{cases} (q^{\frac{i}{4}} - 1)^2 & \text{if } i \text{ is even,} \\ (q^{\frac{i+1}{4}} - 1)(q^{\frac{i-1}{4}} - 1) & \text{if } i \text{ is odd,} \end{cases}$$

and it has a rational place Q_i such that the conductor of $H(Q_i)$ is given by

$$c_i = \begin{cases} q^{i/2} - q^{i/4} & \text{if } i \text{ is even,} \\ q^{i/2} - q^{(i+1)/4} & \text{if } i \text{ is odd.} \end{cases}$$

In the rest of the section, $(C_i)_{i=1}^{\infty}$ is an optimal sequence of one-point algebraic geometric codes defined from $(\mathcal{F}_i)_{i=1}^{\infty}$, and where C_i is of the form $C_{\mathcal{L}}(D_i, \mu_i Q_i)$ or $C_{\mathcal{L}}(D_i, \mu_i Q_i)^{\perp}$. Recall from [24] that we may assume without loss of generality that D_i is chosen in such a way that C_i can be constructed using $\mathcal{O}(n_i{}^3 \log_q^3(n_i))$ operations in $\mathbb{F}_q$.

Theorem H.10. *Let $(\mathcal{F}_i)_{i=1}^{\infty}$ be Garcia-Stichtenoth's second tower of function fields over $\mathbb{F}_q$, where q is a perfect square. Let $(C_i)_{i=1}^{\infty}$ be a corresponding optimal sequence of one-point algebraic geometric codes as described above. Consider R, ρ with $0 \leq R \leq 1 - \frac{1}{\sqrt{q}-1}$ and $0 \leq \rho \leq \min\{R, \frac{1}{\sqrt{q}-1}\}$, and assume that $\dim C_i / n_i \to R$. For all sequences of positive integers $(m_i)_{i=1}^{\infty}$ with $m_i/n_i \to \rho$, it holds that $\delta = \liminf_{i\to\infty} d_{m_i}(C_i)/n_i$ satisfies*

$$\delta \geq 1 - R + 2\rho - \frac{1}{\sqrt{q} - 1}.$$

Proof. We may assume that C_i is of the form $C_{\mathcal{L}}(D_i, \mu_i Q_i)$ or $C_{\mathcal{L}}(D_i, \mu_i Q_i)^{\perp}$, with $2g(\mathcal{F}_i) - 2 < \mu_i < n_i$ and $(\mu_i - g(\mathcal{F}_i))/n_i \to R$. As $\lim_{i\to\infty} c_i/n_i = \lim_{i\to\infty} g(\mathcal{F}_i)/n_i = 1/(\sqrt{q} - 1)$, the result follows from Proposition H.6 or Proposition H.7. □

6 The parameters $\Lambda^{(1)}(\varepsilon_1)$ and $\Lambda^{(2)}(\varepsilon_2)$ for algebraic geometric code based schemes

In Section 3 we estimated $\Omega^{(1)}$ and $\Omega^{(2)}$ for asymptotically good sequences of schemes based on algebraic geometric codes coming from optimal towers of function fields, the sequences being called asymptotically good if $\Omega^{(1)} > 0$ and $\Omega^{(2)} < 1$. Employing the analysis in Section 5 together with (H.7) and (H.9) we are now able to give a more complete picture of the information leakage and reconstruction by providing also estimates on $\Lambda^{(1)}(\varepsilon_1)$ and $\Lambda^{(2)}(\varepsilon_2)$. We emphasize that the below theorems apply also in the cases where one or both of the conditions $\Omega^{(1)} > 0$ and $\Omega^{(2)} < 1$ fails to hold. Throughout the section recall that by definition the numbers ε_1 and ε_2 always satisfy $0 \leq \varepsilon_1, \varepsilon_2 \leq 1$.

Theorem H.11. *For the sequence of linear ramp secret sharing schemes described in Theorem H.4 we have the following estimates: If* $1/A(q) \leq 1 - R_2$ *and* $\varepsilon_1 \geq \big(\frac{q}{q-1}\frac{1}{A(q)} - \frac{1}{q-1}(1-R_2)\big)/L$ *then* $\Lambda^{(1)}(\varepsilon_1) \geq R_2 + \varepsilon_1 L$. *If* $1/A(q) \leq R_1$ *and* $\varepsilon_2 \geq \big(\frac{q}{q-1}\frac{1}{A(q)} - \frac{1}{q-1}R_1\big)/L$ *then* $\Lambda^{(2)}(\varepsilon_2) \leq R_1 - \varepsilon_2 L$.

Proof. Apply Theorem H.8 with $\rho = \varepsilon_1 L$ and $\rho = \varepsilon_2 L$, respectively, in combination with (H.7) and (H.9), respectively. □

Theorem H.12. *For the sequence of linear ramp secret sharing schemes described in Theorem H.4 we have the following estimates:* $\Lambda^{(1)}(\varepsilon_1) \geq \frac{q}{q-1}(R_2 - \frac{1}{A(q)}) + \varepsilon_1 L$ *and* $\Lambda^{(2)}(\varepsilon_2) \leq \frac{q}{q-1}(R_1 + \frac{1}{A(q)}) - \frac{1}{q-1} - \varepsilon_2 L$.

Proof. Apply Theorem H.9 in combination with (H.7) and (H.9). □

Observe that from Theorem H.12 we get an estimate on $\Lambda^{(1)}(0)$ wich is $q/(q-1)$ times as large as the estimate on $\Omega^{(1)}$ in Section 3. Hence, the studied sequences of secret sharing schemes are more secure than previously anticipated. A similar remark holds regarding reconstruction.

Theorem H.13. *Let q be a perfect square. For the sequence of linear ramp secret sharing schemes described in Theorem H.4 we have the following estimates: If* $R_2 \geq 1/(\sqrt{q}-1)$ *and* $\varepsilon_1 \leq \frac{1}{\sqrt{q}-1}\frac{1}{L}$ *then* $\Lambda^{(1)}(\varepsilon_1) \geq R_2 + 2\varepsilon_1 L - \frac{1}{\sqrt{q}-1}$. *If* $R_1 \leq 1 - \frac{1}{\sqrt{q}-1}$ *and* $\varepsilon_2 \leq \frac{1}{\sqrt{q}-1}\frac{1}{L}$ *then* $\Lambda^{(2)}(\varepsilon_2) \leq R_1 - 2\varepsilon_2 L + \frac{1}{\sqrt{q}-1}$. *The i-th scheme in the sequence can be constructed using* $\mathcal{O}(n_i^3 \log(n_i)^3)$ *operations in* $\mathbb{F}_q$.

Proof. Apply Theorem H.10 in combination with (H.7) and (H.9). □

We finally remark that when q is a perfect square, then similarly to Theorem H.13, one can assume in Theorem H.11 and Theorem H.12 that the *i*-th scheme in the sequence can be constructed using $\mathcal{O}(n_i^3 \log(n_i)^3)$ operations in $\mathbb{F}_q$.

Acknowledgments

The authors gratefully acknowledge the support from The Danish Council for Independent Research (DFF-4002-00367), from the Spanish MINECO/FEDER (MTM2015-65764-C3-2-P), from Japan Society for the Promotion of Science (23246071 and 26289116), from the Villum Foundation through their VELUX Visiting Professor Programme 2013-2014, and from the "Program for Promoting the Enhancement of Research Universities" at Tokyo Institute of Technology. They also thank I. Cascudo and R. Cramer for helpful discussions.

References

[1] A. Bassa, P. Beelen, A. Garcia, H. Stichtenoth, Towers of function fields over non-prime finite fields, *Moscow Mathematical Journal*, 15:1–29, 2015.

[2] G.R. Blakley, Safeguarding cryptographic keys, *Proc. of the National Computer Conference 1979*, 48:313–317, 1979

[3] G.R. Blakley, C. Meadows, Security of ramp schemes, Advances in cryptology—CRYPTO 1984, *Lecture Notes in Comput. Sci.*, 196:242–268, 1995.

[4] I. Cascudo, R. Cramer, C. Xing, Bounds on the threshold gap in secret sharing and its applications, *IEEE Trans. Inform. Theory*, 59:5600–5612, 2013. DOI:10.1109/TIT.2013.2264504

[5] I. Cascudo, R. Cramer, C. Xing, Torsion limits and Riemann-Roch systems for function fields and applications, *IEEE Trans. Inform. Theory*, 60:3871–3888, 2014. DOI:10.1109/TIT.2014.2314099

[6] H. Chen, R. Cramer, Algebraic geometric secret sharing schemes and secure multi-party computations over small fields, in: Advances in cryptology—CRYPTO 2006, *Lecture Notes in Comput. Sci.*, 4117:521–536, 2006. DOI:10.1007/11818175_31

[7] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, V. Vaikuntanathan, Secure computation from random error correcting codes, in: Advances in cryptology—EUROCRYPT 2007, *Lecture Notes in Comput. Sci.*, 4515:291–310, 2007. DOI:10.1007/978-3-540-72540-4_17

[8] H. Chen, R. Cramer, R. de Haan, I. Cascudo, Strongly multiplicative ramp schemes from high degree rational points on curves, in: Advances in cryptology—EUROCRYPT 2008, *Lecture Notes in Comput. Sci.*, 4965:451–470, 2008. DOI:10.1007/978-3-540-78967-3_26

[9] T. M. Cover, J. A. Thomas, *Elements of Information Theory*, 2nd edition, Wiley Interscience, 2006.

[10] R. Cramer, I.B. Damgård, N. Döttling, S. Fehr, G. Spini, Linear secret sharing schemes from error correcting codes and universal hash functions, in: Advances in cryptology—EUROCRYPT 2015, *Lecture Notes in Comput. Sci.*, 9057:313–336, 2015.

[11] A. Garcia, H. Stichtenoth, On the asymptotic behaviour of some towers of function fields over finite fields, *Journal of Number Theory*, 61:248–273, 1996. DOI:10.1006/jnth.1996.0147

[12] O. Geil, S. Martin, R. Matsumoto, D. Ruano, Y. Luo, Relative generalized Hamming weights of one-point algebraic geometric codes, *IEEE Trans. Inform. Theory*, 60:5938–5949, 2014. DOI:10.1109/TIT.2014.2345375

[13] J. Goldman, G.-C. Rota, On the foundations of combinatorial theory IV: Finite vector spaces and Eulerian generating functions, *Studies in Applied Mathematics*, 49:239–258, 1970.

[14] T. Helleseth, T. Klöve, V. I. Leveshtein, Ø. Ytrehus, Bounds on the minimum support weights, *IEEE Trans. Inform. Theory*, 41:432–440, 1995.

[15] T. Høholdt, J.H. van Lint, R. Pellikaan, Algebraic geometry codes, in: V.S. Pless, W.C. Huffman (Eds.), *Handbook of Coding Theory*, 1:871–961, Elsevier, Amsterdam, 1998.

[16] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Tokyo*, 28:721-–724, 1981.

[17] J. Kurihara, T. Uyematsu, R. Matsumoto, Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hamming weight, *IEICE Trans. Fundamentals*, E95-A:2067–2075, 2012. DOI:10.1587/transfun.E95.A.2067

[18] Y. Luo, C. Mitrpant, A.J. Han Vinck, K. Chen, Some new characters on the wire-tap channel of type II, *IEEE Trans. Inform. Theory*, 51:1222–1229, 2005. DOI:10.1109/TIT.2004.842763

[19] R. Matsumoto, Gilbert-Varshamov-type bound for relative dimension length profile, *IEICE Comm. Express*, 2 (8):343–346, 2013. DOI:10.1587/comex.2.343

[20] R. Matsumoto, New asymptotic metrics for relative generalized Hamming weight, *Proceedings of IEEE International Symposium on Information Theory*, 3142–3144, 2014. DOI:10.1109/ISIT.2014.6875413

[21] W. Ogata and K. Kurosawa, Some basic properties of general nonperfect secret sharing schemes, J. UCS 4(8):690–704, 1998. DOI:10.3217/jucs-004-08-0690

[22] R. Pellikaan, H. Stichtenoth, F. Torres, Weierstrass semigroups in an asymptotically good tower of function fields, *Finite Fields Appl.*, 4: 381–392, 1998. DOI:10.1006/ffta.1998.0217

[23] A. Shamir, How to share a secret, *Commun. ACM*, 22 (11):612–613, 1979. DOI:10.1145/359168.359176

[24] K.W. Shum, I. Aleshnikov, P.V. Kumar, H. Stichtenoth, V. Deolaikar, A low-complexity algorithm for the construction of algebraic-geometric codes better than the Gilbert-Varshamov bound, *IEEE Trans. Inform. Theory*, 47:2225–2241, 2001. DOI:10.1109/18.945244

[25] H. Stichtenoth, Algebraic Function Fields and Codes, Springer-Verlag, 1993.

[26] M.A. Tsfasman, S.G. Vlăduţ, Geometric approach to higher weights, *IEEE Trans. Inform. Theory*, 41:1564–1588, 1995. DOI:10.1109/18.476213

[27] S.G. Vlăduţ, V.G. Drinfeld, The number of points of an algebraic curve, *Funktsional. Anal. i Prilozhen.*, 17:68–69, 1983.

[28] V.K. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Inform. Theory*, 37:1412–1418, 1991. DOI:10.1109/18.133259

[29] H. Yamamoto, Secret sharing system using (k,L,n) threshold scheme, *Electronics and Communications in Japan (Part I: Communication)*, 69:46–54, 1986

[30] H. Yamamoto, On secret sharing communication systems with two or three channels, IEEE Trans. Information Theory 32(3): 387–393, 1986.

[31] M. Yoshida and T. Fujiwara, Secure construction for nonlinear function threshold secret sharing, Proc. 2007 IEEE ISIT, pp. 1041–1045, 2007. DOI:10.1109/ISIT.2007.4557361

[32] M. Yoshida, T. Fujiwara, and M. P. C. Fossorier, Optimum general threshold secret sharing. Proc. ICITS 2012, pp.187–204, 2012. DOI:10.1007/978-3-642-32284-6_11

1 Proof of Theorem H.2

In this appendix we give a proof of Theorem H.2. The theorem is an improvement of [20, Th. 9], the improvement stating that the RGHWs of primary and dual nested linear code pairs can get *simultaneously* asymptotically as close to the Singleton bound (H.10) as wanted. We use the notation and results in [13, 18–20]. In particular, we use the concept of relative dimension length profile (RDLP) as appears in [18, Sec. III]. For $1 \leq d \leq n$, and linear codes $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ define

$$\begin{aligned} K_d(C_1, C_2) &= \max\{\dim(C_1 \cap V_I) - \dim(C_2 \cap V_I) \mid \\ &\qquad I \subset \{1, \ldots, n\}, \#I = d\}, \end{aligned}$$

where $V_I = \{\mathbf{x} \in \mathbb{F}_q^n \mid x_i = 0 \text{ if } i \notin I\}$. The sequence $(K_d(C_1, C_2))_{d=1}^n$ is then the RDLP of the pair $C_2 \subsetneq C_1$ and is known to be non-decreasing [18, Prop. 1]. Our interest in the RDLP comes from the following result corresponding to the first part of [18, Th. 3]:

$$M_m(C_1, C_2) = \min\{d \mid K_d(C_1, C_2) \geq m\}. \tag{18}$$

As in [13, 19], we define for integers a, u, v, w the numbers:

$$N_1(w, u) = \frac{\prod_{i=0}^{u-1}(q^w - q^i)}{\prod_{i=0}^{u-1}(q^u - q^i)}, \quad N_2(w, u, v) = \frac{\prod_{i=0}^{v-1}(q^w - q^{u+i})}{\prod_{i=0}^{v-1}(q^v - q^i)},$$

and $N_3(w, u, v, a) = N_1(u, a)N_2(w - a, u - a, v - a)$. The meaning of N_1 is [13], [19, Lem. 5 and 6]:

Lemma .10. *Let W be an $\mathbb{F}_q$-linear vector space and let u, v, $w = \dim W$ be non-negative integers. If $u \leq w$, then $N_1(w, u)$ is the number of subspaces $U \subset W$ of dimension u. Furthermore, if U is fixed and $u \leq v \leq w$, then $N_1(w - u, v - u)$ is the number of $\mathbb{F}_q$-linear vector spaces V such that $U \subset V \subset W$ and* $\dim V = v$.

From [19, Lem. 9] we have:

Lemma .11. *Consider fixed integers $1 \leq k_2 < k_1 < n$ and a fixed set $I \subset \{1, \ldots, n\}$ with $\#I = d$. Let s be an integer with $s \leq \min\{d, k_1 - k_2\}$. The number of linear code pairs $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ such that* $\dim C_1 = k_1$, $\dim C_2 = k_2$, *and* $\dim(C_1 \cap V_I) - \dim(C_2 \cap V_I) = s$, *equals*

$$N_4(n, k_1, k_2, d, s) = \sum_{a=0}^{\min\{d-s, k_1-s, k_2\}} \Big(N_1(d, a)$$
$$N_2(n - a, d - a, k_2 - a)N_3(n - k_2, d - a, k_1 - k_2, s)\Big).$$

We next extend [19, Cor. 3].

Theorem .14. *Consider fixed integers $1 \leq k_2 < k_1 < n$, $1 \leq d \leq n$, $1 \leq d^\perp \leq n$, $1 \leq s \leq \min\{d,\ k_1 - k_2\}$, and $1 \leq s^\perp \leq \min\{d^\perp,\ k_1 - k_2\}$. There exists a nested linear code pair $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ such that* $\dim C_1 = k_1$, $\dim C_2 = k_2$, *$M_s(C_1, C_2) > d$ and $M_{s^\perp}(C_2^\perp, C_1^\perp) > d^\perp$, if*

$$N_1(n, k_2)N_1(n - k_2, k_1 - k_2) > \binom{n}{d} \sum_{\sigma=s}^{k_1-k_2} N_4(n, k_1, k_2, d, \sigma)$$
$$+ \binom{n}{d^\perp} \sum_{\sigma^\perp=s^\perp}^{k_1-k_2} N_4(n, n - k_2, n - k_1, d^\perp, \sigma^\perp).$$

Proof. By Lemma .10, the term $N_1(n,k_2)N_1(n-k_2,k_1-k_2)$ is the total number of pairs $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ such that $\dim C_1 = k_1$ and $\dim C_2 = k_2$. On the other hand, by Lemma .11, the number of pairs $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ such that $\dim C_1 = k_1$, $\dim C_2 = k_2$ and $K_d(C_1, C_2) \geq s$ is at most $\binom{n}{d}\sum_{\sigma=s}^{k_1-k_2} N_4(n,k_1,k_2,d,\sigma)$. Similarly, the number of pairs $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ such that $\dim C_1 = k_1$, $\dim C_2 = k_2$ and $K_{d^\perp}(C_2^\perp, C_1^\perp) \geq s^\perp$ is at most $\binom{n}{d^\perp}\sum_{\sigma^\perp=s^\perp}^{k_1-k_2} N_4(n,n-k_2,n-k_1,d^\perp,\sigma^\perp)$. The inequality therefore ensures the existence of a code pair $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ with $\dim C_1 = k_1$, $\dim C_2 = k_2$, $K_d(C_1,C_2) < s$ and $K_{d^\perp}(C_2^\perp, C_1^\perp) < s^\perp$. But the RDLP is non-decreasing and $K_n(C_1,C_2) = K_n(C_2^\perp, C_1^\perp) = k_1 - k_2$ which is larger than or equal to s and s'. Therefore there exists a smallest index j such that $K_j(C_1,C_2) \geq s$ and a smallest index $j^\perp$ such that $K_{j^\perp}(C_2^\perp, C_1^\perp) \geq s^\perp$ and $j > d$ as well as $j^\perp > d^\perp$ hold. The theorem now follows from (18). □

To apply Theorem .14 in an asymptotic setting we will need a couple of lemmas.

Lemma .12. *Define* $\pi(q) = \prod_{i=1}^{\infty}(1-q^{-i})$. *Then*

$$\pi(q)q^{u(w-u)} \leq N_1(w,u) \leq \pi(q)^{-1}q^{u(w-u)}, \tag{19}$$

$$N_2(w,u,v) \leq \pi(q)^{-1}q^{v(w-v)},$$

$$N_3(w,u,v,a) \leq \pi(q)^{-2}q^{a(u-a)}q^{(v-a)(w-v)}. \tag{20}$$

Proof. The inequality (19) is [14, Cor. 2] and the last two inequalities correspond to [20, Lem. 3] except that $\pi(q)^{-2}$ in (20) by a mistake was there written $\pi(q)^{-1}$ and similarly $q^{a(u-a)}$ was written $q^{u(u-a)}$. □

The next lemma corresponds to [9, Ex. 11.1.3].

Lemma .13. *Let* $H_q(x) = -x\log_q(x) - (1-x)\log_q(1-x)$, *then*

$$\frac{1}{n+1}q^{nH_q(m/n)} \leq \binom{n}{m} \leq q^{nH_q(m/n)}.$$

With the above machinery we can now give the promised proof.

Proof of Theorem H.2. Let R_1, R_2, δ, $\delta^\perp$, τ and $\tau^\perp$ be as in the theorem (in particular assume (H.13) to hold). Let $(n_i)_{i=1}^{\infty}$ be a strictly increasing sequence of positive integers and define $k_1(i) = \lfloor n_i R_1 \rfloor$, $k_2(i) = \lceil n_i R_2 \rceil$, $s(i) = \lceil n_i \tau \rceil$, $s^\perp(i) = \lceil n_i \tau^\perp \rceil$, $d(i) = \lfloor n_i \delta \rfloor$ and $d^\perp(i) = \lfloor n_i \delta^\perp \rfloor$. Using Theorem .14, we will show that for i large enough there exist nested linear codes $C_2(i) \subsetneq C_1(i) \subset \mathbb{F}_q^{n_i}$ of dimensions $k_2(i)$ and $k_1(i)$, respectively, with

$$M_{s(i)} \geq d(i), \quad \text{and} \quad M_{s^\perp(i)} \geq d^\perp(i). \tag{21}$$

Observe that (H.13) implies that

$$k_1(i) + d(i) - n_i - s(i) < 0, \tag{22}$$

$$(n_i - k_2(i)) + d^{\perp}(i) - n_i - s^{\perp}(i) < 0, \tag{23}$$

which we will need later in the proof. For brevity, we will write k_1, k_2, d, $d^{\perp}$, s, $s^{\perp}$, and n rather than $k_1(i)$, $k_2(i)$, $d(i)$, $d^{\perp}(i)$, $s(i)$, $s^{\perp}(i)$, and n_i. Applying Lemma .12, Lemma .13, and Theorem .14 we see that a sufficient condition for the existence of a linear code pair satisfying (21) is

$$\begin{aligned}
& \pi(q)^2 q^{k_2(n-k_2)} q^{(k_1-k_2)(n-k_1)} \\
> \; & q^{nH_q(d/n)} \sum_{\sigma=s}^{k_1-k_2} \sum_{a=0}^{\min\{d-\sigma,k_1-\sigma,k_2\}} \Big[\pi(q)^{-1} q^{a(d-a)} \\
& \pi(q)^{-1} q^{(k_2-a)(n-a-k_2+a)} \pi(q)^{-2} q^{\sigma(d-a-\sigma)} q^{(k_1-k_2-\sigma)(n-k_2-k_1+k_2)} \Big] \\
& + q^{nH_q(d^{\perp}/n)} \sum_{\sigma^{\perp}=s^{\perp}}^{k_1-k_2} \sum_{a=0}^{\min\{d^{\perp}-\sigma^{\perp},n-k_2-\sigma^{\perp},n-k_1\}} \Big[\pi(q)^{-1} q^{a(d^{\perp}-a)} \\
& \pi(q)^{-1} q^{(n-k_1-a)(n-a-n+k_1+a)} \pi(q)^{-2} q^{\sigma^{\perp}(d^{\perp}-a-\sigma^{\perp})} q^{(k_1-k_2-\sigma^{\perp})k_2} \Big].
\end{aligned}$$

But then another sufficient condition (named Condition A) for the existence of a nested code pair satisfying (21) is

$$\begin{aligned}
& q^{k_2(n-k_2)+(k_1-k_2)(n-k_1)} > \\
& f(q,n) \max \Big\{ q^{a(d-a)+(k_2-a)(n-k_2)+\sigma(d-a-\sigma)+(k_1-k_2-\sigma)(n-k_1)} \mid \\
& \qquad s \leq \sigma \leq k_1 - k_2, 0 \leq a \leq \min\{d-\sigma, k_1-\sigma, k_2\} \Big\} + \\
& f^{\perp}(q,n) \max \Big\{ q^{a(d^{\perp}-a)+(n-k_1-a)k_1+\sigma^{\perp}(d^{\perp}-a-\sigma^{\perp})+(k_1-k_2-\sigma^{\perp})k_2} \mid \\
& \qquad s^{\perp} \leq \sigma^{\perp} \leq k_1 - k_2, \text{ and} \\
& \qquad 0 \leq a \leq \min\{d^{\perp}-\sigma^{\perp}, n-k_2-\sigma^{\perp}, n-k_1\} \Big\},
\end{aligned}$$

where $f(q,n) = \pi(q)^{-6} q^{nH_q(d/n)} n^2$, and where $f^{\perp}(q,n) = \pi(q)^{-6} q^{nH_q(d^{\perp}/n)} n^2$. Consider now the expression $\sigma(k_1 + d - n - \sigma - a)$, which contains the terms in the first exponent on the right-hand side of Condition A related to σ. As a function in σ, this is a downward parabola intersecting the first axis in $\sigma = 0$. For $s \leq \sigma$, it follows from (22) and $0 \leq a$ that $k_1 + d - n - \sigma - a < 0$. Hence, the maximal value of $\sigma(k_1 + d - n - \sigma - a)$ for $s \leq \sigma$ is attained when $\sigma = s$, and we therefore substitute σ with s in Condition A. In a similar fashion, we see from (23) that $\sigma^{\perp}$ can be replaced with $s^{\perp}$. After these substitutions, the terms related to a in the first exponent on the right-hand side of Condition A become $-a^2 + a(k_2 + d - n - s)$, which is equal to 0 for $a = 0$ and negative for $a > 0$, as a consequence of (22). Similarly, the terms related to a in the last exponent on the right-hand side become $-a^2 + a(d^{\perp} - k_1 - s^{\perp})$ which again is equal to 0 for $a = 0$ and negative for $a > 0$ as a consequence of (23). Hence, we can substitute a with 0 in Condition A. After the above substitutions, Condition A simplifies to

$$\begin{aligned} q^{k_2(n-k_2)+(k_1-k_2)(n-k_1)} \qquad &> f(q,n)q^{k_2(n-k_2)+s(d-s)+(k_1-k_2-s)(n-k_1)} \\ &+ f^{\perp}(q,n)q^{(n-k_1)k_1+s^{\perp}(d^{\perp}-s^{\perp})+(k_1-k_2-s^{\perp})k_2}. \end{aligned}$$

In this formula, we now replace the two expressions on the right-hand side with the largest one multiplied by 2. We then take the logarithm over q and finally divide by n^2. Assume that the first term on the right-hand side of Condition A is greater than or equal to the last term. After simplifying equal terms on both sides and using the definition of k_1, d and s, we see that Condition A holds if

$$0 > g(i) + \tau(\delta - \tau) - \tau(1 - R_1), \tag{24}$$

where $g(i) = \log_q(2f(q, n_i))/n_i^2$, which goes to 0 as i goes to infinity. Similarly, if the last term on the right-hand side is greater than or equal to the first term, we see that Condition A holds if

$$0 > g^{\perp}(i) + \tau^{\perp}(\delta^{\perp} - \tau^{\perp}) - \tau^{\perp} R_2, \tag{25}$$

where $g^{\perp}(i) = \log_q(2f^{\perp}(q, n_i))/n_i^2$, which again goes to 0 as i goes to infinity. Finally, for i large enough, (24) follows from the first part of (H.13), since $\tau > 0$, and (25) follows from the last part of (H.13), since $\tau^{\perp} > 0$. Therefore, Condition A holds for i large enough and we are done.

Paper I

Bounding the number of common zeros of multivariate polynomials and their consecutive derivatives

Olav Geil[1] and Umberto Martínez-Peñas[1]

The paper has been submitted to
Combinatorics, Probability and Computing, 26 pages.

[1] Department of Mathematical Sciences, Aalborg University, Aalborg 9220, Denmark

Abstract

We upper bound the number of common zeros over a finite grid of multivariate polynomials and an arbitrary finite collection of their consecutive Hasse derivatives (in a coordinate-wise sense). To that end, we make use of the tool from Gröbner basis theory known as footprint. Then we establish and prove extensions to this context of a family of well-known results in algebra and combinatorics. These include Alon's combinatorial Nullstellensatz [1], existence and uniqueness of Hermite interpolating polynomials over a grid, estimations on the parameters of evaluation codes with consecutive derivatives [19], and bounds on the number of zeros of a polynomial by DeMillo and Lipton [7], Schwartz [24], Zippel [25, 26], and Alon and Füredi [2].

Keywords: Footprint bound, Gröbner basis, Hasse derivative, Hermite interpolation, multiplicity, Nullstellensatz, Schwartz-Zippel bound.

MSC: 11T06, 12D10, 13P10.

1 Introduction

Estimating the number of zeros of a polynomial over a field $\mathbb{F}$ has been a central problem in algebra, where one of the main inconveniences is counting *repeated zeros*, that is, *multiplicities*. In the univariate case, this is easily solved by defining the multiplicity of a zero as the minimum positive integer r such that the first r *consecutive derivatives* of the given polynomial vanish at that zero. In addition, Hasse derivatives [13] are used instead of classical derivatives in order to give meaningful information over fields of positive characteristic. In this way, the number of zeros of a polynomial, counted with multiplicities, is upper bounded by its degree. Formally:

$$\sum_{a \in \mathbb{F}} m(F(x), a) \leq \deg(F(x)). \tag{I.1}$$

If $\mathcal{V}_{\geq r}(F(x))$ denotes the set of zeros of $F(x)$ of multiplicity at least r, then a weaker, but still sharp, bound is the following:

$$\#\mathcal{V}_{\geq r}(F(x)) \cdot r \leq \deg(F(x)). \tag{I.2}$$

In the multivariate case, the standard approach is to consider the first r consecutive Hasse derivatives as those whose multiindices have order less than r, where the order of a multiindex $(i_1, i_2, \ldots, i_m)$ is defined as $\sum_{j=1}^{m} i_j$. We will use the terms *standard multiplicities* to refer to this type of multiplicities. In this work, we consider arbitrary finite families $\mathcal{J}$ of multiindices that are consecutive in a coordinate-wise sense: if $(i_1, i_2, \ldots, i_m)$ belongs to $\mathcal{J}$ and $k_j \leq i_j$, for $j = 1, 2, \ldots, m$, then $(k_1, k_2, \ldots, k_m)$ also belongs to $\mathcal{J}$. Obviously, the (finite) family $\mathcal{J}$ of multiindices of order less than a given positive integer r satisfies this property, hence is a particular case.

Our main contribution is an upper bound on the number of common zeros over a grid of a family of polynomials and their (Hasse) derivatives corresponding to a finite set $\mathcal{J}$ of consecutive multiindices. This upper bound makes use of the technique from Gröbner basis theory known as *footprint* [10, 15], and can be seen as an extension of the classical *footprint bound* [6, Section 5.3] in the sense of (I.2). A first extension for standard multiplicities has been given as Lemma 2.4 in the expanded version of [23].

We will then show that this bound is sharp for ideals of polynomials, characterize those which satisfy equality, and give as applications extensions of known results in algebra and combinatorics: Alon's combinatorial Nullstellensatz [1, 3, 5, 20, 22], existence and uniqueness of Hermite interpolating polynomials [9, 18, 21], estimations on the parameters of evaluation codes with consecutive derivatives [11, 18, 19], and the bounds by DeMillo and Lipton [7], Schwartz [24], Zippel [25, 26], and Alon and Füredi [2].

The bound given by Schwartz in [24, Lemma 1] can also be derived by those given by DeMillo and Lipton [7], and Zippel [25, Theorem 1], [26, Proposition 3] (see Proposition I.48 below), and is referred to as the *Schwartz-Zippel bound* in many works in the literature [8, 11, 18, 19]. Interestingly, an extension of such bound for standard multiplicities in the sense of (I.1) has been recently given in [8, Lemma 8], but as Counterexample 7.4 in [4] shows, no straightforward extension of the footprint bound in the sense of (I.1) seems possible (recall that we will give a bound in the sense of (I.2)). To conclude this work, we give an extension of the Schwartz-Zippel bound to derivatives with weighted order less than a given positive integer, which we will call *weighted multiplicities*. This bound is inspired by [8, Lemma 8], and we will discuss its connection with our extension of the footprint bound.

The results are organized as follows: We start with some preliminaries in Section 2. We then give the main bound in Section 3, together with some particular cases, an interpretation of the bound, and sharpness and equality conditions. In Section 4, we give a list of applications. Finally, in Section 5 we give an extension of the Schwartz-Zippel bound in the sense of (I.1) to weighted multiplicities, and discuss the connections with the bound in Section 3.

Notation

Throughout this paper, $\mathbb{F}$ denotes an arbitrary field. We denote by $\mathbb{F}[\mathbf{x}] = \mathbb{F}[x_1, x_2, \ldots, x_m]$ the ring of polynomials in the m variables $x_1, x_2, \ldots, x_m$ with coefficients in $\mathbb{F}$. A multiindex is a vector $\mathbf{i} = (i_1, i_2, \ldots, i_m) \in \mathbb{N}^m$, where $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$, and as usual we use the notation $\mathbf{x}^{\mathbf{i}} = x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m}$. We also denote $\mathbb{N}_+ = \{1, 2, 3, \ldots\}$.

In this work, $\preceq$ denotes the coordinate-wise partial ordering in $\mathbb{N}^m$, that is, $(i_1, i_2, \ldots, i_m) \preceq (j_1, j_2, \ldots, j_m)$ if $i_k \leq j_k$, for all $k = 1, 2, \ldots, m$. We will use $\preceq_m$ to denote a given monomial ordering in the set of monomials of $\mathbb{F}[\mathbf{x}]$ (see [6, Section 2.2]), and we denote by $\mathrm{LM}_{\preceq_m}(F(\mathbf{x}))$ the leading monomial of $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ with respect to $\preceq_m$, or just $\mathrm{LM}(F(\mathbf{x}))$ if there is no confusion about $\preceq_m$. Finally, the notation $\langle A \rangle$ means ideal generated by A in a ring, and $\langle A \rangle_{\mathbb{F}}$ means vector space over $\mathbb{F}$ generated by A.

2 Consecutive derivatives

In this work, we consider Hasse derivatives, introduced first in [13]. They coincide with usual derivatives except for multiplication with a non-zero constant factor when the corresponding multiindex contains no multiples of the characteristic of the field, and they have the advantage of not being identically zero otherwise.

Definition I.1 (Hasse derivative [13]). Let $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ be a polynomial. Given another family of independent variables $\mathbf{z} = (z_1, z_2, \ldots, z_m)$, the polynomial $F(\mathbf{x}+\mathbf{z})$ can be written uniquely as

$$F(\mathbf{x}+\mathbf{z}) = \sum_{\mathbf{i} \in \mathbb{N}^m} F^{(\mathbf{i})}(\mathbf{x})\mathbf{z}^{\mathbf{i}},$$

for some polynomials $F^{(\mathbf{i})}(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$, for $\mathbf{i} \in \mathbb{N}^m$. For a given multiindex $\mathbf{i} \in \mathbb{N}^m$, we define the $\mathbf{i}$-th Hasse derivative of $F(\mathbf{x})$ as the polynomial $F^{(\mathbf{i})}(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$.

We next formalize the concept of zero of a polynomial of at least a given multiplicity as that of common zero of the given polynomial and a given finite family of its derivatives:

Definition I.2. Let $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ be a polynomial, let $\mathbf{a} \in \mathbb{F}^m$ be an affine point, and let $\mathcal{J} \subseteq \mathbb{N}^m$ be a finite set. We say that $\mathbf{a}$ is a zero of $F(\mathbf{x})$ of multiplicity at least $\mathcal{J}$ if $F^{(\mathbf{i})}(\mathbf{a}) = 0$, for all $\mathbf{i} \in \mathcal{J}$.

The concept of *consecutive derivatives*, in a coordinate-wise sense, can be formalized by the concept of *decreasing sets* of multiindices (recall that $\preceq$ denotes the coordinate-wise ordering in $\mathbb{N}^m$):

Definition I.3 (Decreasing sets). We say that the set $\mathcal{J} \subseteq \mathbb{N}^m$ is decreasing if whenever $\mathbf{i} \in \mathcal{J}$ and $\mathbf{j} \in \mathbb{N}^m$ are such that $\mathbf{j} \preceq \mathbf{i}$, it holds that $\mathbf{j} \in \mathcal{J}$.

Observe that the finite set $\mathcal{J} = \{(i_1, i_2, \ldots, i_m) \in \mathbb{N}^m : \sum_{j=1}^m i_j < r\}$, for a positive integer r, is decreasing. Moreover, if $m = 1$, then these are all possible decreasing finite sets. The concept of weighted orders and weighted multiplicities shows that this is not the case when $m > 1$:

Definition I.4 (Weighted multiplicities). Fix a vector of positive weights $\mathbf{w} = (w_1, w_2, \ldots, w_m) \in \mathbb{N}_+^m$. Given a multiindex $\mathbf{i} = (i_1, i_2, \ldots, i_m) \in \mathbb{N}^m$, we define its weighted order as

$$\mid \mathbf{i} \mid_{\mathbf{w}} = i_1 w_1 + i_2 w_2 + \cdots + i_m w_m. \tag{I.3}$$

Let $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ be a polynomial and let $\mathbf{a} \in \mathbb{F}^m$ be an affine point. We say that $\mathbf{a}$ is a zero of $F(\mathbf{x})$ of weighted multiplicity $r \in \mathbb{N}$, and we write

$$m_{\mathbf{w}}(F(\mathbf{x}), \mathbf{a}) = r,$$

if $F^{(\mathbf{i})}(\mathbf{a}) = 0$, for all $\mathbf{i} \in \mathbb{N}^m$ with $\mid \mathbf{i} \mid_{\mathbf{w}} < r$, and $F^{(\mathbf{j})}(\mathbf{a}) \neq 0$, for some $\mathbf{j} \in \mathbb{N}^m$ with $\mid \mathbf{j} \mid_{\mathbf{w}} = r$.

We also introduce the definition of weighted degree, which will be convenient for different results in the following sections:

Definition I.5 (Weighted degrees). Let $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ be a polynomial and let $\mathbf{w} \in \mathbb{N}_+^m$ be a vector of positive weights. We define the weighted degree of $F(\mathbf{x})$ as

$$\deg_{\mathbf{w}}(F(\mathbf{x})) = \max\{\mid \mathbf{i} \mid_{\mathbf{w}} : F_{\mathbf{i}} \neq 0\},$$

where $F(\mathbf{x}) = \sum_{\mathbf{i} \in \mathbb{N}^m} F_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}$ and $F_{\mathbf{i}} \in \mathbb{F}$, for all $\mathbf{i} \in \mathbb{N}^m$.

Other interesting sets of consecutive derivatives that we will consider throughout the paper are those given by bounding each index separately, that is, sets of the form $\mathcal{J} = \{(i_1, i_2, \ldots, i_m) \in \mathbb{N}^m : i_j < r_j, j = 1, 2, \ldots, m\}$, for a given $(r_1, r_2, \ldots, r_m) \in \mathbb{N}_+^m$, where $\preceq$ denotes the coordinate-wise partial ordering.

3 The footprint bound for consecutive derivatives

In this section, we will give an extension of the footprint bound [6, Section 5.3] to upper bound the number of common zeros over a finite grid of a family of polynomials and a given set of their consecutive derivatives, as in Definition I.2. We give some particular cases and an interpretation of the bound. We conclude by studying its sharpness.

Throughout the section, fix a decreasing finite set $\mathcal{J} \subseteq \mathbb{N}^m$, an ideal $I \subseteq \mathbb{F}[\mathbf{x}]$ and finite subsets $S_1, S_2, \ldots, S_m \subseteq \mathbb{F}$. Write $S = S_1 \times S_2 \times \cdots \times S_m$, and denote by $G_j(x_j) \in \mathbb{F}[x_j]$ the defining polynomial of S_j, that is, $G_j(x_j) = \prod_{s \in S_j}(x_j - s)$, for $j = 1, 2, \ldots, m$. The three objects involved in our bound are the following:

Definition I.6. We define the ideal

$$I_{\mathcal{J}} = I + \left\langle \left\{ \prod_{j=1}^{m} G_j(x_j)^{r_j} : (r_1, r_2, \ldots, r_m) \notin \mathcal{J} \right\} \right\rangle$$

and the set of zeros of multiplicity at least $\mathcal{J}$ of the ideal I in the grid $S = S_1 \times S_2 \times \cdots \times S_m$ as

$$\mathcal{V}_{\mathcal{J}}(I) = \left\{ \mathbf{a} \in S : F^{(\mathbf{i})}(\mathbf{a}) = 0, \forall F(\mathbf{x}) \in I, \forall \mathbf{i} \in \mathcal{J} \right\}.$$

Finally, given a monomial ordering $\preceq_m$, we define the footprint of an ideal $J \subseteq \mathbb{F}[\mathbf{x}]$ as

$$\Delta_{\preceq_m}(J) = \left\{ \mathbf{x}^{\mathbf{i}} : \mathbf{x}^{\mathbf{i}} \notin \langle \mathrm{LM}(J) \rangle \right\},$$

where $\mathrm{LM}(J) = \{\mathrm{LM}(F(\mathbf{x})) : F(\mathbf{x}) \in J\}$ with respect to the monomial ordering $\preceq_m$. We write $\Delta(J)$ if there is no confusion about the monomial ordering.

3.1 The general bound

Theorem I.1. *For any monomial ordering, it holds that*

$$\#\mathcal{V}_{\mathcal{J}}(I) \cdot \#\mathcal{J} \leq \#\Delta\left(I_{\mathcal{J}}\right). \tag{I.4}$$

The rest of the subsection is devoted to the proof of this result. The first auxiliary tool is the Leibniz formula, which follows by a straightforward computation (see also [14, pages 144–155]):

Lemma I.7 (Leibniz formula). *Let* $F_1(\mathbf{x}), F_2(\mathbf{x}), \ldots, F_s(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ *and let* $\mathbf{i} \in \mathbb{N}^m$. *It holds that*

$$\left(\prod_{j=1}^{s} F_j(\mathbf{x}) \right)^{(\mathbf{i})} = \sum_{\mathbf{i}_1 + \mathbf{i}_2 + \cdots + \mathbf{i}_s = \mathbf{i}} \left(\prod_{j=1}^{s} F_j^{(\mathbf{i}_j)}(\mathbf{x}) \right).$$

The second auxiliary tool is the existence of Hermite interpolating polynomials with Hasse derivatives. For our purposes, a *separated-variables* extension of univariate Hermite interpolation over grids is enough. This extension is straightforward and seems to be known in the literature (see [21, Section 3.1]), but we give a short proof in the Appendix for convenience of the reader.

Definition I.8. We define the evaluation map on a finite set $T \subseteq \mathbb{F}^m$ with derivatives corresponding to multiindices in $\mathcal{J}$ as

$$\begin{aligned} \mathrm{Ev} : & \mathbb{F}[\mathbf{x}] \longrightarrow \mathbb{F}^{\#T \cdot \#\mathcal{J}} \\ & F(\mathbf{x}) \mapsto \left(\left(F^{(\mathbf{i})}(\mathbf{a}) \right)_{\mathbf{i} \in \mathcal{J}} \right)_{\mathbf{a} \in T}. \end{aligned} \tag{I.5}$$

Lemma I.9 (Hermite interpolation). *The evaluation map* $\mathrm{Ev} : \mathbb{F}[\mathbf{x}] \longrightarrow \mathbb{F}^{\#T \cdot \#\mathcal{J}}$ *defined in (I.5) is surjective, for all finite sets* $T \subseteq \mathbb{F}^m$ *and* $\mathcal{J} \subseteq \mathbb{N}^m$.

Proof. See the Appendix. □

With these tools, we may now prove Theorem I.1:

Proof of Theorem I.1. Fix multiindices $\mathbf{r} = (r_1, r_2, \ldots, r_m) \notin \mathcal{J}$ and $\mathbf{i} = (i_1, i_2, \ldots, i_m) \in \mathcal{J}$, and define $G(\mathbf{x}) = \prod_{j=1}^{m} G_j(x_j)^{r_j}$. By Lemma I.7, it holds that

$$G^{(\mathbf{i})}(\mathbf{x}) = \prod_{j=1}^{m} \left(G_j(x_j)^{r_j} \right)^{(i_j)}. \tag{I.6}$$

Furthermore, if $r > i$ and $F(x) \in \mathbb{F}[x]$, then there exists $H(x) \in \mathbb{F}[x]$ such that

$$\left(F(x)^r \right)^{(i)} = \sum_{i_1+i_2+\cdots+i_r=i} \left(\prod_{j=1}^{r} F^{(i_j)}(x) \right) = H(x)F(x)^{r-i}, \tag{I.7}$$

again by Lemma I.7, since at least $r - i > 0$ indices i_j must be equal to 0, for each $(i_1, i_2, \ldots, i_m) \in \mathbb{N}^m$ such that $\sum_{j=1}^{m} i_j = i$. Finally, since $\mathcal{J}$ is decreasing, it holds that $\mathbf{r} - \mathbf{i}$ has at least one positive coordinate. Hence, combining (I.6) and (I.7), we see that $G^{(\mathbf{i})}(\mathbf{a}) = 0$, for all $\mathbf{a} \in \mathcal{V}_{\mathcal{J}}(I) \subseteq S$. This implies that

$$\mathrm{Ev}(F(\mathbf{x})) = \mathbf{0}, \quad \forall F(\mathbf{x}) \in I_{\mathcal{J}},$$

by the definition of the ideal $I_{\mathcal{J}}$ and the set $\mathcal{V}_{\mathcal{J}}(I)$, and where we consider $T = \mathcal{V}_{\mathcal{J}}(I)$ in the definition of Ev (Definition I.8).

Therefore, the evaluation map Ev can be extended to the quotient ring

$$\mathrm{Ev} : \mathbb{F}[\mathbf{x}]/I_{\mathcal{J}} \longrightarrow \mathbb{F}^{\#\mathcal{V}_{\mathcal{J}}(I) \cdot \#\mathcal{J}},$$

which is again surjective, since the original evaluation map is surjective by Lemma I.9. Since the domain and codomain of this map are $\mathbb{F}$-linear vector spaces and the map itself is also $\mathbb{F}$-linear, we conclude that

$$\#\mathcal{V}_{\mathcal{J}}(I) \cdot \#\mathcal{J} = \dim_{\mathbb{F}} \left(\mathbb{F}^{\#\mathcal{V}_{\mathcal{J}}(I) \cdot \#\mathcal{J}} \right) \leq \dim_{\mathbb{F}} \left(\mathbb{F}[\mathbf{x}]/I_{\mathcal{J}} \right).$$

Finally, Proposition 4 in [6, Section 5.3] says that the monomials in $\Delta(J)$ constitute a basis of $\mathbb{F}[\mathbf{x}]/J$, for an ideal $J \subseteq \mathbb{F}[\mathbf{x}]$. This fact implies that

$$\dim_{\mathbb{F}} \left(\mathbb{F}[\mathbf{x}]/I_{\mathcal{J}} \right) = \#\Delta \left(I_{\mathcal{J}} \right),$$

and the result follows. □

3.2 Some particular cases

In this subsection, we derive some particular cases of Theorem I.1. We start with the classical form of the footprint bound (see Proposition 8 in [6, Section 5.3], and [10, 15]):

Corollary I.10 ([6, 10, 15]). *Setting $\mathcal{J} = \{\mathbf{0}\}$, we obtain that*

$$\#\mathcal{V}(I) \leq \#\Delta\left(I + \langle G_1(x_1), G_2(x_2), \ldots, G_m(x_m)\rangle\right),$$

where $\mathcal{V}(I)$ denotes the set of zeros of the ideal I in S.

The case of zeros of standard multiplicity at least a given positive integer was first obtained as Lemma 2.4 in the extended version of [23], and reads as follows:

Corollary I.11 ([23]). *Given an integer $r \in \mathbb{N}_+$, and setting $\mathcal{J} = \{(i_1, i_2, \ldots, i_m) \in \mathbb{N}^m : \sum_{j=1}^{m} i_j < r\}$, we obtain that*

$$\#\mathcal{V}_{\geq r}(I) \cdot \binom{m+r-1}{m} \leq \#\Delta\left(I + \left\langle\left\{\prod_{j=1}^{m} G_j(x_j)^{r_j} : \sum_{j=1}^{m} r_j = r\right\}\right\rangle\right),$$

where $\mathcal{V}_{\geq r}(I)$ denotes the set of zeros of multiplicity at least r of the ideal I in S.

Another particular case is obtained when upper bounding each coordinate of the multiindices separately:

Corollary I.12. *Given a multiindex $(r_1, r_2, \ldots, r_m) \in \mathbb{N}_+^m$, and setting $\mathcal{J} = \{(i_1, i_2, \ldots, i_m) \in \mathbb{N}^m : i_j < r_j, j = 1, 2, \ldots, m\}$, we obtain that*

$$\#\mathcal{V}_{\mathcal{J}}(I) \cdot \prod_{j=1}^{m} r_j \leq \#\Delta\left(I + \langle G_1(x_1)^{r_1}, G_2(x_2)^{r_2}, \ldots, G_m(x_m)^{r_m}\rangle\right).$$

Finally, we obtain a footprint bound for weighted multiplicities:

Corollary I.13. *Given an integer $r \in \mathbb{N}_+$, a vector of positive weights $\mathbf{w} = (w_1, w_2, \ldots, w_m) \in \mathbb{N}_+$, and setting $\mathcal{J} = \{\mathbf{i} \in \mathbb{N}^m :\mid \mathbf{i} \mid_{\mathbf{w}} < r\}$, we obtain that*

$$\#\mathcal{V}_{\geq r, \mathbf{w}}(I) \cdot \mathrm{B}(\mathbf{w}; r) \leq \#\Delta\left(I + \left\langle\left\{\prod_{j=1}^{m} G_j(x_j)^{r_j} : \sum_{j=1}^{m} r_j w_j \geq r\right\}\right\rangle\right),$$

where $\mathcal{V}_{\geq r, \mathbf{w}}(I)$ denotes the set of zeros of weighted multiplicity at least r of the ideal I in S, and where $\mathrm{B}(\mathbf{w}; r) = \#\{\mathbf{i} \in \mathbb{N}^m :\mid \mathbf{i} \mid_{\mathbf{w}} < r\}$.

To conclude, we give a more explicit form of the bound in the previous corollary by estimating the number $B(\mathbf{w}; r)$:

Corollary I.14. *Given an integer $r \in \mathbb{N}_+$ and a vector of positive weights $\mathbf{w} = (w_1, w_2, \ldots, w_m) \in \mathbb{N}_+$, it holds that*

$$\binom{m+r-1}{m} \leq w_1 w_2 \cdots w_m B(\mathbf{w}; r). \tag{I.8}$$

In particular, we deduce from the previous corollary that

$$\#\mathcal{V}_{\geq r,\mathbf{w}}(I)\cdot\binom{m+r-1}{m}$$
$$\leq w_1w_2\cdots w_m\cdot\#\Delta\left(I+\left\langle\left\{\prod_{j=1}^{m}G_j(x_j)^{r_j}:\sum_{j=1}^{m}r_jw_j\geq r\right\}\right\rangle\right).$$

Proof. Define the map $T_{\mathbf{j}}:\mathbb{N}^m\longrightarrow\mathbb{N}^m$ by

$$T_{\mathbf{j}}(\mathbf{i})=(i_1w_1+j_1,i_2w_2+j_2,\ldots,i_mw_m+j_m),$$

for all $\mathbf{i}=(i_1,i_2,\ldots,i_m),\mathbf{j}=(j_1,j_2,\ldots,j_m)\in\mathbb{N}^m$. Now define $\mathcal{J}(\mathbf{w};r)=\{\mathbf{i}\in\mathbb{N}^m:\mid\mathbf{i}\mid_{\mathbf{w}}<r\}$. By the Euclidean division, we see that

$$\mathcal{J}((1,1,\ldots,1);r)\subseteq\bigcup_{\mathbf{j}\in\prod_{k=1}^{m}[0,w_k)}T_{\mathbf{j}}\left(\mathcal{J}\left(\mathbf{w};r\right)\right).$$

By counting elements on both sides of the inclusion, the result follows. □

3.3 Interpreation of the bound and illustration of the set $\Delta(I_{\mathcal{J}})$

In this subsection, we give a graphical description of the footprint $\Delta(I_{\mathcal{J}})$ which will allow us to provide an interpretation of the bound (I.4).

First, we observe that by adding the polynomials $\prod_{i=1}^{m}G_i(x_i)^{r_i}$, for $(r_1,r_2,\ldots,r_m)\notin\mathcal{J}$, we are bounding the set of points $\Delta(I_{\mathcal{J}})$ by a certain subset $\mathcal{J}_S\subseteq\mathbb{N}^m$, which we now define:

Definition I.15. We define the set

$$\mathcal{J}_S=\left\{\mathbf{i}\in\mathbb{N}^m:\mathbf{i}\not\succeq(r_1\#S_1,r_2\#S_2,\ldots,r_m\#S_m),\forall(r_1,r_2,\ldots,r_m)\notin\mathcal{J}\right\}.$$

For clarity, we now give a description of this set by a positive defining condition that follows from the properties of the Euclidean division and the fact that $\mathcal{J}$ is decreasing.

Lemma I.16. *It holds that*

$$\mathcal{J}_S=\{\,(p_1\#S_1+t_1,p_2\#S_2+t_2,\ldots,p_m\#S_m+t_m)\in\mathbb{N}^m:$$
$$(p_1,p_2,\ldots,p_m)\in\mathcal{J},0\leq t_j<\#S_j,\forall j=1,2,\ldots,m\}.$$

We may then state the fact that the footprint is bounded by this set as follows:

Lemma I.17. *It holds that*

$$\Delta(I_{\mathcal{J}})\subseteq\{\mathbf{x}^{\mathbf{i}}:\mathbf{i}\in\mathcal{J}_S\}.$$

Moreover, the set $\mathcal{J}_S$ can be easily seen as the union of $\#\mathcal{J}$ m-dimensional rectangles in $\mathbb{N}^m$ whose sides have lengths $\#S_1$, $\#S_2$, ..., $\#S_m$, respectively. In particular, we obtain the following:

Lemma I.18. *It holds that*

$$\#\mathcal{J}_S = \#S \cdot \#\mathcal{J}. \tag{I.9}$$

The footprint bound (I.4) can then be interpreted as follows: Consider the set $\mathcal{J}_S \subseteq \mathbb{N}^m$. For each $\mathbf{x}^{\mathbf{i}} \in \mathrm{LM}(I_{\mathcal{J}})$, remove from $\mathcal{J}_S$ all points $\mathbf{j}$ such that $\mathbf{i} \preceq \mathbf{j}$. The remaining points correspond to the multiindices in $\Delta(I_{\mathcal{J}})$, and thus there are $\#\Delta(I_{\mathcal{J}})$ of them.

In particular, if $F_1(\mathbf{x}), F_2(\mathbf{x}), \ldots, F_t(\mathbf{x}) \in I$, then we may only remove the points corresponding to $\mathrm{LM}(F_i(\mathbf{x}))$, for $i = 1, 2, \ldots, t$, and we obtain an upper bound on $\#\Delta(I_{\mathcal{J}})$.

Example I.19. Let us assume now that $m = 2$, $\#S_1 = \#S_2 = 2$, and $\mathcal{J} = \{(0,1), (1,1), (2,1), (0,0), (1,0), (2,0), (3,0), (4,0), (5,0)\}$.

In Figure I.1, top image, we represent by black dots the monomials whose multiindices belong to $\mathcal{J}_S$. Blank dots correspond to multiindices that do not belong to $\mathcal{J}_S$. Among all dots, medium-sized and large dots correspond to multiindices that belong to $\mathcal{J}$ when each coordinate is multiplied by 2, and the largest blank dots correspond to minimal multiindices that do not belong to $\mathcal{J}_S$.

In Figure I.1, bottom image, we represent in the same way the set $\Delta(I_{\mathcal{J}})$, whenever $\langle \mathrm{LM}(I_{\mathcal{J}}) \rangle$ is generated by $x_1^2 x_2^3$, $x_1^8 x_2$, and the leading monomials of $G_1(x_1)^{r_1} G_2(x_2)^{r_2}$, for minimal $(r_1, r_2) \notin \mathcal{J}$, which in this case are x_2^4, $x_1^6 x_2^2$ and x_1^{12}.

In conclusion, the bound (I.4) says that the number of zeros in S of I of multiplicity at least $\mathcal{J}$ is at most 3.

As a consequence of this interpretation, we may deduce the following useful fact:

Lemma I.20. *Assume that the finite set $\mathcal{J} \subseteq \mathbb{N}^m$ is decreasing and $\mathbf{x}^{\mathbf{i}} = \mathrm{LM}(F(\mathbf{x}))$ with respect to some monomial ordering, for some polynomial $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$. If $\mathbf{i} \in \mathcal{J}_S$, then it holds that*

$$\#\Delta(\langle F(\mathbf{x}) \rangle_{\mathcal{J}}) < \#S \cdot \#\mathcal{J}. \tag{I.10}$$

We conclude with a simple description of $\mathcal{J}_S$ in the cases of multiindices bounded by weighted orders and multiindices bounded on each coordinate separately, which follow by straightforward calculations:

Remark I.21. *Given a vector of positive weights $\mathbf{w} = (w_1, w_2, \ldots, w_m) \in \mathbb{N}_+^m$, a positive integer $r \in \mathbb{N}_+$, and $\mathcal{J} = \{\mathbf{r} \in \mathbb{N}^m : \mid \mathbf{r} \mid_{\mathbf{w}} < r\}$, it holds that*

$$\mathcal{J}_S = \left\{ (i_1, i_2, \ldots, i_m) \in \mathbb{N}^m : \sum_{j=1}^{m} \left\lfloor \frac{i_j}{\#S_j} \right\rfloor w_j < r \right\}.$$

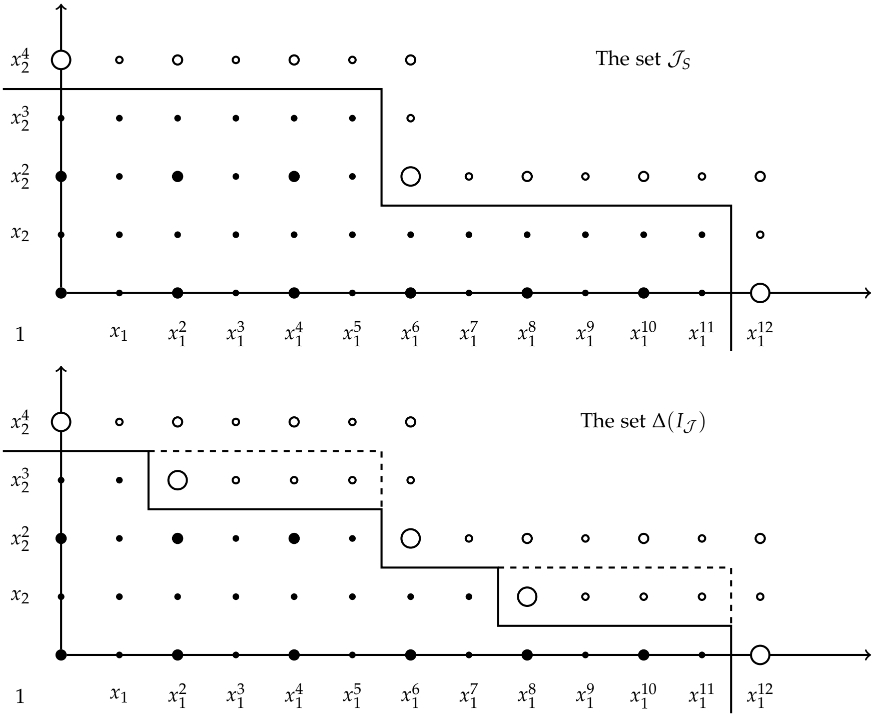

Fig. I.1: Illustration of the sets $\mathcal{J}_S$ and $\Delta(I_{\mathcal{J}})$ in $\mathbb{N}^m$.

On the other hand, given $(r_1, r_2, \ldots, r_m) \in \mathbb{N}_+^m$ *and* $\mathcal{J} = \{(i_1, i_2, \ldots, i_m) \in \mathbb{N}^m : i_j < r_j,\ j = 1, 2, \ldots, m\}$*, it holds that*

$$\mathcal{J}_S = \left\{(i_1, i_2, \ldots, i_m) \in \mathbb{N}^m : i_j < r_j \# S_j, j = 1, 2, \ldots, m\right\}.$$

3.4 Sharpness and equality conditions

To conclude the section, we study the sharpness of the bound (I.4). We will give sufficient and necessary conditions on the ideal I for (I.4) to be an equality, and we will see that (I.4) is the sharpest bound that can be obtained as a strictly increasing function of the size of the footprint $\Delta(I_{\mathcal{J}})$.

We start by defining the ideal associated to a set of points and a set of multiindices.

Definition I.22. Given $\mathcal{V} \subseteq \mathbb{F}^m$, we define

$$I(\mathcal{V}; \mathcal{J}) = \left\{F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}] : F^{(\mathbf{i})}(\mathbf{a}) = 0, \forall \mathbf{a} \in \mathcal{V}, \forall \mathbf{i} \in \mathcal{J}\right\}.$$

In the next proposition we show that this set is indeed an ideal and gather other properties similar to those of ideals and algebraic sets in algebraic geometry.

Proposition I.23. *Given a set of points $\mathcal{V} \subseteq \mathbb{F}^m$, the set $I(\mathcal{V}; \mathcal{J})$ in the previous definition is an ideal in $\mathbb{F}[\mathbf{x}]$. Moreover, the following properties hold:*

1. $I \subseteq I(\mathcal{V}_{\mathcal{J}}(I); \mathcal{J})$.
2. $\mathcal{V} \subseteq \mathcal{V}_{\mathcal{J}}(I(\mathcal{V}; \mathcal{J}))$.
3. $I = I(\mathcal{V}_{\mathcal{J}}(I); \mathcal{J})$ *if, and only if,* $I = I(\mathcal{W}; \mathcal{J})$ *for some set* $\mathcal{W} \subseteq \mathbb{F}^m$.
4. $\mathcal{V} = \mathcal{V}_{\mathcal{J}}(I(\mathcal{V}; \mathcal{J}))$ *if, and only if,* $\mathcal{V} = \mathcal{V}_{\mathcal{J}}(K)$, *for some ideal* $K \subseteq \mathbb{F}[\mathbf{x}]$.

Proof. The fact that $I(\mathcal{V}; \mathcal{J})$ is an ideal follows from the Leibniz formula (Lemma I.7) and the fact that $\mathcal{J}$ is decreasing. The properties in items 1, 2, 3, and 4 follow as in classical algebraic geometry and are left to the reader. □

The following is the main result of the subsection:

Theorem I.2. *Fixing a monomial ordering, the bound (I.4) is an equality if, and only if,*

$$I_{\mathcal{J}} = I\left(\mathcal{V}_{\mathcal{J}}(I); \mathcal{J}\right). \tag{I.11}$$

In particular, for any choice of decreasing finite set $\mathcal{J} \subseteq \mathbb{N}^m$ and a finite set of points $\mathcal{V} \subseteq \mathbb{F}^m$, there exists an ideal, $I = I(\mathcal{V}; \mathcal{J})$, satisfying equality in (I.4).

Proof. With notation as in the proof of Theorem I.1, the evaluation map $\mathrm{Ev} : \mathbb{F}[\mathbf{x}] \longrightarrow \mathbb{F}^{\#\mathcal{V}_{\mathcal{J}}(I) \cdot \#\mathcal{J}}$ from Definition I.8 is $\mathbb{F}$-linear and surjective by Lemma I.9. By definition, its kernel is

$$\mathrm{Ker}(\mathrm{Ev}) = I(\mathcal{V}_{\mathcal{J}}(I); \mathcal{J}).$$

On the other hand, we saw in the proof of Theorem I.1 that $I_{\mathcal{J}} \subseteq \mathrm{Ker}(\mathrm{Ev})$. This means that the evaluation map

$$\mathrm{Ev} : \mathbb{F}[\mathbf{x}]/I_{\mathcal{J}} \longrightarrow \mathbb{F}^{\#\mathcal{V}_{\mathcal{J}}(I) \cdot \#\mathcal{J}}$$

is an isomorphism if, and only if, $I_{\mathcal{J}} = I(\mathcal{V}_{\mathcal{J}}(I); \mathcal{J})$.

Finally, the fact that this evaluation map is an isomorphism is equivalent to (I.4) being an equality, by the proof of Theorem I.1. Together with Proposition I.23 and the fact that $I = I_{\mathcal{J}}$ if $I = I(\mathcal{V}; \mathcal{J})$ by the proof of Theorem I.1, the theorem follows. □

Thanks to this result, we may establish that the bound (I.4) is the sharpest bound that is a strictly increasing function of the size of the footprint $\Delta(I_{\mathcal{J}})$, in the following sense: If equality holds for such a bound, then it holds in (I.4).

Corollary I.24. *Let $f : \mathbb{N} \longrightarrow \mathbb{R}$ be a strictly increasing function, and assume that*

$$\#\mathcal{V}_{\mathcal{J}}(I) \leq f(\#\Delta(I_{\mathcal{J}})), \tag{I.12}$$

for all ideals $I \subseteq \mathbb{F}[\mathbf{x}]$. If equality holds in (I.12) for a given ideal $I \subseteq \mathbb{F}[\mathbf{x}]$, then equality holds in (I.4) for such ideal.

Proof. First we have that $I_{\mathcal{J}} \subseteq I(\mathcal{V}_{\mathcal{J}}(I); \mathcal{J})$ as we saw in the proof of the previous theorem. Hence the reverse inclusion holds for their footprints and thus

$$f\left(\#\Delta\left(I\left(\mathcal{V}_{\mathcal{J}}(I); \mathcal{J}\right)\right)\right) \leq f(\#\Delta(I_{\mathcal{J}})). \tag{I.13}$$

Now, since $\mathcal{V}_{\mathcal{J}}(I) = \mathcal{V}_{\mathcal{J}}(I(\mathcal{V}_{\mathcal{J}}(I); \mathcal{J}))$ by Proposition I.23, and equality holds in (I.12) for I, we have that

$$f(\#\Delta(I_{\mathcal{J}})) = \#\mathcal{V}_{\mathcal{J}}(I) = \#\mathcal{V}_{\mathcal{J}}(I(\mathcal{V}_{\mathcal{J}}(I); \mathcal{J})) \leq f(\#\Delta(I(\mathcal{V}_{\mathcal{J}}(I); \mathcal{J}))). \tag{I.14}$$

Combining (I.13) and (I.14), and using that f is strictly increasing, we conclude that

$$\#\Delta(I(\mathcal{V}_{\mathcal{J}}(I); \mathcal{J})) = \#\Delta(I_{\mathcal{J}}),$$

which implies that equality holds in (I.4) for I by Theorem I.2, and we are done. □

4 Applications of the footprint bound for consecutive derivatives

In this section, we present a brief collection of applications of Theorem I.1, which are extensions to consecutive derivatives of well-known important results from the literature. Throughout the section, we will fix again finite sets $S_1, S_2, \ldots, S_m \subseteq \mathbb{F}$ and $S = S_1 \times S_2 \times \cdots \times S_m$.

4.1 Alon's combinatorial Nullstellensatz

The combinatorial Nullstellensatz is a non-vanishing theorem by Alon [1, Theorem 1.2] with many applications in combinatorics. It has been extended to non-vanishing theorems for standard multiplicities in [3, Corollary 3.2] and for multisets (sets with multiplicities) in [20, Theorem 6].

In this subsection, we establish and prove a combinatorial Nullstellensatz for consecutive derivatives and derive the well-known particular cases as corollaries. The formulation in [1, Theorem 1.1] is equivalent in essence. We will extend that result in the next subsection in terms of Gröbner bases.

Theorem I.3. *Let $\mathcal{J} \subseteq \mathbb{N}^m$ be a decreasing finite set, let $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ be a non-zero polynomial, and let $\mathbf{x}^{\mathbf{i}} = \mathrm{LM}(F(\mathbf{x}))$ for some monomial ordering. If $\mathbf{i} \in \mathcal{J}_S$, then there exist $\mathbf{s} \in S$ and $\mathbf{j} \in \mathcal{J}$ such that*

$$F^{(\mathbf{j})}(\mathbf{s}) \neq 0.$$

Proof. By Lemma I.20, the assumptions imply that

$$\#\Delta(\langle F(\mathbf{x})\rangle_{\mathcal{J}}) < \#S \cdot \#\mathcal{J}.$$

On the other hand, Theorem I.1 implies that

$$\#\mathcal{V}_{\mathcal{J}}(F(\mathbf{x})) \cdot \#\mathcal{J} \leq \#\Delta(\langle F(\mathbf{x})\rangle_{\mathcal{J}}).$$

Therefore not all points in S are zeros of $F(\mathbf{x})$ of multiplicity at least $\mathcal{J}$, and the result follows. □

We now derive the original theorem [1, Theorem 1.2]. This constitutes an alternative proof. See also [22] for another recent short proof.

Corollary I.25 ([1]). *Let $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$. Assume that the coefficient of $\mathbf{x}^{\mathbf{i}}$ in $F(\mathbf{x})$ is not zero and $\deg(F(\mathbf{x})) =\mid \mathbf{i} \mid$. If $\#S_j > i_j$ for all $j = 1, 2, \ldots, m$, then there exist $s_1 \in S_1$, $s_2 \in S_2$, ..., $s_m \in S_m$, such that*

$$F(s_1, s_2, \ldots, s_m) \neq 0.$$

Proof. First, there exists a graded monomial ordering such that $\mathbf{x}^{\mathbf{i}} = \mathrm{LM}(F(\mathbf{x}))$ since $\deg(F(\mathbf{x})) =\mid \mathbf{i} \mid$. Now, the assumption implies that

$$\mathbf{i} \not\succeq (r_1\#S_1, r_2\#S_2, \ldots, r_m\#S_m),$$

for all $\mathbf{r} = (r_1, r_2, \ldots, r_m)$ such that $r_j = 1$ for some j, and the rest are zero. These are in fact all minimal multiindices not in $\mathcal{J} = \{\mathbf{0}\}$. Thus the result follows from the previous theorem. □

The next consequence is a combinatorial Nullstellensatz for weighted multiplicities, where the particular case $w_1 = w_2 = \ldots = w_m = 1$ coincides with [3, Corollary 3.2] (recall the definition of weighted degree from Definition I.5):

Corollary I.26. *Let $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$, let $\mathbf{w} = (w_1, w_2, \ldots, w_m) \in \mathbb{N}_+^m$ and let $r \in \mathbb{N}_+$. Assume that the coefficient of $\mathbf{x}^{\mathbf{i}}$ in $F(\mathbf{x})$ is not zero and $\deg_{\mathbf{w}}(F(\mathbf{x})) =\mid \mathbf{i} \mid_{\mathbf{w}}$.*

Assume also that, for all $\mathbf{r} = (r_1, r_2, \ldots, r_m)$ with $\mid \mathbf{r} \mid_{\mathbf{w}} \geq r$, there exists a j such that $r_j\#S_j > i_j$. Then there exist $s_1 \in S_1$, $s_2 \in S_2$, ..., $s_m \in S_m$, and some $\mathbf{j} \in \mathbb{N}^m$ with $\mid \mathbf{j} \mid_{\mathbf{w}} < r$, such that

$$F^{(\mathbf{j})}(s_1, s_2, \ldots, s_m) \neq 0.$$

Proof. It follows from Theorem I.3 as the previous corollary. □

We conclude with a combinatorial Nullstellensatz for multiindices bounded on each coordinate separately:

Corollary I.27. *Let $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$, let $(r_1, r_2, \ldots, r_m) \in \mathbb{N}_+^m$, and assume that $\mathbf{x}^{\mathbf{i}} = \mathrm{LM}(F(\mathbf{x}))$, $\mathbf{i} = (i_1, i_2, \ldots, i_m)$, for some monomial ordering and $i_j < r_j \# S_j$, for all $j = 1, 2, \ldots, m$. There exist $s_1 \in S_1$, $s_2 \in S_2$, …, $s_m \in S_m$, and some $\mathbf{j} = (j_1, j_2, \ldots, j_m) \in \mathbb{N}^m$ with $j_k < r_k$, for all $k = 1, 2, \ldots, m$, such that*

$$F^{(\mathbf{j})}(s_1, s_2, \ldots, s_m) \neq 0.$$

4.2 Gröbner bases of ideals of zeros in a grid

An equivalent but more refined consequence is obtaining a Gröbner basis for ideals $I(S; \mathcal{J})$ associated to the whole grid S and to a consecutive finite set of derivatives (recall Definition I.22). This result is also usually referred to as combinatorial Nullstellensatz in many works in the literature (see [1, Theorem 1.1], [3, Theorem 3.1] and [20, Theorem 1]). We briefly recall the notion of Gröbner basis. We will also make repeated use of the Euclidean division on the multivariate polynomial ring and its properties. See [6, Chapter 2] for more details.

Definition I.28 (Gröbner bases). Given a monomial ordering $\preceq_m$ and an ideal $I \subseteq \mathbb{F}[\mathbf{x}]$, we say that a finite family of polynomials $\mathcal{F} \subseteq I$ is a Gröbner basis of I with respect to $\preceq_m$ if

$$\langle \mathrm{LM}_{\preceq_m}(I) \rangle = \langle \mathrm{LM}_{\preceq_m}(\mathcal{F}) \rangle .$$

Moreover, we say that $\mathcal{F}$ is reduced if, for any two distinct $F(\mathbf{x}), G(\mathbf{x}) \in \mathcal{F}$, it holds that $\mathrm{LM}_{\preceq_m}(F(\mathbf{x}))$ does not divide any monomial in $G(\mathbf{x})$.

Recall that a Gröbner basis of an ideal generates it as an ideal. To obtain reduced Gröbner bases, we need a way to minimally generate decreasing finite sets in $\mathbb{N}^m$, which is given by the following object:

Definition I.29. For any decreasing finite set $\mathcal{J} \subseteq \mathbb{N}^m$, we define

$$\mathcal{B}_{\mathcal{J}} = \{\mathbf{i} \notin \mathcal{J} : \mathbf{j} \notin \mathcal{J} \text{ and } \mathbf{j} \preceq \mathbf{i} \Longrightarrow \mathbf{i} = \mathbf{j}\}.$$

The main result of this subsection is the following:

Theorem I.4. *For any decreasing finite set $\mathcal{J} \subseteq \mathbb{N}^m$, the family*

$$\mathcal{F} = \left\{ \prod_{j=1}^{m} G_j(x_j)^{r_j} : (r_1, r_2, \ldots, r_m) \in \mathcal{B}_{\mathcal{J}} \right\}$$

is a reduced Gröbner basis of the ideal $I(S;\mathcal{J})$ *with respect to any monomial ordering. In particular, for any* $F(\mathbf{x}) \in I(S;\mathcal{J})$*, there exist polynomials* $H_{\mathbf{r}}(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ *such that*

$$\deg(H_{\mathbf{r}}(\mathbf{x})) + \sum_{j=1}^{m} r_j \deg(G_j(x_j)) \leq \deg(F(\mathbf{x})),$$

for $\mathbf{r} = (r_1, r_2, \ldots, r_m) \in \mathcal{B}_{\mathcal{J}}$*, and*

$$F(\mathbf{x}) = \sum_{\mathbf{r} \in \mathcal{B}_{\mathcal{J}}} \left(H_{\mathbf{r}}(\mathbf{x}) \prod_{j=1}^{m} G_j(x_j)^{r_j} \right).$$

Proof. It suffices to prove that, if $F(\mathbf{x}) \in I(S;\mathcal{J})$ and we divide it by the family $\mathcal{F}$ (in an arbitrary order), then the remainder must be the zero polynomial.

Performing such division, we obtain $F(\mathbf{x}) = G(\mathbf{x}) + R(\mathbf{x})$, where $R(\mathbf{x})$ is the remainder of the division and $G(\mathbf{x}) \in I(S;\mathcal{J})$. Assume that $R(\mathbf{x}) \neq 0$ and let $\mathbf{x}^{\mathbf{i}}$ be the leading monomial of $R(\mathbf{x})$ with respect to the chosen monomial ordering. Since no leading monomial of the polynomials in $\mathcal{F}$ divides $\mathbf{x}^{\mathbf{i}}$, we conclude that

$$\mathbf{i} \not\succeq (r_1 \# S_1, r_2 \# S_2, \ldots, r_m \# S_m),$$

for all minimal $\mathbf{r} = (r_1, r_2, \ldots, r_m) \notin \mathcal{J}$, that is, for all $\mathbf{r} \in \mathcal{B}_{\mathcal{J}}$. Thus by Theorem I.3, we conclude that not all points in S are zeros of $R(\mathbf{x})$ of multiplicity at least $\mathcal{J}$, which is absurd since $R(\mathbf{x}) = F(\mathbf{x}) - G(\mathbf{x}) \in I(S;\mathcal{J})$, and we are done.

The fact that $\mathcal{F}$ is reduced follows from observing that the multiindices $\mathbf{r} \in \mathcal{B}_{\mathcal{J}}$ are minimal among those not in $\mathcal{J}$. The last part of the theorem follows by performing the Euclidean division. □

The following particular case is [1, Theorem 1.1]:

Corollary I.30 ([1]). *If* $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ *vanishes at all points in* S*, then there exist polynomials* $H_j(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ *such that* $\deg(H_j(\mathbf{x})) + \deg(G_j(x_j)) \leq \deg(F(\mathbf{x}))$*, for* $j = 1, 2, \ldots, m$*, and*

$$F(\mathbf{x}) = \sum_{j=1}^{m} H_j(\mathbf{x}) G_j(x_j).$$

To study the case of weighted multiplicities, we observe the following:

Remark I.31. *Given a vector of positive weights* $\mathbf{w} = (w_1, w_2, \ldots, w_m) \in \mathbb{N}_+^m$*, a positive integer* $r \in \mathbb{N}_+$*, and the set* $\mathcal{J} = \{\mathbf{i} \in \mathbb{N}^m :\mid \mathbf{i} \mid_{\mathbf{w}} < r\}$*, it holds that* $\mathcal{B}_{\mathcal{J}} = \mathcal{B}_{\mathbf{w}}$*, where*

$$\mathcal{B}_{\mathbf{w}} = \left\{ (i_1, i_2, \ldots, i_m) \in \mathbb{N}^m : r \leq \sum_{j=1}^{m} i_j w_j < r + \min\left\{ w_j : i_j \neq 0 \right\} \right\}.$$

We then obtain the next consequence, where the particular case $w_1 = w_2 = \ldots = w_m = 1$ coincides with [3, Theorem 3.1].

Corollary I.32. *Given a vector of positive weights $\mathbf{w} = (w_1, w_2, \ldots, w_m) \in \mathbb{N}_+^m$ and a positive integer $r \in \mathbb{N}_+$, if $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ vanishes at all points in S with weighted multiplicity at least r, then there exist polynomials $H_{\mathbf{r}}(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ such that $\deg(H_{\mathbf{r}}(\mathbf{x})) + \sum_{j=1}^m r_j \deg(G_j(x_j)) \leq \deg(F(\mathbf{x}))$, for all $\mathbf{r} = (r_1, r_2, \ldots, r_m) \in \mathcal{B}_{\mathbf{w}}$, and*

$$F(\mathbf{x}) = \sum_{\mathbf{r} \in \mathcal{B}_{\mathbf{w}}} \left(H_{\mathbf{r}}(\mathbf{x}) \prod_{j=1}^m G_j(x_j)^{r_j} \right).$$

We conclude with the case of multiindices bounded on each coordinate separately:

Corollary I.33. *Given a vector $(r_1, r_2, \ldots, r_m) \in \mathbb{N}_+^m$, if $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ is such that $F^{(\mathbf{j})}(\mathbf{s}) = 0$, for all $\mathbf{s} \in S$ and all $\mathbf{j} = (j_1, j_2, \ldots, j_m) \in \mathbb{N}^m$ satisfying $j_k < r_k$, for all $k = 1, 2, \ldots, m$, then there exist polynomials $H_j(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ such that $\deg(H_j(\mathbf{x})) + r_j \deg(G_j(x_j)) \leq \deg(F(\mathbf{x}))$, for all $j = 1, 2, \ldots, m$, and*

$$F(\mathbf{x}) = \sum_{j=1}^m H_j(\mathbf{x}) G_j(x_j)^{r_j}.$$

Proof. It follows from Theorem I.4 observing that, if $\mathcal{J} = \{(j_1, j_2, \ldots, j_m) \in \mathbb{N}^m : j_k < r_k, \ k = 1, 2, \ldots, m\}$, then

$$\mathcal{B}_{\mathcal{J}} = \left\{ r_j \mathbf{e}_j \in \mathbb{N}^m : j = 1, 2, \ldots, m \right\},$$

where $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_m \in \mathbb{N}^m$ are the vectors in the canonical basis. □

4.3 Hermite interpolation over grids with consecutive derivatives

In the appendix we show that the evaluation map (Definition I.8) is surjective. This has been used to prove Theorem I.1. In this subsection, we see that the combinatorial Nullstellensatz (Theorem I.3) implies that the evaluation map over the whole grid S, with consecutive derivatives, is an isomorphism when taking an appropriate domain. More concretely, we show the existence and uniqueness of Hermite interpolating polynomials over S with derivatives in $\mathcal{J}$ when choosing monomials in $\mathcal{J}_S$. Finding appropriate sets of points, derivatives and polynomials to guarantee existence and uniqueness of Hermite interpolating polynomials has been extensively studied [9, 18, 21]. The next result is new to the best of our knowledge:

Theorem I.5. *Given a decreasing finite set $\mathcal{J} \subseteq \mathbb{N}^m$, the evaluation map in Definition I.8 for the finite set $S = S_1 \times S_2 \times \cdots \times S_m$, defined as*

$$\mathrm{Ev} : \langle \mathcal{J}_S \rangle_{\mathbb{F}} \longrightarrow \mathbb{F}^{\#S \cdot \#\mathcal{J}},$$

is a vector space isomorphism. In other words, for all $b_{\mathbf{j},\mathbf{a}} \in \mathbb{F}$, where $\mathbf{j} \in \mathcal{J}$ and $\mathbf{a} \in S$, there exists a unique polynomial of the form

$$F(\mathbf{x}) = \sum_{\mathbf{i} \in \mathcal{J}_S} F_{\mathbf{i}} \mathbf{x}^{\mathbf{i}} \in \mathbb{F}[\mathbf{x}],$$

where $F_{\mathbf{i}} \in \mathbb{F}$ for all $\mathbf{i} \in \mathcal{J}_S$, such that $F^{(\mathbf{j})}(\mathbf{a}) = b_{\mathbf{j},\mathbf{a}}$, for all $\mathbf{j} \in \mathcal{J}$ and all $\mathbf{a} \in S$.

Proof. The map is one to one by Theorem I.3, and both vector spaces have the same dimension over $\mathbb{F}$ by Lemma I.18, hence the map is a vector space isomorphism. □

Remark I.34. *Observe that we may similarly prove that the following two maps are vector space isomorphisms:*

$$\langle \mathcal{J}_S \rangle_{\mathbb{F}} \xrightarrow{\rho} \mathbb{F}[\mathbf{x}]/I(S;\mathcal{J}) \xrightarrow{\mathrm{Ev}} \mathbb{F}^{\#S \cdot \#\mathcal{J}},$$

where ρ is the projection to the quotient ring. We may then extend the notion of reduction of a polynomial as follows (see [5, Section 3.1] and [9, Section 6.3], for instance): Given $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$, we define its reduction over the set S with derivatives in $\mathcal{J}$ as

$$G(\mathbf{x}) = \rho^{-1}\left(F(\mathbf{x}) + I(S;\mathcal{J})\right).$$

As an immediate consequence, we obtain the following result on Hermite interpolation with weighted multiplicities:

Corollary I.35. *For every vector of positive weights $\mathbf{w} = (w_1, w_2, \ldots, w_m) \in \mathbb{N}_+^m$, every positive integer $r \in \mathbb{N}_+$, and elements $b_{\mathbf{j},\mathbf{a}} \in \mathbb{F}$, for $\mathbf{j} \in \mathbb{N}^m$ with $\mid \mathbf{j} \mid_{\mathbf{w}} < r$ and for $\mathbf{a} \in S$, there exists a unique polynomial of the form*

$$F(\mathbf{x}) = \sum_{\mathbf{i} \in \mathbb{N}^m} F_{\mathbf{i}} \mathbf{x}^{\mathbf{i}},$$

where $F_{\mathbf{i}} \in \mathbb{F}$ for all $\mathbf{i} = (i_1, i_2, \ldots, i_m) \in \mathbb{N}^m$, and $F_{\mathbf{i}} = 0$ whenever

$$\sum_{j=1}^{m} \left\lfloor \frac{i_j}{\#S_j} \right\rfloor w_j \geq r,$$

such that $F^{(\mathbf{j})}(\mathbf{a}) = b_{\mathbf{j},\mathbf{a}}$, for all $\mathbf{j} \in \mathbb{N}^m$ with $\mid \mathbf{j} \mid_{\mathbf{w}} < r$ and all $\mathbf{a} \in S$.

We conclude with the case of multiindices bounded on each coordinate separately:

Corollary I.36. *Given $(r_1, r_2, \ldots, r_m) \in \mathbb{N}_+^m$ and given elements $b_{\mathbf{j},\mathbf{a}} \in \mathbb{F}$, for $\mathbf{j} = (j_1, j_2, \ldots, j_m) \in \mathbb{N}^m$ with $j_k < r_k$, for all $k = 1, 2, \ldots, m$, and for $\mathbf{a} \in S$, there exists a unique polynomial of the form*

$$F(\mathbf{x}) = \sum_{i_1=0}^{r_1 \# S_1 - 1} \sum_{i_2=0}^{r_2 \# S_2 - 1} \cdots \sum_{i_m=0}^{r_m \# S_m - 1} F_{\mathbf{i}} \mathbf{x}^{\mathbf{i}},$$

such that $F^{(\mathbf{j})}(\mathbf{a}) = b_{\mathbf{j},\mathbf{a}}$, for all $\mathbf{j} = (j_1, j_2, \ldots, j_m) \in \mathbb{N}^m$ with $j_k < r_k$, for all $k = 1, 2, \ldots, m$, and all $\mathbf{a} \in S$.

4.4 Evaluation codes with consecutive derivatives

In this subsection, we extend the notion of *evaluation code* from the theory of error-correcting codes (see [11, Section 2] and [16, Section 4.1], for instance) to evaluation codes with consecutive derivatives. By doing so, we generalize *multiplicity codes* [19], which have been shown to achieve good parameters in decoding, local decoding and list decoding [18, 19]. We compute the dimensions of the new codes and give a lower bound on their minimum Hamming distance.

Definition I.37. Given a decreasing finite set $\mathcal{J} \subseteq \mathbb{N}^m$ and a set of monomials $\mathcal{M} \subseteq \mathcal{J}_S$, we define the $\mathbb{F}$-linear code (that is, the $\mathbb{F}$-linear vector space)

$$\mathcal{C}(S, \mathcal{M}, \mathcal{J}) = \mathrm{Ev}\left(\langle \mathcal{M} \rangle_{\mathbb{F}}\right) \subseteq \mathbb{F}^{\# S \cdot \# \mathcal{J}},$$

where Ev is the evaluation map from Definition I.8.

As in [19], we will consider these codes over the alphabet $\mathbb{F}^{\#\mathcal{J}}$, that is, each evaluation $\left(F^{(\mathbf{i})}(\mathbf{a})\right)_{\mathbf{i} \in \mathcal{J}} \in \mathbb{F}^{\#\mathcal{J}}$, for $\mathbf{a} \in S$, constitutes one symbol of the alphabet. Thus each codeword has length $\#S$ over this alphabet. This leads to the following definition of minimum Hamming distance of an $\mathbb{F}$-linear code:

Definition I.38. Given an $\mathbb{F}$-linear code $\mathcal{C} \subseteq \left(\mathbb{F}^{\#\mathcal{J}}\right)^{\#S}$, we define its minimum Hamming distance as

$$d_H(\mathcal{C}) = \min\left\{ \mathrm{wt_H}(\mathbf{c}) : \mathbf{c} \in \mathcal{C}, \mathbf{c} \neq \mathbf{0} \right\},$$

where, for any $\mathbf{c} \in \left(\mathbb{F}^{\#\mathcal{J}}\right)^{\#S}$, $\mathrm{wt_H}(\mathbf{c})$ denotes the number of its non-zero components over the alphabet $\mathbb{F}^{\#\mathcal{J}}$.

As a consequence of Theorem I.5, we may exactly compute the dimensions of the codes in Definition I.37 and give a lower bound on their minimum Hamming distance:

Corollary I.39. *The code in Definition I.37 satisfies that*

$$\dim_{\mathbb{F}}(\mathcal{C}(S,\mathcal{M},\mathcal{J})) = \#\mathcal{M}, \quad \textit{and}$$

$$d_H(\mathcal{C}(S,\mathcal{M},\mathcal{J})) \geq \left\lceil \frac{\min\left\{\#\Delta(\langle F(\mathbf{x})\rangle_{\mathcal{J}}) : F(\mathbf{x}) \in \langle\mathcal{M}\rangle_{\mathbb{F}}\right\}}{\#\mathcal{J}} \right\rceil.$$

Remark I.40. *Given a vector of positive weights $\mathbf{w} = (w_1, w_2, \ldots, w_m) \in \mathbb{N}_+^m$, a positive integer $r \in \mathbb{N}_+$, and a set of monomials*

$$\mathcal{M} \subseteq \left\{ x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m} : \sum_{j=1}^{m} \left\lfloor \frac{i_j}{\#S_j} \right\rfloor w_j < r \right\},$$

we may define, as a particular case of the codes in Definition I.37, the corresponding weighted multiplicity code as the $\mathbb{F}$-linear code

$$\mathcal{C}(S,\mathcal{M},\mathbf{w},r) = \mathrm{Ev}\left(\langle\mathcal{M}\rangle_{\mathbb{F}}\right) \subseteq \left(\mathbb{F}^{\mathrm{B}(\mathbf{w};r)}\right)^{\#S}.$$

Observe that weighted multiplicity codes contain as particular cases classical Reed-Muller codes (see [17, Section 13.2]), by choosing $\mathbf{w} = (r, r, \ldots, r)$ for a given $r \in \mathbb{N}_+$, and classical multiplicity codes [19] by choosing $\mathbf{w} = (1, 1, \ldots, 1)$ and an arbitrary $r \in \mathbb{N}_+$. Therefore, choices of $\mathbf{w} \in \mathbb{N}^m$ such that $1 \leq w_i \leq r$, for $i = 1, 2, \ldots, m$, give codes with the same length but intermediate alphabet sizes between those of Reed-Muller and multiplicity codes. This has the extra flexibility (see [19, Section 1.2]) of choosing alphabets of sizes $\#\left(\mathbb{F}^{\mathrm{B}(\mathbf{w};r)}\right)$ (whenever $\mathbb{F}$ is finite), where

$$1 \leq \mathrm{B}(\mathbf{w};r) \leq \binom{m+r-1}{m}.$$

4.5 Bounds by DeMillo, Lipton, Zippel, Alon and Füredi

In this subsection, we obtain a weaker but more concise version of the bound (I.4) for a single polynomial, which has as particular cases the bounds by DeMillo and Lipton [7], Zippel [25, Theorem 1], [26, Proposition 3], and Alon and Füredi [2, Theorem 5]. We observe that Counterexample 7.4 in [4] shows that a straightforward extension of these bounds to standard multiplicities as in (I.1) is not possible, in contrast with the Schwartz bound [24, Lemma 1], which has been already extended in [8, Lemma 8].

Theorem I.6. *For any decreasing finite set $\mathcal{J} \subseteq \mathbb{N}^m$ and any polynomial $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$, if $\mathbf{x}^{\mathbf{i}} = \mathrm{LM}(F(\mathbf{x})) \in \mathcal{J}_S$, for some monomial ordering, then it holds that*

$$\#\left(S \setminus \mathcal{V}_{\mathcal{J}}(F(\mathbf{x}))\right) \#\mathcal{J} \geq \#\left\{\mathbf{j} \in \mathcal{J}_S : \mathbf{j} \succeq \mathbf{i}\right\}. \tag{I.15}$$

Proof. First, from the bound (I.4) and Lemma I.18, we obtain that

$$\#\left(S \setminus \mathcal{V}_{\mathcal{J}}(F(\mathbf{x}))\right) \#\mathcal{J} \geq \#S\#\mathcal{J} - \#\Delta(\langle F(\mathbf{x})\rangle_{\mathcal{J}}) = \#\left(\mathcal{J}_S \setminus \Delta(\langle F(\mathbf{x})\rangle_{\mathcal{J}})\right), \quad \text{(I.16)}$$

where we consider $\Delta(\langle F(\mathbf{x})\rangle_{\mathcal{J}}) \subseteq \mathbb{N}^m$ by abuse of notation. As explained in Subsection 3.3, we may lower bound $\#\left(\mathcal{J}_S \setminus \Delta(\langle F(\mathbf{x})\rangle_{\mathcal{J}})\right)$ by the number of multiindices $\mathbf{j} \in \mathcal{J}_S$ satisfying $\mathbf{j} \succeq \mathbf{i}$, and we are done. □

The following consequence summarizes the results by DeMillo and Lipton [7], and Zippel [25, Theorem 1], [26, Proposition 3]:

Corollary I.41 ([7, 25, 26]). *Let $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ be such that its degree in the j-th variable is $d_j \in \mathbb{N}$, for $j = 1, 2, \ldots, m$. If $d_j < \#S_j$, for $j = 1, 2, \ldots, m$, then the number of non-zeros in S of $F(\mathbf{x})$ is at least*

$$\prod_{j=1}^{m} \left(\#S_j - d_j\right).$$

Proof. The result is the particular case $\mathcal{J} = \{\mathbf{0}\}$ of the previous theorem using any monomial ordering and the facts that $\mathcal{J}_S = S$ and $i_j \leq d_j$, for $j = 1, 2, \ldots, m$. □

The following is a similar bound due to Alon and Füredi [2, Theorem 5]:

Corollary I.42 ([2]). *Let $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$. If not all points in S are zeros of $F(\mathbf{x})$, then the number of its non-zeros in S is at least*

$$\min\left\{\prod_{j=1}^{m} y_j : 1 \leq y_j \leq \#S_j, \sum_{j=1}^{m} y_j \geq \sum_{j=1}^{m} \#S_j - \deg(F(\mathbf{x}))\right\}.$$

Proof. The result follows from Theorem I.6 as in the previous corollary, taking any monomial ordering and considering $y_j = \#S_j - i_j$, for $j = 1, 2, \ldots, m$. □

We omit the case of weighted multiplicities. In the next section, we will give an extension of the Schwartz bound [24, Lemma 1] to weighted multiplicities in the sense of (I.1), which is stronger than the bound in Corollary I.13 in some cases.

We conclude with the case of multiindices bounded on each coordinate separately:

Corollary I.43. *Let $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ with $\mathbf{x}^{\mathbf{i}} = \mathrm{LM}(F(\mathbf{x}))$, $\mathbf{i} = (i_1, i_2, \ldots, i_m)$, for some monomial ordering. If $i_j < r_j\#S_j$, for $j = 1, 2, \ldots, m$, then the number N of elements $\mathbf{s} \in S$ such that $F^{(\mathbf{j})}(\mathbf{s}) \neq 0$, for some $\mathbf{j} = (j_1, j_2, \ldots, j_m) \in \mathbb{N}^m$ with $j_k < r_k$, for all $k = 1, 2, \ldots, m$, satisfies*

$$N \cdot \prod_{j=1}^{m} r_j \geq \prod_{j=1}^{m} \left(r_j\#S_j - i_j\right).$$

4.6 The Schwartz-Zippel bound on the whole grid

In the next section, we will give an extension of the Schwartz bound [24, Lemma 1] for weighted multiplicities that can be proven as the extensions to standard multiplicities given in [8, Lemma 8] and [11, Theorem 5]. In this subsection, we observe that the case where all points in S are zeros of a given weighted multiplicity follows from Corollary I.26:

Corollary I.44. *Let $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$, let $\mathbf{w} = (w_1, w_2, \ldots, w_m) \in \mathbb{N}_+^m$, let $r \in \mathbb{N}_+$, and assume that $s = \#S_1 = \#S_2 = \ldots = \#S_m$. If all points in $S = S_1 \times S_2 \times \cdots \times S_m$ are zeros of $F(\mathbf{x})$ of weighted multiplicity at least r, then*

$$r\#S \leq \deg_{\mathbf{w}}(F(\mathbf{x}))s^{m-1}.$$

Proof. Assume that the bound does not hold, take $\mathbf{x}^{\mathbf{i}}$ such that $\mid \mathbf{i} \mid_{\mathbf{w}} = \deg_{\mathbf{w}}(F(\mathbf{x}))$ and whose coefficient in $F(\mathbf{x})$ is not zero, and take a vector $\mathbf{r} = (r_1, r_2, \ldots, r_m) \in \mathbb{N}^m$ with $\mid \mathbf{r} \mid_{\mathbf{w}} \geq r$. Then

$$sw_1r_1 + sw_2r_2 + \cdots + sw_mr_m \geq sr > \deg_{\mathbf{w}}(F(\mathbf{x})) = \mid \mathbf{i} \mid_{\mathbf{w}},$$

hence there exists a j such that $r_j\#S_j > i_j$. By Corollary I.26, some element in S is not a zero of $F(\mathbf{x})$ of weighted multiplicity at least r, which contradicts the assumptions and we are done. □

5 The Schwartz-Zippel bound for weighted multiplicities

As we will see in Proposition I.48, the Schwartz bound [24, Lemma 1] can be derived by those given by DeMillo and Lipton [7], and Zippel [25, Theorem 1], [26, Proposition 3], and is usually referred to as the Schwartz-Zippel bound. This bound has been recently extended to standard multiplicities in [8, Lemma 8], and further in [11, Theorem 5]. In this section, we observe that it may be easily extended to weighted multiplicities (see Definition I.4), due to the additivity of weighted order functions. We show the sharpness of this bound and compare it with the bound (I.4) with some examples, whenever it makes sense to compare both bounds.

5.1 The bound

Theorem I.7. *Let $\mathbf{w} = (w_1, w_2, \ldots, w_m) \in \mathbb{N}_+^m$ be a vector of positive weights, let $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ and let $\mathbf{x}^{\mathbf{i}} = \mathrm{LM}(F(\mathbf{x}))$, $\mathbf{i} = (i_1, i_2, \ldots, i_m)$, with respect to the lexicographic ordering. It holds that*

$$\sum_{\mathbf{a} \in S} m_{\mathbf{w}}(F(\mathbf{x}), \mathbf{a}) \leq \#S \sum_{j=1}^{m} \frac{i_j w_j}{\#S_j}. \tag{I.17}$$

When $w_1 = w_2 = \ldots = w_m = 1$, observe that [11, Theorem 5] is recovered from this theorem, and [8, Lemma 8] is recovered from the next corollary. Observe also that this corollary is stronger than Corollary I.44.

Corollary I.45. *Let $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ and $\mathbf{w} \in \mathbb{N}_+^m$. If $s = \#S_1 = \#S_2 = \ldots = \#S_m$, then*

$$\sum_{\mathbf{a} \in S} m_{\mathbf{w}}(F(\mathbf{x}), \mathbf{a}) \leq \deg_{\mathbf{w}}(F(\mathbf{x})) s^{m-1}.$$

To prove Theorem I.7, we need an auxiliary lemma, whose proof can be directly translated from those of [8, Lemma 5] and [8, Corollary 7]:

Lemma I.46. *If $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ and $\mathbf{a} = (a_1, a_2, \ldots, a_m) \in \mathbb{F}^m$, then*

1. $m_{\mathbf{w}}\left(F^{(\mathbf{i})}(\mathbf{x}), \mathbf{a}\right) \geq m_{\mathbf{w}}(F(\mathbf{x}), \mathbf{a}) - \mid \mathbf{i} \mid_{\mathbf{w}}$, *for all* $\mathbf{i} \in \mathbb{N}^m$, *and*
2. $m_{\mathbf{w}}\left(F(\mathbf{x}), \mathbf{a}\right) \leq m_{w_m}(F(a_1, a_2, \ldots, a_{m-1}, x_m), a_m)$.

We may now prove Theorem I.7. We follow closely the steps given in the proof of [8, Lemma 8].

Proof of Theorem I.7. We will prove the result by induction on m, where the case $m = 1$ follows from (I.1). Fix then $m > 1$. We may assume without loss of generality that $x_1 \prec_m x_2 \prec_m \ldots \prec_m x_m$, where $\preceq_m$ is the lexicographic ordering. Write $\mathbf{x}' = (x_1, x_2, \ldots, x_{m-1})$. There are unique polynomials $F_j(\mathbf{x}') \in \mathbb{F}[\mathbf{x}']$, for $j = 1, 2, \ldots, t$, such that

$$F(\mathbf{x}) = \sum_{j=0}^{t} F_j(\mathbf{x}') x_m^j,$$

where $\mathrm{LM}(F(\mathbf{x})) = \mathrm{LM}(F_t(\mathbf{x}')) x_m^t$. Let $\mathbf{a} = (a_1, a_2, \ldots, a_m) \in S$ and write $\mathbf{a}' = (a_1, a_2, \ldots, a_{m-1})$ and $\mathbf{w}' = (w_1, w_2, \ldots, w_{m-1})$. Take $\mathbf{k} \in \mathbb{N}^{m-1}$ such that $\mid \mathbf{k} \mid_{\mathbf{w}'} = m_{\mathbf{w}'}(F_t(\mathbf{x}'), \mathbf{a}')$ and $F_t^{(\mathbf{k})}(\mathbf{a}') \neq 0$. By the previous lemma, we see that

$$\begin{aligned} m_{\mathbf{w}}(F(\mathbf{x}), \mathbf{a}) &\leq \mid (\mathbf{k}, 0) \mid_{\mathbf{w}} + m_{\mathbf{w}}\left(F^{(\mathbf{k},0)}(\mathbf{x}), \mathbf{a}\right) \\ &\leq m_{\mathbf{w}'}(F_t(\mathbf{x}'), \mathbf{a}') + m_{w_m}\left(F^{(\mathbf{k},0)}(\mathbf{a}', x_m), a_m\right). \end{aligned}$$

Summing these inequalities over all $a_m \in S_m$ and applying the case $m = 1$, we obtain that

$$\sum_{a_m \in S_m} m_{\mathbf{w}}(F(\mathbf{x}), \mathbf{a}) \leq m_{\mathbf{w}'}(F_t(\mathbf{x}'), \mathbf{a}') \# S_m + w_m t.$$

Using this last inequality, summing over $a_i \in S_i$, for $i = 1, 2, \ldots, m-1$, and applying the case of $m-1$ variables, it follows that

$$\sum_{\mathbf{a} \in S} m_{\mathbf{w}}(F(\mathbf{x}), \mathbf{a}) \leq \sum_{a_1 \in S_1} \cdots \sum_{a_{m-1} \in S_{m-1}} m_{\mathbf{w}'}(F_t(\mathbf{x}'), \mathbf{a}') \# S_m + w_m t \frac{\# S}{\# S_m}$$
$$\leq \sum_{j=1}^{m-1} w_j i_j \frac{\# S}{\# S_j} + w_m t \frac{\# S}{\# S_m},$$

and the result follows. □

5.2 Sharpness of the bound

In this subsection, we prove the sharpness of the bound (I.17), whose proof can be translated word by word from that of [12, Proposition 7]. Therefore, we only present a sketch of the proof:

Proposition I.47. *For all finite sets $S_1, S_2, \ldots, S_m \subseteq \mathbb{F}$, $S = S_1 \times S_2 \times \cdots \times S_m$, all vectors of positive weights $\mathbf{w} = (w_1, w_2, \ldots, w_m) \in \mathbb{N}_+^m$ and all $\mathbf{i} = (i_1, i_2, \ldots, i_m) \in \mathbb{N}^m$, there exists a polynomial $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ such that $\mathbf{x}^{\mathbf{i}} = \mathrm{LM}(F(\mathbf{x}))$ with respect to the lexicographic ordering, and such that*

$$\sum_{\mathbf{a} \in S} m_{\mathbf{w}}(F(\mathbf{x}), \mathbf{a}) = \# S \sum_{j=1}^{m} \frac{i_j w_j}{\# S_j}.$$

Sketch of proof. Denote $s_j = \# S_j$ and $S_j = \left\{ a_1^{(j)}, a_2^{(j)}, \ldots, a_{s_j}^{(j)} \right\}$, and choose $r_k^{(j)} \in \mathbb{N}$ such that $i_j = r_1^{(j)} + r_2^{(j)} + \cdots + r_{s_j}^{(j)}$, for $k = 1, 2, \ldots, s_j$ and $j = 1, 2, \ldots, m$. Now define

$$F(\mathbf{x}) = \prod_{j=1}^{m} \prod_{k=1}^{s_j} \left(x_j - a_k^{(j)} \right)^{r_k^{(j)}}.$$

Now, fixing integers $1 \leq k_j \leq s_j$, for $j = 1, 2, \ldots, m$, translating the point $\left(a_{k_1}^{(1)}, a_{k_2}^{(2)}, \ldots, a_{k_m}^{(m)} \right)$ to the origin $\mathbf{0}$, and using the Gröbner basis from Corollary I.32, we see that

$$m_{\mathbf{w}} \left(F(\mathbf{x}), \left(a_{k_1}^{(1)}, a_{k_2}^{(2)}, \ldots, a_{k_m}^{(m)} \right) \right) = r_{k_1}^{(1)} w_1 + r_{k_2}^{(2)} w_2 + \cdots + r_{k_m}^{(m)} w_m,$$

for all $k_j = 1, 2, \ldots, s_j$ and all $j = 1, 2, \ldots, m$. The result then follows by summing these multiplicities. □

5.3 Comparison with the footprint bound

In this subsection, we will compare the bounds (I.4) and (I.17) whenever it makes sense to do so. To that end, we will write them as follows: fix a vector of positive weights $\mathbf{w} = (w_1, w_2, \ldots, w_m) \in \mathbb{N}_+^m$, a positive integer $r \in \mathbb{N}_+$, and a polynomial $F(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ such that $\mathbf{x}^{\mathbf{i}} = \mathrm{LM}(F(\mathbf{x}))$, $\mathbf{i} = (i_1, i_2, \ldots, i_m)$, with respect to the lexicographic ordering. We first consider the footprint bound as in Corollary I.13:

$$\#\mathcal{V}_{\geq r,\mathbf{w}}(F(\mathbf{x})) \cdot \mathrm{B}(\mathbf{w};r) \leq \#\Delta\left(\left\langle \{F(\mathbf{x})\} \bigcup \left\{ \prod_{j=1}^{m} G_j(x_j)^{r_j} : \sum_{j=1}^{m} r_j w_j \geq r \right\} \right\rangle\right). \tag{I.18}$$

And next we consider the bound (I.17) as follows:

$$\#\mathcal{V}_{\geq r,\mathbf{w}}(F(\mathbf{x})) \cdot r \leq \#S \sum_{j=1}^{m} \frac{i_j w_j}{\#S_j}. \tag{I.19}$$

First we observe that the bound (I.18) also holds for any other monomial ordering, and not only the lexicographic one, as is the case with (I.19). Second we observe that (I.19) gives no information whereas (I.18) does, whenever

$$\sum_{j=1}^{m} \left\lfloor \frac{i_j}{\#S_j} \right\rfloor w_j < r \leq \sum_{j=1}^{m} \frac{i_j w_j}{\#S_j}, \tag{I.20}$$

by the discussion in Subsection 3.3.

Next, we observe that when we do not count multiplicities, that is, $w_1 = w_2 = \ldots = w_m = r = 1$, the footprint bound implies the Schwartz bound via Theorem I.6:

Proposition I.48. *If $w_1 = w_2 = \ldots = w_m = r = 1$, that is, $\mathcal{J} = \{\mathbf{0}\}$, it holds that $\mathrm{B}(\mathbf{w};r) = 1$ and*

$$\#\Delta\left(\langle F(\mathbf{x}), G_1(x_1), G_2(x_2), \ldots, G_m(x_m)\rangle\right) \leq \#S - \prod_{j=1}^{m} \left(\#S_j - i_j\right) \leq \#S \sum_{j=1}^{m} \frac{i_j}{\#S_j}.$$

In particular, (I.18) implies (I.19) in this case.

Moreover, when $m = 1$ and we count multiplicities, all bounds coincide, giving (I.2). In the following example we show that this is not the case in general. As we will see, each bound, (I.18) and (I.19), can be tighter than the other one in different cases, hence complementing each other:

Example I.49. Consider $m = 2$, $w_1 = 2$, $w_2 = 3$, $r = 5$ and $\#S_1 = \#S_2 = 4$. Thus we have that

$$\mathcal{J} = \{(0,0), (1,0), (0,1), (2,0)\}, \quad \text{and}$$

$$\mathcal{J}_S = ([0,11] \times [0,3]) \cup ([0,3] \times [0,7])\,.$$

Consider all pairs $(i_1, i_2) \in \mathcal{J}_S$ and polynomials $F(x_1, x_2)$ such that $\mathrm{LM}(F(x_1, x_2)) = x_1^{i_1} x_2^{i_2}$, with respect to the lexicographic ordering. In Figure I.2, we show the upper bounds on the number of zeros of $F(x_1, x_2)$ of weighted multiplicity at least 5 given by (I.18) and (I.19), respectively. As is clear from the figure, in some regions of the set $\mathcal{J}_S$, the first bound is tighter than the second (bold numbers in the first table) and vice versa (bold numbers in the second table). Furthermore the first bound gives non-trivial information in the region given by (I.20), where the second does not (depicted by dashes).

x_1^7	**15**	**15**	**15**	**15**								
x_1^6	14	**14**	**15**	**15**								
x_1^5	13	13	**14**	**15**								
x_1^4	12	13	14	15								
x_1^3	9	10	11	12	14	**14**	**14**	**14**	**15**	**15**	**15**	**15**
x_1^2	6	7	9	10	12	12	**13**	**13**	**14**	**14**	**15**	**15**
x_1	3	4	6	8	10	10	**11**	**12**	**13**	**13**	**14**	**15**
1	0	2	4	6	8	9	10	11	12	**13**	**14**	**15**
	1	x_2	x_2^2	x_2^3	x_2^4	x_2^5	x_2^6	x_2^7	x_2^8	x_2^9	x_2^{10}	x_2^{11}

x_1^7	–	–	–	–								
x_1^6	14	–	–	–								
x_1^5	**12**	13	15	–								
x_1^4	**9**	**11**	**12**	**14**								
x_1^3	**7**	**8**	**10**	12	**13**	15	–	–	–	–	–	–
x_1^2	**4**	**6**	**8**	**9**	**11**	12	14	–	–	–	–	–
x_1	**2**	4	**5**	**7**	**8**	10	12	13	15	–	–	–
1	0	**1**	**3**	**4**	**6**	**8**	**9**	11	12	14	–	–
	1	x_2	x_2^2	x_2^3	x_2^4	x_2^5	x_2^6	x_2^7	x_2^8	x_2^9	x_2^{10}	x_2^{11}

Fig. I.2: Upper bounds on the number of zeros of weighted multiplicity at least $r = 5$ when $w_1 = 2$, $w_2 = 3$ and $\#S_1 = \#S_2 = 4$, from Example I.49.

A Proof of Lemma I.9

In this appendix, we give the proof of Lemma I.9. We first treat the univariate case ($m = 1$) in the classical form. The proof for Hasse derivatives can be directly translated from the result for classical derivatives:

Lemma I.50. *Let $a_1, a_2, \ldots, a_n \in \mathbb{F}$ be pair-wise distinct and let $M \in \mathbb{N}_+$. There exist polynomials $F_{i,j}(x) \in \mathbb{F}[x]$ such that*

$$F_{i,j}^{(k)}(a_l) = \delta_{i,k}\delta_{j,l},$$

for all $i, k = 0, 1, 2, \ldots, M$ and all $j, l = 1, 2, \ldots, n$, where δ denotes the Kronecker delta.

Now, since $\mathcal{J}$ is finite, we may fix an integer M such that $\mathcal{J} \subseteq [0, M]^m$. Similarly, we may find a finite set $S \subseteq \mathbb{F}$ such that $T \subseteq S^m$. Denote then $s = \#S$ and $S = \{a_1, a_2, \ldots, a_s\}$, and let $F_{i,j,k}(x_k) \in \mathbb{F}[x_k]$ be polynomials as in the previous lemma in each variable x_k, for $i = 0, 1, 2, \ldots, M$, $j = 1, 2, \ldots, s$ and $k = 1, 2, \ldots, m$. Define now

$$F_{\mathbf{i},\mathbf{j}}(\mathbf{x}) = F_{i_1,j_1,1}(x_1)F_{i_2,j_2,2}(x_2) \cdots F_{i_m,j_m,m}(x_m) \in \mathbb{F}[\mathbf{x}],$$

for $\mathbf{i} = (i_1, i_2, \ldots, i_m) \in [0, M]^m$ and $\mathbf{j} = (j_1, j_2, \ldots, j_m) \in [1, s]^m$. By the previous lemma and Lemma I.7, we see that

$$F_{\mathbf{i},\mathbf{j}}^{(\mathbf{k})}\left(a_{l_1}, a_{l_2}, \ldots, a_{l_m}\right) = \left(\delta_{i_1,k_1}\delta_{i_2,k_2} \cdots \delta_{i_m,k_m}\right)\left(\delta_{j_1,l_1}\delta_{j_2,l_2} \cdots \delta_{j_m,l_m}\right) = \delta_{\mathbf{i},\mathbf{k}}\delta_{\mathbf{j},\mathbf{l}},$$

for all $\mathbf{i}, \mathbf{k} \in [0, M]^m$ and all $\mathbf{j}, \mathbf{l} \in [1, s]^m$. Finally, given values $b_{\mathbf{i},\mathbf{j}} \in \mathbb{F}$, for $\mathbf{i} \in \mathcal{J}$ and $\mathbf{j} \in T$, define

$$F(\mathbf{x}) = \sum_{\mathbf{i} \in \mathcal{J}} \sum_{\mathbf{j} \in T} b_{\mathbf{i},\mathbf{j}} F_{\mathbf{i},\mathbf{j}}(\mathbf{x}) \in \mathbb{F}[\mathbf{x}].$$

We see that $\mathrm{Ev}(F(\mathbf{x})) = ((b_{\mathbf{i},\mathbf{j}})_{\mathbf{i} \in \mathcal{J}})_{\mathbf{j} \in T}$, and we are done.

Acknowledgment

The authors gratefully acknowledge the support from The Danish Council for Independent Research (Grant No. DFF-4002-00367). The second listed author also gratefully acknowledges the support from The Danish Council for Independent Research via an EliteForsk-Rejsestipendium (Grant No. DFF-5137-00076B).

References

[1] N. Alon, "Combinatorial Nullstellensatz," *Combinatorics, Probability and Computing*, vol. 8, no. 1-2, pp. 7–29, 1999.

[2] N. Alon and Z. Füredi, "Covering the cube by affine hyperplanes," *European Journal of Combinatorics*, vol. 14, no. 2, pp. 79–83, 1993.

[3] S. Ball and O. Serra, "Punctured combinatorial Nullstellensätze," *Combinatorica*, vol. 29, no. 5, pp. 511–522, 2009.

[4] A. Bishnoi, P. L. Clark, A. Potukuchi, and J. R. Schmitt, "On zeros of a polynomial in a finite grid," *Combinatorics, Probability and Computing (to appear)*, 2017, preprint: https://arxiv.org/abs/1508.06020.

[5] P. L. Clark, "The combinatorial Nullstellensätze revisited," *Electronic Journal of Combinatorics*, vol. 21, pp. 1–17, 2014.

[6] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2007.

[7] R. A. Demillo and R. J. Lipton, "A probabilistic remark on algebraic program testing," *Information processing letters*, vol. 7, no. 4, pp. 193–195, 1978.

[8] Z. Dvir, S. Kopparty, S. Saraf, and M. Sudan, "Extensions to the method of multiplicities, with applications to Kakeya sets and mergers," *SIAM Journal on Computing*, vol. 42, no. 6, pp. 2305–2328, 2013.

[9] M. Gasca and T. Sauer, "Polynomial interpolation in several variables," *Advances in Computational Mathematics*, vol. 12, no. 4, pp. 1–377, 2000.

[10] O. Geil and T. Høholdt, "Footprints or generalized Bezout's theorem," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 635–641, 2000.

[11] O. Geil and C. Thomsen, "Weighted Reed–Muller codes revisited," *Designs, Codes and Cryptography*, vol. 66, no. 1, pp. 195–220, 2013.

[12] ——, "More results on the number of zeros of multiplicity at least r," *Discrete Mathematics*, vol. 340, no. 5, pp. 1028–1038, 2017.

[13] H. Hasse, "Theorie der höheren differentiale in einem algebraischen funktionenkörper mit vollkommenem konstantenkörper bei beliebiger charakteristik." *Journal für die reine und angewandte Mathematik*, vol. 175, pp. 50–54, 1936.

[14] J. W. P. Hirschfeld, G. Korchmaros, and F. Torres, *Algebraic Curves over a Finite Field*. Princeton University Press, 2008.

[15] T. Høholdt, "On (or in) the Blahut footprint," in *Codes, Curves, and Signals: Common Threads in Communications*, A. Vardy, Ed. Boston, MA: Springer US, 1998, pp. 3–7.

[16] T. Høholdt, J. H. van Lint, and R. Pellikaan, "Algebraic geometry codes," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam: Elsevier, 1998, vol. 1, pp. 871–961.

[17] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.

[18] S. Kopparty, "List-decoding multiplicity codes," *Theory of Computing*, vol. 11, no. 5, pp. 149–182, 2015.

[19] S. Kopparty, S. Saraf, and S. Yekhanin, "High-rate codes with sublinear-time decoding," *Journal of the ACM*, vol. 61, no. 5, pp. 28:1–28:20, 2014.

[20] G. Kós and L. Rónyai, "Alon's Nullstellensatz for multisets," *Combinatorica*, vol. 32, no. 5, pp. 589–605, 2012.

[21] R. A. Lorentz, "Multivariate Hermite interpolation by algebraic polynomials: A survey," *Journal of Computational and Applied Mathematics*, vol. 122, no. 1–2, pp. 167–201, 2000, numerical Analysis in the 20th Century Vol. II: Interpolation and Extrapolation.

[22] M. Michałek, "A short proof of combinatorial Nullstellensatz," *The American Mathematical Monthly*, vol. 117, no. 9, pp. 821–823, 2010.

[23] R. Pellikaan and X.-W. Wu, "List decoding of q-ary Reed-Muller codes," *IEEE Transactions on Information Theory*, vol. 50, no. 4, pp. 679–682, 2004, extended version: http://www.win.tue.nl/~ruudp/paper/43-exp.pdf.

[24] J. T. Schwartz, "Fast probabilistic algorithms for verification of polynomial identities," *Journal of the ACM*, vol. 27, no. 4, pp. 701–717, 1980.

[25] R. Zippel, "Probabilistic algorithms for sparse polynomials," in *Proceedings of the International Symposiumon on Symbolic and Algebraic Computation*, ser. EUROSAM '79. London, UK: Springer-Verlag, 1979, pp. 216–226.

[26] ——, "An explicit separation of relativised random and polynomial time and relativised deterministic polynomial time," Ithaca, NY, USA, Tech. Rep., 1989.

ISSN (online): 2446-1636
ISBN (online): 978-87-7210-063-0

AALBORG UNIVERSITY PRESS