University of Kentucky

UKnowledge

Theses and Dissertations--Mathematics

Mathematics

2019

The State of Lexicodes and Ferrers Diagram Rank-Metric Codes

Jared E. Antrobus
University of Kentucky, jaredantrobus@gmail.com
Author ORCID Identifier:
https://orcid.org/0000-0001-6635-2736
Digital Object Identifier: https://doi.org/10.13023/etd.2019.309

Right click to open a feedback form in a new tab to let us know how this document benefits you.

Recommended Citation

STUDENT AGREEMENT:

I represent that my thesis or dissertation and abstract are my original work. Proper attribution has been given to all outside sources. I understand that I am solely responsible for obtaining any needed copyright permissions. I have obtained needed written permission statement(s) from the owner(s) of each third-party copyrighted matter to be included in my work, allowing electronic distribution (if such use is not permitted by the fair use doctrine) which will be submitted to UKnowledge as Additional File.

I hereby grant to The University of Kentucky and its agents the irrevocable, non-exclusive, and royalty-free license to archive and make accessible my work in whole or in part in all forms of media, now or hereafter known. I agree that the document mentioned above may be made available immediately for worldwide access unless an embargo applies.

I retain all other ownership rights to the copyright of my work. I also retain the right to use in future works (such as articles or books) all or part of my work. I understand that I am free to register the copyright to my work.

REVIEW, APPROVAL AND ACCEPTANCE

The document mentioned above has been reviewed and accepted by the student's advisor, on behalf of the advisory committee, and by the Director of Graduate Studies (DGS), on behalf of the program; we verify that this is the final, approved version of the student's thesis including all changes required by the advisory committee. The undersigned agree to abide by the statements above.

<div align="right">

Jared E. Antrobus, Student

Dr. Heide Gluesing-Luerssen, Major Professor

Dr. Peter Hislop, Director of Graduate Studies

</div>

The State of Lexicodes and Ferrers Diagram Rank-Metric Codes

_____

DISSERTATION
_____

A dissertation submitted in partial
fulfillment of the requirements for
the degree of Doctor of Philosophy
in the College of Arts and Sciences
at the University of Kentucky

By
Jared E. Antrobus
Lexington, Kentucky

Director: Dr. Heide Gluesing-Luerssen, Professor of Mathematics
Lexington, Kentucky
2019

ABSTRACT OF DISSERTATION

The State of Lexicodes and Ferrers Diagram Rank-Metric Codes

In coding theory we wish to find as many codewords as possible, while simultaneously maintaining high distance between codewords to ease the detection and correction of errors. For linear codes, this translates to finding high-dimensional subspaces of a given metric space, where the induced distance between vectors stays above a specified minimum. In this work I describe the recent advances of this problem in the contexts of lexicodes and Ferrers diagram rank-metric codes.

In the first chapter, we study lexicodes. For a ring R, we describe a lexicographic ordering of the left R-module R^n. With this ordering we set up a greedy algorithm which sequentially selects vectors for which all linear combinations satisfy a given property. The resulting output is called a lexicode. This process was discussed earlier in the literature for fields and chain rings. We describe a generalization of the algorithm to finite principal ideal rings.

In the second chapter, we investigate Ferrers diagram rank-metric codes, which play a role in the construction of subspace codes. A well-known upper bound for dimension of these codes is conjectured to be sharp. We describe several solved cases of the conjecture, and further contribute new ones. In addition, probabilities for maximal Ferrers diagram codes and MRD codes are investigated in a new light. It is shown that for growing field size, the limiting probability depends highly on the Ferrers diagram.

KEYWORDS: coding theory, lexicode, Ferrers diagram, rank-metric, MRD code

Author's signature:_____Jared E. Antrobus_____

Date:_____July 21, 2019_____

The State of Lexicodes and Ferrers Diagram Rank-Metric Codes

By
Jared E. Antrobus

Director of Dissertation: Dr. Heide Gluesing-Luerssen

Director of Graduate Studies: Dr. Peter Hislop

Date: July 21, 2019

Dedicated to my family, my friends, my mentors,
and to those who we've lost along the way,
and to the mathematicians who came before, and those who will come after.

ACKNOWLEDGMENTS

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1 Lexicodes over Finite Principal Ideal Rings

This chapter is a faithful reproduction of [1]. It reflects the first of the two major projects represented in this dissertation.

Lexicodes, or lexicographic codes, were first introduced by Levenstein [34] in 1960 with the goal to construct binary codes with a desired minimal Hamming distance. They are obtained by ordering all binary vectors lexicographically and applying a greedy algorithm that selects the vectors that have at least the desired Hamming distance from all previously selected vectors. Interestingly, the resulting codes turn out to be linear. Later in 1986, Conway/Sloane [10] generalized the idea to codes over fields of characteristic 2. Focusing primarily on codewords realized as winning positions in game theory, they showed that the resulting lexicodes are always additive, and they are linear if the field size is 2^{2^k} for some $k \geq 0$. Many well-known codes, such as the Hamming codes and the extended binary Golay code, turn out to be lexicodes; for a brief overview see [10].

In all the above cases the vectors of the search space $\mathbb{F}^n$ are ordered by suitably interpreting them as binary representation of integers. In 1993, Brualdi/Pless [6] generalized the theory to using arbitrary ordered bases of $\mathbb{F}_2^n$ and ordering the space by using the lexicographic ordering on the coefficient vectors. Among other things, they proved that the resulting codes are again linear.

In 1997 this result has been further generalized by Van Zanten [52] by allowing other selection criteria instead of the Hamming distance. More precisely, Van Zanten presented the following simple algorithm for constructing codes satisfying some property P over the lexicographically ordered space $\mathbb{F}_2^n$:

Denote the vectors selected so far by C.

Select the next vector x in the list $\mathbb{F}_2^n$ such that $P[x + y]$ holds true for all $y \in C$.

Update C to $C \cup \{x\}$.

As in the earlier cases where the property P was a desired minimum Hamming weight, it turns out that the resulting code is linear [52]. The result is generalized to codes over fields of characteristic 2 and, again, linearity is established if the field is of size 2^{2^k} for some k and the field elements are ordered suitably.

In 2005, a shift in the construction of lexicodes occurred by imposing linearity of the code via an adjustment of the greedy algorithm. In [53] Van Zanten/Suparta considered the search space $\mathbb{F}^n$ for general fields $\mathbb{F}$ and ordered it into level sets based on an ordered basis along with some fixed, yet arbitrary, ordering of the field elements. Choosing a selection property P on $\mathbb{F}^n$ that is invariant under scalar multiplication, they set up the following greedy algorithm:

Denote the vectors selected so far by C.

In the next level set, find the first vector x such that $P[x + y]$ is true for all $y \in C$.

Update C to $C + \mathbb{F}x$.

The resulting lexicode is clearly linear. However, in this variant it is not a priori clear whether all added vectors $\alpha x + y, \alpha \in \mathbb{F}, y \in C$, satisfy the selection property. Fortunately, this is indeed the case as established in [53]. Another interesting feature of the algorithm is that each level set is searched only once: if the search is successful the algorithm moves on to the next level set after its update. It is proved in [53] that the algorithm is nevertheless exhaustive in that it does not miss any admissible vectors.

In 2014, Guenda et al. [24] generalize the results from [53] to codes over commutative chain rings R. In that case, the selection property for R^n has to be invariant under multiplication by units. Moreover, the test for $P[x+y]$ in the above algorithm needs to be replaced by $P[\gamma^j x + y]$ for all j, where γ is a generator of the maximal ideal.

In this paper we revisit the results of [24] and extend them to codes over, possibly noncommutative, finite principal ideal rings. In this case a code (of length n) is a left submodule of R^n. As in [24] we consider selection properties that are invariant under multiplication by units. Only this guarantees meaningful results of the greedy algorithm. The algorithm is essentially as the above one with $\mathbb{F}$ replaced by R in the update, and with $P[x+y]$ replaced by $P[\gamma x + y]$, where γ runs through a set of generators of the nonzero left ideals of R. While these are the obvious generalizations of the chain ring case, special attention needs to be paid to the ordering of the space R^n. Again it is based on an ordered basis along with an ordering of the ring elements. However, the latter one needs to be chosen with care for the greedy algorithm to produce good results. More precisely, the ordering of the ring has to respect containment of (nonzero) left ideals, see Definition 1.2.1. Only then it is guaranteed that the algorithm is exhaustive and the resulting codes are maximal within the set of all codes satisfying the given property. The exhaustiveness is nontrivial and proven with the aid of the stable range property of finite principal ideal rings. Even though the same stipulations on the ordering of the ring also apply to chain rings, this has not been addressed explicitly in [24]. This may be due to the fact that many chain rings, such as $\mathbb{Z}_{p^r} := \mathbb{Z}/p^r\mathbb{Z}$ for any prime p and other small chain rings, come with a 'natural' order, which seems to have been tacitly assumed in [24]. These orderings do indeed respect containments of ideals.

An interesting role is played by the value of the selection property for the zero vector. It is not hard to see that the lexicode is free if the zero vector does not satisfy the selection property. However, even though we may easily toggle the value of the property for the zero vector between true and false, the outcome of the greedy algorithm may fundamentally change. This is illustrated by various examples in Section 1.4. In addition, the lexicode heavily depends on the ordering of the ring elements (even if the ordering respects ideal containment). This is also true in the field case where even the dimension of the lexicode may depend on the ordering. In Section 1.4 we present an abundance of examples illustrating the various features of the algorithm and, in particular, the dependence of the lexicode on the ordering.

The paper is organized as follows. In the next section we recall crucial properties of finite principal ideal rings and discuss various weight functions as well as other properties that may serve as selection criteria for a greedy algorithm. In Section 1.2

we introduce respectful orderings on R and establish their existence. We use such an ordering along with an ordered basis of the left R-module R^n to order the module lexicographically. Section 1.3 is devoted to the greedy algorithm and its properties. Finally, in Section 1.4 we present examples illustrating the various features of the algorithm and the dependence of the lexicode on the ordering.

1.1   Stable Range, Weights, and Multiplicative Properties

We begin with some basic ring-theoretic properties that will be needed later on. Let R denote any (non-commutative) ring with identity. We use the notation R^* for the group of units of R.

The ring R is said to have *(left) stable range 1* if for any $p, q \in R$ the identity $Rp + Rq = R$ implies the existence of some $t \in R$ such that $tp + q \in R^*$; see [33, (20.10)]. Right stable range 1 is defined similarly. In [32, Thm. 1.8] Lam shows that left and right stable range 1 are actually equivalent properties. We have the following characterization of rings with stable range 1.

Theorem 1.1.1 ([32, Thm. 1.9] or [8, Thm. 2.9])**.** *The ring R has stable range 1 if and only if for all $p, q, d \in R$ satisfying $Rp + Rq = Rd$ there exists $t \in R$ and $u \in R^*$ such that $tp + q = ud$.*

Since semilocal rings have stable range 1 by Bass' Theorem we immediately have

Theorem 1.1.2 (Bass' Theorem, [33, (20.9)])**.** *Every finite ring has stable range 1.*

In this paper we focus on finite principal left ideal rings. Recall that a ring is called a *principal left ideal ring* if every left ideal is principal. In [39, p. 364] Nechaev showed that every finite principal left ideal ring is a principal ideal ring (that is, each left ideal and each right ideal is principal). Hence from now on we will call such a ring a *principal ideal ring*, but will work with the left ideals later on. One may notice that finite principal ideal rings are Frobenius rings because they have a principal (left) socle, see [27, Thm. 1]. A special case of finite principal ideal rings are finite chain rings. A *finite left chain ring* is a finite ring wherein the left ideals are linearly ordered with respect to inclusion. A left chain ring is also a right chain ring and therefore we call these rings simply *chain rings*. Furthermore, a chain ring R can be characterized as a local ring whose maximal ideal is principal and generated by some nilpotent element $\gamma \in R$. If e is the nilpotency index of γ then the ideals of R are given by the chain $R = (1) \supsetneq (\gamma) \supsetneq (\gamma^2) \supsetneq \cdots \supsetneq (\gamma^{e-1}) \supsetneq (\gamma^e) = (0)$. For all this, see, for instance, [39] by Nechaev or [29, Thm. 2.1] by Honold/Landjev.

We now turn to codes over R. The following definition is standard. Throughout, all modules are left R-modules.

Definition 1.1.3. Let $n \in \mathbb{N}$. A *code of length n over the alphabet R* is a left submodule of R^n.

Bass' Theorem leads to a well-known and extremely useful consequence.

3

Proposition 1.1.4 ([55, Prop. 5.1]). *Let R be any finite ring and M a left R-module. Let $a, b \in M$ be such that $Ra = Rb$. Then $ua = b$ for some $u \in R^*$.*

Note that if R has stable range 1, then Proposition 1.1.4 follows immediately for the module $M = R$ since $R0 + Rb = Ra$ implies $b = ua$ for some $u \in R^*$ thanks to Theorem 1.1.1. In fact, [32, Theorem 1.9(3)] shows that for the case $M = R$ the property in Proposition 1.1.4 characterizes stable range 1.

The next corollary follows trivially.

Corollary 1.1.5. *Let R and M be as in Proposition 1.1.4. Then the group R^* acts naturally on M by $(u, a) \mapsto ua$. The orbits of this group action are exactly the sets of generators for the distinct cyclic left submodules of M. In particular, the orbits of the action of R^* on R are the sets of generators for the distinct principal left ideals of R.*

The following simple property will be crucial later on. It is immediate from the fact that every finite principal ideal ring R is Frobenius, thus self-injective and therefore every free R-module of finite rank is injective, hence splits.

Theorem 1.1.6. *Let R be a finite principal ideal ring and let N, M be free left R-modules of finite rank such that M is a submodule of N. Then M is a direct summand of N, that is, there is a submodule P of N such that $M \oplus P = N$.*

We now turn to various coding-theoretic weight functions. Let R be any finite ring. A map $w : R \longrightarrow \mathbb{R}$ satisfying $w(0) = 0$ is called a *weight function* on R. Any such weight w has a natural extension to vectors $(x_1, \ldots, x_n) \in R^n$ via the rule

$$w(x_1, \ldots, x_n) = \sum_{i=1}^{n} w(x_i). \tag{1.1}$$

Here are some special instances of weight functions.

Definition 1.1.7. Let R be a ring.

(a) The *Hamming weight* $\mathrm{wt_H}$ on R is defined by the rule $\mathrm{wt_H}(0) = 0$ and $\mathrm{wt_H}(x) = 1$ for all $x \in R \setminus \{0\}$.

(b) Let $R = M_k(\mathbb{F})$, the ring of $k \times k$-matrices over the finite field $\mathbb{F}$. We define the rank weight of $X \in R$ as the rank of X, denoted by $\mathrm{rk}(X)$. For a vector $x = (X_1, \ldots, X_n) \in M_k(\mathbb{F}_q)^n$ we define the *rank sum* as in (1.1) via $\mathrm{rankSum}(x) = \sum_{i=1}^{n} \mathrm{rk}(X_i)$.

(c) On any finite ring R set $\mathrm{wt_U}(a) = 1$ if $a \in R^*$ and $\mathrm{wt_U}(a) = 0$ otherwise. Then $\mathrm{wt_U}(x_1, \ldots, x_n)$ counts the number of units in the vector $(x_1, \ldots, x_n)$.

(d) On $R = \mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$ the *Lee weight* is defined as $\mathrm{wt_L}(x) = \min(x, m - x)$ and the *Euclidean weight* is defined as $\mathrm{wt_E}(x) = \min(x, m - x)^2$.

4

In addition to the above, the homogeneous weight plays a prominent role in ring-linear coding. The following definition is taken from [23, Definition 1.2] by Greferath/Schmidt. In the same paper the authors also establish existence and uniqueness of the homogeneous weight for all finite rings.

Definition 1.1.8. Let R be a finite ring. A function $\omega : R \to \mathbb{R}$ is called the (normalized left) *homogeneous weight* if $\omega(0) = 0$ and it satisfies the following properties.

(i) If $Ra = Rb$ for $a, b \in R$, then $\omega(a) = \omega(b)$.

(ii) For every $a \in R$ we have $\sum_{x \in Ra} \omega(x) = |Ra|$.

Example 1.1.9. On $\mathbb{Z}_2$ and $\mathbb{Z}_3$ the Hamming weight and Lee weight agree, and the homogeneous weight agrees with these up to a factor 2 and 1.5, respectively. On $\mathbb{Z}_4$, the normalized homogeneous weight agrees with the Lee weight and is given by the values $\omega(0) = 0$, $\omega(1) = \omega(3) = 1$, $\omega(2) = 2$. For $m > 4$, the Hamming weight, Lee weight, and homogeneous weight on $\mathbb{Z}_m$ are mutually distinct.

In the next sections we will discuss a greedy algorithm that results in codes having a pre-specified property. The property serves as the selection criterion in the algorithm. We will also need the property to be invariant (called multiplicative in [24]) in the following sense.

Definition 1.1.10. Let R be a ring. A boolean function $P : R^n \longrightarrow \{\text{true}, \text{false}\}$ is called a *property* on R^n. We call P *left invariant* if $P[x] = P[ux]$ for all $u \in R^*$.

For the purpose of this paper it will be beneficial to describe a property in set-theoretic form by specifying the set containing all elements having the given property.

Remark 1.1.11. From now on we identify a property $P : R^n \longrightarrow \{\text{true}, \text{false}\}$ with the *property set* $\mathcal{T} := \{x \in R^n \mid P[x] = \text{true}\}$, which collects all elements satisfying the given property. Then P is left invariant if and only if $\mathcal{T}$ is invariant under left multiplication by R^*. In other words, P is left invariant if and only if $\mathcal{T}$ is the union of R^*-orbits, where the latter are the orbits of the left natural group action of R^* on R^n. From now on, we will simply call the set $\mathcal{T}$ a property.

Many selection properties may be desirable in order to construct codes. The following are some commonly desired properties.

Example 1.1.12. (a) Let w be any of the weights introduced in Definition 1.1.7(a) – (c), Definition 1.1.8 or the Lee or Euclidean weight on $\mathbb{Z}_4$ (see 1.1.7(d)). Extend w to R^n as in (1.1). In all these cases $w(ux) = w(x)$ for $x \in R^n$ and $u \in R^*$. Therefore the property $\mathcal{T} = \{x \in R^n \mid w(x) \geq \delta\}$ is left invariant for any $\delta \in \mathbb{R}$. The same is true for the property $\mathcal{T} = \{x \in R^n \mid w(x) \in S\}$, where S is a pre-specified set of admissible weight values (such as even weights). In particular, $\mathcal{T} = \{x \in M_k(\mathbb{F})^n \mid \text{rankSum}(x) \geq \delta\}$ is an invariant property on $M_k(\mathbb{F})^n$ for any $\delta > 0$.

(b) Let R be any commutative ring and denote by $x \cdot y := \sum_{i=1}^n x_i y_i$ the standard dot product on R^n. Then the property $\mathcal{T} = \{x \in R^n \mid x \cdot x = 0\}$ is invariant because

for any $u \in R^*$ we have $(ux) \cdot (ux) = u^2(x \cdot x)$. The same property is in general not invariant if R is not commutative (as one easily verifies for the matrix ring $M_2(\mathbb{F}_2)$).

(c) Let $I \subseteq R$ be a left ideal of R. On R^n define $\mathcal{T} = \{x \in R^n \mid \sum_{i=1}^n x_i \in I\}$. Then $\mathcal{T}$ is left invariant.

Of course, there are plenty of other invariant properties over finite rings. For example, the sum of the entries being a unit is an invariant property. However, this property is not useful for our purposes. Indeed, we will aim at constructing *linear* codes with a desired property, and thus in order to obtain non-trivial codes we need the property to be reasonably conserved upon multiplication by arbitrary ring elements. Similarly, the property that the sum of the entries is a zero divisor (even though preserved by multiplication with any ring element) will often not lead to codes with more than one generator as this property is scarcely preserved under addition.

One particular property can, for many rings, be used to construct self-orthogonal codes. Let us summarize the necessary information about self-orthogonal codes.

Remark 1.1.13. Let R be a commutative ring. On R^n consider the (invariant) property $\mathcal{T} = \{x \in R^n \mid x \cdot x = 0\}$, where $x \cdot y$ denotes the standard dot product, see Example 1.1.12(b). If the characteristic of R is odd then a linear code $C \subseteq R^n$ satisfies

$$x \cdot x = 0 \text{ for all } x \in C \Longrightarrow x \cdot y = 0 \text{ for all } x, y \in C.$$

This follows immediately from $0 = (x + y) \cdot (x + y) = x \cdot x + 2(x \cdot y) + y \cdot y = 2(x \cdot y)$, and since 2 is not a zero divisor, we obtain the desired result. Recall that the dual code of $C \subseteq R^n$ is defined as $C^\perp := \{y \in R^n \mid y \cdot x = 0 \text{ for all } x \in C\}$ and that C is *self-orthogonal* (resp. *self-dual*) if $C \subseteq C^\perp$ (resp. $C = C^\perp$). The above shows that if the characteristic of R is odd, then

$$C \subseteq \mathcal{T} \Longleftrightarrow C \subseteq C^\perp.$$

Self-orthogonality is thus characterized by a suitable property for the individual elements of the code (instead of pairs of elements). Finally, we remark that if R is a finite principal ideal ring, and thus in particular a Frobenius ring, and $C \subseteq R^n$ a code, then $|C| \cdot |C^\perp| = |R^n|$; see [28, Cor. 5].

Note that the logical operators AND and OR of properties as boolean functions simply amount to intersection and union of the associated property sets, respectively. Since the intersection and union of unions of R^*-orbits is again a union of R^*-orbits, we conclude that the family of left invariant properties is closed under AND and OR.

This allows us to address whether or not the zero vector has the specified property, which will play an interesting role in Section 1.3. Most standard properties are not satisfied by the zero vector; for instance $\mathcal{T} = \{x \in R^n \mid \mathrm{wt_H}(x) \geq \delta\}$, where $\delta > 0$. By the above we can easily add or delete 0 from any invariant property $\mathcal{T}$ without compromising invariance because the properties $\{0\}$ and $R^n \setminus \{0\}$ are both invariant themselves. Hence we have

Corollary 1.1.14. *For any left invariant property $\mathcal{T}$ on R^n the properties $\mathcal{T} \cup \{0\}$ and $\mathcal{T} \setminus \{0\}$ are left invariant.*

Note that moving from $\mathcal{T}$ to the property $\mathcal{T} \cup \{0\}$ forces 0 to assume the given property, whereas moving to the property $\mathcal{T} \setminus \{0\}$ strips 0 of the given property.

1.2 Orderings of R and R^n

For the remainder of this paper, R denotes a (noncommutative) finite principal ideal ring. Furthermore, R^n is always considered as a free left R-module in the natural way. We use $R\{v_1, \ldots, v_k\}$ to denote the submodule generated by the vectors $v_1, \ldots, v_k \in R^n$.

For the greedy algorithm in the next section we need a total order on the vectors in R^n. This will be achieved by picking an ordered basis of R^n and fixing an order on the scalars in R. The latter needs to have a specific property for the algorithm to work properly.

Definition 1.2.1. A total order $<$ on R is called *respectful* if for all $x, y \in R \setminus \{0\}$ it satisfies

$$Rx \supsetneq Ry \implies \text{ there exists some } \alpha \in R^* \text{ such that } \alpha x < uy \text{ for all } u \in R^*.$$

In combination with Proposition 1.1.4 this tells us that in a respectful ordering for every nonzero $x \in R$ there is *some* generator of Rx that comes before *all* nonzero elements of Rx that are not generators. In particular, the smallest nonzero element in a respectfully ordered ring is a unit. The zero element may appear at any position in a respectful order. Note that any total order of a finite field is respectful.

Theorem 1.2.2. *Every finite principal ideal ring has a respectful ordering.*

Proof. Consider the poset of R^*-orbits with the partial order

$$R^*y \leq R^*x :\Longleftrightarrow y = rx \text{ for some } r \in R. \tag{1.2}$$

Choose a linear extension L of this poset (for existence, see [48, p. 110]). Then by definition $R^*y \leq R^*x$ implies $R^*y \leq_L R^*x$. On each R^*-orbit choose a total order. Moreover, for x, y such that $R^*x \neq R^*y$ define $x < y \Longleftrightarrow R^*x >_L R^*y$. This results in a total order on R with the additional property $R^*y <_L R^*x \Longleftrightarrow x < uy$ for all $u \in R^*$, and therefore

$$Rx \supsetneq Ry \implies y = rx \text{ for some } r \in R \implies R^*y <_L R^*x \implies x < uy \text{ for all } u \in R^*.$$

Hence the total order is respectful. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \square$

Note that (1.2) simply means $R^*y \leq R^*x :\Longleftrightarrow Ry \subseteq Rx$. Hence, thanks to Corollary 1.1.5, we have an order isomorphism between the poset of R^*-orbits and the poset of left ideals, and we may consider the linear extension as an extension of the poset of left ideals (with inclusion).

In the proof of Theorem 1.2.2 we actually proved the existence of an ordering satisfying a stronger property than respectfulness. Instead of showing the existence of *some* unit $\alpha \in R^*$ such that $\alpha x < uy$ for all $u \in R^*$, we actually showed that we may pick $\alpha = 1$. This is always the case for orderings that "respect a linear extension of the poset of left ideals". For general respectful orderings, other values of α may be necessary. Note also that the construction in the proof leads to $x < 0$ for all $x \in R \setminus \{0\}$. Again, respectfulness alone does not demand this property.

Example 1.2.3. (a) Consider the ring $\mathbb{Z}_{12}$. Then $L : (0) < (6) < (4) < (3) < (2) < (1) = \mathbb{Z}_{12}$ is a linear extension of the poset of ideals, and $1 < 5 < 7 < 11 < 2 < 10 < 3 < 9 < 4 < 8 < 6 < 0$ is an ordering of $\mathbb{Z}_{12}$ that respects L. Note that $R^* = \{1, 5, 7, 11\}$, $R^*2 = \{2, 10\}$, $R^*3 = \{3, 9\}$, $R^*4 = \{4, 8\}$, and $R^*6 = \{6\}$. Thus as in the above proof we have an order on the set of R^*-orbits as well as an order within each R^*-orbit itself.

(b) On any integer residue ring $\mathbb{Z}_m$, the natural order $0 < 1 < \ldots < m - 1$ is respectful. This follows from the fact that the poset of ideals is anti-isomorphic to the poset of positive divisors of m. However, if $\mathbb{Z}_m$ is not a field then this order does not respect any linear extension because $(m - 1) = (-1) = \mathbb{Z}_m \supsetneq I$ for any proper ideal I, but $m - 1 > a$ for all $a \in \{0, \ldots, m - 2\}$ in the natural order.

(c) Consider the ring $R = M_2(\mathbb{F}_2)$. Then the total order

$$R^* \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} <_L R^* \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} <_L R^* \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} <_L R^* \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} <_L R^* \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

is a linear extension of (1.2). Fixing a total order within each R^*-orbit, we obtain a respectful ordering on R. As in the above proof this would make the zero matrix the largest element. However, since respectfulness itself does not make any assumption on the zero element, we may actually move the zero matrix to anywhere in the ordering. The most natural choice is for the zero matrix to be the smallest element. In this case the above leads, for instance, to the ordering

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} < \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} < \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} < \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} < \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} < \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$
$$< \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} < \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} < \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} < \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} < \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$
$$< \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} < \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} < \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} < \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} < \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

(d) A total order on a finite chain ring R with ideals $R = (1) \supsetneq (\gamma) \supsetneq \ldots \supsetneq (\gamma^{e-1}) \supsetneq (\gamma^e) = (0)$ is respectful if and only if the following is satisfied: for any $0 \le i < j \le e - 1$ there is some $\alpha \in R^*$ such that $\alpha\gamma^i < u\gamma^j$ for all $u \in R^*$.

We now define a lexicographic ordering on R^n. It is based on a total order of R together with an ordered basis of R^n. The total order need not be respectful. The

latter will only be necessary in the next section for the greedy algorithm to produce desirable results. For the following definition, $<_{\text{lex}}$ denotes the lexicographic ordering on R^n induced by the total ordering $<$ on R.

Definition 1.2.4. Let R be a finite principal ideal ring with a total order $<$. Fix an ordered basis $B = \{b_1, \ldots, b_n\}$ of the free left R-module R^n. Let $V_0 = \{0\}$ and for $1 \leq i \leq n$ let $V_i = R\{b_1, \ldots, b_i\}$ be the submodule of R^n generated by the first i vectors in B. Thus $V_i = Rb_i + V_{i-1}$. We define the following *lexicographic ordering* on R^n and denote it also by $<$:
for $x \in V_l \setminus V_{l-1}$ and $y \in V_m \setminus V_{m-1}$ set

$$x < y :\Longleftrightarrow \left[l < m \quad \text{or} \quad (l = m \text{ and } (x_n, \ldots, x_1) <_{\text{lex}} (y_n, \ldots, y_1)) \right], \qquad (1.3)$$

where $(x_1, \ldots, x_n)$, $(y_1, \ldots, y_n)$ are the coefficient vectors of x and y with respect to the chosen basis B, that is $x = \sum_{j=1}^n x_j b_j$, $y = \sum_{j=1}^n y_j b_j \in R^n$. We call $V_i \setminus V_{i-1}$ the *i-th level set* of the ordered space R^n.

In the case where 0 is the least element of the ordered ring R, the lexicographic ordering above simplifies to $x < y \Longleftrightarrow (x_n, \ldots, x_1) <_{\text{lex}} (y_n, \ldots, y_1)$.

The lexicographic ordering on R^n induces the ordering of levels

$$\{0\} = V_0 \ < \ V_1 \setminus V_0 \ < \ V_2 \setminus V_1 \ < \ \ldots \ < \ V_n \setminus V_{n-1}, \qquad (1.4)$$

and where each level set is ordered according to (1.3). Thus the ordering on R only dictates the ordering within each level set, but not the ordering between the levels. The latter is dictated by the chosen ordered basis B.

Example 1.2.5. Consider the ring $\mathbb{Z}_4$ equipped with the ordering $1 < 3 < 2 < 0$, which respects the chain of ideals $(1) \supsetneq (2) \supsetneq (0)$. Let $B = \{100, 010, 001\}$ be the standard basis for $\mathbb{Z}_4^3$. Then the lexicographic ordering from Definition 1.2.4 is given by (1.4) and the internal ordering of the level sets:

$$
\begin{aligned}
V_0 \ &= \{000\}, \\
V_1 \setminus V_0 &= \{100 < 300 < 200\}, \\
V_2 \setminus V_1 &= \{110 < 310 < 210 < 010 < 130 < 330 \\
&\qquad < 230 < 030 < 120 < 320 < 220 < 020\}, \\
V_3 \setminus V_2 &= \{111 < 311 < 211 < 011 < 131 < \ldots < 002\}.
\end{aligned}
$$

Notice that the zero element acts here in two different ways: it "naturally" sorts the levels $V_i \setminus V_{i-1}$, but dictates an unusual sorting within each level.

1.3 The Greedy Algorithm

We now introduce a greedy algorithm that produces codes over a given finite principal ideal ring such that all (nonzero) codewords have a given pre-specified property. The algorithm generalizes the ones presented by Van Zanten and Suparta in [53] for codes over finite fields and by Guenda et al. in [24] for codes over finite chain rings.

Throughout, let R be a finite principal ideal ring. Moreover, let Γ be a fixed set of generators of the nonzero left ideals in R. In other words, Γ is a set of orbit representatives of the nonzero R^*-orbits of R (see Corollary 1.1.5). The following algorithm itself does not need the respectfulness of the ordering on R, but the properties of the resulting codes heavily rely on it. Thus we restrict ourselves to respectful orderings on R.

Algorithm 1.3.1. Fix a respectful ordering $<$ on R and an ordered basis B of R^n. Consider the resulting lexicographic ordering on the left R-module R^n as in Definition 1.2.4. Let $\mathcal{T}$ be a left invariant property on R^n.

1. Put $C_0 = \{0\}$. Set $i = 1$.

2. Search for the first (smallest) vector $a_i \in V_i \setminus V_{i-1}$ such that
$$\{\gamma a_i + c \mid \gamma \in \Gamma,\ c \in C_{i-1}\} \subseteq \mathcal{T}.$$

3. • If such a_i exists, let $C_i := \{ra_i + c \mid r \in R,\ c \in C_{i-1}\} = Ra_i + C_{i-1}$.
   • If no such a_i exists, let $C_i := C_{i-1}$.

4. • If $i < n$, set $i := i + 1$ and return to Step 2.
   • If $i = n$, stop and output C_n.

We call C_n a *lexicode* (or *lexicographic code*) with respect to the given ordering, basis, and property $\mathcal{T}$ and denote it by $C(<, B, \mathcal{T})$.

The generated codes C_i clearly depend on the chosen basis B, which determines the level sets $V_i \setminus V_{i-1}$, as well as on the ordering on R, which determines the ordering within the level sets. Examples of this dependence will be provided in Section 1.4.

We wish to point out that we explicitly allow invariant properties $\mathcal{T}$ for which $0 \notin \mathcal{T}$. While this may seem odd because we aim at constructing linear codes, this does indeed lead to interesting outcomes – as we will show later. Note that the algorithm always adds the zero vector to the code.

The definition of Γ and Proposition 1.1.4 immediately imply

Remark 1.3.2. Let $\mathcal{T}$ be a left invariant property on R^n, and C a left submodule of R^n such that $C \setminus \{0\} \subseteq \mathcal{T}$. Let $x \in R^n$. Then
$$\{\gamma x + c \mid \gamma \in \Gamma,\ c \in C\} \subseteq \mathcal{T} \iff \{rx + c \mid r \in R \setminus \{0\},\ c \in C\} \subseteq \mathcal{T}.$$

As a consequence, the resulting sets C_i do not depend on the choice of the generator set Γ. The use of Γ in the algorithm merely serves to reduce the number of tests in the selection step (Step 2.). If R is a finite field, we may choose $\Gamma = \{1\}$, and the algorithm reduces to Algorithm A in [53] by Van Zanten and Suparta. If R is a finite chain ring with ideal chain $R = (1) \supsetneq (\gamma) \supsetneq \ldots \supsetneq (\gamma^{e-1}) \supsetneq (\gamma^e) = (0)$, we may choose $\Gamma = \{1, \gamma, \gamma^2, \ldots, \gamma^{e-1}\}$, and the algorithm equals Algorithm A in [24] by Guenda et al. The above remark fails in general if $\mathcal{T}$ is not left invariant; see also Example 1.4.2(a) later in this paper.

The next theorem generalizes [52, Theorem 2.2] for lexicodes over $\mathbb{F}_2$, [53, Theorem 2.2] for lexicodes over $\mathbb{F}_q$, and [24, Theorem 4] for lexicodes over finite chain rings.

Theorem 1.3.3. *Consider Algorithm 1.3.1. Then for each i the set C_i is a code, i.e., a submodule of R^n, and $C_i \setminus \{0\} \subseteq \mathcal{T}$.*

Proof. Left linearity of each C_i is clear. The second statement is clearly true for C_0. Suppose now that $C_{i-1} \setminus \{0\} \subseteq \mathcal{T}$. If $C_i = C_{i-1}$, then there is nothing to prove. Else let a_i be the selected vector from $V_i \setminus V_{i-1}$. Then by Remark 1.3.2 $\{ra_i + c \mid r \in R \setminus \{0\}, c \in C_{i-1}\} \subseteq \mathcal{T}$. Since $C_i = Ra_i + C_{i-1}$, this establishes the desired result. □

Note that in Step 2 of Algorithm 1.3.1 we only select one (if any) vector a_i in the level $V_i \setminus V_{i-1}$, update C_{i-1} to $C_i := Ra_i + C_{i-1}$, and then move on to the next level $V_{i+1} \setminus V_i$. The next theorem justifies abandoning the search through the rest of $V_i \setminus V_{i-1}$. Indeed, as we will see, the respectfulness of the ordering on R guarantees that any vector $x \in V_i \setminus V_{i-1}$ such that $\{\gamma x + c \mid \gamma \in \Gamma, c \in C_i\} \subseteq \mathcal{T}$ is already in C_i. Therefore this theorem generalizes the result of [53, Theorem 2.1] for lexicodes over $\mathbb{F}_q$, and the result of [24, Lemma 3] for lexicodes over finite chain rings.

Theorem 1.3.4. *Consider Algorithm 1.3.1 and the resulting nested codes $C_0 \subseteq \ldots \subseteq C_n$. Let $x \in V_i \setminus V_{i-1}$ be such that $\{\gamma x + c \mid \gamma \in \Gamma, c \in C_i\} \subseteq \mathcal{T}$. Then $x \in C_i$.*

Proof. We induct on i. For the base case, the statement is trivially true because $V_0 = \{0\} = C_0$.

Let $1 \leq i \leq n$ and assume the statement holds for all indices less than i. Let $x \in V_i \setminus V_{i-1}$ be such that $\{\gamma x + c \mid \gamma \in \Gamma, c \in C_i\} \subseteq \mathcal{T}$. Then there must have been some selected vector $a_i \in V_i \setminus V_{i-1}$. Thus $C_i = Ra_i + C_{i-1}$. Setting $\hat{R} := R \setminus \{0\}$ we have $\hat{R}x + C_i \subseteq \mathcal{T}$ and hence $\hat{R}x + Ra_i + C_{i-1} \subseteq \mathcal{T}$. Note that V_i/V_{i-1} is isomorphic to R via the map $\rho(\sum_{l=1}^{i} r_l b_l + V_{i-1}) = r_i$. Since R is a principal ideal ring, we conclude that $\rho(Rx + Ra_i + V_{i-1}) = Rd$ for some $d \in R$, and therefore

$$Rx + Ra_i \subseteq Rdb_i + V_{i-1}. \tag{1.5}$$

Clearly, $d \neq 0$. We show next that $Rdb_i + V_{i-1} \subseteq Ra_i + V_{i-1}$. Write $a_i = pb_i + w$ and $x = qb_i + w'$, where $p, q \in R \setminus \{0\}$ and $w, w' \in V_{i-1}$. Then $\rho(ra_i + sx + V_{i-1}) = rp + sq$ for all $r, s \in R$, and therefore $Rd = Rp + Rq$. Hence there exist $a, b \in R$ such that $ap + bq = d$ and by Theorem 1.1.1 we may even assume that b is a unit. Then $\hat{R}b = \hat{R}$ and therefore $y := aa_i + bx$ satisfies

$$\hat{R}y + C_{i-1} \subseteq \hat{R}bx + Ra_i + C_{i-1} = \hat{R}x + Ra_i + C_{i-1} \subseteq \mathcal{T}. \tag{1.6}$$

This shows that y satisfies the selection criterion of the algorithm. Let us now relate y to the actually selected vector a_i. From $Rd = Rp + Rq$ we obtain $Rp \subseteq Rd$. If $Rp \subsetneq Rd$, then respectfulness implies $p > \alpha d$ for some $\alpha \in R^*$. Thus $a_i > \alpha y$. But then (1.6) tells us that αy would have been selected in the algorithm, and this contradicts the selection of a_i. Hence $Rp = Rd$ and thus $Rq \subseteq Rp$. This in turn implies $x \in Ra_i + V_{i-1}$, say $x = \beta a_i + v$ for some $\beta \in R$ and $v \in V_{i-1}$. As a consequence,

$$\hat{R}v + C_{i-1} = \hat{R}(x - \beta a_i) + C_{i-1} \subseteq \hat{R}x + Ra_i + C_{i-1} \subseteq \mathcal{T},$$

and by induction $v \in C_{i-1}$. Hence $x = \beta a_i + v \in C_i$, as desired. □

In the above proof we obtained $Rp = Rd$ and thus $Rq \subseteq Rp$. Showing this containment was the sole purpose of introducing the vector y. For the case of finite chain rings, all left ideals are comparable and the containment $Rq \subseteq Rp$ follows immediately from the respectful ordering, so the proof becomes greatly simplified.

As the proof above suggests, the existence of $\beta \in R \setminus \{0\}$ and $v \in V_{i-1}$ such that $x = \beta a_i + v$ is not trivial over rings (it is clearly always the case over fields). Only the respectfulness of the ordering on R guarantees this step for principal ideal rings, and in Example 1.4.1(b) we show that the above theorem is indeed not true if the ordering of R is not respectful. For this reason our proof completes the one given in [24, Lemma 3], where this detail seems to have been overlooked since no specifics on the ordering of the ring elements are given. It seems, however, that only respectful orderings were used in the examples in [24].

In Example 1.4.2 we show that the previous theorem also fails if either the property $\mathcal{T}$ is not left invariant or the ring is not a principal ideal ring.

The examples in the next section suggest that the use of a respectful ordering in Algorithm 1.3.1 produces large codes. As we show next, these codes are in fact maximal if $0 \in \mathcal{T}$. The maximality in the sense of the following theorem is not true if $0 \notin \mathcal{T}$; see Example 1.4.5. But we do obtain a certain analogy for the case where $0 \notin \mathcal{T}$, as we will show below. Recall from Corollary 1.1.14 that we may toggle between $0 \in \mathcal{T}$ and $0 \notin \mathcal{T}$ as desired. For instance, we may toggle between the property $\mathcal{T} = \{x \in R^n \mid \mathrm{wt_H}(x) \geq \delta\}$ and $\mathcal{T}' = \{x \in R^n \mid \mathrm{wt_H}(x) \geq \delta \text{ or } x = 0\}$.

Theorem 1.3.5. *Let $<$ and B be as in Algorithm 1.3.1 and let $\mathcal{T}$ be a left invariant property such that $0 \in \mathcal{T}$. Then the lexicode $C(<, B, \mathcal{T})$ is maximal (with respect to inclusion) in the poset of all codes contained in $\mathcal{T}$.*

Proof. Recall the codes C_i from Algorithm 1.3.1. Suppose contrarily that there is some linear code C satisfying $\mathcal{T}$ such that $C_n \subsetneq C \subseteq R^n$. Let $x \in C \setminus C_n$. Then $\{\gamma x + c \mid \gamma \in \Gamma, c \in C_n\} \subseteq \mathcal{T}$ by assumption (here $0 \in \mathcal{T}$ is crucial because $\gamma x + c$ may be zero). Since x lies in $V_i \setminus V_{i-1}$ for some $i = 1, \ldots, n$ and $\{\gamma x + c \mid \gamma \in \Gamma, c \in C_i\} \subseteq \mathcal{T}$, Theorem 1.3.4 implies that $x \in C_i \subseteq C_n$, a contradiction. $\square$

We now turn to the case where $0 \notin \mathcal{T}$.

Theorem 1.3.6. *Let $<$ and B be as in Algorithm 1.3.1 and let $\mathcal{T}$ be a left invariant property such that $0 \notin \mathcal{T}$. Then each code C_i generated by Algorithm 1.3.1 is free, and the selected vectors form a basis for C_i.*

Proof. Let $a_{j_1} < \ldots < a_{j_k}$ be the vectors selected by Algorithm 1.3.1 to generate C_i. Suppose that the vectors are linearly dependent, say $\sum_{l=1}^t \lambda_l a_{j_l} = 0$ for some scalars $\lambda_l \in R$ with $\lambda_t \neq 0$. Note that $a_{j_1} < \ldots < a_{j_t}$ generate some $C_{i'}$ and $a_{j_1} < \ldots < a_{j_{t-1}}$ are in $C_{i'-1}$. Remark 1.3.2 tells us that $\{ra_{j_t} + c \mid r \in R \setminus \{0\}, c \in C_{i'-1}\} \subseteq \mathcal{T}$. In particular $\lambda_t a_{j_t} + \sum_{l=1}^{t-1} \lambda_l a_{j_l} \in \mathcal{T}$, contradicting $0 \notin \mathcal{T}$. Therefore the vectors $a_{j_1}, \ldots, a_{j_k}$ form a linearly independent set. Since by construction C_i is generated by these vectors, we obtain the desired result. $\square$

We now obtain the analogue of Theorem 1.3.5.

Theorem 1.3.7. *If $<$ is a respectful ordering of R and $\mathcal{T}$ is a left invariant property where $0 \notin \mathcal{T}$, then the code $C := C(<, B, \mathcal{T})$ generated by Algorithm 1.3.1 is maximal (with respect to inclusion) in the poset $\{C \subseteq R^n \mid C \text{ is free and } C \setminus \{0\} \subseteq \mathcal{T}\}$.*

Proof. By Theorems 1.3.6 and 1.3.3, the module C is free with basis $\{a_{j_1}, \ldots, a_{j_k}\}$, and $C \setminus \{0\} \subseteq \mathcal{T}$. Suppose contrarily that there is some free linear code $\tilde{C}$ such that $\tilde{C} \setminus \{0\} \subseteq \mathcal{T}$ and $C \subsetneq \tilde{C} \subseteq R^n$. By Theorem 1.1.6 there exists a submodule C' such that $C \oplus C' = \tilde{C}$. Hence there exists some $x \in \tilde{C} \setminus C$ such that $\{a_{j_1}, \ldots, a_{j_k}, x\}$ is linearly independent. Thus $rx + c \neq 0$ for all $r \in R \setminus \{0\}$, $c \in C$ and thus $\{rx + c \mid r \in R \setminus \{0\}, c \in C\} \subseteq \mathcal{T}$. Let $i \in \{1, \ldots, n\}$ such that $x \in V_i \setminus V_{i-1}$. Then Theorem 1.3.4 tells us that $x \in C_i$, contradicting that $x \notin C$. $\qquad \square$

In Examples 1.4.5 and 1.4.7 we illustrate the different outcomes of the algorithm when we add or subtract the zero vector from the property set $\mathcal{T}$ (i.e., in the sense of Remark 1.1.11, if we toggle $P[0]$ between true and false). In general, but not always, if $0 \notin \mathcal{T}$ one obtains a significantly smaller code. More importantly, even though switching to the property $\mathcal{T} \cup \{0\}$ simply widens the selection criterion, the algorithm does not always produce a lexicode that contains the lexicode for the property $\mathcal{T}$.

The following result shows that with a suitable choice of the lexicographic ordering on R^n every free code satisfying an invariant property can be obtained as a 'partial lexicode', that is, a code obtained when stopping the algorithm after a certain number of rounds. In combination with the previous theorems this result may be used to test whether a given code is maximal among all codes satisfying the property or, if not, extend it to a maximal code.

Theorem 1.3.8. *Any free linear code $C \subseteq R^n$ satisfying the invariant property $\mathcal{T}$ for all nonzero $x \in C$ is a subcode of a lexicode $C(<, B, \mathcal{T})$ for some suitable respectful ordering $<$ on R and a suitable basis B of R^n.*

Proof. Since C is free, it has some basis $\{b_1, \ldots, b_k\}$. By Theorem 1.1.6, we can extend this to a basis $B = \{b_1, \ldots, b_n\}$ of R^n. Choose a respectful ordering on R starting with $0 < 1 < \ldots$. Running Algorithm 1.3.1 with this basis B and respectful ordering, the first vector in the level set $V_i \setminus V_{i-1}$ is b_i. Note that $rb_i + c \neq 0$ for all $r \in R \setminus \{0\}$, $c \in V_{i-1}$. Thus, $\{rb_i + c \mid r \in R \setminus \{0\}, c \in V_{i-1}\} \subseteq \mathcal{T}$ for $i < k$ (regardless of whether or not $0 \in \mathcal{T}$), and the algorithm selects $a_i = b_i$ for every $i = 1, \ldots, k$. Then $C = C_k \subseteq C(<, B, \mathcal{T})$. $\qquad \square$

We strongly believe that Theorem 1.3.8 is true for general (i.e., non-free) codes. However, an abundance of examples shows that only a very judicious choice of basis of R^n leads to a lexicode containing the given code (but the given code is not necessarily a 'partial lexicode'!). Unfortunately, we are not able to provide a description of such a basis and a proof of its existence.

1.4   Examples of Lexicodes

We start with an example showing that the respectfulness of the ordering is necessary for Theorem 1.3.4 to be true, even over a finite chain ring.

Example 1.4.1. (a) Consider $\mathbb{Z}_4^4$ with standard basis $B = \{1000, 0100, 0010, 0001\}$ and the property $\mathcal{T} = \{x \mid x \cdot x = 0\}$. Using the natural, thus respectful, ordering $0 < 1 < 2 < 3$, the selected vectors are $a_1 = 2000, a_2 = 0200, a_3 = 0020$, and $a_4 = 1111$. The resulting lexicode $C_4 = R\{a_1, a_2, a_3, a_4\}$ has cardinality 32 and is clearly not free.

(b) Consider now the non-respectful ordering $0 < 2 < 1 < 3$ on $\mathbb{Z}_4$. Using the same basis of $\mathbb{Z}_4^4$ and the same property as in (a), the algorithm generates the lexicode $C_4 = R\{a_1, a_2, a_3, a_4\}$ of size 16 with selected vectors $a_1 = 2000, a_2 = 0200, a_3 = 0020$, and $a_4 = 0002$. Observe that this code is strictly contained in the one from (a). The vector $x = 1111 \in V_4 \setminus V_3$ satisfies $\{\gamma x + c \mid \gamma \in \Gamma = \{1, 2\}, c \in C_3\} \subseteq \mathcal{T}$, where C_3 is the code from the previous iteration of the algorithm. But x is not in C_4. This is due to the fact that x cannot be written in the form $x = \beta a_4 + v$ for any $\beta \in R$, $v \in V_3$; see proof of Theorem 1.3.4. In other words, the vector 0002 was selected instead of 1111 (or some other vector with a unit in the last entry), which would not have happened with a respectful ordering.

The following examples show that Theorem 1.3.4 is not true in general if either the property is not left invariant or the ring is not a principal ideal ring.

Example 1.4.2. (a) Consider the field $R = \mathbb{Z}_3 = \{0, 1, 2\}$ with the natural order $0 < 1 < 2$, which is respectful. Let $\mathcal{T} = \{2\}$. Then $\mathcal{T}$ is not invariant because $2 \cdot 2 \notin \mathcal{T}$. In R^1 with standard basis $e_1 = 1$ the lexicode resulting from Algorithm 1.3.1 is $C = \mathbb{Z}_3$. It does not satisfy Theorem 1.3.3. Note that due to the non-invariance of $\mathcal{T}$ even Remark 1.3.2 is not true.

(b) Consider the ring $R := \mathbb{F}_2[x, y]/(x^2, xy, y^2) = \{0, x, y, x+y, 1, 1+x, 1+y, 1+x+y\}$. Note that the last 4 elements are the units of R. The ring has 4 non-trivial ideals given by $(x), (y), (x+y), (x, y)$. The first three are principal and have cardinality 2, the last one is not principal and has cardinality 4. Based on this and Definition 1.1.8 the homogeneous weight on R turns out to be

$$\omega(0) = 0, \quad \omega(x) = \omega(y) = \omega(x+y) = 2, \quad \omega(u) = \frac{1}{2} \text{ for all } u \in R^*.$$

In R^1 consider the invariant property $\mathcal{T} = \{x \mid \omega(x) \geq 2 \text{ or } x = 0\}$. Moreover, consider any ordering of the ring elements[1] and the standard basis $e_1 = 1$. Then Algorithm 1.3.1 results in the lexicode $C = C_1 = (w) = \{0, w\}$, where w is the first nonunit element in the ordering of R. As a consequence, Theorem 1.3.4 is not satisfied for $i = 1$ because every element in $\{0, x, y, x+y\}$ satisfies the property. For the same reason, Theorem 1.3.5 is not satisfied. All of this shows that for non-principal ideal rings, the search in Step 2. of Algorithm 1.3.1 should continue through each entire level $V_i \setminus V_{i-1}$.

---

[1] Note that the definition of respectfulness for an ordering is based on principal left ideals. If we simply ignore the non-principal ideal (x, y) and follow Definition 1.2.1, then any ordering of the form $0 < 1 <$ "rest" may be called respectful. However, this case is not useful in the endeavors to come.

The next example illustrates that different respectful orderings may generate different codes. Part (b) shows that, for codes over fields, even the dimension of the resulting code depends on the choice of the respectful ordering.

Example 1.4.3. (a) Consider the reverse standard basis $B = \{001, 010, 100\}$ for $\mathbb{Z}_4^3$ and the selection property $\mathcal{T} = \{x \mid \mathrm{wt_L}(x) \geq 2\}$, where $\mathrm{wt_L}$ is the Lee weight; see Definition 1.1.7(d). Note that $0 \notin \mathcal{T}$. Since $\mathbb{Z}_4^* = \{1, 3\}$, a total ordering $<$ on $\mathbb{Z}_4$ is respectful iff $1 < 2$ or $3 < 2$. We obtain the following cases: (i) Using any of the respectful orderings $r_1 < 0 < r_2 < r_3$, where $r_1 \in \mathbb{Z}_4^*$, we obtain the lexicode $C = \mathbb{Z}_4\{011, 103\}$ (the two given vectors are not necessarily the vectors a_i selected by the algorithm). (ii) With any of the respectful orderings $r_1 < r_2 < r_3 < r_4$, where $\{r_1, r_2\} = \mathbb{Z}_4^*$, we obtain the lexicode $C = \mathbb{Z}_4\{011, 102\}$. (iii) With any other respectful ordering we obtain the lexicode $C = \mathbb{Z}_4\{011, 101\}$. In each case the resulting lexicode has cardinality 16.

(b) Consider the field $\mathbb{F} = \mathbb{F}_7$ and in $\mathbb{F}^3$ define the codes $C = \mathbb{F}\{100, 010\}$, $D = \mathbb{F}\{001\}$. Let $\mathcal{T} = C \cup D$. Note that $\mathcal{T}$ is invariant and $0 \in \mathcal{T}$. Fix the ordered basis $B = \{113, 331, 100\}$ of $\mathbb{F}^3$. (i) Using the respectful ordering $0 < 1 < 2 < 3 < 4 < 5 < 6$ the algorithm returns $a_2 = 1(331) + 2(113) = 550$, thus $C_2 = \mathbb{F}\{550\}$, and $a_3 = 100$. Hence $C(<, B, \mathcal{T}) = C$. (ii) Using the respectful ordering $0 < 1 < 4 < 3 < 2 < 5 < 6$ the algorithm returns $a_2 = 1(331) + 4(113) = 006$, thus $C_2 = \mathbb{F}\{001\}$, and there is no return for a_3. Thus $C(<, B, \mathcal{T}) = D$.

Of course, the output of the algorithm also depends on the choice of the basis B. Again, even the dimension of the lexicode (e.g., for field alphabets) depends on B. The choice of basis may also decide on whether the lexicode is free or not.

Example 1.4.4. (a) Let $\mathbb{F}$ be any finite field. Consider the codes $C = \mathbb{F}\{100, 010\}$ and $D = \mathbb{F}\{001\}$ in $\mathbb{F}^3$. Let $\mathcal{T} = C \cup D$. Fix any total ordering $<$ on $\mathbb{F}$. Using the basis $B = \{100, 010, 001\}$, the algorithm returns the code C, whereas with the basis $B' = \{001, 010, 100\}$ it returns D.

(b) Consider the codes $C = \mathbb{Z}_4\{200, 020\}$, $D = \mathbb{Z}_4\{001\}$ in the module $\mathbb{Z}_4^3$. Using the same property as in (a) and the standard basis of $\mathbb{Z}_4^3$, the algorithm returns the non-free code C, whereas with the reverse standard basis it returns the free code D.

We now illustrate the result of the greedy algorithm when toggling between $0 \in \mathcal{T}$ and $0 \notin \mathcal{T}$.

Example 1.4.5. Consider any respectful ordering on $\mathbb{Z}_4$ and the module $\mathbb{Z}_4^3$ with the standard basis. Let $\mathcal{T} = \{x \mid \mathrm{wt_L}(x) \geq 6\}$, where $\mathrm{wt_L}$ is again the Lee weight. Clearly, $\mathcal{T}$ is invariant, and actually $\mathcal{T} = \{222\}$. But since $2 \cdot 222 = 000$ and $000 \notin \mathcal{T}$, Algorithm 1.3.1 returns the zero code. If we toggle $\mathcal{T}$ to $\mathcal{T} \cup \{000\}$, then 222 is selected and we obtain the non-free code $\{000, 222\}$. All of this shows that Theorem 1.3.5 fails if $0 \notin \mathcal{T}$.

Example 1.4.6. We consider the exact situation of Example 1.4.1(a) with the only difference that we toggle $\mathcal{T}$ to $\mathcal{T} \setminus \{0\}$. Thus $\mathcal{T} = \{x \mid x \cdot x = 0 \text{ and } x \neq 0\}$. Using the same respectful ordering and the same basis, Algorithm 1.3.1 returns the code $C = \mathbb{Z}_4\{1111\}$. It is a free subcode of the lexicode returned in Example 1.4.1(a).

Example 1.4.7. Consider $R := \mathbb{Z}_{10}$ with the natural, thus respectful, ordering $0 < 1 < \ldots < 9$. By Definition 1.1.8 the homogeneous weight on R is given by

$$\omega(0) = 0, \ \omega(5) = 2, \ \omega(u) = \frac{3}{4} \text{ for } u \in \{1, 3, 7, 9\}, \ \omega(r) = \frac{5}{4} \text{ for } r \in \{2, 4, 6, 8\}.$$

(a) Consider now the invariant property $\mathcal{T} = \{x \mid \omega(x) \geq 2\}$ on the module R^3, where the homogeneous weight is extended to vectors as in (1.1). Thus $0 \notin \mathcal{T}$. Using the ordered basis $B = \{001, 010, 100\}$ of R^3, Algorithm 1.3.1 returns $C_1 = \{0\}$, $C_2 = C_3 = R\{012\}$. Hence $C_3 = C(<, B, \mathcal{T})$ is indeed a free code with basis $\{012\}$ and cardinality 10.

(b) With the same data as in (a), but where we switch to the property set $\mathcal{T} \cup \{0\}$, the algorithm returns $C' := C_3 = R\{005, 021, 201\}$. The code C' is not free and has cardinality 50. A minimal generating set is given by $\{201, 820\}$. One should note that the code C from (a), which is free, is not a subcode of C'. In fact, $C \cap C' = \{0\}$, though all we did is switch from the property $\mathcal{T}$ to $\mathcal{T} \cup \{0\}$.

Let us now turn to the construction of self-orthogonal codes. Recall from Remark 1.1.13 that over a commutative ring with odd characteristic we achieve self-orthogonality using the (invariant) property $\mathcal{T} = \{x \mid x \cdot x = 0\}$. Obviously $0 \in \mathcal{T}$. In (c) of the following example we provide a case where the property $\mathcal{T} \setminus \{0\}$ produces a free code *of the same size* as the lexicode for the property $\mathcal{T}$. The fact that we obtain in both cases lexicodes of the same size is remarkable because, more often than not, codes generated with $\mathcal{T} \setminus \{0\}$ are much smaller than their counterparts with $\mathcal{T} \cup \{0\}$.

Example 1.4.8. For all examples we consider the property $\mathcal{T} = \{x \mid x \cdot x = 0\}$.

(a) On $\mathbb{F}_5^4$ consider the reverse standard basis $B = \{e_4, e_3, e_2, e_1\}$ and fix the natural ordering $0 < 1 < 2 < 3 < 4$ on $\mathbb{F}_5$. Then Algorithm 1.3.1 returns $C_1 = \{0\}, C_2 = C_3 = \mathbb{F}_5\{0012\}$ and $C := C(<, B, \mathcal{T}) = C_4 = \mathbb{F}_5\{0012, 1200\}$, which by Theorem 1.3.3 and Remark 1.1.13 is self-orthogonal, that is, $C \subseteq C^\perp$. Since $\dim(C) = 2$ we conclude that $C = C^\perp$, that is, C is self-dual. This also shows that C is not a proper subcode of a code satisfying property $\mathcal{T}$ (thus illustrating Theorem 1.3.5).

(b) In the same way we obtain in $\mathbb{F}_7^4$ (using the natural ordering and the reverse standard basis) the self-dual code $C = \mathbb{F}_7\{0123, 1035\}$.

(c) Over the ring $\mathbb{Z}_9$ with the natural ordering and the reverse standard basis of $\mathbb{Z}_9^4$ we obtain the lexicode $C := C(<, B, \mathcal{T}) = \mathbb{Z}_9\{0003, 0030, 0300, 3000\}$, which is not free and has 81 elements. If we switch to the property $\mathcal{T} \setminus \{0\}$, we obtain the free lexicode $C' := \mathbb{Z}_9\{0114, 1048\}$ of cardinality 81. From the identity $|C| \cdot |C^\perp| = 9^4$ (see Remark 1.1.13) we conclude that both codes are actually self-dual and thus maximally self-orthogonal.

Over rings with even characteristic, Remark 1.1.13 is no longer sufficient, and self-orthogonality cannot be described by an invariant property. However, over the alphabet $\mathbb{Z}_4$ it is known that if $C \subseteq \mathbb{Z}_4^n$ is a code such that the Euclidean weight of each codeword $x \in C$ satisfies $\mathrm{wt}_E(x) \equiv 0 \mod 8$ then C is self-orthogonal; see [30,

16

Thm. 12.2.4]. Clearly, the greedy algorithm allows us to construct such triply-even codes (that is, the Euclidean weight of each codeword is divisible by 8) by using the property $\mathcal{T} = \{x \in \mathbb{Z}_4^n \mid \mathrm{wt_E}(x) \equiv 0 \mod 8\}$, and it arises the question as to when this code is maximal within the class of all *self-orthogonal* codes. Using the standard form for generator matrices of codes over $\mathbb{Z}_4$ and the resulting standard form for the dual code, see [30, pp. 469], it is not hard to see that every self-orthogonal code over $\mathbb{Z}_4$ is contained in a self-dual code. This implies that the greedy algorithm for the above property $\mathcal{T}$ produces a triply-even self-orthogonal code which is maximal within the class of all self-orthogonal codes if and only if it is self-dual. In this context recall that triply-even self-dual codes exist only if the length n is divisible by 8; see [30, Cor. 12.5.5].

Example 1.4.9. Consider $\mathbb{Z}_4^5$ with the property $\mathcal{T} = \{x \mid \mathrm{wt_E}(x) \equiv 0 \mod 8\}$ and the reverse standard basis $B = \{e_5, \ldots, e_1\}$. Using the natural ordering $0 < 1 < 2 < 3$ on $\mathbb{Z}_4$ we obtain the triply-even lexicode

$$C(<, B, \mathcal{T}) = \mathbb{Z}_4\{00022, 00202, 02002, 20002\},$$

which has cardinality 16. It is clearly contained in the self-dual code

$$C = \mathbb{Z}_4\{00002, 00020, 00200, 02000, 20000\},$$

which is not triply-even. Many more examples of self-orthogonal lexicodes over $\mathbb{Z}_4$, including triply-even self-dual codes of length 8, are given in [24, Table 2].

We briefly touch upon a selection property that arises in the context of DNA codes.

Example 1.4.10. Consider $\mathbb{Z}_4^4$ with the invariant property $\mathcal{T} = \{x \mid \mathrm{wt_U}(x) \leq 2\}$; see Definition 1.1.7(c). Using the natural ordering $<$ on $\mathbb{Z}_4$ and the reverse standard basis B on $\mathbb{Z}_4^4$, one obtains the lexicode $C(<, B, \mathcal{T}) = \mathbb{Z}_4\{0001, 0010, 0200, 2000\}$, which has cardinality 64. This idea could prove useful in constructing DNA codes with bounded GC-content, as discussed in [5], by suitably identifying the elements of $\mathbb{Z}_4$ with the 4 nucleotides A, G, T, C. However, we wish to add that codes with *constant* GC-content appear to be more useful for DNA computing as they guarantee a uniform hybridization process [37]. These codes are clearly nonlinear and thus do not fall in the realm of this paper.

We close this analysis with an example over a noncommutative ring.

Example 1.4.11. Let $R = M_2(\mathbb{F}_2)$ be respectfully ordered as in Example 1.2.3(c). Consider R^3 with the reverse standard basis $B = \{e_3, e_2, e_1\}$, thus

$$e_1 = (I_2, 0, 0), \ e_2 = (0, I_2, 0), \ e_3 = (0, 0, I_2).$$

We use the selection property $\mathcal{T} = \{x \mid \mathrm{rankSum}(x) \geq 2\}$, see Example 1.1.7(b). Then Algorithm 1.3.1 produces the lexicode $C(<, B, \mathcal{T}) = R\{(0, I_2, I_2), (I_2, 0, I_2)\}$, which is free of dimension 2 (as it has to be according to Theorem 1.3.6), thus cardinality 256.

Chapter 2 Ferrers Diagram Rank-Metric Codes

This chapter is a reproduction of [2], with added detail in some areas. It reflects the second of the two major projects represented in this dissertation.

For random linear network coding, see [9] by Chou et al. and [26] by Ho et al., the natural coding-theoretical objects are subspace codes. This observation by Koetter et al. [31, 47] has led to extensive research efforts for constructions and decoding of subspace codes [4, 13, 14, 17, 19, 20, 21, 22, 25, 36, 41, 46, 47, 50, 54].

One way to construct good subspace codes utilizes rank-metric codes. These are subspaces (or subsets) of some matrix space $\mathbb{F}_q^{m \times n}$ endowed with the rank metric $\mathrm{d}_{\mathrm{rk}}(A, B) = \mathrm{rk}(A - B)$. This naturally leads to the task of constructing large rank-metric codes with a given rank distance, and many of the above mentioned articles contribute to this question. Already in the 70's, Delsarte [12] and independently in the 80's Gabidulin [15] show that the maximum dimension of an $m \times n$-rank-metric code with rank distance δ is given by $m(n - \delta + 1)$ if $n \leq m$. Codes attaining this bound are called MRD codes (maximum rank-distance codes), and both authors provide a construction of such codes. These MRD codes, now known as Gabidulin codes, are constructed within the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^m}^n$, which is naturally isometric to $(\mathbb{F}_q^{m \times n}, \mathrm{d}_{\mathrm{rk}})$. They are not just $\mathbb{F}_q$-linear but even $\mathbb{F}_{q^m}$-linear. More recently, a lot of attention has been paid to the existence and construction of MRD codes that are not equivalent to Gabidulin codes and not necessarily $\mathbb{F}_{q^m}$-linear. Most notably, in [44] Sheekey presents a construction of MRD-codes that are not equivalent to Gabidulin codes. Further contributions have been made by de la Cruz et al. [11] and Trombetti/Zhou [51].

A very straightforward construction of good subspace codes with the aid of rank-metric codes is the lifting construction [31]: to each matrix M in the given rank-metric code one associates the row space of the matrix $(I \mid M)$, where I is the identity matrix of suitable size. While this simple construction leads to subspace codes with good distance, it usually does not produce large codes. A remedy has been introduced by Etzion/Silberstein [14]: obviously a matrix of the form $(I \mid M) \in \mathbb{F}^{m \times (m+n)}$ is in reduced row echelon form (RREF) with pivot indices $1, \ldots, m$. This observation has led to the *multilevel construction*, where for each level a rank-metric code in $\mathbb{F}^{m \times n}$ is used to construct a subspace code in $\mathbb{F}^{m+n}$ with all representing $m \times (m + n)$-matrices being in RREF with a fixed set of general pivot indices. For this to work out properly, the matrices in the given rank-metric code have to be supported by the Ferrers diagram associated with the list of pivot indices; see [14] and Remark 2.1.5 later in this paper. As a result, the multilevel construction leads to the task of constructing large Ferrers diagram codes with a given rank distance. In [14] the authors provide an upper bound for the dimension of a rank-metric code supported by a given Ferrers diagram $\mathcal{F}$ and with a given rank distance δ. In this paper, codes attaining this bound will be called maximal $[\mathcal{F}; \delta]$-codes. To this day, it is not clear whether maximal $[\mathcal{F}; \delta]$-codes exist for all pairs $(\mathcal{F}; \delta)$ and all finite fields. Several cases have been settled by Etzion et al. [13, 14] and Gorla/Ravagnani [22] and, more

recently, by Liu et al. [35] and Zhang/Ge [56], but the general case remains widely open. In [3] Ballico studies the existence of maximal $[\mathcal{F}; \delta]$-codes over number fields.

In this paper we survey some of these results and extend them to further classes of pairs $(\mathcal{F}; \delta)$. In particular, we provide a family of pairs $(\mathcal{F}; \delta)$ for which maximal $[\mathcal{F}; \delta]$-codes can be realized for any finite field $\mathbb{F}_q$ as subfield subcodes of Gabidulin codes (or other $\mathbb{F}_{q^m}$-linear MRD codes). Since Gabidulin codes can be efficiently decoded, the same is true for such subfield subcodes. We also illustrate that for general pairs $(\mathcal{F}; \delta)$ such a subfield subcode construction is not possible. This is due to the non-existence of invariant subspaces in those cases. Furthermore, we present constructions for the special case where $\mathcal{F}$ is the $n \times n$-upper triangle and the rank is $n - 1$. In this case the dimension of a maximal $[\mathcal{F}; n - 1]$-code is just 3, and despite the simplicity of the situation no construction of maximal $[\mathcal{F}; n - 1]$-codes over arbitrary finite fields was known before.

Finally, we turn to the proportion of maximal $[\mathcal{F}; \delta]$-codes within the space of all N-dimensional codes in $\mathbb{F}_q^{m \times n}$ with shape $\mathcal{F}$, and where N is the dimension of a maximal $[\mathcal{F}; \delta]$-code. Special attention will be paid to the limiting proportion as q tends to infinity. If this limit is 1, we call maximal $[\mathcal{F}; \delta]$-codes generic. We will see that $[\mathcal{F}; \delta]$-codes are generic if and only if there exists an N-dimensional $[\mathcal{F}; \delta]$-code over any algebraically closed field of positive characteristic. This will tell us that genericity depends highly on the shape $\mathcal{F}$; in particular MRD codes are not generic (which has also recently been observed by Byrne/Ravagnani [7]). The latter contrasts recent results in [40] by Neri et al., who showed that MRD codes are generic if one restricts oneself to $\mathbb{F}_{q^m}$-linear rank-metric codes. Finally, for several nongeneric cases we provide upper bounds on the proportion. Among other things we will see that the limiting proportion of $[m \times n; \delta]$-MRD codes is upper bounded by $(1/e)^{(\delta-1)(n-\delta+1)}$ as $q, m \to \infty$, with equality if $n = \delta = 2$ (improving upon bounds in [7]). This is derived from the fact [49] that the proportion of matrices in $\mathbb{F}_q^{m \times m}$ with empty spectrum is asymptotic to $1/e$ as $q, m \to \infty$. It remains an open question whether there exist parameters (m, n, δ) for which the limiting proportion of $[m \times n; \delta]$-MRD codes is zero.

2.1 Background and Preliminary Results

Throughout, let q be a prime power and $\mathbb{F}_q$ be a finite field of order q. For any $m \in \mathbb{N}$ consider the field extension $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Let $B = (x_1, \ldots, x_m)$ be an ordered basis of $\mathbb{F}_{q^m}$ as an $\mathbb{F}_q$-vector space. Then we have the coordinate map

$$\phi_B : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q^m, \quad a := \sum_{i=1}^{m} \alpha_i x_i \longmapsto \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} =: [a]_B$$

We also write $[a]_B$ for $\phi_B(a)$. The isomorphism ϕ_B extends to the isomorphism

$$\phi_B : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^{m \times n}, \quad (a_1, \ldots, a_n) \longmapsto \big([a_1]_B, \ldots, [a_n]_B\big). \tag{2.1}$$

On the vector space $\mathbb{F}_q^{m\times n}$ we define the rank metric as $\mathrm{d}_{\mathrm{rk}}(A,B) := \mathrm{rk}(A-B)$. It is well-known that this is indeed a metric. (See Appendix A for a proof.) Furthermore, on the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^m}^n$ we define the rank weight as $\mathrm{rk}(a_1,\ldots,a_n) = \dim_{\mathbb{F}_q}\langle a_1,\ldots,a_n\rangle$, where throughout this paper the notation $\langle\ \rangle$ stands for the $\mathbb{F}_q$-subspace generated by the indicated elements. The rank weight induces the rank metric on $\mathbb{F}_{q^m}^n$ in the obvious way. It is clear that ϕ_B is an isometry (i.e., a metric-preserving isomorphism) between $\mathbb{F}_{q^m}^n$ and $\mathbb{F}_q^{m\times n}$.

Definition 2.1.1. An $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{m\times n}$ or $\mathbb{F}_{q^m}^n$ is called a *rank-metric code*. The *(minimal) rank distance* of the rank-metric code C is defined as $\mathrm{d}_{\mathrm{rk}}(C) := \min\{\mathrm{rk}(z)\mid z\in C\backslash\{0\}\}$. An $[m\times n, k;\delta]_q$-code is a rank-metric code in $\mathbb{F}_q^{m\times n}$ or $\mathbb{F}_{q^m}^n$ of $\mathbb{F}_q$-dimension k and rank distance δ. The same terminology will be used for $\mathbb{F}$-subspaces of $\mathbb{F}^{m\times n}$ for an infinite field $\mathbb{F}$.

Note that in general a rank-metric code in $\mathbb{F}_{q^m}^n$ is only required to be $\mathbb{F}_q$-linear and not necessarily $\mathbb{F}_{q^m}$-linear.

A well-studied class of rank-metric codes are those attaining the maximum possible dimension for a given size $m\times n$ and rank distance δ. In the case where $n\leq m$, the *Singleton bound* (see Appendix A) tells us that the dimension k of an $[m\times n, k;\delta]_q$-code is at most $m(n-\delta+1)$, and codes attaining this bound are called *MRD codes* (maximum rank distance codes), denoted as $[m\times n;\delta]$-MRD codes. An MRD code in $\mathbb{F}_{q^m}^n$ may even be an $\mathbb{F}_{q^m}$-linear subspace, in which case we call it an $\mathbb{F}_{q^m}$-linear $[m\times n;\delta]$-MRD code.

We now turn to matrices supported by Ferrers diagrams. Throughout, for any $n\in\mathbb{N}$ let $[n]$ denote the set $\{1,\ldots,n\}$.

Definition 2.1.2. A $m\times n$-*Ferrers diagram* $\mathcal{F}$ is a subset of $[m]\times[n]$ with the following properties:

(i) if $(i,j)\in\mathcal{F}$ and $j<n$, then $(i,j+1)\in\mathcal{F}$ (right aligned),

(ii) if $(i,j)\in\mathcal{F}$ and $i>1$, then $(i-1,j)\in\mathcal{F}$ (top aligned).

For $j=1,\ldots,n$ let $c_j = |\{(i,j)\mid 1\leq i\leq m,\ (i,j)\in\mathcal{F}\}|$, i.e., c_j is the number of dots in the j-th column (see Figure 2.1). We may identify the Ferrers diagram $\mathcal{F}$ with the tuple $[c_1,\ldots,c_n]$. The tuple satisfies $c_1\leq c_2\leq\ldots\leq c_n$.

Note that we allow $c_1=0$ and $c_n<m$. Thus the size $m\times n$ of $\mathcal{F}$ is not fixed by the tuple $[c_1,\ldots,c_n]$. However, for each Ferrers diagram the natural choices of m and n are the number of nonempty rows and columns, respectively. Removing empty rows and columns leads to the case where $c_1>0$ and $c_n=m$. This is further discussed in the paragraph after Definition 2.1.11.

Example 2.1.3. The Ferrers diagram $\mathcal{F}=[c_1,\ldots,c_n]$ can be visualized as an array of top-aligned and right-aligned dots where the j-th column has c_j dots. Just like for matrices we index the rows from top to bottom and the columns from left to right. For instance, $\mathcal{F}=[1,2,4,4,5]$ is given by
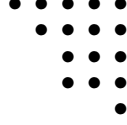
Figure 2.1: $\mathcal{F} = [1, 2, 4, 4, 5]$

For the rest of this section, let $\mathbb{F}$ denote an arbitrary, possible infinite field (unless specified otherwise).

Definition 2.1.4. (a) The support of a matrix $M = (m_{ij}) \in \mathbb{F}^{m \times n}$ is defined as the set $\operatorname{supp}(M) := \{(i, j) \mid m_{ij} \neq 0\}$. For a given $m \times n$-Ferrers diagram $\mathcal{F}$ we say that M has *shape* $\mathcal{F}$ if $\operatorname{supp}(M) \subseteq \mathcal{F}$. The subspace of $\mathbb{F}^{m \times n}$ of all matrices with shape $\mathcal{F}$ is denoted by $\mathbb{F}[\mathcal{F}]$.

(b) Let $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$ be a rank-metric code and let $\mathcal{F}$ be an $m \times n$-Ferrers diagram. If $\mathcal{C} \subseteq \mathbb{F}[\mathcal{F}]$, that is, every matrix in $\mathcal{C}$ has shape $\mathcal{F}$, then $\mathcal{C}$ is called a *Ferrers diagram code* of shape $\mathcal{F}$. An $[m \times n, k; \delta]$-code in $\mathbb{F}[\mathcal{F}]$ is called an $[\mathcal{F}, k; \delta]$-code, or an $[\mathcal{F}; \delta]$-code if the dimension is not specified. If $\mathbb{F} = \mathbb{F}_q$, we also use the notation $[\mathcal{F}, k; \delta]_q$-code and $[\mathcal{F}; \delta]_q$-code.

For the Ferrers diagram $\mathcal{F} = [m, \ldots, m]$ an $[\mathcal{F}, k; \delta]_q$-code is thus an $[m \times n, k; \delta]_q$-code. Note that it does not make sense to talk about $[\mathcal{F}, k; \delta]_q$-codes in $\mathbb{F}_{q^m}^n$ because the shape of the corresponding matrices in $\mathbb{F}_q^{m \times n}$ depends on the chosen basis B for the isomorphism in (2.1). We will make use of this fact later in Section 2.2.

Remark 2.1.5. Let us briefly relate Ferrers diagram codes to subspaces codes. All $m \times n$-matrices with the same Ferrers diagram shape $\mathcal{F}$ can be extended to $m \times (m+n)$-matrices in reduced row echelon form (RREF) with the same pivot indices by inserting standard basis vectors. For instance, matrices with shape $\mathcal{F}$ as in Figure 2.1 lead to RREF's of the form

$$\begin{pmatrix} 1 & \bullet & 0 & \bullet & 0 & 0 & \bullet & \bullet & 0 & \bullet \\ 0 & 0 & 1 & \bullet & 0 & 0 & \bullet & \bullet & 0 & \bullet \\ 0 & 0 & 0 & 0 & 1 & 0 & \bullet & \bullet & 0 & \bullet \\ 0 & 0 & 0 & 0 & 0 & 1 & \bullet & \bullet & 0 & \bullet \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \bullet \end{pmatrix}.$$

Precisely, let $\mathcal{F} = [c_1, \ldots, c_n]$ and set $t_i = |\{j \mid c_j \leq i\}|$ for $i = 1, \ldots, m-1$ and $t_0 = 0$. Then the pivot indices of the resulting $m \times (m+n)$-matrix in RREF are at positions $t_0 + 1, t_1 + 2, t_2 + 3, \ldots, t_{m-1} + m$. In this way Ferrers diagram codes give rise to subspace codes via the row spaces of the resulting matrices in RREF. The multilevel construction by Etzion/Silberstein [14] tells us how to combine various Ferrers shapes to ensure the quality of the subspace code. Not surprisingly, the rank distance of the Ferrers diagram codes plays a crucial role.

The above discussion leads to the question as to what the maximum possible dimension k of an $[\mathcal{F}, k; \delta]$-code is. In [14] Etzion/Silberstein present an upper bound on the dimension via a simple counting argument. We need the following notation.

Definition 2.1.6. Let $\mathcal{F} = [c_1, \ldots, c_n]$ be an $m \times n$-Ferrers diagram and let $\delta \in \mathbb{N}$. For $j = 0, \ldots, \delta - 1$ define

$$\nu_j := \nu_j(\mathcal{F}; \delta) = \left\{ \begin{array}{c} \text{number of dots in } \mathcal{F} \text{ after removing the} \\ \text{top } j \text{ rows and rightmost } \delta - 1 - j \text{ columns} \end{array} \right\}$$

$$= \sum_{t=1}^{n-\delta+1+j} \max\{c_t - j, 0\}.$$

Furthermore, set $\nu_{\min} := \nu_{\min}(\mathcal{F}; \delta) = \min\{\nu_0, \ldots, \nu_{\delta-1}\}$.

Note that $\nu_{\min} = 0$ whenever $\delta > \min\{m, n\}$. Moreover, $\nu_{\min} = 0 \iff c_{n-\delta+1+j} \leq j$ for some $j \in \{0, \ldots, \delta - 1\}$. A simple Linear Algebra argument establishes the following upper bound on $[\mathcal{F}; \delta]_q$-codes.

Theorem 2.1.7 ([14, Thm. 1]). *Let $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$ be an $[\mathcal{F}; \delta]$-code. Then*

$$\dim(\mathcal{C}) \leq \nu_{min}(\mathcal{F}; \delta).$$

Proof. Contrarily assume that there exists an $[\mathcal{F}, \nu_i + 1, \delta]$ code $\mathcal{C}$ for some $i \in \{0, \ldots, \delta - 1\}$. Let $B = \{B_1, \ldots, B_{\nu_i+1}\}$ be linearly independent in $\mathcal{C}$. Let A_i be the set obtained from $\mathcal{F}$ by deleting the topmost i rows and the rightmost $\delta - i - 1$ columns, hence $|A_i| = \nu_i$. Since $|B| = \nu_i + 1$, there exists a nontrivial linear combination $Y = \sum_{j=1}^{\nu_i+1} \alpha_j B_j$ in which the ν_i entries of A_i are all zeros. We know $Y \neq 0$ because B is linearly independent. The top i rows of Y contribute at most rank i, and the right $\delta - 1 - i$ columns contribute at most rank $\delta - 1 - i$. So we have $\mathrm{rk}(Y) \leq \delta - 1$, a contradiction to $\mathcal{C}$ having minimum rank-distance δ. $\square$

This gives rise to the following definition.

Definition 2.1.8. An $[\mathcal{F}; \delta]$-code $\mathcal{C} \subseteq \mathbb{F}^{m \times n}$ is called *maximal* if $\dim(\mathcal{C}) = \nu_{\min}(\mathcal{F}; \delta)$.

In the same paper [14], Etzion/Silberstein formulate the following conjecture for Ferrers diagram codes over finite fields.

Conjecture 2.1.9. *For every $m \times n$-Ferrers diagram $\mathcal{F}$, every $1 \leq \delta \leq \min\{m, n\}$ and every finite field $\mathbb{F}_q$ there exists a maximal $[\mathcal{F}; \delta]_q$-code.*

The conjecture is certainly true for any $\mathcal{F}$ and $\delta = 1$: set $\mathcal{C} = \{E_{ij} \mid (i, j) \in \mathcal{F}\}$, where $E_{ij} \in \mathbb{F}_q^{m \times n}$ denotes the standard basis matrix with a one in position (i, j) and zeros elsewhere (this is even true for arbitrary fields). Conjecture 2.1.9 has been proven for several cases of $(\mathcal{F}; \delta)$ but may still be considered as widely open. We will revisit some of the established cases later in the paper and settle the conjecture for further cases. For algebraically closed fields the conjecture is not true in general. In Section 2.5 we will discuss this more closely and relate the existence of a maximal $[\mathcal{F}; \delta]$-code over $\overline{\mathbb{F}_q}$ with genericity over large finite fields.

Let us return to Conjecture 2.1.9 for finite fields. The simplest case for $\delta \geq 2$ is the case where $\mathcal{F} = [m, \ldots, m]$, that is, $\mathcal{F}$ is the full rectangle and does not put any

restrictions on the matrices. If without loss of generality $n \leq m$, then $\nu_{\min}(\mathcal{F}; \delta) = m(n - \delta + 1)$, recovering the Singleton bound. In other words, a maximal $[\mathcal{F}; \delta]$-code is an $[m \times n; \delta]$-MRD code. The existence of such codes has been established by Delsarte [12] and later recovered by Gabidulin [15]. We recall Gabidulin's construction here, but the two are essentially the same.

Theorem 2.1.10 ([12, Thm. 5.4 and 6.3], [15, Thm. 6/7]). *Let $m \geq n$, $\delta \in [n]$, and let $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$. Set $\ell = n - \delta + 1$ and*

$$
M := M(g_1, \ldots, g_n; \ell) = \begin{pmatrix} g_1 & \cdots & g_n \\ g_1^q & \cdots & g_n^q \\ \vdots & & \vdots \\ g_1^{q^{\ell-1}} & \cdots & g_n^{q^{\ell-1}} \end{pmatrix} \in \mathbb{F}_{q^m}^{\ell \times n}.
$$

Then the row space $\mathrm{rowsp}(M) := \{uM \mid u \in \mathbb{F}_{q^m}^\ell\} \subseteq \mathbb{F}_{q^m}^n$ is called a Gabidulin *code. It is an $\mathbb{F}_{q^m}$-linear $[m \times n; \delta]_q$-MRD code.*

Note that $\mathcal{C}$ has dimension ℓ over $\mathbb{F}_{q^m}$ (since M has full row rank), and thus its $\mathbb{F}_q$-dimension is $m\ell = m(n - \delta + 1)$, as desired. One may check Appendix A for a more detailed proof.

The remainder of this section is devoted to a few simple facts that turn out to be quite useful. The simple properties given below in Remarks 2.1.12 and 2.1.14 have already been used in the literature (for instance in the proof of [13, Thm. 7]), but it seems nonetheless beneficial to formally introduce the according notions. The terminology in Definition 2.1.11(b) below will be particularly convenient. It is a generalization of [45] where the same notion is used for a more specific case. The relevance of pending dots is, of course, that if Conjecture 2.1.9 is true, then these dots are not necessary for the existence of maximal $[\mathcal{F}; \delta]_q$-codes.

Definition 2.1.11. (a) Let $\mathcal{F}_i$ be $m_i \times n$-Ferrers diagrams with the same number of columns. $\mathcal{F}_1 \subseteq \mathcal{F}_2$ simply means set-theoretic inclusion, thus $(i, j) \in \mathcal{F}_1$ implies $(i, j) \in \mathcal{F}_2$.

(b) Let $\delta \in [n]$ and $\mathcal{F}_2$ be an $m_2 \times n$-Ferrers diagram. If there exists an $m_1 \times n$-Ferrers diagram $\mathcal{F}_1 \subsetneq \mathcal{F}_2$ such that $\nu_{\min}(\mathcal{F}_1; \delta) = \nu_{\min}(\mathcal{F}_2; \delta)$, then the dots in $\mathcal{F}_2 \setminus \mathcal{F}_1$ are called *pending dots of $\mathcal{F}_2$* with respect to δ.

Note that comparing two Ferrers diagrams as sets only makes sense in the context where both have the same number of columns. The diagrams $[1, 2, 3, 4]$ and $[0, 1, 2, 3, 4]$ are certainly the same, but as sets of points they look very different. Recall that Definition 2.1.2 includes $m \times n$-Ferrers diagrams $\mathcal{F} = [c_1, \ldots, c_n]$ with $c_1 = 0$ and $c_n < m$. This allows us to pad a diagram with empty rows and columns to make it a desired size for the purpose of comparison. In the same way we may delete empty rows or columns in order to obtain a Ferrers diagram where the first column and last row are non-empty.

Remark 2.1.12. Let $\mathcal{F}_1 \subseteq \mathcal{F}_2$ be $m_i \times n$-Ferrers diagrams such that $\nu_{\min}(\mathcal{F}_1; \delta) = \nu_{\min}(\mathcal{F}_2; \delta)$. Then the existence of a maximal $[\mathcal{F}_1; \delta]$-code implies the existence of a maximal $[\mathcal{F}_2; \delta]$-code over the same field. This is clear because each matrix with shape $\mathcal{F}_1$ also has shape $\mathcal{F}_2$.

Example 2.1.13. (a) Consider the Ferrers diagram $\mathcal{F} = [1, 2, 4, 4, 5]$ shown in Figure 2.1. Then $\mathcal{F}$ does not have any pending dots with respect to $\delta = 2$ or $\delta = 3$, but the dot at position $(4, 3)$ is pending with respect to $\delta = 4$.

  (b) For $\mathcal{F} = [1, 3, 3, 4, 5]$ and $\delta = 4$ the dots at positions $(1, 1)$ and $(2, 3)$ are both pending as individual dots, that is, removing either one of them does not decrease $\nu_{\min}(\mathcal{F}; \delta) = 4$. However, removing both of them will decrease it to 3.

  (c) In [13, Ex. 5] the authors present a construction for a maximal $[\mathcal{F}; 3]_q$-code where $\mathcal{F} = [2, 4, 4, 6, 8]$ for fields $\mathbb{F}_q$ with $q \geq 4$. However, the bottom 4 dots are pending and removing them leads to the Ferrers diagram $\mathcal{F}' = [2, 4, 4, 5, 5]$, for which the authors present a construction of maximal $[\mathcal{F}'; 3]_q$-codes for arbitrary fields in [13, Thm. 2]. Thus, not only does the latter construction work for all finite fields, it also does not need the positions of the pending dots. We will revisit [13, Thm. 2] in Theorem 2.2.1.

Remark 2.1.14. Let $\delta \in [n]$ and $\mathcal{F}'$, $\mathcal{F}$ be $m \times n$-Ferrers diagrams such that $\mathcal{F}' \subsetneq \mathcal{F}$ and $|\mathcal{F} \setminus \mathcal{F}'| = 1$ (that is, $\mathcal{F}'$ is obtained from $\mathcal{F}$ by removing one dot). Suppose $\nu_{\min}(\mathcal{F}'; \delta) = \nu_{\min}(\mathcal{F}; \delta) - 1$. Then the existence of a maximal $[\mathcal{F}; \delta]$-code over the field $\mathbb{F}$ implies the existence of a maximal $[\mathcal{F}'; \delta]$-code over $\mathbb{F}$. Indeed, let $\mathcal{C}$ be an $[\mathcal{F}, k; \delta]$-code, where $k = \nu_{\min}(\mathcal{F}; \delta)$. Let $\{(i, j)\} = \mathcal{F} \setminus \mathcal{F}'$. We can clearly choose a basis $\{A_1, \ldots, A_k\}$ of $\mathcal{C}$ such that $(A_s)_{i,j} = 0$ for all $1 \leq s \leq k - 1$. Then $\{A_1, \ldots, A_{k-1}\}$ is a basis of a maximal $[\mathcal{F}'; \delta]$-code.

This reduction technique is certainly not a new result, and is fairly obvious. Nevertheless, we include the following simple example to illustrate its power.

Example 2.1.15. Let $\delta = 3$. Figure 2.2 shows all 4×4-Ferrers diagrams for which Conjecture 2.1.9 can be confirmed via reduction described in Remark 2.1.14 starting with a $[4 \times 4; 3]$-MRD code. The number in the bottom right corner is $\nu_{\min}(\mathcal{F}; 3)$ for the given Ferrers diagram $\mathcal{F}$. Later in this paper we will establish Conjecture 2.1.9 for $n \times n$-upper triangular matrices with $\delta = 3$ (see Corollary 2.2.10). Figure 2.3 shows all 4×4-Ferrers diagrams for which Conjecture 2.1.9 can be confirmed via reduction as in Remark 2.1.14 starting from the upper triangular shape.

The only 4×4-Ferrers diagram with positive $\nu_{\min}$ not appearing in these charts is $\mathcal{F} = [1, 3, 3, 4]$. This case has been dealt with by Etzion et al. [13, Ex. 7] by making use of a suitable extension of a Gabidulin code. We present a simple alternative construction.
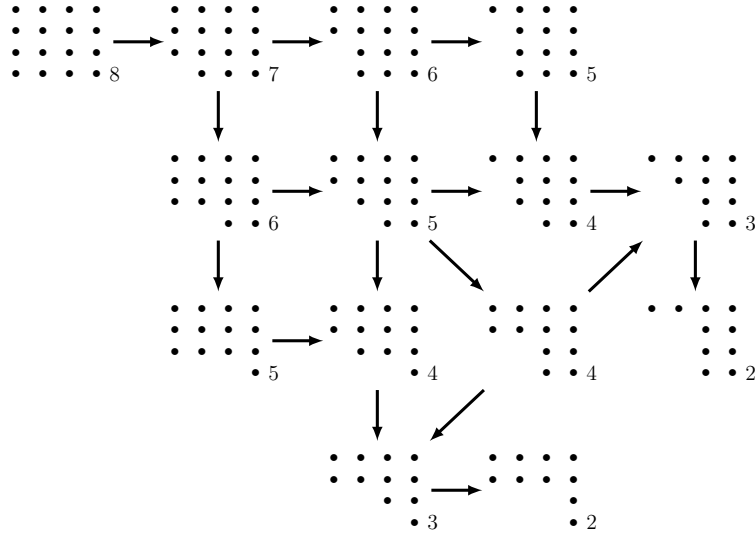
Figure 2.2: Reduction for 4×4-diagrams with $\delta = 3$ starting from $\mathcal{F} = [4, 4, 4, 4]$.
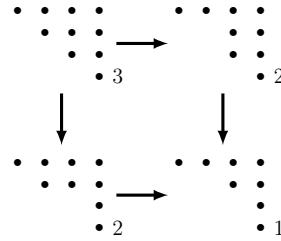
Figure 2.3: Reduction for 4×4-diagrams with $\delta = 3$ starting from $\mathcal{F} = [1, 2, 3, 4]$.

Example 2.1.16. Let $\delta = 3$ and consider the 4×4-Ferrers diagram $\mathcal{F} = [1, 3, 3, 4]$ shown in Figure 2.4. Then $\nu_{\min} = 4$. In order to construct a maximal $[\mathcal{F}; 3]_q$-code over any finite field $\mathbb{F} = \mathbb{F}_q$, we start with a $[3 \times 3; 3]$-MRD code, hence its dimension is 3.
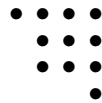
Figure 2.4: $\mathcal{F} = [1, 3, 3, 4]$

We may choose a basis B_1, B_2, B_3 of this code in the form

$$
B_1 = \begin{pmatrix} 1 & a_{12}^{(1)} & a_{13}^{(1)} \\ 0 & a_{22}^{(1)} & a_{23}^{(1)} \\ 0 & a_{32}^{(1)} & a_{33}^{(1)} \end{pmatrix}, \quad
B_2 = \begin{pmatrix} 0 & a_{12}^{(2)} & a_{13}^{(2)} \\ 1 & a_{22}^{(2)} & a_{23}^{(2)} \\ 0 & a_{32}^{(2)} & a_{33}^{(2)} \end{pmatrix}, \quad
B_3 = \begin{pmatrix} 0 & a_{12}^{(3)} & a_{13}^{(3)} \\ 0 & a_{22}^{(3)} & a_{23}^{(3)} \\ 1 & a_{32}^{(3)} & a_{33}^{(3)} \end{pmatrix}
$$

(see also Example 2.1.17(a) below). Hence the general linear combination is

$$B(\lambda) := \lambda_1 B_1 + \lambda_2 B_2 + \lambda_3 B_3 = \begin{pmatrix} \lambda_1 & p_{12} & p_{13} \\ \lambda_2 & p_{22} & p_{23} \\ \lambda_3 & p_{32} & p_{33} \end{pmatrix}, \text{ where } p_{ij} = \sum_{\ell=1}^{3} a_{ij}^{(\ell)} \lambda_\ell.$$

Rank distance 3 guarantees that $(a_{22}^{(1)}, a_{32}^{(1)}) \neq (0,0)$. We assume without loss of generality that $a_{22}^{(1)} \neq 0$. Define now $A_1, \ldots, A_4 \in \mathbb{F}^{4 \times 4}$ such that their general linear combination has the form

$$A(\lambda) = \sum_{\ell=1}^{4} \lambda_\ell A_\ell = \begin{pmatrix} \lambda_4 & \lambda_1 & p_{12} & p_{13} \\ 0 & \lambda_2 & p_{22} & p_{23} \\ 0 & \lambda_3 & p_{32} + \lambda_4 & p_{33} \\ 0 & 0 & 0 & \lambda_4 \end{pmatrix}.$$

It remains to show that $\mathrm{rk}(A(\lambda)) \geq 3$ for all $\lambda = (\lambda_1, \ldots, \lambda_4) \neq 0$. This is clear if $\lambda_4 = 0$. Thus let $\lambda_4 \neq 0$. In this case

$$\mathrm{rk} A(\lambda) \geq 3 \iff \mathrm{rk} \begin{pmatrix} \lambda_2 & p_{22} \\ \lambda_3 & p_{32} + \lambda_4 \end{pmatrix} \geq 1.$$

The right hand side is clearly true if $(\lambda_2, \lambda_3) \neq (0,0)$. In the case where $(\lambda_2, \lambda_3) = (0,0)$, the matrix on the right hand side has second column $(a_{22}^{(1)} \lambda_1, a_{32}^{(1)} \lambda_1 + \lambda_4)^\mathsf{T}$, and the assumption $a_{22}^{(1)} \neq 0$ along with $(\lambda_1, \lambda_4) \neq (0,0)$ guarantees that this vector is nonzero. All of this establishes the existence of optimal $[\mathcal{F}; 3]_q$-codes over any field $\mathbb{F}_q$. We will return to this particular Ferrers diagram $\mathcal{F}$ in Example 2.3.3 and Corollary 2.6.9/Example 2.6.10. In the former we will show that a maximal $[\mathcal{F}; 3]_q$-code cannot be found as an $\mathbb{F}_q$-linear subspace of an $\mathbb{F}_{q^4}$-linear $[4 \times 4; 3]$-MRD code. In the latter we will discuss the probability that a random choice of 4 matrices with shape $\mathcal{F}$ generate a maximal $[\mathcal{F}; 3]_q$-code.

We close the section with a well-known example utilizing companion matrices. Part (b) and (c) below are simple instances of the aforementioned reduction methods.

Example 2.1.17. (a) Consider the case $m = n = \delta$, thus $\ell = 1$. Let $B = (1, \alpha, \ldots, \alpha^{m-1})$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and consider the matrix $M = (1, \alpha, \ldots, \alpha^{m-1}) \in \mathbb{F}_{q^m}^{1 \times m}$. Let $f = \sum_{i=0}^{m} f_i x^i \in \mathbb{F}_q[x]$ be the monic minimal polynomial of α over $\mathbb{F}_q$ (thus $f_m = 1$). Then the matrix code $\phi_B(\mathrm{rowsp}(M)) \subseteq \mathbb{F}_q^{m \times m}$ is the m-dimensional code given by

$$\phi_B(\mathrm{rowsp}(M)) = \langle I, C, \ldots, C^{m-1} \rangle, \text{ where } C = \begin{pmatrix} 0 & 0 & \cdots & 0 & -f_0 \\ 1 & 0 & \cdots & 0 & -f_1 \\ 0 & 1 & \cdots & 0 & -f_2 \\ & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -f_{m-1} \end{pmatrix},$$

that is, C is the companion matrix of f. For any $i \in [m]$ the code $\mathcal{C} = \langle I, C, \ldots, C^{i-1} \rangle$ is a maximal $[\mathcal{F}; m]_q$-code for the $m \times m$-Ferrers diagram $\mathcal{F} = [i, i+1, \ldots, m, \ldots, m]$ (thus $c_t = \min\{i-1+t, m\}$ and the last i columns have m dots).

(b) The previous code can be used to cover further Ferrers diagrams. Choose $t \leq i - 1$ and delete the t rightmost columns of all matrices in $\mathcal{C}$. This yields an $m \times n$-Ferrers diagram code $\tilde{\mathcal{C}}$ with shape $\tilde{\mathcal{F}} = [i, i+1, \ldots, m, \ldots, m]$, where $n = m-t$ (and the rightmost $i-t$ columns have m dots). The code $\tilde{\mathcal{C}}$ clearly has dimension i and thus is a maximal $[\tilde{\mathcal{F}}; n]_q$-code because $\nu_{\min}(\tilde{\mathcal{F}}; n) \leq \nu_0(\tilde{\mathcal{F}}; n) = i$.

(c) We can go even further. Consider an $m \times n$-Ferrers diagram $\mathcal{F} = [c_1, \ldots, c_n]$ where $c_j \geq c_1 + j - 1$ for $j = 2, \ldots, n$ (hence $c_1 \leq m - n + 1$). Then $\nu_{\min}(\mathcal{F}; n) = c_1$ and this remains true even after removing the dots at positions (i, j) with $i > c_1 + j - 1$, i.e., these dots are pending. Removing them leads to the Ferrers diagram $\tilde{\mathcal{F}}$ as in (b) with $i = c_1$. Hence there exists a maximal $[\mathcal{F}; n]_q$-code.

2.2 Maximal Ferrers Diagram Codes as Subspaces of MRD Codes

In this section we present a class of pairs $(\mathcal{F}; \delta)$ for which maximal $[\mathcal{F}; \delta]_q$-codes can be found as $\mathbb{F}_q$-subspaces of some (in fact any) $\mathbb{F}_{q^m}$-linear MRD code with the same rank distance.

We start with two well-known results (Theorem 2.2.1 and Corollary 2.2.3) and their proofs, which will help to generalize them. For the rest of the paper we fix $n \leq m$, and throughout this section we assume $2 \leq \delta \leq n$ (as the existence of maximal $[\mathcal{F}; 1]$-codes is trivial).

Recall the isomorphism $\phi_B : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^{m \times n}$ from (2.1) based on a chosen ordered basis B of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. For the following result note that every $\mathbb{F}_{q^m}$-linear MRD code in $\mathbb{F}_{q^m}^n$ has a systematic generator matrix. This is a consequence of [15, Thm. 2].

Theorem 2.2.1 ([14, Thm. 2], [16, Sec. 2.5], [22, Cor. 19]). *Let $\mathcal{F} = [c_1, \ldots, c_n]$ be an $m \times n$-Ferrers diagram such that $c_j = m$ for all $j = n - \delta + 2, \ldots, n$ (that is, the last $\delta - 1$ columns of $\mathcal{F}$ have the maximum number of m dots). Set $\ell = n - \delta + 1$ and let $G = (I_\ell \mid A) \in \mathbb{F}_{q^m}^{\ell \times n}$ be a generator matrix of an $\mathbb{F}_{q^m}$-linear $[m \times n; \delta]$-MRD code (for instance, a Gabidulin code). Let $B = (x_1, \ldots, x_m)$ be an ordered basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Then the subspace*

$$\mathcal{C} = \left\{ \phi_B\big((u_1, \ldots, u_\ell)G\big) \mid u_t \in \langle x_1, \ldots, x_{c_t} \rangle \text{ for } t = 1, \ldots, \ell \right\} \subseteq \mathbb{F}_q^{m \times n}$$

is a maximal $[\mathcal{F}; \delta]_q$-code. Furthermore, $\nu_{\min}(\mathcal{F}; \delta) = \nu_0 = \sum_{t=1}^{\ell} c_t$.

Proof. Note that $\mathcal{C}$ is clearly an $\mathbb{F}_q$-vector space. Next, let $(u_1, \ldots, u_\ell) \in \mathbb{F}_{q^m}^\ell$ be such that $u_t \in V_t := \langle x_1, \ldots, x_{c_t} \rangle$. Set $(u_1, \ldots, u_\ell)A = (v_1, \ldots, v_{n-\ell})$. Then

$$\phi_B\big((u_1, \ldots, u_\ell)G\big) = \big([u_1]_B, \ldots, [u_\ell]_B, [v_1]_B, \ldots, [v_{n-\ell}]_B\big) =: M.$$

28

By choice of u_t, it follows that the matrix M has indeed shape $\mathcal{F}$. Here it is crucial that the last $\delta - 1$ columns of $\mathcal{F}$ are full and therefore do not impose any restrictions on the coordinate vectors of $v_1, \ldots, v_{n-\ell}$. Clearly, $d_{rk}(\mathcal{C}) =: \delta' \geq \delta$ because $\mathcal{C}$ is a subspace of an MRD code of distance δ. Finally, $\dim_{\mathbb{F}_q}(\mathcal{C}) = \sum_{t=1}^{\ell} \dim V_t = \sum_{t=1}^{\ell} c_t = \nu_0(\mathcal{F}; \delta) \geq \nu_0(\mathcal{F}; \delta') \geq \nu_{\min}(\mathcal{F}; \delta')$, where the first inequality is strict iff $\delta' > \delta$. Now the upper bound in Theorem 2.1.7 implies $\delta' = \delta$ and $\dim_{\mathbb{F}_q}(\mathcal{C}) = \nu_0(\mathcal{F}; \delta) = \nu_{\min}(\mathcal{F}; \delta)$. □

One may note that, once $\nu_{\min}(\mathcal{F}; \delta) = \nu_0 = \sum_{t=1}^{\ell} c_t$ is established, the result above also follows from the reduction process described in Remark 2.1.14. Indeed, for $\hat{\mathcal{F}} = [m] \times [n]$ we have $\nu_{\min}(\hat{\mathcal{F}}; \delta) = m(n - \delta + 1)$ and, since $c_t = m$ for $t > \ell$, we conclude $\nu_{\min}(\mathcal{F}; \delta) = \nu_{\min}(\hat{\mathcal{F}}; \delta) - |\hat{\mathcal{F}} \setminus \mathcal{F}|$. This has already been observed in [14, Rem. 6] and [22, Cor. 19].

Since we may always reduce to the case where $c_n = m$ by removing empty rows, the next result follows immediately.

Corollary 2.2.2. *Let $\delta = 2$. Then Conjecture 2.1.9 holds true for all Ferrers diagrams $\mathcal{F}$ and fields $\mathbb{F}_q$.*

The next result bears similarity to Theorem 2.2.1, but arrives at the same conclusion with a weaker assumption thanks to the consideration of pending dots.

Corollary 2.2.3 ([13, Thm. 3] and [22, Thm. 23]). *Let $\mathcal{F} = [c_1, \ldots, c_n]$ be an $m \times n$-Ferrers diagram such that $c_j \geq n$ for all $j = n - \delta + 2, \ldots, n$ (that is, the last $\delta - 1$ columns have at least n dots). Then there exists a maximal $[\mathcal{F}; \delta]_q$-code. More precisely, all dots at positions (i, j) with $i > \hat{m} = \max\{c_{n-\delta+1}, n\}$ are pending, and there exists a maximal $[\hat{\mathcal{F}}; \delta]_q$-code where $\hat{\mathcal{F}} = [\hat{c}_1, \ldots, \hat{c}_n]$ with $\hat{c}_t = \min\{c_t, \hat{m}\}$.*

Proof. Set $\ell = n - \delta + 1$. We show first that $\nu_{\min}(\mathcal{F}; \delta) = \nu_0 = \sum_{t=1}^{\ell} c_t$. Using Definition 2.1.6 we compute for any $j = 1, \ldots, \delta - 1$

$$\nu_j = \sum_{t=1}^{\ell+j} \max\{c_t - j, 0\} \geq \sum_{t=1}^{\ell} (c_t - j) + \sum_{t=\ell+1}^{\ell+j} (n - j) \geq \nu_0 + j(n - j - \ell) \geq \nu_0.$$

Let now $\hat{m} = \max\{c_\ell, n\}$ and consider the $\hat{m} \times n$-Ferrers diagram $\hat{\mathcal{F}} = [\hat{c}_1, \ldots, \hat{c}_n]$, where

$$\hat{c}_t = \min\{c_t, \hat{m}\} = \begin{cases} c_t, & \text{for } t = 1, \ldots, \ell, \\ \hat{m}, & \text{for } t = \ell + 1, \ldots, n. \end{cases}$$

Then the Ferrers diagram $\hat{\mathcal{F}}$ satisfies the assumptions of Theorem 2.2.1. Thus there exists a maximal $[\hat{\mathcal{F}}; \delta]_q$-code and its dimension is given by $\nu_{\min}(\hat{\mathcal{F}}; \delta) = \sum_{t=1}^{\ell} \hat{c}_t = \sum_{t=1}^{\ell} c_t = \nu_{\min}(\mathcal{F}; \delta)$. Since $\hat{\mathcal{F}} \subseteq \mathcal{F}$ Remark 2.1.12 concludes the proof. □

In [13, Thm. 8], Etzion et al. take the above idea further, tackling the case where the rightmost $\delta - 1$ columns contain at least $n - 1$ dots, assuming other criteria were also met. More recently Liu et al. [35, Thm. 3.13] generalize the argument to handle $n - r$ dots, again requiring further restrictions on the shape. In particular, the first r columns combined may have no more than $m - n + r$ dots.

In Theorem 2.2.1 we could choose any ordered basis B to obtain the desired maximal $[\mathcal{F}; \delta]_q$-code as a subfield subcode. In Theorem 2.2.6 below we will prove a generalization of Theorem 2.2.1 for which we will have to make a judicious choice of basis. The construction and assumptions differ from [35, Thm. 3.13]. We first need the following lemmas.

Lemma 2.2.4. *Let V be an m-dimensional vector space and $V_1, \ldots, V_t$ be subspaces of V with $\dim V_j \geq d_j$. Then $\dim \left(\bigcap_{j=1}^{t} V_j \right) \geq \sum_{j=1}^{t} d_j - (t-1)m$.*

Proof. We induct on the number of subspaces. Clearly the statement holds for $t = 1$. Assume the statement holds for $t - 1$ subspaces. Then

$$\dim \left(\bigcap_{j=1}^{t} V_j \right) = \dim \left(V_t \cap \bigcap_{j=1}^{t-1} V_j \right) = \dim V_t + \dim \left(\bigcap_{j=1}^{t-1} V_j \right) - \underbrace{\dim \left(V_t + \bigcap_{j=1}^{t-1} V_j \right)}_{\leq m}$$

$$\geq d_t + \sum_{j=1}^{t-1} d_j - (t-2)m - m = \sum_{j=1}^{t} d_j - (t-1)m. \qquad \square$$

Lemma 2.2.5. *Let $G = (I_\ell \mid A) \in \mathbb{F}_{q^m}^{\ell \times n}$ be the generator matrix of an $\mathbb{F}_{q^m}$-linear MRD code (thus, its rank distance is $n - \ell + 1$). Let $A = (a_{ij})$. Then $rk(1, a_{1j}, \ldots, a_{\ell j}) = \ell + 1$ for all $j = 1, \ldots, n - \ell$, i.e., the entries of this vector are linearly independent over $\mathbb{F}_q$. In particular, $a_{ij} \notin \mathbb{F}_q$ for all (i, j).*

Proof. Consider without loss of generality $j = 1$. Let $\lambda_0 + \sum_{i=1}^{\ell} \lambda_i a_{i1} = 0$ for some $\lambda_i \in \mathbb{F}_q$. Then $(\lambda_1, \ldots, \lambda_\ell)G = (\lambda_1, \ldots, \lambda_\ell, -\lambda_0, b_1, \ldots, b_{n-\ell-1})$ for some $b_i \in \mathbb{F}_{q^m}$. Since all λ_i are in $\mathbb{F}_q$, this vector has rank at most $n - \ell$, whereas the code has distance $n - \ell + 1$. Thus the vector is zero and hence $\lambda_i = 0$ for all i, as desired. $\square$

Now we are ready to establish the following result.

Theorem 2.2.6. *Let $\mathcal{F} = [c_1, \ldots, c_n]$ be an $m \times n$-Ferrers diagram. Let $2 \leq \delta \leq n$ and $\ell = n - \delta + 1$. Set $\varepsilon = \sum_{t=\ell+1}^{n} (m - c_t)$, that is, ε is the number of dots missing in the rightmost $\delta - 1$ columns of $\mathcal{F}$. Suppose*

$$c_t \leq c_{\ell+1} - \varepsilon(\ell + 1 - t) \text{ for } t = 1, \ldots, \ell. \tag{2.2}$$

Let $G = (I_\ell \mid A) \in \mathbb{F}_{q^m}^{\ell \times n}$ be the generator matrix of an $\mathbb{F}_{q^m}$-linear $[m \times n; \delta]$-MRD code. Then there exists an ordered basis $B = (x_1, \ldots, x_m)$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ such that the subspace

$$\mathcal{C} = \left\{ \phi_B \big((u_1, \ldots, u_\ell)G \big) \mid u_t \in \langle x_1, \ldots, x_{c_t} \rangle \text{ for } t = 1, \ldots, \ell \right\} \tag{2.3}$$

is a maximal $[\mathcal{F}; \delta]_q$-code. In this case $\nu_{min}(\mathcal{F}; \delta) = \nu_0 = \sum_{t=1}^{\ell} c_t$.

Theorem 2.2.1 is the special case where $\varepsilon = 0$. In this case the inequalities (2.2) are vacuous.

Proof. For any $u = (u_1, \ldots, u_\ell) \in \mathbb{F}_{q^m}^\ell$ we have

$$uG = (u_1, \ldots, u_\ell, v_1, \ldots, v_{n-\ell}), \quad \text{where } (v_1, \ldots, v_{n-\ell}) = uA. \tag{2.4}$$

As in the proof of Theorem 2.2.1, for any fixed basis B, we may choose $u_1, \ldots, u_\ell$ such that the first ℓ columns of the matrix $\phi_B(uG)$ adhere to the desired shape $\mathcal{F}$. However, now we also have to accommodate the last $n - \ell$ columns. We show that for a specific choice of basis B this can indeed be achieved.

Let $A = (a_{ij})_{i\in[\ell]}^{j\in[n-\ell]}$. Then $a_{ij} \notin \mathbb{F}_q$ for all i, j thanks to Lemma 2.2.5. In particular, $a_{ij} \neq 0$. Consider any chain of subspaces

$$V_1 \subsetneq V_2 \subsetneq \ldots \subsetneq V_m = \mathbb{F}_{q^m},$$

such that $\dim V_i = i$. For $t \in [\ell]$ set $W_t = \bigcap_{j=1}^{n-\ell} V_{c_{\ell+j}} a_{tj}^{-1}$. Since $\dim(V_{c_{\ell+j}} a_{tj}^{-1}) = c_{\ell+j}$, Lemma 2.2.4 implies that

$$\dim(W_t) \geq \sum_{j=1}^{n-\ell} c_{\ell+j} - (n - \ell - 1)m = m - \varepsilon \quad \text{for all } t \in [\ell].$$

Consider the chain of subspaces

$$V_{c_{\ell+1}} \cap \bigcap_{j=1}^\ell W_j \subseteq V_{c_{\ell+1}} \cap \bigcap_{j=2}^\ell W_j \subseteq \ldots \subseteq V_{c_{\ell+1}} \cap W_\ell \subseteq V_{c_{\ell+1}} \subseteq \mathbb{F}_{q^m}.$$

By Lemma 2.2.4 and (2.2) we have for $t \in [\ell]$

$$\dim\left(V_{c_{\ell+1}} \cap \bigcap_{j=t}^\ell W_j\right) \geq c_{\ell+1} + \sum_{j=t}^\ell \dim(W_j) - (\ell - t + 1)m$$

$$\geq c_{\ell+1} + (\ell - t + 1)(m - \varepsilon) - (\ell - t + 1)m$$

$$= c_{\ell+1} - (\ell - t + 1)\varepsilon$$

$$\geq c_t.$$

This allows us to choose an ordered basis $B = (x_1, \ldots, x_m)$ of $\mathbb{F}_{q^m}$ such that

$$x_1, \ldots, x_{c_t} \in V_{c_{\ell+1}} \cap \bigcap_{j=t}^\ell W_j \quad \text{for } t \in [\ell].$$

Now we can prove that the code $\mathcal{C}$ in (2.3) has shape $\mathcal{F}$. Consider uG as in (2.4), and where $u_t \in \langle x_1, \ldots, x_{c_t} \rangle$. Then the first ℓ columns of $\phi_B(uG)$ conform to the shape of $\mathcal{F}$. Moreover,

$$u_t a_{tj} \in \langle x_1, \ldots, x_{c_t} \rangle a_{tj} \subseteq W_t a_{tj} \subseteq V_{c_{\ell+j}} \quad \text{for } t \in [\ell] \text{ and } j \in [n - \ell].$$

Thus $v_j = \sum_{t=1}^\ell u_t a_{tj} \in V_{c_{\ell+j}}$ for $j \in [n - \ell]$ and all of this shows that $\phi_B(uG)$ indeed has shape $\mathcal{F}$. Finally, $\sum_{t=1}^\ell \dim \langle x_1, \ldots, x_{c_t} \rangle = \sum_{t=1}^\ell c_t = \nu_0(\mathcal{F}; \delta) \geq \nu_{min}(\mathcal{F}; \delta')$, where $\delta' \geq \delta$ is the rank distance of $\mathcal{C}$. As in the proof of Theorem 2.2.1 we conclude that $\delta' = \delta$ and the code $\mathcal{C}$ in (2.3) is a maximal $[\mathcal{F}; \delta]_q$-code. $\qquad\square$

The inequalities (2.2) can be regarded as a staircase condition: the first ℓ columns must not have any dots below the staircase which starts at the last dot in column $\ell+1$ and goes left and upward with step size ε; see the next example. In fact, Inequality (2.2) is trivially true for $t > \ell$ and thus *no* column reaches below the staircase.

We wish to point out that in [56, Thm. 3.2 and 3.6] Zhang/Ge establish the existence of further cases of maximal $[\mathcal{F}; \delta]_q$-codes by imposing a rapid increase of the column indices. The conditions are very different from ours and imply the existence of a tower of subfields of $\mathbb{F}_{q^m}$. As the examples in [56] show, in most cases a large number of pending dots is used for the constructions.

Example 2.2.7. Consider $\mathcal{F} = [1, 3, 5, 7, 7, 8, 8, 8]$ and $\delta = 6$. Then $\ell = 3$ and $\varepsilon = 2$. The staircase condition (2.2) is indeed satisfied as can also be seen by Figure 2.5. Hence maximal $[\mathcal{F}; 6]_q$-codes exist over every field $\mathbb{F}_q$. Note that the three dots in the bottom row are pending in the sense of Definition 2.1.11. However, deleting them leads to a Ferrers diagram with fewer rows than columns. Swapping rows and columns accordingly yields the 8×7- Ferrers diagram $\tilde{\mathcal{F}} = [5, 5, 6, 6, 7, 7, 8]$. No previous construction provides us with a maximal $[\tilde{\mathcal{F}}; 6]_q$-code and thus Remark 2.1.12 cannot be utilized for the given pair $(\mathcal{F}; 6)$.
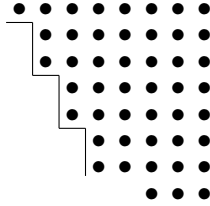
Figure 2.5: Staircase Condition as in Theorem 2.2.6

Remark 2.2.8. A particularly nice case of Theorem 2.2.6 arises when the last $\delta - 2$ columns of $\mathcal{F}$ are full (i.e., have m dots). In this case $\varepsilon = m - c_{\ell+1}$ and (2.2) reads as $c_t \leq m - (m - c_{\ell+1})(\ell + 2 - t)$ for $t \in [\ell]$.

Example 2.2.9. Consider the 6×6-Ferrers diagram $\mathcal{F} = [1, 2, 4, 5, 6, 6]$, shown in Figure 2.6, and let $\delta = 4$, hence $\ell = n - \delta + 1 = 3$. Then $\varepsilon = 1$ and we are in the situation of Remark 2.2.8. The conditions $c_t \leq m - (m - c_4)(\ell + 2 - t) = 6 - (6 - 5)(5 - t) = 1 + t$ for $t = 1, \dots, \ell$ are indeed satisfied and thus maximal $[\mathcal{F}; 4]_q$-codes exist over every field $\mathbb{F}_q$. An analogous comment as in Example 2.2.7 applies to the two pending dots in the last row.

The following is immediate with Remark 2.2.8.

Corollary 2.2.10. *Conjecture 2.1.9 holds true for $n \times n$-upper triangular matrices with $\delta = 3$.*

We also obtain an analogue to Corollary 2.2.3. It arises as a generalization of the situation discussed in Remark 2.2.8.
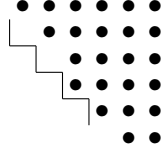
Figure 2.6: Staircase Condition as in Remark 2.2.8

Corollary 2.2.11. *Let $\ell = n - \delta + 1$ and $\mathcal{F} = [c_1, \ldots, c_n]$ be an $m \times n$-Ferrers diagram such that $c_t \geq n$ for all $t = \ell + 2, \ldots, n$ (that is, the last $\delta - 2$ columns of $\mathcal{F}$ have at least n dots) and such that*

$$c_t \leq n - (n - c_{\ell+1})(\ell + 2 - t) \text{ for } t \in [\ell].$$

Then all dots at positions (i, j) where $i > \max\{c_{\ell+1}, n\}$ are pending and there exists a maximal $[\mathcal{F}; \delta]_q$-code for any field $\mathbb{F}_q$.

Proof. If $c_{\ell+1} \geq n$, the result is in Corollary 2.2.3. Thus let us assume $c_{\ell+1} < n$. Set

$$\hat{c}_t = \min\{c_t, n\} = \begin{cases} c_t, & \text{if } t \leq \ell + 1, \\ n, & \text{if } t \geq \ell + 2, \end{cases}$$

and let $\hat{\mathcal{F}} = [\hat{c}_1, \ldots, \hat{c}_n]$. Then $\hat{\mathcal{F}}$ is an $n \times n$-Ferrers diagram satisfying the staircase condition of Remark 2.2.8. In particular, $\nu_{\min}(\hat{\mathcal{F}}; \delta) = \nu_0(\hat{\mathcal{F}}; \delta)$. Moreover, $\hat{\mathcal{F}} \subseteq \mathcal{F}$ and $\nu_0(\hat{\mathcal{F}}; \delta) = \sum_{t=1}^{\ell} \hat{c}_t = \nu_0(\mathcal{F}; \delta)$. Thus $\nu_j(\mathcal{F}; \delta) \geq \nu_j(\hat{\mathcal{F}}; \delta) \geq \nu_{\min}(\hat{\mathcal{F}}; \delta) = \nu_0(\hat{\mathcal{F}}; \delta) = \nu_0(\mathcal{F}; \delta)$ for all $j \in \{1, \ldots, \delta - 1\}$. This tells us that a maximal $[\hat{\mathcal{F}}; \delta]_q$-code is also a maximal $[\mathcal{F}; \delta]_q$-code and the existence of the former has been established in Theorem 2.2.6 and Remark 2.2.8. $\qquad\square$

Example 2.2.12. Let $\delta = 5$ and $\mathcal{F} = [3, 4, 5, 6, 6, 7]$. Then the last $\delta - 2 = 3$ columns have at least $n = 6$ dots and the staircase condition from Corollary 2.2.11 is satisfied. Hence there exists a maximal $[\mathcal{F}; 5]_q$-code over any field $\mathbb{F}_q$, and the bottom dot is pending.
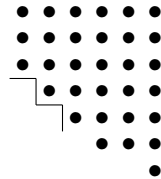
Figure 2.7: Staircase Condition as in Corollary 2.2.11

We close this section with a few instances where a maximum $[\mathcal{F}; \delta]_q$-code can be realized as an $\mathbb{F}_q$-subspace of an $\mathbb{F}_{q^m}$-linear $[m \times n; \delta]$-MRD code even though none of the staircase conditions are satisfied. We need the following lemma.

Lemma 2.2.13. *Given $m \geq n \geq \delta$. Set $\ell = n - \delta + 1$. Furthermore, let $a_1, \ldots, a_\ell \in \mathbb{F}_{q^m}$ be such that $rk(1, a_1, \ldots, a_\ell) = \ell + 1$. Then there exists a matrix $A \in \mathbb{F}_{q^m}^{\ell \times (n-\ell)}$, such that its first column is given by $(a_1, \ldots, a_\ell)^\intercal$ and $\mathcal{C} = rowsp(I_\ell \mid A)$ is an $\mathbb{F}_{q^m}$-linear $[m \times n; \delta]$-MRD code.*

Proof. Let $G' = (I \mid B) \in \mathbb{F}_{q^m}^{\ell \times n}$ generate an MRD code, and denote the first column of B by $(b_1, \ldots, b_\ell)^\intercal$. Then $rk(1, b_1, \ldots, b_\ell) = \ell + 1$ thanks to Lemma 2.2.5. Hence there exists an $\mathbb{F}_q$-isomorphism $\phi : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_{q^m}$ such that $\phi(b_i) = a_i$ for $i = 1, \ldots, \ell$ and $\phi(1) = 1$. Set $G = \phi(G')$, where we apply ϕ entrywise to the matrix. Then G is of the form $G = (I \mid A)$, where the first column of A is as desired. Furthermore, G generates an MRD code. This follows from the $\mathbb{F}_q$-linearity of ϕ along with the MRD criterion given in [15, Thm. 2], which says that a matrix $G \in \mathbb{F}_{q^m}^{\ell \times n}$ generates an MRD code iff for every $U \in \mathrm{GL}_n(\mathbb{F}_q)$ each maximal minor of GU is nonzero. $\qquad\square$

Example 2.2.14. Let $\mathcal{F} = [2, 2, 4, 4]$ and let $\delta = 4$. Thus $\nu_{\min} = 2$. Choose an $\mathbb{F}_{q^4}$-linear $[4 \times 4; 4]$-MRD code generated by $G = (1, \beta, \beta', \beta'') \in \mathbb{F}_{q^4}^{1 \times 4}$. Suppose $B = (x_1, x_2, x_3, x_4)$ is a basis such that $\{\phi_B(uG) \mid u \in \langle x_1, x_2 \rangle\}$ has shape $\mathcal{F}$. The shape implies $\langle x_1, x_2 \rangle \beta \subseteq \langle x_1, x_2 \rangle$. From this one easily derives $\langle 1, \beta \rangle = \langle 1, x_1^{-1} x_2 \rangle$ as well as $\beta x_1^{-1} x_2 \in \langle 1, x_1^{-1} x_2 \rangle$. In other words, $\beta^2 \in \langle 1, \beta \rangle$. Such an element clearly exists and any basis of the form $B = (1, \beta, x_3, x_4)$ leads to the desired Ferrers diagram code. All of this shows that the MRD code generated by $(1, \beta, \beta', \beta'')$ admits a maximal $[\mathcal{F}; 4]$-code iff β has degree 2. We conclude that some, but not every, $\mathbb{F}_{q^4}$-linear $[4 \times 4; 4]$-MRD code contains, for a suitable basis B, a maximal $[\mathcal{F}; 4]_q$-code.

The following result provides us with maximal Ferrers diagram codes for certain diagrams with at most 3 distinct column indices. The construction bears some resemblance to [56, Thm. 3.2]. However, while the latter requires pending dots for many Ferrers diagrams this is not the case for our construction. Such an example, not covered by any of the constructions in [56] and not having any pending dots, will be presented below in Example 2.2.16.

Proposition 2.2.15. *Let $3 \leq \delta \leq n \leq m$ and put $\ell = n - \delta + 1$. Let $b \in \mathbb{N}$ be a common divisor of m and $\ell + 1$. Then there exists a maximal $[\mathcal{F}; \delta]_q$-code, where*

$$\mathcal{F} = [\underbrace{b, \ldots, b}_{\ell - b + 1}, \underbrace{\ell + 1, \ldots, \ell + 1}_{b}, \underbrace{m, \ldots, m}_{\delta - 2}].$$

Proof. Let $\alpha \in \mathbb{F}_{q^m}$ be a primitive element, and put $\beta = \alpha^{(q^m - 1)/(q^b - 1)}$. Define the $\mathbb{F}_q$-subspace

$$V = \left\langle \alpha^i \beta^j \, \middle| \, 0 \leq i < \frac{\ell + 1}{b}, \, 0 \leq j < b \right\rangle_{\mathbb{F}_q} \subset \mathbb{F}_{q^m}.$$

Using that $b \leq m/2$, one easily verifies that $s := (\ell + 1)/b - 1 < (q^m - 1)/(q^b - 1)$, and therefore the described generators form a basis of V. Thus $\dim_{\mathbb{F}_q}(V) = \ell + 1$. Let B be a basis of $\mathbb{F}_{q^m}$, whose first $\ell + 1$ elements are the given basis of V in the order

$$1, \beta, \ldots, \beta^{b-1} \mid \alpha, \alpha\beta, \ldots, \alpha\beta^{b-1} \mid \alpha^2, \alpha^2\beta, \ldots, \alpha^2\beta^{b-1} \mid \ldots \mid \alpha^s, \alpha^s\beta, \ldots, \alpha^s\beta^{b-1}. \quad (2.5)$$

Note that $\mathbb{F}_q[\beta] = \mathbb{F}_{q^b}$, and thus β^b is an $\mathbb{F}_q$-linear combination of $1, \ldots, \beta^{b-1}$. This in turn implies that V is β-invariant. By Lemma 2.2.13 there exists a matrix $G = (I_\ell \mid A) \in \mathbb{F}_{q^m}^{\ell \times n}$ generating an $\mathbb{F}_{q^m}$-linear MRD code, and where the first column of A is given by the transpose of

$$(\alpha, \alpha\beta, \ldots, \alpha\beta^{b-1} \mid \alpha^2, \alpha^2\beta, \ldots, \alpha^2\beta^{b-1} \mid \ldots \mid \alpha^s, \alpha^s\beta, \ldots, \alpha^s\beta^{b-1} \mid \beta, \ldots, \beta^{b-1}). \quad (2.6)$$

Put

$$\mathcal{C} = \phi_B\big\{(u_1, \ldots, u_\ell)G \,\big|\, u_1, \ldots, u_{\ell-b+1} \in \langle 1, \beta, \ldots, \beta^{b-1}\rangle \text{ and } u_{\ell-b+2}, \ldots, u_\ell \in V\big\}.$$

Then $\dim(\mathcal{C}) = b(\ell-b+1) + (\ell+1)(b-1) = \nu_0(\mathcal{F}; \delta)$ and $\mathcal{C}$ has rank distance $\delta' \geq \delta$. It remains to see that $\mathcal{C}$ is supported on $\mathcal{F}$. This is clearly the case for the first ℓ coordinates of any codeword $(u_1, \ldots, u_\ell)G$ thanks to the choice of B and (2.5), and it is trivially true for the last $\delta - 2$ coordinates. The $(\ell+1)$-st coordinate is the scalar product of $(u_1, \ldots, u_\ell)$ and the vector in (2.6). By the β-invariance of V this product is in V, and thus its coordinate vector has zero entries in the last $m - \ell - 1$ positions due to the choice of the basis B. Thus $\mathcal{C}$ is an $[\mathcal{F}; \delta']_q$-code of dimension $\nu_0(\mathcal{F}; \delta)$. As in the proof of Theorem 2.2.1 this yields the desired result. $\qquad\square$

Let us briefly revisit Example 2.2.14. Then $\mathcal{F}$ is as in the last proposition ($\ell = 1$, $b = 2$, and $s = 0$), and the case where the entry β of G has degree 2 is the situation from the previous proof.

We conclude this section with an example, which has been mentioned explicitly in [13, Sec. VIII] as an open case, and can now be settled thanks to Proposition 2.2.15.

Example 2.2.16. Let $m = n = 6$ and $\delta = 4$. Hence $\ell = n - \delta + 1 = 3$. Choosing $b = 2$ leads to the Ferrers diagram $\mathcal{F} = [2, 2, 4, 4, 6, 6]$. In this case $\nu_{\min}(\mathcal{F}; \delta) = 8 = \nu_j$ for all $j = 0, \ldots, 3$. Thus $\mathcal{F}$ has no pending dots w.r.t. δ. The matrix G of the previous proof takes the form

$$G = \begin{pmatrix} 1 & 0 & 0 & \alpha & b_1 & c_1 \\ 0 & 1 & 0 & \alpha\beta & b_2 & c_2 \\ 0 & 0 & 1 & \beta & b_3 & c_3 \end{pmatrix} \in \mathbb{F}_{q^6}^{3 \times 6},$$

where α is a primitive element of $\mathbb{F}_{q^6}$ and $\beta := \alpha^{(q^6-1)/(q^2-1)}$. The desired maximal $[\mathcal{F}; 4]_q$-code is given by

$$\mathcal{C} := \big\{\phi_B\big((u_1, u_2, u_3)G\big) \,\big|\, u_1, u_2 \in \langle 1, \beta\rangle, \, u_3 \in \langle 1, \beta, \alpha, \alpha\beta\rangle\big\}, \quad (2.7)$$

which is indeed 8-dimensional. It is worth mentioning that maximal $[\mathcal{F}; 4]_q$-codes are extremely scarce. Indeed, using SageMath and testing 100,000,000 tuples of 8 random matrices of shape $\mathcal{F}$ over $\mathbb{F}_2$ did not lead to a single maximal $[\mathcal{F}; 4]_2$-code. In Section 2.5 we will discuss more generally the probability that a random selection of $\nu_{\min}(\mathcal{F}; \delta)$ matrices in $\mathbb{F}_q[\mathcal{F}]$ generates a maximal $[\mathcal{F}; \delta]_q$-code.

2.3 Ferrers Diagram Codes not Obtainable from MRD Codes

In Example 2.2.14 we illustrated that for certain pairs $(\mathcal{F}; \delta)$ a maximal $[\mathcal{F}; \delta]_q$-code can be realized as an $\mathbb{F}_q$-linear subspace of a suitably chosen $\mathbb{F}_{q^m}$-linear MRD code. We now present pairs $(\mathcal{F}; \delta)$ that do not allow the realization of a maximal $[\mathcal{F}; \delta]_q$-code as a subfield subcode of *any* $\mathbb{F}_{q^m}$-linear MRD code. In order to do so we need the following simple lemma.

Lemma 2.3.1. *Let $a \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$ and suppose there is an $\mathbb{F}_q$-subspace V of $\mathbb{F}_{q^m}$ that is invariant under multiplication by a. Then $\gcd(\dim_{\mathbb{F}_q} V, m) > 1$.*

Proof. Let the subfield $\mathbb{F}_q[a]$ have order q^r. Then $r > 1$ and $r \mid m$. By assumption V is an $\mathbb{F}_q[a]$-subspace of $\mathbb{F}_{q^m}$. Hence $\dim_{\mathbb{F}_q} V = tr$, where $t := \dim_{\mathbb{F}_q[a]} V$. This proves the statement. $\qquad\square$

Corollary 2.3.2. *Let $\mathcal{F} = [c_1, \ldots, c_n]$ be an $m \times n$-Ferrers diagram and $2 \leq \delta \leq n$. Set $\ell = n - \delta + 1$. Suppose*

$$c_\ell = c_{\ell+1} < m \quad and \quad \gcd(c_\ell, m) = 1.$$

If $\nu_{min}(\mathcal{F}; \delta) = \nu_0(\mathcal{F}; \delta) = \sum_{t=1}^{\ell} c_t$, then a maximal $[\mathcal{F}; \delta]_q$-code does not exist as an $\mathbb{F}_q$-subspace of an $\mathbb{F}_{q^m}$-linear $[m \times n; \delta]$-MRD code.

Note that in the situation of this corollary, the step size $\varepsilon = \sum_{t=\ell+1}^{n}(m - c_t)$ from Theorem 2.2.6 is positive and the staircase condition (2.2) is not satisfied.

Proof. Suppose by contradiction that $G = (I_\ell \mid A) \in \mathbb{F}_{q^m}^{\ell \times n}$ generates an MRD code that contains a maximal $[\mathcal{F}; \delta]$-code. This means, there exists a basis $B = (x_1, \ldots, x_m)$ of $\mathbb{F}_{q^m}$ such that

$$\phi_B\big((u_1, \ldots, u_\ell)G\big) \text{ has shape } \mathcal{F} \text{ for all } u_t \in \langle x_1, \ldots, x_{c_t} \rangle, \, t \in [\ell].$$

Set $V := \langle x_1, \ldots, x_{c_\ell} \rangle$. Then $u_t \in V$ for all $t \in [\ell]$. Let $uA = (v_1, \ldots, v_{n-\ell})$. Then $v_1 = \sum_{t=1}^{\ell} u_t a_t$, where $(a_1, \ldots, a_\ell)^\intercal$ is the first column of A, and $c_\ell = c_{\ell+1}$ implies $v_1 \in V$. Since this has to be true for all choices of $u_1, \ldots, u_\ell$, we obtain in particular that $u_\ell a_\ell \in V$ for all $u_\ell \in V$ and conclude that V is a_ℓ-invariant. By Lemma 2.2.5 the element a_ℓ is not in $\mathbb{F}_q$, and thus Lemma 2.3.1 leads to a contradiction to the given coprimeness of c_ℓ and m. $\qquad\square$

Now we are ready to present some examples.

Example 2.3.3. For $\mathcal{F} = [1, 3, 3, 4]$ and $\delta = 3$ we have $\ell = 2$ and $c_2 = c_3 = 3$. Thus, by Corollary 2.3.2 a maximal $[\mathcal{F}; 3]_q$-code is not realizable as an $\mathbb{F}_q$-subspace of an $\mathbb{F}_{q^4}$-linear $[4 \times 4; 3]$-MRD code. As we saw in Example 2.1.16, such codes can nevertheless easily be constructed in an ad-hoc manner. In Example 2.6.10 we will return to this Ferrers diagram and discuss the probability that 4 randomly chosen matrices in $\mathbb{F}_q[\mathcal{F}]$ generate a maximal $[\mathcal{F}; \delta]_q$-code.

Example 2.3.4. Let $\mathcal{F}$ be the 5×5-Ferrers diagram $\mathcal{F} = [1, 3, 4, 4, 5]$ and $\delta = 3$. Then $\ell = 3$ and $\nu_{\min}(\mathcal{F}; \delta) = c_1 + c_2 + c_3 = 8$, $c_3 = c_4 = 4$, $\gcd(c_3, m) = 1$ (and $\mathcal{F}$ has no pending dots w.r.t. $\delta = 3$). Again, Corollary 2.3.2 implies that a maximal $[\mathcal{F}; 3]$-code cannot be obtained as an $\mathbb{F}_q$-subspace of an $\mathbb{F}_{q^5}$-linear $[5 \times 5; 3]$-MRD code. In this case a maximal $[\mathcal{F}; \delta]_q$-code can be obtained by [13, Construction 2, Thm. 8]. The assumptions of [13, Thm. 8] are indeed met: (1) the last $\delta - 1$ columns have at least $n - 1$ dots, (2) the first $n - \delta + 1$ columns have at most $n - 1$ dots[1], (3) $m \geq n - 1 + c_1$.

Example 2.3.5. Consider the 5×5-Ferrers diagram $\mathcal{F} = [2, 2, 5, 5, 5]$ with $\delta = 5$ and $\ell = n - \delta + 1 = 1$. Hence $c_\ell = c_{\ell+1} = 2$ and $\nu_{\min}(\mathcal{F}; 5) = c_1 = 2$. Thus, as above, a maximal $[\mathcal{F}; 5]$-code cannot be realized as an $\mathbb{F}_q$-subspace of an $\mathbb{F}_{q^5}$-linear $[5 \times 5; 5]$-MRD code. However, such a code can easily be obtained as follows. First of all, $\mathcal{F}$ has a pending dot at $(5, 3)$. Removing that dot leads to a Ferrers diagram covered by [13, Thm. 9]. The simple proof shows how to construct the desired maximal $[\mathcal{F}; 5]_q$-code over any field $\mathbb{F}_q$.

2.4 The Upper Triangular Shape and Distance $n - 1$

In this short section we establish the existence of maximal $n \times n$-Ferrers diagram codes of upper triangular shape with rank distance $n - 1$ in two different ways. The first one is by induction on n and a pure existence result. The second one is an explicit construction based on an irreducible polynomial. We leave it as an open problem whether either construction can be generalized to upper triangular matrices with rank distance $\delta < n - 1$.

We start with the recursive construction for which the following lemma is crucial. We denote the column space of a matrix M by $\mathrm{colsp}(M)$.

Lemma 2.4.1. *Let $\mathbb{F} = \mathbb{F}_q$ and $A, B \in \mathbb{F}^{n \times n}$ be such that $\mathrm{colsp}(B) \nsubseteq \mathrm{colsp}(A)$. Then there exist vectors $v, w \in \mathbb{F}^n$ such that for all $(\lambda, \mu) \in \mathbb{F}^2 \setminus \{(0, 0)\}$*

$$rk(\lambda A + \mu B) \leq n - 1 \implies \lambda v + \mu w \notin colsp(\lambda A + \mu B).$$

Proof. Choose $v \in \mathrm{colsp}(B) \setminus \mathrm{colsp}(A)$. It suffices to show the existence of a vector $w \in \mathbb{F}^n$ such that $\lambda v + w \notin \mathrm{colsp}(\lambda A + B)$ whenever $\mathrm{rk}(\lambda A + B) \leq n - 1$.

To this end, set $M_\lambda := \lambda A + B$ and define $\mathcal{M} = \{\lambda \in \mathbb{F} \mid \mathrm{rk}(M_\lambda) \leq n - 1\}$. Moreover, for each $\lambda \in \mathcal{M}$ define the affine map

$$f_\lambda : \mathbb{F}^n \longrightarrow \mathbb{F}^n, \quad x \longmapsto M_\lambda x - \lambda v.$$

Then for any $z \in \mathbb{F}^n$ we have $z \in \mathrm{im}(f_\lambda) \iff \lambda v + z \in \mathrm{colsp}(M_\lambda)$. Hence we need to show the existence of a vector $w \in \mathbb{F}^n \setminus \mathcal{J}$, where $\mathcal{J} = \bigcup_{\lambda \in \mathcal{M}} \mathrm{im}(f_\lambda)$. Note that $|\mathcal{M}| \leq q$ and $|\mathrm{im}(f_\lambda)| \leq q^{n-1}$ for all $\lambda \in \mathcal{M}$. Thus $|\mathcal{J}| \leq q^n$. Clearly, if $|\mathcal{M}| < q$ we have $|\mathcal{J}| < q^n$, as desired. Hence let $\mathcal{M} = \mathbb{F}_q$. In this case the union is not disjoint

---

[1]This assumption is not explicitly mentioned in [13, Construction 2, Thm. 8] but is in fact necessary; see also the paragraph after the proof of Thm. 8 in [13].

because by choice of v we have $v = Bx$ for some $x \in \mathbb{F}^n$ and thus $v = f_0(x) = f_{-1}(0)$. Thus, again $|\mathcal{J}| < q^n$. □

Now we can establish the existence of maximal $[\mathcal{F}; n-1]_q$-codes for the $n \times n$-upper triangle $\mathcal{F}$.

Theorem 2.4.2. *Let $\mathcal{F} = [1, 2, \ldots, n]$, thus $\mathbb{F}_q[\mathcal{F}]$ is the space of upper triangular matrices over $\mathbb{F}_q$. Let $\delta = n - 1$, hence $\nu_{min}(\mathcal{F}; n - 1) = 3$. Then for every q there exists a maximal $[\mathcal{F}; n - 1]_q$-code. Thus, Conjecture 2.1.9 is true for the pair $(\mathcal{F}; n - 1)$.*

Proof. We induct on n. For $n = 2$ the statement is trivially true since the matrices

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \text{ and } C = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

generate a 3-dimensional code over any field, and the minimum prescribed distance is only $1 = n - 1$.

Suppose now the statement is true for size n and that A, B, C generate a maximal $[\mathcal{F}; n - 1]_q$-code in $\mathbb{F}^{n \times n}$. Assume $\mathrm{colsp}(B) \nsubseteq \mathrm{colsp}(A)$.

By Lemma 2.4.1 there exist $v, w \in \mathbb{F}^n$ such that $\lambda v + \mu w \notin \mathrm{colsp}(\lambda A + \mu B)$ whenever $\mathrm{rk}(\lambda A + \mu B) = n - 1$. Define the (upper triangular) matrices

$$\widehat{A} = \left(\begin{array}{c|c} A & v \\ \hline 0 & 0 \end{array} \right), \widehat{C} = \left(\begin{array}{c|c} B & w \\ \hline 0 & 0 \end{array} \right), \widehat{B} = \left(\begin{array}{c|c} C & 0 \\ \hline 0 & 1 \end{array} \right) \in \mathbb{F}^{(n+1) \times (n+1)}.$$

Consider a general linear combination

$$\Omega := \lambda\widehat{A} + \mu\widehat{C} + \nu\widehat{B} = \left(\begin{array}{c|c} \lambda A + \mu B + \nu C & \lambda v + \mu w \\ \hline 0 & \nu \end{array} \right).$$

If $\nu \neq 0$ then clearly $\mathrm{rk}(\Omega) \geq n$, while for $\nu = 0$ the choice of v, w also guarantees that $\mathrm{rk}(\Omega) = n$. This shows that $\widehat{A}, \widehat{B}, \widehat{C}$ generate a maximal $[\widehat{\mathcal{F}}, n]_q$-code in $\mathbb{F}^{(n+1) \times (n+1)}$, where $\widehat{\mathcal{F}} = [1, 2, \ldots, n+1]$. Finally note that $\mathrm{colsp}(\widehat{B}) \nsubseteq \mathrm{colsp}(\widehat{A})$, and we may apply the induction step again to this triple of matrices. □

We conclude this section with an explicit construction, this time not relying on recursion.

Construction 2.4.3. Let

$$A = \begin{pmatrix} 0 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix}$$

be $n \times n$ matrices. Choose elements $c, d \in \mathbb{F}_q$ such that $y^2 + dy - c \in \mathbb{F}_q[y]$ is irreducible.

Case i: If n is even, put

$$
C = \begin{pmatrix}
1 & d & -1 & & & & & & \\
 & 0 & \boxed{\begin{matrix} 0 & 1 \\ c & d \end{matrix}} & -1 & & & & \\
 & & & 0 & & \ddots & & \\
 & & & & \ddots & & -1 & \\
 & & & & & 0 & \boxed{\begin{matrix} 0 & 1 \\ c & d \end{matrix}} \\
 & & & & & & & 0
\end{pmatrix}.
$$

Case ii: If n is odd, put

$$
C = \begin{pmatrix}
1 & d & -1 & & & & & \\
 & 0 & \boxed{\begin{matrix} 0 & 1 \\ c & d \end{matrix}} & -1 & & & \\
 & & & 0 & & \ddots & & \\
 & & & & \ddots & & -1 & \\
 & & & & & 0 & \boxed{\begin{matrix} 0 & 1 \\ c & d \end{matrix}} & -1 \\
 & & & & & & 0 & 0 \\
 & & & & & & & c
\end{pmatrix}.
$$

We define the code $\mathcal{C} = \langle A, B, C \rangle_{\mathbb{F}_q}$.

Theorem 2.4.4. *The output code $\mathcal{C}$ in Construction 2.4.3 is a maximal $[\mathcal{F}; n-1]_q$ code, where $\mathcal{F} = [1, 2, \ldots, n]$ is the $n \times n$ upper triangular Ferrers diagram.*

Proof. Clearly $\mathrm{rk}(xA + yB) \geq n - 1$ if $(x, y) \neq (0, 0) \in \mathbb{F}_q^2$. It remains to consider the rank of $\Omega := xA + yB + C$.

39

Case i: Assume n is even. If $x = 0$, then

$$\Omega = \begin{pmatrix} 1 & y+d & -1 & & & & & \\ & 0 & y & 1 & & & & \\ & & c & y+d & -1 & & & \\ & & & 0 & \ddots & & & \\ & & & & \ddots & -1 & & \\ & & & & & 0 & y & 1 \\ & & & & & & c & y+d \\ & & & & & & & 0 \end{pmatrix}.$$

Each copy of $\begin{pmatrix} y & 1 \\ c & y+d \end{pmatrix}$ contributes 2 rank because of our choice of c and d.
The top row contributes 1 more, so $\mathrm{rk}(\Omega) = n - 1$.

Now suppose $x \neq 0$. We then have

$$\Omega = \begin{pmatrix} 1 & y+d & -1 & & & & & \\ & x & y & 1 & & & & \\ & & x+c & y+d & -1 & & & \\ & & & x & & \ddots & & \\ & & & & \ddots & & -1 & \\ & & & & & x & y & 1 \\ & & & & & & x+c & y+d \\ & & & & & & & x \end{pmatrix}.$$

If $x \neq -c$, then the main diagonal guarantees $\mathrm{rk}(\Omega) = n$. If $x = -c$, we have

$$\Omega = \begin{pmatrix} 1 & y+d & -1 & & & & & \\ & -c & y & 1 & & & & \\ & & 0 & y+d & -1 & & & \\ & & & -c & & \ddots & & \\ & & & & \ddots & y+d & -1 & \\ & & & & & -c & y & 1 \\ & & & & & & 0 & y+d \\ & & & & & & & -c \end{pmatrix}.$$

40

Each copy of $\begin{pmatrix} y+d & -1 \\ -c & y \end{pmatrix}$ contributes 2 rank, again because of our choice of c and d. Since $-c \neq 0$, the rightmost column contributes 1 more, so $\mathrm{rk}(\Omega) = n-1$.

Case ii: Assume n is odd. If $x = 0$, then

$$\Omega = \begin{pmatrix}
1 & y+d & -1 & & & & & & \\
 & 0 & \boxed{\begin{matrix} y & 1 \end{matrix}} & & & & & & \\
 & & \boxed{\begin{matrix} c & y+d \end{matrix}} & -1 & & & & & \\
 & & & 0 & & \ddots & & & \\
 & & & & \ddots & & -1 & & \\
 & & & & & 0 & \boxed{\begin{matrix} y & 1 \end{matrix}} & & \\
 & & & & & & \boxed{\begin{matrix} c & y+d \end{matrix}} & -1 & \\
 & & & & & & & 0 & y \\
 & & & & & & & & c
\end{pmatrix}.$$

Each copy of $\begin{pmatrix} y & 1 \\ c & y+d \end{pmatrix}$ contributes 2 rank. Since $c \neq 0$, the top and bottom rows each contribute 1 more. Thus $\mathrm{rk}(\Omega) = n - 1$.

Now suppose $x \neq 0$. We then have

$$\Omega = \begin{pmatrix}
1 & y+d & -1 & & & & & & \\
 & x & \boxed{\begin{matrix} y & 1 \end{matrix}} & & & & & & \\
 & & \boxed{\begin{matrix} x+c & y+d \end{matrix}} & -1 & & & & & \\
 & & & x & & \ddots & & & \\
 & & & & \ddots & & -1 & & \\
 & & & & & x & \boxed{\begin{matrix} y & 1 \end{matrix}} & & \\
 & & & & & & \boxed{\begin{matrix} x+c & y+d \end{matrix}} & -1 & \\
 & & & & & & & x & y \\
 & & & & & & & & x+c
\end{pmatrix}.$$

If $x \neq -c$, then again $\operatorname{rk}(\Omega) = n$. If $x = -c$, we have

$$\Omega = \begin{pmatrix} 1 & \boxed{\begin{matrix} y+d & -1 \\ -c & y \end{matrix}} & & & & & & \\ & & 1 & & & & & \\ & & 0 & y+d & -1 & & & \\ & & & -c & & \ddots & & \\ & & & & \ddots & \boxed{\begin{matrix} y+d & -1 \\ -c & y \end{matrix}} & & \\ & & & & & & 1 & \\ & & & & & & 0 & \boxed{\begin{matrix} y+d & -1 \\ -c & y \end{matrix}} \\ & & & & & & & 0 \end{pmatrix}.$$

Each copy of $\begin{pmatrix} y+d & -1 \\ -c & y \end{pmatrix}$ contributes 2 rank. We conclude that $\operatorname{rk}(\Omega) = n-1$.

$\square$

It is particularly interesting that this construction utilizes none of the dots in the top right corner of $\mathcal{F}$. Naturally, one wonders if either of the constructions in this section can be generalized to other rank distances. However, such a generalization is not immediately apparent because with $\delta = n - 2$ we already need six matrices to generate a maximal code.

2.5   On the Genericity of Maximal Ferrers Diagram Codes

In this section we study the likelihood that a randomly chosen Ferrers diagram code of a given dimension has maximum rank. It will turn out that the answer depends highly on the choice of the Ferrers diagram. Special attention will be paid to MRD codes.

For MRD codes the question has also been studied in [40] by Neri et al. (focussing on $\mathbb{F}_{q^m}$-linear MRD codes) and in [7] by Byrne/Ravagnani. We will give more details and compare our results to those as we go along.

As before we assume throughout that $n \leq m$ and $\delta \in [n]$. We cast the following definition.

Definition 2.5.1. Let $\mathcal{F}$ be an $m \times n$-Ferrers diagram and $\delta \in [n]$. Set $N = \nu_{\min}(\mathcal{F}; \delta)$. Then $N \leq |\mathcal{F}| = \dim \mathbb{F}_q[\mathcal{F}]$. Consider the spaces

$$T_q = \{\mathcal{C} \subseteq \mathbb{F}_q[\mathcal{F}] \mid \dim(\mathcal{C}) = N\} \quad \text{and} \quad \hat{T}_q = \{\mathcal{C} \in T_q \mid \operatorname{d_{rk}}(\mathcal{C}) = \delta\},$$

thus $\hat{T}_q$ is the set of maximal $[\mathcal{F}; \delta]_q$-codes. Then the fraction $|\hat{T}_q|/|T_q|$ is called the *proportion of maximal $[\mathcal{F}; \delta]$-codes* (within the space of all N-dimensional subspaces

of $\mathbb{F}_q[\mathcal{F}]$). We say that maximal $[\mathcal{F}; \delta]$-codes are *generic* if

$$\lim_{q \to \infty} \frac{|\hat{T}_q|}{|T_q|} = 1.$$

Of course, investigating genericity does not address the existence of maximal $[\mathcal{F}; \delta]$-codes over any given finite field. Note also that maximal $[\mathcal{F}; 1]$-codes are trivially generic.

It will occasionally be useful for us to express genericity in terms of the probability that randomly chosen matrices generate a maximal $[\mathcal{F}; \delta]$-code. In order to do so, we need to fix the probability distribution on $\mathbb{F}_q^{m \times n}$ such that all entries of a matrix $A = (a_{ij}) \in \mathbb{F}_q^{m \times n}$ are independent and uniformly distributed. Thus, for all (i, j) and all $\alpha \in \mathbb{F}_q$:

$$\mathrm{Prob}\,(a_{ij} = \alpha) = q^{-1}.$$

For a matrix with shape $\mathcal{F}$, the above applies to all entries inside $\mathcal{F}$ whereas all other entries are zero with probability 1. We say that $A_1, \ldots, A_N \in \mathbb{F}_q[\mathcal{F}]$ are *randomly chosen matrices* if they are chosen independently and randomly according to the above distribution. We will frequently, and without specific mention, make use of the well-known identity

$$\left|\left\{M \in \mathbb{F}_q^{a \times b} \,\middle|\, \mathrm{rk}M = b\right\}\right| = \prod_{i=0}^{b-1}(q^a - q^i).$$

Proposition 2.5.2. *Fix a pair $(\mathcal{F}; \delta)$ and let $N = \nu_{min}(\mathcal{F}; \delta)$. Define*

$$P_q := Prob\left(\langle A_1, \ldots, A_N \rangle \text{ is an } [\mathcal{F}, N; \delta]_q\text{-code}\right)$$

for randomly chosen matrices $A_1, \ldots, A_N \in \mathbb{F}_q[\mathcal{F}]$. Then

$$\frac{|\hat{T}_q|}{|T_q|} = P_q \cdot \frac{q^{|\mathcal{F}|N}}{\prod_{i=0}^{N-1}(q^{|\mathcal{F}|} - q^i)}. \tag{2.8}$$

As a consequence, $\lim_{q \to \infty} |\hat{T}_q|/|T_q| = \lim_{q \to \infty} P_q$ and maximal $[\mathcal{F}; \delta]$-codes are generic in the sense of Definition 2.5.1 iff $\lim_{q \to \infty} P_q = 1$.

Proof. In addition to the sets T_q and $\hat{T}_q$ from Definition 2.5.1 define

$$\left.\begin{aligned} W_q &= \{(A_1, \ldots, A_N) \in \mathbb{F}_q[\mathcal{F}]^N \mid \dim \langle A_1, \ldots, A_N \rangle = N\}, \\ \hat{W}_q &= \{(A_1, \ldots, A_N) \in W_q \mid \mathrm{d}_{\mathrm{rk}}\langle A_1, \ldots, A_N \rangle = \delta\}. \end{aligned}\right\} \tag{2.9}$$

Due to the uniform probability, the probability P_q is given by $P_q = |\hat{W}_q|/q^{|\mathcal{F}|N}$. Furthermore, each code $\mathcal{C}$ in T_q has $\alpha := \prod_{i=0}^{N-1}(q^N - q^i)$ ordered bases. In other words, $|T_q|\alpha = |W_q|$ and $|\hat{T}_q|\alpha = |\hat{W}_q|$ which in turn implies

$$\frac{|\hat{T}_q|}{|T_q|} = \frac{|\hat{W}_q|}{|W_q|} = P_q \frac{q^{|\mathcal{F}|N}}{|W_q|}. \tag{2.10}$$

Using $|W_q| = \prod_{i=0}^{N-1}(q^{|\mathcal{F}|} - q^i)$, one arrives at (2.8). The final statements follow from the fact that the rightmost fraction approaches 1 as $q \to \infty$. $\qquad\square$

In the next section we will show that $\mathbb{F}_q$-linear $[m \times n; \delta]$-MRD codes are not generic (unless $n = 1$) and will give an upper bound for the asymptotic probability. This result in stark contrast to the results in [40] by Neri et al., where $\mathbb{F}_{q^m}$-linear rank-metric codes in $\mathbb{F}_{q^m}^n$ are considered. The authors show that $\mathbb{F}_{q^m}$-linear MRD codes are generic within the class of all $\mathbb{F}_{q^m}$-linear rank-metric codes. Let us illustrate the difference of the two settings for $[m \times n; n]$-MRD codes. In this case, the $\mathbb{F}_{q^m}$-linear case amounts to the question whether a randomly chosen matrix of the form

$$G = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^{1 \times n}$$

generates an MRD code. This is obviously equivalent to the question of whether $g_1, \ldots, g_n$ are linearly independent over $\mathbb{F}_q$. The probability for this is $(\prod_{i=0}^{n-1}(q^m - q^i))/(q^{mn})$ and tends to 1 as $q \to \infty$. In the matrix version the same reads as follows. Let $C \in \mathbb{F}_q^{m \times m}$ be the companion matrix of a primitive polynomial. The above asks for the probability that for a randomly chosen matrix $A \in \mathbb{F}_q^{m \times n}$ the matrices $A, CA, \ldots, C^{m-1}A$ span an $[m \times n; n]$-MRD code. But the latter is simply equivalent to A having rank n, which again results in the above given probability.

On the other hand, in the space of all $\mathbb{F}_q$-linear rank-metric codes we have to study the probability that randomly chosen matrices $A_1, \ldots, A_m \in \mathbb{F}_q^{m \times n}$ generate an $[m \times n; n]$-MRD code, which means that for all $(\lambda_1, \ldots, \lambda_m) \in \mathbb{F}_q^m \setminus 0$ the matrix $\sum_{i=1}^m \lambda_i A_i$ has full rank. As one may expect, this property is not generic. We will indeed show this later in Corollary 2.5.13, and in the next section we will provide upper bounds on the probability.

In [7] Byrne/Ravagnani use a combinatorial approach to obtain estimates for the proportion of $\mathbb{F}_q$- and $\mathbb{F}_{q^m}$-linear MRD codes. In [7, Cor. 5.5] they also derive the genericity of $\mathbb{F}_{q^m}$-linear MRD codes, and in [7, Cor. 6.2] they show that the asymptotic proportion of $\mathbb{F}_q$-linear MRD codes is at most 1/2. In Theorem 2.6.6 we will significantly improve upon this upper bound. It should be mentioned, however, that their approach is far more general and also leads to genericity results of other classes of codes.

We now turn to investigating genericity for general pairs $(\mathcal{F}; \delta)$. We show first that genericity is equivalent to the existence of a maximal $[\mathcal{F}; \delta]$-code over an algebraically closed field. To do so, we consider the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}_q$. Recall that Definition 2.1.4 – Theorem 2.1.7 make sense and are valid for matrices over infinite fields as well. Similarly, Definition 2.1.8 and Remarks 2.1.12 and 2.1.14 are valid over any field. We will also need the following result.

Lemma 2.5.3 (Schwartz-Zippel Lemma [43, 57]). *Let $\mathbb{F}$ be any field and fix a nonzero polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ of total degree d. Let S be a finite subset of $\mathbb{F}$ and $s_1, \ldots, s_n$ be independently and uniformly selected from S. Then*

$$Prob\left(f(s_1, \ldots, s_n) = 0\right) \leq \frac{d}{|S|}.$$

Now we are ready to state and prove the following.

Theorem 2.5.4. *Fix a prime power q and let $\overline{\mathbb{F}}$ be the algebraic closure of $\mathbb{F} := \mathbb{F}_q$. Consider an $m \times n$ Ferrers diagram $\mathcal{F}$ and some $\delta \in [n]$ such that $\nu_{min}(\mathcal{F}; \delta) > 0$. Let $N \leq \nu_{min}(\mathcal{F}; \delta)$. The following are equivalent.*

(i) *There exist $A_1, \ldots, A_N \in \overline{\mathbb{F}}[\mathcal{F}]$ such that $\langle A_1, \ldots, A_N \rangle$ is an $[\mathcal{F}, N; \delta]$-code.*

(ii) *The set $\{(A_1, \ldots, A_N) \in \overline{\mathbb{F}}[\mathcal{F}]^N \mid \langle A_1, \ldots, A_N \rangle$ is an $[\mathcal{F}, N; \delta]$-code$\}$ is a nonempty Zariski-open set in $\overline{\mathbb{F}}^{Nt}$, where $t = |\mathcal{F}|$ is the number of dots in $\mathcal{F}$.*

(iii) *Let $P_{q^r, N} = Prob\big(\langle A_1, \ldots, A_N \rangle$ is an $[\mathcal{F}, N; \delta]_{q^r}$-code$\big)$, where $A_1, \ldots, A_N \in \mathbb{F}_{q^r}[\mathcal{F}]$ are randomly chosen. Then $\lim_{r \to \infty} P_{q^r, N} = 1$.*

As a consequence, maximal $[\mathcal{F}; \delta]$-codes are generic iff there exists a maximal $[\mathcal{F}; \delta]$-code over any algebraically closed field of positive characteristic.

One should note that for the equivalence a fixed 'base field' $\mathbb{F}_q$ is considered, along with its field extensions and algebraic closure. Only for the consequence, we need to consider all finite fields due to the definition of genericity.

We believe that the existence of maximal $[\mathcal{F}; \delta]$-codes over an algebraically closed field does not depend on its characteristic but are not able to provide a proof at this point. Later in Theorem 2.5.8 we will encounter an instance where the existence only depends on the combinatorics of $(\mathcal{F}; \delta)$, and not on the choice of algebraically closed field.

Proof. All three statements imply that the matrices $A_1, \ldots, A_N$ are linearly independent, thus we have to focus on the rank of their nontrivial linear combinations. (ii) $\Rightarrow$ (i) is clear and so is (iii) $\Rightarrow$ (i) because $\mathbb{F}_{q^r}[\mathcal{F}] \subseteq \overline{\mathbb{F}}[\mathcal{F}]$ for all $r \in \mathbb{N}$.

For (i) $\Rightarrow$ (ii) we introduce indeterminates $x_{1,1}, \ldots, x_{1,t}, \ldots, x_{N,1}, \ldots, x_{N,t}$ over $\overline{\mathbb{F}}$ (hence they are also indeterminates over every subfield $\mathbb{F}_{q^r}$ of $\overline{\mathbb{F}}$). Define $A_i \in \mathbb{F}[x_{i,1}, \ldots, x_{i,t}]^{m \times n}$ as the matrix with shape $\mathcal{F}$ so that the indeterminates are the entries of A_i at the positions in $\mathcal{F}$ (in some order). For $\ell = 1, \ldots, N$ and further indeterminates $y_1, \ldots, y_N$ set

$$A^{(\ell)}(y) = \sum_{\substack{i=1 \\ i \neq \ell}}^N y_i A_i + A_\ell.$$

In the polynomial ring $R = \mathbb{F}[y_1, \ldots, y_N, x_{1,1}, \ldots, x_{N,t}]$ consider the ideal $I^{(\ell)}$ generated by the $\delta \times \delta$-minors of $A^{(\ell)}(y)$. Define the elimination ideals $I_0^{(\ell)} = I^{(\ell)} \cap \mathbb{F}[x_{1,1}, \ldots, x_{N,t}]$ and let $I_0 = I_0^{(1)} \cdot \ldots \cdot I_0^{(N)}$. Then

$$\mathcal{V}(I_0) := \Big\{ a = (a_{1,1}, \ldots, a_{N,t}) \in \overline{\mathbb{F}}^{Nt} \ \Big| \ f(a) = 0 \text{ for all } f \in I_0 \Big\} \subseteq \overline{\mathbb{F}}^{Nt}$$

is the variety of I_0 over $\overline{\mathbb{F}}$. Thus $\mathcal{V}(I_0) = \bigcup_{\ell=1}^N \mathcal{V}(I_0^{(\ell)})$ and

$$I_0 \neq \{0\} \Longleftrightarrow \mathcal{V}(I_0) \subsetneq \overline{\mathbb{F}}^{Nt} \Longleftrightarrow \text{ there exists } (a_{1,1}, \ldots, a_{N,t}) \in \overline{\mathbb{F}}^{Nt} \setminus \bigcup_{\ell=1}^N \mathcal{V}(I_0^{(\ell)}).$$

The right hand side implies that for the given tuple $(a_{1,1}, \ldots, a_{N,t})$ and for all ℓ and all $\lambda_1, \ldots, \lambda_N \in \overline{\mathbb{F}}$ with $\lambda_\ell = 1$ there exists a polynomial $f \in I^{(\ell)}$ such that $f(\lambda_1, \ldots, \lambda_N, a_{1,1}, \ldots, a_{N,t}) \neq 0$. This in turn means that for the according matrices $A_1, \ldots, A_N \in \overline{\mathbb{F}}[\mathcal{F}]$, every nontrivial linear combination $\sum_{\ell=1}^{N} \lambda_\ell A_\ell$ has at least one nonzero $\delta \times \delta$-minor. In other words, $\mathrm{d_{rk}}(\langle A_1, \ldots, A_N \rangle) \geq \delta$. Even more, every point $(a_{1,1}, \ldots, a_{N,t})$ in the Zariski-open set $\mathcal{Z} := \overline{\mathbb{F}}^{Nt} \setminus \mathcal{V}(I_0)$ leads to such a tuple of matrices. Since (i) guarantees that the set $\mathcal{Z}$ is nonempty, the implication (i) $\Rightarrow$ (ii) follows.

For (i) $\Rightarrow$ (iii) we consider again the ideal I_0. As in the previous part, the assumption implies $I_0 \neq \{0\}$. Fix any nonzero polynomial f in I_0. Thus f is in $\mathbb{F}[x_{1,1}, \ldots, x_{N,t}] \subseteq \overline{\mathbb{F}}[x_{1,1}, \ldots, x_{N,t}]$. Let $A_1, \ldots, A_N \in \mathbb{F}_{q^r}[\mathcal{F}]$ be randomly chosen matrices and denote their entries at the positions in $\mathcal{F}$ by $a_{1,1}, \ldots, a_{N,t}$. The Schwartz-Zippel Lemma 2.5.3 tells us that

$$\mathrm{Prob}\left(f(a_{1,1}, \ldots, a_{N,t}) \neq 0 \right) \geq 1 - \frac{\deg(f)}{q^r}.$$

Since f does not depend on r, we obtain $\lim_{r \to \infty}(1 - \deg(f)/q^r) = 1$. Finally, $f(a_{1,1}, \ldots, a_{N,t}) \neq 0$ implies $\mathrm{d_{rk}}(\langle A_1, \ldots, A_N \rangle) \geq \delta$, and hence we arrive at (iii).

The rest of the theorem is clear from the definition of genericity and the fact that all finite fields with the same characteristic have the same algebraic closure (up to isomorphism). □

The theorem provides us with plenty of pairs $(\mathcal{F}; \delta)$ for which maximal $[\mathcal{F}; \delta]$-codes are not generic. The simplest case is arguably when $\mathcal{F} = [n, \ldots, n]$ is the full $n \times n$-Ferrers diagram and $\delta = n$. In this case Theorem 2.5.4(i) is not even satisfied for $N = 2$ because for every pair of matrices A, B in $\mathrm{GL}_n(\overline{\mathbb{F}})$ the polynomial $\det(A + yB) \in \overline{\mathbb{F}}[y]$ has a root in $\overline{\mathbb{F}}$. Thus, the theorem tells us that $[n \times n; n]$-MRD codes are not generic. In the next section we will present upper bounds on the probability $\mathrm{Prob}\left(\langle A_1, \ldots, A_{\nu_{\min}(\mathcal{F};\delta)} \rangle \text{ is a maximal } [\mathcal{F}; \delta]_q\text{-code} \right)$ for various pairs $(\mathcal{F}; \delta)$ including MRD codes.

We now continue to identify a class of pairs $(\mathcal{F}; \delta)$ for which maximal $[\mathcal{F}; \delta]$-codes are generic. This class appeared already in [13, 22] because it allows the construction of maximal Ferrers diagram codes with the aid of MDS block codes. We follow the line of reasoning in [22, Thm. 32, Cor. 33]. In particular we need the notion of diagonals in a Ferrers diagram.

Definition 2.5.5. Consider the set $[m] \times [n]$. For $r \in [m]$ define the r-th diagonal as

$$D_r = \{(i,j) \mid j - i = n - r\} = \{(i, i + n - r) \mid i = \max\{1, r + 1 - n\}, \ldots, r\}.$$

Thus

$$D_1 = \{(1, n)\}, \; D_2 = \{(1, n - 1), (2, n)\}, \; \ldots, \; D_n = \{(1, 1), (2, 2), \ldots, (n, n)\},$$
$$D_{n+1} = \{(2, 1), (3, 2), \ldots, (n + 1, n)\}, \; \ldots, \; D_m = \{(m + 1 - n, 1), \ldots, (m, n)\}.$$

and $|D_r| = \min\{r, n\}$.

Later we will intersect these diagonals with a given Ferrers diagram. For the 5×4-Ferrers diagram $\mathcal{F}$ in Figure 2.8 we have $|D_r \cap \mathcal{F}| = r$ for $r = 1, \ldots, 4$ and $|D_5 \cap \mathcal{F}| = 2$.
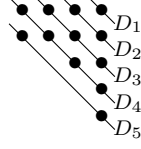

Figure 2.8: The diagonals of a Ferrers diagram

In order to cite known results conveniently, we cast the following definition. The terminology will become clear later.

Definition 2.5.6. Given an $m \times n$-Ferrers diagram $\mathcal{F}$ and $\delta \in [n]$, we call $(\mathcal{F}; \delta)$ *MDS-constructible* if

$$\nu_{\min}(\mathcal{F}; \delta) = \sum_{i=1}^{m} \max\{|D_i \cap \mathcal{F}| - \delta + 1, \, 0\}.$$

Note that only the diagonals of length at least δ contribute to the above sum, and therefore $\sum_{i=1}^{m} \max\{|D_i \cap \mathcal{F}| - \delta + 1, \, 0\} = \sum_{i=\delta}^{m} \max\{|D_i \cap \mathcal{F}| - \delta + 1, \, 0\}$. We will see in Theorem 2.5.8 below that this sum is at most $\nu_{\min}(\mathcal{F}; \delta)$ for all $(\mathcal{F}; \delta)$. The same theorem will show that if $(\mathcal{F}; \delta)$ is MDS-constructible, then maximal $[\mathcal{F}; \delta]$-codes are generic.

Example 2.5.7. (a) Let $a \in \mathbb{N}_0$ and $\mathcal{F} = [a+1, a+2, \ldots, a+n]$ (hence $\mathcal{F}$ is an $n \times n$-upper triangular shape with an $a \times n$-rectangle on top). Let $\delta \in [n]$. Then for $i = \delta, \ldots, a+n$ we have $|D_i \cap \mathcal{F}| - \delta + 1 = \min\{i, n\} - \delta + 1$. Thus

$$\sum_{i=1}^{m} \max\{|D_i \cap \mathcal{F}| - \delta + 1, \, 0\} = \sum_{i=\delta}^{n}(i - \delta + 1) + a(n - \delta + 1)$$
$$= \frac{(n - \delta + 1)(n - \delta + 2)}{2} + a(n - \delta + 1).$$

On the other hand, it is easy to see that $\nu_{\min}(\mathcal{F}; \delta) = \nu_0$ and

$$\nu_0 = \sum_{t=a+1}^{n-\delta+1+a} t = \frac{(n - \delta + a + 1)(n - \delta + a + 2) - a(a + 1)}{2},$$

which equals $\sum_{i=1}^{m} \max\{|D_i \cap \mathcal{F}| - \delta + 1, \, 0\}$. Thus $(\mathcal{F}; \delta)$ is MDS-constructible.

(b) Let $\mathcal{F}$ be the full rectangle, thus $\mathcal{F} = [m] \times [n]$, and let $\delta \in [n]$. Then $\nu_{\min} = m(n - \delta + 1)$ and

$$\sum_{i=\delta}^{m} \max\{|D_i \cap \mathcal{F}| - \delta + 1, \, 0\} = \sum_{i=\delta}^{n}(i - \delta + 1) + \sum_{i=n+1}^{m}(n - \delta + 1)$$
$$= (n - \delta + 1)\frac{2m - n - \delta + 2}{2}.$$

From this one obtains that $(\mathcal{F}; \delta)$ is not MDS-constructible for any δ unless $n = \delta = 1$.

(c) Consider $\delta = 3$ and $\mathcal{F} = [1, 2, 2, 4, 7]$. Then $\nu_{\min} = 5$ and $(\mathcal{F}; 3)$ is MDS-constructible. This is shown in the left diagram of Figure 2.9. We show all diagonals D_i for which $|D_i \cap \mathcal{F}| \geq \delta$. On the other hand, for $\delta = 4$ and $\mathcal{F}' = [2, 2, 4, 4, 6]$ we have $\nu_{\min} = 4$, and $(\mathcal{F}'; 4)$ is not MDS-constructible. The diagram is shown on the right hand side of Figure 2.9.
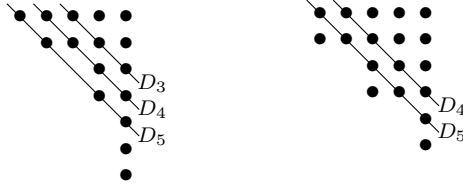

Figure 2.9: $(\mathcal{F}; 3)$ is MDS-constructible and $(\mathcal{F}'; 4)$ is not MDS-constructible

Now we can formulate a particular construction of maximum $[\mathcal{F}; \delta]$-codes over sufficiently large finite fields. It appears in [22, Thm. 32] but actually goes already back to [42, p. 329]. We include the case of algebraically closed fields and present the proof in Appendix B. The construction is based on placing the codewords of suitable MDS-block codes on the diagonals, thus our terminology MDS-constructible.

Theorem 2.5.8. *Consider an $m \times n$-Ferrers diagram $\mathcal{F}$ and $\delta \in [n]$. Then one can construct an $[\mathcal{F}; \delta]$-code of dimension at least $\sum_{i=\delta}^{m} \max\{|D_i \cap \mathcal{F}| - \delta + 1, \, 0\}$ over any field of size at least $\max\{|D_i \cap \mathcal{F}| - 1 \mid i = \delta, \dots, m\}$ (including infinite fields). Hence*

$$\nu_{min}(\mathcal{F}; \delta) \geq \sum_{i=\delta}^{m} \max\{|D_i \cap \mathcal{F}| - \delta + 1, \, 0\}.$$

As a consequence, if $(\mathcal{F}; \delta)$ is MDS-constructible there exists a maximal $[\mathcal{F}; \delta]$-code over any algebraically closed field and thus maximal $[\mathcal{F}; \delta]$-codes are generic.

Example 2.5.9. (a) For the pairs $(\mathcal{F}; \delta)$ discussed in Example 2.5.7(a) and (c), $[\mathcal{F}; \delta]$-codes are generic.

(b) Consider $\mathcal{F} = [1, 3, 3, 4]$ and $\delta = 3$; see Example 2.1.16. Then $(\mathcal{F}; 3)$ is not MDS-constructible, and in Corollary 2.6.9 we will see that maximal $[\mathcal{F}; 3]$-codes are not generic.

We now turn to the special case where $\delta = n$. We make use of another result by Gorla/Ravagnani [22].

Theorem 2.5.10 ([22, Thm. 16]). *Let $\overline{\mathbb{F}}$ be an algebraically closed field and $\mathcal{F} = [c_1, \dots, c_n]$. Set*

$$c := \min\{c_t - t + 1 \mid t = 1, \dots, n\}.$$

Then the maximum possible dimension of an $[\mathcal{F}; n]$-code over $\overline{\mathbb{F}}$ is $\max\{c, 0\}$. Thanks to Theorem 2.1.7 we thus have $c \leq \nu_{min}(\mathcal{F}; n)$.

Thus, by Theorem 2.1.7 maximal $[\mathcal{F}; n]$-codes over $\overline{\mathbb{F}}$ exist iff $c = \nu_{\min}(\mathcal{F}; n)$. This occurs only in exceptional cases. Part (a) of the next theorem deals with the case that $\nu_{\min}(\mathcal{F}; n)$ is attained by $\nu_j(\mathcal{F}; n)$ for some $j > 0$ (and possibly also by $\nu_0(\mathcal{F}; n)$). In this case there exists a maximal $[\mathcal{F}; n]$-code over $\overline{\mathbb{F}}$ exactly in the trivial case where $\nu_{\min}(\mathcal{F}; n) = 1$. Part (b) concerns the case where $\nu_{\min}(\mathcal{F}; n)$ is attained exclusively by $\nu_0(\mathcal{F}; n)$ and thus equals c_1. In this case there exists a maximal $[\mathcal{F}; n]$-code over $\overline{\mathbb{F}}$ iff the Ferrers diagram extends to or below the diagonal that starts at position $(c_1, 1)$, which is D_{n+c_1-1}.

Theorem 2.5.11. *Let $\overline{\mathbb{F}}$ be an algebraically closed field and $\mathcal{F} = [c_1, \ldots, c_n]$. Then*

$$\nu_{min}(\mathcal{F}; n) = 0 \Longleftrightarrow c_t < t \text{ for some } t \in [n].$$

Suppose $c_t \geq t$ for all $t \in [n]$.

(a) *Suppose $\nu_{min}(\mathcal{F}; n) = \nu_j(\mathcal{F}; n)$ for some $j > 0$. Then the following are equivalent.*

  (i) *$(\mathcal{F}; n)$ is MDS-constructible.*

  (ii) *There exists a maximal $[\mathcal{F}; n]$-code over $\overline{\mathbb{F}}$.*

  (iii) *$\nu_{min}(\mathcal{F}; n) = 1$.*

  (iv) *There exists $s \in [n]$ such that $c_s = s$ and $c_t \leq s - 1$ for $t = 1, \ldots, s - 1$ (thus $c_{s-1} = s - 1$).*

  Moreover, (iv) implies $\nu_{min}(\mathcal{F}; n) = \nu_{s-1}(\mathcal{F}; n)$. Finally, if $m > n$ and $c_t \geq m - n + t$ for all t, then $(\mathcal{F}; n)$ is not MDS-constructible.

(b) *Suppose $\nu_{min}(\mathcal{F}; n) = \nu_0(\mathcal{F}; n) < \nu_j(\mathcal{F}; n)$ for all $j > 0$. Then the following are equivalent.*

  (i) *$(\mathcal{F}; n)$ is MDS-constructible.*

  (ii) *There exists a maximal $[\mathcal{F}; n]$-code over $\overline{\mathbb{F}}$.*

  (iii) *$c_1 = \min\{c_t - t + 1 \mid t = 1, \ldots, n\}$ (and thus $c_1 \leq m - n + 1$).*

Proof. The equivalence is immediate with Definition 2.1.6 applied to $\delta = n$. Let now $c_t \geq t$ for all t. Hence $c > 0$ for c as in Theorem 2.5.10.

(a) The implication (i) $\Rightarrow$ (ii) is in Theorem 2.5.8 and (iii) $\Rightarrow$ (ii) is trivial. (iv) $\Rightarrow$ (iii) follows from

$$\nu_{s-1}(\mathcal{F}; n) = \sum_{t=1}^{s} \max\{c_t - s + 1, 0\} = \sum_{t=1}^{s-1} \max\{c_t - s + 1, 0\} + c_s - s + 1 = 1$$

along with $\nu_{\min}(\mathcal{F}; n) \geq 1$. In particular, $\nu_{\min}(\mathcal{F}; n) = \nu_{s-1}(\mathcal{F}; n)$.

In order to show (ii) $\Rightarrow$ (iv) let r be such that $c_r - r + 1 = \min\{c_t - t + 1 \mid t = 1, \ldots, n\}$. Theorem 2.5.10 tells us that the maximum dimension of an $[\mathcal{F}; n]$-code

over $\overline{\mathbb{F}}$ is given by $c_r - r + 1$. Note that (ii) means that $\nu_{\min}(\mathcal{F}; n) = c_r - r + 1$. Let $j > 0$ such that $\nu_{\min}(\mathcal{F}; n) = \nu_j(\mathcal{F}; n)$. Then

$$c_r - r + 1 = \nu_j(\mathcal{F}; n) = \sum_{t=1}^{j} \max\{c_t - j, 0\} + c_{j+1} - j \geq c_{j+1} - j = c_{j+1} - (j+1) + 1 \geq c_r - r + 1.$$

Thus we have equality everywhere. In particular, the second inequality yields $c_{j+1} - (j + 1) = c_r - r$. The first inequality implies that $\sum_{t=1}^{j} \max\{c_t - j, 0\} = 0$, which in turn means that $c_t \leq j$ for $t \in [j]$. Since $j > 0$ this is not a vacuous statement and thus $c_j \leq j$ for some j. Now the definition of r yields $c_r - r \leq c_j - j \leq 0$. Thus $c_r = r$ and $c_j = j$ as well as $c_{j+1} = j + 1$, and (iv) follows for $s = j + 1$.

It remains to show that (ii) implies (i). Consider the diagonal $D_n = \{(t, t) \mid t = 1, \ldots, n\}$. The assumption $c_t \geq t$ for all t shows that the dots at (c_t, t) are all on or below this diagonal. Therefore, $|D_n \cap \mathcal{F}| = |D_n| = n$. As a consequence, $\sum_{i=n}^{m} \max\{|D_i \cap \mathcal{F}| - n + 1, 0\} \geq 1 = \nu_{\min}(\mathcal{F}; n)$. Hence Theorem 2.5.8 implies equality, as desired.

Finally, the consequence for $m > n$ follows from the contradiction

$$1 = \nu_{\min}(\mathcal{F}; n) = \min\{c_t - t + 1 \mid t = 1, \ldots, n\} \geq m - n + 1 \geq 2.$$

(b) Again, (i) $\Rightarrow$ (ii) is in Theorem 2.5.8. For (ii) $\Rightarrow$ (iii) we note that $\nu_0 = c_1$. Hence there exists a c_1-dimensional $[\mathcal{F}; n]$-code over $\overline{\mathbb{F}}$ and Theorem 2.5.10 implies (iii). It remains to show (iii) $\Rightarrow$ (i). Consider the diagonal $D_{n+c_1-1} = \{(c_1 + t - 1, t) \mid t = 1, \ldots, n\}$. It contains the dot of $\mathcal{F}$ at $(c_1, 1)$. Furthermore, since $c_t \geq c_1 + t - 1$ for all t, the dots of $\mathcal{F}$ at positions (c_t, t) are on or below D_{n+c_1-1} for all t. Thus $|D_{n+c_1-1} \cap \mathcal{F}| = n$. Thanks to the top-alignedness of $\mathcal{F}$ we obtain $|D_i \cap \mathcal{F}| = n$ for all $i = n, \ldots, n + c_1 - 1$. This shows that $\sum_{i=n}^{m} \max\{|D_i \cap \mathcal{F}| - n + 1, 0\} \geq c_1 = \nu_{\min}(\mathcal{F}; n)$. Hence $(\mathcal{F}; n)$ is MDS-constructible. $\square$

The previous result generalizes the scenario used in the proof of [22, Prop. 17]. Here is a case different from that scenario.

Example 2.5.12. Let $\mathcal{F} = [4, 4, 6, 6]$ and $\delta = 4$. Then $\nu_{\min}(\mathcal{F}; 4) = 4 = c_1 < \nu_j(\mathcal{F}; 4)$ for $j = 1, 2, 3$. Furthermore, $c_1 \not\leq m - n + 1$, and therefore there exists no maximal $[\mathcal{F}; 4]$-code over $\overline{\mathbb{F}}$ by Theorem 2.5.11(b). As a consequence, maximal $[\mathcal{F}; 4]$-codes are not generic, which means that the probability of the event "4 randomly chosen matrices of shape $\mathcal{F}$ generate a maximal $[\mathcal{F}; 4]_q$-code" is bounded away from 1 (for growing q). We can be more precise. If $A_1, \ldots, A_4 \in \mathbb{F}_q[\mathcal{F}]$ generate a maximal $[\mathcal{F}; 4]_q$-code, then their submatrices consisting of the first 4 rows and first 2 columns generate a $[4 \times 2; 2]_q$-MRD code. In Proposition 2.6.3 we will see that this happens with a probability less than 0.375. Thus the latter is an upper bound for the probability of maximal $[\mathcal{F}; 4]_q$-codes.

It is worth noting that in both parts of Theorem 2.5.11 the existence of a maximal $[\mathcal{F}; n]$-code over *some* algebraically closed field implies the existence of a maximal $[\mathcal{F}; n]$-code over *any* finite field $\mathbb{F}_q$. This is obvious in the situation of Theorem 2.5.11(a) because $\nu_{\min} = 1$, and for the case in 2.5.11(b) the existence of maximal $[\mathcal{F}; n]$-codes has been established in Example 2.1.17(c).

We summarize the previous results.

Corollary 2.5.13. *Let $\mathcal{F} = [c_1, \ldots, c_n]$ be an $m \times n$-Ferrers diagram. Then*

$$\text{maximal } [\mathcal{F}; n]\text{-codes are generic} \Longleftrightarrow (\mathcal{F}; n) \text{ is MDS-constructible.}$$

In particular, maximal $[m \times n; n]$-MRD codes are not generic whenever $n > 1$ (see also Example 2.5.7(b)). Moreover, if $(\mathcal{F}; n)$ is MDS-constructible then $\nu_{min}(\mathcal{F}; n) = 1$ or $\nu_{min}(\mathcal{F}; n) = \nu_0(\mathcal{F}; n) = c_1 < \nu_j(\mathcal{F}; n)$ for all $j > 0$.

We strongly believe that the equivalence is true for any rank $2 \leq \delta \leq n$ and note that "$\Leftarrow$" has already been established in Theorem 2.5.8. The case of general rank δ is much more interesting than $\delta = n$ as it allows for more MDS-constructible pairs $(\mathcal{F}; \delta)$; see the left Ferrers diagram in Figure 2.9.

We conclude this section with the following observation. In [13, Thm. 7] Etzion et al. provide in essence the same construction of maximal $[\mathcal{F}; \delta]$-codes over sufficiently large fields as in Theorem 2.5.8. However, their assumption is, on first sight, different from $(\mathcal{F}; \delta)$ being MDS-constructible. In Appendix B we show that these assumptions are actually equivalent.

2.6 Probabilities for Nongeneric Ferrers Diagram Codes

In this section we focus on the non-generic case and provide some upper bounds on the proportion of maximal $[\mathcal{F}; \delta]_q$-codes. In particular, in Theorem 2.6.6 we provide an upper bound for the proportion of MRD codes, which is exact for $[m \times 2; 2]_q$-MRD codes; see Corollary 2.6.5. These two results improve on [7, Cor. 6.2], where Byrne/Ravagnani show that the asymptotic proportion is upper bounded by $1/2$.

The main tool in our considerations is the following result about spectrum-free matrices.

Theorem 2.6.1. *The spectrum of a matrix $A \in \mathbb{F}_q^{n \times n}$ is defined as $\sigma(A) = \{\lambda \in \mathbb{F}_q \mid \lambda \text{ is an eigenvalue of } A\}$. We call A spectrum-free if $\sigma(A) = \emptyset$. Set*

$$s_n(q) = |\{A \in \mathbb{F}_q^{n \times n} \mid \sigma(A) = \emptyset\}|.$$

Set $\gamma_n(q) = |GL_n(\mathbb{F}_q)| = \prod_{j=0}^{n-1}(q^n - q^j)$ and $a_0(q) = 1$ and $a_j(q) = (-1)^j \prod_{\ell=1}^{j} \frac{1}{q^\ell - 1}$ for $j \geq 1$. Then the generating function of $s_n(q)/\gamma_n(q)$ satisfies

$$1 + \sum_{n=1}^{\infty} \frac{s_n(q)}{\gamma_n(q)} u^n = \frac{1}{1-u} \prod_{r \geq 1} \left(1 - \frac{u}{q^r}\right)^{q-1} \tag{2.11}$$

and

$$s_n(q) = \gamma_n(q) \left(\sum_{j=0}^{n} \sum_{\substack{i_1, \ldots, i_{q-1} \in \mathbb{N}_0: \\ i_1 + \ldots + i_{q-1} = j}} a_{i_1}(q) \cdot \ldots \cdot a_{i_{q-1}}(q) \right). \tag{2.12}$$

51

Furthermore, the proportion of spectrum-free matrices in $\mathbb{F}_q^{n\times n}$ behaves as follows:

$$\lim_{n\to\infty}\frac{s_n(q)}{q^{n^2}}=\prod_{r\geq 1}\left(1-\frac{1}{q^r}\right)^q=\lim_{n\to\infty}\left(\frac{\gamma_n(q)}{q^{n^2}}\right)^q\quad and\quad \lim_{q\to\infty}\frac{s_n(q)}{q^{n^2}}=\sum_{j=0}^n\frac{(-1)^j}{j!}.$$

(2.13)

One may note that the expression for $a_j(q)$ can be rewritten as $a_j(q)=1/(q;q)_j$, where $(q;q)_j$ is the q-Pochhammer symbol.

Proof. The main parts of the statements above are in [49] and [38]: Identity (2.11) is given in [38, p. 7] and (2.12) appears in [49, p. 176]. As for the limits in (2.13), note that (2.11) leads to $\lim_{n\to\infty}\frac{s_n(q)}{\gamma_n(q)}=\prod_{r\geq 1}\left(1-\frac{1}{q^r}\right)^{q-1}$ (see also [38, p. 8]). On the other hand, clearly $\frac{\gamma_n(q)}{q^{n^2}}=\prod_{r=1}^n\left(1-\frac{1}{q^r}\right)$. Taking the limit for $n\to\infty$ leads to the first parts of (2.13).

It remains to determine $\lim_{q\to\infty}\frac{s_n(q)}{q^{n^2}}$. Note first that

$$\lim_{q\to\infty}\frac{s_n(q)}{q^{n^2}}=\lim_{q\to\infty}\frac{s_n(q)}{\gamma_n(q)}=\lim_{q\to\infty}\sum_{j=0}^n b_j(q),\quad\text{where }b_j(q)=\sum_{i_1+\ldots+i_{q-1}=j}a_{i_1}(q)\cdots a_{i_{q-1}}(q).$$

Hence it suffices to consider $\lim_{q\to\infty}b_j(q)$. To do so, we need the type of the weak compositions involved in the definition of $b_j(q)$. We say that a weak composition $i_1+\ldots+i_{q-1}=j$ is of type $(t_1,\ldots,t_j)$ if $t_k=|\{l\in[q-1]:i_l=k\}|$ for $k\in[j]$. Then the number of weak compositions of j of type $(t_1,\ldots,t_j)$ is given by $\frac{\prod_{i=1}^{t_1+\ldots+t_j}(q-i)}{t_1!\cdot\ldots\cdot t_j!}$, and thus

$$b_j(q)=\sum_{t_\ell\in\mathbb{N}_0:\,t_1+2t_2+\ldots+jt_j=j}c(t_1,\ldots,t_j;q),$$

where

$$c(t_1,\ldots,t_j;q):=\frac{\prod_{i=1}^{t_1+\ldots+t_j}(q-i)}{t_1!\cdot\ldots\cdot t_j!}\cdot\prod_{k=1}^j(a_k(q))^{t_k}=\frac{\prod_{i=1}^{t_1+\ldots+t_j}(q-i)}{t_1!\cdot\ldots\cdot t_j!}\cdot\prod_{k=1}^j\left(\frac{(-1)^k}{\prod_{i=1}^k(q^i-1)}\right)^{t_k}.$$

As a polynomial in q, the degree of the numerator of $c(t_1,\ldots,t_j;q)$ is $t_1+\ldots+t_j$, and the degree of the denominator is $\sum_{k=1}^j t_k\binom{k+1}{2}$. Notice that

$$\sum_{k=1}^j t_k\binom{k+1}{2}\geq\sum_{k=1}^j t_k\cdot k=j\geq t_1+\ldots+t_j$$

with equality in both steps if and only if $t_1=j$ and $t_2=\ldots=t_j=0$. Therefore

$$\lim_{q\to\infty}b_j(q)=\lim_{q\to\infty}c(j,0,\ldots,0;q)=\lim_{q\to\infty}\frac{\prod_{i=1}^j(q-i)}{j!}\cdot\left(\frac{-1}{q-1}\right)^j=\frac{(-1)^j}{j!}.$$

All of this shows that $\lim_{q\to\infty}\frac{s_n(q)}{q^{n^2}}=\lim_{q\to\infty}\sum_{j=0}^n b_j(q)=\sum_{j=0}^n\frac{(-1)^j}{j!}$.　　$\square$

Let us have a closer look at the limit in (2.13).

Remark 2.6.2. (a) The infinite product $\pi(q) := \prod_{r \geq 1} \left(1 - \frac{1}{q^r}\right)^q$ takes, for instance, the following approximate values:

q	2	3	5	31	179
$\pi(q)$	0.0833986	0.175735	0.254108	0.349996	0.364794

It is not hard to show that

$$\lim_{q \to \infty} (1 - 1/q^r)^q = \begin{cases} 1/e, & \text{if } r = 1, \\ 1, & \text{if } r > 1, \end{cases}$$

and thus $\lim_{q \to \infty} \pi(q) = 1/e \approx 0.36788$.

(b) By (2.13) we may approximate $\frac{s_n(q)}{q^{n^2}}$ by $\left(\frac{\gamma_n(q)}{q^{n^2}}\right)^q$. This is already a very good approximation for small values of n (for instance, $\left|\left(\frac{\gamma_n(q)}{q^{n^2}}\right)^q - \frac{s_n(q)}{q^{n^2}}\right| \leq 0.000081$ for $n = 7$ and $q = 3$). Since $\frac{s_n(q)}{q^{n^2}}$ is the fraction of spectrum-free matrices and $\left(\frac{\gamma_n(q)}{q^{n^2}}\right)^q$ the fraction of q-tuples of invertible matrices within $(\mathbb{F}_q^{n \times n})^q$, the approximation may be interpreted as follows: for any randomly chosen matrices A and $A_1, \ldots, A_q \in \mathbb{F}_q^{n \times n}$,

$$\text{Prob}\,(\lambda I - A \text{ is nonsingular for all } \lambda \in \mathbb{F}_q) \approx \text{Prob}\,(A_1, \ldots, A_q \text{ are nonsingular}).$$

That is, the q dependent matrices $\lambda I - A$, $\lambda \in \mathbb{F}_q$, behave just like q independently chosen matrices $A_1, \ldots, A_q$ (with respect to nonsingularity). However, computer experiments show that for two randomly chosen matrices $A, B \in \mathbb{F}^{n \times n}$ the probability that all $q^2 + q + 1$ dependent matrices $\lambda I + \alpha A + \beta B$, where the first nonzero coefficient is normalized to 1, are nonsingular is much larger than $\left(\frac{\gamma_n(q)}{q^{n^2}}\right)^{q^2 + q + 1}$.

We turn now to MRD codes. We start with the case of $[m \times 2; 2]$-MRD codes. In this case $\nu_{\min} = \nu_0 = m < \nu_1$ and therefore Theorem 2.5.11(b) tells us that there exists no $[m \times 2; 2]$-MRD code over an algebraically closed field (which can also be seen from the proof below as there are no spectrum-free matrices over an algebraically closed field). Thus $[m \times 2; 2]$-MRD codes are not generic. In order to present an interval for the according probability, we will first consider normalized matrices in the sense described next, and thereafter relate the result to the proportion of MRD codes in the sense of Definition 2.5.1. Interestingly enough, we will see below that even though there are no MRD codes over the algebraic closure, the probability does not approach zero for growing field size.

Proposition 2.6.3. *Let* $\mathbb{F} = \mathbb{F}_q$ *and*

$$A_1 = \begin{pmatrix} 1 & a_1^1 \\ 0 & a_2^1 \\ \vdots & \vdots \\ 0 & a_m^1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & a_1^2 \\ 1 & a_2^2 \\ \vdots & \vdots \\ 0 & a_m^2 \end{pmatrix}, \quad \ldots, A_m = \begin{pmatrix} 0 & a_1^m \\ 0 & a_2^m \\ \vdots & \vdots \\ 1 & a_m^m \end{pmatrix} \in \mathbb{F}^{m \times 2},$$

where $a_1^1, \ldots, a_m^m$ are randomly chosen field elements. Set $\mathcal{C} = \langle A_1, \ldots, A_m \rangle$. Then

$$Prob\left(\mathcal{C} \text{ is an } [m \times 2; 2]\text{-MRD code}\right) = \frac{s_m(q)}{q^{m^2}}.$$

As a consequence, as $q \to \infty$ the probability approaches $\sum_{j=0}^m \frac{(-1)^j}{j!}$, which is in the interval $[0.333, 0.375]$ for all $m \geq 3$.

Proof. Recall that an $[m \times 2; 2]$-MRD code has dimension m. Clearly, the code $\mathcal{C}$ given in the proposition has dimension m and therefore we only have to discuss the rank distance. A general linear combination of the given matrices has the form

$$A(\lambda) := \sum_{\alpha=1}^m \lambda_\alpha A_\alpha = \begin{pmatrix} \lambda_1 & \sum_{\alpha=1}^m a_1^\alpha \lambda_\alpha \\ \vdots & \vdots \\ \lambda_m & \sum_{\alpha=1}^m a_m^\alpha \lambda_\alpha \end{pmatrix}.$$

Thus $A(\lambda) = (\lambda \mid M\lambda)$, where $\lambda = (\lambda_1, \ldots, \lambda_m)^\mathsf{T}$ and

$$M = \begin{pmatrix} a_1^1 & \cdots & a_1^m \\ \vdots & & \vdots \\ a_m^1 & \cdots & a_m^m \end{pmatrix} \in \mathbb{F}^{m \times m}. \tag{2.14}$$

As a consequence,

$$\mathrm{rk}(A(\lambda)) = 2 \text{ for all } \lambda \in \mathbb{F}^m \setminus 0 \iff \sigma(M) = \emptyset.$$

Now the result follows from the definition of $s_m(q)$ in Theorem 2.6.1 and from (2.13). $\qquad \square$

In order to relate the above probability, based on a sample space of normalized matrices, to the proportion of MRD codes as in Definition 2.5.1, we need the following lemma. A general version for arbitrary pairs $(\mathcal{F}; \delta)$ can be derived as well, but is not needed for the rest of this paper.

Lemma 2.6.4. *Consider $\mathcal{F} = [m] \times [n]$ and $\delta = n$, thus $\ell = 1$ and $N = \nu_{min}(\mathcal{F}; \delta) = m$. Recall the spaces W_q and $\hat{W}_q$ from (2.9). Denote by $A_i^{(1)}$ the first column of the matrix A_i and define*

$$V_q = \{(A_1, \ldots, A_m) \in (\mathbb{F}_q^{m \times n})^m \mid (A_1^{(1)}, \ldots, A_m^{(1)}) = I_m\} \subseteq W_q,$$
$$\hat{V}_q = \{(A_1, \ldots, A_m) \in V_q \mid d_{rk}\langle A_1, \ldots, A_m \rangle = n\} = \hat{W}_q \cap V_q.$$

Then the proportion of $[m \times n; n]$-MRD codes in the space of all m-dimensional $(m \times n)$-rank-metric codes is given by

$$\frac{|\hat{T}_q|}{|T_q|} = \frac{|\hat{W}_q|}{|W_q|} = \frac{|\hat{V}_q|}{|V_q|} \frac{\prod_{i=0}^{m-1}(q^{mn} - q^{i+m(n-1)})}{\prod_{i=0}^{m-1}(q^{mn} - q^i)}, \tag{2.15}$$

and thus $\lim_{q \to \infty} |\hat{T}_q|/|T_q| = \lim_{q \to \infty} |\hat{V}_q|/|V_q|$.

Proof. The stated identity for the limits is clear because the rightmost factor in (2.15) approaches 1 as $q \to \infty$. The first identity in (2.15) is already in (2.10), and thus we need to establish the second identity. Reading each matrix A_i columnwise as a vector in $\mathbb{F}^{mn}$, we may identify $(\mathbb{F}_q^{m \times n})^m$ with $\mathbb{F}_q^{mn \times m}$. Then

$$W_q = \{M \in \mathbb{F}_q^{mn \times m} \mid \mathrm{rk}(M) = m\} \quad \text{and} \quad V_q = \{(I_m \mid B)^\intercal \mid B \in \mathbb{F}_q^{m \times m(n-1)}\}.$$

Notice also that, thanks to $\delta = n$, the first columns of any tuple $(A_1, \ldots, A_m)$ in $\hat{W}_q$ are linearly independent. Thus $\hat{W}_q \subseteq \{(B_1 \mid B_2)^\intercal \mid B_1 \in \mathrm{GL}_m(\mathbb{F}_q), B_2 \in \mathbb{F}_q^{m \times m(n-1)}\}$. This shows that $|\hat{W}_q| = |\hat{V}_q|\gamma_m(q)$, where $\gamma_m(q) = |\mathrm{GL}_m(\mathbb{F}_q)|$. Furthermore, $|V_q| = q^{m^2(n-1)}$ and $|W_q| = \prod_{i=0}^{m-1}(q^{mn} - q^i)$. Using that $\gamma_m(q) = \prod_{i=0}^{m-1}(q^m - q^i)$, we arrive at

$$\frac{|\hat{W}_q|}{|W_q|} = \frac{|\hat{V}_q|}{|V_q|} \cdot \frac{\gamma_m(q)q^{m^2(n-1)}}{\prod_{i=0}^{m-1}(q^{mn} - q^i)} = \frac{|\hat{V}_q|}{|V_q|} \cdot \frac{\prod_{i=0}^{m-1}(q^{mn} - q^{i+m(n-1)})}{\prod_{i=0}^{m-1}(q^{mn} - q^i)}. \qquad \square$$

In the case where $\delta = n = 2$, the probability determined in Proposition 2.6.3 is the fraction $|\hat{V}_q|/|V_q|$, and thus (2.15) leads to the following proportion.

Corollary 2.6.5. *The proportion of $[m \times 2; 2]_q$-MRD codes within the space of all m-dimensional rank-metric codes in $\mathbb{F}_q^{m \times 2}$ is given by*

$$\frac{s_m(q)}{q^{m^2}} \cdot \frac{\prod_{i=0}^{m-1}(q^{2m} - q^{i+m})}{\prod_{i=0}^{m-1}(q^{2m} - q^i)},$$

and converges to $\sum_{j=0}^{m} \frac{(-1)^j}{j!}$ as $q \to \infty$.

For more general cases we obtain more conditions for the rank distance. Since these conditions are not independent events on the random entries, we can only provide upper bounds on the probability by restricting to a subset of independent events.

Theorem 2.6.6. *Let $\mathbb{F} = \mathbb{F}_q$, $\delta \in [n]$, and $\ell = n - \delta + 1$. For $(\alpha, \beta) \in [m] \times [\ell]$ let $B_{\alpha,\beta} = (a_{i,j}^{(\alpha,\beta)}) \in \mathbb{F}^{m \times (n-\ell)}$ be randomly chosen matrices and set*

$$A_{\alpha,\beta} = \big(\underbrace{0 \mid \cdots \mid 0 \mid e_\alpha \mid 0 \mid \cdots \mid 0}_{\ell \text{ columns}} \mid B_{\alpha,\beta}\big) \in \mathbb{F}^{m \times n},$$

where e_α, the α-th standard basis vector in $\mathbb{F}^m$, is in the β-th column. Then the rank-metric code $\mathcal{C} = \langle A_{\alpha,\beta} \mid (\alpha, \beta) \in [m] \times [\ell] \rangle$ satisfies

$$Prob\big(\mathcal{C} \text{ is an } [m \times n; \delta]\text{-MRD code}\big) \leq \left(\frac{s_m(q)}{q^{m^2}}\right)^{(\delta-1)\ell}.$$

Proof. Note that by construction the matrices $A_{1,1}, \ldots, A_{m,\ell}$ are linearly independent and thus $\dim \mathcal{C} = m\ell = m(n - \delta + 1)$, as desired. Hence it remains to discuss the

rank distance. In order to do so, we consider, for all fixed β, linear combinations of the form $\sum_{\alpha=1}^{m} \lambda_\alpha A_{\alpha,\beta}$. For $(\beta, j) \in [\ell] \times [\delta - 1]$ define

$$M_{\beta,j} = \begin{pmatrix} a_{1,j}^{(1,\beta)} & \cdots & a_{1,j}^{(m,\beta)} \\ \vdots & & \vdots \\ a_{m,j}^{(1,\beta)} & \cdots & a_{m,j}^{(m,\beta)} \end{pmatrix} \in \mathbb{F}^{m \times m}. \tag{2.16}$$

Thus $M_{\beta,j}$ consists of the j-th columns of $B_{1,\beta}, \ldots, B_{m,\beta}$. Let us now consider the linear combination $\sum_{\alpha=1}^{m} \lambda_\alpha A_{\alpha,\beta}$. After deleting the $\ell - 1$ zero columns, this matrix has the form

$$\left(\lambda \mid M_{\beta,1}\lambda \mid \ldots \mid M_{\beta,n-\ell}\lambda \right), \quad \text{where } \lambda = (\lambda_1, \ldots, \lambda_m)^\intercal. \tag{2.17}$$

As a consequence, $\mathrm{rk}\left(\sum_{\alpha=1}^{m} \lambda_\alpha A_{\alpha,\beta} \right) = \delta$ implies that λ is not an eigenvector of any $M_{\beta,j}$. Since this has to be true for all $\lambda \in \mathbb{F}^m \setminus 0$, we conclude that $\sigma(M_{\beta,j}) = \emptyset$ for all $j = 1, \ldots, \delta - 1$. All of this shows that if $\mathrm{d}_{\mathrm{rk}}(\mathcal{C}) = \delta$, then $\sigma(M_{\beta,j}) = \emptyset$ for all $(\beta, j) \in [\ell] \times [\delta - 1]$. Since the $\ell(\delta - 1)$ matrices $M_{\beta,j}$ are independently chosen, the probability of the latter is $(s_m(q)/q^{m^2})^{(\delta-1)\ell}$, as desired. $\qquad \square$

Note that in the above proof we ignore an abundance of further conditions on the data $a_{i,j}^{(\alpha,\beta)}$ and therefore the probability is in fact much smaller than the given upper bound. However, these additional conditions are not independent and therefore difficult to quantify.

Let us have a closer look at the case where $\delta = n$, thus $\ell = 1$. In this case the above proof tells us the following.

Corollary 2.6.7. *Consider the situation of Theorem 2.6.6 with $\delta = n$, thus $\ell = 1$. Then*

$\mathcal{C}$ is an $[m \times n; n]_q$-MRD code

$$\Longleftrightarrow \sigma\left(\sum_{j=1}^{n-1} \mu_j M_{1,j} \right) = \emptyset \text{ for all } (\mu_1, \ldots, \mu_{n-1}) \in \mathbb{F}_q^{n-1} \setminus 0.$$

Proof. Since $\delta = n$, the code $\mathcal{C}$ is given by $\{\sum_{\alpha=1}^{m} \lambda_\alpha A_{\alpha,1} \mid \lambda_\alpha \in \mathbb{F}_q\}$, and for any $\lambda = (\lambda_1, \ldots, \lambda_m) \in \mathbb{F}_q^m \setminus 0$ the matrix $A(\lambda) := \sum_{\alpha=1}^{m} \lambda_\alpha A_{\alpha,1}$ equals the matrix in (2.17). We thus obtain $\mathrm{rk}A(\lambda) = n$ iff $\mu_0 \lambda \neq \sum_{j=1}^{n-1} \mu_j M_{1,j}\lambda$ for all $(\mu_0, \ldots, \mu_{n-1}) \in \mathbb{F}_q^n \setminus 0$. This leads to the desired equivalence. $\qquad \square$

Example 2.6.8. For $[4 \times 3; 3]_q$-MRD codes we conducted computer experiments consisting of 10 million trials, each of which generated 2 random 4×4 matrices over $\mathbb{F}_q$, serving as $M_{1,1}$ and $M_{1,2}$ in the proof of Corollary 2.6.7. In each trial, we checked if all nontrivial linear combinations of these two matrices were spectrum-free – or equivalently, if the associated matrices $A_1, \ldots, A_4 \in \mathbb{F}_q^{4 \times 3}$ generated MRD codes. Table 2.1 presents, for various values of q, the estimated relative frequencies of spectrum-free subspaces $\langle M_{1,1}, M_{1,2} \rangle$. In other words, this estimates the proportion

Table 2.1: Estimated proportions for $[4 \times 3; 3]_q$-MRD codes

q	2	3	5	7	11
Upper Bound	0.008	0.0313	0.065	0.083	0.102
$|\hat{V}_q|/|V_q|$	0.0005357	0.0000689	0.0001913	0.00028	0.0003732
Proportion of MRD codes	0.000165	0.000039	0.000146	0.000234	0.000336

$|\hat{V}_q|/|V_q|$ from Lemma 2.6.4. Next, (2.15) tells us that multiplying these proportions by $\prod_{i=0}^{3}(q^{12} - q^{i+8})/(q^{12} - q^i)$ gives us the proportion of MRD codes inside the space of all 4-dimensional rank-metric codes in $\mathbb{F}_q^{4 \times 3}$. We also compare our findings with the upper bound given in Theorem 2.6.6. The frequency for $q = 2$ was performed by exhaustive search, instead of by random experiment.

We wish to point out that our results do not preclude the existence of parameter sets (m, n, δ) for which the proportion of $[m \times n; \delta]_q$-MRD codes approaches 0 as $q \to \infty$. In such a case, the non-MRD codes would be generic (and the MRD codes would be sparse in the language of [7]). Indeed, $[3 \times 3; 3]$-MRD codes are sparse as has been recently shown in [18].

We conclude this paper with, once again, the Ferrers diagram $\mathcal{F} = [1, 3, 3, 4]$ and $\delta = 3$.

Corollary 2.6.9. *Let $\mathbb{F} = \mathbb{F}_q$. Consider the 4×4-Ferrers diagram $\mathcal{F} = [1, 3, 3, 4]$ and let $\delta = 3$. Let*

$$A_1 = \begin{pmatrix} 1 & 0 & a_{13}^1 & a_{14}^1 \\ 0 & 0 & a_{23}^1 & a_{24}^1 \\ 0 & 0 & a_{33}^1 & a_{34}^1 \\ 0 & 0 & 0 & a_{44}^1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 1 & a_{13}^2 & a_{14}^2 \\ 0 & 0 & a_{23}^2 & a_{24}^2 \\ 0 & 0 & a_{33}^2 & a_{34}^2 \\ 0 & 0 & 0 & a_{44}^2 \end{pmatrix},$$

$$A_3 = \begin{pmatrix} 0 & 0 & a_{13}^3 & a_{14}^3 \\ 0 & 1 & a_{23}^3 & a_{24}^3 \\ 0 & 0 & a_{33}^3 & a_{34}^3 \\ 0 & 0 & 0 & a_{44}^3 \end{pmatrix}, \quad A_4 = \begin{pmatrix} 0 & 0 & a_{13}^4 & a_{14}^4 \\ 0 & 0 & a_{23}^4 & a_{24}^4 \\ 0 & 1 & a_{33}^4 & a_{34}^4 \\ 0 & 0 & 0 & a_{44}^4 \end{pmatrix}$$

be randomly chosen in $\mathbb{F}_q[\mathcal{F}]$. Then

$$Prob\left(\langle A_1, \ldots, A_4 \rangle \text{ is a maximal } [\mathcal{F}; 3]_q\text{-code}\right) \leq \frac{s_3(q)}{q^9} \prod_{i=2}^{4}\left(1 - \frac{1}{q^i}\right) \frac{q^7 - 2q^4 + q}{q^7}.$$

The right hand side tends to $1/3$ as $q \to \infty$.

Proof. Consider a linear combination $\lambda_2 A_2 + \lambda_3 A_3 + \lambda_4 A_4$. If this matrix has rank 3 for all $(\lambda_2, \lambda_3, \lambda_4) \neq 0$, then the submatrices

$$\begin{pmatrix} 1 & a_{13}^2 \\ 0 & a_{23}^2 \\ 0 & a_{33}^2 \end{pmatrix}, \quad \begin{pmatrix} 0 & a_{13}^3 \\ 1 & a_{23}^3 \\ 0 & a_{33}^3 \end{pmatrix}, \quad \begin{pmatrix} 0 & a_{13}^4 \\ 0 & a_{23}^4 \\ 1 & a_{33}^4 \end{pmatrix}$$

generate a $[3\times 2; 2]$-MRD code. The probability for this is given by $s_3(q)/q^9$ according to Proposition 2.6.3. Furthermore, the last columns of A_2, A_3, A_4 have to be linearly independent, and the according probability is $q^{-12}\prod_{i=0}^{2}(q^4 - q^i) = \prod_{i=2}^{4}(1 - q^{-i})$. Finally, the last two columns of A_1 have to be linearly independent, which has a probability of

$$\frac{(q^3 - 1)\big((q-1)q^3 + (q^3 - q)\big)}{q^7} = \frac{q^7 - 2q^4 + q}{q^7}.$$

Since the events are independent, we obtain the stated upper bound. $\qquad\square$

The probability $P_q := \text{Prob}\,(\langle A_1, \ldots, A_4\rangle$ is a maximal $[\mathcal{F}; 3]_q$-code) can be related to the proportion of maximal $[\mathcal{F}; 3]_q$-codes in the sense of Definition 2.5.1. Indeed, similarly to Lemma 2.6.4, one obtains $|\hat{T}_q|/|T_q| = P_q \prod_{i=0}^{3}(q^{11} - q^{i+7})/(q^{11} - q^i)$.

Example 2.6.10. Consider the scenario of the last corollary for $q = 2$ and $q = 3$. Then the upper bound for the probability is given by

$$\text{Prob}\,(\langle A_1, \ldots, A_4\rangle \text{ is a maximal } [\mathcal{F}; 3]_2\text{-code}) \leq 0.044,$$
$$\text{Prob}\,(\langle A_1, \ldots, A_4\rangle \text{ is a maximal } [\mathcal{F}; 3]_3\text{-code}) \leq 0.1376.$$

These estimates clearly leave out crucial conditions and therefore the true probabilities are much smaller. Indeed, using SageMath and testing 1,000,000 quadruples of random matrices of the above form shows that the probability is about 0.00042 for $q = 2$ and about 0.0041 for $q = 3$. For larger q the actual probability appears to be around 0.03. Yet, as we have seen in Example 2.1.16, it is not hard to construct maximal $[\mathcal{F}; 3]_q$-codes over any field $\mathbb{F}_q$.

2.7 Open Problems

We presented constructions of maximal $[\mathcal{F}; \delta]_q$-codes for various classes of pairs $(\mathcal{F}; \delta)$, but the general Conjecture 2.1.9 remains wide open. The difficulty of the problem may in part be due to its highly 'noncanonical' nature in the sense that solutions, for most pairs $(\mathcal{F}; \delta)$, depend on the choice of basis. This is also evidenced by the genericity results of the last two sections leading to very different situations depending on the pair $(\mathcal{F}; \delta)$. While we do not entirely exclude the existence of a universal approach to the construction of maximal Ferrers diagram codes, we believe that further methods tailored to specific types of pairs $(\mathcal{F}; \delta)$ are necessary to settle the conjecture. We list some specific questions that arise from our considerations.

(a) Can one classify pairs $(\mathcal{F}; \delta)$ according to the approachability of the construction problem? A first step would be the generalization of Corollary 2.5.13 to general rank $\delta \geq 2$, which would then tell us that maximal $[\mathcal{F}; \delta]$-codes are generic if and only if $(\mathcal{F}; \delta)$ is MDS-constructible.

(b) The proofs of Theorems 2.2.1 and 2.2.6 leave some freedom in the choice of the basis B. Can a suitable choice provide us with more specific maximal Ferrers diagram codes that can be exploited further, for instance, as in Example 2.1.16?

(c) Can one characterize the pairs $(\mathcal{F}; \delta)$ for which maximal $[\mathcal{F}; \delta]$-codes can be realized as subfield subcodes of $\mathbb{F}_{q^m}$-linear MRD codes with the same rank distance?

(d) Can maximal $[\mathcal{F}; \delta]_q$-codes be realized as subcodes of $\mathbb{F}_q$-linear MRD codes, for instance those presented in [11, 44, 51]? The simplest case may be $m = n = \delta$. In this case MRD codes are known as spreadsets in finite geometry and well studied.

(e) Can the constructions in Section 2.4 be generalized to other highly regular Ferrers shapes and other ranks?

(f) In [18] it has been shown that the asymptotic proportion of $[3 \times 3; 3]$-MRD codes approaches 0 as $q \to \infty$. Can one characterize parameter sets (m, n, δ) for which MRD codes are sparse? Are there pairs $(\mathcal{F}; \delta)$ for which the asymptotic proportion of maximal $[\mathcal{F}; \delta]$-codes approaches 0?

2.8 Classification of Solved Cases

We attempt to classify all $(\mathcal{F}; \delta)$ pairs for which there exists a known maximal $[\mathcal{F}; \delta]_q$ code over any finite field $\mathbb{F}_q$. There are an abundance of results related to this subject, so we try here to identify the $(\mathcal{F}; \delta)$ pairs which are still under question.

Omitted Information

Throughout, we let $\mathcal{F}$ be an $m \times n$ Ferrers diagram, and assume $m \geq n$. The case where $n > m$ is covered by symmetry. We say $\mathcal{F} = [c_1, \ldots, c_n]$, where c_t denotes the number of dots in column t of $\mathcal{F}$. In all cases we assume $c_1 \geq 1$ and $c_n = m$.

The $m \times n$ Ferrers diagrams are in bijection with integer lattice paths from $(0,0)$ to (m, n), consisting of m east steps and n north steps. Exactly n of these $m+n$ steps must be north steps, so there are $\binom{m+n}{n}$ such Ferrers diagrams. However, these include cases where the first row and rightmost column are not full. With the restrictions that $c_1 \geq 1$ and $c_n = m$, we instead consider the number of $(m-1) \times (n-1)$ bottom-left subdiagrams. The count then becomes $\binom{m+n-2}{n-1}$. For large m and n, this number rises quickly. We attempt to reduce this to a more manageable quantity by eliminating some large classes of solved cases.

- We omit pairs $(\mathcal{F}; 1)$, since these are trivially solved. The vector space $\mathbb{F}[\mathcal{F}]$ is a maximal $[\mathcal{F}; 1]$ code over any field F.

- We omit pairs $(\mathcal{F}; 2)$, since these are solved by [13, Theorem 2].

Hence we may restrict to cases where $m \geq n \geq \delta \geq 3$.

- We omit $(\mathcal{F}; \delta)$ whenever $\nu_{\min}(\mathcal{F}; \delta) = 0$, since these are vacuous cases.

- We omit $(\mathcal{F}; \delta)$ pairs for which $\nu_{\min}(\mathcal{F}; \delta) = 1$, since these cases are trivially solved by a single rank δ matrix with shape $\mathcal{F}$.

The next two omissions will cut down significantly on uninteresting cases.

- If $\mathcal{F}$ is an $m \times n$ diagram and $\nu_{\min}(\mathcal{F}; \delta) = m(n - \delta + 1) - (mn - |\mathcal{F}|)$, then a maximal $[\mathcal{F}; \delta]_q$ code can be obtained by restricting an $[m \times n; \delta]_q$ MRD code. We omit these cases.

- In lieu of [13, Theorem 3], we omit all $(\mathcal{F}; \delta)$ pairs such that $\mathcal{F}$ is an $m \times n$ Ferrers diagram and the rightmost $\delta - 1$ columns of $\mathcal{F}$ each have at least n dots.

The next omission removes some unsolved cases from the list, whenever a smaller diagram ought to be considered instead. This has been done to cut down significantly on the size of the catalog.

- If $\mathcal{F}$ has pending dots with respect to δ, then a smaller diagram may be considered instead, and we omit the pair $(\mathcal{F}; \delta)$.

Catalog of $(\mathcal{F}; \delta)$ pairs

We sort first by m, n, and δ respectfully in ascending order, then by $[c_1, \ldots, c_n]$ in lexicographic order. High-priority $(\mathcal{F}; \delta)$ pairs, including those which would imply solutions to others via reduction as in Remark 2.1.14, are marked by $\star$. Pairs whose solutions would be implied by a high-priority pair are considered to be low-priority, and are marked by $-$.

If the diagram you are looking for is not listed, first remove any pending dots. A smaller diagram (or the transpose of one) may be listed.

Table 2.2: 4×3 diagrams, $\delta = 3$

$\mathcal{F}$	δ	$\nu_{\min}$	Solution (if known)
$[2, 2, 4]$	3	2	Combine $[2 \times 2; 2]_q$ and $[2 \times 1; 1]_q$ MRD codes via the construction in [13, Theorem 9].

Table 2.3: 4×4 diagrams, $\delta = 3$

$\mathcal{F}$	δ	$\nu_{\min}$	Solution (if known)
$[1, 2, 3, 4]$	3	3	Staircase theorem. See Corollary 2.2.10.
$[1, 3, 3, 4]$	3	4	See [13, Example 7] and Example 2.1.16.

Table 2.4: 4×4 diagrams, $\delta = 4$

$\mathcal{F}$	δ	$\nu_{\min}$	Solution (if known)
$[2, 2, 4, 4]$	4	2	Combine two $[2 \times 2; 2]_q$ MRD codes via the construction in [13, Theorem 9].

Table 2.5: 5×4 diagrams, $\delta = 3$

$\mathcal{F}$	δ	$\nu_{\min}$	Solution (if known)
$[2, 2, 2, 5]$	3	3	Combine $[2 \times 3; 2]_q$ and $[3 \times 1; 1]_q$ MRD codes via the construction in [13, Theorem 9].
$[2, 2, 3, 5]$	3	4	–
$[2, 3, 3, 5]$	3	5	–
$[3, 3, 3, 5]$	3	6	$\star$

Table 2.6: 5×4 diagrams, $\delta = 4$

$\mathcal{F}$	δ	$\nu_{\min}$	Solution (if known)
$[2, 3, 3, 5]$	4	2	Combine a $[[2, 3, 3]; 3]_q$ code and a $[2 \times 1; 1]_q$ MRD code via the construction in [13, Theorem 9].
$[3, 3, 4, 5]$	4	3	$\star$

Table 2.7: 5×5 diagrams, $\delta = 3$

$\mathcal{F}$	δ	$\nu_{\min}$	Solution (if known)
$[1, 2, 2, 4, 5]$	3	5	Reduce from $[1, 2, 3, 4, 5]$.
$[1, 2, 3, 4, 5]$	3	6	Staircase theorem. See Corollary 2.2.10.
$[1, 2, 4, 4, 5]$	3	7	Reduce from $[1, 4, 4, 4, 5]$.
$[1, 3, 3, 4, 5]$	3	7	Reduce from $[1, 4, 4, 4, 5]$.
$[1, 3, 4, 4, 5]$	3	8	Reduce from $[1, 4, 4, 4, 5]$.
$[1, 4, 4, 4, 5]$	3	9	The rightmost $\delta - 1$ columns have at least $n - 1$ dots and $m - n + 1 \geq c_1$. See [13, Construction 2 and Theorem 8].

Table 2.8: 5×5 diagrams, $\delta = 4$

$\mathcal{F}$	δ	$\nu_{\min}$	Solution (if known)
$[1, 1, 3, 3, 5]$	4	2	Combine $[1 \times 2; 1]_q$, $[2 \times 2; 2]_q$, and $[2 \times 1; 1]_q$ MRD codes via the construction in [13, Theorem 9].
$[1, 2, 3, 4, 5]$	4	3	Recursive construction. See Theorem 2.4.2.
$[1, 3, 3, 5, 5]$	4	4	$\star$
$[1, 3, 4, 4, 5]$	4	4	Reduce from $[1, 4, 4, 4, 5]$.
$[1, 4, 4, 4, 5]$	4	5	The rightmost $\delta - 1$ columns have at least $n - 1$ dots and $m - n + 1 \geq c_1$. See [13, Construction 2 and Theorem 8].
$[2, 2, 2, 5, 5]$	4	3	Combine $[2 \times 3; 2]_q$ and $[3 \times 2; 2]_q$ MRD codes via the construction in [13, Theorem 9].
$[2, 2, 3, 5, 5]$	4	4	$\star$
$[2, 2, 4, 4, 5]$	4	4	$\star$
$[2, 3, 4, 5, 5]$	4	5	$-$
$[2, 4, 4, 5, 5]$	4	6	$\star$

Table 2.9: 5×5 diagrams, $\delta = 5$

$\mathcal{F}$	δ	$\nu_{\min}$	Solution (if known)
$[2, 2, 4, 5, 5]$	5	2	Combine a $[2 \times 2; 2]_q$ MRD code and a maximal $[[2, 3, 3]; 3]_q$ code via the construction in [13, Theorem 9].
$[2, 3, 3, 5, 5]$	5	2	Combine a maximal $[[2, 3, 3]; 3]_q$ code and a $[2 \times 2; 2]_q$ MRD code via the construction in [13, Theorem 9].
$[3, 3, 5, 5, 5]$	5	3	$\star$

Table 2.10: 6×4 diagrams, $\delta = 4$

$\mathcal{F}$	δ	$\nu_{\min}$	Solution (if known)
$[3, 3, 3, 6]$	4	3	Combine $[3 \times 3; 3]_q$ and $[3 \times 1; 1]_q$ MRD codes via the construction in [13, Theorem 9].

Table 2.11: 6×5 diagrams, $\delta = 3$

$\mathcal{F}$	δ	$\nu_{\min}$	Solution (if known)
$[2,2,2,2,6]$	3	4	Combine $[2 \times 4; 2]_q$ and $[4 \times 1; 1]_q$ MRD codes via the construction in [13, Theorem 9].
$[2,2,2,3,6]$	3	5	–
$[2,2,2,4,6]$	3	6	–
$[2,2,3,3,6]$	3	6	–
$[2,2,3,4,6]$	3	7	–
$[2,2,4,4,6]$	3	8	See Proposition 2.2.15.
$[2,3,3,3,6]$	3	7	–
$[2,3,3,4,6]$	3	8	–
$[2,3,4,4,6]$	3	9	–
$[2,4,4,4,6]$	3	10	–
$[3,3,3,3,6]$	3	8	–
$[3,3,3,4,6]$	3	9	–
$[3,3,4,4,6]$	3	10	–
$[3,4,4,4,6]$	3	11	–
$[4,4,4,4,6]$	3	12	$\star$

Table 2.12: 6×5 diagrams, $\delta = 4$

$\mathcal{F}$	δ	$\nu_{\min}$	Solution (if known)
$[1,3,3,4,6]$	4	4	$\star$
$[2,3,3,5,6]$	4	5	$\star$
$[2,3,4,4,6]$	4	5	–
$[2,4,4,4,6]$	4	6	$\star$
$[3,3,3,6,6]$	4	6	See Proposition 2.2.15.
$[3,3,4,5,6]$	4	6	–
$[3,4,4,5,6]$	4	7	–
$[4,4,4,4,6]$	4	7	–
$[4,4,4,5,6]$	4	8	$\star$

Table 2.13: 6×5 diagrams, $\delta = 5$

$\mathcal{F}$	δ	$\nu_{\min}$	Solution (if known)
$[2, 2, 4, 4, 6]$	5	2	Combine two $[2 \times 2; 2]_q$ MRD codes and a $[2 \times 1; 1]_q$ MRD code via the construction in [13, Theorem 9].
$[3, 3, 3, 6, 6]$	5	3	Combine $[3 \times 3; 3]_q$ and $[3 \times 2; 2]_q$ MRD codes via the construction in [13, Theorem 9].
$[3, 3, 4, 5, 6]$	5	3	$\star$
$[4, 4, 4, 6, 6]$	5	4	$\star$
$[4, 4, 5, 5, 6]$	5	4	$\star$

Table 2.14: 6×6 diagrams, $\delta = 3$

$\mathcal{F}$	δ	$\nu_{\min}$	Solution (if known)
$[1, 2, 2, 2, 5, 6]$	3	7	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 2, 2, 3, 5, 6]$	3	8	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 2, 2, 4, 5, 6]$	3	9	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 2, 2, 5, 5, 6]$	3	10	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 2, 3, 3, 5, 6]$	3	9	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 2, 3, 4, 5, 6]$	3	10	Reduce from $[1, 5, 5, 5, 5, 6]$. Alternatively, see the staircase theorem in Theorem 2.2.6.
$[1, 2, 3, 5, 5, 6]$	3	11	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 2, 4, 4, 5, 6]$	3	11	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 2, 4, 5, 5, 6]$	3	12	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 2, 5, 5, 5, 6]$	3	13	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 3, 3, 3, 5, 6]$	3	10	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 3, 3, 4, 5, 6]$	3	11	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 3, 3, 5, 5, 6]$	3	12	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 3, 4, 4, 5, 6]$	3	12	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 3, 4, 5, 5, 6]$	3	13	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 3, 5, 5, 5, 6]$	3	14	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 4, 4, 4, 5, 6]$	3	13	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 4, 4, 5, 5, 6]$	3	14	Reduce from $[1, 5, 5, 5, 5, 6]$.

Table 2.14: 6×6 diagrams, $\delta = 3$

$\mathcal{F}$	δ	$\nu_{\min}$	Solution (if known)
$[1, 4, 5, 5, 5, 6]$	3	15	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 5, 5, 5, 5, 6]$	3	16	The rightmost $\delta - 1$ columns have at least $n - 1$ dots and $m - n + 1 \geq c_1$. See [13, Construction 2 and Theorem 8].

Table 2.15: 6×6 diagrams, $\delta = 4$

$\mathcal{F}$	δ	$\nu_{\min}$	Solution (if known)
$[1, 1, 3, 4, 4, 6]$	4	5	–
$[1, 1, 4, 4, 4, 6]$	4	6	$\star$
$[1, 2, 3, 4, 5, 6]$	4	6	–
$[1, 2, 4, 4, 5, 6]$	4	7	$\star$
$[1, 3, 3, 4, 6, 6]$	4	7	–
$[1, 3, 3, 5, 5, 6]$	4	7	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 3, 4, 4, 6, 6]$	4	8	–
$[1, 3, 4, 5, 5, 6]$	4	8	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 3, 5, 5, 5, 6]$	4	9	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 4, 4, 4, 6, 6]$	4	9	$\star$
$[1, 4, 4, 5, 5, 6]$	4	9	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 4, 5, 5, 5, 6]$	4	10	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 5, 5, 5, 5, 6]$	4	11	The rightmost $\delta - 1$ columns have at least $n - 1$ dots and $m - n + 1 \geq c_1$. See [13, Construction 2 and Theorem 8].
$[2, 2, 2, 2, 6, 6]$	4	4	Combine $[2 \times 4; 2]_q$ and $[4 \times 2; 2]_q$ MRD codes via the construction in [13, Theorem 9].
$[2, 2, 2, 3, 6, 6]$	4	5	Reduce from $[2, 2, 4, 4, 6, 6]$.
$[2, 2, 2, 4, 6, 6]$	4	6	Reduce from $[2, 2, 4, 4, 6, 6]$.
$[2, 2, 3, 3, 6, 6]$	4	6	Reduce from $[2, 2, 4, 4, 6, 6]$.
$[2, 2, 3, 4, 6, 6]$	4	7	Reduce from $[2, 2, 4, 4, 6, 6]$.
$[2, 2, 3, 5, 5, 6]$	4	7	–
$[2, 2, 4, 4, 6, 6]$	4	8	See Example 2.2.16 or Proposition 2.2.15.

Table 2.15: 6×6 diagrams, $\delta = 4$

$\mathcal{F}$	δ	$\nu_{\min}$	Solution (if known)
$[2, 2, 4, 5, 5, 6]$	4	8	–
$[2, 2, 5, 5, 5, 6]$	4	9	$\star$
$[2, 3, 3, 5, 6, 6]$	4	8	–
$[2, 3, 4, 5, 6, 6]$	4	9	–
$[2, 3, 5, 5, 6, 6]$	4	10	–
$[2, 4, 4, 5, 6, 6]$	4	10	–
$[2, 4, 5, 5, 6, 6]$	4	11	–
$[2, 5, 5, 5, 6, 6]$	4	12	$\star$

Table 2.16: 6×6 diagrams, $\delta = 5$

$\mathcal{F}$	δ	$\nu_{\min}$	Solution (if known)
$[1, 1, 3, 4, 4, 6]$	5	2	Combine a $[1 \times 2; 1]_q$ MRD code, a maximal $[[2, 3, 3]; 3]_q$ code, and a $[2 \times 1; 1]_q$ MRD code via the construction in [13, Theorem 9].
$[1, 2, 3, 4, 5, 6]$	5	3	Staircase theorem. See Theorem 2.2.6.
$[1, 3, 3, 4, 6, 6]$	5	4	$\star$
$[1, 3, 3, 5, 5, 6]$	5	4	$\star$
$[1, 4, 4, 5, 6, 6]$	5	5	$\star$
$[1, 4, 5, 5, 5, 6]$	5	5	Reduce from $[1, 5, 5, 5, 5, 6]$.
$[1, 5, 5, 5, 5, 6]$	5	6	The rightmost $\delta - 1$ columns have at least $n - 1$ dots and $m - n + 1 \geq c_1$. See [13, Construction 2 and Theorem 8].
$[2, 2, 3, 5, 5, 6]$	5	4	$\star$
$[2, 2, 4, 4, 6, 6]$	5	4	$\star$
$[2, 3, 3, 5, 6, 6]$	5	5	$\star$
$[2, 3, 5, 5, 5, 6]$	5	5	$\star$
$[2, 4, 4, 6, 6, 6]$	5	6	$\star$
$[2, 4, 5, 5, 6, 6]$	5	6	–
$[2, 5, 5, 5, 6, 6]$	5	7	$\star$
$[3, 3, 3, 6, 6, 6]$	5	6	See Proposition 2.2.15.

Table 2.16: 6×6 diagrams, $\delta = 5$

$\mathcal{F}$	δ	$\nu_{\min}$	Solution (if known)
$[3, 3, 5, 5, 6, 6]$	5	6	$\star$
$[3, 4, 5, 6, 6, 6]$	5	7	$-$
$[3, 5, 5, 6, 6, 6]$	5	8	$\star$

Table 2.17: 6×6 diagrams, $\delta = 6$

$\mathcal{F}$	δ	$\nu_{\min}$	Solution (if known)
$[2, 2, 4, 4, 6, 6]$	6	2	Combine three $[2 \times 2; 2]_q$ MRD codes via the construction in [13, Theorem 9].
$[2, 3, 3, 5, 6, 6]$	6	2	$\star$
$[3, 3, 3, 6, 6, 6]$	6	3	Combine two $[3 \times 3; 3]_q$ MRD codes via the construction in [13, Theorem 9].
$[4, 4, 6, 6, 6, 6]$	6	4	$\star$

Appendices

Appendix A: Rank Distance and Gabidulin Codes

Proposition. *The rank distance $d_{rk}(A, B) = rk(A - B)$ is a metric.*

Proof. For $A, B, C \in \mathbb{F}_q^{m \times n}$, $d_{rk}(A, B)$ is clearly nonnegative, is zero if and only if $A = B$, and $d_{rk}(A, B) = d_{rk}(B, A)$. Furthermore, the triangle inequality

$$
\begin{aligned}
\mathrm{rk}(A - B) &\leq \mathrm{rk}(A - B \mid B - C) \\
&= \mathrm{rk}(A - C \mid B - C) \\
&\leq \mathrm{rk}(A - C) + \mathrm{rk}(B - C)
\end{aligned}
$$

is satisfied. $\qquad\square$

Proposition (Rank-Metric Singleton Bound)**.** *Let $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ be a (not necessarily linear) rank-metric code with $d_{rk}(\mathcal{C}) = \delta$. Then*

$$
|\mathcal{C}| \leq \min\{q^{n(m-\delta+1)}, q^{m(n-\delta+1)}\}.
$$

Proof. Without loss of generality, assume $n \leq m$. Then $m(n - \delta + 1) \leq n(m - \delta + 1)$.

We have $d_{rk}(M, N) \geq \delta$ for all $M, N \in \mathcal{C}$, $M \neq N$, hence $M - N$ has at least δ nonzero columns. Using the $\mathbb{F}_q$-isomorphism $\phi_B^{-1} : \mathbb{F}_q^{m \times n} \to \mathbb{F}_{q^m}^n$, we have $\phi_B^{-1}(\mathcal{C}) \subseteq \mathbb{F}_{q^m}^n$. Then $\phi_B^{-1}(M - N)$ has at least δ nonzero entries, hence in $\mathbb{F}_{q^m}^n$ we have $d_{\mathrm{Ham}}(\phi_B^{-1}(M), \phi^{-1}(N)) \geq \delta$. Then

$$
|\mathcal{C}| \leq (q^m)^{n-d+1}
$$

by [30, Theorem 2.4.1]. $\qquad\square$

Proposition. *If $\mathcal{C}$ is a Gabidulin code, then $\phi_B(\mathcal{C})$ is an MRD code.*

Proof. Let $n \leq m$ and let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a Gabidulin code with $\dim_{\mathbb{F}_{q^m}}(\mathcal{C}) = \ell$. Then $\mathcal{C} = \mathrm{rowsp}(G)$, where

$$
G = \begin{pmatrix} g_1 & \cdots & g_n \\ g_1^{q^1} & \cdots & g_n^{q^1} \\ \vdots & & \vdots \\ g_1^{q^{\ell-1}} & \cdots & g_n^{q^{\ell-1}} \end{pmatrix} \in \mathbb{F}_{q^m}^{\ell \times n}
$$

and $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$ are linearly independent. Let $f = (f_0, \ldots, f_{\ell-1}) \in \mathbb{F}_{q^m}^\ell$. We want to show that $\phi_B(fG)$ has rank at least $n - \ell + 1$. Put

$$
\hat{f} = f_0 x + f_1 x^q + f_2 x^{q^2} + \ldots + f_{\ell-1} x^{q^{\ell-1}}.
$$

Then

$$
fG = \begin{bmatrix} \hat{f}(g_1) & \cdots & \hat{f}(g_n) \end{bmatrix}.
$$

68

By Frobenius, $\hat{f} : \langle g_1, \ldots, g_n \rangle_{\mathbb{F}_q} \to \mathbb{F}_{q^m}$ is an $\mathbb{F}_q$-linear map. But $\hat{f}$ has at most $q^{\ell-1}$ roots, hence $\dim_{\mathbb{F}_q}(\ker \hat{f}) \le \ell - 1$. We then have

$$\mathrm{rk}(\phi_B(fG)) = \dim_{\mathbb{F}_q} \left\langle \hat{f}(g_1), \ldots, \hat{f}(g_n) \right\rangle_{\mathbb{F}_q} = \dim_{\mathbb{F}_q}(\mathrm{im}\hat{f}) \ge n - \ell + 1,$$

where the inequality follows from rank-nullity. We conclude that $\delta := \mathrm{d}_{\mathrm{rk}}(\phi_B(\mathcal{C})) \ge n - \ell + 1$. The Singleton bound gives the reverse inequality, so $\ell = n - \delta + 1$, and $\dim_{\mathbb{F}_q} \phi_B(\mathcal{C}) = m(n - \delta + 1)$. $\qquad\square$

The above proof also demonstrates that G has rank ℓ, since for nonzero $f \in \mathbb{F}_{q^m}^{\ell}$ we have $\mathrm{rk}(\phi_B(fG)) > 0$.

Appendix B: MDS-Constructibility

Proof of Theorem 2.5.8. Let F be a field with at least $\max\{|D_i \cap \mathcal{F}| - 1 \mid i = \delta, \ldots, m\}$ elements. We follow the construction in [22, Thm. 32]. Let $\mathcal{I} := \{i : |D_i \cap \mathcal{F}| - \delta + 1 > 0\} = \{i_1, \ldots, i_z\}$. For all $i \in \mathcal{I}$ set $n_i := |D_i \cap \mathcal{F}|$ and choose a matrix $G_i \in F^{(n_i - \delta + 1) \times n_i}$ such that every full size minor is nonzero. For finite fields this simply means that G_i is the generator matrix of an MDS code and thus exists due to our condition on the field size. If F is infinite such matrices also exist: consider the entries as distinct indeterminates over F. Then the full-size minors are distinct nonzero polynomials, and choosing a point outside the variety (over F) of these minors, provides the entries of the desired matrix. Now we have $\mathrm{wt}_{\mathrm{H}}(uG_i) \ge \delta$ for all $u \in F^{n_i - \delta + 1} \setminus \{0\}$, where $\mathrm{wt}_{\mathrm{H}}(v) = |\{j \mid v_j \ne 0\}|$ denotes the Hamming weight, just like for vectors over finite fields. For $(v_{i_1}, \ldots, v_{i_z}) \in \mathrm{rowsp}(G_{i_1}) \times \ldots \times \mathrm{rowsp}(G_{i_z})$ define $A := A(v_{i_1}, \ldots, v_{i_z}) \in F^{m \times n}$ as the matrix with the vector v_{i_j} at the positions of $D_{i_j} \cap \mathcal{F}$ (which has indeed cardinality n_{i_j}) and set all other entries equal to zero. Define

$$\mathcal{C} = \{A(v_{i_1}, \ldots, v_{i_z}) \mid (v_{i_1}, \ldots, v_{i_z}) \in \mathrm{rowsp}(G_{i_1}) \times \ldots \times \mathrm{rowsp}(G_{i_z})\}.$$

By construction $\mathcal{C} \subseteq F[\mathcal{F}]$ (note that we do not make use of dots of $\mathcal{F}$ outside the specified diagonals). Furthermore, $\dim \mathcal{C} = \sum_{i \in \mathcal{I}}(n_i - \delta + 1) = \sum_{i=\delta}^{m} \max\{|D_i \cap \mathcal{F}| - \delta + 1, 0\}$. Finally, $\mathrm{d}_{\mathrm{rk}}(\mathcal{C}) = \delta$, which can be seen as follows. Choose any nonzero matrix $A \in \mathcal{C}$. Let $t \in \mathcal{I}$ be maximal such that the t-th diagonal of A is nonzero. By construction this diagonal contains at least δ nonzero entries and therefore $\mathrm{rk}(A) \ge \delta$. The rest is obvious or follows from Theorem 2.5.4. $\qquad\square$

In the rest of this appendix we show that the assumption used in [13, Thm. 7] for the construction of maximal $[\mathcal{F}; \delta]$-codes over sufficiently large fields is equivalent to $(\mathcal{F}; \delta)$ being MDS-constructible. We need the following notions. Let $\alpha \in \{0, \ldots, \delta - 1\}$ be such that $\nu_{\min}(\mathcal{F}; \delta) = \nu_\alpha(\mathcal{F}; \delta)$. Denote by $\mathcal{F}_{(\alpha)}$ the Ferrers diagram obtained by deleting the first α rows and last $\delta - 1 - \alpha$ columns from $\mathcal{F}$. Thus $\nu_{\min}(\mathcal{F}; \delta) = |\mathcal{F}_{(\alpha)}|$. We call the diagonal D_s an *MDS diagonal* of $(\mathcal{F}; \delta)$ w.r.t. α if it satisfies:

(a) $|D_s \cap (\mathcal{F} \setminus \mathcal{F}_{(\alpha)})| = \delta - 1$. In other words, D_s has α dots in the first α rows and $\delta - 1 - \alpha$ dots in the last $\delta - 1 - \alpha$ columns of $\mathcal{F}$.

(b) There are no dots in $\mathcal{F}_{(\alpha)}$ below the diagonal D_s and there is at least one dot in $\mathcal{F}_{(\alpha)}$ on D_s.

It is shown in [13, Thm. 7] that if $(\mathcal{F}; \delta)$ has an MDS diagonal, then maximal $[\mathcal{F}; \delta]$-codes over sufficiently large fields can be constructed with the aid of MDS codes (similarly to the construction in Theorem 2.5.8). In fact we have

Proposition. *Given any pair $(\mathcal{F}; \delta)$. Then*

$$(\mathcal{F}; \delta) \text{ has an MDS diagonal} \Longleftrightarrow (\mathcal{F}; \delta) \text{ is MDS-constructible.}$$

Proof. Consider Figure B1 in which we indicate the row indexed by α and the column indexed by $n - \delta + 2 + \alpha$. Thus the lower left corner contains the Ferrers diagram $\mathcal{F}_{(\alpha)}$.
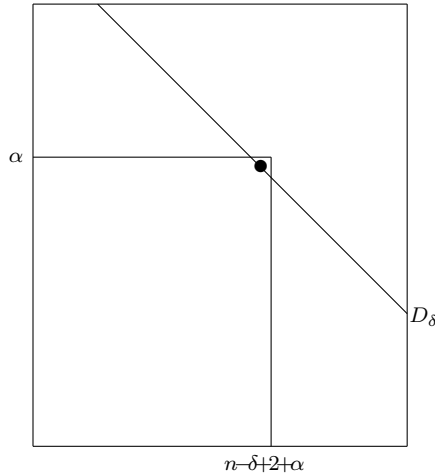

Figure B1: MDS diagonal vs. MDS-constructible

The upper right dot in $\mathcal{F}_{(\alpha)}$ is at position $(\alpha + 1, \, n - \delta + 1 + \alpha)$ and thus on the diagonal D_δ. Therefore the only diagonals potentially intersecting with $\mathcal{F}_{(\alpha)}$ are D_s where $s \geq \delta$. These are also the only diagonals that may contribute to $\sum_{i=\delta}^{m} \max\{|D_i \cap \mathcal{F}| - \delta + 1, \, 0\}$. We compute

$$(\mathcal{F}; \delta) \text{ is MDS-constructible} \Longleftrightarrow |\mathcal{F}_{(\alpha)}| = \sum_{s=\delta}^{m} \max\{|D_s \cap \mathcal{F}| - \delta + 1, \, 0\}$$

$$\Longleftrightarrow |D_s \cap \mathcal{F}| = \delta - 1 + |D_s \cap \mathcal{F}_{(\alpha)}| \text{ for all } s \text{ such that } D_s \cap \mathcal{F}_{(\alpha)} \neq \emptyset$$

$$\Longleftrightarrow D_s \text{ has } \delta - 1 \text{ dots outside } \mathcal{F}_{(\alpha)} \text{ for all } s \text{ such that } D_s \cap \mathcal{F}_{(\alpha)} \neq \emptyset$$

$$\Longleftrightarrow D_{\tilde{s}} \text{ is an MDS diagonal, where } \tilde{s} \text{ is maximal such that } D_{\tilde{s}} \cap \mathcal{F}_{(\alpha)} \neq \emptyset. \; \square$$

70

Bibliography

[1] J. Antrobus and H. Gluesing-Luerssen. Lexicodes over finite principal ideal rings. *Designs, Codes and Cryptography*, 86(11):2661–2676, 2018.

[2] J. Antrobus and H. Gluesing-Luerssen. Maximal Ferrers diagram codes: constructions and genericity considerations. *arXiv preprint arXiv:1804.00624v2. Accepted for publication in IEEE-IT*, 2018.

[3] E. Ballico. Linear subspaces of matrices associated to a Ferrers diagram and with a prescribed lower bound for their rank. *Linear Algebra and its Applications*, 483:30–39, 2015.

[4] E. Ben-Sasson, T. Etzion, A. Gabizon, and N. Raviv. Subspace polynomials and cyclic subspace codes. *IEEE Transactions on Information Theory*, 62(3):1157–1165, 2016.

[5] N. Bennenni, K. Guenda, and T. A. Gulliver. Greedy construction of DNA codes and new bounds. *arXiv preprint arXiv:1505.06262*, 2015.

[6] R. A. Brualdi and V. Pless. Greedy codes. In *Information Theory, 1993. Proceedings. 1993 IEEE International Symposium on*, pages 366–366. IEEE, 1993.

[7] E. Byrne and A. Ravagnani. Partition-balanced families of codes and asymptotic enumeration in coding theory. *arXiv preprint arXiv:1805.02049*, 2018.

[8] M. Canfell. Completion of diagrams by automorphisms and Bass' first stable range condition. *Journal of algebra*, 176(2):480–503, 1995.

[9] P. A. Chou, Y. Wu, and K. Jain. Practical network coding. In *Proceedings of the annual Allerton conference on communication control and computing*, volume 41 of number 1, pages 40–49. The University; 1998, 2003.

[10] J. Conway and N. Sloane. Lexicographic codes: error-correcting codes from game theory. *IEEE Transactions on Information Theory*, 32(3):337–348, 1986.

[11] J. de la Cruz, M. Kiermaier, A. Wassermann, and W. Willems. Algebraic structures of MRD codes. *Advances in Mathematics of Communications*, 10(3):499–510, 2016.

[12] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *Journal of Combinatorial Theory, Series A*, 25(3):226–241, 1978.

[13] T. Etzion, E. Gorla, A. Ravagnani, and A. Wachter-Zeh. Optimal Ferrers diagram rank-metric codes. *IEEE Transactions on Information Theory*, 62(4):1616–1630, 2016.

[14] T. Etzion and N. Silberstein. Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams. *IEEE Transactions on Information Theory*, 55(7):2909–2919, 2009.

[15] E. M. Gabidulin. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii*, 21(1):3–16, 1985.

[16] E. M. Gabidulin and N. I. Pilipchuk. Rank subcodes in multicomponent network coding. *Problems of information transmission*, 49(1):40–53, 2013.

[17] E. M. Gabidulin, N. I. Pilipchuk, and M. Bossert. Decoding of random network codes. *Problems of information transmission*, 46(4):300–320, 2010.

[18] H. Gluesing-Luerssen. On the sparseness of certain MRD codes. *arXiv preprint arXiv:1906.11691*, 2019.

[19] H. Gluesing-Luerssen, K. Morrison, and C. Troha. Cyclic orbit codes and stabilizer subfields. *Advances in Mathematics of Communications*, 9(2):177–197, 2015.

[20] H. Gluesing-Luerssen and C. Troha. Construction of subspace codes through linkage. *Advances in Mathematics of Communications*, 10(3):525–540, 2016.

[21] E. Gorla and A. Ravagnani. Partial spreads in random network coding. *Finite Fields and Their Applications*, 26:104–115, 2014.

[22] E. Gorla and A. Ravagnani. Subspace codes from Ferrers diagrams. *Journal of Algebra and Its Applications*, 16(07):1750131, 2017.

[23] M. Greferath and S. E. Schmidt. Finite-ring combinatorics and MacWilliams' equivalence theorem. *Journal of Combinatorial Theory, Series A*, 92(1):17–28, 2000.

[24] K. Guenda, T. A. Gulliver, and S. A. Sheikholeslam. Lexicodes over rings. *Designs, codes and cryptography*, 72(3):749–763, 2014.

[25] D. Heinlein and S. Kurz. Coset construction for subspace codes. *IEEE Transactions on Information Theory*, 63(12):7651–7660, 2017.

[26] T. Ho, R. Koetter, M. Medard, D. R. Karger, and M. Effros. The benefits of coding over routing in a randomized setting, 2003.

[27] T. Honold. Characterization of finite Frobenius rings. In volume 76, number 6, pages 406–415. Springer, 2001.

[28] T. Honold and I. Landjev. MacWilliams identities for linear codes over finite Frobenius rings. In *Finite Fields and Applications*, pages 276–292. Springer, 2001.

[29] T. Honold, I. Landjev, et al. Linear codes over finite chain rings. *Journal of Combinatorics*, 7(1):Research Paper 11, 2001.

[30] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge university press, 2010.

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

[32] T. Lam. A crash course on stable range, cancellation, substitution and exchange. *Journal of Algebra and Its Applications*, 3(03):301–343, 2004.

[33] T. Lam. *A First Course in Noncommutative Rings*, volume Graduate Text in Mathematics, 2nd edn, vol. 131. Springer, New York, 2001.

[34] V. Levenshtein. A class of systematic codes. *Doklady Akademii Nauk SSSR*, 131(5):1011–1014, 1960.

[35] S. Liu, Y. Chang, and T. Feng. Constructions for optimal Ferrers diagram rank-metric codes. *IEEE Transactions on Information Theory*, 2019.

[36] H. Mahdavifar and A. Vardy. Algebraic list-decoding of subspace codes. *IEEE Transactions on Information Theory*, 59(12):7814–7828, 2013.

[37] O. Milenkovic and N. Kashyap. On the design of codes for DNA computing. In *Coding and Cryptography*, pages 100–119. Springer, Berlin, 2006.

[38] K. Morrison et al. Integer sequences and matrices over finite fields. *J. Integer Seq*, 9(2):06–2, 2006.

[39] A. A. Nechaev. Finite principal ideal rings. *Matematicheskii Sbornik*, 133(3):350–366, 1973.

[40] A. Neri, A.-L. Horlemann-Trautmann, T. Randrianarisoa, and J. Rosenthal. On the genericity of maximum rank distance and Gabidulin codes. *Designs, Codes and Cryptography*, 86(2):341–363, 2018.

[41] S. Puchinger, J. R. né Nielsen, W. Li, and V. Sidorenko. Row reduction applied to decoding of rank-metric and subspace codes. *Designs, Codes and Cryptography*, 82(1-2):389–409, 2017.

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

[43] J. T. Schwartz. Probabilistic algorithms for verification of polynomial identities. In *International Symposium on Symbolic and Algebraic Manipulation*, pages 200–215. Springer, 1979.

[44] J. Sheekey. A new family of linear maximum rank distance codes. *Advances in Mathematics of Communications*, 10(3):475–488, 2016.

[45] N. Silberstein and A.-L. Trautmann. Subspace codes based on graph matchings, Ferrers diagrams, and pending blocks. *IEEE Transactions on Information Theory*, 61(7):3937–3953, 2015.

[46] D. Silva and F. R. Kschischang. Fast encoding and decoding of Gabidulin codes. In *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, pages 2858–2862. IEEE, 2009.

[47] D. Silva, F. R. Kschischang, and R. Koetter. A rank-metric approach to error control in random network coding. *IEEE transactions on information theory*, 54(9):3951–3967, 2008.

[48] R. Stanley. Enumerative combinatorics, vol. i. *Bull. Amer. Math. Soc*, 17:360–365, 1987.

[49] R. Stong. Some asymptotic results on finite vector spaces. *Adv. in Appl. Math*, 9(2):167–199, 1988.

[50] A.-L. Trautmann, F. Manganiello, M. Braun, and J. Rosenthal. Cyclic orbit codes. *IEEE Transactions on Information Theory*, 59(11):7386–7404, 2013.

[51] R. Trombetti and Y. Zhou. A new family of MRD codes in $\mathbb{F}_q^{2n \times 2n}$ with right and middle nuclei $\mathbb{F}_q^n$. *IEEE Transactions on Information Theory*, 2018.

[52] A. Van Zanten. Lexicographic order and linearity. *Designs, Codes and Cryptography*, 10(1):85–97, 1997.

[53] A. Van Zanten and I. N. Suparta. On the construction of linear q-ary lexicodes. *Designs, codes and Cryptography*, 37(1):15–29, 2005.

[54] A. Wachter-Zeh, V. Afanassiev, and V. Sidorenko. Fast decoding of Gabidulin codes. *Designs, codes and cryptography*, 66(1-3):57–73, 2013.

[55] J. A. Wood. Duality for modules over finite rings and applications to coding theory. *American journal of Mathematics*, 121(3):555–575, 1999.

[56] T. Zhang and G. Ge. Constructions of optimal Ferrers diagram rank metric codes. *Designs, Codes and Cryptography*, 87(1):107–121, 2019.

[57] R. Zippel. Probabilistic algorithms for sparse polynomials. In *International Symposium on Symbolic and Algebraic Manipulation*, pages 216–226. Springer, 1979.

Vita

Jared Evan Antrobus

Place of Birth:

- Edgewood, Kentucky

Education:

- University of Kentucky, Lexington, KY
  M.A. in Mathematics, Dec. 2016

- Northern Kentucky University, Highland Heights, KY
  B.S. in Mathematics & Statistics, May 2014
  summa cum laude

Professional Positions:

- Graduate Teaching Assistant, University of Kentucky Fall 2014–Spring 2019

Honors

- Enochs Scholarship in Algebra, University of Kentucky

- Max Steckler Fellowship, University of Kentucky

- Outstanding Senior in Mathematics, Northern Kentucky University

Publications & Preprints:

- Jared Antrobus and Heide Gluesing-Luerssen. "Maximal Ferrers Diagram Codes: Constructions and Genericity Considerations". Preprint 2018; arXiv: 1804.00624v2. Accepted for publication in IEEE-IT.

- Chris Christensen and Jared Antrobus and Edward Simpson. "Aligning JN-25 Messages in Depth Using Weights When the Code Groups Scan". Cryptologia 43.2 (2019): 84-137.

- Jared Antrobus and Heide Gluesing-Luerssen. "Lexicodes over finite principal ideal rings." Designs, Codes and Cryptography 86.11 (2018): 2661-2676.

- Chris Christensen and Jared Antrobus. "Cracking the Japanese JN-25 Cipher." Math Horizons 24.3 (2017): 22-25.

- Chris Christensen and Jared Antrobus. "The story of Mamba: Aligning messages against recovered additives." Cryptologia 39.3 (2015): 210-243.