Constructions, decoding and automorphisms of subspace codes

Trautmann, Anna-Lena

Abstract: Subspace codes are a family of codes used for (among others) random network coding, which is a model for multicast communication. These codes are defined as sets of vector spaces over a finite field. The main research problems arising in this area are the construction of codes with large cardinality for a given length and minimum distance and the development of fast and efficient decoding algorithms for these codes. In this thesis we address both of these problems and improve the known results from different aspects. We mainly focus on constant dimension codes, which is a subclass of subspace codes where each codeword has the same fixed dimension. First, we give new code constructions which improve the lower bounds on the size of constant dimension codes. To do so we introduce the concept of pending dots and pending blocks and use these to modify the lifted Ferrers diagram rank metric code construction. With our new constructions we can construct larger codes than known so far for certain parameter sets. Then we introduce orbit codes and show that these codes can be seen as the analogs of linear codes in classical block coding theory. We study the subclass of cyclic orbit codes in more detail and show what type of codes can be constructed as cyclic orbit codes. Moreover, we develop several decoding algorithms that are more efficient than other known algorithms for certain code parameters. The first two algorithms are minimum distance decoders while the last one is a more general list decoder. First we use the structure of the family of Desarguesian spread codes to decode these codes in some extension field of the underlying finite field. For the second algorithm we use the structure of orbit codes to come up with a syndrome type decoding algorithm (in analogy to syndrome decoding of linear block codes). Then we use the Plücker embedding to describe the balls of a given radius in the set of all vector spaces of a given dimension, which we can use to describe a list decoding algorithm in this embedding. Together with the fact that the family of lifted Gabidulin codes can be described by equations in the Plücker embedding, we come up with a list decoder for lifted Gabidulin codes that works by solving a system of equations in the Plücker embedding. Furthermore, we study the isometry classes and automorphism groups of subspace codes, both of which are of great interest from a theoretical point of view. We show what type of isometries for general subspace codes exist and then investigate the isometry classes and automorphism groups of some known constant dimension code constructions. Sogenannte Subspace Codes sind Codes, die unter anderem für Zufalls-Netzwerk- Kodierung (auch Random Network Coding genannt) gebraucht werden, was wiederum ein Modell für Multicast-Kommunikation ist. Diese Codes werden als Mengen von Vek- torräumen über einem endlichen Körper definiert. Die zwei Hauptprobleme, mit denen man sich in der Forschung beschäftigt, sind zum einen die Konstruktion solcher Codes und zum anderen die Entwicklung von dazugehörigen effizienten Dekodieralgorithmen. In der vorliegenden Arbeit befassen wir uns mit beiden Problemen und verbessern die bereits bekannten Ergebnisse aus verschiedenen Aspekten. Dabei konzentrieren wir uns hauptsächlich auf Constant Dimension Codes, die eine Unterklasse der Subspace Codes sind, wobei alle Elemente des Codes die gleiche Dimension haben. Zunächst erläutern wir neue Konstruktionen für Constant Dimension Codes, die für gegebene Parameter wie Länge und Minimaldistanz Codes mit mehr Elementen erzeugen als die bekannten Konstruktionen. Dafür führen wir sogenannte Pending Dots und Pending Blocks ein und benutzen diese, um die Lifted Ferrers Diagram Rank Metric Code-Konstruktion zu erweitern. Mit diesen neuen Konstruktionen können wir für bestimmte Parameter grössere Codes als bisher bekannt erzeugen. Danach beschäftigen wir uns mit Orbit Codes und zeigen, dass diese Codes als Analogons zu den linearen Codes in der klassischen Block-Kodierungstheorie angesehen werden können. Wir untersuchen ausführlich die Unterklasse der zyklischen Orbit Codes und

zeigen, welche Codes als zyklische Orbit Codes konstruiert werden können. Des weiteren entwickeln wir drei Dekodieralgorithmen, die im Vergleich zu den bereits bekannten Algorithmen für bestimmte Parameter effizienter arbeiten. Die zwei ersten Algorithmen sind Minimaldistanz-Dekodierer, der dritte hingegen ist ein allgemeinerer List-Dekodierer. Für den ersten Algorithmus nutzen wir die Struktur der sogenannten Desargueschen Spread Codes, um diese Codes in einem Erweiterungskörper des eigentlichen endlichen Körpers zu dekodieren. Der zweite Algorithmus ist ein Syndrom-Dekodieralgorithmus für Orbit Codes, ähnlich dem Syndrom-Dekodierer für lineare Block-Codes. Dann verwenden wir die Plücker-Einbettung, um Kugeln mit gegebenem Radius in der Menge aller Vektorräume mit gleicher Dimension zu beschreiben. Dies nutzen wir wiederum, um einen List-Dekodieralgorithmus in der Plücker-Einbettung zu beschreiben. Da man ausserdem die Familie der gelifteten Gabidulin-Codes mit Gleichungen in der Plücker-Einbettung beschreiben kann, erhalten wir einen List-Dekodierer für diese Codefamilie, der allein durch das Lösen eines Gleichungssystems funktioniert. Zusätzlich untersuchen wir die Isometrieklassen und Automorphismen von Sub- space Codes, was aus theoretischer Sicht interessante Ergebnisse liefert. Wir zeigen, welche Abbildungen Isometrien von generellen Subspace Codes sind und untersuchen die Iso-metrieklassen und Automorphismengruppen einiger bekannter Code-Konstruktionen.

Constructions, Decoding and Automorphisms of Subspace Codes

Dissertation

zur

Erlangung der naturwissenschaftlichen Doktorwürde
(Dr. sc. nat.)

vorgelegt der

Mathematisch-naturwissenschaftlichen Fakultät

der

Universität Zürich

von

Anna-Lena Trautmann

aus

Deutschland

Promotionskomitee

Prof. Dr. Joachim Rosenthal (Vorsitz)
Dr. Felix Fontein
Prof. Dr. Leo Storme (Begutachter)

Zürich, 2013

To Bärbel and Wolfgang.

Acknowledgements

I would like to heartily thank my advisor Joachim Rosenthal for his continuos guidance and support in all matters during my PhD time. His motivation, enthusiasm and knowledge were of big help for my research and the writing of this thesis.

Warm thanks also go to Leo Storme and Joan-Josep Climent for reviewing and commenting this thesis, as well as as everyone who proofread parts of it. All their help is well appreciated.

I owe my deepest gratitude to my coauthors Joachim, Felice, Michael, Natalia, Davide, Kyle, Felix and Thomas. This thesis would not have been possible without them.

Big appreciation goes to my various math friends for their motivation, advice and joy during these last years, especially Virtu, Felice, Urs, Tamara, Maike, Ivan, Elisa and Michael.

The financial support of the Swiss National Science Foundation and the University of Zurich is gratefully acknowledged.

Last but definitely not least I want to thank Johannes for his support in all non-scientific matters. You are my everything.

Anna-Lena Trautmann

Synopsis

Subspace codes are a family of codes used for (among others) random network coding, which is a model for multicast communication. These codes are defined as sets of vector spaces over a finite field. The main research problems arising in this area are the construction of codes with large cardinality for a given length and minimum distance and the development of fast and efficient decoding algorithms for these codes. In this thesis we address both of these problems and improve the known results from different aspects. We mainly focus on constant dimension codes, which is a subclass of subspace codes where each codeword has the same fixed dimension.

First, we give new code constructions which improve the lower bounds on the size of constant dimension codes. To do so we introduce the concept of pending dots and pending blocks and use these to modify the lifted Ferrers diagram rank metric code construction. With our new constructions we can construct larger codes than known so far for certain parameter sets. Then we introduce orbit codes and show that these codes can be seen as the analogs of linear codes in classical block coding theory. We study the subclass of cyclic orbit codes in more detail and show what type of codes can be constructed as cyclic orbit codes.

Moreover, we develop several decoding algorithms that are more efficient than other known algorithms for certain code parameters. The first two algorithms are minimum distance decoders while the last one is a more general list decoder. First we use the structure of the family of Desarguesian spread codes to decode these codes in some extension field of the underlying finite field. For the second algorithm we use the structure of orbit codes to come up with a syndrome type decoding algorithm (in analogy to syndrome decoding of linear block codes). Then we use the Plücker embedding to describe the balls of a given radius in the set of all vector spaces of a given dimension, which we can use to describe a list decoding algorithm in this embedding. Together with the fact that the family of lifted Gabidulin codes can be described by equations in the Plücker embedding we come up with a list decoder for lifted Gabidulin codes that works by solving a system of equations in the Plücker embedding.

Furthermore, we study the isometry classes and automorphism groups of subspace codes, both of which are of great interest from a theoretical point of view. We show what type of isometries for general subspace codes exist and then investigate the isometry classes and automorphism groups of some known constant dimension code constructions.

Übersicht

Sogenannte Subspace Codes sind Codes, die unter anderem für Zufalls-Netzwerk-Kodierung (auch Random Network Coding genannt) gebraucht werden, was wiederum ein Modell für Multicast-Kommunikation ist. Diese Codes werden als Mengen von Vektorräumen über einem endlichen Körper definiert. Die zwei Hauptprobleme, mit denen man sich in der Forschung beschäftigt, sind zum einen die Konstruktion solcher Codes und zum anderen die Entwicklung von dazugehörigen effizienten Dekodieralgorithmen. In der vorliegenden Arbeit befassen wir uns mit beiden Problemen und verbessern die bereits bekannten Ergebnisse aus verschiedenen Aspekten. Dabei konzentrieren wir uns hauptsächlich auf Constant Dimension Codes, die eine Unterklasse der Subspace Codes sind, wobei alle Elemente des Codes die gleiche Dimension haben.

Zunächst erläutern wir neue Konstruktionen für Constant Dimension Codes, die für gegebene Parameter wie Länge und Minimaldistanz Codes mit mehr Elementen erzeugen als die bekannten Konstruktionen. Dafür führen wir sogenannte Pending Dots und Pending Blocks ein und benutzen diese, um die Lifted Ferrers Diagram Rank Metric Code-Konstruktion zu erweitern. Mit diesen neuen Konstruktionen können wir für bestimmte Parameter grössere Codes als bisher bekannt erzeugen. Danach beschäftigen wir uns mit Orbit Codes und zeigen, dass diese Codes als Analogons zu den linearen Codes in der klassischen Block-Kodierungstheorie angesehen werden können. Wir untersuchen ausführlich die Unterklasse der zyklischen Orbit Codes und zeigen, welche Codes als zyklische Orbit Codes konstruiert werden können.

Des weiteren entwickeln wir drei Dekodieralgorithmen, die im Vergleich zu den bereits bekannten Algorithmen für bestimmte Parameter effizienter arbeiten. Die zwei ersten Algorithmen sind Minimaldistanz-Dekodierer, der dritte hingegen ist ein allgemeinerer List-Dekodierer. Für den ersten Algorithmus nutzen wir die Struktur der sogenannten Desargueschen Spread Codes, um diese Codes in einem Erweiterungskörper des eigentlichen endlichen Körpers zu dekodieren. Der zweite Algorithmus ist ein Syndrom-Dekodieralgorithmus für Orbit Codes, ähnlich dem Syndrom-Dekodierer für lineare Block-Codes. Dann verwenden wir die Plücker-Einbettung, um Kugeln mit gegebenem Radius in der Menge aller Vektorräume mit gleicher Dimension zu beschreiben. Dies nutzen wir wiederum, um einen List-Dekodieralgorithmus in der Plücker-Einbettung zu beschreiben. Da man ausserdem die Familie der gelifteten Gabidulin-Codes mit Gleichungen in der Plücker-Einbettung beschreiben kann, erhalten wir einen List-Dekodierer für diese Codefamilie, der allein durch das Lösen eines Gleichungssystems funktioniert.

Zusätzlich untersuchen wir die Isometrieklassen und Automorphismen von Subspace Codes, was aus theoretischer Sicht interessante Ergebnisse liefert. Wir zeigen, welche Abbildungen Isometrien von generellen Subspace Codes sind und untersuchen die Isometrieklassen und Automorphismengruppen einiger bekannter Code-Konstruktionen.

Contents

Introduction **1**

1 Preliminaries **3**

1.1 Random Linear Network Coding 3

1.2 Error-Correction and Decoding 5

1.3 Bounds on the Size of Constant Dimension Codes 8

1.4 Finite Fields and Irreducible Polynomials 11

2 Code Constructions **13**

2.1 Lifted Rank-Metric Codes 13

2.2 Lifted Ferrers Diagram Codes 18

2.3 The Pending Dots Extension 22

2.4 The Pending Blocks Constructions 27

2.4.1 Constructions for $(n, N, 2, k)_q$-Codes 29

2.4.2 Construction for $(n, N, k-1, k)_q$-Codes 34

2.5 Orbit Codes 39

2.5.1 Orbit Codes in $\mathcal{G}_q(k, n)$ 40

2.5.2 The Analogy to Linear Block Codes 42

2.5.3 Cardinality and Minimum Distance of Cyclic Orbit Codes . . . 43

2.5.4 Constructing Cyclic Orbit Codes 51

3 Decoding Subspace Codes **55**

3.1 Spread Decoding in Extension Fields 55

3.1.1 The Decoding Algorithm 57

3.2 Syndrome Decoding of Orbit Codes 63

3.2.1 A Decoder for Irreducible Cyclic Orbit Codes 64

3.3 List Decoding in the Plücker Embedding 68

3.3.1 The Plücker Embedding of $\mathcal{G}_q(k,n)$ 68
3.3.2 List Decoding of Lifted Rank-Metric Codes 74

4 Isometry Classes and Automorphism Groups **83**
4.1 Isometry of Subspace Codes 84
4.2 Isometry and Automorphisms of Known Code Constructions 88
4.2.1 Spread Codes 88
4.2.2 Orbit Codes 91
4.2.3 Lifted Rank-Metric Codes 92

Bibliography **97**

Introduction

Subspace codes or *projective space codes* are a class of codes that can be used for different applications in modern communications and technologies. The main interest in these codes arose when Kötter and Kschischang showed how to use them for non-coherent linear network coding [34], which is a model for multicast communication. In this model a source wants to send the same information to several receivers over a network channel. Many real-life applications of multicast can be found, a prominent example is data streaming over the Internet. The multicast network channel can be modeled by a directed graph with a source, several sinks as receivers and many inner nodes which each have incoming and outgoing edges. An example of the multicast model with four receivers can be found in Figure 1. If one allows each inner node to

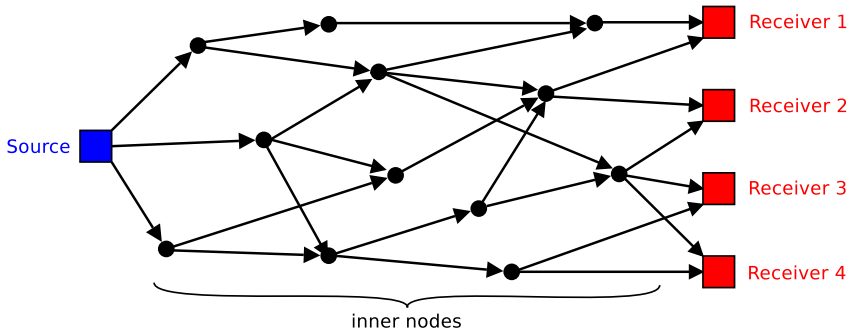


Figure 1: *The multicast model.*

transmit a random linear combination of its incoming information along the outgoing edges, one speaks of *random* or *non-coherent linear network coding*. This setting will be explained in more detail in Section 1.1.

Recently, it was shown, e.g. in [10, 45], how *distributed storage* follows the same model as multicast communication when the aspects of error correction and node repair are taken into account. The main idea is that one stores some given information, encoded in several small packets, in different storage nodes of a network. Then, whenever a node fails and does not return any information, one can use an erasure correcting code to reconstruct the information. But when a node fails in the sense that it returns corrupted information, one needs an error correcting code. In some applications one wants to do node repair every now and then, even if the stored information is not

needed at that moment. Then a new "repaired" node contacts several old nodes and stores a linear combination of their information. After several node repairs, this model is equivalent to random linear network coding, as explained above.

Moreover, subspace codes are useful for authentication purposes. In [61] it was shown how these codes can be used for validating if a sent message is from the correct sender or if it was intercepted and corrupted by an attacker. This is why these codes are also called *linear authentication codes* in this context.

In [42] Marshall, Rosenthal, Schipani and Trautmann explained yet another application for subspace codes in biometric authentication. The main point in this topic is that one needs to store highly delicate data, e.g. a fingerprint or an iris scan, and decide if another print or scan is similar enough to the original one to be from the same person, in which case we want to authenticate. For the decision if the committed data is similar enough, one can use an error-correcting code. In [42] the authors adapted the *fuzzy vault* scheme of [30] to work with subspace codes instead of BCH-codes and showed how this improves the security of such an authentication system.

In this thesis we give several new results on different aspects of subspace codes. For this we first explain the random linear network coding setting in detail and give some other preliminary results needed later in Chapter 1.

Chapter 2 deals with constructions of subspace codes. We first explain the known lifting constructions in Sections 2.1 and 2.2 and then introduce our new extensions of those in Sections 2.3 and 2.4. The last section of this chapter is devoted to orbit codes, which is a different way of constructing subspace codes, analogous to linear codes in classical block coding theory.

In Chapter 3 we focus on decoding algorithms for subspace codes. We explain two minimum distance decoders for different families of codes in Sections 3.1 and 3.2. Afterwards we introduce the Plücker embedding and show how it can be used for list decoding subspace codes. In Section 3.3.2 we derive an explicit list decoding algorithm for the family of lifted rank-metric codes.

Finally, we investigate the isometries and automorphism groups of subspace codes in Chapter 4. These are useful for comparing codes among each other and counting how many codes with equivalent coding theoretic properties there are. Moreover, automorphism groups have been found useful for certain decoding algorithms in classical coding theory, which might be done in a similar matter for subspace codes in future research. In Section 4.1 we derive the set of dimension-preserving isometries of subspace codes. Afterwards, in Section 4.2, we investigate the isometry classes and automorphism groups of some of the code constructions explained in Chapter 2.

Chapter 1
Preliminaries

1.1 Random Linear Network Coding

As already mentioned in the introduction, a general network channel is represented by a directed acyclic graph with three different types of vertices, namely *sources*, i.e. vertices with no incoming edges, *sinks*, i.e. vertices with no outgoing edges, and *inner nodes*, i.e. vertices with incoming and outgoing edges. One assumes that at least one source and one sink exist. The source is sometimes also called the *sender* and the sinks are also called the *receivers*. Under *linear* network coding the inner nodes are allowed to forward linear combinations of the incoming information vectors. The use of linear network coding possibly improves the transmission rate in comparison to just forwarding information at the inner nodes [1]. This can be illustrated in the example of the butterfly network (Figure 1.1): The source S wants to send the same information,

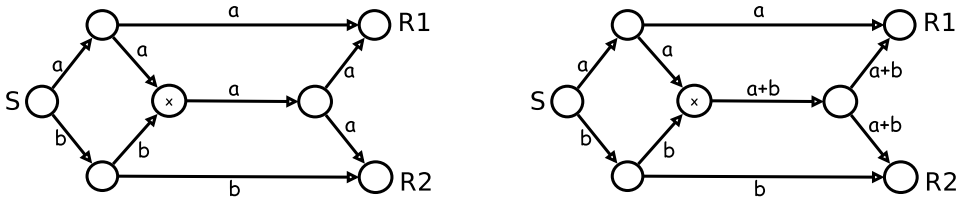


Figure 1.1: *The butterfly network under the forwarding and the network coding model.*

a and b, to both receivers $R1$ and $R2$. Under forwarding every inner node forwards the incoming information and thus has to decide on either a or b (in this example on a) at the bottleneck vertex, marked by x. Thus, $R1$ does not receive b. With linear network coding we allow the bottleneck vertex to send the sum of the two incoming informations, which allows both receivers to recover both a and b with a simple operation.

In this linear network coding setting, when the topology of the underlying network is unknown or time-varying, one speaks of *random* or *non-coherent* (linear) network coding. This setting was first studied in [28], and a mathematical model was introduced in [34], where the authors show that it makes sense to use vector spaces instead of vectors as codewords. In this model the source injects a basis of the respective codeword into

the network, and the inner nodes forward a random linear combination of their incoming vectors. Therefore, each sink receives linear combinations of the vectors injected by the source, which span the same vector space as the sent vectors, if no errors occurred during transmission.

In coding practice the base field is a finite field:

Definition 1.1: $\mathbb{F}_q$ denotes the *finite field* having q elements, where q is the power of a prime number p. Then p is called the *characteristic* of $\mathbb{F}_q$. $\mathbb{F}_q^\times := \mathbb{F}_q \backslash \{0\}$ denotes the set of all invertible elements of $\mathbb{F}_q$.

More information on finite fields and their construction will be given in Section 1.4.

Definition 1.2: We denote the set of all subspaces of $\mathbb{F}_q^n$ by $\mathcal{P}_q(n)$. The set of all k-dimensional subspaces of $\mathbb{F}_q^n$ is called the *Grassmannian* and is denoted by $\mathcal{G}_q(k,n)$.

Remark 1.3: Instead of $\mathcal{P}_q(n)$, one can also find the notation $\mathrm{PG}(n-1,q)$, i.e. the *projective geometry* of dimension $n-1$ over $\mathbb{F}_q$ (see e.g. [26]), in the literature for the set of all subspaces of $\mathbb{F}_q^n$. Since we mainly think of subspaces non-projectively in this work we prefer the notation $\mathcal{P}_q(n)$.

We can now give a simple definition of subspace codes.

Definition 1.4: A *subspace code* $\mathcal{C}$ is a subset of $\mathcal{P}_q(n)$. If all codewords of $\mathcal{C}$ have the same dimension, i.e. if $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ for some k, we call it a *constant dimension code*.

We represent subspaces by matrices such that the rows of these matrices form a basis of the respective subspace. The set of all $k \times n$-matrices with entries from $\mathbb{F}_q$ is denoted by $\mathbb{F}_q^{k\times n}$. Let $U \in \mathbb{F}_q^{k\times n}$ be a matrix of rank k and

$$\mathcal{U} = \mathrm{rs}(U) := \text{row space}(U) \in \mathcal{G}_q(k,n).$$

The row space is invariant under multiplication from the left with an invertible matrix $T \in \mathbb{F}_q^{k\times k}$,

$$\mathcal{U} = \mathrm{rs}(U) = \mathrm{rs}(TU).$$

Thus, there are several matrices that represent a given subspace. But for computational and implementation aspects it is important to have a unique representation of the codewords. Therefore, we use the *reduced row echelon form* (see e.g. [36]) of a matrix representing a subspace, which is unique for a given row space. Moreover, any $k \times n$-matrix can be transformed into reduced row echelon form by multiplication with some invertible matrix $T \in \mathbb{F}_q^{k\times k}$.

1.2 Error-Correction and Decoding

There are two types of errors that may occur during transmission, a decrease in dimension, which is called an *erasure*, and an increase in dimension, called an *insertion*. Assume $\mathcal{U} \in \mathcal{P}_q(n)$ was sent and erasures and insertions occurred during transmission, then the received word is of the type

$$\mathcal{R} = \bar{\mathcal{U}} \oplus \mathcal{E}$$

where $\bar{\mathcal{U}}$ is a subspace of $\mathcal{U}$ and $\mathcal{E} \in \mathcal{P}_q(n)$ is the error space, i.e. $\dim(\mathcal{U} \cap \mathcal{E}) = 0$.

Definition 1.5: A random network coding channel in which both insertions and erasures can happen is called an *operator channel*.

In order to have a notion of decoding capability of some code a suitable metric is required on the set $\mathcal{P}_q(n)$:

Theorem 1.6: *The* subspace distance d_S *is a metric on* $\mathcal{P}_q(n)$*, given by*

$$\begin{aligned} d_S(\mathcal{U},\mathcal{V}) &:= \dim(\mathcal{U}+\mathcal{V}) - \dim(\mathcal{U}\cap\mathcal{V}) \\ &= \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2\dim(\mathcal{U}\cap\mathcal{V}) \end{aligned}$$

for any $\mathcal{U},\mathcal{V} \in \mathcal{P}_q(n)$*. Another metric on* $\mathcal{P}_q(n)$ *is the* injection distance d_I*, defined as*

$$d_I(\mathcal{U},\mathcal{V}) := \max\{\dim(\mathcal{U}),\dim(\mathcal{V})\} - \dim(\mathcal{U}\cap\mathcal{V}).$$

PROOF: The proof that the subspace distance is a metric on $\mathcal{P}_q(n)$ can be found in [34]. For the injection distance it is easy to see that $d_I(\mathcal{U},\mathcal{U}) = 0$ and $d_I(\mathcal{U},\mathcal{V}) \geqslant 0$ for any $\mathcal{U},\mathcal{V} \in \mathcal{P}_q(n)$. It remains to show the triangle inequality:

$$\begin{aligned} & d_I(\mathcal{U},\mathcal{V}) + d_I(\mathcal{V},\mathcal{W}) \\ =& \frac{1}{2}(d_S(\mathcal{U},\mathcal{V}) + d_S(\mathcal{V},\mathcal{W})) + \max\{\dim(\mathcal{U}),\dim(\mathcal{V})\} + \max\{\dim(\mathcal{V}),\dim(\mathcal{W})\} \\ & - \frac{1}{2}(\dim(\mathcal{U}) + 2\dim(\mathcal{V}) + \dim(\mathcal{W})) \\ \geqslant& \frac{1}{2}d_S(\mathcal{U},\mathcal{W}) + \max\{\dim(\mathcal{U}),\dim(\mathcal{V})\} + \max\{\dim(\mathcal{V}),\dim(\mathcal{W})\} \\ & - \frac{1}{2}(\dim(\mathcal{U}) + 2\dim(\mathcal{V}) + \dim(\mathcal{W})) \\ \geqslant& \frac{1}{2}d_S(\mathcal{U},\mathcal{W}) + \max\{\dim(\mathcal{U}),\dim(\mathcal{W})\} - \frac{1}{2}(\dim(\mathcal{U}) + \dim(\mathcal{W})) \\ =& d_I(\mathcal{U},\mathcal{W}), \end{aligned}$$

i.e. $d_I(\mathcal{U},\mathcal{V}) + d_I(\mathcal{V},\mathcal{W}) \geqslant d_I(\mathcal{U},\mathcal{W})$ for any $\mathcal{U},\mathcal{V},\mathcal{W} \in \mathcal{P}_q(n)$ and thus d_I is a metric on $\mathcal{P}_q(n)$. A similar approach for this proof can be found in [47]. □

Remark 1.7: Note that for $\mathcal{U}, \mathcal{V} \in \mathcal{G}_q(k,n)$ (i.e. $\dim(\mathcal{U}) = \dim(\mathcal{V}) = k$) it holds that $d_S(\mathcal{U},\mathcal{V}) = 2d_I(\mathcal{U},\mathcal{V})$.

Definition 1.8: The *minimum injection distance* of a subspace code $\mathcal{C} \subseteq \mathcal{P}_q(n)$ is defined as

$$d_I(\mathcal{C}) = \min\{d_I(\mathcal{U},\mathcal{V}) \mid \mathcal{U},\mathcal{V} \in \mathcal{C}, \mathcal{U} \neq \mathcal{V}\}.$$

The minimum subspace distance is defined analogously.

Since we mainly investigate constant dimension codes in this thesis, by Remark 1.7 it does not matter which distance we use. In the following, if not stated differently, we always use the injection distance. All results can then be carried over to the subspace distance. We henceforth call a code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ with minimum injection distance δ and cardinality N an $(n, N, \delta, k)_q$-code.

Recall that the dual space $\mathcal{U}^\perp$ of some subspace $\mathcal{U} \in \mathcal{G}_q(k,n)$ is defined as

$$\mathcal{U}^\perp := \{v \in \mathbb{F}_q^n \mid vu^T = 0 \ \forall u \in \mathcal{U}\} \in \mathcal{G}_q(n-k,n).$$

Theorem 1.9 ([34]): *Let $\mathcal{C} \subseteq \mathcal{P}_q(n)$ be a subspace code. The* dual code *is defined as*

$$\mathcal{C}^\perp := \{\mathcal{U}^\perp \mid \mathcal{U} \in \mathcal{C}\}.$$

It holds that, if $\mathcal{C}$ is an $(n, N, \delta, k)_q$-code, then $\mathcal{C}^\perp$ is an $(n, N, \delta, n-k)_q$-code.

This theorem implies that for our studies of constant dimension codes, we may restrict ourselves to the case where $n \geqslant 2k$. For the remaining cases the dual codes will give us codes of the same cardinality and minimum distance.

We now focus on different decoding methods for subspace codes.

Definition 1.10: Consider a subspace code $\mathcal{C} \subseteq \mathcal{P}_q(n)$ and a received word $\mathcal{R} \in \mathcal{P}_q(n)$.

1. A *maximum likelihood decoder* decodes to a codeword $\mathcal{U} \in \mathcal{C}$ that maximizes the probability
$$P(\mathcal{R} \text{ received} \mid \mathcal{U} \text{ sent})$$
over all $\mathcal{U} \in \mathcal{C}$.
2. A *minimum distance decoder* chooses the closest codeword to the received word with respect to the subspace or injection distance. If there is more than one closest codeword, the decoder returns "failure".

Lemma 1.11: *Assume that the minimum (injection or subspace) distance of a subspace code $\mathcal{C} \in \mathcal{P}_q(n)$ is δ, and let $\mathcal{R} \in \mathcal{P}_q(n)$ be a received word. If there exists $\mathcal{U} \in \mathcal{C}$ whose distance from $\mathcal{R}$ is at most $\frac{\delta-1}{2}$, then $\mathcal{U}$ is the unique closest codeword and the minimum distance decoder will always decode to $\mathcal{U}$.*

PROOF: If the distance between $\mathcal{U}$ and $\mathcal{R}$ is at most $\frac{\delta-1}{2}$ and the distance between any two codewords is at least δ, then by the triangle inequality it holds that the distance between $\mathcal{R}$ and any other codeword must be at least $\delta - \frac{\delta-1}{2} = \frac{\delta+1}{2}$. This implies the statement. □

Let us assume that both the erasure and the insertion probability are less than some $\epsilon < \frac{1}{2}$. Then, over an operator channel where the insertion probability is equal to the erasure probability, and under the assumption that at most $\frac{\delta-1}{2}$ insertions and erasures happened during transmission, minimum distance decoding with respect to the subspace distance is equivalent to maximum likelihood decoding [34]. On the other hand, in an adversarial model it is more suitable to use a minimum distance decoder with respect to the injection distance to resemble maximum likelihood decoding [47].

Proposition 1.12: *Minimum subspace distance decoding is equivalent to minimum injection distance decoding when $\mathcal{C}$ is a constant dimension code.*

PROOF: Let $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$, $\mathcal{U}, \mathcal{V} \in \mathcal{C}$ and $\mathcal{R} \in \mathcal{P}_q(n)$ be the received word. Then, since $\dim(\mathcal{U}) = \dim(\mathcal{V})$, it holds that

$$\begin{aligned} & d_S(\mathcal{R},\mathcal{U}) \leqslant d_S(\mathcal{R},\mathcal{V}) \\ \iff & \dim(\mathcal{R}) + \dim(\mathcal{U}) - 2\dim(\mathcal{R}\cap\mathcal{U}) \leqslant \dim(\mathcal{R}) + \dim(\mathcal{V}) - 2\dim(\mathcal{R}\cap\mathcal{V}) \\ \iff & \dim(\mathcal{R}\cap\mathcal{U}) \geqslant \dim(\mathcal{R}\cap\mathcal{V}) \\ \iff & \max(\dim(\mathcal{R}),\dim(\mathcal{U})) - \dim(\mathcal{R}\cap\mathcal{U}) \leqslant \max(\dim(\mathcal{R}),\dim(\mathcal{V})) - \dim(\mathcal{R}\cap\mathcal{V}) \\ \iff & d_I(\mathcal{R},\mathcal{U}) \leqslant d_I(\mathcal{R},\mathcal{V}). \end{aligned}$$

Hence, $\mathcal{U}$ is the closest codeword to $\mathcal{R}$ with respect to the subspace distance if and only if $\mathcal{U}$ is the closest codeword to $\mathcal{R}$ with respect to the injection distance. □

Another important concept in coding theory is the problem of *list decoding*. The goal of list decoding is to come up with an algorithm which allows one to compute all codewords which are within some distance of some received subspace. For some $\mathcal{U} \in \mathcal{P}_q(n)$ we denote the ball of radius t with center $\mathcal{U}$ in $\mathcal{P}_q(n)$ by $B_t(\mathcal{U})$. If we want to describe the same ball inside $\mathcal{G}_q(k,n)$ we denote it by $B_t^k(\mathcal{U})$.

Definition 1.13: Given a subspace code $\mathcal{C} \subseteq \mathcal{P}_q(n)$ and a received word $\mathcal{R} \in \mathcal{P}_q(n)$, a *list decoder with error bound t* outputs the list of codewords $\mathcal{U}_1, \ldots, \mathcal{U}_m \in \mathcal{C}$ whose injection distance from $\mathcal{R}$ is at most t. In other words, the list is equal to the set

$$B_t(\mathcal{R}) \cap \mathcal{C}.$$

If $\mathcal{C}$ is a constant dimension code, then the output of the list decoder becomes $B_t^k(\mathcal{R}) \cap \mathcal{C}$.

1.3 Bounds on the Size of Constant Dimension Codes

To have some kind of measure how "good" a code is in terms of its rate and error-correction capability, one uses bounds on the size of codes for a given field, minimum distance and length. We now present some bounds for constant dimension codes. In this case not only the field size q, minimum injection distance δ and length n of the code is given, but also the constant dimension k.

Definition 1.14: We denote by $A_q(n, \delta, k)$ the maximal cardinality of a code $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ with minimum injection distance δ.

Two of the most natural bounds are the sphere packing and the sphere covering bound. In the former one takes the number of elements in the Grassmannian and divides it by the number of elements inside a ball of radius $\lfloor \frac{\delta-1}{2} \rfloor$ around some $\mathcal{U} \in \mathcal{G}_q(k, n)$, in the latter one divides by the cardinality of a ball of radius $\delta - 1$.
Proposition 1.15: *Sphere packing bound:*

$$A_q(n, \delta, k) \leqslant \frac{|\mathcal{G}_q(k, n)|}{\left|B^k_{\lfloor \frac{\delta-1}{2} \rfloor}(\mathcal{U})\right|} = \frac{\begin{bmatrix} n \\ k \end{bmatrix}_q}{\sum\limits_{i=0}^{\lfloor \frac{\delta-1}{2} \rfloor} q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} n-k \\ i \end{bmatrix}_q}$$

Sphere covering bound:

$$A_q(n, \delta, k) \geqslant \frac{|\mathcal{G}_q(k, n)|}{\left|B^k_{\delta-1}(\mathcal{U})\right|} = \frac{\begin{bmatrix} n \\ k \end{bmatrix}_q}{\sum\limits_{i=0}^{\delta-1} q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} n-k \\ i \end{bmatrix}_q}$$

Both of these bounds were first derived by Kötter and Kschischang in [34], where one can also find a proof for the formula of the cardinality of the balls. The gap between these two bounds is quite large, so one tries to find tighter bounds. We now present some other upper bounds that are lower than the sphere packing bound.

In the same paper [34] the authors define a puncturing operation on constant dimension codes and with that derive a bound in analogy to the classical Singleton bound:
Proposition 1.16:

$$A_q(n, \delta, k) \leqslant |\mathcal{G}_q(n - \delta + 1, k - \delta + 1)| = \begin{bmatrix} n-\delta+1 \\ n-k \end{bmatrix}_q$$

This bound is always lower and hence stronger than the sphere packing bound.

In [61] the authors Wang, Xing and Safavi-Naini found the following bound:
Proposition 1.17:

$$A_q(n,\delta,k) \leqslant \frac{\begin{bmatrix} n \\ k-\delta+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}_q}$$

This bound is also known as the anticode bound since it can be derived by noticing that $\mathcal{G}_q(k,n)$ is an association scheme and that one can then apply Delsarte's anticode bound [9]. This second point of view is due to Etzion and Vardy [16]. The anticode bound is always stronger than the Singleton-type bound.

One can always associate a binary constant weight block code C to a given constant dimension code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ as follows: The codewords of C are of length q^n-1, where each coordinate is associated to a (different) fixed non-zero element of $\mathbb{F}_q^n$. Each codeword $\mathcal{U}$ of $\mathcal{C}$ has an associated codeword u in C, where a 1-entry in u denotes that the corresponding vector of $\mathbb{F}_q^n$ is in $\mathcal{U}$, and a 0-entry denotes that this vector is not an element of $\mathcal{U}$. Hence, C has constant weight q^k-1 and one can apply the classical Johnson bounds (cf. [38]) to C. Then one also gets bounds on the associated code $\mathcal{C}$ as follows:
Proposition 1.18: *Johnson-type I bound:*

$$A_q(n,\delta,k) \leqslant \left\lfloor \frac{(q^{n-k}-q^{n-k-\delta})(q^n-1)}{(q^{n-k}-1)^2-(q^n-1)(q^{n-k-\delta}-1)} \right\rfloor$$

Johnson-type II bound:

$$\begin{aligned} A_q(n,\delta,k) &\leqslant \left\lfloor \frac{q^n-1}{q^k-1} A_q(n-1,\delta,k-1) \right\rfloor \\ &\leqslant \left\lfloor \frac{q^n-1}{q^k-1} \left\lfloor \dots \left\lfloor \frac{q^{n-k+\delta}-1}{q^\delta-1} \right\rfloor \dots \right\rfloor \right\rfloor \end{aligned}$$

These bounds were first shown by Xia and Fu in [62]. There it was also shown that these bounds always improve the anticode bound and hence also the other above mentioned bounds.

In the special case of $\delta = k$, i.e. codes of maximal minimum distance, Etzion and Vardy derived the following bound in [17]:
Proposition 1.19: *If $k \nmid n$, then*

$$A_q(n,k,k) \leqslant \left\lfloor \frac{q^n-1}{q^k-1} \right\rfloor - 1.$$

If one can find codes such that any of these bounds is attained with equality, it follows that one cannot find any larger codes for the same parameters.

Definition 1.20: We call a code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ with minimum injection distance δ *optimal* if it attains any of the upper bounds on the cardinality of constant dimension codes, i.e. if

$$|\mathcal{C}| = A_q(n, \delta, k).$$

Naturally, any general construction of constant dimension codes gives a new lower bound. Therefore we derive new and tighter lower bounds in Chapter 2.

For completeness we also want to mention at this point that there exist more bounds on the size of constant dimension codes under certain conditions. E.g. Etzion and Silberstein found some bounds on constant dimension codes that contain a lifted rank-metric code of a given size [15]. We show one of these bounds in Chapter 2 when we explain the respective constructions meeting that bound.

1.4 Finite Fields and Irreducible Polynomials

We need the following definitions and results on finite fields and irreducible polynomials over finite fields. For a more detailed introduction to finite fields the reader is referred to [31, 37].

Theorem 1.21 ([31, 37]): *1. A finite field $\mathbb{F}_q$ with q elements exists if and only if q is a power of some prime number p.*
2. For a given q the finite field $\mathbb{F}_q$ is unique (up to isomorphism).
3. For a prime number p the finite field $\mathbb{F}_p$ is isomorphic to $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$.

Recall that a polynomial $p(x) \in \mathbb{F}_q[x]$ is called *irreducible* if for any $a(x), b(x) \in \mathbb{F}_q[x]$

$$p(x) = a(x)b(x) \implies \deg(a(x)) = 0 \text{ or } \deg(b(x)) = 0.$$

Definition 1.22: Let $p(x) = p_0 + p_1 x + \ldots + p_{n-1}x^{n-1} + x^n$ be a monic irreducible polynomial of degree n over the finite field $\mathbb{F}_q$. Then the *companion matrix* M_p of $p(x)$ is given by

$$M_p := \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \ldots & 1 \\ -p_0 & -p_1 & -p_2 & \ldots & -p_{n-1} \end{pmatrix}.$$

Remark 1.23: In some literature the companion matrix of a polynomial is defined as the transpose of our previous definition. Nonetheless, all results related to companion matrices are analogous in both settings.

Theorem 1.24 ([31]): *Let $p(x) = p_0 + p_1 x + \ldots + p_{n-1}x^{n-1} + x^n$ be a monic irreducible polynomial of degree n over the finite field $\mathbb{F}_q$ and $\alpha \in \mathbb{F}_{q^n}$ a root of $p(x)$. Then the extension field $\mathbb{F}_{q^n}$ can be represented by*

$$\mathbb{F}_{q^n} \cong \mathbb{F}_q[x]/p(x) \cong \mathbb{F}_q[\alpha] \cong \mathbb{F}_q[M_p].$$

Lemma 1.25 ([37]): *For any finite field $\mathbb{F}_q$ the multiplicative group $\mathbb{F}_q^\times$ is cyclic, i.e. it can be generated by one element.*

An irreducible polynomial $p(x) \in \mathbb{F}_q[x]$ of degree n is called *primitive* if any of its roots is a multiplicative generator of $\mathbb{F}_{q^n}^\times$.

Lemma 1.26 ([37]): *If $p(x) \in \mathbb{F}_q[x]$ is a primitive polynomial, then the multiplicative group generated by M_p has order $q^n - 1$.*

In the setting of Lemma 1.26, the group generated by M_p is known as the *Singer*

group. This notation is used e.g. by Kohnert et al. in their subspace code construction [12, 33]. Elsewhere M_p is called *Singer cycle* or *cyclic projectivity* (e.g. in [26]).

The following fact is well-known and can easily be verified.

Theorem 1.27: *Let α be a root of a monic irreducible polynomial $p(x) \in \mathbb{F}_q[x]$ of degree n. Then $\mathbb{F}_{q^n} \cong \mathbb{F}_q[\alpha]$ can be seen as an n-dimensional vector space over $\mathbb{F}_q$. The map*

$$\begin{aligned} \phi^{(n)} : \mathbb{F}_q^n &\longrightarrow \mathbb{F}_{q^n} \cong \mathbb{F}_q[\alpha] \\ (u_1, \ldots, u_n) &\longmapsto \sum_{i=0}^{n-1} u_{i+1}\alpha^i. \end{aligned}$$

is an isomorphism. The analog holds for the other representations of $\mathbb{F}_{q^n}$.

Remark 1.28: In the finite field $\mathbb{F}_q[x]/p(x)$, the modular multiplication of an element $v(x) = v_0 + v_1 x + \ldots + v_{n-1}x^{n-1}$ by x always yields

$$v(x) \cdot x = -v_{n-1}p_0 + \sum_{i=1}^{n-1}(v_{i-1} - v_{n-1}p_i)x^i \mod p(x).$$

If we apply $\phi^{(n)^{-1}}$ to it, we get $\phi^{(n)^{-1}}(v(x) \cdot x) = (v_0, v_1, \ldots, v_{n-1})M_p$.

If we substitute the indeterminate x in the polynomials $v \in \mathbb{F}_q$ by the generator $\alpha \in \mathbb{F}_{q^n}^\times$, the modular multiplication with x corresponds to the multiplication with α and hence to multiplication with the companion matrix M_p:

Theorem 1.29 ([53]): *Let $p(x)$ be a monic irreducible polynomial over $\mathbb{F}_q$ of degree n and M_p its companion matrix. Furthermore let $\alpha \in \mathbb{F}_{q^n}^\times$ be a root of $p(x)$. Then the multiplication with M_p respectively α commutes with the mapping ϕ, i.e. for all $v \in \mathbb{F}_q^n$ we get*

$$\phi^{(n)}(vM_p) = \phi^{(n)}(v)\alpha.$$

We denote by $\mathrm{Aut}(\mathbb{F}_q) := \{\varphi : \mathbb{F}_q \to \mathbb{F}_q \mid \varphi \text{ is isomorphism}\}$ the *automorphism group* of the finite field $\mathbb{F}_q$. Furthermore, we denote by $\mathrm{Gal}(\mathbb{F}_{q^k}, \mathbb{F}_q)$ the *Galois group* of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$, i.e. the set of all automorphisms of $\mathbb{F}_{q^k}$ that fix the subfield $\mathbb{F}_q$.

Theorem 1.30 ([37]): *The distinct elements of $\mathrm{Gal}(\mathbb{F}_{q^k}, \mathbb{F}_q)$ are exactly the mappings $\varphi_1, \ldots, \varphi_k$, defined by $\varphi_j(x) = x^{q^j}$ for any $x \in \mathbb{F}_{q^k}$.*

Chapter 2
Code Constructions

In this chapter we introduce and explain several constructions for constant dimension codes. These constructions can be divided into two large classes, namely lifted matrix codes and orbit codes, where the first class contains different constructions, corresponding to the first four sections of this chapter. Inside each section we repeat known results and then state our improvements or other results related to them.

2.1 Lifted Rank-Metric Codes

There is a complete theory of matrix codes with the rank distance, which can be used to construct constant dimension codes. We now give a brief overview on the most important definitions and results of this topic.

Theorem 2.1 ([19]): *Let $A, B \in \mathbb{F}_q^{m\times n}$ be two matrices. It holds that*

$$d_R(A,B) := \operatorname{rank}(A-B)$$

defines a metric on $\mathbb{F}_q^{m\times n}$. It is called the rank distance.

Definition 2.2: A *linear rank-metric code* is simply a subspace of $\mathbb{F}_q^{m\times n}$. The minimum rank distance of a code $C \subseteq \mathbb{F}_q^{m\times n}$ is defined as

$$d_R(C) := \min\{d_R(A,B) \mid A, B \in C, A \neq B\}.$$

The following two theorems can be found in [19]:

Theorem 2.3: *Let $C \subseteq \mathbb{F}_q^{m\times n}$ be a linear rank-metric code with minimum rank distance δ. Then*

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

Theorem 2.4: *For any set of parameters $n, m \geqslant \delta \in \mathbb{N}$ and arbitrary field size there exist codes attaining the bound of Theorem 2.3. These codes are called* maximum rank distance (MRD) codes.

A general construction for MRD codes was given by Gabidulin in [19], which we will explain in the following. These codes are called *Gabidulin codes* and can be seen as the analogs of Reed-Solomon codes for the rank metric. Assume you want to construct an MRD code $C \subseteq \mathbb{F}_q^{m\times n}$ with minimum rank distance δ, where $m \geqslant n$. We can represent each column of a codeword as an element of the isomorphic extension field, i.e. $\mathbb{F}_{q^m} \cong \mathbb{F}_q^m$, and view the MRD code as a linear block code over $\mathbb{F}_{q^m}$. Let $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$. If the generator matrix of our code in extension field representation is of the form

$$G = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[1]} & g_2^{[1]} & \cdots & g_n^{[1]} \\ g_1^{[2]} & g_2^{[2]} & \cdots & g_n^{[2]} \\ \vdots & \vdots & \vdots & \vdots \\ g_1^{[n-\delta]} & g_2^{[n-\delta]} & \cdots & g_n^{[n-\delta]} \end{pmatrix},$$

where $[i] = q^i$, then the code in matrix representation has minimum rank distance δ and dimension $m(n-\delta+1)$, i.e. it is an MRD code. If you want to construct an MRD code $C \subseteq \mathbb{F}_q^{m\times n}$, where $m < n$, you can use the construction from before to construct the transpose elements of the code.

Example 2.5: Let $m = n = \delta = 2$ and α be a root of $x^2 + x + 1$ such that $\mathbb{F}_{2^2} = \mathbb{F}_2[\alpha]$. Moreover let $g_1 = 1, g_2 = \alpha$. Then the generator matrix is $G = (1\ \alpha)$ and the codewords are

$$(0\ 0) \cong \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, (1\ \alpha) \cong \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, (\alpha\ \alpha+1) \cong \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, (\alpha+1\ 1) \cong \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

We will now explain how to use MRD codes for the construction of constant dimension codes. To distinguish between them we denote matrices by normal font letters and subspaces by curly letters. In the same manner we denote rank-metric codes by C and subspace codes by $\mathcal{C}$.

Definition 2.6: For a given rank-metric code $C \subseteq \mathbb{F}_q^{k\times n}$ the set

$$\mathrm{lift}(C) := \left\{ \mathrm{rs}\begin{bmatrix} I_k & A \end{bmatrix} | A \in C \right\}$$

is called the *lifting* of C.

Theorem 2.7 ([48]): *If $C \subseteq \mathbb{F}_q^{k\times(n-k)}$ is an MRD code of minimum rank distance δ, then $\mathrm{lift}(C) \subseteq \mathcal{G}_q(k,n)$ is a constant dimension code with minimum injection distance δ. Moreover,*

$$|\mathrm{lift}(C)| = q^{(n-k)(k-\delta+1)}.$$

Note that, since we restrict ourselves to $n \geqslant 2k$, it holds that $k \leqslant n-k$. Hence, the cardinality formula in Theorem 2.7 follows directly from Theorem 2.3.

Remark 2.8: Lifting a Gabidulin code is analogous to the Reed-Solomon-like construction from Kötter and Kschischang [34]. We do not want to explain this construction in detail here, but the interested reader is referred to [34].

Naturally, appending 0-columns in front of all code elements does not change the minimum distance. Thus, if $C \subseteq \mathbb{F}_q^{k\times(n-k-\ell)}$ is an MRD code of minimum rank distance δ, then

$$\left\{\mathrm{rs}\left[\begin{array}{ccc} 0_{k\times\ell} & I_{k\times k} & M \end{array}\right] | M \in C\right\}$$

is an $(n, q^{(n-k-\ell)(k-\delta+1)}, \delta, k)_q$-code. This fact can be used to construct even larger codes, which has also been observed in, among others, [17, 20]. We will now give our own formulation of this construction and derive an exact formula for the cardinality of these codes, which we call the *multi-component lifted MRD codes*.

Theorem 2.9: *Let C_j be some MRD code with minimum rank distance δ in $\mathbb{F}_q^{k\times(n-k-j\delta)}$ for $j = 0, \ldots, \lfloor\frac{n-k}{\delta}\rfloor$. Then*

$$\mathcal{C}_j = \left\{\mathrm{rs}\left[\begin{array}{ccc} 0_{k\times j\delta} & I_{k\times k} & M \end{array}\right] \mid M \in C_j\right\}$$

are called the component codes and the union

$$\mathcal{C} = \bigcup_{j=0}^{\lfloor\frac{n-k}{\delta}\rfloor} \mathcal{C}_j$$

is an $(n, N, \delta, k)_q$-code, where

$$N = \sum_{i=0}^{\lfloor\frac{n-2k}{\delta}\rfloor} q^{(k-\delta+1)(n-k-\delta i)} + \sum_{i=\lfloor\frac{n-2k}{\delta}\rfloor+1}^{\lfloor\frac{n-k}{\delta}\rfloor} \lceil q^{k(n-k+1-\delta(i+1))}\rceil.$$

If $k = \delta$ and $n \equiv r \mod k$ (such that $0 \leqslant r < k$), it holds that

$$N = \frac{q^n - q^{r+k}}{q^k - 1} + 1 = q^r\left(\frac{q^{n-r}-1}{q^k-1} + q^{-r} - 1\right).$$

PROOF: We will first prove the minimum distance. It follows from Theorem 2.7 that

the distance between any elements of the same component $\mathcal{C}_i$ is greater than or equal to δ. Now let $U \in \mathcal{C}_i$ and $V \in \mathcal{C}_{i+1}$. Since the identity blocks are shifted by δ positions, the maximal intersection is $(k-\delta)$-dimensional. Thus

$$d_I(U,V) = k - \dim(U \cap V) \geqslant k - (k-\delta) = \delta.$$

Let us now investigate the size of the code. The subspace component code $\mathcal{C}_i$ is as large as the corresponding MRD code (which is of size $k \times (n-k-i\delta)$), thus

$$|\mathcal{C}_i| = \begin{cases} \lceil q^{(n-k-\delta i)(k-\delta+1)} \rceil & \text{for } n-k-\delta i \geqslant k \\ \lceil q^{k(n-k+1-\delta(i+1))} \rceil & \text{for } n-k-\delta i < k \end{cases}.$$

As $n-k-\delta i \geqslant k \Leftrightarrow i \leqslant \frac{n-2k}{\delta}$ and we look at codes with $n \geqslant 2k$, we proved the general formula. For $\delta = k$ it holds that

$$N = \sum_{i=0}^{\lfloor \frac{n}{k} \rfloor - 2} q^{n-k(i+1)} + \sum_{i=\lfloor \frac{n}{k} \rfloor - 1}^{\lfloor \frac{n}{k} \rfloor - 1} \lceil q^{k(n-k+1-k(i+1))} \rceil = \sum_{i=0}^{\lfloor \frac{n}{k} \rfloor - 2} q^{n-k(i+1)} + \lceil q^{k(n-k+1-k\lfloor \frac{n}{k} \rfloor)} \rceil$$

$$= \frac{q^n - q^{k+n-k\lfloor \frac{n}{k} \rfloor}}{q^k - 1} + \lceil q^{k(n-k+1-k\lfloor \frac{n}{k} \rfloor)} \rceil.$$

Note that $n - k\lfloor \frac{n}{k} \rfloor = r$, if $n \equiv r \mod k$. Thus, the exponent of the second summand is non-positive and the formula for N follows. □

These multi-component lifted MRD codes attain the Johnson-type II bound (see Proposition 1.18) for some certain cases, as explained in the following.

Corollary 2.10: *1. If $\delta = k$ and $k|n$, the code construction of Theorem 2.9 is optimal.*
2. If $\delta = k, q = 2$ and $k|n-1$, the code construction of Theorem 2.9 is optimal.

PROOF: 1. Assume that $k|n$. Then the cardinality of a multi-component lifted MRD code with parameters $(n, N, \delta, k)_q$ is

$$N = \frac{q^n - q^k}{q^k - 1} + 1 = \frac{q^n - 1}{q^k - 1},$$

hence it meets the Johnson-type II bound.

2. Assume now that $k \geqslant 2$ (otherwise it is a trivial code), $k|n-1$ and $q = 2$. Then the cardinality of the code is

$$N = \frac{2^n - 2^{k+1}}{2^k - 1} + 1 = \frac{2^n - 2}{2^k - 1} - 1 = \left\lfloor \frac{2^n - 1}{2^k - 1} \right\rfloor - 1,$$

which attains the bound given in Proposition 1.19. □

Remark 2.11: In the case of $k|n$ and $\delta = k$, these optimal codes are also called *spread codes* [39]. The name arises from the well-known geometrical object *k-spread* of $\mathbb{F}_q^n$ which is defined as a set of k-dimensional subspaces of $\mathbb{F}_q^n$ such that any pair of elements intersects only trivially and the whole set covers the whole space $\mathbb{F}_q^n$. Note that, besides lifting MRD codes, there exist also other constructions for spread codes, some of which are explained in Sections 2.5 and 3.1.

Example 2.12: We want to construct a spread code in $\mathcal{G}_2(2,4)$. Denote by C the Gabidulin code from Example 2.5. Then the component codes are

$$\mathcal{C}_1 = \text{lift}(C) \quad \text{and} \quad \mathcal{C}_2 = \text{rs}[\, 0_{2\times 2}\ I_{2\times 2}\,]$$

and $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$ is the desired code with minimum distance 2 and cardinality 5.

Remark 2.13: Constant dimension codes in $\mathcal{G}_q(k,n)$ where $k \nmid n$ and $\delta = k$ are also known as *(strictly) partial spreads*. Results on partial spreads can be found in [6, 7], among others. The decoding of partial spread codes was studied e.g. in [23, 35]. Moreover, it was proven in [35] that the second statement of Corollary 2.10 also holds for $q > 2$.

2.2 Lifted Ferrers Diagram Codes

One can generalize the lifting idea to general reduced row echelon forms of matrices, where the unit column vectors are not necessarily in the first k columns. This idea was first introduced by Etzion and Silberstein [13]. First, let us briefly provide some definitions needed for this construction.

We denote the matrix representation of a vector space $\mathcal{U} \in \mathcal{G}_q(k,n)$ in reduced row echelon form by $\mathrm{RREF}(\mathcal{U}) \in \mathbb{F}_q^{k\times n}$.

Definition 2.14: The *identifying vector* of $\mathcal{U} \in \mathcal{G}_q(k,n)$, denoted by $v(\mathcal{U})$ is the binary vector of length n and weight k, such that the k ones of $v(\mathcal{U})$ are exactly in the positions where $\mathrm{RREF}(\mathcal{U})$ has the leading ones (also called the *pivots*).

All the binary vectors of length n and weight k can be considered as the identifying vectors of all the subspaces in $\mathcal{G}_q(k,n)$. These $\binom{n}{k}$ vectors partition $\mathcal{G}_q(k,n)$ into the $\binom{n}{k}$ different classes, where each class consists of all subspaces in $\mathcal{G}_q(k,n)$ with the same identifying vector. These classes are also called the *(Schubert) cells* of $\mathcal{G}_q(k,n)$ [8, 59].

Definition 2.15: The *Ferrers tableaux form* of a subspace $\mathcal{U} \in \mathcal{G}_q(k,n)$, denoted by $\mathcal{F}(\mathcal{U})$, is obtained from $\mathrm{RREF}(\mathcal{U})$ by first removing the zeros to the left of the leading coefficient from each row of $\mathrm{RREF}(\mathcal{U})$, and then removing the columns which contain the leading ones. All the remaining entries are shifted to the right. The *Ferrers diagram* of $\mathcal{U}$, denoted by $\mathcal{F}_{\mathcal{U}}$, is obtained from $\mathcal{F}(\mathcal{U})$ by replacing the entries of $\mathcal{F}(\mathcal{U})$ with dots.

In general, a Ferrers diagram is a collection of dots such that the rows have a decreasing and the columns have an increasing number of dots (from top to bottom and from left to right, respectively).

Example 2.16: Let $\mathcal{U}$ be the subspace in $\mathcal{G}_2(3,8)$ with the following generator matrix in reduced row echelon form:

$$\mathrm{RREF}(\mathcal{U}) = \begin{pmatrix} \mathbf{1} & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Its identifying vector is $v(\mathcal{U}) = (10110000)$, and its Ferrers tableaux form and Ferrers diagram are given by

$$\mathcal{F}(\mathcal{U}) = \begin{matrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & \\ 0 & 1 & 1 & 1 & \end{matrix}, \qquad \mathcal{F}_{\mathcal{U}} = \begin{matrix} \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet & \\ \bullet & \bullet & \bullet & \bullet & \end{matrix}.$$

Given $v(\mathcal{U})$, the unique corresponding $\mathcal{F}_{\mathcal{U}}$ can be found. For this, consider the zeros of $v(\mathcal{U})$ – each zero after the first one represents a column in the Ferrers diagram, where the number of dots in the column is equal to the number of ones before the zero in $v(\mathcal{U})$.

Example 2.17: Consider $k = 3, n = 5$ and $v(\mathcal{U}) = (11010)$. Then the corresponding Ferrers diagram is

$$\begin{array}{cc} \bullet & \bullet \\ \bullet & \bullet \\ & \bullet \end{array}.$$

On the other hand, given $\mathcal{F}(\mathcal{U})$, the unique corresponding subspace $\mathcal{U} \in \mathcal{G}_q(k, n)$ can easily be found, as illustrated in the following.

Example 2.18: Let $q = 3, k = 2, n = 4$ and

$$\mathcal{F}(\mathcal{U}) = \begin{array}{cc} 2 & 0 \\ & 1 \end{array}.$$

Then, by the shape of $\mathcal{F}(\mathcal{U})$, the identifying vector must be $v(\mathcal{U}) = (1010)$ and it follows that

$$\mathcal{U} = \mathrm{rs}\begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

In the following we will consider Ferrers diagram rank-metric codes which are generalizations of the classical rank-metric codes from the previous section.

Definition 2.19: Let $\mathcal{F}$ be a Ferrers diagram with m dots in the rightmost column and ℓ dots in the top row. A code $C_{\mathcal{F}} \subseteq \mathbb{F}_q^{m\times\ell}$ is an $[\mathcal{F}, \rho, \delta]$-*Ferrers diagram rank-metric (FDRM) code* if

- for all codewords of $C_{\mathcal{F}}$, all entries not in $\mathcal{F}$ are zeros,
- it forms a linear subspace of dimension ρ of $\mathbb{F}_q^{m\times\ell}$, and
- the rank distance between any two distinct codewords is at least δ.

Remark 2.20: If $\mathcal{F}$ is a rectangular $m \times \ell$ diagram with $m\ell$ dots then the FDRM code is a classical rank-metric code, as explained in Section 2.1.

The following theorem provides an upper bound on the cardinality of $C_{\mathcal{F}}$. It can be seen as a generalization of Theorem 2.3.

Theorem 2.21 ([14]): *Let $\mathcal{F}$ be a Ferrers diagram and $C_{\mathcal{F}}$ the corresponding FDRM code. Then $|C_{\mathcal{F}}| \leqslant q^{\min_i\{w_i\}}$, where w_i is the number of dots in $\mathcal{F}$ which are not contained in the first i rows and the rightmost $\delta - 1 - i$ columns ($0 \leqslant i \leqslant \delta - 1$).*

Definition 2.22: A code which attains the bound of Theorem 2.21 is called a *Ferrers diagram maximum rank distance (FDMRD) code.*

Remark 2.23: In [14] some code constructions attaining the bound of Theorem 2.21 are given. These constructions work for any Ferrers diagram if $\delta = 1, 2$ and for some special cases for $\delta \geqslant 3$. We do not want to explain these constructions in detail here, but refer the interested reader to [14].

Example 2.24: We want to find a FDMRD code with minimum rank distance $\delta = 2$ for the Ferrers diagram

$$\mathcal{F} = \begin{array}{ccc} \bullet & \bullet & \bullet \\ & & \bullet \\ & & \bullet \end{array}.$$

The code

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

fulfills all the conditions, i.e. it fits $\mathcal{F}$, forms a subspace of dimension 2 and has minimum rank distance 2.

Definition 2.25: For a codeword $A \in C_{\mathcal{F}} \subseteq \mathbb{F}_q^{k\times(n-k)}$ let $A_{\mathcal{F}}$ denote the part of A related to the entries of $\mathcal{F}$ in A. Given a FDRM code $C_{\mathcal{F}}$, a *lifted FDRM code* $\mathcal{C}_{\mathcal{F}}$ is defined as follows:

$$\mathcal{C}_{\mathcal{F}} = \text{lift}(C_{\mathcal{F}}) := \{\mathcal{U} \in \mathcal{G}_q(k,n) \mid \mathcal{F}(\mathcal{U}) = A_{\mathcal{F}},\ A \in C_{\mathcal{F}}\}.$$

This definition is the generalization of the definition of a lifted rank-metric code (see Definition 2.6). For this, note that all the codewords of a lifted MRD code have the same identifying vector of the type $(11\ldots100\ldots0)$. In analogy, the following theorem is the generalization of the result given in Theorem 2.7.

Theorem 2.26 ([14]): *If $C_{\mathcal{F}} \subseteq \mathbb{F}_q^{k\times(n-k)}$ is an $[\mathcal{F},\rho,\delta]$-Ferrers diagram rank-metric code, then its lifted code $\mathcal{C}_{\mathcal{F}}$ is an $(n,q^\rho,\delta,k)_q$-constant dimension code.*

As before, we can now construct multi-component lifted FDRM codes. As a first step one needs to decide which identifying vectors one wants to use for the component codes. The following result gives some insight into this decision. Recall, that the Hamming distance d_H is defined as $d_H(u,v) = \text{wt}(u-v)$ for any $u,v \in \mathbb{F}_q^n$ [38].
Proposition 2.27 ([14]): *For $\mathcal{U},\mathcal{V} \in \mathcal{G}_q(k,n)$ it holds that $d_I(\mathcal{U},\mathcal{V}) \geqslant \frac{1}{2}d_H(v(\mathcal{U}),v(\mathcal{V}))$. Moreover, if $v(\mathcal{U}) = v(\mathcal{V})$ then $d_I(\mathcal{U},\mathcal{V}) = d_R(RREF(\mathcal{U}),RREF(\mathcal{V}))$.*

Thus, we can now formulate the construction of *multi-component lifted FDRM codes*, also called the *multi-level construction*, as explained in [14].

Theorem 2.28: *The following construction produces an $(n,N,\delta,k)_q$-code $\mathcal{C}$:*

- *Choose a binary block code $\mathbb{C} \subseteq \mathbb{F}_2^n$ of constant weight k and minimum Hamming distance 2δ.*
- *Use each codeword $v_i \in \mathbb{C}$ as the identifying vector of a component code and construct the corresponding lifted FDRM code $\mathcal{C}_i$ with minimum rank distance δ.*

- *The union* $\mathcal{C} = \bigcup_{i=1}^{|\mathbb{C}|} C_i$ *is the final code.*

Example 2.29: We want to construct a $(6, N, 2, 3)_q$-code, hence we start with a binary linear code of length 6, weight 3 and Hamming distance 4:

$$\mathbb{C} = \{(111000), (100110), (010101)\}$$

The corresponding reduced row echelon forms and Ferrers diagrams are:

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

We can fill the Ferrers diagrams with FDMRD codes with minimum rank distance 2 of size q^6, q^2 and q, respectively (see Remark 2.23). The union of the lifting of these codes is a $(6, q^6 + q^2 + q, 2, 3)_q$-code.

Remark 2.30: The size of these codes depends mainly on the choice of the identifying vectors. It is conjectured that lexicographic binary constant weight codes are the best choice (cf. [14]), and for this choice one gets constant dimension codes that are at least as large as the respective multi-component lifted MRD codes from Section 2.1, where equality is attained if $\delta = k$.

2.3 The Pending Dots Extension

Now we want to show how one can improve the previous construction by using *pending dots*. The results of this subsection were first published by Trautmann and Rosenthal in [55].

The main idea is that some identifying vectors lead to a Ferrers diagram where one can remove dots and still achieve the same size of the corresponding FDRM code. We can improve the size of the multicomponent lifted FDRM codes if we take these removable dots into account.

Example 2.31: All of the following Ferrers diagrams give rise to a FDRM code with minimum rank distance 2 of size q^3, since the minimum number of dots not contained either in the first row or in the last column is 3:

Definition 2.32: Let $\mathcal{F}$ be a Ferrers diagram and f_{ij} be the dot in the i-th row and j-th column of $\mathcal{F}$. $\mathcal{F}\backslash\{f_{ij}\}$ denotes the Ferrers diagram $\mathcal{F}$ after removing f_{ij}. We call a set of dots $\mathcal{F}_P$ *pending* if the dots are in the first row and the leftmost columns of $\mathcal{F}$ and

$$|C_{\mathcal{F}}| = |C_{\mathcal{F}\backslash\mathcal{F}_P}|.$$

One can also define pending dots in the rightmost column on the very bottom and translate the following results to that setting.

Remark 2.33: For $\delta = 1$ there are never any pending dots, since the dimension of the corresponding FDMRD code is the number of all dots.

Example 2.34: In Example 2.31 the first and the second Ferrers diagrams lead to the same-size FDRM code. Thus, the top leftmost dot of the first diagram is pending. In the third Ferrers diagram the first three dots of the top row are pending.

One can compute the number of pending dots from the respective identifying vector as follows. We consider the case $\delta = 2$, where we know from Theorem 2.21 that the dimension of the FDMRD code is the minimum of the number of dots not contained in the first row and the number of dots not contained in the last column.

Proposition 2.35: *Let $\delta = 2$ and $v \in \mathbb{F}_2^n$ be an identifying vector of weight k with the corresponding Ferrers diagram $\mathcal{F}$. Moreover, let z_i be the number of zeros between the i-th and the $(i+1)$-th one of v for any $0 \leqslant i \leqslant k$. Then the number of pending dots in the first row of $\mathcal{F}$ is*

$$n - k - z_0 - \max\{i \in \{0, \ldots, k\} \mid z_i > 0\}$$

if this value is positive. Otherwise, there are no pending dots in the first row of $\mathcal{F}$.

PROOF: With the formula from Theorem 2.21 we know that we have pending dots in the first row whenever the number of dots in the first row is greater than the number of dots in the last column, since then the minimum number of dots not contained in the first row or the number of dots not contained in the last column is attained in the former case. The number of dots in the first row of $\mathcal{F}$ is $n-k-z_0$ and the number of dots in the last column is $\max\{i \in \{0,\ldots,k\} \mid z_i > 0\}$, which implies the statement. Note that, if $n-k-z_0-\max\{i \in \{0,\ldots,k\} \mid z_i > 0\} < 0$, then one would have pending dots in the last column. □

We need the following main result about pending dots for our extended code construction.

Theorem 2.36: *Let $\mathcal{U}$ and $\mathcal{V}$ be two subspaces in $\mathcal{G}_q(k,n)$ with $d_H(v(\mathcal{U}),v(\mathcal{V})) = 2\delta-2$, such that the leftmost one of $v(\mathcal{U})$ is in the same position as the leftmost one of $v(\mathcal{V})$. If $\mathcal{U}$ and $\mathcal{V}$ have a common pending dot and this dot is assigned with different values, respectively, then $d_I(\mathcal{U},\mathcal{V}) \geqslant \delta$.*

PROOF: From the Hamming distance of the identifying vectors we know that

$$\operatorname{rank}\begin{bmatrix} RREF(\mathcal{U}) \\ RREF(\mathcal{V}) \end{bmatrix} \geqslant k+\delta-1.$$

Moreover, the first row of $RREF(\mathcal{U})$ and the first row of $RREF(\mathcal{V})$ are linearly independent since they share the pivot in the same position but differ in at least one pending dot position. Together with the fact that all other leading ones appear to the right of the pending dots, we know that

$$\operatorname{rank}\begin{bmatrix} RREF(\mathcal{U}) \\ RREF(\mathcal{V}) \end{bmatrix} \geqslant k+\delta,$$

which is equivalent to $d_I(\mathcal{U},\mathcal{V}) \geqslant \delta$. □

Example 2.37: Let $n=7, k=3, \delta=2$ and consider the identifying vector (1001100), that gives rise to the matrix

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

where the dot in the box marks the position of the pending dot. We fix it once as 0 and once as 1 and assign

$$\mathcal{U} = \operatorname{rs}\begin{pmatrix} 1 & \boxed{0} & \bullet & 0 & 0 & \bullet & \bullet \\ 0 & 0 & 0 & 1 & 0 & \bullet & \bullet \\ 0 & 0 & 0 & 0 & 1 & \bullet & \bullet \end{pmatrix}, \mathcal{V} = \operatorname{rs}\begin{pmatrix} 1 & \boxed{1} & \bullet & 0 & 0 & \bullet & \bullet \\ 0 & 0 & 0 & 1 & 0 & \bullet & \bullet \\ 0 & 0 & 0 & 0 & 1 & \bullet & \bullet \end{pmatrix}.$$

Then $d_H(v(\mathcal{U}),v(\mathcal{V})) = 0$ but $d_I(\mathcal{U},\mathcal{V}) \geqslant 1$ for any values filling the remaining dots.

We can now modify the construction of Theorem 2.28 as follows.

Theorem 2.38: *The following construction produces an $(n, N, \delta, k)_q$-code $\mathcal{C}$:*

- *Choose a binary block code $\mathbb{C} \subseteq \mathbb{F}_2^n$ of constant weight k and minimum Hamming distance $2\delta - 2$, such that any elements $v, w \in \mathbb{C}$ with $d_H(v, w) = 2\delta - 2$ have the first one in the same position and a common pending dot in the corresponding Ferrers diagram, which can be fixed with distinct values from $\mathbb{F}_q$ for each distinct element, respectively.*
- *Use each codeword $v_i \in \mathbb{C}$ as the identifying vector of a component code and construct the corresponding lifted FDRM code $\mathcal{C}_i$ with minimum rank distance δ.*
- *The union $\mathcal{C} = \bigcup_{i=1}^{|\mathbb{C}|} \mathcal{C}_i$ is the final code.*

PROOF: Let $\mathcal{U}, \mathcal{V} \in \mathcal{C}$ be two codewords. If $d_H(v(\mathcal{U}), v(\mathcal{V})) \geqslant 2\delta$, then, by Proposition 2.27, $d_I(\mathcal{U}, \mathcal{V}) \geqslant \delta$. If $d_H(v(\mathcal{U}), v(\mathcal{V})) = 2\delta - 2$, then the pending dots imply the minimum distance by Theorem 2.36. □

As before, we choose the identifying vectors in our examples in lexicographic order.

Example 2.39: We want to construct a code in $\mathcal{G}_q(3, 7)$ with minimum injection distance 2.

1. We choose the first identifying vector $v_1 = (1110000)$, whose Ferrers diagram has no pending dot and it can be filled with an FDMRD code of size q^8.
2. The second identifying vector $v_2 = (1001100)$ (with $d_H(v_1, v_2) = 4$) leads to a Ferrers diagram with one pending dot. Fix the pending dot as 0 and fill the remaining Ferrers diagram with an FDMRD code of size q^4:
$$\begin{pmatrix} 1 & \boxed{0} & \bullet & 0 & 0 & \bullet & \bullet \\ 0 & 0 & 0 & 1 & 0 & \bullet & \bullet \\ 0 & 0 & 0 & 0 & 1 & \bullet & \bullet \end{pmatrix}$$
3. The next identifying vector $v_3 = (1001010)$ (with $d_H(v_1, v_3) = 4, d_H(v_2, v_3) = 2$) leads to a Ferrers diagram with a pending dot in the same position as before. Fix the pending dot as 1 and fill the remaining Ferrers diagram with an FDMRD code of size q^3:
$$\begin{pmatrix} 1 & \boxed{1} & \bullet & 0 & \bullet & 0 & \bullet \\ 0 & 0 & 0 & 1 & \bullet & 0 & \bullet \\ 0 & 0 & 0 & 0 & 0 & 1 & \bullet \end{pmatrix}$$
4. The next identifying vector $v_4 = (1000101)$ (with $d_H(v_1, v_4) = 4, d_H(v_2, v_4) = 2$, $d_H(v_3, v_4) = 4$) leads to a Ferrers diagram with a pending dot in the same position as before. (Actually there are two pending dots but we only need the one from before.) Fix the pending dot as 1. The echelon-Ferrers form can be filled with a Ferrers diagram code of size q.
$$\begin{pmatrix} 1 & \boxed{1} & \bullet & \bullet & 0 & \bullet & 0 \\ 0 & 0 & 0 & 0 & 1 & \bullet & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

5. The next identifying vectors $(0101001), (0100110), (0010011)$ have Hamming distance 4 to any other identifying vector and lead to FDMRD codes of size q^2, q^2 and 1, respectively.

Hence we constructed a $(7, q^8+q^4+q^3+2q^2+q+1, 2, 3)_q$-code, which is larger than the code constructed by the classical multi-level construction from the previous section.

The following table shows some examples where the new construction leads to larger codes than the classical construction (with a lexicographic block code $\mathbb{C}$) for $\delta = 2$.

n	k	classical lifted FDRM construction	new pending dots construction
7	3	$q^8+q^4+q^3+2q^2+1$	$q^8+q^4+q^3+2q^2+q+1$
8	3	$q^{10}+q^6+q^5+2q^4+q^3+q^2$	$q^{10}+q^6+q^5+2q^4+2q^3+2q^2+q+1$
9	3	$q^{12}+q^8+q^7+2q^6+q^5+q^4+1$	$q^{12}+q^8+q^7+2q^6+2q^5+3q^4+2q^3+$ $2q^2+q+1$

Table 2.1: *Sizes of codes $\subseteq \mathcal{G}_q(k,n)$ with minimum injection distance 2.*

Based on this pending dots construction Etzion and Silberstein came up with a modified construction for $k = 3$ and $\delta = 2$ in [15], which they showed to be optimal under the condition that a maximal lifted MRD code is contained in the constant dimension code. This construction includes our example from Table 2.1 for $k = 3$ and $n = 8$. Since we will need this construction in the sequel we will now briefly describe it.

To do so we need the following lemma which follows from a one-factorization and near-one-factorization of a complete graph.

Lemma 2.40 ([58]): *Let D be the set of all binary vectors of length m and weight 2.*

- *If m is even, D can be partitioned into $m-1$ classes, each of $\frac{m}{2}$ vectors with pairwise disjoint positions of ones;*
- *If m is odd, D can be partitioned into m classes, each of $\frac{m-1}{2}$ vectors with pairwise disjoint positions of ones.*

Theorem 2.41 ([15]): *Let $n \geqslant 8$ and $q^2+q+1 \geqslant \ell$, where $\ell = n-4$ for odd n and $\ell = n-3$ for even n. The following construction produces an $(n, N, 2, 3)_q$-code $\mathcal{C}$, where*

$$N = q^{2(n-3)} + \begin{bmatrix} n-3 \\ 2 \end{bmatrix}_q.$$

Construction:

- *By Lemma 2.40, we partition the set of weight-2 vectors of $\mathbb{F}_2^{n-3}$ into ℓ classes $P_1, P_2, \ldots, P_\ell$ and define the following four sets of identifying vectors:*

$$\mathcal{A}_0 = \{(111||0\ldots0)\},$$

$$\mathcal{A}_1 = \{(001||y) \mid y \in P_1\},$$
$$\mathcal{A}_2 = \{(010||y) \mid y \in P_i, 2 \leqslant i \leqslant \min\{q+1, \ell\}\},$$
$$\mathcal{A}_3 = \begin{cases} \{(100||y) \mid y \in P_i,\ q+2 \leqslant i \leqslant \ell\} & \text{if } \ell > q+1 \\ \varnothing & \text{if } \ell \leqslant q+1 \end{cases}.$$

Elements with the same prefix and distinct suffices from the same class P_i have Hamming distance 4. When we use the same prefix for two different classes P_i, P_j, we assign different values in the pending dots of the Ferrers tableaux forms.

- *For each identifying vector from $\mathcal{A}_0, \ldots, \mathcal{A}_3$ construct the corresponding lifted FDMRD code $\mathcal{C}_i$ with rank distance 4. Note that the Ferrers diagrams used here are without the pending dots used in the step before.*
- *The union $\bigcup_{i=0}^{\ell} \mathcal{C}_i$ forms the final code $\mathcal{C}$.*

As already mentioned, this construction attains the following bound for $k = 3$:

Theorem 2.42 ([15]): *Let $k \geqslant 3$. If an $(n, N, k-1, k)_q$-constant dimension code $\mathcal{C}$ contains an $(n, q^{(n-k)(k-\delta+1)}, k-1, k)_q$-lifted MRD code then*

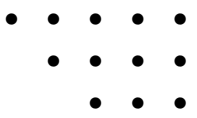
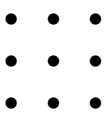
$$N \leqslant q^{2(n-k)} + A_q(n-k, k-2, k-1).$$

2.4 The Pending Blocks Constructions

We now want to extend the definition of pending dots to a two-dimensional setting. Most of the results of this section were first published by Silberstein and Trautmann in [46].

Definition 2.43: Let $\mathcal{F}$ be a Ferrers diagram with m dots in the rightmost column and ℓ dots in the top row. We say that the $\ell_1 < \ell$ leftmost columns of $\mathcal{F}$ form a *pending block* if the upper bound on the size of FDMRD code $C_{\mathcal{F}}$ from Theorem 2.21 is equal to the upper bound on the size of $C_{\mathcal{F}}$ without the ℓ_1 leftmost columns.

Example 2.44: Consider the following Ferrers diagrams:

$\mathcal{F}_1 =$  , $\mathcal{F}_2 =$  .

For $\delta = 3$, by Theorem 2.21, both codes $C_{\mathcal{F}_1}$ and $C_{\mathcal{F}_2}$ have $|C_{\mathcal{F}_i}| \leqslant q^3$, $i = 1, 2$. The diagram $\mathcal{F}_1$ has the pending block  and the diagram $\mathcal{F}_2$ has no pending block.

Definition 2.45: Let $\mathcal{F}$ be a Ferrers diagram with m dots in the rightmost column and ℓ dots in the top row, and let $\ell_1 \leqslant \ell, m_1 < m$ such that the m_1-th row has $\ell - \ell_1 + 1$ many dots. If the $(m_1 + 1)$-th row of $\mathcal{F}$ has less dots than the m_1-th row of $\mathcal{F}$, then the ℓ_1 leftmost columns of $\mathcal{F}$ are called a *quasi-pending block* (of size $m_1 \times \ell_1$).

As in the one-dimensional case, one could also define (quasi-)pending blocks in the lowest rows and rightmost columns of a Ferrers diagram. The following results are then easily carried over to that case.

Remark 2.46: A pending block is also a quasi-pending block.

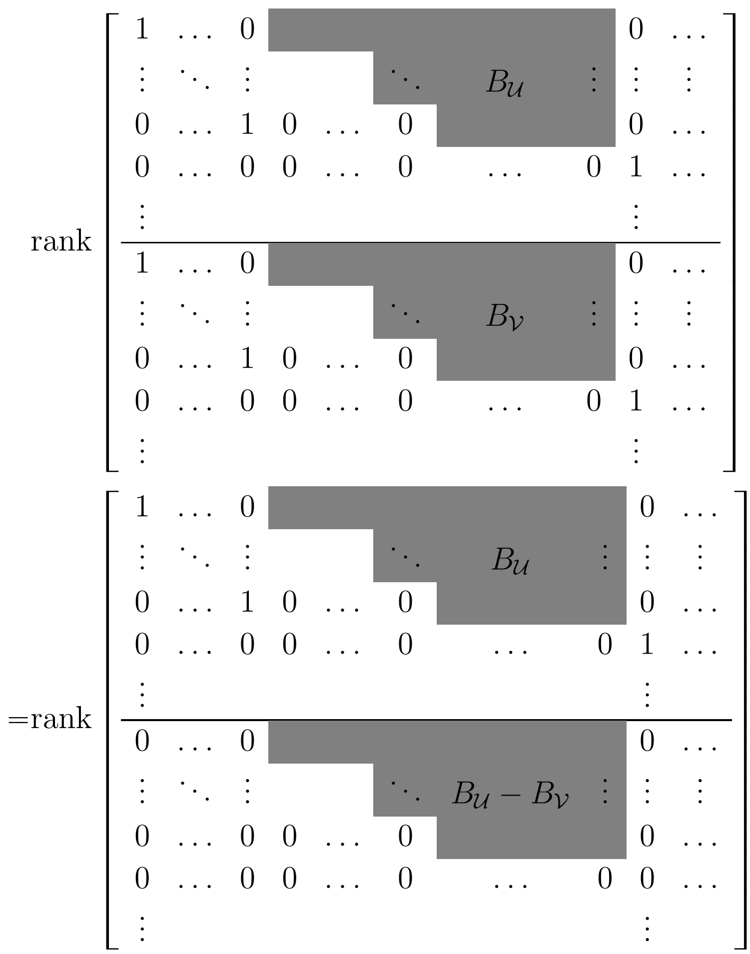
Theorem 2.47: *Let $\mathcal{U}, \mathcal{V} \in \mathcal{G}_q(k, n)$, such that the first m_1 ones of $v(\mathcal{U})$ and $v(\mathcal{V})$ are in the same positions and* $\mathrm{RREF}(\mathcal{U})$, $\mathrm{RREF}(\mathcal{V})$ *have a quasi-pending block of size $m_1 \times \ell_1$ in the same position. Let $d_H(v(\mathcal{U}), v(\mathcal{V})) = 2\delta$ and denote the submatrices of $\mathcal{F}(\mathcal{U})$ and $\mathcal{F}(\mathcal{V})$ corresponding to the quasi-pending blocks by $B_{\mathcal{U}}$ and $B_{\mathcal{V}}$, respectively. Then $d_I(\mathcal{U}, \mathcal{V}) \geqslant \delta + \mathrm{rank}(B_{\mathcal{U}} - B_{\mathcal{V}})$.*

PROOF: Since the first ones of the identifying vectors are in the same position, it has to hold that the first m_1 pivots of $\mathrm{RREF}(\mathcal{U})$ and $\mathrm{RREF}(\mathcal{V})$ are in the same columns. To compute the rank of

$$\begin{bmatrix} \mathrm{RREF}(\mathcal{U}) \\ \mathrm{RREF}(\mathcal{V}) \end{bmatrix}$$

we permute the columns such that the m_1 first pivot columns are to the very left, then the columns of the pending block, then the other pivot columns and then the rest

(WLOG in the following figure we assume that the $(m_1 + 1)$-th pivots are also in the same column):



The additional pivots of RREF($\mathcal{U}$) and RREF($\mathcal{V}$) (to the right in the above representation) that were in different columns in the beginning are still in different columns, hence it follows that

$$\operatorname{rank}\begin{bmatrix} \mathrm{RREF}(\mathcal{U}) \\ \mathrm{RREF}(\mathcal{V}) \end{bmatrix} \geqslant k + \frac{1}{2} d_H(v(\mathcal{U}), v(\mathcal{V})) + \operatorname{rank}(B_{\mathcal{U}} - B_{\mathcal{V}}),$$

which implies the statement with the formula

$$d_I(\mathcal{U}, \mathcal{V}) = \operatorname{rank}\begin{bmatrix} \mathrm{RREF}(\mathcal{U}) \\ \mathrm{RREF}(\mathcal{V}) \end{bmatrix} - k \geqslant k + \delta + \operatorname{rank}(B_{\mathcal{U}} - B_{\mathcal{V}}) - k.$$

□

In analogy to the pending dots scenario, this theorem implies that for the construction of an $(n, M, \delta, k)_q$-code, by filling the (quasi-)pending blocks with a suitable FDRM code, one can choose a set of identifying vectors with lower minimum Hamming distance than 2δ.

2.4.1 Constructions for $(n, N, 2, k)_q$-Codes

In this subsection we present a construction based on quasi-pending blocks for $(n, M, 4, k)_q$-codes with $k \geqslant 4$ and $n \geqslant 2k + 2$. This construction will then give rise to new lower bounds on the size of constant dimension codes with this minimum distance. Moreover, we will give some extension of this construction and give an additional construction for new codes from known codes in the end of the section. First we need the following results.

Lemma 2.48: *Let $n \geqslant 2k + 2$ and $v \in \mathbb{F}_2^n$ be an identifying vector of weight k, such that there are $k - 2$ many ones in the first k positions of v. Then the Ferrers diagram arising from v has more or equally many dots in the first row than in the last column.*

PROOF: Because of the distribution of the ones, it holds that the number of dots in the first row of the Ferrers diagram is

$$n - k - 2 + i, \quad i \in \{0, 1, 2\}$$

and the number of dots in the last column of the Ferrers diagram is

$$k - 2 + j, \quad j \in \{0, 1, 2\}.$$

Since we assume that $n \geqslant 2k + 2$, the number of dots in the first row is always greater or equal to the number of dots in the last column. □

Then it follows from Theorem 2.21:

Corollary 2.49: *The upper bound for the dimension of a FDRM code with minimum rank distance 2 in the setting of Lemma 2.48 is the number of dots that are not in the first row.*

Lemma 2.50: *The number of all matrices filling the Ferrers diagrams arising from all elements of $\mathbb{F}_q^k$ of weight $k - 2$ as identifying vectors is $\nu := \sum_{j=0}^{k-2} \sum_{i=j}^{k-2} q^{i+j} - 1$.*

PROOF: Assume the first zero is in the j-th and the second zero is in the i-th position of the identifying vector. Then the corresponding Ferrers diagram has $j - 1$ dots in the first column and $i - 2$ dots in the second column. I.e., there are

$$\sum_{j=1}^{k-1} \sum_{i=j+1}^{k} (j - 1) + (i - 2) = \sum_{j=0}^{k-2} \sum_{i=j}^{k-2} i + j$$

dots over all and we can fill each diagram with i dots with q^i many different matrices. The formula follows, since we have to subtract 1 for the summand where $i = j = 0$. □

We can now describe the first construction for $(n, N, 2, k)_q$-codes with $k \geqslant 4$ and $n \geqslant 2k + 2$.

Construction 2.51: First, by Lemma 2.40, we partition the weight-2 vectors of $\mathbb{F}_2^{n-k}$ into classes $P_1, \ldots, P_\ell$ of size $\frac{\bar{\ell}}{2}$ (where $\ell = \bar{\ell} - 1 = n - k - 1$ if $n - k$ even and $\ell = \bar{\ell} + 1 = n - k$ if $n - k$ odd) with pairwise disjoint positions of the ones.

- We define the following sets of identifying vectors (of weight k):

$$\begin{aligned}\mathcal{A}_0 &= \{(1\ldots1||0\ldots0)\}\\ \mathcal{A}_1 &= \{(0011\ldots1||y) \mid y \in P_1\},\\ \mathcal{A}_2 &= \{(0101\ldots1||y) \mid y \in P_2,\ldots,P_{q+1}\},\\ &\vdots\\ \mathcal{A}_{\binom{k}{2}} &= \{(1\ldots1100||y) \mid y \in P_\mu,\ldots,P_\nu\}.\end{aligned}$$

  such that the prefixes in $\mathcal{A}_1,\ldots,\mathcal{A}_{\binom{k}{2}}$ are all vectors of $\mathbb{F}_2^k$ of weight $k-2$. The number of P_i's used in each set depends on the size of the quasi-pending block arising in the k leftmost columns of the respective matrices. Thus, ν is the value from Lemma 2.50 and $\mu := \nu - q^{2(k-2)}$.
- For each vector v_j in a given $\mathcal{A}_i$ for $i \in \{2,\ldots,\binom{k}{2}\}$ assign a different matrix filling for the quasi-pending block in the k leftmost columns of the respective matrices. Fill the remaining part of the Ferrers diagram with a suitable FDMRD code of the minimum rank distance 2 and lift the code to obtain $\mathcal{C}_{i,j}$. Define $\mathcal{C}_i = \bigcup_{j=1}^{|\mathcal{A}_i|}\mathcal{C}_{i,j}$.
- Take the largest known code $\bar{\mathcal{C}} \subseteq \mathcal{G}_q(k,n-k)$ with minimum injection distance 2 and append k zero columns in front of every matrix representation of the codewords. Call this code $\tilde{\mathcal{C}}$.
- The union

$$\mathcal{C} = \bigcup_{i=0}^{\binom{k}{2}}\mathcal{C}_i \cup \tilde{\mathcal{C}}$$

  forms the final code $\mathcal{C}$, where $\mathcal{C}_0$ is the lifted MRD code corresponding to $\mathcal{A}_0$.

Remark 2.52: If $\ell < \nu$, then we use only the sets $\mathcal{A}_0,\ldots,\mathcal{A}_i$ (where $i \leqslant \binom{k}{2}$) such that all of $P_1,\ldots,P_\ell$ are used once.

Theorem 2.53: *A code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ constructed according to Construction 2.51 has minimum injection distance* 2.

PROOF: Let $\mathcal{U},\mathcal{V} \in \mathcal{C}$ be two codewords. If both are from $\tilde{\mathcal{C}}$, the distance is given by definition of $\tilde{\mathcal{C}}$. If $\mathcal{U}$ is from $\tilde{\mathcal{C}}$ and $\mathcal{V}$ is not, then $d_H(v(\mathcal{U}),v(\mathcal{V})) \geqslant 2(k-2)$. Since $k \geqslant 4$, it follows that $d_I(\mathcal{U},\mathcal{V}) \geqslant 2$. For the rest we distinguish four different cases:

1. If $v(\mathcal{U}) = v(\mathcal{V})$, then the FDMRD code implies the distance.
2. If $v(\mathcal{U}) \neq v(\mathcal{V})$ and both $v(\mathcal{U}),v(\mathcal{V})$ are in the same set $\mathcal{A}_i$ for some i, then $d_H(v(\mathcal{U}),v(\mathcal{V})) \geqslant 2$ (because of the structure of the P_i's). The quasi-pending blocks then imply by Theorem 2.47 that $d_I(\mathcal{U},\mathcal{V}) \geqslant 1+1=2$.
3. If $v(\mathcal{U}) \in \mathcal{A}_0, v(\mathcal{V}) \in \mathcal{A}_j$, where $j > 0$, then $d_H(v(\mathcal{U}),v(\mathcal{V})) \geqslant 4$. Hence, $d_I(\mathcal{U},\mathcal{V}) \geqslant 2$.
4. If $v(\mathcal{U}) \in \mathcal{A}_i, v(\mathcal{V}) \in \mathcal{A}_j$, where $i \neq j$ and $i,j > 0$, then $d_H(v(\mathcal{U}),v(\mathcal{V})) \geqslant 4$ because the first k coordinates have minimum distance $\geqslant 2$ and the last $n-k$

coordinates have minimum distance $\geqslant 2$, since they are in different P_i's. Hence, $d_I(\mathcal{U}, \mathcal{V}) \geqslant 2$.

□

Theorem 2.54: *If $\ell \leqslant \nu$, a code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ constructed according to Construction 2.51 has cardinality*

$$|\mathcal{C}| = q^{(k-1)(n-k)} + q^{(n-k-2)(k-3)} \begin{bmatrix} n-k \\ 2 \end{bmatrix}_q + A_q(n-k, 2, k).$$

PROOF: It holds that $|\mathcal{C}_0| = q^{(k-1)(n-k)}$ and $|\tilde{\mathcal{C}}| = A_q(n-k,2,k)$. Because of the assumption on k and q it follows from Lemma 2.50 that all the $y_i \in \mathbb{F}_2^{n-k}$ are used for the identifying vectors, hence the submatrices corresponding to the Ferrers diagrams in the lower two rows are in one-to-one correspondence with $\mathcal{G}_q(2, n-k)$, which has

$$\begin{bmatrix} n-k \\ 2 \end{bmatrix}_q$$

elements. Moreover, we can fill the second to $(k-2)$-th row of the Ferrers diagrams with all possible values in the construction of the FDMRD code, hence there are $q^{(n-k-2)(k-3)}$ possibilities for these dots. Together with the size of $\mathcal{C}_0$ and $\tilde{\mathcal{C}}$, we have the lower bound on the code size. □

Example 2.55: We want to construct a $(10, N, 2, 4)_2$-code. We partition the binary vectors of length 6 and weight 2 into the following 5 classes:

$$P_1 = \{110000, 001010, 000101\}, P_2 = \{101000, 010001, 000110\},$$
$$P_3 = \{011000, 100100, 000011\}, P_4 = \{010100, 100010, 001001\},$$
$$P_5 = \{100001, 010010, 001100\}.$$

Then we define the identifying vectors as

$$\begin{aligned}
\mathcal{A}_0 &= \{(1111||000000)\},\\
\mathcal{A}_1 &= \{(0011||110000), (0011||001010), (0011||000101)\},\\
\mathcal{A}_2 &= \{(0101||y) \mid y \in P_2 \cup P_3\}, \text{ using one pending dot},\\
\mathcal{A}_3 &= \{(1001||y) \mid y \in P_4 \cup P_5\}, \text{ using one of the two pending dots.}
\end{aligned}$$

The lifted FDMRD code for $\mathcal{A}_0$ has 2^{18}, the one for $\mathcal{A}_1$ has $2^{12} + 2^7 + 2^5$ elements, etc. The union of all these lifted FDMRD codes has cardinality

$$N = 2^{18} + 2^4 \begin{bmatrix} 6 \\ 2 \end{bmatrix}_2 = 2^{18} + 10416.$$

We can then add a $(6, 21, 2, 4)_2$-code (the dual of a $(6, 21, 2, 2)$-spread code) with four zero columns appended in front of each codeword and get a final code size of $2^{18} + 10437$.

In comparison, the multi-component lifted MRD code from Section 2.1 has cardinality $2^{18} + 4113$.

We can now retrieve a lower bound on the size of constant dimension codes for minimum injection distance 2.

Corollary 2.56: *Let $k \geqslant 4, n \geqslant 2k+2$ and $\sum_{j=0}^{k-2} \sum_{i=j}^{k-2} q^{i+j} - 1 \geqslant n-k$ if $n-k$ is odd (otherwise $\geqslant n-k-1$). Then*

$$A_q(n,4,k) \geqslant q^{(k-1)(n-k)} + q^{(n-k-2)(k-3)} \begin{bmatrix} n-k \\ 2 \end{bmatrix}_q + A_q(n-k,2,k).$$

Proposition 2.57: *This bound is always tighter than the one given by the multi-component lifted MRD code construction from Theorem 2.9.*
PROOF: The cardinality from Theorem 2.9 with $\delta = 2$ is given by

$$\begin{aligned} N &= \sum_{i=0}^{\lfloor \frac{n-2k}{2} \rfloor} q^{(k-1)(n-k-2i)} + \sum_{i=\lfloor \frac{n-2k}{2} \rfloor + 1}^{\lfloor \frac{n-k}{2} \rfloor} q^{k(n-k+1-2(i+1))} \\ &\leqslant q^{(k-1)(n-k)} + \sum_{i=1}^{\lfloor \frac{n-2k}{2} \rfloor} q^{(k-1)(n-k-2i)} + \sum_{i=\lfloor \frac{n-2k}{2} \rfloor + 1}^{\lfloor \frac{n-k}{2} \rfloor} q^{k(n-k+1-2(i+1))} \\ &\leqslant q^{(k-1)(n-k)} + q^{(k-3)(n-k-2)} \sum_{i=1}^{\lfloor \frac{n-2k}{2} \rfloor} q^{2(n-ki+i-3)} + A_q(n-k,2,k) \end{aligned}$$

hence, it remains to show that

$$\sum_{i=1}^{\lfloor \frac{n-2k}{2} \rfloor} q^{2(n-ki+i-3)} \leqslant \begin{bmatrix} n-k \\ 2 \end{bmatrix}_q.$$

This is true because

$$\begin{aligned} \begin{bmatrix} n-k \\ 2 \end{bmatrix}_q &= \frac{(q^{n-k}-1)(q^{n-k-1}-1)}{(q^2-1)(q-1)} \\ &= \begin{cases} \left(\sum_{i=1}^{\frac{n-k}{2}} q^{n-k-2i}\right)\left(\sum_{i=1}^{\frac{n-k}{2}} q^{n-k-1-i}\right) & \text{if } n-k \text{ is even} \\ \left(\sum_{i=1}^{\frac{n-k-1}{2}} q^{n-k-2i-1}\right)\left(\sum_{i=1}^{\frac{n-k+1}{2}} q^{n-k-i}\right) & \text{if } n-k \text{ is odd} \end{cases} \\ &\geqslant \sum_{i=1}^{\frac{n-k-1}{2}} q^{2n-2k-3i-1} \geqslant \sum_{i=1}^{\frac{n-k-1}{2}} q^{2(n-ki+i-3)} \geqslant \sum_{i=1}^{\lfloor \frac{n-2k}{2} \rfloor} q^{2(n-ki+i-3)}. \end{aligned}$$

□

Note that in the construction we did not use the dots in the quasi-pending blocks for the calculation of the size of a FDMRD code. Thus, the bound of Corollary 2.56 is not tight. To make it tighter, one can use less pending blocks and larger FDMRD

codes, as illustrated in the following construction. We denote by P_y the class of suffixes which contains the suffix vector y (in the partition according to Lemma 2.40).

Construction 2.58: First, in addition to $\mathcal{A}_0$ of Construction 2.51, we define the following sets of identifying vectors:

$$\bar{\mathcal{A}}_1 = \{(11...1100||y) \mid y \in P_{1100...00}\}, \bar{\mathcal{A}}_2 = \{(11...1010||y) \mid y \in P_{1010...00}\},$$

$$\bar{\mathcal{A}}_3 = \{(11...0110||y) \mid y \in P_{1001...00}\}, \bar{\mathcal{A}}_4 = \{(11...1001||y) \mid y \in P_{0110...00}\}.$$

All the other identifying vectors are distributed as in Construction 2.51, using possible pending blocks. Then we construct the respective lifted FDMRD codes, where we now consider the whole Ferrers diagram (and not only the one of the last $n-k$ columns) for $\bar{\mathcal{A}}_1, \ldots, \bar{\mathcal{A}}_4$. The other identifying vectors are treated as in Construction 2.51.

With this construction, we get larger FDMRD codes for $\bar{\mathcal{A}}_1, \ldots, \bar{\mathcal{A}}_4$ but we also have a stricter condition on q and k such that all P_i's are used (compared to Construction 2.51). I.e., the lower bound on the cardinality becomes

Corollary 2.59: *If* $\sum_{j=0}^{k-2}\sum_{i=j}^{k-2} q^{i+j} - \sum_{i=4}^{5} q^{2k-i} - 2q^{2k-6} \geqslant n-k$, *then*

$$A_q(n,4,k) \geqslant q^{(k-1)(n-k)} + q^{(n-k-2)(k-3)} \begin{bmatrix} n-k \\ 2 \end{bmatrix}_q + (q^{2(k-3)}-1)q^{(k-1)(n-k-2)}$$

$$+(q^{2(k-3)-1}-1)q^{(k-1)(n-k-2)-1} + 2(q^{2(k-4)}-1)q^{(k-1)(n-k-2)-2} + A_q(n-k,4,k).$$

Remark 2.60: One can use the idea of Construction 2.58 on more $\mathcal{A}_i$'s, as long as there are enough pending blocks such that all P_i's are used.

Another modification of the previous constructions is explained in the following. It does not give rise to a general formula on the size of codes for arbitrary q, k, n but one can construct codes for specific parameters, that appear to be the largest known codes in some cases.

Construction 2.61: Consider Construction 2.51, but instead of using all the P_i-classes, use the classes which contribute the most codewords more than once with disjoint prefixes.

Example 2.62: Consider the setting of Example 2.55. We want to again construct a $(10, N, 2, 4)_2$-code. We define $\mathcal{A}_0$ as previously and

$$\mathcal{A}_1 = \{(1100||y) \mid y \in P_1\}, \mathcal{A}_2 = \{(0011||y) \mid y \in P_1\},$$

$$\mathcal{A}_3 = \{(0110||y) \mid y \in P_4\}, \mathcal{A}_4 = \{(1001||y) \mid y \in P_4\},$$

$$\mathcal{A}_5 = \{(1010||y) \mid y \in P_2 \cup P_3\}, \mathcal{A}_6 = \{(0101||y) \mid y \in P_2 \cup P_3\},$$

where we use the pending dot in $\mathcal{A}_5$ and $\mathcal{A}_6$. Note that we do not use P_5. Also, the FDMRD codes are now constructed for the whole Ferrers diagrams (without the pending dot), and not only for the last 6 columns. We can again add $A_2(6,2,4) = 21$ codewords corresponding to $\tilde{\mathcal{C}}$ in Construction 2.51. The size of the final code is $2^{18} + 37477$. The largest previously known code was obtained by the multi-level construction and has size $2^{18} + 34768$ [14].

2.4.2 Construction for $(n, N, k-1, k)_q$-Codes

In this section we provide a recursive construction for $(n, N, k-1, k)_q$-codes, which uses the pending dots based construction described in Theorem 2.41 as an initial step. This construction provides a new lower bound on the cardinality of $(n, M, k-1, k)_q$-codes containing a lifted MRD code for general k.

First, we need the following generalization of Lemma 2.48.

Lemma 2.63: *Let $n-k-2 \geqslant n_1 \geqslant k-2$ and v be an identifying vector of length n and weight k, such that there are $k-2$ many ones in the first n_1 positions of v. Then the Ferrers diagram arising from v has more or equally many dots in any of the first $k-2$ rows than in the last column.*

PROOF: Naturally, the last column of the Ferrers diagram has at most k many dots. Since there are $k-2$ many ones in the first n_1 positions of v, it follows that there are $n-n_1-2$ zeros in the last $n-n_1$ positions of v. Thus, there are at least $n-n_1-2$ many dots in any but the lower two rows of the Ferrers diagram arising from v. Therefore, if $n-n_1-2 \geqslant k \iff n-k-2 \geqslant n_1$ the Ferrers diagram arising from v has more or equally many dots in any of the first $k-2$ rows than in the last column. It holds that any column has at most as many dots as the last one. □

Then it follows from Theorem 2.21:

Corollary 2.64: *The upper bound for the dimension of a Ferrers diagram code with minimum rank distance $k-1$ in the setting of Lemma 2.63 is the number of dots that are not in the first $k-2$ rows.*

Remark 2.65: If an $m \times \ell$-Ferrers diagram has δ rows with ℓ dots each, then the construction of [14] provides respective FDMRD codes of minimum distance $\delta+1$ attaining the bound of Theorem 2.21.

Lemma 2.66: *For an $m \times \ell$-Ferrers diagram where the j-th row has at least x more dots than the $(j+1)$-th row for $1 \leqslant j \leqslant m-1$ and the lowest row has x many dots, one can construct a FDMRD code with minimum rank distance m and cardinality q^x as follows. For each codeword take a different $w \in \mathbb{F}_q^x$ and fill the first x dots of every row with this vector, whereas all other dots are filled with zeros.*

PROOF: The minimum distance follows easily from the fact that the positions of the w's in each row have no column-wise intersection. Since they are all different, any difference of two codewords has a non-zero entry in each row and it is already row-reduced.

The cardinality is clear, hence it remains to show that this attains the bound of Theorem 2.21. Plugging in $i = k-1$ in Theorem 2.21 we get that the dimension of the code is less than or equal to the number of dots in the last row, which is achieved by this construction. □

Construction 2.67: Let $s = \sum_{i=3}^{k} i$, $n \geqslant s+2+k$ and $q^2+q+1 \geqslant \ell$, where $\ell = n-s$

for odd $n-s$ (or $\ell = n-s-1$ for even $n-s$).

- *Identifying vectors:* In addition to the identifying vector $v_{00}^k = (11\ldots1100\ldots0)$ of the lifted MRD code $\mathcal{C}_*^k$ (of size $q^{2(n-k)}$ and distance $2(k-1)$), the other identifying vectors of the codewords are defined as follows. First, by Lemma 2.40, we partition the weight-2 vectors of $\mathbb{F}_2^{n-s}$ into classes $P_1, \ldots, P_\ell$ of size $\frac{\bar{\ell}}{2}$ (where $\ell = \bar{\ell} - 1 = n-s-1$ if $n-s$ even and $\ell = \bar{\ell}+1 = n-s$ if $n-s$ odd) with pairwise disjoint positions of the ones. We define the sets of identifying vectors by a recursion. Let v_0 and $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3 \subseteq \mathbb{F}_q^{n-s+3}$ as defined in Theorem 2.41. Then $v_{00}^3 = v_0$,
$$\mathcal{A}_0^3 = \varnothing,\ \mathcal{A}_i^3 = \mathcal{A}_i,\ 1 \leqslant i \leqslant 3.$$
For $k \geqslant 4$ we define:
$$\mathcal{A}_0^k = \{v_{01}^k, \ldots, v_{0k-3}^k\},$$
where $v_{0j}^k = (000\ w_j^k\ ||v_{0j-1}^{k-1})$ $(1 \leqslant j \leqslant k-3)$, such that the w_j^k are all different weight-1 vectors of $\mathbb{F}_2^{k-3}$. Furthermore we define:
$$\begin{aligned}
\mathcal{A}_1^k &= \{(0010\ldots00||z) \mid z \in \mathcal{A}_1^{k-1}\},\\
\mathcal{A}_2^k &= \{(0100\ldots00||z) \mid z \in \mathcal{A}_2^{k-1}\},\\
\mathcal{A}_3^k &= \{(1000\ldots00||z) \mid z \in \mathcal{A}_3^{k-1}\},
\end{aligned}$$
such that the prefixes of the vectors in $\cup_{i=0}^3 \mathcal{A}_i^k$ are vectors of $\mathbb{F}_2^k$ of weight 1. Note that the suffix $y \in \mathbb{F}_q^{n-s}$ (from Theorem 2.41) in all the vectors from $\mathcal{A}_1^k$ belongs to P_1, the suffix y in all the vectors from $\mathcal{A}_2^k$ belongs to $\cup_{i=2}^{\min\{q+1,\ell\}} P_i$, and the suffix y in all the vectors from $\mathcal{A}_3^k$ belongs to $\cup_{i=q+2}^{\ell} P_i$. (The set $\mathcal{A}_3^k$ is empty if $\ell \leqslant q+1$.)
- *Pending blocks:*
  - All Ferrers diagrams that correspond to the vectors in $\mathcal{A}_1^k$ have a common pending block with $k-3$ rows and $\sum_{i=3}^{k-j} i$ dots in the j-th row, for $1 \leqslant j \leqslant k-3$. We fill each of these pending blocks with a different element of a suitable FDMRD code with minimum rank distance $k-3$ and size q^3, according to Lemma 2.66. Note that the initial conditions imply that $q^3 \geqslant \bar{\ell}$, i.e. we always have enough fillings for the pending block to use all elements of the given set P_i.
  - All Ferrers diagrams that correspond to the vectors in $\mathcal{A}_2^k$ have a common pending block with $k-2$ rows and $\sum_{i=3}^{k-j} i+1$ dots in the j-th row, $1 \leqslant j \leqslant k-2$. Every vector which has a suffix y from the same P_i will have the same value $a_i \in \mathbb{F}_q$ in the first entry in each row of the common pending block, s.t. the vectors with suffixes from the different classes will have different values in these entries. (This corresponds to a FDMRD code of distance $k-2$ and size q.) Given the filling of the first entries of every row, all the other entries of the pending blocks are filled by a FDMRD code with minimum distance $k-3$, according to Lemma 2.66.

  - All Ferrers diagrams that correspond to the vectors in $\mathcal{A}_3^k$ have a common pending block with $k-2$ rows and $\sum_{i=3}^{k-j} i + 2$ dots in the j-th row, $1 \leqslant j \leqslant k-2$. The filling of these pending blocks is analogous to the previous case, but for the suffixes from the different P_i-classes we fix the first two entries in each row of a pending block. Hence, there are q^2 different possibilities.
- *Ferrers tableaux forms:* On the dots corresponding to the last $n-s-2$ columns of the Ferrers diagrams for each vector v_j in a given $\mathcal{A}_i^k$, $0 \leqslant i \leqslant 3$, we construct a FDMRD code with minimum distance $k-1$ (according to Remark 2.65) and lift it to obtain $\mathcal{C}_{i,j}^k$. We define $\mathcal{C}_i^k = \bigcup_{j=1}^{|\mathcal{A}_i^k|} \mathcal{C}_{i,j}^k$.
- *Code:* The final code is defined as

$$\mathcal{C}^k = \bigcup_{i=0}^{3} \mathcal{C}_i^k \cup \mathcal{C}_*^k.$$

Remark 2.68: The existence and size of the pending blocks for $\mathcal{A}_1^k, \mathcal{A}_2^k, \mathcal{A}_3^k$ follows directly from Corollary 2.64.

Theorem 2.69: *The code $\mathcal{C}^k$ obtained by Construction 2.67 has minimum injection distance $k-1$.*

PROOF: Let $\mathcal{U}, \mathcal{V} \in \mathcal{C}^k, \mathcal{U} \neq \mathcal{V}$. If $v(\mathcal{U}) = v(\mathcal{V})$ then by Lemma 2.26 $d_I(\mathcal{U}, \mathcal{V}) \geqslant k-1$. Next, assume that $v(\mathcal{U}) \neq v(\mathcal{V})$. Note that, according to the definition of the identifying vectors, $d_I(\mathcal{U}, \mathcal{V}) \geqslant \frac{1}{2} d_H(v(\mathcal{U}), v(\mathcal{V})) = k-1$ for $(\mathcal{U}, \mathcal{V}) \in \mathcal{C}_*^k \times \mathcal{C}_i^k$, $0 \leqslant i \leqslant 3$, for $(\mathcal{U}, \mathcal{V}) \in \mathcal{C}_0^k \times \mathcal{C}_0^k$, and for $(\mathcal{U}, \mathcal{V}) \in \mathcal{C}_i^k \times \mathcal{C}_j^k$, $i \neq j$.
Now let $\mathcal{U}, \mathcal{V} \in \mathcal{C}_i^k$, for some $1 \leqslant i \leqslant 3$.

- If the suffixes of $v(\mathcal{U})$ and $v(\mathcal{V})$ of length $n-s$ belong to the same class P_t, then $d_H(v(\mathcal{U}), v(\mathcal{V})) = 4$ and $d_R(B_\mathcal{U}, B_\mathcal{V}) = k-3$, for the common pending block submatrices $B_\mathcal{U}, B_\mathcal{V}$ of $\mathcal{F}(\mathcal{U}), \mathcal{F}(\mathcal{V})$, respectively. Then by Theorem 2.47, $d_I(\mathcal{U}, \mathcal{V}) \geqslant 2 + (k-3) = k-1$.
- If the suffixes of $v(\mathcal{U})$ and $v(\mathcal{V})$ of length $n-s$ belong to different classes, say P_{t_1}, P_{t_2} respectively, then $d_H(v(\mathcal{U}), v(\mathcal{V})) \geqslant 2$ and $d_R(B_\mathcal{U}, B_\mathcal{V}) = k-2$, for the common pending block submatrices $B_\mathcal{U}, B_\mathcal{V}$ of $\mathcal{F}(\mathcal{U}), \mathcal{F}(\mathcal{V})$, respectively. Then by Theorem 2.47, $d_I(\mathcal{U}, \mathcal{V}) \geqslant 1 + (k-2) = k-1$.

Hence, for any $\mathcal{U}, \mathcal{V} \in \mathcal{C}^k$ it holds that $d_I(\mathcal{U}, \mathcal{V}) \geqslant k-1$. □

Theorem 2.70: *The code $\mathcal{C}^k$ obtained by Construction 2.67 has cardinality*

$$|\mathcal{C}^k| = q^{2(n-k)} + q^{2(n-(k+(k-1)))} + \ldots + q^{2(n-(\sum_{i=3}^{k} i))} + \begin{bmatrix} n-(\sum_{i=3}^{k} i) \\ 2 \end{bmatrix}_q .$$

PROOF: First observe that, for all identifying vectors except v_{00}^k, the additional line of dots of the corresponding Ferrers diagrams does not increase the cardinality compared

to the previous recursion step, due to Lemma 2.63. The only identifying vector that contributes additional words to $\mathcal{C}^k$ is v_{00}^k, and thus $|\mathcal{C}^k| = |\mathcal{C}^{k-1}| + q^{2(n-k)}$ for any $k \geqslant 4$. Inductively, the cardinality formula follows, together with the cardinality formula for $k = 3$ from Theorem 2.41. □

Corollary 2.71: *Let $n \geqslant s + 2 + k$ and $q^2 + q + 1 \geqslant \ell$, where $s = \sum_{i=3}^{k} i$ and $\ell = n - s$ for odd $n - s$ (or $\ell = n - s - 1$ for even $n - s$). Then*

$$A_q(n, k-1, k) \geqslant \sum_{j=3}^{k} q^{2(n-\sum_{i=j}^{k} i)} + \begin{bmatrix} n - (\sum_{i=3}^{k} i) \\ 2 \end{bmatrix}_q .$$

Example 2.72: Let $k = 4$, $\delta = 3$, $n = 13$, and $q = 2$. The code $\mathcal{C}^4$ obtained by Construction 2.67 has cardinality

$$2^{18} + 2^{12} + \begin{bmatrix} 6 \\ 2 \end{bmatrix}_q = 2^{18} + 4747.$$

The largest previously known code was of cardinality $2^{18} + 4357$ [14].

Example 2.73: Let $k = 5$, $\delta = 4$, $n = 19$, and $q = 2$. The code $\mathcal{C}^5$ obtained by Construction 2.67 has cardinality

$$2^{28} + 2^{20} + 2^{14} + \begin{bmatrix} 7 \\ 2 \end{bmatrix}_q = 2^{28} + 1067627.$$

The largest previously known code was of cardinality $2^{28} + 1052778$ [14]. We now illustrate the construction:

First, we partition the set of suffixes $y \in \mathbb{F}_2^7$ of weight 2 into 7 classes, $P_1, \ldots, P_7$ of size 3 each. The identifying vectors of the code are partitioned as follows:

$$\begin{aligned}
v_{00}^5 &= (11111||0000||000||0000000), \\
\mathcal{A}_0^5 &= \{(00001||1111||000||0000000), (00010||0001||111||0000000)\} \\
\mathcal{A}_1^5 &= \{(00100||0010||001||y) \mid y \in P_1\} \\
\mathcal{A}_2^5 &= \{(01000||0100||010||y) \mid y \in \{P_2, P_3\}\} \\
\mathcal{A}_3^5 &= \{(10000||1000||100||y) \mid y \in \{P_4, P_5, P_6, P_7\}\}
\end{aligned}$$

To demonstrate the idea of the construction we will consider the set $\mathcal{A}_2^5$. All the codewords corresponding to $\mathcal{A}_2^5$ have the common pending block

$$B = \begin{array}{cccccccccc} \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & & \\ & & & & & \bullet & \bullet & \bullet & \bullet & . \\ & & & & & & & & \bullet & \end{array}$$

Then, to distinguish between the two classes P_2 and P_3, we assign the following values to B, respectively:

$$\begin{array}{ccccccccc} 1 & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ & & & & 1 & \bullet & \bullet & \bullet & \\ & & & & & & & 1 & \end{array} \qquad \begin{array}{ccccccccc} 0 & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ & & & & & & 0 & \bullet & \bullet & \bullet \\ & & & & & & & & 0 \end{array}$$

For the remaining dots of B we construct a FDMRD code of distance 2 (here $a = 0$ for P_2 or $a = 1$ for P_3):

$$\begin{array}{cccccccccc} a & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & & a & 0 & 0 & 0, & & & & & a & 1 & 0 & 0, \\ & & & & & & & a & & & & & & & & a \end{array}$$

$$\begin{array}{cccccccccc} a & 0 & 1 & 0 & 0 & 0 & 0 & 0 & a & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ & & & & a & 0 & 1 & 0, & & & & & a & 0 & 0 & 1, \\ & & & & & & & a & & & & & & & & a \end{array}$$

$$\begin{array}{cccccccccc} a & 1 & 1 & 0 & 0 & 0 & 0 & 0 & a & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ & & & & a & 1 & 1 & 0, & & & & & a & 1 & 0 & 1, \\ & & & & & & & a & & & & & & & & a \end{array}$$

$$\begin{array}{cccccccccc} a & 0 & 1 & 1 & 0 & 0 & 0 & 0 & a & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ & & & & a & 0 & 1 & 1, & & & & & a & 1 & 1 & 1. \\ & & & & & & & a & & & & & & & & a \end{array}$$

Since both P_2 and P_3 contain only three elements, we only need to use three of the above tableaux to assign a different filling of the common pending block for the different elements corresponding to $\mathcal{A}_2^5$. We proceed analogously for the pending blocks of $\mathcal{A}_1^5, \mathcal{A}_3^5$. Then we fill the Ferrers diagrams corresponding to the last 7 columns of the identifying vectors with an FDMRD code of minimum rank distance 4 and lift these elements. Moreover, we add the lifted MRD code corresponding to v_{00}^5, which has cardinality 2^{28}. The number of codewords which corresponds to the set $\mathcal{A}_0^5$ is $2^{20} + 2^{14}$. The number of codewords that correspond to $\mathcal{A}_1^5 \cup \mathcal{A}_2^5 \cup \mathcal{A}_3^5$ is $\begin{bmatrix} 7 \\ 2 \end{bmatrix}_q$.

2.5 Orbit Codes

In this section we consider a new point of view: we derive subspace codes from group actions—such codes are called *orbit codes* [41, 54]. In Section 2.5.2 we show that this group theoretic approach yields a certain generalization of a classical linear block code to subspace codes. Moreover, we investigate in more detail orbit codes that arise from cyclic groups, called *cyclic orbit codes*, in Sections 2.5.3 and 2.5.4.

First we introduce the basic definitions and notation of groups acting on sets we need for our further investigations. These definitions and preliminary results can be found in [11, 32].

Definition 2.74: Let G be a finite multiplicative group with one-element 1_G and let X denote a finite set. A *(right) group action* of G on X is a mapping

$$\begin{aligned} X \times G &\longrightarrow X \\ (x, g) &\longmapsto xg \end{aligned}$$

such that $x1_G = x$ and $x(gg') = (xg)g'$ holds for all $x \in X$ and $g, g' \in G$. The fundamental property is that

$$x \sim_G x' :\Longleftrightarrow \exists g \in G : x' = xg$$

defines an equivalence relation on X. The induced equivalence classes are the *orbits* of G on X. The orbit of $x \in X$ is abbreviated by

$$xG := \{xg \mid g \in G\}$$

and we denote the set of all orbits of G on X by

$$X/G := \{xG \mid x \in X\}.$$

A transversal of the orbits X/G, denoted by $\mathcal{T}(X/G)$, is a minimal subset of X such that $X/G := \{xG \mid x \in \mathcal{T}(X/G)\}$, i. e. it is a set of representatives of the orbits.

In the same manner one can define a left group action of G on X. Then the orbit of $x \in X$ under G is denoted by Gx and the set of all orbits of G on X is denoted by $G\backslash X := \{Gx \mid x \in X\}$.

Definition 2.75: The *stabilizer* of an element $x \in X$ is the set of group elements that fix x:

$$\mathrm{Stab}_G(x) := \{g \in G \mid xg = x\}.$$

Proposition 2.76: *Stabilizers are subgroups of G having the property that the stabiliz-*

ers of different elements of the same orbit are conjugated subgroups:

$$\mathrm{Stab}_G(xg) = g^{-1}\mathrm{Stab}_G(x)g \quad \forall g \in G.$$

If H is a subgroup of G and $g \in G$, the set Hg is called a *right coset of H in G*. The *Fundamental Lemma of Group Actions* states that an orbit can be bijectively mapped onto the right cosets of the stabilizer:

Lemma 2.77 ([11, 32]): *The mapping, defined by*

$$\begin{aligned} xG &\longrightarrow \mathrm{Stab}_G(x)\backslash G \\ xg &\longmapsto \mathrm{Stab}_G(x)g. \end{aligned}$$

is bijective. In particular, if $\mathcal{T}(\mathrm{Stab}_G(x)\backslash G)$ denotes a transversal between $\mathrm{Stab}_G(x)$ and G, the mapping

$$\begin{aligned} \mathcal{T}(\mathrm{Stab}_G(x)\backslash G) &\longrightarrow xG \\ g &\longmapsto xg \end{aligned}$$

is also one-to-one.

As an immediate consequence we obtain the equation for the orbit size:

Proposition 2.78:

$$|xG| = \frac{|G|}{|\mathrm{Stab}_G(x)|}$$

2.5.1 Orbit Codes in $\mathcal{G}_q(k,n)$

Now we consider orbit codes in the Grassmannian. The results of this subsection were first published in [54].

Definition 2.79: The general linear group of degree n, denoted by GL_n, is the set of all invertible $n \times n$-matrices with entries in $\mathbb{F}_q$. If we have to specify the underlying field $\mathbb{F}_q$ we will write $\mathrm{GL}_n(q)$:

$$\mathrm{GL}_n(q) := \{A \in \mathbb{F}_q^{n\times n} \mid \mathrm{rank}(A) = n\}.$$

Proposition 2.80: *Multiplication with GL_n-elements actually defines a group action from the right on the linear lattice $\mathcal{P}_q(n)$ by*

$$\begin{aligned} \mathcal{P}_q(n) \times \mathrm{GL}_n &\longrightarrow \mathcal{P}_q(n) \\ (\mathcal{U}, A) &\longmapsto \mathcal{U}A := \{vA \mid v \in \mathcal{U}\}. \end{aligned}$$

Since GL_n is rank-preserving when acting on matrices, it induces an action on the Grassmannian:

$$\mathcal{G}_q(k,n) \times \mathrm{GL}_n \longrightarrow \mathcal{G}_q(k,n)$$

$$(\mathcal{U}, A) \longmapsto \mathcal{U}A.$$

Since any two k-subspaces can be mapped onto each other by an invertible matrix, the orbit of the general linear group GL_n *on any k-subspace* $\mathcal{U}$ *is the whole set of all k-subspaces. Thus, we say that* GL_n acts transitively *on* $\mathcal{G}_q(k,n)$.

Now the definition of an orbit code in the Grassmannian is straightforward.

Definition 2.81: The orbits of a subgroup of the general linear group GL_n on the Grassmannian $\mathcal{G}_q(k,n)$ are called *(subspace) orbit codes.*

Lemma 2.82: *Since* GL_n *is rank-preserving on* $\mathbb{F}_q^{k\times n}$*, it is also injection distance-preserving on* $\mathcal{G}_q(k,n)$*, i.e. for* $\mathcal{U}, \mathcal{V} \in \mathcal{G}_q(k,n)$ *and* $A \in \mathrm{GL}_n$

$$d_I(\mathcal{U}, \mathcal{V}) = d_I(\mathcal{U}A, \mathcal{V}A).$$

Theorem 2.83: *Let* $\mathcal{U} \in \mathcal{G}_q(k,n)$*,* G *be a subgroup of* GL_n *and* $\mathcal{C} = \mathcal{U}G$ *be an orbit code.*

1. *The code* $\mathcal{C}$ *has size*

$$|\mathcal{C}| = \frac{|G|}{|\mathrm{Stab}_G(\mathcal{U})|} = \frac{|G|}{|G \cap \mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{U})|}.$$

2. *The minimum distance* $d_I(\mathcal{C})$ *of the code satisfies*

$$d_I(\mathcal{C}) = \min\{d_I(\mathcal{U}, \mathcal{U}A) \mid A \in \mathcal{T}(\mathrm{Stab}_G(\mathcal{U})\backslash G), A \notin \mathrm{Stab}_G(\mathcal{U})\}.$$

3. *The stabilizers in* GL_n *of different codewords* $\mathcal{V}, \mathcal{W} \in \mathcal{C}$ *are conjugate subgroups, i. e. there exists* $A \in G$ *with*

$$\mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{V}) = A^{-1}\mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{W})A.$$

and

$$\mathrm{Stab}_G(\mathcal{V}) = A^{-1}\mathrm{Stab}_G(\mathcal{W})A.$$

4. *In particular,* $|\mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{V})| = |\mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{W})|$*, respectively* $|\mathrm{Stab}_G(\mathcal{V})| = |\mathrm{Stab}_G(\mathcal{W})|$.

PROOF: The first part follows from Proposition 2.78, the second from Lemma 2.82 and the last two from Proposition 2.76. □

Proposition 2.84: *Let* $\mathcal{U}_0 = \mathrm{rs}[\, I_{k\times k}\ 0_{k\times(n-k)} \,]$*. It holds that*

$$\mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{U}_0) = \left\{ \left(\begin{array}{c|c} A_1 & 0 \\ \hline A_3 & A_4 \end{array} \right) \mid A_1 \in \mathrm{GL}_k, A_3 \in \mathbb{F}_q^{(n-k)\times k}, A_4 \in \mathrm{GL}_{n-k} \right\}.$$

Since GL_n *acts transitively on* $\mathcal{G}_q(k,n)$*, we know that for any* $\mathcal{U} \in \mathcal{G}_q(k,n)$ *there exists* $B \in \mathrm{GL}_n$ *such that* $\mathcal{U} = \mathcal{U}_0 B$ *and hence*

$$\mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{U}) = B^{-1}\mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{U}_0)B.$$

PROOF: It follows from the block matrix multiplication rules that

$$\mathrm{rs}[\, I_{k\times k}\ 0_{k\times(n-k)}\,] \left(\begin{array}{c|c} A_1 & A_2 \\ \hline A_3 & A_4 \end{array}\right) = \mathrm{rs}[\, A_1\ A_2\,]$$

and thus to be in the stabilizer of $\mathcal{U}_0$ it has to hold that $A_1 \in \mathrm{GL}_k$ (since then $\mathrm{rs}[A_1\ A_2] = \mathrm{rs}[\, I_{k\times k}\ A_1^{-1}A_2\,]$) and $A_2 = 0$. Then, to make it full-rank, A_4 needs to be invertible. □

Theorem 2.85: *Let $\mathcal{U} \in \mathcal{G}_q(k,n)$, G a subgroup of GL_n and $\mathcal{C} = \mathcal{U}G$ be an orbit code. Then the dual satisfies $\mathcal{C}^\perp = (\mathcal{U}^\perp)G^T$ where $G^T = \{A^T \mid A \in G\}$.*

PROOF: The statement immediately follows from the identity $(\mathcal{U}A)^\perp = (\mathcal{U}^\perp)(A^{-1})^T$ and the fact that $G^T = \{A^T \mid A \in G\} = \{(A^{-1})^T \mid A \in G\}$. □

2.5.2 The Analogy to Linear Block Codes

We now want to explain why orbit codes can be seen as the analog of linear codes for classical block codes. To do so we will describe how linear codes can be described as orbits of an additive group, which will then give rise to similar properties for orbit codes and linear codes, concerning the minimum distance and cardinality of these codes.

These results were first published by Trautmann, Manganiello, Braun and Rosenthal in [53].

Theorem 2.86: *Let $C \subseteq \mathbb{F}_q^n$ be a linear code of dimension k. Then C is the orbit of an additive group, which preserves the Hamming distance.*

PROOF: For any vector $v \in \mathbb{F}_q^n$ the mapping

$$\begin{aligned} \tau_v : \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q^n \\ w &\longmapsto \tau_v(w) := w + v \end{aligned}$$

defines a bijection. Since C is a linear subspace and thus an additive group the set $G = \{\tau_c \mid c \in C\}$ forms a group with respect to the composition. The map

$$\begin{aligned} \mathbb{F}_q^n \times G &\longrightarrow \mathbb{F}_q^n \\ (w, \tau_c) &\longmapsto \tau_c(w) = w + c \end{aligned}$$

defines a group action, preserving the Hamming distance:

$$d_H(w_1, w_2) = d_H(w_1 + c, w_2 + c) = d_H(\tau_c(w_1), \tau_c(w_2)).$$

Then C can be defined as the orbit of G of any element $c^* \in C$:

$$C = c^*G = \{\tau_c(c^*) \mid c \in C\} = \{c^* + c \mid c \in C\}.$$ □

In analogy to Theorem 2.83 we can then deduce the cardinality and minimum distance from the orbit property:

Corollary 2.87: *Let $C \subseteq \mathbb{F}_q^n$ be a linear code of dimension k, $c^* \in C$ and $G = \{\tau_c \mid c \in C\}$.*

1. *The code C has cardinality*

$$|C| = \frac{|G|}{|\mathrm{Stab}_G(c^*)|} = |G| = q^k.$$

2. *The minimum Hamming distance $d_H(C)$ of the code satisfies*

$$\begin{aligned} d_H(C) &= \min\{d_H(c^*, \tau_c(c^*)) \mid \tau_c \in \mathcal{T}(\mathrm{Stab}_G(c^*)\backslash G), \tau_c \notin \mathrm{Stab}_G(c^*)\} \\ &= \min\{d_H(c^*, c^* + c) \mid c \in C, c \neq 0\}. \end{aligned}$$

If $c^* = 0$, then $d_H(C) = \min\{\mathrm{weight(c)} \mid \mathrm{c} \in \mathrm{C}\backslash\{0\}\}$, which is the known formula for the distance of linear block codes.

Remark 2.88: This analogy between linear block codes and subspace orbit codes can furthermore be used to develop syndrome or coset leader decoding algorithms for orbit codes, which will be explained in Section 3.2.

2.5.3 Cardinality and Minimum Distance of Cyclic Orbit Codes

In the following we want to investigate the cardinality and minimum distance of orbit codes. To do so we restrict ourselves to cyclic orbit codes in the following.

Definition 2.89: We call an orbit code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ *cyclic* if it is the orbit of a cyclic subgroup of GL_n on some $\mathcal{U} \in \mathcal{G}_q(k,n)$.

We can use the following fact to reduce the number of subgroups to be investigated.
Lemma 2.90: *Let $A \in \mathrm{GL}_n$, G be a subgroup of GL_n and $H := A^{-1}GA$ the conjugate group. Moreover, let $\mathcal{U} \in \mathcal{G}_q(k,n)$ and $\mathcal{V} = \mathcal{U}A$. Then the codes $\mathcal{U}G$ and $\mathcal{V}H$ have the same cardinality and minimum injection distance.*
PROOF: Let $C \in G$ and $B = A^{-1}CA \in H$. Since GL_n is distance-preserving, the statement follows with

$$d_I(\mathcal{V}, \mathcal{V}B) = d_I(\mathcal{U}A, \mathcal{U}AB) = d_I(\mathcal{U}A, \mathcal{U}AA^{-1}CA) = d_I(\mathcal{U}, \mathcal{U}C). \qquad \square$$

Naturally, if two matrices $A, B \in \mathrm{GL}_n$ are similar, i.e. there exists $C \in \mathrm{GL}_n$ such that $C^{-1}AC = B$, then the groups generated by them are conjugate. The converse is not generally true, because a cyclic group might have more than one generator. Hence,

the isometric cyclic orbit codes correspond to the different conjugacy classes of elements of GL_n. A canonical transversal of the similarity classes in GL_n can be obtained from the different rational canonical forms [24, Chapter 6.7] of the matrices. The interested reader can find more information on the rational canonical form and conjugacy classes of cyclic subgroups of GL_n in [24, 41, 53].

In this section we will show how to compute the cardinality and minimum distance of cyclic orbit codes using the polynomial extension field representation of the elements of the starting point of the orbit.

We will explain in detail the case of irreducible cyclic orbit codes and give some remarks in the end how to generalize this to arbitrary cyclic subgroups of GL_n.

Definition 2.91:
1. A matrix $A \in \mathrm{GL}_n$ is called *irreducible* if $\mathbb{F}_q^n$ contains no non-trivial A-invariant subspace, otherwise it is called *reducible*.
2. A non-trivial subgroup G of GL_n is called *irreducible* if $\mathbb{F}_q^n$ contains no non-trivial G-invariant subspace, otherwise it is called *reducible*.

Remark 2.92: A cyclic group is irreducible if and only if its generator matrix is irreducible. Moreover, an invertible matrix is irreducible if and only if its characteristic polynomial is irreducible. The rational canonical form of such an invertible matrix is the companion matrix of its characteristic polynomial.

It follows that any cyclic irreducible subgroup of GL_n is conjugate to a group generated by a companion matrix of an irreducible polynomial. Therefore, according to Lemma 2.90, it is sufficient to characterize the orbits of cyclic groups generated by companion matrices of irreducible polynomials of degree n.

Irreducible Codes

From now on let $p(x) \in \mathbb{F}_q[x]$ be irreducible of degree n, $\alpha \in \mathbb{F}_{q^n}$ a root of it and M_p its companion matrix. Moreover, we need the following notation.

Definition 2.93: A *multiset* is a generalization of the notion of set in which members are allowed to appear more than once. To distinguish it from usual sets $\{x \in X\}$ we will denote multisets by $\{\{x \in X\}\}$. The number of times an element x belongs to the multiset X is the *multiplicity* of that element, denoted by $m_X(x)$.

The following theorem shows how to compute the cardinality and minimum distance of an irreducible cyclic orbit code by examining the polynomial representation of the initial point of the orbit. It is a generalization of [33, Lemma 1].

Theorem 2.94: *Let $\mathcal{U} \in \mathcal{G}_q(k,n)$ and $G = \langle M_p \rangle$. Denote by $O_1, \ldots, O_\ell$ the distinct*

orbits of G on $\mathbb{F}_q^n\backslash\{0\}$. Assume the orbits are of the type

$$\phi^{(n)}(O_i) = \{\tilde{p}_i(\alpha)\alpha^j \mid j = 1, \ldots, \mathrm{ord}(M_p)\} \quad \forall\, i = 1, \ldots, \ell$$

for some fixed $\tilde{p}_i(\alpha) \in \mathbb{F}_q[\alpha]$. Then for a given orbit O_i it holds that for any $u_j \in \mathcal{U}$ that is on O_i there exists $b_{(i,j)} \in \mathbb{Z}_{\mathrm{ord}(M_p)}$ such that

$$\phi^{(n)}(u_j) = \tilde{p}_i(\alpha)\alpha^{b_{(i,j)}}.$$

For $i = 1, \ldots, \ell$ define

$$a_{(i,\mu,\lambda)} := b_{(i,\mu)} - b_{(i,\lambda)}$$

and the difference multisets

$$D_i := \{\{a_{(i,\mu,\lambda)} \mid \mu, \lambda \in \{1, \ldots, \mathrm{ord}(M_p) - 1\}, \mu \neq \lambda\}\},$$

$$D := \bigcup_{i=1}^{\ell} D_i.$$

Let $d := \log_q(\max\{m_D(a) \mid a \in D\} + 1)$. If $d < k$, then the orbit of G on $\mathcal{U}$ is a code of cardinality $\mathrm{ord}(M_p)$ and minimum injection distance $k - d$.

PROOF: First we compute the minimum distance of the code. We know from Theorem 2.83 that it suffices to compute the minimum distance and therefore the intersection of $\mathcal{U}$ with $\mathcal{U}M_p^h$ for $h = 1, \ldots, \mathrm{ord}(M_p) - 1$. A non-zero element $\tilde{p}_i(\alpha)\alpha^{b_{(i,j)}} \in \phi^{(n)}(\mathcal{U})$ is also in $\phi^{(n)}(\mathcal{U}M_p^h)$ if and only if there exists $\tilde{p}_i(\alpha)\alpha^{b_{(i,j')}} \in \phi^{(n)}(\mathcal{U})$ such that

$$\alpha^{b_{(i,j)}} = \alpha^{b_{(i,j')}+h}$$

$$\iff b_{(i,j)} - b_{(i,j')} \equiv h \mod \mathrm{ord}(M_p).$$

But by assumption there are at most $q^d - 1$ many pairs of elements of $\phi^{(n)}(\mathcal{U})$ fulfilling this condition. Thus,

$$\dim(C_0 \cap C_h) \leqslant d \quad \forall h \in \{1, \ldots, q^n - 2\}.$$

Since we chose d minimal, this inequality is actually an equality for some h, hence the minimum distance of the code is $k - d$.

The cardinality of the code follows from the fact that $d < k$, which implies that all elements of the orbit are distinct. □

Proposition 2.95: *In the setting of Theorem 2.94, if $d = k$, one gets orbit elements with full intersection which means they are the same vector space.*

1. *Let $D' := D\backslash\{\{a \in D \mid m_D(a) = q^k - 1\}\}$ and $d' := \log_q(\max\{m_{D'}(a) \mid a \in D'\} + 1)$. Then the minimum distance of the code is $k - d'$.*
2. *Let m be the least element of D of multiplicity $q^k - 1$. Then the cardinality of the code is m.*

PROOF: 1. Since the minimum distance of the code is only taken between distinct vector spaces, one has to consider the largest intersection of two elements whose dimension is less than k.

2. Since
$$\mathcal{U}M_p^m = \mathcal{U} \implies \mathcal{U}M_p^{lm} = \mathcal{U} \quad \forall l \in \mathbb{N}$$
and the elements of D are taken modulo the order of M_p, one has to choose the minimal element of the multiset $\{\{a \in D \mid m_D(a) = q^k - 1\}\}$ for the number of distinct vector spaces in the orbit. □

As a direct consequence of Theorem 2.94 and Proposition 2.95, Algorithm 2.1 states how to compute the cardinality and minimum injection distance of an irreducible cyclic orbit code from the initial point of the orbit.

Algorithm 2.1 Computing cardinality and minimum distance of irreducible cyclic orbit codes in $\mathcal{G}_q(k,n)$

Require: $p(x) \in \mathbb{F}_q[x]$ irreducible of degree n, α a root of $p(x)$ and $\mathcal{U} = \{0, u_1, \ldots, u_{q^k-1}\} \in \mathcal{G}_q(k,n)$
  for u in $\mathcal{U}\backslash\{0\}$ **do**
    find the orbit O_i that u is on
    store $b_{i,j} := \log_\alpha\left(\frac{\phi^{(n)}(u)}{\tilde{p}_i(\alpha)}\right)$
  end for
  for i in $\{1, \ldots, \ell\}$ **do**
    for j, j' in $\{1, \ldots, \mathrm{ord}(M_p) - 1\}$, $j \neq j'$ **do**
      add the value $b_{i,j} - b_{i,j'}$ to the multiset D
    end for
  end for
  set $d := \log_q(\max\{m_D(a) \mid a \in D\} + 1)$
  if $d \neq k$ **then**
    return $\mathrm{ord}(\alpha), k - d$
  else
    set $d' := \log_q(\max\{m_D(a) \mid a \in D \text{ and } m_D(a) < d\} + 1)$
    set $m := \min\{a \in D \mid m_D(a) = d\}$
    return $m, k - d'$
  end if

Example 2.96: Consider the irreducible polynomial $p(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$. Let α be a root of $p(x)$ and M_p its companion matrix. Then $\mathbb{F}_{2^4}\backslash\{0\}$ is partitioned by $\langle\alpha\rangle$ into
$$\{\alpha^i | i = 0, \ldots, 4\} \cup \{\alpha^i(\alpha + 1) | i = 0, \ldots, 4\} \cup \{\alpha^i(\alpha^2 + 1) | i = 0, \ldots, 4\}.$$
Consider
$$u_1 = {\phi^{(4)}}^{-1}(1) = {\phi^{(4)}}^{-1}(\alpha^0) = (1000)$$

$$u_2 = {\phi^{(4)}}^{-1}(\alpha^3 + \alpha^2) = {\phi^{(4)}}^{-1}(\alpha^2(\alpha + 1)) = (0011)$$
$$u_3 = u_1 + u_2 = {\phi^{(4)}}^{-1}(\alpha^3 + \alpha^2 + 1) = {\phi^{(4)}}^{-1}(\alpha^4(\alpha^2 + 1)) = (1011)$$

i.e. each u_i is on a different orbit of $\langle M_p \rangle$ and $\mathcal{U} = \{0, u_1, u_2, u_3\}$ is a vector space. Then the orbit of $\langle M_p \rangle$ on $\mathcal{U}$ has minimum injection distance 2 and cardinality 5, hence it is a spread code.

Note that, if $p(x)$ is primitive, there is only one orbit of G on $\mathbb{F}_q^n \backslash \{0\}$. This fact simplifies the computations as illustrated in the following example.

Example 2.97: Consider the primitive polynomial $p(x) = x^6 + x + 1 \in \mathbb{F}_2[x]$. Let α be a root of $p(x)$ and M_p its companion matrix. Consider

$$\mathcal{U} = \mathrm{rs} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix},$$

then

$$\phi^{(6)}(\mathcal{U}) = \{0, \alpha^0, \alpha^8, \alpha^{10}, \alpha^{48}, \alpha^{61}, \alpha^{20}, \alpha^{59}\}$$

and

$$D = \pm\{\{8, 10, 15, 2, 20, 4, 2, 23, 10, 12, 12, 25, 12, 10, 14, 13, 28, 11, 22, 2, 24\}\} \mod 63.$$

Any element in D occurs at most $3 = 2^2 - 1$ times and some elements appear exactly 3 times, thus the code $\mathcal{U}\langle M_p \rangle$ has minimum injection distance $3 - 2 = 1$ and cardinality $2^6 - 1 = 63$.

Completely reducible codes

Definition 2.98: We call an orbit code *completely reducible* if its generating group is completely reducible. In general, a group is *completely reducible* or *semisimple* if it is the direct product of irreducible groups. For the GL_n-action on $\mathbb{F}_q^n$ a subgroup H of GL_n is completely reducible if $\mathbb{F}_q^n$ is the direct sum of subspaces $V_1, \ldots, V_i$ which are H-invariant but do not have any H-invariant proper subspaces.

Remark 2.99: In the cyclic case these groups are exactly the ones where the blocks of the rational canonical form of the generator matrix are companion matrices of irreducible polynomials, i.e. all the elementary divisors have exponent 1. Because of this property one can use the theory of irreducible cyclic orbit codes block-wise to compute the minimum distances of the block component codes and hence the minimum distance of the whole code.

For simplicity we will explain how the theory from before generalizes in the case of generator matrices whose rational canonical form has two blocks that are companion matrices of primitive polynomials. The generalization to an arbitrary number of blocks and general irreducible polynomials is then straightforward.

Assume our generator matrix M_p is of the type

$$M_p = \begin{pmatrix} P_1 & 0 \\ 0 & P_2 \end{pmatrix}$$

where P_1, P_2 are companion matrices of the primitive polynomials $p_1(x), p_2(x) \in \mathbb{F}_q[x]$ with $\deg(p_1) = n_1, \deg(p_2) = n_2$, respectively. Furthermore let

$$U = \begin{bmatrix} U_1 & U_2 \end{bmatrix}$$

be the matrix representation of the starting point $\mathcal{U} \in \mathcal{G}_q(k,n)$ such that $U_1 \in \mathbb{F}_q^{k \times n_1}, U_2 \in \mathbb{F}_q^{k \times n_2}$. Then

$$\mathcal{U}M_p^i = \mathrm{rs}\begin{bmatrix} U_1 P_1^i & U_2 P_2^i \end{bmatrix}.$$

The algorithm for computing the minimum distance of the orbit code is analogous to Algorithm 2.1, but it is now set in $\mathbb{F}_{q^{n_1}} \times \mathbb{F}_{q^{n_2}}$.

Theorem 2.100: *Let α_1, α_2 be primitive elements of $\mathbb{F}_{q^{n_1}}, \mathbb{F}_{q^{n_2}}$, respectively.*

$$\begin{aligned} \phi^{(n_1,n_2)} &: \mathbb{F}_q^n \longrightarrow \mathbb{F}_{q^{n_1}} \times \mathbb{F}_{q^{n_2}} \\ (u_1, \ldots, u_n) &\longmapsto (\phi^{(n_1)}(u_1, \ldots, u_{n_1}), \phi^{(n_2)}(u_{n_1+1}, \ldots, u_n)) \end{aligned}$$

is a vector space isomorphism. Moreover, $u = vM_p^i$ for some $u, v \in \mathbb{F}_q^n$ if and only if

1. $\phi^{(n_1)}(u_1, \ldots, u_{n_1}) = \phi^{(n_1)}(v_1, \ldots, v_{n_1})\alpha_1^i$ *and*
2. $\phi^{(n_2)}(u_{n_1+1}, \ldots, u_n) = \phi^{(n_2)}(v_{n_1+1}, \ldots, v_n)\alpha_2^i$.

PROOF: $\phi^{(n_1,n_2)}$ is a vector space isomorphism because $\phi^{(n_1)}$ and $\phi^{(n_2)}$ are. The second statement follows since

$$\begin{aligned} u = vM_p^i &\iff \phi^{(n_1,n_2)}(u) = \phi^{(n_1,n_2)}(vM_p^i) \\ &\iff \phi^{(n_1)}((u_1, \ldots, u_{n_1})) = \phi^{(n_1)}((v_1, \ldots, v_{n_1})P_1^i) \text{ and} \\ &\qquad \phi^{(n_2)}((u_{n_1+1}, \ldots, u_n)) = \phi^{(n_2)}((v_{n_1+1}, \ldots, v_n)P_2^i). \end{aligned}$$

□

Thus, if $\phi^{(n_1)}(u_i) \neq 0$ and $\phi^{(n_2)}(u_i) \neq 0$ for all non-zero elements u_i of a given vector space $\mathcal{U} \in \mathcal{G}_q(k,n)$, in the algorithm we have to create the difference set of all 2-tuples corresponding to the powers of α_1 and α_2 and proceed as usual.

Proposition 2.101: *Assume $\mathcal{U} = \{0, u_1, \ldots, u_{q^k-1}\} \in \mathcal{G}_q(k,n)$, and for all u_i there exist b_i, b_i' such that*

$$\phi^{(n_1,n_2)}(u_i) = (\alpha_1^{b_i}, \alpha_2^{b_i'}) \qquad \forall i = 1, \ldots, q^k - 1.$$

Let d be minimal such that any element of the multiset

$$D := \left\{\left\{(b_m - b_\ell \mod (q^{n_1} - 1), b_m' - b_\ell' \mod (q^{n_2} - 1)) \mid \ell, m \in \mathbb{Z}_{q^k-1}, \ell \neq m\right\}\right\}$$

has multiplicity less than or equal to $q^d - 1$. If $d < k$ then the orbit of the group generated by M_p on $\mathcal{U}$ is an orbit code of cardinality $\mathrm{ord}(M_p) = \mathrm{lcm}(q^{n_1} - 1, q^{n_2} - 1)$ and minimum injection distance $k - d$.

Since it is possible that $u = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$ is non-zero but all $u_1 = \cdots = u_{n_1} = 0$ (or the second part of the coefficients), we have to take the zero element into account when counting intersection elements:

Theorem 2.102: *Assume $\mathcal{U} = \{0, u_1, \ldots, u_{q^k-1}\} \in \mathcal{G}_q(k, n)$, and for all u_i either*

1. $\phi^{(n_1,n_2)}(u_i) = (\alpha_1^{b_i}, \alpha_2^{b'_i})$,
2. $\phi^{(n_1,n_2)}(u_i) = (\alpha_1^{b_i}, 0)$ *or*
3. $\phi^{(n_1,n_2)}(u_i) = (0, \alpha_2^{b'_i})$.

Denote by S_1, S_2, S_3 the sets of all elements of the first, second and third type, respectively, and construct the difference sets

$$D_1 := \{\{(b_m - b_\ell \mod (q^{n_1} - 1), b'_m - b'_\ell \mod (q^{n_2} - 1)) \mid u_\ell, u_m \in S_1, \ell \neq m\}\},$$
$$D_2 := \{\{(b_m - b_\ell \mod (q^{n_1} - 1), j) \mid u_\ell, u_m \in S_2, \ell \neq m, j = 1, \ldots, q^{n_2} - 1\}\},$$
$$D_3 := \{\{(j, b'_m - b'_\ell \mod (q^{n_2} - 1)) \mid u_\ell, u_m \in S_3, \ell \neq m, j = 1, \ldots, q^{n_1} - 1\}\}$$

and

$$D := D_1 \cup D_2 \cup D_3.$$

Let d be minimal such that any element of D has multiplicity less than or equal to $q^d - 1$. If $d < k$ then the orbit of the group generated by M_p on $\mathcal{U}$ is an orbit code of cardinality $\mathrm{ord}(M_p) = \mathrm{lcm}(q^{n_1} - 1, q^{n_2} - 1)$ and minimum injection distance $k - d$.

PROOF: Like in the irreducible case we want to count the number of intersecting elements and use the fact that $\langle P_1 \rangle$ and $\langle P_2 \rangle$ act transitively on $\mathbb{F}_q^{n_1} \backslash \{0\}$ and $\mathbb{F}_q^{n_2} \backslash \{0\}$, respectively. Let $\pi_1 : \mathbb{F}_q^n \to \mathbb{F}_q^{n_1}, (u_1, \ldots, u_n) \mapsto (u_1, \ldots, u_{n_1})$ and $\pi_2 : \mathbb{F}_q^n \to \mathbb{F}_q^{n_2}$, $(u_1, \ldots, u_n) \mapsto (u_{n_1+1}, \ldots, u_{n_2})$.

1. Assume $u \in S_3$, i.e. $\pi_1(u) = 0$. Then

$$\pi_1(uM_p^i) = \pi_1(u)P_1^i = 0 \quad \forall\, i = 1, \ldots, \mathrm{ord}(M_p).$$

   Thus, $uM_p^j \neq v$ for all $v \in S_1 \cup S_2$ and $j = 1, \ldots, \mathrm{ord}(M_p)$, i.e. intersection with u can only happen inside S_3. On the other hand, if $\pi_2(u) = \pi_2(u)P_2^j$ for some j, then also $u = uM_p^j$, which is why the second entry of the tuple can run over all possible values.
2. For $u \in S_2$ the analog holds.
3. For $u \in S_1$ we can use Proposition 2.101.

Since we have to check if some of the intersections inside the sets S_1, S_2, S_3 occur at the same element of the orbit we have to count the intersection inside the union of the difference sets. □

Remark 2.103: Like in the irreducible case, if $d = k$, one gets orbit elements with full intersection. Let $D' := D \backslash \{\{a = (a_1, a_2) \in D \mid m_D(a) = q^k - 1\}\}$ and $d' := \log_q(\max\{m_{D'}(a) \mid a \in D'\} + 1)$. Then the minimum distance of the code is $k - d'$. Moreover, let $m := \min\{\mathrm{lcm}(a_1, a_2) \mid a = (a_1, a_2) \in D, m_D(a) = q^k - 1\}$. Then the

cardinality of the code is $m-1$.

Non-completely reducible codes

If a matrix has a rational canonical form with blocks that are companion matrices of non-irreducible polynomials, the group generated by it is not completely reducible. In this subsection we will explain how the theory from the previous subsections has to be changed to be used for cyclic orbit codes arising from these non-completely reducible matrices. For simplicity we will describe the case of matrices whose characteristic polynomials are squares of an irreducible polynomial. This can easily be generalized to higher exponents. Along the lines of the previous subsection one can then translate the theory to more than one irreducible factor block-wise.

Let $p(x) \in \mathbb{F}_q[x]$ be irreducible of degree $\frac{n}{2}$ and $f(x) = p^2(x)$. Denote by M_f the companion matrix of $f(x)$. Since a root of $f(x)$ is also a root of $p(x)$ we cannot use it to represent $\mathbb{F}_q[x]_{<n} \cong \mathbb{F}_q^n$. Therefore we will now use polynomials in the variable x and the vector space isomorphism

$$\begin{aligned} \phi : \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q[x]_{<n} \\ (u_1, \ldots, u_n) &\longmapsto \sum_{i=1}^{n} u_i x^{i-1}. \end{aligned}$$

Then the following analogy to Theorem 1.29 still holds:
Proposition 2.104:

$$\phi(uM_f) = \phi(u)x \mod f(x).$$

Hence, one can still translate the question of finding the intersection number into the polynomial setting by finding the respective x^i that maps one element to another element of the initial point $\mathcal{U} \in \mathcal{G}_q(k,n)$. The difference to the cases before is that we do not have a field structure anymore, thus in general we cannot divide one element by the other modulo $f(x)$ to find the corresponding x^i. More precisely, we can only divide by the units of $\mathbb{F}_q[x]/f(x)$. In the other cases we can find the x^i by brute force.

Theorem 2.105: *Assume* $\mathcal{U} = \{0, u_1, \ldots, u_{q^k-1}\} \in \mathcal{G}_q(k,n)$,

$$\phi(u_i) = \phi(u_j)x^{b_{ij}}$$

for all $\phi(u_i), \phi(u_j)$ *that lie on the same orbit of* $\langle x \rangle$ *and* d *be minimal such that any element of the multiset*

$$D := \{\{b_{ij} \mod (q^n - 1) \mid i, j \in \mathbb{Z}_{q^k-1}, i \neq j\}\}$$

has multiplicity less than or equal to $q^d - 1$. *If* $d < k$ *then the orbit of the group generated by* M_f *on* $\mathcal{U}$ *is an orbit code of cardinality* $q^{\frac{n}{2}} - 1$ *and minimum injection distance* $k - d$.

2.5.4 Constructing Cyclic Orbit Codes

In this subsection we show that cyclic orbit codes contain some of the best known subspace codes. The following spread construction was given by Trautmann and Rosenthal in [56].

Theorem 2.106: *Assume $k|n$ and $c := \frac{q^n-1}{q^k-1}$. Naturally, the subfield $\mathbb{F}_{q^k} \subseteq \mathbb{F}_{q^n}$ is also an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$. If $\alpha \in \mathbb{F}_{q^n}$ is primitive, i.e. a generator of $\mathbb{F}_{q^n}^\times$, then it holds that $\mathbb{F}_{q^k} = \{\alpha^{ic} \mid i = 0, \ldots, q^k - 2\} \cup \{0\}$ and the set*

$$\mathcal{S} = \left\{\alpha^i \cdot \mathbb{F}_{q^k} \mid i = 0, \ldots, c-1\right\}$$

is a spread of $\mathbb{F}_{q^n}$ and thus defines a spread code in $\mathcal{G}_q(k, n)$.

PROOF: From Theorem 1.21 we know that $\mathbb{F}_{q^k}$ is unique. From Lemma 1.25 we know that $\mathbb{F}_{q^k}^\times$ is a cyclic subgroup of $\mathbb{F}_{q^n}^\times = \langle\alpha\rangle$ of order $q^k - 1$, which includes $1 = \alpha^0$. Together, this implies that $\mathbb{F}_{q^k} = \{\alpha^{ic} \mid i = 0, \ldots, q^k - 2\} \cup \{0\}$. It follows, that any element of $\mathcal{S}$ is indeed a vector space. Furthermore, it is easy to see that any two elements of $\mathcal{S}$ intersect only in 0. A simple counting argument then proves that it is a spread. □

Example 2.107: Over the binary field let $p(x) = x^6 + x + 1$ be primitive, α a root of $p(x)$ and M_p its companion matrix.

1. For the 3-dimensional spread compute $c = \frac{63}{7} = 9$ and construct a basis for the starting point of the orbit:

   $$\begin{aligned} u_1 &= \phi^{-1}(\alpha^0) = \phi^{-1}(1) = (100000) \\ u_2 &= \phi^{-1}(\alpha^c) = \phi^{-1}(\alpha^9) = \phi^{-1}(\alpha^4 + \alpha^3) = (000110) \\ u_3 &= \phi^{-1}(\alpha^{2c}) = \phi^{-1}(\alpha^{18}) = \phi^{-1}(\alpha^3 + \alpha^2 + \alpha + 1) = (111100) \end{aligned}$$

   The starting point is

   $$\mathcal{U} = \mathrm{rs}\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

   and the orbit of the group generated by M_p of $\mathcal{U}$ has cardinality 9 and minimum injection distance 3, i.e. it is a spread code.
2. For the 2-dimensional spread compute $c = \frac{63}{3} = 21$ and construct a basis for the starting point of the orbit:

   $$\begin{aligned} u_1 &= \phi^{-1}(\alpha^0) = \phi^{-1}(1) = (100000) \\ u_2 &= \phi^{-1}(\alpha^c) = \phi^{-1}(\alpha^{21}) = \phi^{-1}(\alpha^2 + \alpha + 1) = (111000) \end{aligned}$$

   The starting point is

   $$\mathcal{U} = \mathrm{rs}\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

and the orbit of the group generated by M_p of $\mathcal{U}$ has cardinality 21 and minimum injection distance 2, i.e. it is a spread code.

Therefore, irreducible cyclic orbit codes include this family of optimal codes. But what about irreducible cyclic orbit codes for minimum injection distance other than k? By computer search we found codes of length $\frac{q^n-1}{q-1}$ and minimum distance $k-1$ for some randomly chosen sets of $q \in \{2,3\}, k \in \{1,\dots,10\}, n \in \{4,\dots,100\}$. By the Singleton-type bound (Proposition 1.16) a cyclic orbit code cannot be better, i.e. for the given cardinality the minimum distance has to be less than or equal to $k-1$ (under the assumption that $k \geqslant 2$).

To sum up, we can construct the following irreducible cyclic orbit codes:

1. If $k|n$ we can construct optimal codes with minimum injection distance k and cardinality $\frac{q^n-1}{q^k-1}$ for any q (spread codes).
2. We conjecture that for any $k, n, q \in \mathbb{N}$ we can construct codes of minimum distance $k-1$ and cardinality $\frac{q^n-1}{q-1}$.

Since any irreducible cyclic orbit code in $\mathcal{G}_q(k,n)$ has cardinality less than or equal to $\frac{q^n-1}{q-1}$, one of the few cases left to study for optimization is non-irreducible cyclic orbit codes with minimum distance k in the case that $k \nmid n$.

The following proposition from [53] gives us some insight on this matter.

Proposition 2.108: *Let $p_1(x), \dots, p_t(x) \in \mathbb{F}_q[x]$ be monic irreducible polynomials and $e_1, \dots, e_t \in \mathbb{N}$. Denote $n_i = \deg(p_i^{e_i}(x))$ for $i = 1, \dots, t$ and let $M_i \in \mathrm{GL}_{n_i}$ be the respective companion matrix of $p_i^{e_i}(x)$. Moreover, let $k_i \leqslant n_i$, $U_i \in \mathbb{F}_q^{k_i \times n_i}$ be matrices of full rank, and define $\mathcal{C}_i := \mathrm{rs}(U_i)\langle M_i\rangle$. Furthermore, let $M := \mathrm{diag}(M_1, \dots, M_t) \in \mathrm{GL}_n$ be a block diagonal matrix, $U := \mathrm{diag}(U_1, \dots, U_t)$, $\mathcal{U} = \mathrm{rs}(U) \in \mathcal{G}_q(k,n)$ and $\mathcal{C} = \mathcal{U}\langle M\rangle$. It holds that $\mathcal{C} \in \mathcal{G}_q(k,n)$ where $k = \sum_{i=1}^t k_i$, $n = \sum_{i=1}^t n_i$ and*

$$|\mathcal{C}| = \mathrm{lcm}\big(|\mathcal{C}_i| \mid i \in \{1,\dots,t\}\big)$$

and

$$d_I(\mathcal{C}) \geqslant \min_{i\in\{1,\dots,t\}} \{d_I(\mathcal{C}_i)\}.$$

Moreover, we can distinguish the following cases:

- *If $\gcd(|\mathcal{C}_i|, |\mathcal{C}_j|) = 1$ for all $i \neq j$, then*

$$d_I(\mathcal{C}) = \min_{i\in\{1,\dots,t\}} \{d_I(\mathcal{C}_i)\}.$$

- *If $J = \big\{i \in \{1,\dots,t\} \mid |\mathcal{C}_i| = |\mathcal{C}|\big\} \neq \varnothing$, then*

$$d_I(\mathcal{C}) \geqslant \sum_{j\in\{1,\dots,t\}\setminus J} d_I(\mathcal{C}_j).$$

PROOF: 1. We first derive the cardinality of $\mathcal{C}$. Let $j := \min\{i \in \mathbb{N} \mid \mathcal{U} = \mathcal{U}M^i\}$. Then

$$\mathrm{rank}\begin{pmatrix} U \\ UM^j \end{pmatrix} = \mathrm{rank}\begin{pmatrix} \mathrm{diag}(\mathrm{U}_1,\dots,\mathrm{U}_\mathrm{t}) \\ \mathrm{diag}(\mathrm{U}_1\mathrm{M}_1^\mathrm{j},\dots,\mathrm{U}_\mathrm{t}\mathrm{M}_\mathrm{t}^\mathrm{j}) \end{pmatrix} = \sum_{i=1}^t \mathrm{rank}\begin{pmatrix} U_i \\ U_iM_i^j \end{pmatrix} = k.$$

Since the i-th summand is greater or equal to k_i and we know that $k = \sum_{i=1}^{t} k_i$, it follows that the i-th summand is equal to k_i, for $i = 1, \ldots, k$. Hence, $\mathrm{rs}(U_i) = \mathrm{rs}(U_i)M_i^j$, which implies that $|\mathcal{C}_i|$ divides j for all $i \in \{1, \ldots, t\}$. By minimality we obtain the formula of the cardinality.

2. To show the bound on the minimum distance, assume without loss of generality that $d_I(\mathcal{C}_1) \leqslant d_I(\mathcal{C}_i)$ for $i \in \{1, \ldots, t\}$. Define

$$d_i := \max_{1 \leqslant j < |\mathcal{C}_1|} \left\{ \dim(\mathrm{rs}(U_i) \cap \mathrm{rs}(U_i)M_i^j) \right\}$$

$i \in \{1, \ldots, t\}$. For $1 \leqslant j < |\mathcal{C}|$, it holds that

$$\mathrm{rank} \begin{pmatrix} U \\ UM^j \end{pmatrix} = \sum_{i=1}^{t} \mathrm{rank} \begin{pmatrix} U_i \\ U_i M_i^j \end{pmatrix} \geqslant 2k_1 - d_1 + \sum_{i=2}^{t} k_i = k + k_1 - d_1.$$

It follows that

$$\begin{aligned} d_I(\mathcal{C}) &= 2 \min_{1 \leqslant j < |\mathcal{C}|} \left\{ \mathrm{rank} \begin{pmatrix} U \\ UM^j \end{pmatrix} \right\} - 2k \\ &\geqslant 2(k + k_1 - d_1) - 2k = 2k_1 - 2d_1 = d_I(\mathcal{C}_1). \end{aligned}$$

The inequality becomes an equality if $\gcd(|\mathcal{C}_i|, |\mathcal{C}_j|) = 1$ for any $i \neq j$, since then for every $0 \leqslant h < |\mathcal{C}_1|$ there exists a $1 \leqslant g < |\mathcal{C}|$ such that for $1 < i \leqslant t$

$$g \equiv h \mod |\mathcal{C}_1| \quad \text{and} \quad g \equiv 0 \mod |\mathcal{C}_i|,$$

i.e. $\mathcal{U}_1 \neq \mathcal{U}_1 M_1^g = \mathcal{U}_1 M_1^h$ and $\mathcal{U}_i = \mathcal{U}_i M^g$. It follows that $d_I(\mathcal{U}, \mathcal{U}M^g) = d_I(\mathcal{C}_1)$. If instead $J := \{i \in \{1, \ldots, t\} \mid |\mathcal{C}_i| = |\mathcal{C}|\}$ is non-empty, then for any $1 \leqslant j < |\mathcal{C}|$ it holds that

$$\mathrm{rank} \begin{pmatrix} U \\ UM^j \end{pmatrix} \geqslant \sum_{i \in J} k_i + \sum_{i \notin J} (2k_i - d_i) = k + \sum_{i \notin J} (k_i - d_i).$$

This implies that

$$d_I(\mathcal{C}) \geqslant \sum_{j \notin J} d_I(\mathcal{C}_j).$$

□

It follows that a completely reducible code of the above described form cannot have larger cardinality for the same parameters q, k, n and minimum distance δ compared to an irreducible cyclic orbit code. This becomes clear by looking at the cardinalities, where it always holds that

$$\prod_{i=1}^{t} (q^{n_i} - 1) \leqslant q^{\sum_{i=1}^{t} n_i} - 1.$$

Thus, it seems that, besides the spread codes, cyclic orbit codes are much smaller than other known code constructions for the same parameters. To tackle this problem one can consider unions of cyclic orbit codes. This idea for primitive cyclic orbit codes of constant dimension 3 and minimum subspace distance 4 was already pursued in [17, 33]. In these papers, the respective authors found such codes for $n \in \{6, \ldots, 14\}$ that are larger than the corresponding lifted rank-metric codes from Section 2.1.

Chapter 3

Decoding Subspace Codes

This chapter is devoted to decoding algorithms for subspace codes. There are several types of decoders, as explained in Section 1.2. In this chapter we first illustrate a minimum distance decoder for spread codes, and then a syndrome type decoder for orbit codes. Furthermore, we will study the Plücker embedding and its use for list decoding constant dimension codes. In the end we will come up with a complete list decoder for lifted MRD codes.

3.1 Spread Decoding in Extension Fields

Recall the construction of a spread code as a multicomponent lifted MRD code from Section 2.1. Instead of using Gabidulin's construction for MRD codes one can use the $\mathbb{F}_q$-algebra of a companion matrix of an irreducible polynomial as follows.

Theorem 3.1 ([39]): *Let $p(x) \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree k and $M_p \in \mathbb{F}_q^{k\times k}$ its companion matrix. Then the following set is a spread code in $\mathcal{G}_q(k,n)$:*

$$\left\{\mathrm{rs}\left[\begin{array}{cccc} B_0 & B_1 & \dots & B_{\ell-1}\end{array}\right] \mid B_i \in \mathbb{F}_q[M_p]\right\}$$

For normalization purposes we represent a subspace from above by the matrix representation such that the first non-zero block is the identity.

Example 3.2: Let $p(x) = x^2 + x + 1$ and hence $M_p = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Then

$$\mathbb{F}_2[M_p] = \left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\}$$

and the following set is a spread code in $\mathcal{G}_2(2,6)$:

$$\{\mathrm{rs}[I_{2\times 2}\ B_1\ B_2] \mid B_1, B_2 \in \mathbb{F}_2[M_p]\} \cup \{\mathrm{rs}[0_{2\times 2}\ I_{2\times 2}\ B_2] \mid B_2 \in \mathbb{F}_2[M_p]\} \cup \mathrm{rs}[0_{2\times 2}\ 0_{2\times 2}\ I_{2\times 2}].$$

We can now translate this construction from the companion matrix to an extension field setting and use it for developing a decoding algorithm. These results were

published by Manganiello and Trautmann in [40]. Since they exist for any degree over $\mathbb{F}_q$, we choose primitive polynomials and their companion matrices for the spread code constructions.

For the remainder of this section assume that $k|n$ and let $\ell = \frac{n}{k}$. Moreover, let $\alpha \in \mathbb{F}_{q^k}$ be a primitive element of $\mathbb{F}_{q^k}$ and $\beta \in \mathbb{F}_{q^n}$ a primitive element of $\mathbb{F}_{q^n}$ as an extension field of $\mathbb{F}_{q^k}$. The polynomial $p(x) \in \mathbb{F}_q[x]$ denotes the primitive polynomial of degree k such that $p(\alpha) = 0$ and $M_p \in \mathbb{F}_q^{k\times k}$ its companion matrix. We know from Lemma 1.26 that $\operatorname{ord}(\alpha) = \operatorname{ord}(M_p) = q^k - 1$.

Proposition 3.3: *Let $e_1, \dots, e_n$ be the unit vectors of $\mathbb{F}_q^n$. Then*

$$\bigcup_{i=0}^{\ell-1} \{\beta^i, \alpha\beta^i, \dots, \alpha^{k-1}\beta^i\}$$

is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and

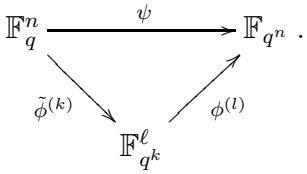
$$\begin{aligned} \psi : \mathbb{F}_q^n &\longrightarrow \mathbb{F}_{q^n} \\ e_i &\longmapsto \alpha^{(i-1 \mod k)}\beta^{\lfloor \frac{i-1}{k} \rfloor} \quad \text{for } i = 1, \dots, n \end{aligned}$$

is a vector space isomorphism.

PROOF: Let $\phi^{(l)}, \phi^{(k)}$ be like in Theorem 1.27 and define $\tilde{\phi}^{(k)} : \mathbb{F}_q^n \to \mathbb{F}_{q^k}^\ell$,

$$\tilde{\phi}^{(k)}(v_1, \dots, v_n) := \left(\phi^{(k)}(v_1, \dots, v_k), \dots, \phi^{(k)}(v_{n-k+1}, \dots, v_n)\right).$$

Then $\phi^{(l)}, \tilde{\phi}^{(k)}$ are vector space isomorphisms and $\psi = \phi^{(l)} \circ \tilde{\phi}^{(k)}$ satisfies the following diagram



□

Lemma 3.4: *Denote by $M_p[i]$ the i-th row vector of M_p. Then*

$$\phi^{(k)}(M_p^h[i]) = \alpha^{h+i-1}$$

for $i = 1, \dots, k$ and $h = 1, \dots, q^k - 1$.

PROOF: It is easy to see that $\phi^{(k)}(M_p[i]) = \alpha^i$ for $i \in \{1, \dots, k\}$. Moreover, $\phi^{(k)}$ is commutative with the multiplication with M_p and α for all $u = (u_1, \dots, u_k) \in \mathbb{F}_q^k$ (see Theorem 1.29),

$$\implies \phi^{(k)}(M_p^h[i]) = \phi^{(k)}(M_p[i]M_p^{h-1}) = \phi^{(k)}(M_p[i])\alpha^{h-1} = \alpha^{h+i-1}.$$ □

Theorem 3.5: *In the setting of Theorem 3.1, define*

$$\gamma_j := \begin{cases} 0 & \text{if } B_j = 0 \\ \alpha^h & \text{if } B_j = M_p^h \end{cases} \in \mathbb{F}_{q^k}.$$

Then it holds that $\tilde{\phi}^{(k)}\left(\mathrm{rs}\left[\begin{array}{cccc} B_0 & B_1 & \dots & B_{\ell-1} \end{array}\right]\right) = \mathbb{F}_{q^k} \cdot (\gamma_0, \dots, \gamma_{\ell-1})$ *and*

$$\psi\left(\mathrm{rs}\left[\begin{array}{cccc} B_0 & B_1 & \dots & B_{\ell-1} \end{array}\right]\right) = \mathbb{F}_{q^k} \cdot \sum_{j=0}^{\ell-1} \gamma_j \beta^j.$$

Hence, we can uniquely identify each spread code element by the respective normalized $\gamma = (\gamma_0, \dots, \gamma_{\ell-1}) \in \mathbb{F}_{q^k}^{\ell}$.

PROOF: Denote by $B_j[i]$ the i-th row vector of the block B_j. From Lemma 3.4 we know that $\phi^{(k)}(B_j[i]) = \alpha^{i-1}\gamma_j$. As α is a primitive element of $\mathbb{F}_{q^k}$, the set of all elements of the vector space is mapped to $\mathbb{F}_{q^k} \cdot (\gamma_0, \dots, \gamma_{\ell-1})$.

The second statement follows since the power of β corresponds to the position of the block B_j. Thus, ψ maps the i-th row of the whole matrix to

$$\sum_{j=0}^{\ell-1} \alpha^{i-1}\gamma_j\beta^j = \alpha^{i-1} \sum_{j=0}^{\ell-1} \gamma_j\beta^j \quad \forall i = 1, \dots, k.$$

□

Example 3.6: Consider the spread code in $\mathcal{G}_2(2, 6)$ from Example 3.2. Let α be a root of $p(x) = x^2 + x + 1$ (hence $\mathbb{F}_4 \cong \mathbb{F}_2[\alpha]$) and $\beta \in \mathbb{F}_{64}$ be such that $\mathbb{F}_{64} \cong \mathbb{F}_4[\beta]$. It holds that

$$\psi(\mathrm{rs}\left[\begin{array}{cccccc} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{array}\right]) = \mathbb{F}_4 \cdot (1 + \alpha\beta^2),$$

i.e. the respective (normalized) element from $\mathbb{F}_4^3$ is $\gamma = (1, 0, \alpha)$.

Corollary 3.7: *A spread code* $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ *constructed according to Theorem 3.1 is isomorphic to* $\mathcal{G}_{q^k}(1, \ell)$.

PROOF: Since a spread code covers the whole space and $\tilde{\phi}^{(k)}$ maps a codeword to an $\mathbb{F}_{q^k}$-linear subspace with basis vector γ, the statement holds. □

Remark 3.8: Since $\mathcal{G}_{q^k}(1, \ell)$ is isomorphic to the projective space $\mathbb{P}^{\ell-1}(\mathbb{F}_{q^k})$ of dimension $\ell - 1$ over $\mathbb{F}_{q^k}$, spreads of this type are also known as $\mathbb{F}_q$*-linear representations of* $\mathbb{P}^{\ell-1}(\mathbb{F}_{q^k})$ or *Desarguesian* $(k-1)$*-spreads* [3].

3.1.1 The Decoding Algorithm

One can now use the $\mathbb{F}_q$-linear representation of $\mathbb{P}^{\ell-1}(\mathbb{F}_{q^k})$ for the decoding procedure of this type of spread codes. Recall from Proposition 1.12 that instead of a minimum

injection distance decoder we can equivalently use a minimum subspace distance decoder. In this case the latter turns out to be the easier description, which is why we use the subspace distance in this section. Thus, our spread codes have minimum subspace distance $2\delta = 2k$.

First, assume only erasures and no errors happened during transmission. Then any received vector space $\mathcal{R} \in \mathcal{P}_q(n)$ with $\dim(\mathcal{R}) \geqslant 1$ can be decoded to its closest codeword, since the number of errors and erasures is less than or equal to $k - 1 = \frac{2\delta-2}{2}$. For decoding choose an element of the received space $r \in \mathcal{R}$ and compute $\gamma = (\gamma_0, \ldots, \gamma_{\ell-1}) \in \mathbb{F}_{q^k}^{\ell}$ such that

$$\psi(r) = \alpha^{i-1} \sum_{j=0}^{\ell-1} \gamma_j \beta^j$$

for some i. For this, divide r into ℓ blocks of size k, $r_1, \ldots, r_\ell$, and find the first non-zero block, denoted by r_s. It holds that $r_s = {\phi^{(k)}}^{-1}(\alpha^{i-1})$, since the first non-zero block is the identity matrix in the construction. Then γ can be computed by ℓ divisions in $\mathbb{F}_{q^k}$ of the image under $\phi^{(k)}$ of each block by r_s, i.e.

$$\gamma = (\phi^{(k)}(r_1)\phi^{(k)}(r_s)^{-1}, \ldots, \phi^{(k)}(r_\ell)\phi^{(k)}(r_s)^{-1}).$$

Example 3.9: Let $q = 2$, $p(x) = x^3 + x + 1$ and $\mathcal{C}$ be the corresponding binary spread code in $\mathcal{G}_2(3, 6)$, according to Theorem 3.1. Moreover, let α be a root of $p(x)$ (hence $\mathbb{F}_8 \cong \mathbb{F}_2[\alpha]$) and $\beta \in \mathbb{F}_{64}$ such that $\mathbb{F}_{64} \cong \mathbb{F}_8[\beta]$. Let $r = (110|101)$ be a received vector. It holds that $\psi(r) = (1 + \alpha) + (1 + \alpha^2)\beta$. The first three entries of r indicate that you have to divide by $1 + \alpha$ to compute the normalized γ:

$$(1 + \alpha + (1 + \alpha^2)\beta)(1 + \alpha)^{-1} = 1 + (1 + \alpha)\beta$$

Hence, $\gamma = (1, 1 + \alpha) = (1, \alpha^3)$, which identifies the codeword

$$\mathrm{rs}\left[\begin{array}{c|c} I & I + M_p \end{array}\right] = \mathrm{rs}\left[\begin{array}{c|c} I & M_p^3 \end{array}\right] = \mathrm{rs}\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right].$$

But what if errors were inserted during transmission? Let $\mathcal{U} \in \mathcal{C}$ be the sent codeword and denote by k' the dimension of the received vector space $\mathcal{R} \in \mathcal{P}_q(n)$.

Lemma 3.10: *For correct decoding it has to hold that*

$$\begin{aligned} & d_S(\mathcal{U}, \mathcal{R}) \leqslant \lfloor \tfrac{2\delta-1}{2} \rfloor \\ \iff \quad & k + k' - 2\dim(\mathcal{U} \cap \mathcal{R}) \leqslant k - 1 \\ \iff \quad & \dim(\mathcal{U} \cap \mathcal{R}) \geqslant \tfrac{k'+1}{2}. \end{aligned}$$

Therefore, one needs to find $\lceil \frac{k'+1}{2} \rceil$ linearly independent elements of $\mathcal{R}$ with the same respective γ, called $\gamma_{\max}$, to uniquely decode to the codeword

$$\psi^{-1}\left(\mathbb{F}_{q^k} \cdot \sum_{j=0}^{\ell-1} \gamma_{\max j} \beta^j\right).$$

Remark 3.11: Since we do not know if any or which of the elements of $\mathcal{R}$ are erroneous, it is in general not enough to examine only a basis of $\mathcal{R}$. Instead one needs to examine possibly all elements of the vector space $\mathcal{R}$.

A first basic decoding algorithm in this extension field representation is given in Algorithm 3.1. All field operations are done over $\mathbb{F}_{q^k}$.

Algorithm 3.1 Basic decoding algorithm for Desarguesian spread codes.

Require: the received vector space $\mathcal{R} \in \mathcal{P}_q(n)$, $k' = \dim(\mathcal{R})$
  for each $v \in \mathcal{R}$ **do**
    divide v into blocks $v_0, \ldots, v_{\ell-1}$ of length k
    $v_s :=$ the first block from the left with non-zero entries
    $a := (\phi^{(k)}(v_s))^{-1}$
    store $\gamma_v := (\phi^{(k)}(v_0) \cdot a, \ldots, \phi^{(k)}(v_{\ell-1}) \cdot a)$
  end for
  $\gamma_{\max} :=$ the element of highest multiplicity in $\{\gamma_v | v \in \mathcal{R}\}$
  if there are $\geqslant \lceil \frac{k'+1}{2} \rceil$ linearly independent $v \in \mathcal{R}$ such that $\gamma_v = \gamma_{\max}$ **then**
    return $\phi^{-1}(\mathbb{F}_{q^k} \cdot \sum_{j=0}^{\ell-1} \gamma_{\max_j} \beta^j)$
  else
    return "not decodable"
  end if

We improve the algorithm by systematically choosing the linear combinations of the basis vectors of the received space to work with. For it, note that errors are canceled out in some linear combinations of elements, as illustrated in the following example.

Example 3.12: Assume $\mathcal{U} \in \mathcal{C}$ was sent and consider two elements of the received space $r_1, r_2 \in \mathcal{R}$ containing the same error $e \in \mathbb{F}_q^n$, i.e.

$$r_1 = \sum_{u \in \mathcal{U}} \lambda_u u + e \quad , \quad r_2 = \sum_{u \in \mathcal{U}} \mu_u u + e.$$

Then

$$r_1 + (q-1)r_2 = \sum_{u \in \mathcal{U}} \lambda_u u + e - \sum_{u \in \mathcal{U}} \lambda_u u - e = \sum_{u \in \mathcal{U}} (\lambda_u - \mu_u) u \quad \in \mathcal{U}.$$

Let us generalize this idea to arbitrary numbers of errors.

Theorem 3.13: *Let $u_1, \ldots, u_k \in \mathbb{F}_q^n$ be a basis of the sent codeword $\mathcal{U} \in \mathcal{G}_q(k,n)$ and $r_1, \ldots, r_{k'} \in \mathbb{F}_q^n$ a basis of the received space $\mathcal{R}$. Assume $f < k'$ linearly independent error vectors were inserted during transmission, i.e. $\mathcal{R} = \bar{\mathcal{U}} \oplus \mathcal{E}$, where $\bar{\mathcal{U}}$ is a vector subspace of $\mathcal{U}$ and $\mathcal{E}$ is the vector space of dimension f spanned by the error vectors. Then the set*

$$\left\{ \sum_{i \in I} \lambda_i r_i \mid \lambda_i \in \mathbb{F}_q, I \subset \{1, \ldots, k'\}, |I| = f+1 \right\}$$

contains $k' - f$ linearly independent elements of $\mathcal{U}$.

PROOF: Inductively on f:

1. If $f = 0$, then $r_1, \ldots, r_{k'} \in \mathcal{U}$.
2. If $f = 1$, assume $r_1, \ldots, r_\ell \notin \bar{\mathcal{U}}$ and $r_{\ell+1}, \ldots, r_{k'} \in \bar{\mathcal{U}}$. Then there exist $\lambda_i \in \mathbb{F}_q, \mu_i \in \mathbb{F}_q \backslash \{0\}$ such that
$$r_i = \sum_{j=1}^{k} \lambda_{ij} u_j + \mu_i e \quad \forall\, i = 1, \ldots, \ell$$
where $e \in \mathcal{E}$ denotes the error vector. Hence $\forall\, i, h = 1, \ldots, \ell$
$$r_i + r_h = \sum_{j=1}^{k} (\lambda_{ij} + \lambda_{hj}) u_j + (\mu_i + \mu_h) e$$
$$\implies r_i + (-\mu_i \mu_h^{-1}) r_h = \sum_{j=1}^{k} (\lambda_{ij} - \mu_i \mu_h^{-1} \lambda_{hj}) u_j \quad \in \bar{\mathcal{U}}.$$
Then the elements $r_{\ell+1}, \ldots, r_{k'}, r_1 + (-\mu_1 \mu_2^{-1}) r_2, \ldots, r_1 + (-\mu_1 \mu_\ell^{-1}) r_\ell$ are $k' - 1$ linearly independent elements without errors.
3. If more errors, say $e_1, \ldots, e_f$, were inserted, then one can inductively "erase" $f - 1$ errors in the linear combinations of at most f elements. Write the received elements as
$$r_i = \sum_{j=1}^{k} \lambda_{ij} u_j + \sum_{j=1}^{f} \mu_{ij} e_j \quad \forall\, i = 1, \ldots, k'$$
with $\lambda_{ij}, \mu_{ij} \in \mathbb{F}_q$. Assume $\mu_{1f}, \ldots, \mu_{\ell f} \neq 0$ and $\mu_{(l+1)f}, \ldots, \mu_{k'f} = 0$, i.e. the first ℓ elements involve e_f and the others do not.
From above we know that the linear combinations of any two elements of $r_1, \ldots, r_\ell$ include $\ell - 1$ linearly independent elements without e_f. Denote them by $m_1, \ldots, m_{\ell-1}$. Naturally these elements are also linearly independent from $r_{\ell+1}, \ldots, r_{k'}$. Use the induction step on $m_1, \ldots, m_{\ell-1}, r_{\ell+1}, \ldots, r_{k'}$ to get $k' - 1 - (f-1) = k' - f$ linearly independent elements without errors. □

Corollary 3.14: *In the setting of Theorem 3.13 assume that $\mathcal{R}$ is decodable, i.e. $d_S(\mathcal{R}, \mathcal{U}) \leqslant \lfloor \frac{2\delta - 1}{2} \rfloor = k - 1$. Then there are at least $\lceil \frac{k'+1}{2} \rceil$ linearly independent elements of $\mathcal{U}$ in the set*
$$\mathcal{L} := \left\{ \sum_{i \in I} \lambda_i r_i \mid \lambda_i \in \mathbb{F}_q, I \subset \{1, \ldots, k'\}, |I| = f + 1 \right\}.$$

PROOF: Let $\bar{f}$ denote the number of erasures. Then $d_S(\mathcal{R}, \mathcal{U}) = f + \bar{f}$ and $\bar{f} = f + k - k'$. Thus,
$$f + \bar{f} \leqslant k - 1 \iff 2f + k - k' \leqslant k - 1 \iff f \leqslant \frac{k' - 1}{2}.$$

With Theorem 3.13 it follows that $\mathcal{L}$ contains $k' - f \geqslant \frac{k'+1}{2}$ linearly independent vectors of the sent vector space. □

We use this fact to modify Algorithm 3.1 as follows: We choose a basis $r_1, \ldots, r_{k'}$ of the received space $\mathcal{R} \in \mathcal{P}_q(n)$ and compute γ_{r_i} for $i = 1, \ldots, k'$. Then we compute the respective γ of all linear combinations of two basis elements, then of three elements etc. As before we can stop the process and decode to a codeword as soon as we have more than or equal to $\lceil \frac{k'+1}{2} \rceil$ linearly independent elements with the same γ. This way, if f errors occurred, we do not have to consider all elements of $\mathcal{R}$ but only the linear combinations of at most f of the basis vectors.

We illustrate the improvement obtained by Corollary 3.14 in Figures 3.1 and 3.2, which compare the numbers $q^k - 1$ (red graph) and $\sum_{i=1}^{f+1} \binom{k}{i}(q-1)^i$ (blue graph) for different values of q and f. For the labeling of the axes we use the notation e5 := 10^5 and e6 := 10^6.

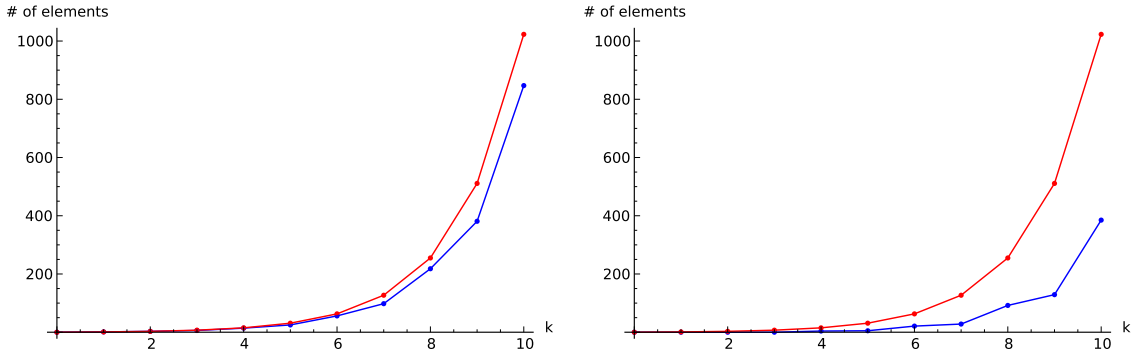


Figure 3.1: *Improvement of Cor. 3.14 for* $q = 2, f = \lfloor \frac{k}{2} \rfloor$ *and* $q = 2, f = \lfloor \frac{k}{2} \rfloor - 2$.

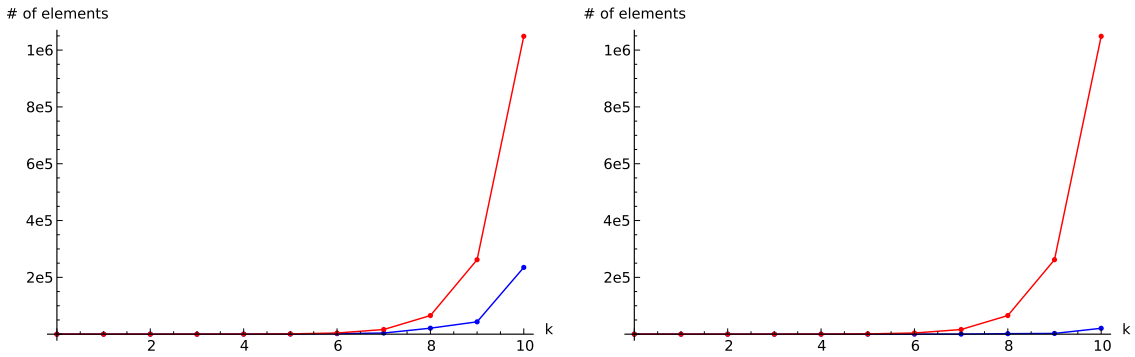


Figure 3.2: *Improvement of Cor. 3.14 for* $q = 4, f = \lfloor \frac{k}{2} \rfloor$ *and* $q = 4, f = \lfloor \frac{k}{2} \rfloor - 2$.

Remark 3.15: Moreover, note that a linear combination of elements with the same γ is always another element with γ. Since we need to find linearly independent elements, it is therefore enough to check only combinations of elements with different respective γ's.

Complexity of the Algorithm

For a better understanding of the complexity of the algorithm we first consider binary spread codes and then generalize it. Note that the algorithm works for received spaces of arbitrary dimension.

Consider a spread code $\mathcal{C} \subseteq \mathcal{G}_2(k,n)$ and a code word $\mathcal{U} \in \mathcal{C}$. Let $\mathcal{R} = \bar{\mathcal{U}} \oplus \mathcal{E}$ be the received word, such that $\bar{\mathcal{U}}$ is a subspace of $\mathcal{U}$. If $\dim(\mathcal{R}) = k'$ and $\dim(\mathcal{E}) = f$, then the algorithm computes the sums of at most $f+1$ basis vectors, which are $\binom{k'}{f+1}$ many. For each sum it proceeds with an inversion and at most $\frac{n}{k} - 1$ multiplications over $\mathbb{F}_{2^k}$. The complexity of inverting is upper-bounded by $\mathcal{O}(k^2)$ over $\mathbb{F}_2$ and the one of multiplying by $\mathcal{O}(k \log k)$ over $\mathbb{F}_2$ using the fast Fourier transform [21, Chapter 8.2]. Using the approximation $\binom{k'}{f+1} \approx \frac{k'^{f+1}}{(f+1)!}$, the overall complexity is upper-bounded by $\mathcal{O}(nkk'^{f+1})$ operations over $\mathbb{F}_2$.

Over $\mathbb{F}_q$ one needs to consider not only sums but $\mathbb{F}_q$-linear combinations of the basis vectors of $\mathcal{R}$. Thus we get an upper bound of $\binom{qk'}{f+1}$ combinations to check, which implies the following.

Theorem 3.16: *The overall complexity of Algorithm 3.1 is upper-bounded by* $\mathcal{O}(nk(qk')^{f+1})$ *operations over* $\mathbb{F}_q$.

The complexity reduces when some of the generators of the sent codeword are not influenced by the errors since in this case the algorithm has to check only linear combinations of a smaller amount of basis vectors of the received space.

In the following we compare this complexity with the one of the spread decoding algorithm shown in [22] and the decoding algorithms for Reed-Solomon like codes from [34, 48] in the case of $q = 2$ and $k = k'$. In [22] the authors present a minimum distance decoder for their spread code construction. The complexity of their algorithm is $\mathcal{O}((n-k)k^3)$. If the dimension of the error space is minimal the two algorithms have similar performance. When applied to spread codes the complexities of the algorithms presented in [34] and [48] are $\mathcal{O}(n^2(n-k)^2)$ and $\mathcal{O}(k(n-k)^3)$, respectively. The algorithm proposed in this section performs better if the dimension of the codewords, of the received space and of the error space are small.

3.2 Syndrome Decoding of Orbit Codes

As already mentioned in Section 2.5.2 one can define a syndrome decoder for orbit codes, in analogy to syndrome decoding of linear block codes. In this section we will first describe the general decoding idea for general orbit codes and then give an explicit syndrome decoding algorithm for irreducible cyclic orbit codes. To do so we must assume that the received word $\mathcal{R} \in \mathcal{P}_q(n)$ has the same dimension as the code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$, i.e. $\dim(\mathcal{R}) = k$. The results of this section were first published by Trautmann, Manganiello, Braun and Rosenthal in [53].

Recall the syndrome (or coset leader) decoder for linear block codes [38, Chapter 1]:

Proposition 3.17: *The following algorithm is a minimum distance decoder for a linear block code $C \subseteq \mathbb{F}_q^n$:*

1. *The code C is the orbit of the additive group C of the zero-point (see Section 2.5). The other orbits of C on $\mathbb{F}_q^n$ are given by $O_i = v_i + C$ for some non-zero $v_i \in \mathbb{F}_q^n$, $i = 1, \dots, m$.*
2. *Choose one lowest-weight vectors ℓ_i for each orbit O_i as the* coset leaders *for $i = 1, \dots, m$. The coset leader s_0 for C is the zero-vector.*
3. *The syndromes s_i are defined as $s_i = \ell_i H^T$, where H is the parity check matrix of the code C.*
4. *For a received vector $r \in \mathbb{F}_q^n$, compute rH^T and compare with the syndromes to decide which orbit, say O_j, r is on.*
5. *Output the codeword $c = r - \ell_j$.*

To generalize the ideas of this decoding algorithm we need the following mapping.

Definition 3.18: Like in Definition 2.74, let G be a group acting on some finite set X and $\mathfrak{T} := \mathcal{T}(X/G)$ be a transversal of the different orbits. Then the *canonizing mapping* $\gamma_{\mathfrak{T}}$ is defined as:

$$\begin{aligned} \gamma_{\mathfrak{T}} : X &\longrightarrow G \\ x &\longmapsto g \text{ such that } xg \in \mathfrak{T}. \end{aligned}$$

Remark 3.19: In Propositions 3.17, the map $\gamma_j(r) := r - \ell_j$ functions as the canonizing mapping of the transversal $\mathfrak{T} = \{\ell_0, \dots, \ell_m\}$.

In analogy to Propositions 3.17, the following theorem describes a coset leader minimum distance decoder for subspace orbit codes. The interested reader can find an abstract description of such a decoder for general codes defined as orbits under some group action on a metric set in [53].

Theorem 3.20: *Let $\mathcal{U}_0 \in \mathcal{G}_q(k,n)$, G be a subgroup of GL_n and $\mathcal{U}_0 G$ an orbit code. Moreover, let $\mathfrak{T} = \mathcal{T}(\mathcal{G}_q(k,n)/G) = \{\mathcal{U}_0, \mathcal{U}_1, \dots, \mathcal{U}_m\}$ be a transversal of the orbits, such*

that for $i = 1, \ldots, m$ it holds that $d_I(\mathcal{U}_0, \mathcal{U}_i) \leqslant d_I(\mathcal{U}_0, \mathcal{V})$ for all $\mathcal{V} \in \mathcal{U}_i G$. Then

$$\begin{aligned} \mathrm{dec}_{\mathcal{C}} : \mathcal{G}_q(k,n) &\longrightarrow \mathcal{C} \\ \mathcal{R} &\longmapsto \mathcal{U}\gamma_{\mathfrak{T}}(\mathcal{R})^{-1} \end{aligned}$$

yields a minimum distance decoder, i. e. $\mathcal{U}\gamma_{\mathfrak{T}}(\mathcal{R})^{-1} \in \mathcal{C}$ is the closest codeword to $\mathcal{R} \in \mathcal{G}_q(k,n)$.

PROOF: Assume that $\mathcal{R}$ is in the orbit of $\mathcal{U}_j$. The aim is to find a codeword $\bar{\mathcal{U}} \in \mathcal{C} = \mathcal{U}_0 G$, such that $d_I(\bar{\mathcal{U}}_0, \mathcal{R})$ is minimal. Let $A := \gamma_{\mathfrak{T}}(\mathcal{R})$ be the group element of G that maps $\mathcal{R}$ onto the orbit representative $\mathcal{U}_j$, i. e. $\mathcal{U}_j = \mathcal{R}A$. Then we obtain

$$d_I(\mathcal{U}_0, \mathcal{U}_j) = d_I(\mathcal{U}_0, \mathcal{R}A) = d_I(\mathcal{U}_0 A^{-1}, \mathcal{R}) = d_I(\mathcal{U}_0 \gamma_{\mathfrak{T}}(\mathcal{R})^{-1}, \mathcal{R}).$$

Since we know that $d_I(\mathcal{U}_0, \mathcal{U}_i)$ is minimal between elements of $\mathcal{C} = \mathcal{U}_0 G$ and $\mathcal{U}_i G$ we get that $d_I(\mathcal{U}_0 \gamma_{\mathfrak{T}}(\mathcal{R})^{-1}, \mathcal{R})$ is also minimal. Hence $\bar{\mathcal{U}} := \mathcal{U}_0 \gamma_{\mathfrak{T}}(\mathcal{R})^{-1}$ is the closest codeword to $\mathcal{R}$. □

We illustrate the subspace syndrome decoder in Figure 3.3.

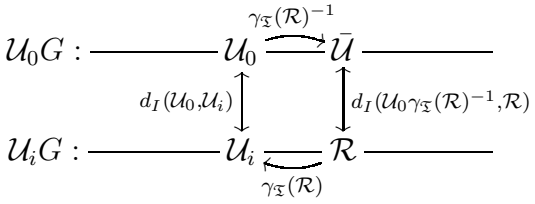


Figure 3.3: *Visualization of the coset leader minimum distance decoder.*

Thus, we have a general description for a syndrome or coset leader decoder for subspace orbit codes. The crucial point now is to find suitable and efficient canonizing mappings for a given subgroup of GL_n. In the next subsection we will derive such a canonizing mapping for the family of irreducible cyclic orbit codes.

3.2.1 A Decoder for Irreducible Cyclic Orbit Codes

Recall, that irreducible cyclic orbit codes are defined as orbits in the Grassmannian under the action of a cyclic and irreducible subgroup of GL_n. As representatives of each conjugacy class it is sufficient to investigate groups generated by companion matrices of irreducible polynomials, as explained in Section 2.5.

The main idea is that the pairwise quotients of the extension field representation of the elements of a subspace are invariant for all elements of the same orbit. On the other hand the set of all these quotients is necessarily different for subspaces of different

orbits. Hence, these can function as syndromes to determine which orbit the received word is on. For the special case of $k = 3$ and $\delta = 2$ this idea was already pursued in [12].

Algorithm 3.2 describes a syndrome decoder for an orbit code $\mathcal{C} = \mathcal{U}_0\langle M_p\rangle$, where $\mathcal{U}_0 \in \mathcal{G}_q(k,n)$ and M_p is the companion matrix of an irreducible monic polynomial $p(x) \in \mathbb{F}_q[x]$ of degree n, and a received word $\mathcal{R} \in \mathcal{G}_q(k,n)$.

Algorithm 3.2 Syndrome decoding algorithm for irreducible cyclic orbit codes.

Require: For each orbit store the initial points $\mathcal{U}_i$ and the syndromes for each orbit $S_i = \{u_\ell/u_m \mid u_\ell, u_m \in \mathcal{U}_i\backslash\{0\}, u_\ell \neq u_m\}$ in extension field representation for $i = 0, \ldots, m$.
for each $u \in \mathcal{R}\backslash\{0\}$ **do**
  for each $v \in \mathcal{R}\backslash\{0, u\}$ **do**
    store the quotient $b_{u,v} := u/v$ in extension field representation in the list L
    $i := i + 1$
  end for
end for
find the syndrome set S_j that contains all $b_{u,v} \in L$
find $\gamma(\alpha)$ such that $\forall b_{u,v} \in L\ \exists\, x_i, y_i \in \mathcal{U}_j : x_i b_{u,v} = y_i$ and $x_i\gamma(\alpha) = u$
return $\mathcal{U}_0\gamma^{-1}(M_p)$

Remark 3.21: Usually one needs only a subset of all quotients to uniquely determine the orbit, as can be seen in the following examples.

Example 3.22: Consider $\mathcal{G}_2(2,4)$ and the primitive polynomial $p(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Let α be a root of $p(x)$ and M_p the companion matrix of $p(x)$. The three distinct orbits of $\langle M_p\rangle$ are given by the initial points

$$\mathcal{U}_0 = \mathrm{rs}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \cong \{0, 1, \alpha + \alpha^2, 1 + \alpha + \alpha^2\},$$
$$\mathcal{U}_1 = \mathrm{rs}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \cong \{0, 1, \alpha, 1 + \alpha\},$$
$$\mathcal{U}_2 = \mathrm{rs}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cong \{0, 1, \alpha^2, 1 + \alpha^2\}.$$

The orbit on the first initial point is the spread code that we want to consider. The quotient sets for the three orbits are

$$S_0: \quad \{(\alpha + \alpha^2)^{\pm 1}\}.$$

$$S_1: \quad \{\alpha^{\pm 1}, \alpha^{\pm 3}, (1 + \alpha)^{\pm 1}\}$$

$$S_2: \quad \{\alpha^{\pm 2}, (\alpha^2 + \alpha^3)^{\pm 1}, (1 + \alpha^2)^{\pm 1}\}$$

Since these sets are pairwise distinct, it is enough to compute the quotient of only one pair of the received vectors to uniquely decide on the orbit. Assume e.g. that we received

$$\mathcal{R} = \mathrm{rs}\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \cong \{0, 1+\alpha^2+\alpha^3, \alpha+\alpha^3, 1+\alpha+\alpha^2\},$$

then we compute

$$(\alpha+\alpha^3)/(1+\alpha^2+\alpha^3) = \alpha+\alpha^2+\alpha^3 = (1+\alpha)^{-1}$$

hence $\mathcal{R}$ is on the orbit of $\mathcal{U}_1$. Then we find the canonizing mapping

$$\gamma(\alpha) = 1/(1+\alpha) = (1+\alpha)^{-1}.$$

Thus, $\mathcal{U}_1(I+M_p)^{-1} = \mathcal{U}_1(M_p+M_p^3) = \mathcal{R}$, and we decode to the codeword

$$\mathcal{U}_0(M_p+M_p^3) = \mathrm{rs}\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix},$$

which is one of the closest codewords to $\mathcal{R}$.

The following example considers the ternary case. For simplicity we will use the logarithmic notation of the polynomials. Nonetheless, one could do everything also in polynomial form.

Example 3.23: Consider $\mathcal{G}_3(2,4)$ and the primitive polynomial $p(x) = x^4+x^3+1 \in \mathbb{F}_3[x]$. Let α be a root of $p(x)$ and M_p the companion matrix of $p(x)$. The four distinct orbits of $\langle M_p \rangle$ are given by the initial points

$$\mathcal{U}_0 = \mathrm{rs}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \cong \{0, 1, \alpha^{10}, \alpha^{20}, \alpha^{30}, \alpha^{40}, \alpha^{50}, \alpha^{60}, \alpha^{70}\},$$

$$\mathcal{U}_1 = \mathrm{rs}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \cong \{0, 1, \alpha, \alpha^{28}, \alpha^{37}, \alpha^{40}, \alpha^{41}, \alpha^{68}, \alpha^{77}\},$$

$$\mathcal{U}_2 = \mathrm{rs}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cong \{0, 1, \alpha^2, \alpha^{18}, \alpha^{25}, \alpha^{40}, \alpha^{42}, \alpha^{58}, \alpha^{65}\},$$

$$\mathcal{U}_3 = \mathrm{rs}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \cong \{0, 1, \alpha^5, \alpha^{11}, \alpha^{19}, \alpha^{40}, \alpha^{45}, \alpha^{51}, \alpha^{59}\}.$$

The orbit on the first initial point is the spread code that we want to consider. Note that the respective quotient sets $S_0, \ldots, S_3$ are again distinct. Assume that you received

$$\mathcal{R} = \mathrm{rs}\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \cong \{0, \alpha, \alpha^4, \alpha^5, \alpha^{32}, \alpha^{41}, \alpha^{44}, \alpha^{45}, \alpha^{72}\}.$$

Then we compute e.g.

$$\alpha^4/\alpha = \alpha^{40}/\alpha^{37} = \alpha^3$$

i.e. $\mathcal{R}$ is on the orbit of $\mathcal{U}_1$ and the inverse of the canonizing mapping is

$$\gamma^{-1}(\alpha) = \alpha^4/\alpha^{40} = \alpha/\alpha^{37} = \alpha^{44}.$$

Hence, we decode to

$$\mathcal{U}_0 M_p^{44} = \mathcal{U}_0 M_p^4 = \mathrm{rs} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Note that for any $\mathcal{U} \in \mathcal{G}_3(2,4)$ it holds that $\mathcal{U}M_p^i = \mathcal{U}M_p^{i+40}$.

In the same manner one can syndrome decode in $\mathcal{G}_q(k,n)$ for larger parameters. If $k \geqslant 3$ though, one needs more than just one quotient to uniquely determine the orbit and respective canonizer mapping for the received space.

Remark 3.24: The complexity of Algorithm 3.2, together with Remark 3.21, depends mainly on the number of quotients one has to compute to uniquely determine the orbit. Denote this number by ρ. The algorithm performs ρ many divisions and then k many multiplications over $\mathbb{F}_{q^n}$ for decoding. Moreover, the costs for looking up the orbit needs to be taken into account, which depends on the number of orbits there are in $\mathcal{G}_q(k,n)$ under the action of the corresponding irreducible cyclic group.

For the cases where ρ and the number of orbits are small (like in the examples before), the algorithm presented here has a better complexity than the other known algorithms, mentioned at the end of Section 3.1. The trade-off here is that the algorithm needs a lot of storage for the quotient sets of all orbits.

3.3 List Decoding in the Plücker Embedding

In this section we investigate the Plücker embedding of the Grassmannian and how it can be used for list decoding of constant dimension codes. Moreover, we give an explicit list decoding algorithm for lifted rank-metric codes that works by solving a system of linear bilinear equations in the Plücker embedding. The main results of this section were published by Rosenthal and Trautmann in [43, 44, 51] and by Trautmann, Rosenthal and Silberstein in [57].

3.3.1 The Plücker Embedding of $\mathcal{G}_q(k,n)$

To introduce the Plücker embedding we need the following notations.

$$\binom{[n]}{k} := \{(i_1,\ldots,i_k) \mid i_\ell \in \{1,\ldots,n\} \forall \ell, i_1 < \cdots < i_k\}$$

is the set of ordered monomials of length k with integer values up to n. If $U \in \mathbb{F}_q^{k\times n}$ and $(i_1,\ldots,i_k) \in \binom{[n]}{k}$, then we denote by $M_{i_1,\ldots,i_k}(U)$ the determinant of the submatrix of U, consisting of all columns of U indexed by $i_1,\ldots,i_k$. A determinant of a submatrix is also called a *minor* of the matrix. We need the following orders on $\binom{[n]}{k}$:

Definition 3.25: Let $(i_1,\ldots,i_k),(j_1,\ldots,j_k) \in \binom{[n]}{k}$. We define

$$(i_1,\ldots,i_k) < (j_1,\ldots,j_k) :\iff \exists N \in \mathbb{N} : i_\ell = j_\ell \ \forall \ell < N \text{ and } i_N < j_N,$$

$$(i_1,\ldots,i_k) \preceq (j_1,\ldots,j_k) :\iff i_\ell \leqslant j_\ell \ \forall \ell \in \{1,\ldots,k\}.$$

Naturally, for both orders it holds that

$$(i_1,\ldots,i_k) = (j_1,\ldots,j_k) :\iff i_\ell = j_\ell \ \forall \ell \in \{1,\ldots,k\}.$$

The total order $<$ is called the *lexicographic order*. The partial order $\prec$ is also known as the *Bruhat order*.

The finite projective space of dimension $n-1$, denoted by $\mathbb{P}_q^{n-1}$ (or $\mathbb{P}^{n-1}$ if the underlying field is clear from the context), is the set of all 1-dimensional subspaces through the origin of $\mathbb{F}_q^n$. To distinguish them from non-projective coordinates, we denote the projective coordinates of a point in $\mathbb{P}^{n-1}$ by $[x_1 : x_2 : \ldots : x_n]$. It is well-known that one can embed the Grassmannian into projective space as follows.

Theorem 3.26 ([29, 49]): *The map*

$$\begin{aligned}\varphi :\ \mathcal{G}_q(k,n) &\to \mathbb{P}^{\binom{n}{k}-1} \\ \mathrm{rs}(U) &\mapsto [M_{1,2,\ldots,k-1,k}(U) : M_{1,2,\ldots,k-1,k+1}(U) : \ldots : M_{n-k+1,\ldots,n}(U)]\end{aligned}$$

is injective. The image is called the Plücker *or* Grassmann embedding *of* $\mathcal{G}_q(k,n)$*. For* $\mathcal{U} \in \mathcal{G}_q(k,n)$*,* $\varphi(\mathcal{U})$ *constitutes the* Plücker coordinates *of* $\mathcal{U}$*. Note that, by convention, we order the determinants on the right side according to the respective column indices in lexicographic order.*

The Plücker-embedded Grassmannian forms a variety in the projective space:

Theorem 3.27 ([49, 50]): *Let* $n \geqslant 2k$ *and* $(i_1, \ldots, i_{k+1}) \in \binom{[n]}{k+1}, (i_{k+2}, \ldots, i_{2k}) \in \binom{[n]}{k-1}$*. For* $1 \leqslant \ell \leqslant k+1$ *denote by* σ_{i_ℓ} *the permutation such that* $\sigma_{i_\ell}(i_1, \ldots, i_{k+1}) = (i_1, \ldots, i_{\ell-1}, i_{\ell+1}, \ldots, i_{k+1}, i_\ell)$*. The equation*

$$\sum_{j \in \{i_1, \ldots, i_{k+1}\}} \operatorname{sgn}(\sigma_j) x_{i_1, \ldots, i_{k+1} \setminus j} x_{j, i_{k+2}, \ldots, i_{2k}} = 0$$

is called a shuffle relation *or* straightening syzygy *of* $\mathcal{G}_q(k,n)$*. The set of all shuffle relations completely describes* $\varphi(\mathcal{G}_q(k,n))$ *in the projective space of dimension* $\binom{n}{k} - 1$*. I.e.* $[x_{1,\ldots,k} : \ldots : x_{n-k+1,\ldots,n}] \in \mathbb{P}^{\binom{n}{k}-1}$ *describes the Plücker coordinates of an element of* $\mathcal{G}_q(k,n)$ *if and only if* $x_{1,\ldots,k}, \ldots, x_{n-k+1,\ldots,n}$ *fulfill all the shuffle relations.*

Note that in the shuffle relation above the index $(i_1, \ldots, i_{k+1} \setminus i_\ell)$ denotes the index $(i_1, \ldots, i_{\ell-1}, i_{\ell+1}, \ldots, i_{k+1})$ of length k.

Example 3.28: The shuffle relations of $\mathcal{G}_q(2,5)$ are given by

$$x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23} = 0,$$

$$x_{12}x_{35} - x_{13}x_{25} + x_{15}x_{23} = 0,$$

$$x_{12}x_{45} - x_{14}x_{25} + x_{15}x_{24} = 0,$$

$$x_{13}x_{45} - x_{14}x_{35} + x_{15}x_{34} = 0,$$

$$x_{23}x_{45} - x_{24}x_{35} + x_{25}x_{34} = 0.$$

The projective vector $[1:0:0:0:0:0:0:0:0:0]$ fulfills all the equations, hence it constitutes the Plücker coordinates of some element of $\mathcal{G}_q(2,5)$. On the other hand, $[1:0:0:0:0:0:0:1:0:0]$ does not fulfill the first equation since $x_{12} = x_{34} = 1$, hence there is no vector space in $\mathcal{G}_q(2,5)$ with this vector as its Plücker coordinates.

Proposition 3.29: *One can easily verify that there are at most* $\binom{n}{k+1}\binom{n}{k-1}$ *many different shuffle relations describing* $\mathcal{G}_q(k,n)$*.*

One of the great advantages of Plücker-embedding the Grassmannian is that the balls of a given radius t (with respect to the injection distance) form a variety in the Plücker embedding. I.e. we can give explicit equations that define all elements of such a ball. It is easy to compute the balls in the following special case. This fact is again well-known but we want to give our own version of the proof here.

Theorem 3.30: *Define* $\mathcal{U}_0 := \mathrm{rs}[\ I_{k\times k} \quad 0_{k\times(n-k)}\ ]$. *Then*

$$\begin{aligned} B_t^k(\mathcal{U}_0) &= \{\mathcal{V} \in \mathcal{G}_q(k,n) \mid M_{i_1,\ldots,i_k}(V) = 0\ \forall (i_1,\ldots,i_k) \not\leqslant (t+1,\ldots,k,n-t+1,\ldots,n)\} \\ &= \{\mathcal{V} \in \mathcal{G}_q(k,n) \mid M_{i_1,\ldots,i_k}(V) = 0\ \forall (i_1,\ldots,i_k) : i_{k-t} \geqslant k+1\} \end{aligned}$$

where $V \in \mathbb{F}_q^{k\times n}$ *such that* $\mathcal{V} = \mathrm{rs}(V)$.

PROOF: We want to find all $\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_q(k,n)$, such that

$$d_I(\mathcal{U}_0, \mathcal{V}) \leqslant t$$

$$\iff \mathrm{rank} \begin{bmatrix} I_{k\times k} & & 0_{k\times(n-k)} \\ & V & \end{bmatrix} \leqslant t + k,$$

i.e. at least $k-t$ many linearly independent elements of $\mathcal{V}$ have to be in $\mathcal{U}_0$. Thus, we can choose the matrix representation

$$V = \left[\begin{array}{c|c} * & 0_{(k-t)\times(n-k)} \\ \hline * & * \end{array}\right].$$

This implies that all minors of V that contain at least $t+1$ of the $n-k$ rightmost columns are zero (since the column rank is equal to the row rank). At the same time this is also a sufficient condition, since the $*$-blocks can be filled with anything (such that the whole matrix has rank k) and the row space will always be in the ball. Since the monomials are ordered, the condition that $t+1$ many coordinates of $(i_1,\ldots,i_k)$ are in $\{n-k+1,\ldots,n\}$ is equivalent to

$$i_\ell \geqslant k+1 \text{ for some } \ell \in \{1,\ldots,k-t\}$$

$$\iff i_{k-t} \geqslant k+1$$

which is in turn equivalent to

$$(i_1,\ldots,i_k) \not\leqslant (t+1,\ldots,k,n-t+1,\ldots,n). \qquad \square$$

With the knowledge of $B_t^k(\mathcal{U}_0)$ we can also express $B_t^k(\mathcal{U})$ for any $\mathcal{U} \in \mathcal{G}_q(k,n)$. For this, note that for any $\mathcal{U} \in \mathcal{G}_q(k,n)$ there exists an $A \in \mathrm{GL}_n$ such that $\mathcal{U}_0 A = \mathcal{U}$. Moreover,

$$B_t^k(\mathcal{U}_0 A) = B_t^k(\mathcal{U}_0) A.$$

Definition 3.31: For simplicity we denote by $A_{i_1,\ldots,i_k}[j_1,\ldots,j_k]$ the submatrix of A with columns indexed by $i_1,\ldots,i_k$ and rows indexed by $j_1,\ldots,j_k$, and define

$\bar{\varphi} : \mathrm{GL}_n \longrightarrow \mathrm{GL}_{\binom{n}{k}}$

$$A \longmapsto \begin{pmatrix} \det(A_{1,\dots,k}[1,\dots,k]) & \dots & \det(A_{n-k+1,\dots,n}[1,\dots,k]) \\ \vdots & & \vdots \\ \det(A_{1,\dots,k}[n-k+1,\dots,n]) & \dots & \det(A_{n-k+1,\dots,n}[n-k+1,\dots,n]) \end{pmatrix}.$$

Remark 3.32: It is easy to see that $\bar{\varphi}(A)$ has to be invertible, since any set of k rows of A span a different k-dimensional space and the rows of $\bar{\varphi}(A)$ correspond to the Plücker embedding of all those spaces. Since the Plücker embedding is injective we know that all rows of $\bar{\varphi}(A)$ are different and since they are projective coordinates, it follows that all these rows are actually linearly independent.

Lemma 3.33: *Let $\mathcal{U} \in \mathcal{G}_q(k,n)$ and $A \in \mathrm{GL}_n$. It holds that*

$$\varphi(\mathcal{U}A) = \varphi(\mathcal{U})\bar{\varphi}(A).$$

PROOF: Let $U \in \mathbb{F}_q^{k\times n}$ such that $\mathrm{rs}(U) = \mathcal{U}$. Let $V := UA$ and denote by u_{ij}, a_{ij}, v_{ij} the entry in the i-th row and j-th column of U, A, V, respectively. Then it holds that $v_{ij} = \sum_{\ell=1}^{n} u_{i\ell}a_{\ell j}$ and hence $V_{i_1,\dots,i_k} = UA_{i_1,\dots,i_k}$. This implies that

$$\begin{aligned}\varphi(\mathcal{U}A) &= [M_{1,2,\dots,k-1,k}(UA) : M_{1,2,\dots,k-1,k+1}(UA) : \dots : M_{n-k+1,\dots,n}(UA)] \\ &= [\det(V_{1,\dots,k}) : \det(V_{1,2,\dots,k-1,k+1}) : \dots : \det(V_{n-k+1,\dots,n})] \\ &= [\det(UA_{1,\dots,k}) : \det(UA_{1,2,\dots,k-1,k+1}) : \dots : \det(UA_{n-k+1,\dots,n})].\end{aligned}$$

With the Cauchy-Binet formula we know that

$$\det(UA_{i_1,\dots,i_k}) = \sum_{(\ell_1,\dots,\ell_k)\in\binom{[n]}{k}} \det(U_{\ell_1,\dots,\ell_k}) \det(A_{i_1,\dots,i_k}[\ell_1,\dots,\ell_k])$$

and hence

$$\begin{aligned}\varphi(\mathcal{U}A) &= [\det(UA_{1,\dots,k}) : \det(UA_{1,2,\dots,k-1,k+1}) : \dots : \det(UA_{n-k+1,\dots,n})] \\ &= \varphi(\mathcal{U})\bar{\varphi}(A).\end{aligned}$$

□

Theorem 3.34: *Let $\mathcal{U} = \mathcal{U}_0 A \in \mathcal{G}_q(k,n)$. Denote a matrix representation of $\mathcal{V} \in \mathcal{G}_q(k,n)$ by $V \in \mathbb{F}_q^{k\times n}$. Then*

$$B_t^k(\mathcal{U}) = B_t^k(\mathcal{U}_0 A) = \{\mathcal{V} \in \mathcal{G}_q(k,n) \mid M_{i_1,\dots,i_k}(V\bar{\varphi}(A^{-1})) = 0 \forall (i_1,\dots,i_k) : i_{k-t} > k\}.$$

There are always several choices for $A \in \mathrm{GL}_n$ such that $\mathcal{U}_0 A = \mathcal{U}$. Since $GL_{\binom{n}{k}}$ is very large we try to choose A as simple as possible. We explain one such construction and the computation of its inverse in Algorithms 3.3 and 3.4.

It is easy to see that Algorithm 3.3 works, i.e. that it computes an invertible matrix A such that $\mathcal{U} = \mathcal{U}_0 A$.

Algorithm 3.3 Construction of A such that $\mathcal{U} = \mathcal{U}_0 A \in \mathcal{G}_q(k,n)$.

- The first k rows of A are equal to the matrix representation U of $\mathcal{U}$.
- Find the pivot columns of U (assume that U is in RREF).
- Fill up the respective columns of A with zeros in the lower $n-k$ rows.
- Fill up the remaining submatrix of size $(n-k)\times(n-k)$ with an identity matrix.

Algorithm 3.4 Computing A^{-1} for a given A from Algorithm 3.3.

- Find a permutation σ on $\{1,\ldots,n\}$ that permutes the columns of A such that

$$\sigma(A) = \begin{pmatrix} I_{k\times k} & U'' \\ 0 & I_{(n-k)\times(n-k)} \end{pmatrix}.$$

- Then the inverse of that matrix is

$$\sigma(A)^{-1} = \begin{pmatrix} I_{k\times k} & -U'' \\ 0 & I_{(n-k)\times(n-k)} \end{pmatrix}.$$

- Apply σ^{-1} on the rows of $\sigma(A)^{-1}$. The result is A^{-1}.

Proposition 3.35: *Algorithm 3.4 computes the inverse of the input A.*
PROOF: Represent the column permutation σ by a permutation matrix $S \in \mathrm{GL}_n$ (acting from the left on A). It holds that S represents the inverse permutation σ^{-1} on the rows of A when applied from the right. Then one gets $(SA)^{-1}S = A^{-1}S^{-1}S = A^{-1}$.□
Example 3.36: In $\mathcal{G}_2(2,4)$ we want to find

$$B_1^2(\mathcal{U}) = \{\mathcal{V} \in \mathcal{G}_2(2,4) \mid \dim(\mathcal{V}\cap\mathcal{U}) = 1\}$$

for

$$\mathcal{U} = \mathrm{rs}(U) = \mathrm{rs}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

We find the pivot columns U_1, U_3 and build

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then we find the column permutation $\sigma = (23)$ such that

$$\sigma(A) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Now we can easily invert as described in Algorithm 3.4 and see that $\sigma(A)^{-1} = \sigma(A)$. We apply $\sigma^{-1} = \sigma$ on the rows and get

$$A^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then

$$\varphi(A^{-1}) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

We denote a matrix representation of $\mathcal{V} \in \mathcal{G}_q(k,n)$ by $V \in \mathbb{F}_q^{k\times n}$. From Theorem 3.34 we know that

$$\begin{aligned} B_1^2(\mathcal{U}) &= \{\mathcal{V} \in \mathcal{G}_2(2,4) \mid M_{i_1,i_2}(V)\bar{\varphi}(A^{-1}) = 0 \ \forall (i_1,i_2) \not\leq (2,4)\} \\ &= \{\mathcal{V} \in \mathcal{G}_2(2,4) \mid M_{3,4}(V)\bar{\varphi}(A^{-1}) = 0\}. \end{aligned}$$

It holds that $\varphi(\mathcal{V})\bar{\varphi}(A^{-1}) = [M_{1,3}(V) : M_{1,2}(V) : M_{1,3}(V) + M_{1,4}(V) : M_{2,3}(V) : M_{3,4}(V) : M_{2,3}(V) + M_{2,4}(V)]$ and hence

$$\begin{aligned} B_1^2(\mathcal{U}) =& \{\mathcal{V} \in \mathcal{G}_2(2,4) \mid M_{2,3}(V) + M_{2,4}(V) = 0\} \\ =& \{\mathcal{V} \in \mathcal{G}_2(2,4) \mid M_{2,3}(V) = M_{2,4}(V)\}. \end{aligned}$$

Note that we do not even have to compute the whole matrix $\varphi(A^{-1})$ since in this case we only need the last column of it to find the equations that define $B_1^2(\mathcal{U})$.

Proposition 3.37: *The number of equations describing $B_t^k(\mathcal{U})$ around some $\mathcal{U} \in \mathcal{G}_q(k,n)$ is*

$$\tau = \sum_{\ell=0}^{k-t-1} \begin{bmatrix} n-k \\ k-\ell \end{bmatrix} \begin{bmatrix} k \\ \ell \end{bmatrix} = \begin{bmatrix} n \\ k \end{bmatrix} - \sum_{\ell=k-t}^{k} \begin{bmatrix} n-k \\ k-\ell \end{bmatrix} \begin{bmatrix} k \\ \ell \end{bmatrix}.$$

PROOF: It follows from Theorem 3.34 that the number of equations is equal for any $\mathcal{U} \in \mathcal{G}_q(k,n)$. Hence, we can count them in the description of $B_t^k(\mathcal{U}_0)$ from Theorem 3.30. The condition that $(i_1,\ldots,i_k) \not\leq (t+1,\ldots,k,n-t+1,\ldots,n)$ is equivalent to

$$\exists \ell \in \{1,\ldots,k-e\} : i_\ell > k.$$

For such an ℓ there are $k-\ell+1$ entries chosen freely from $\{k+1,\ldots,n\}$ and $\ell-1$ entries from $\{1,\ldots,k\}$. Hence there are

$$\sum_{\ell=1}^{k-t} \begin{bmatrix} n-k \\ k-\ell+1 \end{bmatrix} \begin{bmatrix} k \\ \ell-1 \end{bmatrix} = \sum_{\ell=0}^{k-t-1} \begin{bmatrix} n-k \\ k-\ell \end{bmatrix} \begin{bmatrix} k \\ \ell \end{bmatrix}$$

many elements in $\begin{bmatrix} [n] \\ k \end{bmatrix}$ that are $\not\leq (t+1,\ldots,k,n-t+1,\ldots,n)$, which is equal to the number of equations defining $B_t^k(\mathcal{U})$. □

Remark 3.38: We can generalize all the previous results to received spaces $\mathcal{R} \in \mathcal{P}_q(n)$ with $\dim(\mathcal{R}) \neq k$. I.e. we can describe the ball inside the Grassmannian $\mathcal{G}_q(k,n)$ around a subspace of a different dimension $B_t^k(\mathcal{R})$ by linear equations in the Plücker embedding. For this, one only needs to adjust the conditions for the zero-minors in Theorem 3.30. Then Proposition 3.37 changes analogously. All other results, in particular Theorem 3.34, still hold without any changes.

Example 3.39: We want to describe the ball of radius 1 in $\mathcal{G}_q(2,4)$ around the received word $\mathcal{R} = \mathrm{rs}(1\ 0\ 0\ 0)$. We know that $d_I(\mathcal{R},\mathcal{U}) \leqslant t \iff \dim(\mathcal{R} \cap \mathcal{U}) \geqslant 2-t$ for any $\mathcal{U} \in \mathcal{G}_q(2,4)$. For $t=1$ we get that the dimension of the intersection has to be at least 1. Thus we can choose a matrix representation of the form

$$V = \left[\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ \hline * & * & * & * \end{array}\right]$$

for each vector space in the ball. Hence, the minors not containing the first column have to be zero:

$$B_1^2(\mathcal{R}) = \{\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_q(2,4) \mid M_{2,3}(V) = M_{2,4}(V) = M_{3,4}(V) = 0\}.$$

To sum up, we have an efficient way to describe the balls in the Grassmannian $\mathcal{G}_q(k,n)$ around an arbitrary element of $\mathcal{P}_q(n)$ by linear equations in the Plücker embedding. If in addition one can describe a constant dimension code in the Plücker embedding and efficiently decide if some Plücker coordinates describe a codeword, one has a list decoder for this code. In the next subsection we describe such a list decoder in the Plücker embedding for lifted rank-metric codes.

3.3.2 List Decoding of Lifted Rank-Metric Codes

We will now show how a complete list decoding algorithm in the Plücker embedding can be defined for lifted rank-metric codes. The main idea here is that a subset of the Plücker coordinates of lifted rank-metric codes constitutes a linear block code and can hence be described as a the kernel of a parity check matrix.

Let $C \subseteq \mathbb{F}_q^{k\times(n-k)}$ be an MRD code with minimum rank distance δ. Then by Lemma 2.7 its lifting is a code $\mathcal{C}$ of cardinality $q^{(n-k)(k-\delta+1)}$ in the Grassmannian $\mathcal{G}_q(k,n)$. Let

$$x^{\mathcal{A}} = [x^{\mathcal{A}}_{1,\ldots,k} : \ldots : x^{\mathcal{A}}_{n-k+1,\ldots,n}] \in \mathbb{P}^{\binom{n}{k}-1}$$

be a vector which represents the Plücker coordinates of a subspace $\mathcal{A} \in \mathcal{G}_q(k,n)$.

Lemma 3.40: *If $x^{\mathcal{A}}$ is normalized (i.e. the first non-zero entry is equal to one), then $x^{\mathcal{A}}_{1,\ldots,k} = 1$ for any $\mathcal{A} \in \mathcal{C}$.*

PROOF: Follows from the fact that each element of a lifted rank-metric code has an identity in the first k columns of its reduced row echelon form. □

Let $[k] = \{1, 2, \ldots, k\}$, and let $\underline{i} = \{i_1, i_2, \ldots, i_k\}$ be a set of indices such that $|\underline{i} \cap [k]| = k - 1$. Let $t \in \underline{i}$, such that $t > k$, and $s = [k] \backslash \underline{i}$.

Lemma 3.41: *Consider $A \in C$ and $\mathcal{A} = \mathrm{rs}[\ I_k\ A\ ]$. If $x^{\mathcal{A}}$ is normalized, then $x^{\mathcal{A}}_{\underline{i}} = (-1)^{k-s} A_{s,t-k}$.*

PROOF: It holds that $x^{\mathcal{A}}$ is normalized if its entries are the minors of the reduced row echelon form of $\mathcal{A}$, which is $[\ I_k\ A\ ]$. Because of the identity matrix in the first k columns, the statement follows directly from the definition of the Plücker coordinates. □

Note that we do not have to worry about the normalization since $x^{\mathcal{A}}$ is projective. In the following we will always assume that any element from $\mathbb{P}^{\binom{n}{k}-1}$ is normalized.

With Lemma 3.41 one can easily show, that a subset of the Plücker coordinates of a lifted Gabidulin code forms a linear code over $\mathbb{F}_q$:

Theorem 3.42: *The restriction of the set of Plücker coordinates of an $(n, q^{(n-k)(k-\delta+1)}, \delta, k)_q$-lifted MRD code $\mathcal{C}$ to the set $\{\underline{i} : |\underline{i}| = k, |\underline{i} \cap [k]| = k - 1\}$ forms a linear code C^p over $\mathbb{F}_q$ of length $k(n-k)$, dimension $(n-k)(k-\delta+1)$ and minimum Hamming distance $d_{\min} \geqslant \delta$.*

PROOF: Since C is linear, it holds that for every $A, B \in C$ we have $A + B \in C$. Together with Lemma 3.41 we have the same property when we consider the restriction of the set of Plücker coordinates of a lifted MRD code to the set $\{\underline{i} : |\underline{i}| = k, |\underline{i} \cap [k]| = k - 1\}$. This set is of size $k(n-k)$, and therefore we obtain a linear code C^p of length $k(n-k)$ and the same dimension as C, i.e. $(n-k)(k-\delta+1)$. Since the rank of each non-zero $A \in C$ is greater or equal to δ, also the number of non-zero entries of A has to be greater or equal to δ, hence the minimum Hamming distance $d_{\min}$ of C^p satisfies $d_{\min} \geqslant \delta$. □

Example 3.43: Let $\alpha \in \mathbb{F}_{2^2}$ be a primitive element, fulfilling $\alpha^2 = \alpha + 1$. Let $C \subseteq \mathbb{F}_2^{2\times 2}$ be a Gabidulin MRD code with minimum rank distance $\delta = 2$, whose generator matrix is $G = (\alpha\ 1)$. Hence,

$$C = \{(b\alpha, b) \mid b \in \mathbb{F}_{2^2}\}.$$

The codewords of C, their representation as 2×2 matrices, their lifting to $\mathcal{G}_2(2,4)$ and the respective Plücker coordinates are given in the following table.

vector representation	matrix representation	lifting	Plücker coordinates
$(0,0)$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$	$[1:0:0:0:0:0]$
$(\alpha,1)$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$	$[1:1:0:0:1:1]$
(α^2,α)	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$	$[1:1:1:1:0:1]$
$(1,\alpha^2)$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$	$[1:0:1:1:1:1]$

In this example the second to fifth Plücker coordinates form the linear code $C^p = \{(0000), (1001), (1110), (0111)\}$ of length 4 and dimension 2 in the Hamming space. Its parity-check matrix is

$$H^p = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

In other words, a Plücker coordinate vector $[x_{12} : x_{13} : x_{14} : x_{23} : x_{24} : x_{34}]$ of a vector space from $\mathcal{G}_2(2,4)$ represents a codeword of the lifted Gabidulin code from above if and only if $x_{12} = 1$, $x_{14} + x_{23} = 0$, and $x_{13} + x_{23} + x_{24} = 0$.

If one chooses Gabidulin's construction for a lifted MRD code and $\delta = k$, then one can find a general description for the parity check matrix of the linear code C^p as follows.

Proposition 3.44: *Let $p(x) \in \mathbb{F}_q[x]$ be a monic primitive polynomial of degree $n-k$. Let α be a root of $p(x)$ and M_p the companion matrix of $p(x)$. If $k = \delta$ and the generator matrix of the respective Gabidulin code is $G = (\alpha^{k-1} \;\; \alpha^{k-2} \;\; \dots \;\; \alpha \;\; 1)$, then the parity check matrix H^p is a $(k-1)(n-k) \times k(n-k)$-matrix of the form*

$$H^p = \left(\begin{array}{c|c|c|c|c} I_{(n-k)\times(n-k)} & 0 & \dots & 0 & (-1)^{k-2}(M_p^{-k+1})^T \\ \hline 0 & I_{(n-k)\times(n-k)} & \dots & 0 & (-1)^{k-3}(M_p^{-k+2})^T \\ \hline \vdots & & \ddots & & \vdots \\ \hline 0 & 0 & \dots & I_{(n-k)\times(n-k)} & (M_p^{-1})^T \end{array}\right).$$

PROOF: For simplicity we denote the vector space isomorphism $\phi^{(n-k)}$ by ϕ. With the given generator matrix G, the non-zero codewords of the Gabidulin code are $(\phi(\alpha^{i+k-1}) \;\; \phi(\alpha^{i+k-2}) \;\; \dots \;\; \phi(\alpha^{i+1}) \;\; \phi(\alpha^i))^T$ for $i = 0, \dots, q^{(n-k)} - 2$. Hence, the non-zero codewords of C^p are of the form $(\phi(\alpha^i) \mid -\phi(\alpha^{i+1}) \mid \dots \mid (-1)^{k-2}\phi(\alpha^{i+k-2}) \mid (-1)^{k-1}\phi(\alpha^{i+k-1}))$ (follows from Lemma 3.41). Then it holds that

$$\begin{aligned} &(\phi(\alpha^i) \mid -\phi(\alpha^{i+1}) \mid \dots \mid (-1)^{k-1}\phi(\alpha^{i+k-1})) \begin{pmatrix} I & 0 & \dots & 0 & (-1)^{k-2}(M_p^{-k+1})^T \end{pmatrix}^T \\ &= \phi(\alpha^i) + (-1)^{k-1+k-2}\phi(\alpha^{i+k-1})M_p^{-k+1} \\ &= \phi(\alpha^i) - \phi(\alpha^{i+k-1})M_p^{-k+1} \\ &= \phi(\alpha^i) - \phi(\alpha^i) = 0, \end{aligned}$$

which means that the multiplication of any codeword of C^p with the first block row of H^p results in 0. Analogously one can show the same for the other block rows. Since the matrix H^p has full rank, it follows that this is a parity check matrix of the code. □

Example 3.45: Consider again Example 3.43. It holds that $H^p = [\, I_{2\times 2} \; (M_p^{-1})^T \,]$.

The List Decoding Algorithm

We now have all the machinery needed to describe a list decoding algorithm for lifted rank-metric codes in the Plücker coordinates under the assumption that the received

word has the same dimension as the codewords. Consider a lifted rank-metric code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ with minimum rank distance δ and denote its corresponding linear block code over $\mathbb{F}_q$ (of length $k(n-k)$ and dimension $(n-k)(k-\delta+1)$) by C^p. The corresponding parity check matrix is denoted by H^p. Let $\mathcal{R} = \mathrm{rs}(R) \in \mathcal{G}_q(k,n)$ be the received word and let t be the decoding radius.

We just showed how a subset of the Plücker coordinates of an LG code forms a linear block code that is defined through the parity check matrix H^p. Since we want to describe a list decoding algorithm inside the whole set of Plücker coordinates, we define an extension of H^p as follows:

$$\bar{H}^p = \begin{pmatrix} 0_{(\delta-1)(n-k)\times 1} & H^p & 0_{(\delta-1)(n-k)\times \ell} \end{pmatrix}$$

where $\ell = \binom{n}{k} - k(n-k) - 1$. Then $[x_{1\ldots k} : \ldots : x_{n-k+1\ldots n}]\bar{H}^{pT} = 0$ gives rise to the same equations as $[x_{i_1} : \ldots : x_{i_{k(n-k)}}]H^{pT} = 0$, for $i_1, \ldots, i_{k(n-k)} \in \underline{i}$. For simplicity we will sometimes write $\bar{x}$ for $[x_{1\ldots k} : \ldots : x_{n-k+1\ldots n}]$ in the following.

Algorithm 3.5 states a complete list decoding algorithm for a lifted MRD code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ and a received word $\mathcal{R} \in \mathcal{P}_q(n)$.

Algorithm 3.5 Basic list decoding algorithm.

Require: received word $\mathcal{R}$, decoding radius t, parity check matrix $\bar{H}^p$

Find the equations defining $B_t(\mathcal{R})$ in the Plücker coordinates (cf. Section 3.3.1).

Solve the system of equations, that arise from $\bar{x}\bar{H}^p = 0$, together with the equations of $B_t(\mathcal{R})$, the shuffle relations for G and the equation $x_{1,\ldots,k} = 1$.

return the solutions $\bar{x} = [x_{1\ldots k} : \ldots : x_{n-k+1\ldots n}]$ of this system of equations

Theorem 3.46: *Algorithm 3.5 outputs the complete list L of codewords (in Plücker coordinate representation), such that for each element $\bar{x} \in L$, $d_I(\varphi^{-1}(\bar{x}), \mathcal{R}) \leqslant t$.*

PROOF: The solution set to the shuffle relations is exactly $\varphi(\mathcal{G}_q(k,n))$, i.e. all the elements of $\mathbb{P}^{\binom{n}{k}-1}$ that are Plücker coordinates of a k-dimensional vector space in $\mathbb{F}_q^n$ (see Theorem 3.27). The subset of this set with the condition $x_{1,\ldots,k} = 1$ is exactly the set of Plücker coordinates of elements in $\mathcal{G}_q(k,n)$ whose reduced row echelon form has $I_{k\times k}$ as the left-most columns. Intersecting this with the solution set of the equations given by $\bar{H}^p$ achieves the Plücker coordinates of the lifted MRD code $\mathcal{C}$. The intersection with $B_t^k(\mathcal{R})$ is then given by the additional equations from the first step of the algorithm. Thus the solution set to the whole system of equations consists of the Plücker coordinates of the elements of $\mathcal{C} \cap B_t^k(\mathcal{R})$. □

Example 3.47: We consider the $(4,4,2,2)_2$-code from Example 3.43. Assume we received

$$\mathcal{R}_1 = \mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

We would like to find all words within injection radius 1. Thus we first find the equations for the ball of injection radius 1:

$$B_1^2(\mathcal{U}_0) = \{\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_2(2,4) \mid M_{3,4}(V) = 0\}$$

We construct A_1^{-1} according to Algorithms 3.3 and 3.4

$$A_1^{-1} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

and compute the last column of $\bar{\varphi}(A_1^{-1})$:

$$[1:0:0:1:0:0]^T.$$

Thus, we get that

$$B_1^2(\mathcal{R}_1) = \{\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_2(2,4) \mid M_{1,4}(V) + M_{2,3}(V) = 0\}.$$

Then combining with the parity check equations from Example 3.43 we obtain the following system of linear equations to solve

$$\begin{aligned} x_{13} + x_{14} + x_{24} = 0, \quad & x_{14} + x_{23} = 0 \\ x_{12} + x_{23} = 0, \quad & x_{12} = 1 \end{aligned}$$

where the upper two equations arise from $\bar{H}^p$, the third from $B_1^2(\mathcal{R}_1)$ and the last one is the always given one. This system has the two solutions $(1,1,1,1,0)$ and $(1,0,1,1,1)$ for $(x_{12}, x_{13}, x_{14}, x_{23}, x_{24})$. Since we used all the equations defining the ball in the system of equations, we know that the two codewords corresponding to these two solutions (i.e. the third and fourth in Example 3.43) are the ones with distance 1 from the received space, and we do not have to solve x_{34} at all. The corresponding codewords are

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

Example 3.48: Consider the same code, but now assume we received

$$\mathcal{R}_2 = \mathrm{rs}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

As previously, we construct A_2^{-1} according to Algorithms 3.3 and 3.4

$$A_2^{-1} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and compute the last column of $\bar{\varphi}(A_2^{-1})$:

$$[1:1:0:1:1:1]^T.$$

Thus, we get that

$$B_1^2(\mathcal{R}_2) = \{\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_2(2,4) \mid M_{1,2}(V)+M_{1,3}(V)+M_{2,3}(V)+M_{2,4}(V)+M_{3,4}(V) = 0\}.$$

Then combining with the parity check equations from Example 3.43 and the shuffle relation $x_{12}x_{34} + x_{13}x_{24} + x_{14}x_{23} = 0$ we obtain the following system of linear and bilinear equations

$$\begin{aligned} x_{13} + x_{14} + x_{24} = 0, \quad x_{14} + x_{23} = 0 \\ x_{12} + x_{13} + x_{23} + x_{24} + x_{34} = 0, \quad x_{12} = 1 \\ x_{12}x_{34} + x_{13}x_{24} + x_{14}x_{23} = 0 \end{aligned}$$

We rewrite these equations in terms of the variables, that describe the linear code C^p, $x_{13}, x_{14}, x_{23}, x_{24}$:

$$\begin{aligned} x_{13} + x_{14} + x_{24} = 0 \\ x_{14} + x_{23} = 0 \\ x_{13} + x_{23} + x_{24} + x_{13}x_{24} + x_{14}x_{23} = 1 \end{aligned}$$

This system has three solutions $(1,0,0,1)$, $(0,1,1,1)$, and $(1,1,1,0)$ for $(x_{13}, x_{14}, x_{23}, x_{24})$. The corresponding codewords are

$$\mathrm{rs}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

Remark 3.49: One can easily extend this algorithm to multi-component lifted rank-metric codes. Then one needs to add the following step in the beginning of Algorithm 3.5: *Find the possible component codes that the elements of the ball can be in.*

To find all possible component codes one can use the following fact.

Theorem 3.50: *Let* $\mathcal{R} = \mathrm{rs}[\ R_1\ \ R_2\ \ R_3\ ] \in \mathcal{P}_q(n)$ *with* $\dim(\mathcal{R}) = k'$ *and* $R_1 \in \mathbb{F}_q^{k' \times j}, R_2 \in \mathbb{F}_q^{k' \times k}, R_3 \in \mathbb{F}_q^{k' \times (n-k-j)}$. *Moreover, let* $A \in \mathbb{F}_q^{k \times (n-k-j)}$. *If it holds that* $d_I(\mathrm{rs}[\ 0_{k\times j}\ I_{k\times k}\ A\ ], \mathcal{R}) \leqslant t$, *then the rank of* R_2 *is at least* $\max\{k,k'\} - t$.

PROOF: It holds that

$$\begin{aligned} & d_I(\mathrm{rs}[\ 0_{k\times j}\ I_{k\times k}\ A\ ], \mathrm{rs}(R)) \leqslant t \\ \iff & \mathrm{rank}\begin{pmatrix} 0_{k\times j} & I_{k\times k} & A \\ R_1 & R_2 & R_3 \end{pmatrix} - (k+k') + \max\{k,k'\} \leqslant t \\ \iff & \mathrm{rank}\begin{pmatrix} I_{k\times k} & 0_{k\times j} & A \\ R_2 & R_1 & R_3 \end{pmatrix} \leqslant t + (k+k') - \max\{k,k'\}. \end{aligned}$$

Since any of the lower k' vectors of the matrix on the left side can only be linearly dependent on the upper k rows if not all of the first k entries are zero, it holds that the left side of the inequality is greater than or equal to $k + (k' - \dim(R_2))$. Thus, if $d_I(\mathrm{rs}[\, 0_{k\times j}\ I_{k\times k}\ A\,], \mathcal{R}) \leqslant t$, then

$$k + (k' - \dim(R_2)) \leqslant t + (k + k') - \max\{k, k'\}$$

$$\iff \dim(R_2) \geqslant \max\{k, k'\} - t. \qquad \square$$

Corollary 3.51: *Consider the setting of Theorem 3.50 and a multi-component code $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ as defined in Theorem 2.9. All component codes, that elements of the ball $B_t^k(\mathcal{R})$ could possibly be in, must fulfill the following: If the leading identity block of the component code is in columns $j+1, \ldots, j+k$ for some $j \in \{0, \ldots, n-k\}$, then the rank of the submatrix $R_{j,\ldots,j+k}$ of R is at least $\max\{k, k'\} - t$.*

Therefore, we need to run Algorithm 3.5 for each component code that fulfills the condition of Corollary 3.51 separately to find all codewords of a multicomponent code inside the ball $B_t^k(\mathcal{R})$.

Complexity of the Algorithm

For the analysis of the complexity of Algorithm 3.5 denote by τ the number of equations that define $B_t^k(\mathcal{U})$ from Proposition 3.37.

Lemma 3.52: *Let $A^{-1} \in \mathrm{GL}_n$ be the matrix computed according to Algorithm 3.4, such that $\mathcal{U}_0 A = \mathcal{R}$. Then each column of $\bar{\varphi}(A^{-1})$ has at most $\binom{2k}{k}$ non-zero elements.*

PROOF: Consider the notation of Algorithm 3.4. Since $\sigma(A)^{-1}$ and A^{-1} only differ in a row permutation, it is clear that also $\bar{\varphi}(\sigma(A)^{-1})$ and $\bar{\varphi}(A^{-1})$ only differ in a row permutation. Thus, we want to count the non-zero minors of

$$\sigma(A)^{-1} = \begin{pmatrix} I_k & -U'' \\ 0 & I_{n-k} \end{pmatrix}.$$

Because of the identity blocks it is easy to see that each set of k columns has at least $n - 2k$ zero rows. Since any minor containing one of these zero rows is zero, it follows that at most $\binom{2k}{k}$ of the $\binom{n}{k}$ minors can be non-zero. Then the statement follows. $\square$

Theorem 3.53: *The complexity of Algorithm 3.5 is dominated by solving the system of $\tau + 1 + (\delta - 1)(n - k) + \binom{n}{2k}$ linear and bilinear equations in $\binom{n}{k}$ variables. This has a complexity that is polynomial in n and exponential in k.*

In most of the examples we computed though, we only needed a subset of all equations to get the solutions. For this, note that the actual information is encoded in the rank-metric code part of the matrix representation of the vector space, i.e. in the Plücker coordinates corresponding to C^p. Hence, one does not need the $k \times n$-matrix

representation of the solutions from an application point of view, since the information can be extracted directly from the Plücker coordinate representation of the vector spaces. On the other hand, because of this structure it is also straight-forward to construct the matrix representation by using Lemma 3.41 (i.e. without any computation needed). So, the number of variables in the system could be reduced to $k(n-k)$, and this can decrease the complexity of the algorithm. One can find this illustrated in Examples 3.47 and 3.48.

Bounds on the list size

A question that always arises when thinking about list decoding is how many codewords one has in a ball of a given radius, i.e. the list size of the decoder. Bounds for the list size for classical Gabidulin list decoding have already been derived and can be found e.g. in [60]. We can use these bounds for deriving bounds for the list size of lifted Gabidulin codes. To do so we must again assume that the received word has the same dimension as the codewords.

Theorem 3.54: *The list size of a list decoder for a lifted Gabidulin code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ is less than or equal the list size of a list decoder for the corresponding Gabidulin code $C \subseteq \mathbb{F}_q^{k\times(n-k)}$, with equality when the received word is of the type $\mathcal{R} = \mathrm{rs}[\ I_{k\times k}\ A\ ] \in \mathcal{G}_q(k,n)$ for some $A \in \mathbb{F}_q^{k\times(n-k)}$.*

PROOF: Assume $\mathcal{R} = \mathrm{rs}[\ I_k\ A\ ] \in \mathcal{G}_q(k,n)$. Then $d_I(\mathcal{R}, \mathrm{rs}[\ I_k\ B\ ]) = \mathrm{rank}(A-B)$, for any $B \in \mathbb{F}_q^{k\times(n-k)}$, hence the list sizes of both decoders are equal.

For the general case, i.e. when $\mathcal{R}$ has arbitrary shape, we prove that $|B_t^k(\mathcal{R}) \cap \mathcal{C}| \leqslant |B_t^k(\mathrm{rs}[\ I_k\ \bar{R}\ ]) \cap \mathcal{C}|$ for some $\bar{R} \in \mathbb{F}_q^{k\times(n-k)}$. For this let R be the reduced row echelon form of $\mathcal{R}$. We can write R as follows

$$R = \left(\begin{array}{c|c} J_{\ell\times k} & R_1 \\ \hline 0_{(k-\ell)\times k} & R_2 \end{array}\right),$$

such that $\mathrm{rank}\,(J_{\ell\times k}) = \ell$. If some codeword $\mathcal{U} = \mathrm{rs}[\ I_k\ B\ ]$ of the lifted Gabidulin code is in the ball $B_t^k(\mathcal{R})$, then $\dim(\mathcal{U}\cap\mathcal{R}) \geqslant k-t$ and this intersection can only happen in the row space of $[\ J_{\ell\times k}\ R_1\ ]$. It follows that $\mathcal{U}$ is also in the ball of radius t around the row space of

$$R^* = \left(\begin{array}{c|c} J_{\ell\times k} & R_1 \\ \hline J^C & R_2 \end{array}\right),$$

where $J^C \in \mathbb{F}_q^{(k-\ell)\times k}$ such that the first k columns of R^* form a matrix of rank k. It holds that $\mathrm{rs}(R^*) = \mathrm{rs}[\ I_k\ \bar{R}\ ]$ for some $\bar{R} \in \mathbb{F}_q^{k\times(n-k)}$ and thus the statement follows. □

Corollary 3.55: *Consider a lifted Gabidulin code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ with minimum injection distance δ. Denote by ℓ the list size of a list decoding algorithm which decodes up to*

injection radius t. Then

$$\ell \leqslant \sum_{i=\lfloor \frac{\delta-1}{2} \rfloor+1}^{t} \frac{\begin{bmatrix} k \\ 2i+1-\delta \end{bmatrix}_q}{\begin{bmatrix} i \\ 2i+1-\delta \end{bmatrix}_q}.$$

PROOF: It follows from Theorem 3.54 that the upper bound for the list size of a list decoder for classical Gabidulin codes is also an upper bound for the list size of a list decoder for lifted Gabidulin codes with the corresponding parameters. In this case we used the bound for classical Gabidulin codes from [60]. □

Chapter 4

Isometry Classes and Automorphism Groups

In this chapter we investigate the isometry classes and automorphism groups of subspace codes in general and of constant dimension codes in particular. The results of this chapter were published by Trautmann in [52].

One needs to define isometry classes of subspace codes and a canonical representative of each class to compare codes among each other. On the other hand, a canonical form and automorphism groups are important for the theory of orbit codes, as discussed in Section 2.5, since different subgroups can possibly generate the same orbit. Hence, one needs a canonical way to compare orbit codes among each other. This can be done via the automorphism groups of the codes, since these are the maximal generating groups for a given orbit code and they contain all other generating subgroups of it.

We first need some additional preliminary knowledge for our investigations.

Definition 4.1: The *general semilinear group* $\Gamma\mathrm{L}_n(q)$ is defined as the semidirect product of the general linear group and the automorphism group of $\mathbb{F}_q$, i.e.

$$\Gamma\mathrm{L}_n(q) := \mathrm{GL}_n(q) \rtimes \mathrm{Aut}(\mathbb{F}_q).$$

The multiplication of two elements of $\Gamma\mathrm{L}_n(q)$ is given by

$$(A, \varphi)(B, \varphi') := (A\,\varphi^{-1}(B), \varphi\varphi').$$

If the underlying field is clear from the context we abbreviate $\Gamma\mathrm{L}_n(q)$ by $\Gamma\mathrm{L}_n$.

Lemma 4.2: *The $\Gamma\mathrm{L}_n$-multiplication*

$$\begin{array}{ccc} \mathcal{G}_q(k,n) \times \Gamma\mathrm{L}_n & \longrightarrow & \mathcal{G}_q(k,n) \\ (\mathcal{U}, (A,\varphi)) & \longmapsto & \mathcal{U}(A,\varphi) := \varphi(\mathcal{U}A) \end{array}$$

defines a group action from the right on $\mathcal{G}_q(k,n)$ (for any $k \leqslant n$) and hence on $\mathcal{P}_q(n)$ as well.

PROOF: This is indeed a group action, since

$$\big(\mathcal{U}(A,\varphi)\big)(B,\varphi') = \big(\varphi(\mathcal{U}A)\big)(B,\varphi') = \varphi'\big(\varphi(\mathcal{U}A)B\big) = \varphi'\varphi\big((\mathcal{U}A)\varphi^{-1}(B)\big)$$

$$= \varphi\varphi'\big(\mathcal{U}(A\varphi^{-1}(B))\big) = \mathcal{U}\big(A\varphi^{-1}(B),\varphi\varphi'\big) = \mathcal{U}\big((A,\varphi)(B,\varphi')\big). \qquad \square$$

This action respects the distances d_S, d_I and therefore may be used to define equivalence for subspace codes. In Section 4.1 we will show that this equivalence is the most general one may demand if one also wants to preserve some other elementary properties of subspace codes.

We can now define linear and semilinear automorphisms of subspace codes.

Definition 4.3: The set

$$\mathrm{SAut}(\mathcal{C}) := \mathrm{Stab}_{\Gamma\mathrm{L}_n}(\mathcal{C}) := \big\{(A,\varphi) \in \Gamma\mathrm{L}_n \mid \mathcal{C}(A,\varphi) = \mathcal{C}\big\}$$

is called the *semi-linear automorphism group* of the subspace code $\mathcal{C}$. The *(linear) automorphism group* of $\mathcal{C}$ is defined as

$$\mathrm{Aut}(\mathcal{C}) := \mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{C}) := \{A \in \mathrm{GL}_n \mid \mathcal{C}A = \mathcal{C}\}.$$

Proposition 4.4: $\mathrm{SAut}(\mathcal{C})$ *is a subgroup of* $\Gamma\mathrm{L}_n$ *and* $\mathrm{Aut}(\mathcal{C})$ *is a subgroup of* $\mathrm{SAut}(\mathcal{C})$.
PROOF: It holds that $\mathrm{SAut}(\mathcal{C})$ is closed under multiplication, i.e. for $(A,\varphi),(B,\varphi') \in \mathrm{SAut}(\mathcal{C})$ it holds that

$$\mathcal{C}((A,\varphi)(B,\varphi')) = (\mathcal{C}(A,\varphi))(B,\varphi') = \mathcal{C}(B,\varphi') = \mathcal{C}.$$

Hence, $\mathrm{SAut}(\mathcal{C})$ is a subgroup of $\Gamma\mathrm{L}_n$. Since $\mathrm{Aut}(\mathcal{C})$ consists of the elements of $\mathrm{SAut}(\mathcal{C})$ with $\varphi = id$, the second statement follows. $\square$

Lemma 4.5: *For a given subspace code* $\mathcal{C} \subseteq \mathcal{P}_q(n)$ *it holds that*

$$\lambda I_n \in \mathrm{Aut}(\mathcal{C}) \text{ for all } \lambda \in \mathbb{F}_q^\times.$$

PROOF: One can easily see that $\lambda I_n \in \mathrm{Aut}(\mathcal{U})$ for all $\mathcal{U} \in \mathcal{P}_q(n)$ and $\lambda \in \mathbb{F}_q^\times$. Then the statement follows from the fact that the pointwise stabilizer group is always a subset of the setwise stabilizer group. $\square$

4.1 Isometry of Subspace Codes

An open question is how to define equivalence of subspace codes. Naturally, equivalent codes should have the same ambient space, cardinality, error-correction capability (i.e. minimum distance) and transmission rate (for a fixed ambient space this is given by the maximal dimension of the codewords). Moreover, the distance distribution and

the dimension distribution should be the same. Clearly, these last two conditions imply the minimum distance and maximum dimension.

This work engages in the equivalence maps of subspace codes that, in addition, preserve the dimensions of the codewords. In the following we characterize all such maps.

Definition 4.6: Let d be a metric function on $\mathcal{P}_q(n)$. A distance-preserving map $\iota : \mathcal{P}_q(n) \to \mathcal{P}_q(n)$, i.e. fulfilling

$$d(\mathcal{U}, \mathcal{V}) = d(\iota(\mathcal{U}), \iota(\mathcal{V})) \quad \forall\, \mathcal{U}, \mathcal{V} \in \mathcal{P}_q(n).$$

is called an *isometry* on $\mathcal{P}_q(n)$.

Lemma 4.7: *Any isometry ι is injective and hence, if the domain is equal to the co-domain, bijective. The inverse map ι^{-1} is an isometry as well.*
PROOF:

$$\mathcal{U} \neq \mathcal{V} \Longleftrightarrow d(\mathcal{U}, \mathcal{V}) \neq 0 \Longleftrightarrow d(\iota(\mathcal{U}), \iota(\mathcal{V})) \neq 0 \Longleftrightarrow \iota(\mathcal{U}) \neq \iota(\mathcal{V}) \qquad \square$$

From now on we consider the injection and subspace distance as metric functions on $\mathcal{P}_q(n)$ for the investigation of isometries.
Lemma 4.8: *If $\iota : \mathcal{P}_q(n) \to \mathcal{P}_q(n)$ is an isometry, then $\iota(\{0\}) \in \left\{\{0\}, \mathbb{F}_q^n\right\}$.*
PROOF: We will prove it using the injection distance. The proof for the subspace distance is analogous and can be found in [52].

Assume $\mathcal{U} := \iota(\{0\}) \notin \left\{\{0\}, \mathbb{F}_q^n\right\}$ and let $\mathcal{V} := \iota(\mathbb{F}_q^n)$. It holds that

$$\begin{aligned} & d_I\big(\{0\}, \mathbb{F}_q^n\big) = d_I\big(\iota(\{0\}), \iota(\mathbb{F}_q^n)\big) \\ \Longleftrightarrow \quad & n = d_I(\mathcal{U}, \mathcal{V}) \\ \Longleftrightarrow \quad & n = \max\{\dim(\mathcal{U}), \dim(\mathcal{V})\} - \dim(\mathcal{U} \cap \mathcal{V}). \end{aligned}$$

This implies that $\max\{\dim(\mathcal{U}), \dim(\mathcal{V})\} = \mathbb{F}_q^n$ and $\mathcal{U} \cap \mathcal{V} = \{0\}$. Therefore, either $\mathcal{U} = \mathbb{F}_q^n$ and $\mathcal{V} = \{0\}$ or $\mathcal{V} = \mathbb{F}_q^n$ and $\mathcal{U} = \{0\}$, which contradicts the assumption. $\square$

We can use this fact to show that any isometry on $\mathcal{P}_q(n)$ is either dimension-preserving or dimension-inverting, as shown in the following lemma.
Lemma 4.9: *Let ι be as before and $\mathcal{U} \in \mathcal{P}_q(n)$ arbitrary. Then*

$$\iota(\{0\}) = \{0\} \Longrightarrow \dim(\mathcal{U}) = d_I(\{0\},\mathcal{U}) = d_I(\{0\}, \iota(\mathcal{U})) = \dim(\iota(\mathcal{U}))$$

and on the other hand

$$\iota(\{0\}) = \mathbb{F}_q^n \Longrightarrow \dim(\mathcal{U}) = d_I(\{0\},\mathcal{U}) = d_I(\mathbb{F}_q^n, \iota(\mathcal{U})) = n - \dim(\iota(\mathcal{U})).$$

The same holds for the subspace distance.

In the following, we restrict ourselves to the isometries with $\iota(\{0\}) = \{0\}$ because these are exactly the isometries that keep the dimension of a codeword. Now we want to characterize all these isometries on $\mathcal{P}_q(n)$ with $\iota(\{0\}) = \{0\}$. For it we need the *Fundamental Theorem of Projective Geometry*:

Theorem 4.10 ([2, 4]): *Let $\mathcal{Z}_n := \{\mu I_n \mid \mu \in \mathbb{F}_q^\times\}$ be the set of scalar transformations. Then every order-preserving bijection (with respect to the subset relation) $f : \mathcal{P}_q(n) \to \mathcal{P}_q(n)$, where $n > 2$, is induced by a semilinear transformation (A, φ) from*

$$\mathrm{P\Gamma L}_n := (\mathrm{GL}_n/\mathcal{Z}_n) \rtimes \mathrm{Aut}(\mathbb{F}_q).$$

Theorem 4.11: *For $n > 2$, a map $\iota : \mathcal{P}_q(n) \to \mathcal{P}_q(n)$ is an order-preserving bijection (with respect to the subset relation) of $\mathcal{P}_q(n)$ if and only if it is an isometry with $\iota(\{0\}) = \{0\}$.*

PROOF: We will again prove the statement using the injection distance, where an analogous proof holds for the subspace distance and can be found in [52].

1. "$\Longleftarrow$"
   Let ι be an isometry with $\iota(\{0\}) = \{0\}$. We have to show that for any $\mathcal{U}, \mathcal{V} \in \mathcal{P}_q(n)$ it holds that
   $$\mathcal{U} \subseteq \mathcal{V} \Longleftrightarrow \iota(\mathcal{U}) \subseteq \iota(\mathcal{V}).$$
   From Lemma 4.9 one knows that $\dim(\mathcal{U}) = \dim(\iota(\mathcal{U}))$. Assume that there are $\mathcal{U}, \mathcal{V} \in \mathcal{P}_q(n)$ with $\mathcal{U} \subseteq \mathcal{V}$ and $\iota(\mathcal{U}) \nsubseteq \iota(\mathcal{V})$. This leads to the following contradiction:
   $$\begin{aligned} d_I\big(\iota(\mathcal{U}), \iota(\mathcal{V})\big) &= \max\{\dim(\iota(\mathcal{U})), \dim(\iota(\mathcal{V}))\} - \dim\big(\iota(\mathcal{U}) \cap \iota(\mathcal{V})\big) \\ &> \max\{\dim(\iota(\mathcal{U})), \dim(\iota(\mathcal{V}))\} - \dim(\iota(\mathcal{U})) \\ &= \max\{\dim(\mathcal{U}), \dim(\mathcal{V})\} - \dim(\mathcal{U}) \\ &= \max\{\dim(\mathcal{U}), \dim(\mathcal{V})\} - \dim(\mathcal{U} \cap \mathcal{V}) \\ &= d_I(\mathcal{U}, \mathcal{V}) \end{aligned}$$
   Hence, $\mathcal{U} \subseteq \mathcal{V} \Longrightarrow \iota(\mathcal{U}) \subseteq \iota(\mathcal{V})$. Since ι^{-1} is an isometry as well, the converse also holds. Thus, ι is an order-preserving bijection.
2. "$\Longrightarrow$"
   According to Theorem 4.10 any order-preserving bijection ι of the projective geometry can be expressed by a pair $(A, \varphi) \in \mathrm{P\Gamma L}_n$. Then
   $$\begin{aligned} d_I\big(\iota(\mathcal{U}), \iota(\mathcal{V})\big) &= d_I\big(\varphi(\mathcal{U}A), \varphi(\mathcal{V}A)\big) \\ &= \max\{\dim(\varphi(\mathcal{U}A)), \dim(\varphi(\mathcal{V}A))\} - \dim\big(\varphi(\mathcal{U}A) \cap \varphi(\mathcal{V}A)\big) \\ &= \max\{\dim(\mathcal{U}), \dim(\mathcal{V})\} - \dim\big(\varphi((\mathcal{U} \cap \mathcal{V})A)\big) \end{aligned}$$

$$= d_I(\mathcal{U}, \mathcal{V})$$

thus ι is an isometry with $\iota(\{0\}) = \{0\}$. □

Corollary 4.12: *Every isometry ι on $\mathcal{P}_q(n)$, where $n > 2$, with $\dim(\mathcal{U}) = \dim(\iota(\mathcal{U}))$ for any $\mathcal{U} \in \mathcal{P}_q(n)$, is induced by a semilinear transformation $(A, \varphi) \in \mathrm{P\Gamma L}_n$.*

From now on assume that $n > 2$. This is no real restriction, because subspace codes in an ambient space of dimension 2 are not interesting for application, since the only non-trivial subspaces are the one-dimensional ones. In that case neither the transmission rate is improved compared to forwarding, nor is error-correction possible.

Definition 4.13:
1. Two codes $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{P}_q(n)$ are *linearly isometric* if there exists $A \in \mathrm{PGL}_n := \mathrm{GL}_n/\mathcal{Z}_n$ such that $\mathcal{C}_1 = \mathcal{C}_2 A$. Since it is the orbit of PGL_n on the code, the set of all linearly isometric codes is denoted by $\mathcal{C}_1\mathrm{PGL}_n$.
2. We call $\mathcal{C}_1$ and $\mathcal{C}_2$ *semilinearly isometric* if there exists $(A, \varphi) \in \mathrm{P\Gamma L}n$ such that $\mathcal{C}_1 = \mathcal{C}_2(A, \varphi)$. The set of all semilinearly isometric codes is denoted by $\mathcal{C}_1\mathrm{P\Gamma L}n$.

Clearly linear and semilinear isometry are equivalence relations, so it makes sense to speak of classes of (semi-)linearly isometric codes. Note that the isometries are independent of the underlying metric (d_S or d_I). Note furthermore, that one can replace the projective groups with GL_n and $\Gamma\mathrm{L}_n$, respectively, when computing the isometry classes of subspace codes (this follows from Lemma 4.5).

The interested reader can find a lattice point-of-view of the isometries of subspace codes in [53].

4.2 Isometry and Automorphisms of Known Code Constructions

In this section we examine the isometries and automorphism groups of some known classes of constant dimension codes, namely spread codes, orbit codes and lifted rank-metric codes. All of these constructions were explained in Chapter 2.

4.2.1 Spread Codes

Different constructions for spread codes are known, some of them were explained in Sections 2.1, 2.5 and 3.1, where the latter was the Desarguesian spread construction (or $\mathbb{F}_q$-linear representations of $\mathbb{P}^{\ell-1}(\mathbb{F}_{q^k})$).

Theorem 4.14: *All Desarguesian spread codes are linearly isometric.*

PROOF: Since there is only one spread of lines in $\mathbb{F}_{q^k}^{\ell}$, different Desarguesian spreads of $\mathbb{F}_q^n$ can only arise from the different isomorphisms between $\mathbb{F}_{q^k}$ and $\mathbb{F}_q^k$. As the isomorphisms are linear maps, there exists a linear map between the different spreads arising from them. □

In general, not all spreads are linearly isometric but in the special case of $q = 2, k = 2, n = 4$ they actually are:

Proposition 4.15: *All spread codes in $\mathcal{G}_2(2,4)$ are linearly isometric.*

PROOF: To prove the statement we need the following definitions from [25]: A transversal of $\mathcal{U} \in \mathcal{G}_q(2,4)$ is an element $\mathcal{V} \in \mathcal{G}_q(2,4)$ such that $\dim(\mathcal{U} \cap \mathcal{V}) = 1$. The set of transversals of three elements of $\mathcal{G}_q(2,4)$ is called a regulus. A spread $\mathcal{S} \subset \mathcal{G}_q(2,4)$ is called regular if, when $\mathcal{U}_1, \mathcal{U}_2, \mathcal{U}_3 \in \mathcal{S}$, then the regulus of $\mathcal{U}_1, \mathcal{U}_2, \mathcal{U}_3$ is contained in $\mathcal{S}$.

From [25, Lemma 17.1.3] we know that every spread in $\mathcal{G}_q(2,4)$ is regular. Since in $\mathcal{G}_2(k,2k)$ a spread is Desarguesian if and only if it is regular [27, p. 207], we know that every spread is Desarguesian. Hence all spreads in $\mathcal{G}_2(2,4)$ are linearly isometric. □

We will now investigate the automorphism groups of Desarguesian spreads.

Theorem 4.16: *The linear automorphism group of a Desarguesian spread code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ is isomorphic to* $\mathrm{GL}_{\frac{n}{k}}(q^k) \times \mathrm{Gal}(\mathbb{F}_{q^k}, \mathbb{F}_q)$.

PROOF: Let $\ell := \frac{n}{k}$. We want to find all $\mathbb{F}_q$-linear bijections of $\mathbb{P}^{\ell-1}(\mathbb{F}_{q^k})$. We know that $\mathrm{PGL}_\ell(q^k)$ is the group of all $\mathbb{F}_{q^k}$-linear bijections of $\mathbb{P}^{\ell-1}(\mathbb{F}_{q^k})$. Thus, $\mathrm{PGL}_\ell(q^k) \times \mathrm{Gal}(\mathbb{F}_{q^k}, \mathbb{F}_q)$ is the set of all $\mathbb{F}_q$-linear bijections of $\mathbb{P}^{\ell-1}(\mathbb{F}_{q^k})$. It follows that non-projectively the linear automorphism group of such a spread is isomorphic to $\mathrm{GL}_\ell(q^k) \times \mathrm{Gal}(\mathbb{F}_{q^k}, \mathbb{F}_q)$. □

Corollary 4.17: *Let $\mathcal{S}$ be a Desarguesian spread code in $\mathcal{G}_q(k,n)$. Then*

$$|\mathrm{Aut}(\mathcal{S})| = k \prod_{i=0}^{\frac{n}{k}-1} \left(q^n - q^{ki}\right).$$

PROOF: The statement follows from the fact that $|\mathrm{Gal}(\mathbb{F}_{q^k}, \mathbb{F}_q)| = k$ and $|\mathrm{GL}_{\frac{n}{k}}(q^k)| = \prod_{i=0}^{\frac{n}{k}-1} \left((q^k)^{\frac{n}{k}} - (q^k)^i\right)$. □

Remark 4.18: It was shown in [27, Theorem 25.6.7] that all regular spreads in $\mathcal{G}_q(k,2k)$ are isometric and that the automorphism group of such a regular spread has cardinality $kq^k(q^k-1)(q^{2k}-1)$. This formula coincides with the one from our Corollary 4.17 for $n = 2k$. Since we know that in $\mathcal{G}_2(k,2k)$ a spread is Desarguesian if and only if it is regular [27, p. 207], for $q = 2$ our corollary proves the same statement as [27, Theorem 25.6.7].

Since we would like to represent the finite field automorphisms as invertible matrices we need the following lemma:

Lemma 4.19: *Let $\phi^{(k)} : \mathbb{F}_q^k \to \mathbb{F}_{q^k}$ be the canonical vector space isomorphism and $\varphi \in \mathrm{Gal}(\mathbb{F}_{q^k}, \mathbb{F}_q)$. Then there exists a matrix $A \in \mathrm{GL}_k$ such that*

$$\phi^{(k)}(vA) = \varphi(v).$$

I.e. there is a matrix-representation in GL_k for every element of $\mathrm{Gal}(\mathbb{F}_{q^k}, \mathbb{F}_q)$.

PROOF: The statement follows from the fact that φ is linear and that $\mathbb{F}_q^k$ is isomorphic to $\mathbb{F}_{q^k}$. □

We can now translate the result of Theorem 4.16 to a matrix setting. Since $\mathbb{F}_{q^k}$ is isomorphic to $\mathbb{F}_q[\alpha]$ where α is a root of a monic irreducible polynomial $p(x) \in \mathbb{F}_q[x]$ of degree k but also to $\mathbb{F}_q[M_p]$, where M_p is the companion matrix of $p(x)$, we get:

Corollary 4.20: *The automorphism group of a Desarguesian spread code in $\mathcal{G}_q(k,n)$ is generated by all elements in GL_n where the $k \times k$-blocks are elements of $\mathbb{F}_q[M_p]$ and block diagonal matrices where the blocks represent an element of $\mathrm{Gal}(\mathbb{F}_{q^k}, \mathbb{F}_q)$.*

In Section 3.1 it was shown that the generator matrices of the code words of Desarguesian spreads are of the type

$$U = \begin{bmatrix} B_1 & B_2 & \dots & B_\ell \end{bmatrix}$$

where the blocks B_i are elements of $\mathbb{F}_q[M_p]$ and M_p is the companion matrix of an irreducible polynomial $p(x) \in \mathbb{F}_q[x]$ of degree k. To stay inside this structure (i.e. to apply an automorphism) we can permute the blocks, do block-wise multiplications or do block-wise additions with elements from $\mathbb{F}_q[M_p]$. This coincides with the structure of the automorphism groups from before.

This result is depicted in the following Examples.

Example 4.21: Consider $\mathcal{G}_2(2,4)$. The only binary irreducible polynomial of degree 2 is $p(x) = x^2 + x + 1$, i.e. the corresponding companion matrix is

$$M_p = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

The respective spread code is

$$\mathcal{C} = \left\{ \mathrm{rs}\begin{bmatrix} I & 0 \end{bmatrix}, \mathrm{rs}\begin{bmatrix} I & I \end{bmatrix}, \mathrm{rs}\begin{bmatrix} I & M_p \end{bmatrix}, \mathrm{rs}\begin{bmatrix} I & M_p^2 \end{bmatrix}, \mathrm{rs}\begin{bmatrix} 0 & I \end{bmatrix} \right\},$$

(where $0 = 0_{2\times 2}$ and $I = I_{2\times 2}$) and its automorphism group has 360 elements:

$$\mathrm{Aut}(\mathcal{C}) = \left\langle \begin{pmatrix} & I \\ I & \end{pmatrix}, \begin{pmatrix} I & \\ & M_p \end{pmatrix}, \begin{pmatrix} I & M_p \\ & I \end{pmatrix}, \begin{pmatrix} Q & \\ & Q \end{pmatrix} \right\rangle,$$

where $Q = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2$ represents the only non-trivial automorphism of $\mathbb{F}_{2^2}$, i.e. $x \mapsto x^2$.

A different approach of finding the automorphism group of a spread in $\mathcal{G}_2(2,4)$ can also be found in [25, Corollary 2].

Example 4.22: Consider $\mathcal{G}_3(2,4)$ and the irreducible polynomial $p(x) = x^2 + x + 2$, i.e. the corresponding companion matrix is

$$M_p = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}.$$

We use again the notation $0 = 0_{2\times 2}$ and $I = I_{2\times 2}$. The spread code is defined as

$$\mathcal{C} = \mathrm{rs}\begin{bmatrix} I & 0 \end{bmatrix} \cup \left\{ \mathrm{rs}\begin{bmatrix} I & M_p^i \end{bmatrix} \mid i = 0, \ldots, 7 \right\} \cup \mathrm{rs}\begin{bmatrix} 0 & I \end{bmatrix}$$

and its automorphism group is given by

$$\mathrm{Aut}(\mathcal{C}) = \left\langle \begin{pmatrix} & I \\ I & \end{pmatrix}, \begin{pmatrix} I & \\ & M_p \end{pmatrix}, \begin{pmatrix} I & M_p \\ & I \end{pmatrix}, \begin{pmatrix} Q & \\ & Q \end{pmatrix} \right\rangle,$$

where $Q = \begin{pmatrix} 1 & 0 \\ 2 & 2 \end{pmatrix} \in \mathrm{GL}_2$. Here Q represents the only non-trivial automorphism of $\mathbb{F}_{3^2}$ that fixes $\mathbb{F}_3$, i.e. $x \mapsto x^3$. It holds that $\mathrm{Aut}(\mathcal{C})$ has 11520 elements.

Note that in both examples the first element of the generator sets corresponds to swapping the blocks, the second corresponds to multiplication by M_p and the third element to adding M_p in the second block of the code word generator matrices.

To conclude this subsection we want to give an example of a non-Desarguesian spread and show that its automorphism group has a different cardinality than the ones of a Desarguesian spread of the same parameters.

Example 4.23: In the setting of Example 4.22, one can construct a non-Desarguesian spread as follows:

$$\mathcal{C}' = \left\{ \mathrm{rs}[\ I \quad M_p^i\ ] \mid i \in \{0, 2, 3, 4, 6, 7\} \right\} \cup$$

$$\mathrm{rs}\begin{bmatrix}1&0&0&0\\0&0&0&1\end{bmatrix} \cup \mathrm{rs}\begin{bmatrix}0&1&0&0\\0&0&1&2\end{bmatrix} \cup \mathrm{rs}\begin{bmatrix}1&1&0&0\\0&0&1&0\end{bmatrix} \cup \mathrm{rs}\begin{bmatrix}1&2&0&0\\0&0&1&1\end{bmatrix}.$$

We used the algorithm of [18] to compute its automorphism group, and got a group of size

$$|\mathrm{Aut}(\mathcal{C}')| = 3840$$

which is a third of the size of the automorphism group of the Desarguesian spread in Example 4.22. This implies that $\mathcal{C}$ and $\mathcal{C}'$ are not linearly isometric.

4.2.2 Orbit Codes

In this subsection we will investigate the isometries and automorphism groups of subspace orbit codes. For a more general description of isometries of general codes defined as orbits under some action on a metric set, the interested reader is referred to [53].

Theorem 4.24: *Let $\mathcal{C}_1 = \mathcal{U}_1 G \subseteq \mathcal{G}_q(k,n)$ be a subspace orbit code. Then $\mathcal{C}_2$ is linearly (respectively semilinearly) isometric to $\mathcal{C}_1$ if and only if there exists $S \in \mathrm{GL}_n$ (respectively $S \in \mathrm{PGL}_n$) such that*

$$\mathcal{C}_2 = \mathcal{U}_1 S(S^{-1}GS),$$

i.e. $S^{-1}GS$ is a generating group of $\mathcal{C}_2$. Hence, the isometry classes of orbit codes in $\mathcal{G}_q(k,n)$ correspond to the conjugacy classes of the subgroups of GL_n.

One natural question that arises when studying orbit codes is if there is a canonical representative of all the possible generating groups for a given orbit code. The following proposition shows that the automorphism groups can function as such representatives, since they are always the largest generating group of a given code.

Proposition 4.25:
1. *Every generating group of an orbit code is a subgroup of the automorphism group.*
2. *Every subgroup of the automorphism group containing a generating group is a generating group. Hence, the automorphism group is a generating group of the orbit code.*

PROOF:
1. If $\mathcal{C} = \mathcal{U}G$, then $\mathcal{C}G = \mathcal{U}GG = \mathcal{U}G$.
2. Let G be a generating group of $\mathcal{C}$ and H a supergroup of G, such that H is a subgroup of $\mathrm{Aut}(\mathcal{C})$. Hence, $\mathcal{C} = \mathcal{U}G$ and $\mathcal{C}H = \mathcal{C}$. This implies that $\mathcal{U}H = \mathcal{U}GH = \mathcal{C}H = \mathcal{C}$, since G is a subgroup of H. □

The question of finding elements of the automorphism group can be translated into a stabilizer condition of the initial point of the orbit.

Theorem 4.26: *$A \in \mathrm{GL}_n$ is in the automorphism group of $\mathcal{C} = \mathcal{U}G$ if and only if for every $B' \in G$ there exists a $B'' \in G$ such that*

$$B'AB'' \in \mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{U}).$$

PROOF: It holds that

$$\begin{aligned} A \in \mathrm{Aut}(\mathcal{C}) &\iff \mathcal{C}A = \mathcal{C} \\ &\iff \forall B' \in G\, \exists B^* \in G : \mathcal{U}B'A = \mathcal{U}B^* \\ &\iff \forall B' \in G\, \exists B^* \in G : \mathcal{U}B'AB^{*-1} = \mathcal{U}. \end{aligned}$$

The statement follows with $B'' := B^{*-1} \in G$. □

4.2.3 Lifted Rank-Metric Codes

In this subsection we study the isometries and automorphisms of lifted rank-metric codes. To do so we first repeat some known results about the isometries of classical rank-metric codes. Then we use these results to investigate the isometries of lifted rank-metric codes. Moreover, we show the connection between the automorphism groups of rank-metric and lifted rank-metric codes.

Rank-metric codes are matrix codes, i.e. subsets of $\mathbb{F}_q^{k\times m}$ (in this work we restrict ourselves to the case $k \leqslant m$) equipped with the rank distance

$$d_R(U,V) := \mathrm{rank}(U - V) \quad \text{for } U, V \in \mathbb{F}_q^{k\times m}.$$

Such a matrix code can also be seen as a block code in $\mathbb{F}_{q^m}^k$, where the code words are column vectors of length k. As before we denote rank-metric codes by C and lifted rank-metric codes by $\mathcal{C}$.

The isometry of rank-metric codes (as block codes over $\mathbb{F}_{q^m}^k$) has already been studied by Berger in [5]. One of his main results is the following:

Lemma 4.27 ([5]): *1. The set of $\mathbb{F}_{q^m}$-linear isometries on $\mathbb{F}_{q^m}^k$ equipped with the rank metric is*

$$\mathcal{R}^{\mathrm{lin}}(\mathbb{F}_{q^m}^k) := \mathrm{GL}_k(q) \times \mathbb{F}_{q^m}^{\times}.$$

2. The set of $\mathbb{F}_{q^m}$-semilinear isometries on $\mathbb{F}_{q^m}^k$ equipped with the rank metric is

$$\mathcal{R}^{\mathrm{semi}}(\mathbb{F}_{q^m}^k) := \left(\mathrm{GL}_k(q) \times \mathbb{F}_{q^m}^{\times}\right) \rtimes \mathrm{Aut}(\mathbb{F}_{q^m}).$$

Since we are interested in the matrix representation of these codes and hence also their isometries, let us now translate the previous result to a matrix setting:

Corollary 4.28: *Let $p(x) = \sum_{i=0}^{m} p_i x^i \in \mathbb{F}_q[x]$ be monic and irreducible of degree m and $M_p \in \mathrm{GL}_m(q)$ its companion matrix. Let $\alpha \in \mathbb{F}_{q^m}$ be a root of $p(x)$. Thus, $\mathbb{F}_{q^m} \cong \mathbb{F}_q[\alpha]$. Denote by $\mathrm{Gal}_M(\mathbb{F}_{q^m}) \leqslant \mathrm{GL}_m(q)$ the matrix representation of $\mathrm{Gal}(\mathbb{F}_{q^m}, \mathbb{F}_q)$ (as illustrated in Lemma 4.19 and Examples 4.21 and 4.22). Then the following holds:*

1. *The set of $\mathbb{F}_{q^m}$-linear isometries on $\mathbb{F}_q^{k\times m}$ equipped with the rank metric is $\mathrm{GL}_k(q) \times \mathbb{F}_q^{\times}[M_p]$.*
2. *The set of $\mathbb{F}_{q^m}$-semilinear isometries on $\mathbb{F}_q^{k\times m}$ equipped with the rank metric is $\big(\mathrm{GL}_k(q) \times \mathbb{F}_q^{\times}[M_p]\big) \rtimes \big(\mathrm{Gal}_M(\mathbb{F}_{q^m}) \times \mathrm{Aut}(\mathbb{F}_q)\big)$.*

Here GL_k always acts from the left and $\mathbb{F}_q^{\times}[M_p]$ as well as $\mathrm{Gal}_M(\mathbb{F}_{q^m})$ always act from the right when applied to an element of $\mathbb{F}_q^{k\times m}$.

PROOF: From Theorem 1.29 we know that for any $v \in \mathbb{F}_q^m$ it holds that

$$\phi^{(m)}(vM_p) = \phi^{(m)}(v)\alpha.$$

Since $\mathbb{F}_q[\alpha]$ is isomorphic to $\mathbb{F}_q[M_p]$, we get that multiplying an element of $\mathbb{F}_{q^m}^k$ by $\sum_{i=0}^{m-1} \beta_i \alpha^i \in \mathbb{F}_q[\alpha]$ is isomorphic to multiplying the respective element of $\mathbb{F}_q^{k\times m}$ with $\sum_{i=0}^{m-1} \beta_i M_p^i \in \mathbb{F}_q[M_p]$. Then, together with Lemma 4.27, the first statement follows. The second statement is implied by the fact that $\mathrm{Aut}(\mathbb{F}_{q^m}) = \mathrm{Gal}(\mathbb{F}_{q^m}, \mathbb{F}_q) \times \mathrm{Aut}(\mathbb{F}_q)$.□

Note that an $\mathbb{F}_{q^m}$-linear map is also $\mathbb{F}_q$-linear. On the other hand, there are other $\mathbb{F}_q$-(semi-)linear isometries than the ones mentioned before. E.g. all elements of GL_m are $\mathbb{F}_q$-linear isometries on $\mathbb{F}_q^{k\times m}$, since they are rank-preserving.

We will now show the connection between the isometries of rank-metric codes and their lifted subspace codes.

Theorem 4.29: *If two rank-metric codes in $\mathbb{F}_q^{k\times(n-k)}$ are $\mathbb{F}_{q^{n-k}}$-linearly (respectively $\mathbb{F}_{q^{n-k}}$-semilinearly) isometric in the rank-metric space, their lifted codes are linearly (respectively semilinearly) isometric in the Grassmannian $\mathcal{G}_q(k, n)$.*

PROOF: For simplicity we will first prove the statement for linearly isometric codes: Let $\mathcal{C}_R$ and $\mathcal{C}'_R$ be two $\mathbb{F}_{q^{n-k}}$-linearly isometric rank-metric codes, i.e. $\mathcal{C}'_R = A\mathcal{C}_R M'_p$ with $A \in \mathrm{GL}_k$ and $M'_p \in \mathbb{F}_q[M_p]$, where M_p is the companion matrix of a monic irreducible polynomial in $\mathbb{F}_q[x]$ of degree $n-k$. Then the lifted code of $\mathcal{C}'_R$ is

$$\begin{aligned}
\mathcal{C}' &= \left\{\mathrm{rs}\begin{bmatrix} I_{k\times k} & R' \end{bmatrix} \mid R' \in \mathcal{C}'_R\right\} \\
&= \left\{\mathrm{rs}\begin{bmatrix} I_{k\times k} & ARM'_p \end{bmatrix} \mid R \in \mathcal{C}_R\right\} \\
&= \left\{\mathrm{rs}\begin{bmatrix} A^{-1} & R \end{bmatrix} \mid R \in \mathcal{C}_R\right\} \begin{pmatrix} I_{k\times k} & \\ & M'_p \end{pmatrix} \\
&= \left\{\mathrm{rs}\begin{bmatrix} I_{k\times k} & R \end{bmatrix} \mid R \in \mathcal{C}_R\right\} \begin{pmatrix} A^{-1} & \\ & M'_p \end{pmatrix}
\end{aligned}$$

$$= \mathcal{C} \begin{pmatrix} A^{-1} & \\ & M'_p \end{pmatrix}$$

where $\mathcal{C}$ is the lifted code of $\mathcal{C}_R$. Hence, the lifted codes are linearly isometric.

The semi-linear case then follows together with Corollary 4.28, since an element from $\mathrm{Gal}_M(\mathbb{F}_{q^{n-k}})$ behaves analogously to M'_p in the proof. □

One can easily see, that there are codes that are linearly isometric to a lifted rank-metric code but are not a lifted rank-metric code itself:

Example 4.30: Consider the binary lifted rank-metric code

$$\mathcal{C} = \left\{ \mathrm{rs} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \mathrm{rs} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \right\}.$$

Permute the second and third column of both codewords to get

$$\mathcal{C}' = \left\{ \mathrm{rs} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \mathrm{rs} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \right\}.$$

Then $\mathcal{C}$ and $\mathcal{C}'$ are linearly isometric but $\mathcal{C}'$ is not a lifted rank-metric code.

We now want to investigate which isometries map a lifted rank-metric code to another lifted rank-metric code of the same parameters. Note that it does not make sense to think of $\mathbb{F}_{q^{n-k}}$-linear isometry for the lifted codes, which is why we only study the $\mathbb{F}_q$-linear isometries.

Theorem 4.31: *Let $C \subseteq \mathbb{F}_q^{k\times(n-k)}$ be an arbitrary rank-metric code with minimum distance δ. The following elements map C to another lifted rank-metric code in $\mathbb{F}_q^{k\times(n-k)}$ with the same minimum distance δ and are semilinear isometries:*

$$\left\{ \left(\begin{pmatrix} A & B \\ & C \end{pmatrix}, \varphi \right) \mid A \in \mathrm{GL}_k, C \in \mathrm{GL}_{n-k}, B \in \mathbb{F}_q^{k\times(n-k)}, \varphi \in \mathrm{Aut}(\mathbb{F}_q) \right\}$$

For $\varphi = id$ they are linear isometries.

PROOF: Consider $R, R' \in C$. With the block matrix multiplication rules it follows that

$$\mathrm{rs}\begin{bmatrix} I_{k\times k} & R \end{bmatrix} \begin{pmatrix} A & B \\ & C \end{pmatrix} = \mathrm{rs}\begin{bmatrix} A & B + RC \end{bmatrix} = \mathrm{rs}\begin{bmatrix} I_{k\times k} & A^{-1}(B + RC) \end{bmatrix}.$$

From Corollary 4.28 we know that A^{-1} is a rank-metric isometry. Moreover,

$$\mathrm{rank}\big((B + RC) - (B + R'C)\big) = \mathrm{rank}\big((R - R')C\big) = \mathrm{rank}(R - R')$$

thus $\{A^{-1}(B + RC) \mid R \in C\} \subseteq \mathbb{F}_q^{k\times(n-k)}$ is a rank-metric code with the same minimum distance as C. As A and C are invertible, the whole matrix $\begin{pmatrix} A & B \\ & C \end{pmatrix}$ is in GL_n and the statement follows. □

Remark 4.32: With the notation from Theorem 4.31 the map

$$\begin{aligned} \mathbb{F}_q^{k\times m} &\longrightarrow \mathbb{F}_q^{k\times m} \\ R &\longmapsto A^{-1}(B+RC) \end{aligned}$$

is indeed an isometry but it is not linear, except for the case when $A^{-1}B = 0_{k\times(n-k)}$, which is equivalent to $B = 0_{k\times(n-k)}$, since $A \in \mathrm{GL}_k$. Thus, the elements that map a lifted *linear* rank-metric code to another lifted linear rank-metric code of the same parameters have to fulfill $B = 0_{k\times(n-k)}$, in addition.

In the following we will focus on automorphisms of lifted rank-metric codes. We can again use the knowledge of the automorphism group of a rank-metric code for finding the automorphism group of the respective lifted rank-metric code. For this denote by Aut_R the automorphism group of the rank-metric code.

Proposition 4.33: *Let $\mathcal{C}_R \subseteq \mathbb{F}_q^{k\times(n-k)}$ be a rank-metric code and $\mathcal{C}$ its lifted code. Then*

$$\left\{ \begin{pmatrix} I_{k\times k} & \\ & R \end{pmatrix} \mid R \in \mathrm{Aut}_R(\mathcal{C}_R) \right\} \subseteq \mathrm{Aut}(\mathcal{C}).$$

PROOF: It holds that

$$\left\{ \begin{bmatrix} I_{k\times k} & B \end{bmatrix} \mid B \in \mathcal{C}_R \right\} \begin{pmatrix} I_{k\times k} & \\ & R \end{pmatrix} = \left\{ \begin{bmatrix} I_{k\times k} & BR \end{bmatrix} \mid B \in \mathcal{C}_R \right\}.$$

Since $R \in \mathrm{Aut}_R(\mathcal{C}_R)$, this set is equal to the original one. □

Theorem 4.34: *Let $\mathcal{C}_R \subseteq \mathbb{F}_q^{k\times(n-k)}$ be a rank-metric code and $\mathcal{C}$ its lifted code. Then*

$$\left\{ \begin{pmatrix} I_{k\times k} & \\ & A \end{pmatrix} \mid A \in \mathrm{GL}_{n-k} \right\} \cap \mathrm{Aut}(\mathcal{C}) = \left\{ \begin{pmatrix} I_{k\times k} & \\ & R \end{pmatrix} \mid R \in \mathrm{Aut}_R(\mathcal{C}_R) \right\}.$$

PROOF: From Proposition 4.33 we know that the right side is included in the left. Furthermore,

$$\begin{aligned} &\mathrm{rs}\begin{bmatrix} I_{k\times k} & B_1 \end{bmatrix} \begin{pmatrix} I_{k\times k} & \\ & A \end{pmatrix} = \mathrm{rs}\begin{bmatrix} I_{k\times k} & B_2 \end{bmatrix} \\ \iff &\exists C_1, C_2 \in \mathrm{GL}_k : \begin{bmatrix} C_1 & C_1B_1 \end{bmatrix} \begin{pmatrix} I_{k\times k} & \\ & A \end{pmatrix} = \begin{bmatrix} C_2 & C_2B_2 \end{bmatrix} \\ \iff &C_1 = C_2 \quad \text{and} \quad B_1A = B_2 \end{aligned}$$

i.e. if $\begin{pmatrix} I_{k\times k} & \\ & A \end{pmatrix} \in \mathrm{Aut}(\mathcal{C})$, then $A \in \mathrm{Aut}_R(\mathcal{C}_R)$. □

Hence, if we know the automorphism group of a lifted rank-metric code, we also know the automorphism group of the rank-metric code itself.

Example 4.35: Consider the (non-linear) rank-metric code

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

with four elements and minimum rank distance 1 over $\mathbb{F}_2$. Its automorphism group is

$$\mathrm{Aut}_R(C) = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{F}_2 \right\}.$$

Let $\mathcal{C}$ be the lifted code of C in $\mathcal{G}_2(2,4)$. Then

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

with $|\mathrm{Aut}(\mathcal{C})| = 192$. The second generator and the identity matrix are the corresponding elements described in Theorem 4.34.

Note that $\mathrm{Aut}_R(C)$ can easily be found since $|\mathrm{GL}_2| = 6$, while $\mathrm{Aut}(\mathcal{C})$ was found by computer search, using the algorithm of [18].

Bibliography

[1] R. Ahlswede, N. Cai, S.-Y.R. Li, and R.W. Yeung, *Network information flow*, IEEE Transactions on Information Theory **46** (2000), 1204–1216.

[2] E. Artin, *Geometric algebra*, Interscience tracts in pure and applied mathematics, John Wiley & Sons, 1988.

[3] L. Bader and G. Lunardon, *Desarguesian spreads*, Ricerche di Matematica **60** (2011), no. 1, 15–37.

[4] R. Baer, *Linear algebra and projective geometry*, Pure and applied mathematics, Academic Press, 1952.

[5] T. P. Berger, *Isometries for rank distance and permutation group of Gabidulin codes*, IEEE Transactions on Information Theory **49** (2003), no. 11, 3016 – 3019.

[6] A. Beutelspacher, *Partial spreads in finite projective spaces and partial designs*, Mathematische Zeitschrift **145** (1975), no. 3, 211–229.

[7] ———, *Blocking sets and partial spreads in finite projective spaces*, Geometriae Dedicata **9** (1980), no. 4, 425–449.

[8] A. Björner, M. Las Vergnas, B. Sturmfels, N. White, and G. M. Ziegler, *Oriented matroids*, second ed., Encyclopedia of Mathematics and its Applications, vol. 46, Cambridge University Press, Cambridge, 1999.

[9] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Journal of Research (1973), no. 10, vi+97.

[10] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, *Network coding for distributed storage systems*, IEEE Transactions on Information Theory **56** (2010), no. 9, 4539 –4551.

[11] J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996.

[12] A. Elsenhans, A. Kohnert, and A. Wassermann, *Construction of codes for network coding*, Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems – MTNS (Budapest, Hungary), 2010, pp. 1811–1814.

[13] T. Etzion and N. Silberstein, *Construction of error-correcting codes for random network coding*, IEEE 25th Convention of Electrical and Electronics Engineers in Israel, 2008, pp. 070–074.

[14] ———, *Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams*, IEEE Transactions on Information Theory **55** (2009), no. 7, 2909–

2919.

[15] ———, *Codes and designs related to lifted MRD codes*, IEEE Transactions on Information Theory **59** (2013), no. 2, 1004 –1017.

[16] T. Etzion and A. Vardy, *Error-correcting codes in projective space*, Proceedings of the 2008 IEEE International Symposium on Information Theory (Toronto, Canada), 2008, pp. 871–875.

[17] ———, *Error-correcting codes in projective space*, IEEE Transactions on Information Theory **57** (2011), no. 2, 1165–1173.

[18] T. Feulner, *Canonical forms and automorphisms in the projective space*, preprint (2012).

[19] E. M. Gabidulin, *Theory of codes with maximum rank distance*, Problemy Peredachi Informatsii **21** (1985), no. 1, 3–16.

[20] E. M. Gabidulin and N. I. Pilipchuk, *Multicomponent network coding*, Proceedings of the Seventh International Workshop on Coding and Cryptography (WCC) 2011 (Paris, France), 2011, pp. 443–452.

[21] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, second ed., Cambridge University Press, Cambridge, 2003.

[22] E. Gorla, F. Manganiello, and J. Rosenthal, *An algebraic approach for decoding spread codes*, Advances in Mathematics of Communications (AMC) **6** (2012), no. 4, 443 – 466.

[23] E. Gorla and A. Ravagnani, *Partial spreads in random network coding*, preprint (2013).

[24] I. N. Herstein, *Topics in algebra*, second ed., Xerox College Publishing, Lexington, Mass., 1975.

[25] J. W. P. Hirschfeld, *Finite projective spaces of three dimensions*, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1985, Oxford Science Publications.

[26] ———, *Projective geometries over finite fields*, second ed., Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1998.

[27] J. W. P. Hirschfeld and J. A. Thas, *General Galois geometries*, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1991, Oxford Science Publications.

[28] T. Ho, R. Kötter, M. Medard, D. R. Karger, and M. Effros, *The benefits of coding over routing in a randomized setting*, Proceedings of the 2003 IEEE International Symposium on Information Theory (Kanagawa, Japan), 2003.

[29] W. V. D. Hodge and D. Pedoe, *Methods of algebraic geometry, vol. ii*, vol. 2, Cambridge University Press, 1952.

[30] A. Juels and M. Sudan, *A fuzzy vault scheme*, Designs, Codes and Cryptography **38** (2006), no. 2, 237–257.

[31] D. Jungnickel, *Finite fields, structure and arithmetic*, BI-Wiss.-Verl., 1993.

[32] A. Kerber, *Applied finite group actions*, second ed., Algorithms and Combinatorics,

vol. 19, Springer-Verlag, Berlin, 1999.

[33] A. Kohnert and S. Kurz, *Construction of large constant dimension codes with a prescribed minimum distance*, MMICS (J. Calmet, W. Geiselmann, and J. Müller-Quade, eds.), Lecture Notes in Computer Science, vol. 5393, Springer, 2008, pp. 31–42.

[34] R. Kötter and F. R. Kschischang, *Coding for errors and erasures in random network coding*, IEEE Transactions on Information Theory **54** (2008), no. 8, 3579–3591.

[35] L. Lambert, *Random network coding and designs over Fq*, Master thesis, Ghent University, Ghent, 2013.

[36] S. Lang, *Introduction to linear algebra*, second ed., Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1986.

[37] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, Cambridge, London, 1994, Revised edition.

[38] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North Holland, Amsterdam, 1977.

[39] F. Manganiello, E. Gorla, and J. Rosenthal, *Spread codes and spread decoding in network coding*, Proceedings of the 2008 IEEE International Symposium on Information Theory (Toronto, Canada), 2008, pp. 851–855.

[40] F. Manganiello and A.-L. Trautmann, *Spread decoding in extension fields*, arXiv:1108.5881v1 [cs.IT] (2011).

[41] F. Manganiello, A.-L. Trautmann, and J. Rosenthal, *On conjugacy classes of subgroups of the general linear group and cyclic orbit codes*, Proceedings of the 2011 IEEE International Symposium on Information Theory (St. Petersburg, Russia), 2011, pp. 1916–1920.

[42] K. Marshall, J. Rosenthal, D. Schipani, and A.-L. Trautmann, *Subspace fuzzy vault*, arXiv:1210.7190 [cs.IT] (2012).

[43] J. Rosenthal and A.-L. Trautmann, *A complete characterization of irreducible cyclic orbit codes and their Plücker embedding*, Designs, Codes and Cryptography **66** (2013), 275–289.

[44] ———, *Decoding of subspace codes, a problem of Schubert calculus over finite fields*, Mathematical System Theory – Festschrift in Honor of Uwe Helmke on the Occasion of his Sixtieth Birthday (K. Hüper and J. Trumpf, eds.), CreateSpace, 2013, pp. 353–366.

[45] N. Silberstein, A. S. Rawat, and S. Vishwanath, *Adversarial error resilience in distributed storage using MRD codes and MDS array codes*, arXiv:1202.0800v1 [cs.IT] (2012).

[46] N. Silberstein and A.-L. Trautmann, *New lower bounds for constant dimension codes*, arXiv:1301.5961 [cs.IT] (2013).

[47] D. Silva and F. R. Kschischang, *On metrics for error correction in network coding*, IEEE Transactions on Information Theory **55** (2009), no. 12, 5479–5490.

[48] D. Silva, F. R. Kschischang, and R. Kötter, *A rank-metric approach to error control*

in random network coding, IEEE Transactions on Information Theory **54** (2008), no. 9, 3951 –3967.

[49] B. Sturmfels, *Algorithms in invariant theory*, Texts and Monographs in Symbolic Computation, Springer-Verlag, Vienna, 1993.

[50] B. Sturmfels and N. White, *Gröbner bases and invariant theory*, Advances in Mathematics **76** (1989), no. 2, 245–259.

[51] A.-L. Trautmann, *Plücker embedding of cyclic orbit codes*, Proceedings of the 20th International Symposium on Mathematical Theory of Networks and Systems – MTNS (Melbourne, Australia), 2012, pp. 1–15.

[52] A.-L. Trautmann, *Isometry and automorphisms of constant dimension codes*, Advances in Mathematics of Communications (AMC) **7** (2013), no. 2, 147–160.

[53] A.-L. Trautmann, F. Manganiello, M. Braun, and J. Rosenthal, *Cyclic orbit codes*, IEEE Transactions on Information Theory **PP** (2013), no. 99, 1–18.

[54] A.-L. Trautmann, F. Manganiello, and J. Rosenthal, *Orbit codes - a new concept in the area of network coding*, IEEE Information Theory Workshop (ITW) (Dublin, Ireland), 2010, pp. 1–4.

[55] A.-L. Trautmann and J. Rosenthal, *New improvements on the echelon-Ferrers construction*, Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems – MTNS (Budapest, Hungary), 2010, pp. 405–408.

[56] ———, *A complete characterization of irreducible cyclic orbit codes*, Proceedings of the Seventh International Workshop on Coding and Cryptography (WCC) 2011 (Paris, France), 2011, pp. 219–228.

[57] A.-L. Trautmann, N. Silberstein, and J. Rosenthal, *List decoding of lifted Gabidulin codes via the Plücker embedding*, Preproceedings of the International Workshop on Coding and Cryptography (WCC) 2013 (Bergen, Norway), 2013, pp. 539–549.

[58] J. H. van Lint and R. M. Wilson, *A course in combinatorics*, second ed., Cambridge University Press, 2001.

[59] V. A. Vassiliev, *Introduction to topology*, Student Mathematical Library, vol. 14, American Mathematical Society, Providence, RI, 2001, Translated from the 1997 Russian original by A. Sossinski.

[60] A. Wachter-Zeh, *Bounds on list decoding Gabidulin codes*, Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT) (2012).

[61] H. Wang, C. Xing, and R. Safavi-Naini, *Linear authentication codes: bounds and constructions*, IEEE Transactions on Information Theory **49** (2003), no. 4, 866–872.

[62] S.-T. Xia and F.-W. Fu, *Johnson type bounds on constant dimension codes*, Designs, Codes and Cryptography **50** (2009), no. 2, 163–172.