Spread Codes and more General Network Codes

Dissertation

zur

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

vorgelegt der

Mathematisch-naturwissenschaftlichen Fakultät

der

Universität Zürich

von

Felice Manganiello

aus

Mendrisio TI

Promotionskomitee

Prof. Dr. Joachim J. Rosenthal (Vorsitz)
Prof. Dr. Frank R. Kschischang (University of Toronto)
Prof. Dr. Elisa Gorla (Universität Basel)

Zürich, 2011

To my family.

Acknowledgements

First I want to thank my "Doktorvater" Joachim. He is the one that introduced me to network coding, a very beautiful subject. He gave me the first hints and later complete freedom. As a result I am now able to move my first steps alone in this world, or by using his words, I am able to "prove theorems".

I would also like to thank with all my heart Elisa. She is mainly one of my best friends, but in these past years she also took the role of mentor, collaborator and confidant. I will always remember the time spent hanging out, chatting, phone calling and so on. She is the researcher I would like to become one day.

Next one is Frank. I am grateful to him for accepting to be part of my committee and also for accepting me as a postdoc at the University of Toronto. I look forward for a fruitful collaboration with him next year.

Anna-Lena is also someone I feel gratitude to. Unforgettable are the collaborations with her, but mainly, what still makes me smile, it is her calling me her mentor publicly. It was a pleasure mentoring and collaborating with her.

Thanks also to the University of Zurich and mainly to the Institute of Mathematics for the wonderful environment and the opportunity of travelling I had during these years. Thanks to the Swiss National Science Foundation for funding my first steps as a researcher in the academic world.

My family is also to thank for the extreme support they gave me. They always welcomed my decisions trying their best not influencing them. Without them I would never have fulfilled my dreams.

Last but not least I thank all the friends that crossed my life leaving a permanent mark and that are now spread around the world.

Zusammenfassung

Netzwerk-Kodierung ist ein Teilbereich der Kodierungstheorie, der im Jahr 2000 aus einer Arbeit von Ahlswede et al. entstand. Es geht hierbei um ein Protokoll für Kommunikation in einem Netzwerk mit mehreren Quellen und mehreren Senken, auch als Multicast bezeichnet. Multicast wird heutzutage bei Internetprotokollen für Streaming Media, digitales Fernsehen und Peer-to-Peer Connections verwendet. Kötter und Kschischang stellten im Jahr 2008 ein neues mathematisches Modell für Netzwerk-Kodierung vor, woraus der Bedarf an neuen Code-Konstruktionen entstand. Die vorliegende Arbeit befasst sich mit diesem Thema, indem zwei mathematische Konstruktionen für Netzwerk-Codes, die sogenannten Spread Codes und Orbit Codes, und dazugehörige Dekodieralgorithmen vorgestellt werden.

Spread Codes sind eine Familie von optimalen Codes mit maximaler Minimaldistanz. Ein Spread Code wird mithilfe der Algebra einer Begleitmatrix eines irreduziblen Polynoms konstruiert. Wir erläutern einen effizienten Minimaldistanz-Dekodieralgorithmus, welcher die Struktur dieser Algebra und ein neues Resultat über Unterdeterminanten und die Faktorisierung von Polynomen über endlichen Körpern nutzt.

Orbit Codes sind eine Familie von Codes, die man von der Gruppenaktion der Gruppe der invertierbaren Matrizen auf einem Vektorraum erhält. Diese Codes haben gewisse Ähnlichkeiten mit den linearen Codes aus der klassischen Kodierungstheorie. In dieser Arbeit konzentrieren wir uns auf die zyklischen Orbit Codes, das sind die Codes, die von einer zyklischen Untergruppe generiert werden. Wir bringen das Dekodieren von zyklischen Orbit Codes in Verbindung mit dem sogenannten "Rank Discrete Logarithm Problem". Desweiteren erläutern wir ein Zugehörigkeitskriterium, welches erkennt, ob ein empfangener Vektorraum ein Element des Codes ist oder nicht. Dieses steht in Verbindung mit dem diskreten Logarithmus über einem endlichen Körper.

Abstract

Network coding is a branch of coding theory that arose in 2000 from a work by Ahlswede et al. It is a protocol of communication through a network between many sources and many sinks, also called multicast communication. Multicast communication is employed nowadays in Internet protocol applications of streaming media, digital television and peer–to–peer networking. In 2008 Kötter and Kschischang introduced a new mathematical setting for network coding from which the need of new constructions of codes arose. This thesis gives new sensible contributions in this area by giving two original mathematical constructions of codes for network coding, called spread codes and orbit codes, with their related decoding algorithms.

Spread codes are a family of optimal codes with maximum minimum distance. A spread code is constructed starting from the algebra defined by the companion matrix of an irreducible polynomial. We give an efficient minimum distance decoding algorithm based on the structure of the algebra and which uses an original result on minors of a matrix and the factorization of polynomials over finite fields.

Orbit codes are a family of codes which are obtained by the right action of a subgroup of the group of invertible matrices on a linear space. These codes have some similarities with the family of linear codes in classical coding theory. We focus on cyclic orbit codes, i.e., obtained by cyclic subgroups. We relate the problem of decoding cyclic orbit codes to a problem called rank discrete logarithm problem. We present also a membership criterion for a received space to be an element of the code. This last one relates to the discrete logarithm problem over some multiplicative groups of a finite field.

Contents

List of Algorithms

Chapter 1

Introduction

Network coding is a branch of coding theory that arose in 2000 in the work by Ahlswede, Cai, Li and Yeung [ACLY00]. The problem is easy to set up. One is interested in multicast communication, i.e., a set of sources S communicating with a set of sinks R, over a network which is represented by a directed multigraph as in Figure 1.1. Multicast communication is used nowadays and it is often employed in Internet protocol applications of streaming media, digital television and peer–to–peer networking.

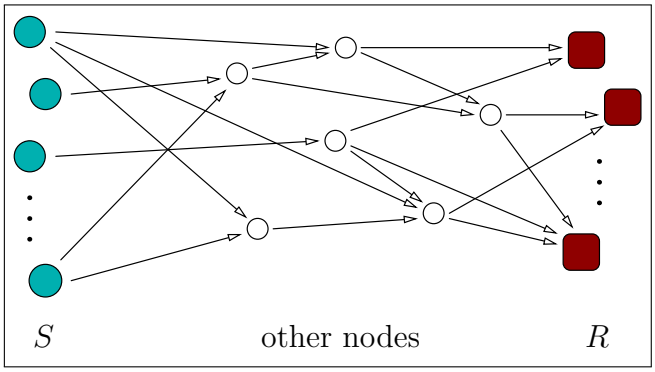


Figure 1.1: Network representation.

The goal of this communication is to maximize the potential of the network by enabling the sources to send the highest possible amount of messages per transmission, meaning per single use of the network. The natural way to send messages through a network is to route information. The nodes constituting the network, in this case, are just able to forward the information they received. This situation is far from being optimal. It is efficient in the case of communication between a single source and a single sink but the situation completely changes when we face multicast communication.

A first example for which just routing information is not enough ap-

peared in [ACLY00] and is represented by the well–known butterfly network. Figure 1.2 depicts this example. A source s communicates two messages to both receivers r_1 and r_2. It is easy to see that by routing, i.e., the situation represented by the left-hand side of Figure 1.2, s needs to send its messages twice. Network coding is a simple idea that improves on routing. One allows the network's internal nodes to play a more active role during the communication. They are allowed to send through the network a combination of their incoming messages. Already for the butterfly network, this simple idea constitutes an important improvement. Indeed, if we also assume for the sinks are able to combine their incoming messages, both r_1 and r_2 receive enough information to reconstruct both the messages in one transmission. The following figure depicts first the routing situation and then the network coding situation where the node v sums together its incoming messages.

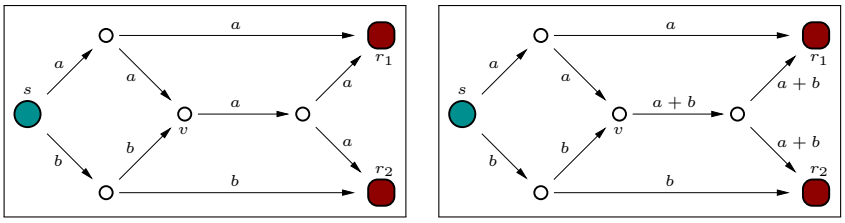


Figure 1.2: Butterfly network communication, first by routing and then by network coding.

The situation showed for the butterfly network is far from being exclusive. We consider especially the case of single–source multicast communication. The rate of communication of a network represents the maximal number of messages sent by a source that all the sinks can reconstruct. This rate is upper bounded by the min–cut of the network. In words, the min–cut represents a bottleneck of the network. It is the minimal set of edges from which messages are forced to pass through in order to get to the sinks.

In [ACLY00] the authors prove that the bound for the rate of communication given by the min–cut is sharp and it can be actually achieved in multicast communication using network coding. A better result comes from the work by Li, Cai and Yeung [LYC03]. They prove that linear network coding is enough to achieve the min–cut bound provided that the size of the base field is large. In order to better understand this last assumption we have to explain exactly what linear network coding means. In linear network coding messages sent by several sources are vectors of $\mathbb{F}_q^n$ where $\mathbb{F}_q$ is the finite field with q elements. In addition, the internal nodes of the network are restricted to forward only linear combinations of their incoming messages.

In order to achieve the maximal rate using linear network coding, one requires knowledge of the structure of the network and control of the linear

combinations the internal nodes are allowed to forward. These are usually unrealistic assumptions. Both sources and sinks ignore this information. An example of this situation is when the structure of the network dynamically changes in time. We speak about random linear network coding when the properties of the networks are unknown to both the sources and the sinks.

The algebraic aspects of network coding emerged with the work by Kötter and Kschischang [KK08b]. The authors introduced a new setting for random linear network coding. As usual in coding theory, we need to start by giving a metric space, the subsets of which will be our codes. Given the linearity of the combinations, the authors suggest to employ as codewords subspaces of a given vector space. Indeed, subspaces are invariant under linear transformations of their elements. Consider $\mathcal{P}(\mathbb{F}_q^n)$ to be the set of all subspaces of $\mathbb{F}_q^n$. This set, together with the subspace distance defined by

$$d(\mathcal{U}, \mathcal{V}) = \dim(\mathcal{U} + \mathcal{V}) - \dim(\mathcal{U} \cap \mathcal{V}) \text{ for all } \mathcal{U}, \mathcal{V} \in \mathcal{P}(\mathbb{F}_q^n),$$

is actually a metric space. Codes are defined to be subsets of $\mathcal{P}(\mathbb{F}_q^n)$. We speak about constant dimension codes when the codewords of the code all have the same dimension.

Consider the situation where a source s sends to the sinks $r \in R$ a codeword $\mathcal{U} \in \mathcal{C} \subseteq \mathcal{P}(\mathbb{F}_q^n)$ where $\mathcal{C}$ is a network code. The communication through the network works in the following way. The source s injects into the network a spanning set of $\mathcal{U}$. Considering error–free communication and that the dimension of $\mathcal{U}$ is less than or equal to the min–cut of the network, all the sinks obtain from the network combinations of the basis vectors which generate the original sent codeword $\mathcal{U}$. Here there are some issues: error–free communication is an unlikely assumption and in addition we consider that neither the source nor the sinks have information about the network, especially its min–cut.

New notions of errors and erasures compatible with the metric space $(\mathcal{P}(\mathbb{F}_q^n), d)$ are introduced in [KK08b]. Errors lead to an increase of the dimension of the codeword. They can be the result of mistakes made during the transmission as well as of vectors injected into the network that are not contained in the codeword. Contrarily, erasures originate a decrease of dimension. Situations in which erasures happen are, for example, a small min–cut or combinations at the level of the internal nodes of the network that annihilate some of the basis vectors during the communication.

The role of mathematics in network coding is the development of "good" codes. There exists no perfect definition of "good" codes. In words, a code is "good" if it satisfies the following properties:

- has a large cardinality, which means it disposes of a big choice of messages to send,

- has a large minimum distance, which corresponds to the possibility of correcting more errors and erasures, and
- there exists a computationally efficient decoding algorithm.

Usually one looks for a trade–off between cardinality and minimum distance, since usually the bigger the cardinality the lower the minimum distance becomes. The existence of bounds for cardinality and minimum distance helps in judging how "good" a code is. In [KK08b] the authors produce upper bounds such as the network coding analog of the Sphere–packing bound and the Singleton bound in classical coding theory. The second one is always sharper then the first one. In [EV08] these two bounds are beaten by the anticode bound. Still, in [KK08b] a lower bound, which is the equivalent of the Gilbert–Varshamov bound in classical coding theory, is given. This lower bound provides the existence of a code with a minimal amount of codewords for a given minimum distance, which however lacks in algebraic structure. As for the decoding algorithm, usually one focuses on the algebraic properties of a code in order to construct it.

In the last decade there was an intense investigation of network coding. We review here some of the results regarding constructions of codes and their decoding algorithms.

The first code construction was introduced by Kötter and Kschischang in [KK08b]. The codes are based on the evaluation of linearized polynomials over a subspace and it is easy to see that this is still a subspace. These codes are called Reed–Solomon like codes for their similarities with Reed–Solomon codes in classical coding theory.

A more general family of codes, which also contains Reed–Solomon like codes, is the subject of the paper [EV08]. The construction is based on binary constant weight codes and Ferrer diagrams.

Another family of codes, this one based on q–analog of designs, appears in [KK08a]. The authors were able to find, by computer search, constant dimension codes based on designs with big cardinalities.

This thesis gives new contributions to the development of these studies. The examples of codes for random linear network coding are not numerous and this field deserves to be further investigated. This work focuses on two original constructions of constant dimension codes and their related decoding algorithms. The two constructions are called *spread codes* and *orbit codes*. We think that these represent a sensible contribution to the development of new "good" codes for network coding.

Spread codes

Spread codes are a family of constant dimension codes first introduced in [MGR08] and further studied in [GMR11]. Spreads of $\mathbb{F}_q^n$ are a collection

of subspaces of $\mathbb{F}_q^n$, all of the same dimension, which partition the ambient space. Such a family of subspaces of $\mathbb{F}_q^n$ exists if and only if the dimension of the subspaces divides the dimension of the ambient space. Spread codes are a particular family of spreads whose definition is given in Theorem 3.1.8. The construction is based on the $\mathbb{F}_q$–algebra $\mathbb{F}_q[P]$ where $P \in GL_k(\mathbb{F}_q)$ is the companion matrix of a monic irreducible polynomial of degree k, which is actually a finite field. In Definition 3.1.10 spread codes are defined as

$$\mathcal{S} = \left\{ \text{rowsp}\begin{pmatrix} A_1 & \cdots & A_r \end{pmatrix} \in \mathfrak{G}_{\mathbb{F}_q}(k,n) \mid A_i \in \mathbb{F}_q[P] \ \forall i \in \{1,\ldots,r\} \right\}$$

where $\mathfrak{G}_{\mathbb{F}_q}(k,n)$ is the Grassmannian of all subspaces of $\mathbb{F}_q^n$ of dimension k.

Since spreads partition the ambient space, spread codes have maximal minimum distance and are optimal. Indeed, it is possible to check that they achieve the anticode bound presented in [EV08]. This family is closely related to the family of Reed–Solomon like codes introduced in [KK08b]. In fact, under certain assumptions, it is possible to extend the existing decoding algorithms for Reed-Solomon like codes to spread codes.

The structure of this special family of spreads, helps us in constructing a minimum distance decoding algorithm which is able to correct up to half the minimum distance of $\mathcal{S}$. In Lemma 3.2.1, we reduce the decoding algorithm for a general spread code (i.e., where $n = rk$ with $r > 2$) to at most $r - 1$ instances of the decoding algorithm for the special case $r = 2$.

We focus then on a decoding algorithm for the spread code

$$\mathcal{S} = \left\{ \text{rowsp}\begin{pmatrix} I & A \end{pmatrix} \mid A \in \mathbb{F}_q[P] \right\} \cup \left\{ \text{rowsp}\begin{pmatrix} 0 & I \end{pmatrix} \right\}.$$

More specifically we present a decoding algorithm with the following specifications:

input: $\mathcal{R} = \text{rowsp}\begin{pmatrix} R_1 & R_2 \end{pmatrix} \in \mathfrak{G}_{\mathbb{F}_q}(k,2k)$,
$P \in GL_k(\mathbb{F}_q)$ the companion matrix of $p \in \mathbb{F}_q[x]$ and
$S \in GL_k(\mathbb{F}_{q^k})$ its diagonalizing matrix.

output: $\mathcal{C} \in \mathcal{S} \subset \mathfrak{G}_{\mathbb{F}_q}(k,2k)$ such that $d(\mathcal{R},\mathcal{C}) < \frac{d(\mathcal{S})}{2} = k$, if such a $\mathcal{C}$ exists.

The equivalence

$$A \in \mathbb{F}_q[P] \iff S^{-1}AS = \text{diag}(\lambda_A, \lambda_A^q, \ldots, \lambda_A^{q^{k-1}}) \text{ for some } \lambda_A \in \mathbb{F}_{q^k},$$

is essential for the construction of the algorithm. Indeed, based on this we first manage to prove a membership criterion in Corollary 3.2.3 which tells when a received space $\mathcal{R} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$ is an element of $\mathcal{S}$.

Consider now the case $\mathcal{R} \notin \mathcal{S}$ and assume there exists a codeword $\mathcal{C} = \text{rowsp}\begin{pmatrix} I & X \end{pmatrix} \in \mathcal{S}$ with $X \in \mathbb{F}_q[P]$ such that $d(\mathcal{R},\mathcal{C}) < \frac{d(\mathcal{S})}{2} = k$. The

distance condition translates into a rank condition, which is more practical from a computational point of view. Indeed

$$d(\mathcal{R},\mathcal{C}) < k \iff \operatorname{rank}\begin{pmatrix} I & X \\ R_1 & R_2 \end{pmatrix} = \operatorname{rank}\begin{pmatrix} I & X \\ 0 & R_1X - R_2 \end{pmatrix} < \frac{3k}{2}$$
$$\iff \operatorname{rank}(S^{-1}R_1S\Delta(\mu) - S^{-1}R_2S) < \frac{k}{2}$$

for a unique value $\mu \in \mathbb{F}_{q^k}$ and where $\Delta(x) = \operatorname{diag}(x, x^q, \ldots, x^{q^{k-1}})$. The uniqueness of μ follows from the uniqueness of the output of a minimum distance decoder.

It follows that we look for the unique common root of all $\lfloor \frac{k+1}{2} \rfloor$ minors of

$$S^{-1}R_1S\Delta(x) - S^{-1}R_2S.$$

Since the degree of the minors is $\sum_{i=1}^{s} q^{k_i}$ for $k_1 < \cdots < k_s < k$, the simple computation of the greatest common divisor would be infeasible. The algorithm focuses then on a unique minor and tests the rank condition for all of its roots in $\mathbb{F}_{q^k}$. Because a minor would have a number of roots which is a power of q, we look for one that has at most $\frac{k}{2}$ roots over $\mathbb{F}_{q^k}$. The search of such a polynomial is the major contribution in the decoding algorithm. We prove Theorem 3.2.8, that such a minor always exists, and we provide an algorithm for finding it.

The minor we look for will have at most $\frac{k}{2}$ roots, each with multiplicity a power of q in general. To find such a minor we first translate the condition on the roots to some conditions on the coefficients of the polynomial itself, as presented in Lemma 3.2.9. Since the coefficients are themselves minors, in the next step we translate these conditions into conditions on minors. These conditions are implicitly related to the ones contained in Lemma 3.2.10. Theorem 3.2.8 is proved by noticing that a minor fulfilling the conditions requested on its $\mathbb{F}_{q^k}$ roots is related to some nonzero minor which can be computed using Algorithm 1 which is a modification of the Gaussian elimination.

We treat separately the case where the received space $\mathcal{R}$, as in the input above has either R_1 or R_2 invertible. In this case we are able to reduce to polynomials with a unique root simply by constructing them from any maximal nonzero minor with consecutive rows and columns. Corollary 3.2.19 delineates this conclusion.

We finish by writing in pseudocode the algorithms related to the decoding of spread codes and we give the complexity of the decoding algorithm for $r = 2$.

Orbit codes

Orbit codes are a broader family of constant dimension codes that was first introduced in [TMR10]. Their name comes from the fact that they are

defined as the right action of a subgroup of $GL_n(\mathbb{F}_q)$ on the Grassmannian $\mathfrak{G}_{\mathbb{F}_q}(k,n)$. Let $\mathcal{U} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$, and $\mathfrak{G} < GL_n(\mathbb{F}_q)$, then an orbit code is the orbit of $\mathcal{U}$ under the action of $\mathfrak{G}$:

$$\mathcal{C} = \{\mathcal{U}A \mid A \in \mathfrak{G}\}.$$

Orbit code have some similarities with linear codes in classical coding theory. Indeed, their minimum distance can be computed by taking the minimum of the distances between the codeword $\mathcal{U}$ and any other $\mathcal{U}A$ with $A \in \mathfrak{G}$ and $\mathcal{U} \neq \mathcal{U}A$, i.e., for any $A \in \mathfrak{G} \setminus Stab(\mathcal{U})$. Moreover, if we denote by $\mathcal{C}^\perp$ the set of $\mathcal{V}^\perp$ for any $\mathcal{V} \in \mathcal{C}$, this is again an orbit code.

In the list of already known constant dimension codes that are also orbit codes we have both spread codes and Reed–Solomon like codes.

After a first glance to the first general properties of orbit codes, we focus on the ones defined by the action of a cyclic subgroup of $GL_n(\mathbb{F}_q)$. Our first goal is to characterize them uniquely up to the equivalence relation given by conjugation over $GL_n(\mathbb{F}_q)$ as defined in Definition 4.2.9. Conjugated codes are not distinguishable from a point of view of their cardinality and distance distribution, the latter defined in Definition 4.2.11. As a consequence conjugate codes have the same decoding capability.

In order to solve this problem we step back and we focus on the characterization of cyclic subgroups of $GL_n(\mathbb{F}_q)$. These results are presented in [MTR11]. It is well known that matrices of $GL_n(\mathbb{F}_q)$ are conjugate if and only if they have the same rational canonical form. We find a similar formulation for cyclic subgroups. In Theorem 4.2.4 we prove that conjugation is an equivalence relation for cyclic subgroups. This theorem states that two cyclic subgroups are conjugate if and only if they have the same cardinality and there exist two generators, one for each subgroup, that are conjugate. In Theorem 4.2.6 we strengthen this result by proving that two subgroups are conjugate if their generators have the same number of elementary divisors, with the same orders and multiplicities.

A simplified version of this theorem can be applied to cyclic orbit codes. For our purpose it is enough to note that cyclic orbit codes are conjugated to the ones defined by cyclic subgroups of $GL_n(\mathbb{F}_q)$ generated by matrices in their rational canonical form. This is proven in Corollary 4.2.13. In Theorem 4.2.14 we construct orbit codes for which it is possible to give a lower bound on their minimum distance.

In the last part we describe the connection between the decoding problem of cyclic orbit codes and the discrete logarithm problem (DLP). In Lemma 4.3.5 we prove that one can decode a cyclic orbit code by solving the rank discrete logarithm problem (RDLP), see Definition 4.3.4. Algorithm 4 depicts a baby–step giant–step algorithm for solving the RDLP.

In the particular case of error–free communication we are able to do better. The problem here is the following: given a received subspace $\mathcal{U}B \in$

$\mathcal{C} = \{\mathcal{U}A^i \mid i \in \mathbb{N}\}$, find an $m \in \mathbb{N}$ such that $\mathcal{U}B = \mathcal{U}A^m$. The main result for this problem is given in Theorem 4.3.8. We are able to reduce the RDLP defined on a cyclic group generated by a matrix A that is diagonalizable over a certain extension field of $\mathbb{F}_q$, to a polynomial amount of DLP's over some small extensions of $\mathbb{F}_q$. Despite the fact that the DLP over a field is in general infeasible, in some cases it is possible to solve it in reasonable time. This is the case for groups with smooth order, for which the DLP is efficiently solvable by using the Pohlig-Hellman algorithm.

This work is organized as follows. In Chapter 2 we give to the reader all the information related to network coding. We start by giving the graph theory background used for representing networks in Section 2.1. Subsection 2.1.1 shows the benefits of using network coding instead of routing in the example of the single–source multicast problem applied to the *butterfly network*. We generalize the conclusions deduced on the butterfly network to all problems of single–source multicast in Subsection 2.1.2. Here we introduce the notion of min–cut and rate of communication. Section 2.2 is devoted to the presentation of the setting introduced by Kötter and Kschischang. Here we focus on the definition of network codes and subspace distance. In 2.2.1 we then focus on errors and erasures and we join them in order to deduce decoding capability of network codes. In Section 2.3 we list some bounds for network codes and in Section 2.4 we speak about the state–of–the–art in code construction and decoding algorithms.

Spread codes are the subject of Chapter 3. In Section 3.1 we focus on the construction of spread codes, also giving their main properties. In Subsection 3.1.1 we explicitly show the connection between spread codes and Reed–Solomon like codes. We introduce the minimum distance decoder for spread codes in Section 3.2. We prove in Subsection 3.2.1 the main theorem of this chapter, namely, Theorem 3.2.8. Subsection 3.2.2 is dedicated to the non–singular case. Finally, in Section 3.3, we write the algorithms for decoding spread codes with a glance also to the complexity of one of them.

Chapter 4 focuses on orbit codes. Similar to Chapter 3 the first section is dedicated to the definition of orbit codes and their general properties. In Section 4.2 we find a characterization of cyclic subgroups of $GL_n(\mathbb{F}_q)$ with respect to the equivalence relation induced by conjugation. In Subsection 4.2.1 we apply these results in order to give some constructions of orbit codes for which we have a lower bound on their minimum distance. Section 4.3 translates the problem of decoding cyclic orbit codes to the rank discrete logarithm problem. We focus in Subsection 4.3.1 on the case of error-free communication. Here we show that the rank discrete logarithm problem reduces to some instances of the discrete logarithm problem.

Chapter 2

Background on network coding

2.1 Network representation

A network employed for communication is modeled by a *directed acyclic multigraph*. We refer to [Die05, Chapter 1] as a reference on graph theory.

Definition 2.1.1. A *directed graph* is a pair $G = (V, E)$ where $E \subseteq V \times V$. The elements of V are called *nodes*, or *vertices*, of the graph G, the elements of E are its *edges*.

The following figure depicts a graphical representation of a directed graph.

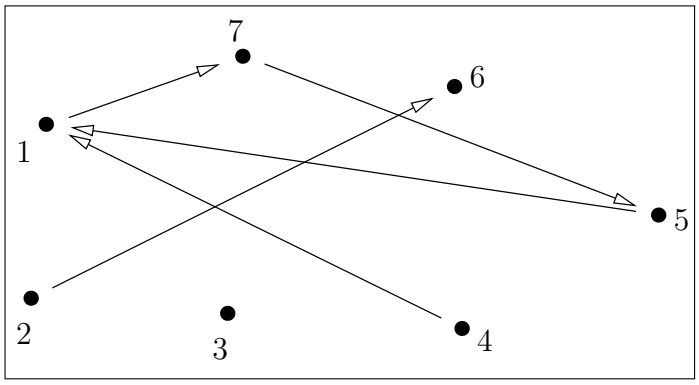


Figure 2.1: The directed graph $G = (V, E)$ with $V = \{1, 2, \ldots, 7\}$ and $E = \{(1, 7), (2, 6), (4, 1), (5, 1), (7, 5)\}$.

Definition 2.1.2. We define the following two projections

$$\begin{array}{rccc} \pi_1 : & V \times V & \to & V \\ & (v_1, v_2) & \mapsto & v_1 \end{array} \qquad \text{and} \qquad \begin{array}{rccc} \pi_2 : & V \times V & \to & V \\ & (v_1, v_2) & \mapsto & v_2 \end{array}$$

and the following sets

$$\text{in}(v) := \{e \in E \mid \pi_2(e) = v\} \text{ the set of its incoming edges, and}$$

$$\text{out}(v) := \{e \in E \mid \pi_1(e) = v\} \text{ the set of its outgoing edges.}$$

An edge $e \in E$ is said to be *directed from* $\pi_1(e)$ *to* $\pi_2(e)$. Two vertices $v_1, v_2 \in G$ are *adjacent*, or *neighbours*, if either $(v_1, v_2) \in E$ or $(v_2, v_1) \in E$.

Definition 2.1.3. Let $G = (V, E)$ and $G' = (V', E')$ be two directed graphs. If $V' \subseteq V$ and $E' \subseteq E$, then G' is a *subgraph* of G, written $G' \subseteq G$. A *path* is a graph $P = (V, E)$ of the form

$$V = \{v_1, \ldots, v_k\} \text{ and } E = \{(v_1, v_2), (v_2, v_3), \ldots, (v_{k-1}, v_k)\}.$$

If $P = (V, E)$ is a path, then the graph $C = (V, E \cup (v_k, v_1))$ is called a *cycle*. Let $v \in V$, the edge (v, v) is called a *loop*.

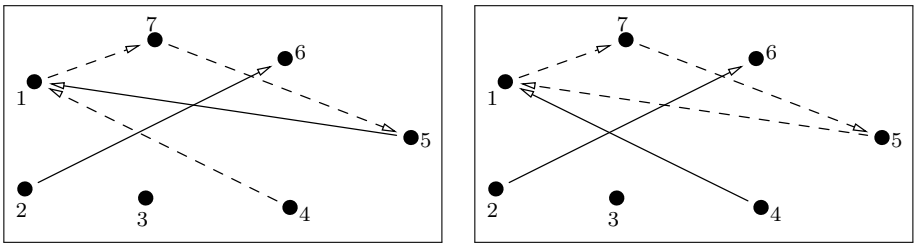


Figure 2.2: A path $P = (\{1, 4, 5, 7\}, \{(4, 1), (1, 7), (7, 5)\}) \subset G$ and a cycle $C = (\{1, 5, 7\}, \{(1, 7), (7, 5), (5, 1)\}) \subset G$.

Definition 2.1.4. A directed graph $G = (V, E)$ is called *acyclic* if it does not contain cycles or loops.

Now that we have defined directed acyclic graphs, we need only to introduce the notion of *multigraphs*.

Definition 2.1.5. A *directed multigraph* is a pair $G = (V, E)$ with $E = (e_1, \ldots, e_k) \in (V \times V)^k$, k representing the number of edges of the graph. In a multigraph we allow multiple edges, i.e., it is possible that $e_i = e_j$ for $1 \leq i \neq j \leq k$.

With a slight abuse of notation we write $e \in E$ if e is an entry of the tuple E, meaning that there exists an i, $1 \leq i \leq k$ such that $e = e_i$. Using this notation we are able to define the following tuples:

$$\text{in}(v) := (e \in E \mid \pi_2(e) = v) \text{ and } \text{out}(v) := (e \in E \mid \pi_1(e) = v).$$

In the next subsection we also use the notation $E' \subseteq E$ when E' is, up to reordering, a partial tuple of E.

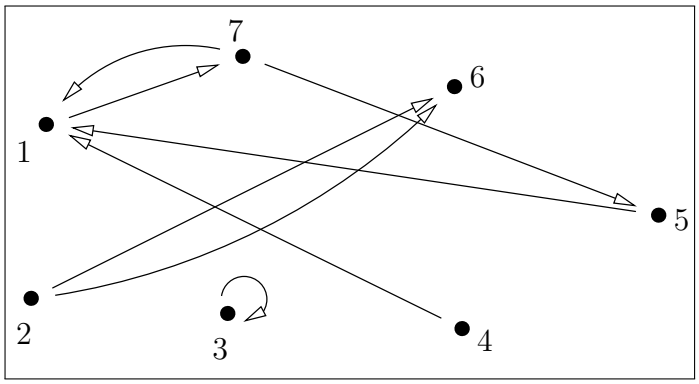


Figure 2.3: The directed multigraph $G = (V, E)$ with $V = \{1, 2, \ldots, 7\}$ and $E = ((1, 7), (2, 6), (2, 6), (3, 3), (4, 1), (5, 1), (7, 5), (7, 1))$.

As previously stated, we represent the network as a *direct acyclic multigraph* $G = (V, E)$. Every edge $e \in E$ represents a channel of the network with "unit capacity", meaning that for unit time, only one message can be sent from $in(e)$ to $out(e)$. Being able to work with multigraphs makes it possible to consider channels with integer capacity greater than one. Indeed, if there exists a channel between two vertices $v_1, v_2 \in V$ with n "units capacity", i.e., being able to send n messages per unit time, this channel is representable by n parallel directed edges from v_1 to v_2. An edge $e \in E$ simply takes in a message from the node $\pi_1(e)$ and sends it to the node $\pi_2(e)$.

From the set of vertices V, we distinguish two subsets $S, R \subset V$. The set S represents the set of the *sources*, and R the set of the *sinks*. By adding some *virtual nodes* in the multigraph, it is possible, without loss of generality, to obtain a graph where

- $S \cap R = \emptyset$,
- $\text{in}(v) = \emptyset$ for all $v \in S$, and
- $\text{out}(v) = \emptyset$ for all $v \in R$.

Figure 2.4 depicts a multicast network representation.

The *multicast problem* is the problem where each sink $r \in R$ is interested in reconstructing all messages sent by all sources $s \in S$. Another problem related to this one is the *unicast problem* where both S and R consist of only one entity. In general in this work we will consider the case of the *single–source multicast problem*, i.e., the problem where the source is unique and all different sinks want to reconstruct the messages sent by the source.

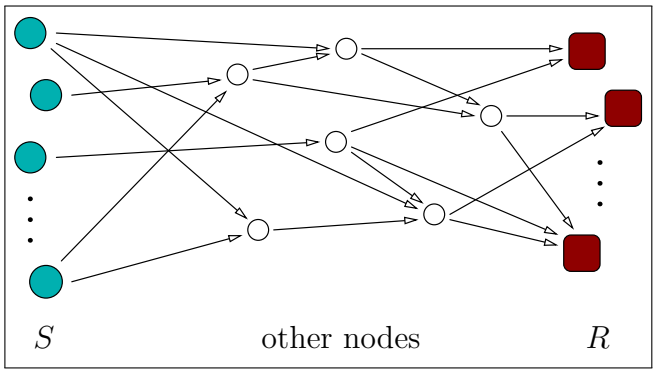


Figure 2.4: Network representation

2.1.1 Network coding vs routing

In this subsection we introduce the notion of *network coding* and, with the help of an example, we show the strength of this network communication protocol with respect to the routing protocol.

Consider a network $G = (V, E)$ with $E = (e_1, \dots, e_k) \in (V \times V)^k$, $S, R \subset V$ respectively the set of sources and the one of sinks where $S \cap R = \emptyset$ and define $O := V \setminus (S \cup R)$. Let M be the set of messages the sources have at their disposal. We will be more specific regarding the set M in Section 2.2. Let $e \in E$, denote by $m_e \in M$ the message sent from the node $\pi_1(e)$ to $\pi_2(e)$. Consider also the following sets of messages related to a node $v \in O$

- $M_{\text{in}}(v) = \{m_e \in M \mid e \in E,\ v = \pi_2(e)\}$ the set of messages that the node $v \in O$ receives from other nodes, and
- $M_{\text{out}}(v) = \{m_e \in M \mid e \in E,\ v = \pi_1(e_i)\}$ the set of messages that the node $v \in O$ sends to other nodes.

We distinguish two different ways of communicating through a network.

Routing Let $v \in O$. For every $e \in \text{out}(v)$, $m_e \in M_{\text{in}}(v)$, meaning that the nodes $v \in O$ forward through channel e an unaltered message chosen from its incoming messages.

Network coding Let $v \in O$. For every $e \in \text{out}(v)$, $m_e = \phi_{v,e}(M_{\text{in}}(v))$ is a combination of the incoming messages $m \in M_{\text{in}}(v)$. The maps $\phi_{v,e}$ are called *local encoding functions*.

Clearly routing can be viewed as a particular case of network coding where the local encoding functions simply return one of the elements of $M_{\text{in}}(v)$ for any $v \in O$.

The rest of the subsection is devoted to illustrate an example, first provided in [ACLY00], where the limitations of routing with respect to network

coding are shown. Consider the network represented in Figure 2.5 called the *butterfly network*.

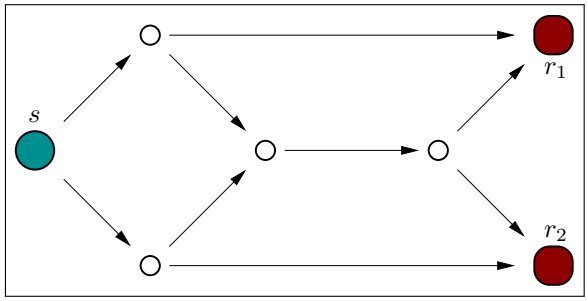


Figure 2.5: Butterfly network.

Let the set of messages M be $\mathbb{F}_q$, i.e., the finite field with q elements. Suppose that each channel can send only one element of $\mathbb{F}_q$ per unit time, or transmission. We focus on the single–source multicast problem. Let $a, b \in \mathbb{F}_q$ be the messages that the source s wants to share with both sinks r_1 and r_2.

Considering the *routing* protocol, the node v forwards only one of its incoming messages. It means that it has to choose between a and b. Because of the symmetry of the network, assume, without loss of generality, that v decides to forward a, as depicted in Figure 2.6.

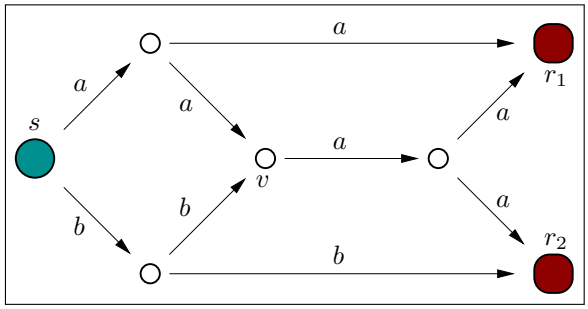


Figure 2.6: Butterfly network with routing.

As a consequence we obtain that the sink r_1 receives only the message a. In order for both sinks to receive both the messages, s needs to retransmit $a, b \in \mathbb{F}_q$ and v has to route $b \in \mathbb{F}_q$ instead of $a \in \mathbb{F}_q$.

If instead we consider the network coding protocol, we are able to transmit the messages $a, b \in \mathbb{F}_q$ only once under the assumption that both the sinks can elaborate the receive information. Indeed, suppose the node v combines the messages simply by adding them together as in Figure 2.7.

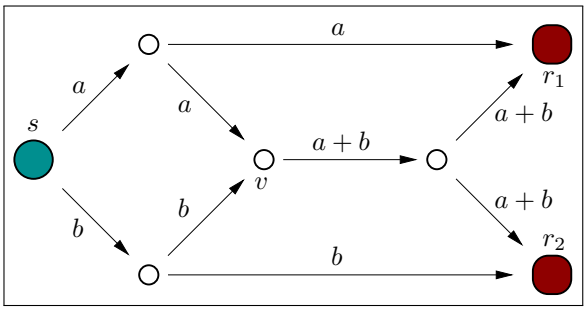


Figure 2.7: Butterfly network with network coding.

In this case both sinks r_1 and r_2 receive enough information in order to recover both messages by the use of an easy subtraction over $\mathbb{F}_q$.

We conclude that the single–source multicast problem, at least in this example, achieves the task of a complete communication in only one transmission by employing network coding. We show in the following subsection that in general for the single–source multicast problem, routing is not enough. Instead, by using network coding we get the best possible performances.

2.1.2 Min–cut and linear network coding

Definition 2.1.6. Let $G = (V, E)$ be a multigraph and $s, r \in V$. An $\{s, r\}$-*separating cut* $C \subset E$ is a set of edges such that every path from s to r contains an edge of C. A $\{s, r\}$-*minimal cut* is a $\{s, r\}$-separating cut with smallest cardinality. The cardinality of a $\{s, r\}$-minimal cut is denoted by $\text{mincut}(s, t)$.

The following figures depict the previous notions on the butterfly network.

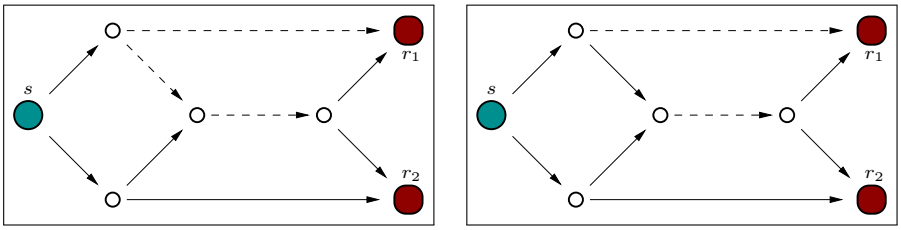


Figure 2.8: An $\{s, r_1\}$-separating cut and $\{s, r_1\}$-minimal cut.

An important notion related to a network is the one of rate of communication. Let $G = (V, E)$ be a directed multigraph and $s, r \in V$. In words, the rate $\mathfrak{r}(s, r)$ is the maximum number of distinct messages sent by s that

the sink r can reconstruct in one transmission. Since any $\{s,r\}$-minimal cut narrows the amount of messages passing through the network, it follows that

$$\mathfrak{r}(s,r) \leq \text{mincut}(s,r). \tag{2.1}$$

In the unicast problem, meaning the communication between a single source s and a single sink r over a network, this rate is achievable by routing. Indeed, by Menger's Theorem [Men27], the $\text{mincut}(s,r)$ corresponds to the number of disjoint paths between s and r and by simply sending different messages over different paths we get that $\mathfrak{r}(s,r) = \text{mincut}(s,r)$.

The situation is different in the case of the single–source multicast problem, i.e., the communication between a single source s and many sinks $r \in R$. The rate of communication $\mathfrak{r}(s,R)$ in this case is the maximum number of distinct messages sent by s that in one transmission any of sinks $r \in R$ can reconstruct. From (2.1) it follows

$$\mathfrak{r}(s,R) \leq \min_{r\in R} \text{mincut}(s,r).$$

This bound is achievable by simply using *linear network coding*. An example is given in Figure 2.7. *Linear network coding* is a particular instance of network coding where the local encoding functions are linear. Let $M = \mathbb{F}_q^n$ for some $n, q \in \mathbb{N}$ such that q is a power of a prime. It means that the source s sends messages in the form of vectors into the network. Every node $v \in V \setminus (s \cup R)$ for any edge $e \in E$ such that $v = \pi_1(e)$, forward to $\pi_2(e)$ the message $\phi_{v,e}(M_{\text{in}}(v))$ which is a linear combination of the vectors of $M_{\text{in}}(v)$.

The theorem stating the rate $\mathfrak{r}(s,R)$ achieves the min–cut bound is the following.

Theorem 2.1.7 ([KM03, Theorem 2])**.** *Consider a network represented by a directed acyclic multigraph $G = (V,E)$, $s \in V$ and $R \subset V$ a nonempty subset such that $s \notin R$, $\text{in}(s) = \emptyset$ and $\text{out}(r) = \emptyset$ for any $r \in R$. Let $M = \mathbb{F}_q^n$. If $q > |R|$, then, for for any $v \in V \setminus (s \cup R)$ and any $e \in \text{out}(v)$, there exists a choice of the linear local encoding functions $\varphi_{v,e}$ for which it holds*

$$\mathfrak{r}(s,R) = \min_{r\in R} \text{mincut}(s,r).$$

The theorem takes into account the knowledge of the structure, or topology, of the network and the possibility to choose the local encoding functions for every node of the network. This information is often unavailable to the sources and the sinks. A practical example in which it is difficult to know the structure of the network is when the latter varies in time. We speak about *random linear network coding*, or *non–coherent linear network coding*, when communication happens on a network by using linear local encoding functions and the network structure is unknown by both sources and sinks.

2.2 Kötter–Kschischang setting

In [KK08b] the authors introduced a new mathematical setting for random linear network coding. In classical coding theory, codes are represented by subsets of a given vector space and its elements are called codewords. For random linear network coding, codes are proposed to be sets of subspaces of a given vector space. Consequently, codewords become subspaces. A motivation for this change is that, unlike vectors, subspaces are invariant under the action of the local encoding functions.

The communication works as follows. A source injects into the network a spanning set of the codeword. Into the network, these vectors are then linearly combined with each other by the local encoding functions. In the case where the dimension of the chosen subspace is less than the min–cut of the network and if no errors nor erasures happen during the transmission, any sink $r \in R$ recovers the codeword simply by collecting the incoming vectors, since these ones generate the sent codeword.

We formally explain the setting introduced by Kötter and Kschischang in [KK08b]. In this section, let $q, k, n \in \mathbb{N}$ be such that $k \leq n$ and q is a power of a prime.

Definition 2.2.1. The *Grassmannian* $\mathfrak{G}_{\mathbb{F}_q}(k,n)$ is the set of all k dimensional subspaces of $\mathbb{F}_q^n$. The *projective space of* $\mathbb{F}_q^n$ $\mathcal{P}(\mathbb{F}_q^n)$ is the set of all subspaces of $\mathbb{F}_q^n$, i.e.,

$$\mathcal{P}(\mathbb{F}_q^n) = \bigcup_{i=0}^{n} \mathfrak{G}_{\mathbb{F}_q}(i,n).$$

It is possible to equip the set $\mathcal{P}(\mathbb{F}_q^n)$, as well as the Grassmannian $\mathfrak{G}_{\mathbb{F}_q}(k,n)$, with a metric.

Definition 2.2.2. We call the *subspace distance* the function d defined as follows

$$\begin{array}{rccc} d: & \mathcal{P}(\mathbb{F}_q^n) \times \mathcal{P}(\mathbb{F}_q^n) & \to & \mathbb{Z} \\ & (\mathcal{U}, \mathcal{V}) & \mapsto & \dim(\mathcal{U}+\mathcal{V}) - \dim(\mathcal{U}\cap\mathcal{V}). \end{array}$$

Lemma 2.2.3 ([KK08b, Lemma 1])**.** *The function d is a metric for the set $\mathcal{P}(\mathbb{F}_q^n)$.*

By using the dimension formula of the sum of two vector spaces, we get the following lemma.

Lemma 2.2.4. *Let $\mathcal{U}, \mathcal{V} \in \mathcal{P}(\mathbb{F}_q^n)$, then*

$$d(\mathcal{U},\mathcal{V}) = \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2\dim(\mathcal{U}\cap\mathcal{V}).$$

When $\mathcal{U}, \mathcal{V} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$ the subspace distance becomes

$$d(\mathcal{U},\mathcal{V}) = 2k - 2\dim(\mathcal{U}\cap\mathcal{V}).$$

This distance can equivalently be defined through *Hasse diagrams*. Hasse diagrams are graphs representing partially ordered sets. We restrict to the theory we need for defining the distance. For more information we direct the reader to [Sta97, Chapter 3].

Definition 2.2.5. A *partially ordered set* P, or *poset*, is a set, which by abuse of notation we denote also by P, together with a binary relation denoted $\leq$ satisfying the following three axioms.

- *Reflexivity*: for any $p \in P$ it holds $p \leq p$.
- *Antisymmetry*: for any $p_1, p_2 \in P$, if $p_1 \leq p_2$ and $p_2 \leq p_1$, then $p_1 = p_2$.
- *Transitivity*: for any $p_1, p_2, p_3 \in P$, if $p_1 \leq p_2$ and $p_2 \leq p_3$, then $p_1 \leq p_3$.

For any poset it is possible to construct its Hasse diagram.

Definition 2.2.6. Let P be a poset. If $p_1, p_2 \in P$ we say that p_2 *covers* p_1 if $p_1 < p_2$, i.e., $p_1 \leq p_2$ and $p_1 \neq p_2$, and if no element $p \in P$ satisfies $p_1 < p < p_2$. A *Hasse diagram* of the poset P is a graph $G_p = (P, E)$ where the nodes are the elements of P and where $\{p_1, p_2\} \in E \subset \{U \subset P \mid |U| = 2\}$ if and only if either p_1 covers p_2 or p_2 covers p_1. In a graphical representation of the Hasse diagram, if $p_1, p_2 \in P$ satisfy $p_1 < p_2$, then we draw the node p_1 in a lower level with respect to the one of p_2.

The set $\mathcal{P}(\mathbb{F}_q^n)$ with the set inclusion $\subseteq$ is a poset. Let us translate the cover relation in the language of subspaces.

Lemma 2.2.7. *Let $\mathcal{U}, \mathcal{V} \in \mathcal{P}(\mathbb{F}_q^n)$. Then, $\mathcal{V}$ covers $\mathcal{U}$ if and only if $\mathcal{U} \subset \mathcal{V}$ and $\dim \mathcal{U} = \dim \mathcal{V} - 1$*

Proof. The proof of this lemma follows from the fact that a necessary condition for a subspace $\mathcal{W} \in \mathcal{P}(\mathbb{F}_q^n)$ such that $\mathcal{U} \subset \mathcal{W} \subset \mathcal{V}$ to exist, is that $\dim(\mathcal{U}) < \dim(\mathcal{W}) < \dim(\mathcal{V})$. □

Figure 2.9 depicts the Hasse diagram of $\mathcal{P}(\mathbb{F}_q^n)$. From the definition of covers it follows that each layer corresponds to a different Grassmannian $\mathfrak{G}_{\mathbb{F}_q}(k, n)$ with $k \leq n$ ordered bottom to top in increasing order with respect to the k.

By the following lemma, we translate the subspace distance on the Hasse diagram.

Lemma 2.2.8. *Let $\mathcal{U}, \mathcal{V} \in \mathcal{P}(\mathbb{F}_q^n)$. Then $d(\mathcal{U}, \mathcal{V})$ corresponds to the length of a shortest path in the Hasse diagram connecting the corresponding nodes.*

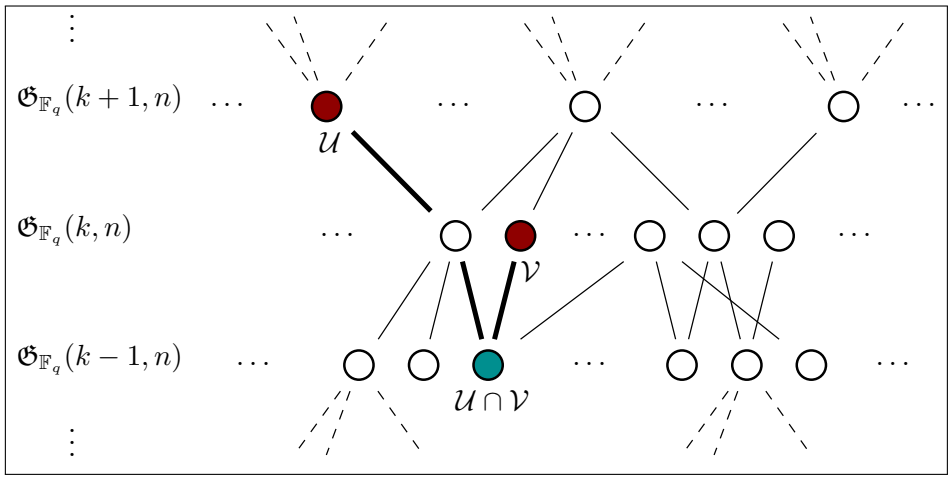


Figure 2.9: Hasse diagram for the poset $\mathcal{P}(\mathbb{F}_q^n)$.

Figure 2.9 shows a minimum path connecting nodes $\mathcal{U} \in \mathfrak{G}_{\mathbb{F}_q}(k+1,n)$ and $\mathcal{V} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$ which are distant $d(\mathcal{U},\mathcal{V}) = 3$.

The following lemma shows how to translate the subspace distance into a rank condition. This is helpful since the rank is more effective from a computational point of view.

Lemma 2.2.9. *Let $\mathcal{U},\mathcal{V} \in \mathcal{P}(\mathbb{F}_q^n)$. It holds that*

$$\operatorname{rank}\begin{pmatrix} U \\ V \end{pmatrix} = \frac{\dim(\mathcal{U}) + \dim(\mathcal{V}) + d(\mathcal{U},\mathcal{V})}{2}$$

for any $U,V \in \mathbb{F}_q^{k\times n}$ such that $\mathcal{U} = \operatorname{rowsp}(U)$ and $\mathcal{V} = \operatorname{rowsp}(V)$. When $\mathcal{U},\mathcal{V} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$, then

$$\operatorname{rank}\begin{pmatrix} U \\ V \end{pmatrix} = k + \frac{d(\mathcal{U},\mathcal{V})}{2}. \tag{2.2}$$

Proof. Let $U,V \in \mathbb{F}_q^{k\times n}$ be matrices such that $\mathcal{U} = \operatorname{rowsp}(U)$ and $\mathcal{V} = \operatorname{rowsp}(V)$. Then

$$\begin{aligned}\operatorname{rank}\begin{pmatrix} U \\ V \end{pmatrix} &= \dim(\mathcal{U}) + \dim(\mathcal{V}) - \dim(\mathcal{U}\cap\mathcal{V}) \\ &= \dim(\mathcal{U}) + \dim(\mathcal{V}) - \frac{\dim(\mathcal{U}) + \dim(\mathcal{V}) - d(\mathcal{U},\mathcal{V})}{2} \\ &= \frac{\dim(\mathcal{U}) + \dim(\mathcal{V}) + d(\mathcal{U},\mathcal{V})}{2},\end{aligned}$$

where the second equality follows from the definition of subspace distance. It is obvious that the rank $\begin{pmatrix} U \\ V \end{pmatrix}$ does not depend on the choice of the matrices $U,V \in \mathbb{F}_q^{k\times n}$. The case $\mathcal{U},\mathcal{V} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$ follows easily. □

Definition 2.2.10. A *code*, or *network code*, $\mathcal{C}$ is a nonempty subset of $\mathcal{P}(\mathbb{F}_q^n)$. We speak about *constant dimension codes* when $\mathcal{C} \subset \mathfrak{G}_{\mathbb{F}_q}(k,n)$, i.e., when all codewords have the same dimension k.

Since $\mathcal{P}(\mathbb{F}_q^n)$ is a metric space, we can define the *minimum distance* of a code.

Definition 2.2.11. Let $\mathcal{C} \subseteq \mathcal{P}(\mathbb{F}_q^n)$ be a code. Then its minimum distance is denoted by

$$d(\mathcal{C}) := \min_{\mathcal{U} \neq \mathcal{V} \in \mathcal{C}} d(\mathcal{U}, \mathcal{V}).$$

The *maximum dimension* of a code $\mathcal{C} \subseteq \mathcal{P}(\mathbb{F}_q^n)$ is denoted by

$$k(\mathcal{C}) := \max_{\mathcal{U} \in \mathcal{C}} \dim(\mathcal{U}).$$

We say that a code $\mathcal{C} \subset \mathcal{P}(\mathbb{F}_q^n)$ is of type $[n, k, \log_q |\mathcal{C}|, d]$ if its maximal dimension is k, it has cardinality $|\mathcal{C}|$ and minimum distance d.

2.2.1 Errors, erasures and the decoding problem

Error–free communications are an unrealistic assumption. As for codes and codewords, the model of errors and erasures from classical coding theory is not suitable for networks which perform linear network coding. In [KK08b] the authors propose a new model for errors and erasures suitable in this setting.

We explain here these notions with the help of the Hasse diagram.

- *Erasure*: it corresponds to a drop of dimension of the subspace. It can be due to an insufficient min–cut of the network or by unlucky choices of some local encoding functions. In the Hasse diagram it consists of moving to a node corresponding to a subspace of the original subspace, meaning to one of its neighbour lower layer's nodes.

- *Error*: it corresponds to an increase of dimension of the original subspace. It can be due to errors during the communication or also insertions of new vectors. In the Hasse diagram it consists of moving to a node which corresponds to a subspace containing the original subspace, meaning to one of its neighbour upper layer's nodes.

Let $\mathcal{C} \subseteq \mathcal{P}(\mathbb{F}_q^n)$ be a network code. A *minimum distance decoder* for the code $\mathcal{C}$ is a procedure that given, as input a $\mathcal{R} \in \mathcal{P}(\mathbb{F}_q^n)$, returns the unique codeword $\mathcal{U} \in \mathcal{C}$ such that $d(\mathcal{U}, \mathcal{R}) \leq d(\bar{\mathcal{U}}, \mathcal{R})$ for all $\bar{\mathcal{U}} \in \mathcal{C}$. Note that since we are requiring uniqueness of the output codeword, when the closest codewords are more than one, a minimum distance decoder would usually fail.

We provide a theorem regarding the capability of correcting a network code $\mathcal{C}$ by a minimum distance decoder.

Theorem 2.2.12 ([KK08b, Theorem 2]). *Let $\mathcal{U} \in \mathcal{C} \subseteq \mathcal{P}(\mathbb{F}_q^n)$. Let $\mathcal{R} \in \mathcal{P}(\mathbb{F}_q^n)$ be such that $\mathcal{R} = \mathcal{U}' \oplus \mathcal{E}$ where $\mathcal{U}' \subseteq \mathcal{U}$ and $\mathcal{E} \in \mathcal{P}(\mathbb{F}_q^n)$ is the t dimensional space generated by the errors. Let $s = \dim(\mathcal{U}) - \dim(\mathcal{U}')$ be the number of erasures. If*

$$2(t+s) < d(\mathcal{C})$$

then $d(\mathcal{U}, \mathcal{R}) < d(\bar{\mathcal{U}}, \mathcal{R})$ for all $\bar{\mathcal{U}} \in \mathcal{C}$.

For the purpose of this work we stop considering general network codes and focus on constant dimension codes. We also introduce another constraint to our setting. We are going to consider that once a codeword $\mathcal{U} \in \mathcal{C} \subset \mathfrak{G}_{\mathbb{F}_q}(k,n)$ is sent, any sink receives from the network a subspace $\mathcal{R} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$. As a consequence, we obtain that the number of erasures and errors during the communication are going to be the same.

Given these assumptions, we resume the following definition of the decoding problem we are interested in solving for constant dimension codes.

Definition 2.2.13. Let $\mathcal{C} \subset \mathfrak{G}_{\mathbb{F}_q}(k,n)$ and $\mathcal{R} \subset \mathfrak{G}_{\mathbb{F}_q}(k,n)$. We say that the space $\mathcal{R}$ is decodable up to half $d(\mathcal{C})$ if there exists a $\mathcal{U} \in \mathcal{C}$ such that $d(\mathcal{U}, \mathcal{R}) < \frac{d(\mathcal{C})}{2}$. We call the *decoding problem* the problem of finding such a $\mathcal{U} \in \mathcal{C}$ given $\mathcal{R}$, provided that such a $\mathcal{U}$ exists.

2.3 Bounds on network codes

Since the body of this thesis consists of studying constant dimension codes, this section will focus on the Grassmannian $\mathfrak{G}_{\mathbb{F}_q}(k,n)$ where q is a power of a prime and $k \leq n$. We provide here a list of bounds.

Definition 2.3.1 ([vLW01, Chapter 24]). The *Gaussian coefficient* $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is defined to be the cardinality of the Grassmannian $\mathfrak{G}_{\mathbb{F}_q}(k,n)$ that is

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

The Gaussian coefficient is often also called in literature the *q-analog of the binomial coefficient*.

As for the binomial coefficient it holds that $\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ n-k \end{bmatrix}_q$.

Lemma 2.3.2 ([KK08b, Lemma 4],[GY08, Lemma 1]). *For the Gaussian coefficient it holds*

$$1 \leq q^{-k(n-k)} \begin{bmatrix} n \\ k \end{bmatrix}_q < K < 4$$

where $K := \prod_{i=1}^{\infty}(1-q^i)^{-1}$.

In order to give network coding analog of the sphere–packing and the sphere–covering bound from classical coding theory, we have to compute how many elements of $\mathfrak{G}_{\mathbb{F}_q}(k,n)$ are close to a given space in $\mathcal{U} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$.

Definition 2.3.3. A ball $B(\mathcal{U},d) \subseteq \mathfrak{G}_{\mathbb{F}_q}(k,n)$ centered in $\mathcal{U} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$ with radius $d \in \mathbb{N}$ is the set

$$B(\mathcal{U},d) = \{\mathcal{V} \in \mathfrak{G}_{\mathbb{F}_q}(k,n) \mid d(\mathcal{U},\mathcal{V}) \leq d\}.$$

Since the subspace distance between spaces of the same dimension is always even, it holds that $B(\mathcal{U},d+1) = B(\mathcal{U},d)$ when $d = 2t$ for some $t \in \mathbb{N}$.

We can now compute the cardinality of these balls.

Lemma 2.3.4 ([KK08b, Theorem 5])**.** *The cardinality of $B(\mathcal{U},2\delta)$ is independent of the choice of the space $\mathcal{U} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$ and it is*

$$|B(\mathcal{U},2\delta)| = \sum_{i=0}^{\delta} |B(\mathcal{U},2i)| = \sum_{i=0}^{\delta} q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} n-k \\ i \end{bmatrix}_q.$$

Using the definition of a ball and its cardinality, we get the following *sphere–packing bound*.

Theorem 2.3.5 ([KK08b, Theorem 6])**.** *Let $\mathcal{C} \subset \mathfrak{G}_{\mathbb{F}_q}(k,n)$ such that $d(\mathcal{C}) \geq 2\delta$ and $\gamma := \lfloor \frac{\delta-1}{2} \rfloor$. Then, it holds*

$$|\mathcal{C}| < 4q^{(k-\gamma)(n-k-\gamma)}.$$

The bound is obtained by dividing the cardinality of $\mathfrak{G}_{\mathbb{F}_q}(k,n)$ by the cardinality of a ball of radius $2\gamma < \frac{2d-1}{2}$. This bound represents the maximal number of elements of $\mathfrak{G}_{\mathbb{F}_q}(k,n)$ such that the balls of radius 2γ centered in them do not intersect.

In the same work the authors also proposed a network coding analog of the *Singleton bound* from classical coding theory, which, they proved is always tighter than the sphere–packing bound.

Theorem 2.3.6 ([KK08b, Theorem 9])**.** *Let $\mathcal{C} \subset \mathfrak{G}_{\mathbb{F}_q}(k,n)$ such that $d(\mathcal{C}) = 2\delta$, it holds that*

$$|\mathcal{C}| \leq \begin{bmatrix} n-(\delta-1) \\ \max\{k,n-k\} \end{bmatrix}_q$$

This bound is constructed by puncturing a network code. The operation of puncturing a code of $\mathfrak{G}_{\mathbb{F}_q}(k,n)$ is explained in [KK08b, Section V.A] and it consists of producing from $\mathcal{C} \subset \mathfrak{G}_{\mathbb{F}_q}(k,n)$ a code $\mathcal{C}' \subset \mathfrak{G}_{\mathbb{F}_q}(k-1,n-1)$ satisfying the following two properties:

- $|\mathcal{C}'| = |\mathcal{C}|$, and

- $d(\mathcal{C}') \geq d(\mathcal{C}) - 2$.

It follows that by puncturing a code $\mathcal{C} \subset \mathfrak{G}_{\mathbb{F}_q}(k,n)$, $\delta - 1$ times, we obtain a code $\mathcal{C}' \subset \mathfrak{G}_{\mathbb{F}_q}(k-(\delta-1), n-(\delta-1))$ and since $d(\mathcal{C}') \geq 2$, its cardinality is bounded by the cardinality of $\mathfrak{G}_{\mathbb{F}_q}(k-(\delta-1), n-(\delta-1))$.

In [EV08] the authors explain that the balls are not the right structure in order to get a good upper bound for the cardinality of a code. They suggest the use of the so–called anticodes of Grassmannians and conclude an even tighter bound than the Singleton one, called anticode bound.

Definition 2.3.7. An anticode $A(d)$ of diameter $d \in \mathbb{N}$ in $\mathfrak{G}_{\mathbb{F}_q}(k,n)$ is any subset of $\mathfrak{G}_{\mathbb{F}_q}(k,n)$ such that $d(\mathcal{U},\mathcal{V}) \leq d$ for any $\mathcal{U},\mathcal{V} \in A(d)$.

The largest anticode in $\mathfrak{G}_{\mathbb{F}_q}(k,n)$ has been shown in [FW86], and from its cardinality we get the following *anticode bound*.

Theorem 2.3.8 ([EV08, Theorem 1])**.** *Let $\mathcal{C} \subset \mathfrak{G}_{\mathbb{F}_q}(k,n)$ such that $d(\mathcal{C}) = 2\delta$, it holds that*

$$|\mathcal{C}| \leq \prod_{i=0}^{k-\delta} \frac{q^{n-i}-1}{q^{k-i}-1}.$$

Also this bound can be sharpened by the following bound.

Theorem 2.3.9 ([EV08, Theorem 4])**.** *Let $\mathcal{C} \subset \mathfrak{G}_{\mathbb{F}_q}(k,n)$ be a code such that $d(\mathcal{C}) = 2\delta$, it holds that*

$$|\mathcal{C}| \leq \left\lfloor \frac{q^n-1}{q^k-1} \left\lfloor \frac{q^{n-1}-1}{q^{k-1}-1} \cdots \left\lfloor \frac{q^{n-k+\delta}-1}{q^\delta-1} \right\rfloor \cdots \right\rfloor \right\rfloor.$$

It is easy to note that by ignoring the floors this bound is the same as the one in Theorem 2.3.8.

We now discuss another kind of bound, the *sphere–covering bound*. This is a lower bound on the cardinality of codes and it is the analog of the one from classical coding theory. As for the sphere–packing bound, it is obtained from the structure of balls. For a code $\mathcal{C} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$ of minimum distance $d(\mathcal{C})$, the bound is computed by looking at the minimum number of balls of given radius $d(\mathcal{C})-2$ that cover the Grassmannian $\mathfrak{G}_{\mathbb{F}_q}(k,n)$. It follows that this bound ensures the existence of a network code with that cardinality for a given distance. It has to be mentioned that the existence of such a code does not usually imply the possibility to express a code in an algebraic way, which means that the resulted code could be difficult to decode.

Theorem 2.3.10 ([KK08b, Theorem 9])**.** *There exists a code $\mathcal{C} \subset \mathfrak{G}_{\mathbb{F}_q}(k,n)$ with minimum distance $d(\mathcal{C}) \geq 2\delta$ such that*

$$|\mathcal{C}| \geq \frac{|\mathfrak{G}_{\mathbb{F}_q}(k,n)|}{|B(\mathcal{U}, 2\delta-2)|} > \frac{1}{16\delta} q^{(k-(\delta-1))(n-k-(\delta-1))}.$$

2.4 Constructions and decoders of network codes

In this section we discuss the state–of–the–art in constructions and decoding algorithms for constant dimension codes starting from [KK08b].

In the paper [KK08b], the authors do not just restrict themselves to providing the new mathematical setting introduced in Section 2.2 for random linear network coding, nor in providing bounds for network codes. They also introduce a construction for network codes and a possible decoding algorithm.

2.4.1 Reed–Solomon like codes

Reed–Solomon codes are a well known class of linear codes from classical coding based on the evaluation of polynomials introduced in [RS60]. For notion from classical coding theory we direct the reader to [MS77].

We consider the following definition of Reed-Solomon codes.

Definition 2.4.1. Let q be a power of a prime and $k, n \in \mathbb{N}$ such that $k \leq n < q$. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ be distinct elements. A *Reed–Solomon code* is defined as

$$RS_q(k,n) = \{(f(\alpha_1), \ldots, f(\alpha_n)) \mid f \in \mathbb{F}_q[x],\ \deg(f) < k\} \subset \mathbb{F}_q^n.$$

We review in the following lemma the properties of Reed–Solomon codes.

Lemma 2.4.2. *A Reed–Solomon code, $RS_q(k,n)$, is a $[n, k, n-k+1]$ linear code, meaning that it is a subspace of $\mathbb{F}_q^n$ of dimension k and minimum Hamming distance $n-k+1$. It follows that Reed–Solomon codes achieve the Singleton bound for classical linear codes.*

The Singleton bound can be found in [MS77, Chapter 1.10, Theorem 11] and codes achieving this bound are called *maximum distance separable codes*.

There exist many different minimum distance decoding algorithms for Reed–Solomon codes, but in the last couple of decades they have become even more subject to research since it was discovered a *list decoding algorithm* for them. Minimum distance decoders are undoubtedly able to correct uniquely up to half the minimum Hamming distance of a code, but they can fail as soon as there exists more than one codeword that is the closest to the input vector. List decoders work in a different way. They are more flexible than the minimum distance ones since they allow as output a short list of codewords that are close to the given input vector. Although the notion of list decoding was proposed by Elias in the late 50's in the work [Eli57], before the mid 90's an efficient list decoding algorithm for Reed–Solomon codes was not yet known. The breakthrough in this direction came from the work [Sud97] by Sudan and then improved in [PV05]. A generalization of the

list decoding algorithm to algebraic geometric codes was then approached by [GS99] and [Gur04].

The construction proposed in [KK08b] is also based on the evaluation of polynomials but with the difference that the considered polynomials are linearized.

Definition 2.4.3. Let $\mathbb{F}_q$ be the finite field with q elements and $n, k \in \mathbb{N}$ with $k \leq n$. Given $r \in \mathbb{N}$, the set of linearized polynomials over $\mathbb{F}_{q^n}$ is

$$L_{\mathbb{F}_{q^n}} := \left\{ f \in \mathbb{F}_{q^n}[x] \;\middle|\; f = \sum_{i=0}^{n} f_i x^{q^i} \right\}.$$

We denote by $L^r_{\mathbb{F}_{q^n}}$ the set of linearized polynomials of degree less than q^r.

Linearized polynomials take their name from the following property. Let $f \in L_{\mathbb{F}_{q^n}}$, $\alpha_1, \alpha_2 \in \mathbb{F}_{q^n}$ and $\lambda_1, \lambda_2 \in \mathbb{F}_q$, then

$$f(\lambda_1\alpha_1 + \lambda_2\alpha_2) = \lambda_1 f(\alpha_1) + \lambda_2 f(\alpha_2).$$

From this remark it follows that if $\mathcal{A} \subset \mathbb{F}_{q^n}$ is a $\mathbb{F}_q$–subspace, then $f(\mathcal{A}) \subset \mathbb{F}_{q^n}$ is still a $\mathbb{F}_q$–subspace. In more detail, if $\alpha_1, \dots \alpha_k \in \mathbb{F}_{q^n}$ is a basis of $\mathcal{A}$, then $f(\alpha_1), \dots, f(\alpha_k)$ span $f(\mathcal{A})$. This is why linearized polynomials are suitable for the construction of network codes.

Definition 2.4.4. Let $\mathbb{F}_{q^n}$ be a finite field and $\alpha_1, \dots, \alpha_k \in \mathbb{F}_{q^n}$ be $\mathbb{F}_q$–linearly independent elements and $\mathcal{A} := \langle \alpha_1, \dots, \alpha_k \rangle$. The set $\mathcal{W} := \mathcal{A} \oplus \mathbb{F}_{q^n}$ is a $\mathbb{F}_q$ vector space of dimension $k + n$. Let $r \leq k$. A *Reed–Solomon like* code is

$$RSL^r_{\mathbb{F}_{q^n}} = \left\{ \langle (\alpha_i, f(\alpha_i)) \mid 1 \leq i \leq k \rangle \mid f \in L^r_{\mathbb{F}_{q^n}} \right\} \subset \mathfrak{G}_{\mathbb{F}_q}(k, k+n).$$

The code $RSL^r_{\mathbb{F}_{q^n}}$ is a code of type $[k+n, k, nr, 2(k-r+1)]$.

Reed–Solomon codes are nearly achieving the Singleton bound, since

$$q^{nr} = |RSL^r_{\mathbb{F}_{q^n}}| =\leq \begin{bmatrix} n+r \\ r \end{bmatrix}_q < 4q^{nr}.$$

We give here a sketch of the decoding algorithm presented in [KK08b] which is closely related to the one of Reed-Solomon codes presented in [Sud97]. Suppose $\mathcal{U} \in RSL^r_{\mathbb{F}_{q^n}}$ is sent and $\mathcal{R} \in \mathcal{P}(\mathbb{F}_q^n)$ with dimension $l = k - s + t$ where s is the number of erasures and t the number of errors that occurs during the communication. Let (x_i, y_i) for $i \in \{1, \dots, l\}$ be a basis of $\mathcal{R}$. The decoding algorithm consists of interpolating a bivariate interpolation polynomial $Q(x, y) = Q_x(x) + Q_y(y)$ such that $Q(x_i, y_i) = 0$ for any $i \in \{1, \dots, l\}$ where $Q_x(x)$ is a linearized polynomial of degree at most q^{d-1} and $Q_y(y)$ a linearized polynomial of degree at most q^{d-r} for $d = \left\lceil \frac{l+r}{2} \right\rceil$. The parameter d is chosen in a way that the univariate linearized polynomial

$Q(x, f(x))$ is identically zero since the number of its zeros, which contains a subspace $\mathcal{V}$ of dimension $k - s$ and such that $\mathcal{V} \subset \mathcal{U} \cap \mathcal{R}$, is greater than the degree of the polynomial. Since $Q(x, f(x)) = Q_y(y - f(x)) + Q(x, f(x))$ but $Q(x, f(x)) = 0$, $f(x)$ can be extracted from $Q_y(y - f(x))$.

A preliminary approach for list decoding Reed–Solomon like codes is presented in [MV10] and follows the approach of [PV05]. Moreover, these codes are strictly related to rank–metric codes which were introduced in [Gab85], in the sense that they can be interpreted as a "lifted" version of Gabidulin codes. These codes live in the metric space of $k \times n$ matrices with a distance, called rank distance, that consists in the rank of the difference of two matrices. A Gabidulin code is a set of matrices maximal with respect to a given minimum rank distance. It is easy to prove that the metric space of $k \times n$ matrices with the rank distance and the space of "lifted" rank metric codes with the subspace distance are isometric. This statement implies the possibility to adapt decoding algorithms for Gabidulin codes to Reed-Solomon like codes. Results on this argument are contained in [SKK08].

2.4.2 Construction based on Ferrer diagrams

The construction, which is the subject of this subsection, appears in [ES09]. For the theory about Ferrer diagrams we refer the reader to [vLW01, Chapter 5]. In words, given $n \in \mathbb{N}$, Ferrer diagrams are a graphical representation of partitions of n, which corresponds to the ways a number n can be expressed as a sum of natural numbers.

Let $k, n \in \mathbb{N}$ with $k < n$ and $C \in \mathbb{F}_2^n$ a binary constant weight k code with minimum Hamming distance 2δ. To every codeword of $c \in C$ there corresponds a constant dimension code $\mathcal{C}_c \subset \mathfrak{G}_{\mathbb{F}_q}(k, n)$. The code $\mathcal{C}_c$ consists of the row space of matrices in row reduced form. The position of the nonzero entries of c correspond to the pivots of the $k \times n$ matrices in row reduced echelon form. The rest of the entries of the matrices, the ones that are not forced to be either 0 or 1 and which correspond to a Ferrer diagram, are then filled with rank metric codes with minimum rank distance δ. The constant dimension code $\mathcal{C}$ defined by the binary constant weight code C is then

$$\mathcal{C} = \bigcup_{c \in C} \mathcal{C}_c.$$

The constant dimension code $\mathcal{C}$ is of type $[n, k, M, 2\delta]$.

Reed-Solomon like codes are actually a subclass of these codes. Spread codes, constant dimension codes that will be explained later, are also codes that can be constructed in this way. In [Ska10] the author presents a generalization of Reed–Solomon like codes which also consists of a subclass of codes explained in this subsection.

A minimum distance decoding algorithm for these codes is clearly a combination of a minimum distance decoder for constant weight binary codes and a minimum distance decoder for rank distance codes.

2.4.3 Construction of q-analog of designs

Another family of constant dimension codes appears in [KK08a]. The authors considered the so called t–(n, k, λ) *design over* $\mathbb{F}_q$, or also q*-analog of a* t–(n, k, λ) *design*, which is a subset $\mathcal{C} \subset \mathfrak{G}_{\mathbb{F}_q}(k, n)$ such that each subspace of dimension t of $\mathbb{F}_q^n$ is contained in exactly λ elements of $\mathcal{C}$.

In the case of Steiner systems, i.e., designs for which $\lambda = 1$, one obtains a constant dimension code of minimum distance $2(k-t+1)$. In [KK08a] the authors give a general method using a prescribed group $\mathfrak{G}$ of automorphisms of a constant dimension code $C \in \mathfrak{G}_{\mathbb{F}_q}(k, n)$ to show the equivalence between the existence of such a code and a solution of a Diophantine system of inequalities.

In the same paper the authors were able to find, by computer search, constant dimension codes which beat in cardinality the ones introduced in the previous subsections. Further studies on these codes are the subject of [EKW10].

Chapter 3

Spread codes

3.1 Definition and first properties

Definition 3.1.1 ([Hir98, Section 4.1]). A subset $\mathcal{S} \subset \mathfrak{G}_{\mathbb{F}_q}(k,n)$ is a spread if it satisfies

- $\mathcal{U} \cap \mathcal{V} = \{0\}$ for all $\mathcal{U}, \mathcal{V} \in \mathcal{S}$ distinct, and
- $\mathbb{F}_q^n = \bigcup_{\mathcal{U}\in\mathcal{S}} \mathcal{U}$.

Theorem 3.1.2 ([Hir98, Theorem 4.1])**.** *A spread exists if and only if $k \mid n$.*

We give now a construction of spreads suitable for use in Random Linear Network Coding (RLNC) based on companion matrices.

Definition 3.1.3. Let $\mathbb{F}_q$ be a finite field and $p = \sum_{i=1}^{k} p_i x^i \in \mathbb{F}_q[x]$ a monic polynomial. We define the companion matrix of p to be the matrix

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & & 1 \\ -p_0 & -p_1 & -p_2 & \cdots & -p_{k-1} \end{pmatrix} \in \mathbb{F}_q^{k\times k}.$$

Let $n = rk$ with $r > 1$, $p \in \mathbb{F}_q[x]$ a monic irreducible polynomial of degree k and $P \in \mathbb{F}_q^{k\times k}$ its companion matrix.

Lemma 3.1.4. *The $\mathbb{F}_q$-algebra $\mathbb{F}_q[P]$ is a finite field, i.e., $\mathbb{F}_q[P] \cong \mathbb{F}_{q^k}$.*

This lemma follows from the definition of order of a polynomial and the following lemma.

Definition 3.1.5. Let $p \in \mathbb{F}_q[x]$ be a nonzero polynomial. If $p(0) \neq 0$, then the least $e \in \mathbb{N}$ for which p divides $x^e - 1$ is called the *order* of p and denoted $\mathrm{ord}(p)$. If $p(0) = 0$, then $p = x^h g$ such that $g(0) \neq 0$ and $\mathrm{ord}(p)$ is defined to be $\mathrm{ord}(g)$.

Lemma 3.1.6 ([LN94, Lemma 6.26]). *Let $p = \sum_{i=0}^{k} p_i x^i \in \mathbb{F}_q[x]$ be a monic polynomial with $k > 0$ and $p(0) \neq 0$ and M_p be its companion matrix. Then* $\mathrm{ord}(p)$ *is equal to the order of M_p in $GL_k(\mathbb{F}_q)$.*

Lemma 3.1.7. *Let $\varphi : \mathbb{F}_{q^k} \to \mathbb{F}_q[P]$ be a ring isomorphism. Denote by $\mathbb{P}^{r-1}(\mathbb{F}_{q^k}) := (\mathbb{F}_{q^k}^r \setminus \{0\})/\sim$ the projective space, where $\sim$ is the following equivalence relation*

$$v \sim w \iff \exists \lambda \in \mathbb{F}_{q^k}^* \text{ such that } v = \lambda w,$$

where $v, w \in \mathbb{F}_{q^k}^r \setminus \{0\}$. Then, the map

$$\begin{array}{rccc} \tilde{\varphi}: & \mathbb{P}^{r-1}(\mathbb{F}_{q^k}) & \to & \mathfrak{G}_{\mathbb{F}_q}(k,n) \\ & [v_1 : \cdots : v_r] & \mapsto & \mathrm{rowsp}\begin{pmatrix} \varphi(v_1) & \cdots & \varphi(v_r) \end{pmatrix}. \end{array}$$

is injective.

Proof. Let $v = [v_1 : \cdots : v_r], w = [w_1 : \cdots : w_r] \in \mathbb{P}^{r-1}(\mathbb{F}_{q^k})$. If $\tilde{\varphi}(v) = \tilde{\varphi}(w)$ there exists an $M \in GL_k(\mathbb{F}_q)$ such that

$$\begin{aligned} \begin{pmatrix} \varphi(v_1) & \cdots & \varphi(v_r) \end{pmatrix} &= M \begin{pmatrix} \varphi(w_1) & \cdots & \varphi(w_r) \end{pmatrix} \\ &= \begin{pmatrix} M\varphi(w_1) & \cdots & M\varphi(w_r) \end{pmatrix} \end{aligned} \tag{3.1}$$

Let $i_v, i_w \in \{1, \ldots, r\}$ be the least indices such that $\varphi(v_{i_v}) \neq 0$ and $\varphi(w_{i_w}) \neq 0$. From (3.1) it follows that $i_v = i_w$. Since, without loss of generality, we can consider $v_{i_v} = w_{i_w} = 1$, it follows that $\varphi(v_{i_v}) = \varphi(w_{i_w}) = I$ and consequently $M = I$. Then, (3.1) becomes

$$\begin{pmatrix} \varphi(v_1) & \cdots & \varphi(v_r) \end{pmatrix} = \begin{pmatrix} \varphi(w_1) & \cdots & \varphi(w_r) \end{pmatrix}$$

leading to $v = w$. □

Theorem 3.1.8 ([MGR08, Theorem 1]). *$\mathcal{S} := \tilde{\varphi}(\mathbb{P}^{r-1}(\mathbb{F}_{q^k}))$ is a spread of $\mathfrak{G}_{\mathbb{F}_q}(k,n)$.*

Proof. The cardinality of $\mathcal{S}$ corresponds to the cardinality of $\mathbb{P}^{r-1}(\mathbb{F}_{q^k})$ that is exactly the maximum number of k-dimensional trivially intersecting subspaces of $\mathbb{F}_q^n$, i.e.

$$\frac{q^n - 1}{q^k - 1} = q^{k(r-1)} + q^{k(r-2)} + \cdots + q^k + 1. \tag{3.2}$$

It remains to be shown that any pair of subspaces in $\mathcal{S}$ only intersect trivially. Equivalently we show that for any $v = [v_1 : \cdots : v_r], w = [w_1 : \cdots : w_r] \in \mathbb{P}^{r-1}(\mathbb{F}_{q^k})$ distinct, the $2k \times n$ matrix

$$\begin{pmatrix} \varphi(v_1) & \cdots & \varphi(v_r) \\ \varphi(w_1) & \cdots & \varphi(w_r) \end{pmatrix} \in \mathbb{F}_q^{2k \times rk} \tag{3.3}$$

has full rank.

Let $i_v, i_w \in \{1, \dots, r\}$ be the least indices such that v_{i_v} and v_{i_w} are nonzero. Without loss of generality $v_{i_v} = v_{i_w} = 1$. If $i_v \neq i_w$, then the submatrix

$$\begin{pmatrix} \varphi(v_{i_v}) & \varphi(v_{i_w}) \\ \varphi(w_{i_v}) & \varphi(w_{i_w}) \end{pmatrix} = \begin{pmatrix} I & \varphi(v_{i_w}) \\ \varphi(w_{i_v}) & I \end{pmatrix}$$

has full rank since either $\varphi(v_{i_w})$ or $\varphi(w_{i_v})$ are nonzero. If $i_v = i_w$, then since $v \neq w$, there exists an index $j \in \{i_v + 1, \dots, r\}$ such that $v_j \neq w_j$ and consequently $\varphi(v_j) \neq \varphi(w_j)$. It follows that a submatrix which has full rank is

$$\begin{pmatrix} \varphi(v_{i_v}) & \varphi(v_j) \\ \varphi(w_{i_v}) & \varphi(w_j) \end{pmatrix} = \begin{pmatrix} I & \varphi(v_j) \\ I & \varphi(w_j) \end{pmatrix}.$$

Both cases imply that the matrix in (3.3) has full rank. □

Definition 3.1.9 ([MGR08, Definition 2]). We call *spread codes* of $\mathfrak{G}_{\mathbb{F}_q}(k, n)$ the subsets $\mathcal{S} \subset \mathfrak{G}_{\mathbb{F}_q}(k, n)$ from Theorem 3.1.8.

In order to simplify the notations we consider the following equivalent definition of spread codes.

Definition 3.1.10. Let $n, k \in \mathbb{N}$ with $k > 0$ and $n = rk$ for some $r \in \mathbb{N}$, $r > 1$. Let $p \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree $k > 0$ and $P \in GL_k(\mathbb{F}_q)$ its companion matrix. Then

$$\mathcal{S} = \left\{ \text{rowsp}\begin{pmatrix} A_1 & \cdots & A_r \end{pmatrix} \in \mathfrak{G}_{\mathbb{F}_q}(k, n) \mid A_i \in \mathbb{F}_q[P] \ \forall i \in \{1, \dots, r\} \right\}$$

is a spread code of $\mathfrak{G}_{\mathbb{F}_q}(k, n)$. Without loss of generality and in order to have a unique representation matrix of the elements of a spread code, we consider the matrices $\begin{pmatrix} A_1 & \cdots & A_r \end{pmatrix}$ to be in row reduced echelon form.

Lemma 3.1.11 ([MGR08])**.** *Let $\mathcal{S} \subset \mathfrak{G}_{\mathbb{F}_q}(k, n)$ be a spread code. Then*

1. *$d(\mathcal{U}, \mathcal{V}) = d_{\min}(\mathcal{S}) = 2k$, for all $\mathcal{U}, \mathcal{V} \in \mathcal{S}$ distinct, i.e., the code has maximal minimum distance, and*

2. *$|\mathcal{S}| = \frac{q^n - 1}{q^k - 1}$, i.e., the code has maximal cardinality with respect to the given minimum distance.*

Proof. Both statements are a consequence of the definition of a spread. Indeed, given $\mathcal{U}, \mathcal{V} \in \mathcal{S}$, since $\mathcal{U} \cap \mathcal{V} = \{0\}$ then

$$d(\mathcal{U}, \mathcal{V}) = \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2\dim(\mathcal{U} \cap \mathcal{V}) = 2k.$$

The cardinality is a consequence of (3.2). □

3.1.1 Relation with Reed–Solomon like codes

Reed-Solomon-like codes are a class of constant–dimension, i.e. codes on $\mathfrak{G}_{\mathbb{F}_q}(k,n)$, introduced in [KK08b]. These codes are strictly related to maximal rank distance codes as introduced in [Gab85]. We give here an equivalent definition of these codes.

Definition 3.1.12. Let $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ be two finite fields. Fix some $\mathbb{F}_q$–linearly independent elements $\alpha_1, \dots, \alpha_k \in \mathbb{F}_{q^n}$. Let $r \in \mathbb{N}$ with $r < k$ and denote with $L^r_{\mathbb{F}_{q^n}} \subset \mathbb{F}_{q^n}[x]$ the set of linearized polynomials of degree less than q^r, i.e., $f \in L^r_{\mathbb{F}_{q^n}}$ if and only if $f = \sum_{i=0}^{r-1} f_i x^{q^i}$ for some $f_i \in \mathbb{F}_{q^n}$. Let $\psi : \mathbb{F}_{q^n} \to \mathbb{F}_q^n$ be an isomorphism of $\mathbb{F}_q$ vector spaces. Then a *Reed-Solomon-like (RSL) code* is defined as

$$RSL^r_{\mathbb{F}_{q^n}} := \left\{ \text{rowsp} \begin{pmatrix} & \psi(f(\alpha_1)) \\ I & \vdots \\ & \psi(f(\alpha_k)) \end{pmatrix} \;\middle|\; f \in L^r_{\mathbb{F}_{q^n}} \right\} \subseteq \mathfrak{G}_{\mathbb{F}_q}(k, k+n).$$

The following proposition establishes a relation between spread codes and RSL codes.

Proposition 3.1.13. *Let $n = rk$, $\mathbb{F}_q \subset \mathbb{F}_{q^k} \subset \mathbb{F}_{q^n}$ finite fields, and $P \in GL_k(\mathbb{F}_q)$ the companion matrix of a monic irreducible polynomial $p \in \mathbb{F}_q[x]$ of degree $k > 0$. Let $\lambda \in \mathbb{F}_{q^k}$ be a root of p, $\mu_1, \dots, \mu_r \in \mathbb{F}_{q^n}$ a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_{q^k}$. Moreover, let $\psi : \mathbb{F}_{q^n} \to \mathbb{F}_q^n$ be the isomorphism of $\mathbb{F}_q$–vector spaces which maps the basis $(\lambda^i \mu_j)_{\substack{0 \le j \le k-1 \\ 1 \le i \le r}}$ to the standard basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then for every choice of $A_0, \dots, A_{r-1} \in \mathbb{F}_q[P]$ there exists a unique linearized polynomial of the form $f = ax$ with $a \in \mathbb{F}_{q^n}$ such that*

$$(A_0 \ \cdots \ A_{r-1}) = \begin{pmatrix} \psi(f(1)) \\ \psi(f(\lambda)) \\ \vdots \\ \psi(f(\lambda^{k-1})) \end{pmatrix}.$$

The constant a is of the form $a = \psi^{-1}(v)$ where $v \in \mathbb{F}_q^n$ is the first row of $(A_0 \ \cdots \ A_{r-1})$.

Proof. We first prove the proposition for $r = 1$. Let $\lambda \in \mathbb{F}_{q^k}$ such that $p(\lambda) = 0$. Let ψ be of the form

$$\begin{aligned} \psi : \mathbb{F}_q[\lambda] &\to \mathbb{F}_q^k \\ v &\mapsto (v_0, \dots, v_{k-1}) \end{aligned} \tag{3.4}$$

where $v = \sum_{i=0}^{k-1} v_i \lambda^i$.

Let $A = \left(a_{i,j}\right)_{1\leq i,j\leq k} \in \mathbb{F}_q[P]$. Since

$$P = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & & 1 \\ -p_0 & -p_1 & -p_2 & \cdots & -p_{k-1} \end{pmatrix}$$

we obtain that $PA = (\bar{a}_{i,j})_{1\leq i,j\leq k}$ where

$$\begin{aligned} \bar{a}_{i,j} &= a_{i+1,j} \text{ for } i \in \{1,\ldots,k-1\}, \text{ and} \\ \bar{a}_{k,j} &= -\sum_{i=1}^{k} a_{i,j}p_{i-1}. \end{aligned} \tag{3.5}$$

We now prove by induction that for every $l \in \mathbb{N}$ the relation

$$P^l = \begin{pmatrix} \psi(\lambda^l) \\ \vdots \\ \psi(\lambda^{l+k-1}) \end{pmatrix} \tag{3.6}$$

holds. For $l = 0$, we have that

$$I = \begin{pmatrix} \psi(1) \\ \vdots \\ \psi(\lambda^{k-1}) \end{pmatrix}.$$

Consider the thesis true for $P^{l-1} = \left(a_{i,j}\right)_{1\leq i,j\leq k}$. By (3.5) we obtain that

$$P^l = PP^{l-1} = \begin{pmatrix} \psi(\lambda^l) \\ \vdots \\ \psi(\lambda^{l+k-2}) \\ \psi(v) \end{pmatrix},$$

where $\psi(v) = (-\sum_{i=1}^{k} a_{i,1}p_{i-1}, \cdots, -\sum_{i=1}^{k} a_{i,k}p_{i-1})$. By the definition of ψ, it follows that

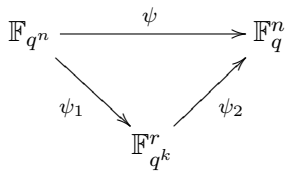
$$\begin{aligned} v &= \sum_{j=1}^{k} \left(-\sum_{i=1}^{k} a_{i,j}p_{i-1} \right) \lambda^{j-1} = -\sum_{i=1}^{k} p_{i-1} \left(\sum_{j=1}^{k} a_{i,j}\lambda^{j-1} \right) \\ &= -\sum_{i=1}^{k} p_{i-1}\lambda^{l+i-2} = \lambda^{l-1} \left(-\sum_{i=1}^{k} p_{i-1}\lambda^{i-1} \right) = \lambda^{l+k-1}. \end{aligned}$$

We are now ready to prove the theorem for $r = 1$ using (3.6). Let $A \in \mathbb{F}_q[P]$, then there exists a polynomial $g = \sum_{i=0}^{k-1} g_i x^i \in \mathbb{F}_q[x]$ such that $g(P) = A$, then

$$\begin{aligned} A = g(P) = \sum_{i=0}^{k-1} g_i P^i &= \sum_{i=0}^{k-1} g_i \begin{pmatrix} \psi(\lambda^i) \\ \vdots \\ \psi(\lambda^{i+k-1}) \end{pmatrix} \\ &= \begin{pmatrix} \sum_{i=0}^{k-1} g_i \psi(\lambda^i) \\ \vdots \\ \sum_{i=0}^{k-1} g_i \psi(\lambda^{i+k-1}) \end{pmatrix} = \begin{pmatrix} \psi(\sum_{i=0}^{k-1} g_i \lambda^i) \\ \vdots \\ \psi(\sum_{i=0}^{k-1} g_i \lambda^{i+k-1}) \end{pmatrix} \\ &= \begin{pmatrix} \psi(\sum_{i=0}^{k-1} g_i \lambda^i) \\ \vdots \\ \psi((\sum_{i=0}^{k-1} g_i \lambda^i)\lambda^{k-1}) \end{pmatrix} = \begin{pmatrix} \psi(f(1)) \\ \vdots \\ \psi(f(\lambda^{k-1})) \end{pmatrix} \end{aligned}$$

where $f = ax$ and $a = \sum_{i=0}^{k-1} g_i \lambda^i$. We deduce that the entries of the first row of A correspond to the coefficients of g.

Let $n = rk$ with $r > 1$. For simplicity, denote the map in (3.4) by $\tilde{\psi}$. The map ψ defined in the theorem satisfies the following diagram



where the maps ψ_1, ψ_2 are defined as follows:

- $\psi_1(v) = (v_1, \ldots, v_r)$ where $v = \sum_{i=1}^{r} v_i \mu_i$, and
- $\psi_2((v_1, \ldots, v_r)) = (\tilde{\psi}(v_1), \ldots, \tilde{\psi}(v_r))$.

For any $i \in \{1, \ldots, r\}$, since $A_i \in \mathbb{F}_q[P]$, there exists an $a_i \in \mathbb{F}_{q^k}$ such that

$$A_i = \begin{pmatrix} \tilde{\psi}(a_i) \\ \vdots \\ \tilde{\psi}(a_i \lambda^{k-1}) \end{pmatrix}.$$

Let $a \in \mathbb{F}_{q^n}$ be such that $\psi(a)$ corresponds to the first row of the matrix $\begin{pmatrix} A_1 & \cdots & A_r \end{pmatrix}$. By the $\mathbb{F}_{q^k}$ linearity of ψ_1 we obtain that

$$\begin{pmatrix} \psi(a) \\ \vdots \\ \psi(a\lambda^{k-1}) \end{pmatrix} = \begin{pmatrix} \psi_2(\psi_1(a)) \\ \vdots \\ \psi_2(\psi_1(a\lambda^{k-1})) \end{pmatrix} = \begin{pmatrix} \psi_2(a_1, \ldots, a_r) \\ \vdots \\ \psi_2(a_1\lambda^{k-1}, \ldots, a_1\lambda^{k-1}) \end{pmatrix}$$
$$= \begin{pmatrix} \tilde{\psi}(a_1) & \cdots & \tilde{\psi}(a_r) \\ \vdots & & \vdots \\ \tilde{\psi}(a_1\lambda^{k-1}) & \cdots & \tilde{\psi}(a_r\lambda^{k-1}) \end{pmatrix} = \begin{pmatrix} A_1 & \cdots & A_r \end{pmatrix}.$$

□

The following corollary shows the explicit relation between spread codes and RSL codes.

Corollary 3.1.14. *Let $\psi_i : \mathbb{F}_{q^{(r-i)k}} \to \mathbb{F}_q^{(r-i)k}$ be isomorphisms of vector spaces that map the basis $(\lambda^j \mu_l)_{\substack{0 \le j \le k-1 \\ 1 \le l \le r-i}}$ to the standard basis of $\mathbb{F}_q^{(r-i)k}$, $\mu_1, \ldots, \mu_{r-i}$ a basis of $\mathbb{F}_{q^{(r-i)k}}$ over $\mathbb{F}_{q^k}$. Then,*

$$\mathcal{S} = \bigcup_{i=1}^{r} \left\{ \operatorname{rowsp} \begin{pmatrix} \underbrace{0 \cdots 0}_{i-1 \text{ times}} & I & \psi_i(f(1)) \\ & & \vdots \\ & & \psi_i(f(\lambda^{k-1})) \end{pmatrix} \;\middle|\; f = ax,\ a \in \mathbb{F}_{q^{(r-i)k}} \right\}$$

Lemma 3.1.15. *Let $\mathcal{S}$ be a spread code, and $\mathcal{R} = \operatorname{rowsp}\begin{pmatrix} R_1 & \cdots & R_r \end{pmatrix} \in \mathfrak{G}_{\mathbb{F}_q}(k, rk)$. Assume there exists a $\mathcal{C} = \operatorname{rowsp}\begin{pmatrix} C_1 & \cdots & C_r \end{pmatrix} \in \mathcal{S}$ such that $d(\mathcal{R}, \mathcal{C}) < \frac{d(\mathcal{S})}{2} = k$. Let $i := \min\{j \in \{1, \ldots, r\} \mid \operatorname{rank}(R_j) > \frac{k-1}{2}\}$. It holds that*

- *$C_j = 0$ for $1 \le j < i$,*
- *$C_i = I$, and*
- *$d(\operatorname{rowsp}\begin{pmatrix} R_i & R_{i+1} & \cdots & R_r \end{pmatrix}, \operatorname{rowsp}\begin{pmatrix} I & C_{i+1} & \cdots & C_r \end{pmatrix}) < k$.*

Lemma 3.1.15 follows from Lemma 3.2.1, which we prove in the next section. This lemma allows us to decode spread codes using a decoding algorithm for RSL codes. Examples of decoding algorithms for RSL codes can be found in [Gab85], [KK08b], [SKK08].

3.2 Decoding Algorithm

Throughout this section let $\mathbb{F}_q$ be a finite field, $p \in \mathbb{F}_q[x]$ a monic irreducible polynomial of degree $k > 0$ and $P \in GL_k(\mathbb{F}_q)$ its companion matrix. Let $S \in GL_k(\mathbb{F}_{q^k})$ be a matrix diagonalizing P, i.e., $S^{-1}PS = \operatorname{diag}(\lambda, \lambda^q, \ldots, \lambda^{q^{k-1}})$ with $\lambda \in \mathbb{F}_{q^k}$ a root of p.

In this section we provide a minimum distance decoding algorithm for spread codes. The following lemma shows how to reduce the minimum distance decoding algorithm in the general case, i.e., $n = rk$, to at most $r - 1$ instances of the same procedure for $n = 2k$ that can be individually run in parallel.

Lemma 3.2.1. *Let $\mathcal{S}$ be a spread code, and $\mathcal{R} = \mathrm{rowsp}\begin{pmatrix} R_1 & \cdots & R_r \end{pmatrix} \in \mathfrak{G}_{\mathbb{F}_q}(k, rk)$. Assume there exists a $\mathcal{C} = \mathrm{rowsp}\begin{pmatrix} C_1 & \cdots & C_r \end{pmatrix} \in \mathcal{S}$ such that $d(\mathcal{R}, \mathcal{C}) < k$. It holds*

$$C_i = 0 \iff \mathrm{rank}(R_i) \leq \frac{k-1}{2}.$$

Proof. $\boxed{\Rightarrow}$ Let $i \in \{1, \ldots, r\}$ be an index such that $C_i = 0$. By the construction of a spread code there exists a $j \in \{1, \ldots, r\}$ with $C_j = I$. It follows that

$$\mathrm{rank}\begin{pmatrix} 0 & I \\ R_i & R_j \end{pmatrix} \leq \mathrm{rank}\begin{pmatrix} C_1 & \cdots & C_r \\ R_1 & \cdots & R_r \end{pmatrix} < \frac{3k}{2} \quad \Rightarrow \quad \mathrm{rank}(R_i) < \frac{k}{2}.$$

$\boxed{\Leftarrow}$ Let $i \in \{1, \ldots, r\}$ be such that $\mathrm{rank}(R_i) \leq \frac{k-1}{2}$ and assume by contradiction that $C_i \in \mathbb{F}_q[P]^*$. It follows that

$$\dim(\mathcal{C} \cap \mathcal{R}) = \dim(\mathrm{rowsp}(C_i) \cap \mathrm{rowsp}(R_i)) = \dim(\mathrm{rowsp}(R_i)) \leq \frac{k-1}{2}$$

which contradicts the assumption that $d(\mathcal{C}, \mathcal{R}) = 2k - 2\dim(\mathcal{C} \cap \mathcal{R}) < k$. □

Algorithm 3 on page 53 is based on this lemma.

Lemma 3.1.15 now follows from Lemma 3.2.1 and from the observation that $d(\mathcal{C}, \mathcal{R}) \geq d(\mathrm{rowsp}\begin{pmatrix} C_i & \cdots & C_r \end{pmatrix}, \mathrm{rowsp}\begin{pmatrix} R_i & \cdots & R_r \end{pmatrix})$.

We can now focus on specifying a minimum distance decoding algorithm for the case where $n = 2k$, i.e.,

$$\mathcal{S} = \left\{\mathrm{rowsp}\begin{pmatrix} I & A \end{pmatrix} \mid A \in \mathbb{F}_q[P]\right\} \cup \left\{\mathrm{rowsp}\begin{pmatrix} 0 & I \end{pmatrix}\right\}$$

where I and 0 are respectively the identity and the zero matrix of size $k \times k$.

Since a minimum-distance decoding algorithm decodes uniquely up to half the minimum distance, we are interested in writing an algorithm with the following specifications.

input: $\mathcal{R} = \mathrm{rowsp}\begin{pmatrix} R_1 & R_2 \end{pmatrix} \in \mathfrak{G}_{\mathbb{F}_q}(k, 2k)$,
$P \in GL_k(\mathbb{F}_q)$ the companion matrix of $p \in \mathbb{F}_q[x]$ and
$S \in GL_k(\mathbb{F}_{q^k})$ its diagonalizing matrix.

output: $\mathcal{C} \in \mathcal{S} \subset \mathfrak{G}_{\mathbb{F}_q}(k, 2k)$ such that $d(\mathcal{R}, \mathcal{C}) < \frac{d(\mathcal{S})}{2} = k$, if such a $\mathcal{C}$ exists.

We now first give a membership criterion for spread codes.

Lemma 3.2.2 ([MGR08, Lemma 5 and Corollary 6])**.** *Let $A \in GL_k(\mathbb{F}_q) \cup \{0\}$. Then the following statements are equivalent.*

1. $A \in \mathbb{F}_q[P]$.
2. $S^{-1}AS$ *is a diagonal matrix.*
3. $AP = PA$.

More specifically, $S^{-1}AS = \mathrm{diag}(\lambda_A, \lambda_A^q, \ldots, \lambda_A^{q^{k-1}})$ *for some* $\lambda_A \in \mathbb{F}_{q^k}$.

Proof. $\boxed{1. \Rightarrow 2.}$ If $A \in \mathbb{F}_q[P]$ then there exists a $g \in \mathbb{F}_q[x]$ such that $A = g(P)$. Since $S^{-1}PS$ is a diagonal matrix, it follows that

$$S^{-1}AS = S^{-1}g(P)S = g(S^{-1}PS)$$

which is a diagonal matrix.

$\boxed{2. \Rightarrow 3.}$ If $S^{-1}AS$ is a diagonal matrix then

$$(S^{-1}AS)(S^{-1}PS) = (S^{-1}PS)(S^{-1}AS)$$

implying that $AP = PA$.

$\boxed{3. \Rightarrow 1.}$ Assume $AP = PA$ and denote $\Delta = S^{-1}PS$. Since the eigenvalues of P are distinct and $\Delta(S^{-1}AS) = (S^{-1}AS)\Delta$ it follows that $S^{-1}AS$ is a diagonal matrix as well with diagonal entries in $\mathbb{F}_{q^k}$. Let $\{1, \lambda, \ldots, \lambda^{k-1}\}$ be a basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. One has an expansion:

$$S^{-1}AS = \sum_{i=0}^{k-1} c_i \Delta^i = \sum_{i=0}^{k-1} \sum_{j=0}^{k-1} c_{i,j} \lambda^j \Delta^i$$

with $c_i \in \mathbb{F}_{q^k}$, $c_{i,j} \in \mathbb{F}_q$ and where the existence of the coefficients c_i's corresponds to the existence of a solution of a linear system of k equations in k indeterminates.

Equivalently we have:

$$A = \sum_{j=0}^{k-1} \left(\sum_{i=0}^{k-1} c_{i,j} P^i \right) \lambda^j.$$

It follows that $A = \sum_{i=0}^{k-1} c_{i,0} P^i$ and $A \in \mathbb{F}_q[P]$.

By the characterization of roots of an irreducible polynomial [LN94, Theorem 2.4], if $\lambda \in \mathbb{F}_q[x]$ is such that $p(\lambda) = 0$, than $p = \prod_{i=0}^{k-1}(x - \lambda^{q^i})$.

It follows that $S^{-1}PS = \mathrm{diag}(\lambda, \cdots, \lambda^{q^{k-1}})$. Let $g \in \mathbb{F}_q[x]$ be a polynomial such that $A = g(P)$, then

$$\begin{aligned} S^{-1}AS = S^{-1}g(P)S = g(S^{-1}PS) = g(\mathrm{diag}(\lambda, \cdots, \lambda^{q^{k-1}})) \\ = \mathrm{diag}(g(\lambda), \cdots, g(\lambda^{q^{k-1}})) = \mathrm{diag}(g(\lambda), \cdots, g(\lambda)^{q^{k-1}}). \end{aligned}$$

□

Corollary 3.2.3 (Membership Criterion)**.** *Let* $\mathcal{R} = \mathrm{rowsp}\begin{pmatrix} R_1 & R_2 \end{pmatrix} \in \mathfrak{G}_{\mathbb{F}_q}(k, 2k)$*. Then* $\mathcal{R} \in \mathcal{S}$ *if and only if either* $R_1 \in GL_k(\mathbb{F}_q)$ *and* $S^{-1}R_1^{-1}R_2S$ *is diagonal or* $R_1 = 0$ *and* $R_2 \in GL_k(\mathbb{F}_q)$*.*

Proof. $\boxed{\Rightarrow}$ This implication is a direct consequence of the definition of a spread code and Lemma 3.2.2.

$\boxed{\Leftarrow}$ If $R_1 = 0$ and $R_2 \in GL_k(\mathbb{F}_q)$, it follows that $\mathrm{rowsp}\begin{pmatrix} R_1 & R_2 \end{pmatrix} = \mathrm{rowsp}\begin{pmatrix} 0 & I \end{pmatrix} \in \mathcal{S}$. If instead $R_1 \in GL_k(\mathbb{F}_q)$, then

$$\mathrm{rowsp}\begin{pmatrix} R_1 & R_2 \end{pmatrix} = \mathrm{rowsp}\begin{pmatrix} I & R_1^{-1}R_2 \end{pmatrix} \in \mathcal{S}$$

since by Lemma 3.2.2 $R_1^{-1}R_2 \in \mathbb{F}_q[P]$ if and only if $S^{-1}R_1^{-1}R_2S$ is a diagonal matrix.

□

Definition 3.2.4. We say that a vector space $\mathcal{R} \in \mathfrak{G}_{\mathbb{F}_q}(k, 2k)$ is *uniquely decodable* by the spread code $\mathcal{S} \subset \mathfrak{G}_{\mathbb{F}_q}(k, 2k)$ if

$$\text{there exists a } \mathcal{C} \in \mathcal{S} \text{ such that } d(\mathcal{R}, \mathcal{C}) < \frac{d(\mathcal{S})}{2} = k. \tag{3.7}$$

We can state the following corollary of Lemma 3.2.1.

Corollary 3.2.5. *Consider* $\mathcal{R} \in \mathfrak{G}_{\mathbb{F}_q}(k, n)$ *satisfying* (3.7)*. The following are equivalent:*

- $\mathrm{rank}(R_1) \leq \frac{k-1}{2}$*, and*
- *the output of a minimum distance decoder is* $\mathrm{rowsp}\begin{pmatrix} 0 & I \end{pmatrix}$*.*

A similar statement holds for R_2*.*

Therefore we can restrict our decoding algorithm to look for codewords of the form $\mathcal{C} = \mathrm{rowsp}\begin{pmatrix} I & A \end{pmatrix}$ where $A \in \mathbb{F}_q[P]$. Since there is an obvious symmetry in the construction of a spread code we can without loss of generality assume that

$$\mathrm{rank}(R_1) \geq \mathrm{rank}(R_2) > \frac{k-1}{2}.$$

With the following theorem we translate Condition (3.7) into a rank condition, and then into a *greatest common divisor* condition. Let M be a matrix of size $k \times k$ and let $J = (j_1, \ldots, j_s)$, $L = (l_1, \ldots, l_s) \in \{1, \ldots, k\}^s$. We denote by $[J; L]_M$ the minor of the matrix M corresponding to the submatrix $\big(J; L\big)_M$ with row indices $j_1, \ldots, j_s$ and column indices $l_1, \ldots, l_s$. We skip the suffix M when the parent matrix is clear from the context. We are now ready to state the next result.

Theorem 3.2.6. *Let $\mathcal{R} \in \mathfrak{G}_{\mathbb{F}_q}(k, n)$ be a subspace with*

$$\operatorname{rank}(R_1) \geq \operatorname{rank}(R_2) > \frac{k-1}{2}.$$

The following are equivalent:

- *$\mathcal{R}$ satisfies (3.7).*
- *Let $\Delta(x) := \operatorname{diag}(x, x^q, x^{q^2}, \ldots, x^{q^{k-1}})$, then there exists a unique $\mu \in \mathbb{F}_{q^k}$ such that*

$$\operatorname{rank}(S^{-1}R_1S\Delta(\mu) - S^{-1}R_2S) \leq \frac{k-1}{2} \tag{3.8}$$

- *$x - \mu = \gcd\left(\left\{[J; L]_{S^{-1}R_1S\Delta(x) - S^{-1}R_2S} \mid J, L \in \{1, \ldots, k\}^{\lfloor \frac{k+1}{2} \rfloor}\right\}, x^{q^k} - x\right)$, for some $\mu \in \mathbb{F}_{q^k}$.*

Proof. The property that $\mathcal{R}$ satisfies (3.7) is equivalent to the existence of a unique matrix $X \in \mathbb{F}_q[P]$ such that

$$\begin{aligned} k - 1 \geq d(\mathcal{R}, \mathcal{C}) &= 2\operatorname{rank}\begin{pmatrix} I & X \\ R_1 & R_2 \end{pmatrix} - 2k \\ &= 2\operatorname{rank}\begin{pmatrix} I & X \\ 0 & R_1X - R_2 \end{pmatrix} - 2k = 2\operatorname{rank}(R_1X - R_2). \end{aligned}$$

Furthermore we get that $\operatorname{rank}(R_1X - R_2) = \operatorname{rank}(S^{-1}R_1S\Delta(x) - S^{-1}R_2S)$ where $\Delta(x) := S^{-1}XS = \operatorname{diag}(x, x^q, \ldots, x^{q^{k-1}})$ is a consequence of Lemma 3.2.2. The existence of a unique solution $X \in \mathbb{F}_q[P]$ is then equivalent to the existence of a unique $\mu \in \mathbb{F}_{q^k}$ such that

$$\operatorname{rank}(S^{-1}R_1S\Delta(\mu) - S^{-1}R_2S) \leq \frac{k-1}{2}.$$

This is equivalent to the condition that all minors of size $\lfloor \frac{k+1}{2} \rfloor$ of $S^{-1}R_1S\Delta(\mu) - S^{-1}R_2S$ are zero. This leads to a nonempty system of polynomials in the variable x having a unique solution $\mu \in \mathbb{F}_{q^k}$. Therefore

$$x - \mu \mid \gcd\left(\left\{[J; L]_{S^{-1}R_1S\Delta(x) - S^{-1}R_2S} \mid J, L \in \{1, \ldots, k\}^{\lfloor \frac{k+1}{2} \rfloor}\right\}, x^{q^k} - x\right).$$

Equality follows from the uniqueness of μ. □

As a corollary one gets the following decoding algorithm. First compute all $\begin{pmatrix} k \\ \lfloor \frac{k+1}{2} \rfloor \end{pmatrix}^2$ minors of size $\lfloor \frac{k+1}{2} \rfloor$ of $S^{-1}R_1S\Delta(x) - S^{-1}R_2S$, then compute their greatest common divisor with $x^{q^k} - x$. In order to decrease the complexity of this first approach we can focus on the factorization of only one non zero minor.

Remark 3.2.7. Let $J, L \in \{1, \ldots, k\}^{\lfloor \frac{k+1}{2} \rfloor}$ such that $[J; L]_{S^{-1}R_1S\Delta(x)-S^{-1}R_2S} \neq 0$. If $\mu \in \mathbb{F}_{q^k}$ is the unique element satisfying the equivalent conditions of Theorem 3.2.6, then

$$x - \mu \mid \gcd\left([J; L]_{S^{-1}R_1S\Delta(x)-S^{-1}R_2S}, x^{q^k} - x\right).$$

The greatest common divisor $\gcd\left([I; J]_{S^{-1}R_1S\Delta(x)-S^{-1}R_2S}, x^{q^k} - x\right)$ is in general non linear, leading to possible multiple solutions over $\mathbb{F}_{q^k}$. In order to find the unique one satisfying the rank condition we compute

$$\operatorname{rank}(S^{-1}R_1S\Delta(\mu) - S^{-1}R_2S)$$

for all $\mu \in \mathbb{F}_{q^k}$ such that $x - \mu \mid \gcd\left([I; J]_{S^{-1}R_1S\Delta(x)-S^{-1}R_2S}, x^{q^k} - x\right)$.

We still can do more in order to reduce the complexity of the algorithm. In the sequel we will:

- eliminate the computation of the *greatest common divisor*, and
- polynomially bound the number of checks we have to perform.

The following subsection is devoted to finding a minor suitable for our purpose.

3.2.1 Existence of a suitable polynomial

We now introduce some operations on tuples that we will use later in this subsection. Let $I = (i_1, \ldots, i_s) \in \{1, \ldots, k\}^s$.

- $i \in I$ means that $i \in \{i_1, \ldots, i_s\}$.
- $L \subset I$ means that $L = (i_{l_1}, \ldots, i_{l_k})$ for $1 \leq l_1 < \cdots < l_k \leq s$.
- $|I| := s$ is the length of the tuple.
- $I \cap J$ denotes the $L \subset I, J$ such that $|L|$ is maximal.
- If $J = (j_1, \ldots, j_r)$ then $I \cup J := (i_1, \ldots, i_s, j_1, \ldots, j_r)$, i.e., $\cup$ denotes the concatenation of tuples.
- If $J \subset I$ then $I \setminus J$ denotes the $L \subset I$ with $|L|$ maximal such that $J \cap L = \emptyset$ where $\emptyset$ is the empty tuple.

- $\min I = \min\{i \mid i \in I\}$, with the convention that $\min \emptyset > \min I$ for any I.

In this subsection we prove the following theorem.

Theorem 3.2.8. *Let* $\mathcal{R} = \operatorname{rowsp}\begin{pmatrix} R_1 & R_2 \end{pmatrix} \in \mathfrak{G}_{\mathbb{F}_q}(k, 2k)$ *satisfying* (3.7) *with* $\operatorname{rank}(R_1) \geq \operatorname{rank}(R_2) > \frac{k-1}{2}$, $S \in GL_k(\mathbb{F}_{q^k})$ *a matrix diagonalizing* P *and* $M \in GL_k(\mathbb{F}_{q^k})$ *such that* $MS^{-1}(R_1 \ R_2)S$ *is in row reduced echelon form. Let* $R(x) := MS^{-1}R_1S\Delta(x) - MS^{-1}R_2S$. *Then, there exist* $J, L \subset I := (1, \ldots, k)$ *with* $|J| = |L| = \lfloor \frac{k+1}{2} \rfloor - (k - \operatorname{rank}(R_1))$ *such that*

$$[J; L]_{R(x)} = \mu \prod_{i \in K} (x^{q^i} - \mu_i),$$

where $K = J \cap L$, $\mu = [J \setminus K; L \setminus K]_{R(0)} \in \mathbb{F}_{q^k}^*$ *and* $\mu_i = \dfrac{[J \setminus (i); L \setminus (i)]_{R(0)}}{[J \setminus K; L \setminus K]_{R(0)}} \in \mathbb{F}_{q^k}$. *In particular if* $\mu \in \mathbb{F}_{q^k}$ *is such that* $\operatorname{rank}(R(\mu)) \leq \frac{k-1}{2}$, *then*

$$\mu \in \left\{ \mu_i^{q^{k-i}} \mid i \in K \right\}.$$

Let $\mathbb{F}$ be a field and let $m \in \mathbb{F}[y_1, \ldots, y_s]$ be a polynomial of the form $m = \sum_{U \subseteq (1,\ldots,s)} a_U y_U$ where $y_U := \prod_{u \in U} y_u$, $a_{(1,\ldots,s)} \neq 0$.

Lemma 3.2.9. *The following are equivalent:*

1. *The polynomial* m *decomposes in linear factors, i.e.,*

$$m = a_{(1,\ldots,s)} \prod_{u \in (1,\ldots,s)} (y_u + \mu_u)$$

where $\mu_u = \dfrac{a_{(1,\ldots,s)\setminus(u)}}{a_{(1,\ldots,s)}} \in \mathbb{F}$.

2. *It holds that*

$$a_U a_V = a_{U \cap V} a_{(1,\ldots,s)} \tag{3.9}$$

for all U, V *such that* $|V| = s - 1$ *and*

$$\min\left((1, \ldots, s) \setminus V\right) < \min\left((1, \ldots, s) \setminus U\right).$$

Proof. We proceed by induction on s.

$\boxed{\Rightarrow}$ If $s = 1$, m is a linear polynomial. Let us now suppose the thesis true for $s - 1$. Then

$$a_{(1,\ldots,s)} \prod_{u \in (1,\ldots,s)} (y_u + \mu_u) = a_{(1,\ldots,s)}(y_s + \mu_s) \left(\sum_{U \subseteq (1,\ldots,s-1)} \tilde{a}_U y_U \right)$$

where $\tilde{a}_{(1,\dots,s-1)} = 1$ and the coefficients $\tilde{a}_U$ with $U \subseteq (1,\dots,s-1)$ satisfy by hypothesis condition (3.9). The coefficients of m are $a_U = \tilde{a}_{U\setminus(s)}$ if $s \in U$, and $a_U = \mu_s \tilde{a}_U$ otherwise. Therefore we only need to prove that (3.9) holds for $U \in (1,\dots,s-1)$. The equality is $a_{(1,\dots,s)}a_U = a_U a_{(1,\dots,s)}$ hence it is trivial.

$\boxed{\Leftarrow}$ The thesis is trivial for $s = 1$. Let us assume that the thesis holds for $s-1$. We explicitly show the extraction of a linear factor of the polynomial.

$$
\begin{aligned}
m &= \sum_{U\subseteq(1,\dots,s)} a_U y_U = \sum_{\substack{U\subseteq(1,\dots,s)\\ 1\in U}} \left(a_U y_U + a_{U\setminus(1)} y_{U\setminus(1)}\right) = \\
&= \sum_{\substack{U\subseteq(1,\dots,s)\\ 1\in U}} \left(a_U y_1 y_{U\setminus(1)} + \frac{a_U a_{(2,\dots,s)}}{a_{(1,\dots,s)}} y_{U\setminus(1)}\right) = \\
&= \left(y_1 + \frac{a_{(2,\dots,s)}}{a_{(1,\dots,s)}}\right) \cdot \left(\sum_{\substack{U\subseteq(1,\dots,s)\\ 1\in U}} a_U y_{U\setminus(1)}\right).
\end{aligned}
$$

The thesis is true by induction.

□

Let $\mathbb{F}[x_{i,j}]_{1\le i,j\le k}$ be a ring of multivariate polynomials where $k \in \mathbb{N}$. We consider the following matrix

$$
M := \begin{pmatrix} x_{1,1} & \cdots & x_{1,k} \\ \vdots & & \vdots \\ x_{k,1} & \cdots & x_{k,k} \end{pmatrix}.
$$

We are now interested in some particular relations among the minors of M.

Lemma 3.2.10. *Let $J = (j_1,\dots,j_k), L = (l_1,\dots,l_k) \in \{1,\dots,k\}^k$, $J_s = (j_1,\dots,j_s)$ and $L_s = (l_1,\dots,l_s)$. Then,*

$$
[J_s; L_s][J; L] = \sum_{t=s+1}^{k} (-1)^{t+s+1} [J_s \cup (j_t); L_s \cup (l_{s+1})][J \setminus (j_t); L \setminus (l_{s+1})].
$$

Proof. Notice that if we consider as convention that $[\emptyset;\emptyset] = 1$, i.e., when $s = 0$, we get the determinant formula.

We proceed by induction on s. Let us consider the case when $s = 1$, i.e., $[J_1; L_1] = \left(x_{j_1,l_1}\right)$. Then,

$$\begin{aligned}
\left(x_{j_1,l_1}\right)[I;I] &= \sum_{t=1}^{k}(-1)^{t+2}x_{j_1,l_1}x_{j_t,l_2}[J\setminus(j_t);L\setminus(l_2)] \\
&= -x_{j_1,l_1}x_{j_1,l_2}[J\setminus(j_1);L\setminus(l_2)] \\
&\quad +\sum_{t=2}^{k}(-1)^{t+2}\left([(j_1,j_t);(l_1,l_2)]+x_{j_t,l_1}x_{j_1,l_2}\right)[J\setminus(j_t);L\setminus(l_2)] \\
&= \sum_{t=2}^{k}(-1)^{t+2}[(j_1,j_t);(l_1,l_2)][J\setminus(j_t);L\setminus(l_2)] \\
&\quad +x_{j_1,l_2}[J;(l_1,l_1,l_3,\ldots,l_k)].
\end{aligned}$$

For $s = 1$ the thesis is true because $[J;(l_1,l_1,l_3,\ldots,l_k)] = 0$ since column l_1 appears twice.

Assume that the thesis is true for $s-1$.

$$[J_s;L_s][J;L] = \sum_{t=1}^{k}(-1)^{t+s+1}x_{j_t,l_{s+1}}[J_s;L_s][J\setminus(j_t);L\setminus(l_{s+1})].$$

Let us now focus on the factor $x_{j_r,l_{s+1}}[J_s;L_s]$ for $r \geq s+1$, we get

$$x_{j_r,l_{s+1}}[J_s;L_s] = [J_s\cup(j_r);L_s\cup(l_{s+1})]+\sum_{t=1}^{s}(-1)^{t+s}x_{j_t,l_{s+1}}[J_s\setminus(j_t)\cup(j_r);L_s].$$

By substitution it follows that

$$\begin{aligned}
[J_s;L_s][J;L] &= \sum_{t=s+1}^{k}(-1)^{t+s+1}[J_s\cup(j_t);L_s\cup(l_{s+1})][J\setminus(j_t);L\setminus(l_{s+1})]+ \\
&\quad +\sum_{t=1}^{s}(-1)^{t+s+1}x_{j_t,l_{s+1}}\Bigg([J_s;L_s][J\setminus(j_t);L\setminus(l_{s+1})]+ \\
&\quad +\sum_{r=s+1}^{k}(-1)^{r+s}[J_s\setminus(j_t)\cup(j_r);L_s][L\setminus(j_r);L\setminus(l_{s+1})]\Bigg) \\
&= \sum_{t=s+1}^{k}(-1)^{t+s+1}[J_s\cup(j_t);L_s\cup(l_{s+1})][J\setminus(j_t);L\setminus(l_{s+1})]+ \\
&\quad +\sum_{t=1}^{s}(-1)^{t+s+1}x_{j_t,l_{s+1}}\left([J_s\setminus(j_t);L_s\setminus(l_s)][J;\bar{L}]\right)
\end{aligned}$$

where $\bar{L} = (l_1,\ldots,l_s,l_s,l_{s+2},\ldots,l_k)$. The repetition of column l_s twice in $\bar{L}$ implies that $[J;\bar{L}] = 0$. The last equality follows from the induction hypothesis. □

Denote by $\mathcal{I}_{s+1} \subset \mathbb{F}[x_{i,j}]_{1\leq i,j\leq n}$ the ideal generated by all minors of size $s+1$ of M not involving entries on the diagonal, i.e.,

$$\mathcal{I}_{s+1} := ([J,L] \mid J,L \in \{1,\dots,k\}^{s+1},\ J \cap L = \emptyset).$$

The following is an easy consequence of Lemma 3.2.10.

Corollary 3.2.11. *Let $J, L \subset I = (1,\dots,k)$ such that $J \cap L = \emptyset$. Then*

$$[J,L][I,I] - [J\cup(i); L\cup(i)][I\backslash(i); I\backslash(i)] = \sum_{l\in I\backslash(J\cup(i))} h_l[J\cup(i), L\cup(l)] \in \mathcal{I}_{s+1},$$

with $h_l \in \mathbb{F}[x_{i,j}]_{1\leq i,j\leq k}$ for any $l \in I \setminus (J \cup (i))$.

We now investigate the minors of a matrix $S^{-1}NS$ where $N \in \mathbb{F}_q^{k\times k}$ and S is a particular matrix diagonalizing P. We start by giving such a matrix S.

Lemma 3.2.12. *Let $P \in GL_k(\mathbb{F}_q)$ to be the companion matrix of a monic irreducible polynomial $p \in \mathbb{F}_q$ of degree $k > 0$, and let $\lambda \in \mathbb{F}_{q^k}$ be a root of p. Then the matrix*

$$S := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \lambda & \lambda^q & \lambda^{q^2} & \cdots & \lambda^{q^{k-1}} \\ \lambda^2 & \lambda^{2q} & \lambda^{2q^2} & \cdots & \lambda^{2q^{k-1}} \\ \vdots & \vdots & \vdots & & \vdots \\ \lambda^{k-1} & \lambda^{(k-1)q} & \lambda^{(k-1)q^2} & \dots & \lambda^{(k-1)q^{k-1}} \end{pmatrix}. \tag{3.10}$$

diagonalizes P.

Proof. The eigenvalues of the matrix P correspond to the roots of the irreducible polynomial $p \in \mathbb{F}_q[x]$. If $\lambda \in \mathbb{F}_{q^k}$ is an element such that $p(\lambda) = 0$, then $p = \prod_{i=0}^{k-1}(x - \lambda^{q^i})$ by [LN94, Theorem 2.4]. It is enough to show that the columns of S correspond to the eigenvectors of P. Let $i \in \{0,\dots,k-1\}$, then

$$P\begin{pmatrix} 1 \\ \lambda^{q^i} \\ \vdots \\ \lambda^{(k-1)q^i} \end{pmatrix} = \begin{pmatrix} \lambda^{q^i} \\ \lambda^{2q^i} \\ \vdots \\ -\sum_{j=0}^{k-1} p_j \lambda^{jq^i} \end{pmatrix} = \begin{pmatrix} \lambda^{q^i} \\ \lambda^{2q^i} \\ \vdots \\ \left(-\sum_{j=0}^{k-1} p_j \lambda^{j}\right)^{q^i} \end{pmatrix}$$

$$= \begin{pmatrix} \lambda^{q^i} \\ \lambda^{2q^i} \\ \vdots \\ \lambda^{kq^i} \end{pmatrix} = \lambda^{q^i} \begin{pmatrix} 1 \\ \lambda^{q^i} \\ \vdots \\ \lambda^{(k-1)q^i} \end{pmatrix}.$$

□

We now investigate the properties of S.

Lemma 3.2.13. *The matrices S and S^{-1} defined by (3.10) satisfy the following properties:*

1. *the entries of the first column of S (respectively, the first row of S^{-1}) form a basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$, and*
2. *the entries of the $(i+1)$-th column of S (respectively, row of S^{-1}) are the q-th power of the ones of the i-th column (respectively, row) for $i = 1, \ldots, k-1$.*

Proof. The two properties for the matrix S come directly from its definition. By [LN94, Definition 2.30] we know that there exists a unique basis $\{\gamma_0, \ldots, \gamma_{k-1}\}$ of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ such that

$$\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\lambda^i \gamma_j) = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases},$$

where $\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha) := 1 + \alpha^q + \cdots + \alpha^{q^{k-1}}$ for $\alpha \in \mathbb{F}_{q^k}$. We have

$$S^{-1} = \begin{pmatrix} \gamma_0 & \gamma_1 & \cdots & \gamma_{k-1} \\ \gamma_0^q & \gamma_1^q & \cdots & \gamma_{k-1}^q \\ \vdots & \vdots & & \vdots \\ \gamma_0^{q^{k-1}} & \gamma_1^{q^{k-1}} & \cdots & \gamma_{k-1}^{q^{k-1}} \end{pmatrix}.$$

□

Theorem 3.2.14. *Let $r \leq k$ and let $N \in \mathbb{F}_q^{r \times k}$ and $S \in \mathbb{F}_{q^k}^{k \times r}$ be two matrices satisfying the following properties:*

- *N has full rank,*
- *the entries of the first column of S form a basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$, and*
- *the entries of the $(i+1)$-th column of S are the q-th power of the ones of the i-th column, for $i = 1, \ldots, r-1$.*

Then $NS \in GL_r(\mathbb{F}_{q^k})$.

Proof. Let

$$N := (n_{ij})_{\substack{1 \leq i \leq r \\ 1 \leq j \leq k}} \text{ and } NS = (t_{ij})_{\substack{1 \leq i \leq r \\ 1 \leq j \leq r}}.$$

Let $S := (s_{ij})_{\substack{1 \leq i \leq k \\ 1 \leq j \leq r}} = \left(s_i^{q^{j-1}}\right)_{\substack{1 \leq i \leq k \\ 1 \leq j \leq r}}$ where $s_1, \ldots, s_k \in \mathbb{F}_{q^k}$ form a basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. Then:

$$t_{ij} := \sum_{l=1}^{k} n_{il} s_{lj} = \sum_{l=1}^{k} n_{il} s_l^{q^{j-1}} = \left(\sum_{l=1}^{k} n_{il} s_l\right)^{q^{j-1}},$$

since the entries of N are in $\mathbb{F}_q$. Let $\tau_i := \sum_{l=1}^{k} n_{il} s_l \in \mathbb{F}_{q^k}$, then

$$NS = \begin{pmatrix} \tau_1 & \tau_1^q & \dots & \tau_1^{q^{r-1}} \\ \tau_2 & \tau_2^q & \dots & \tau_2^{q^{r-1}} \\ \vdots & \vdots & & \vdots \\ \tau_r & \tau_r^q & \dots & \tau_r^{q^{r-1}} \end{pmatrix}.$$

The elements $\tau_1, \dots, \tau_r \in \mathbb{F}_{q^k}$ are linearly independent over $\mathbb{F}_q$. Indeed, the linear combination

$$\sum_{i=1}^{r} \alpha_i \tau_i \quad = \quad \sum_{i=1}^{r} \alpha_i \sum_{l=1}^{k} n_{il} s_l = \sum_{l=1}^{k} \left(\sum_{i=1}^{r} \alpha_i n_{il} \right) s_l$$

is zero only when $\sum_{i=1}^{r} \alpha_i n_{il} = 0$ for $l = 1, \dots, k$. Since N has full rank it follows that $\alpha_1, \dots, \alpha_r$ must all be zero, leading to the linear independence of $\tau_1, \dots, \tau_r$.

Now let $a_0, \dots, a_{r-1} \in \mathbb{F}_{q^k}$ be such that

$$NS \begin{pmatrix} a_0 \\ \vdots \\ a_{r-1} \end{pmatrix} = 0,$$

and consider the linearized polynomial $f = \sum_{i=0}^{r-1} a_i x^{q^{r-i}}$. The elements $\tau_1, \dots, \tau_r$ are by assumption roots of f. Since f is a linear map, the kernel of f contains the subspace $\langle \tau_1, \dots, \tau_r \rangle \subset \mathbb{F}_{q^k}$. Therefore f is a polynomial of degree q^{r-1} with q^r different roots, then $a_0 = \dots = a_{r-1} = 0$. □

Corollary 3.2.15. *Let $S \in GL_k(\mathbb{F}_{q^k})$ be the matrix specified in* (3.10) *and $N \in \mathbb{F}_q^{k \times k}$. Then, for any $J, L \subset (1, \dots, k)$ tuples of consecutive indices and with $|J| = |L| = \operatorname{rank}(N)$, it follows $[J; L]_{S^{-1}NS} \neq 0$.*

Proof. Let $r := \operatorname{rank}(N)$ and $J, L \subset (1, \dots, k)$ with $|J| = |L| = r$, $H := (1, \dots, r)$. Let $N_1 \in \mathbb{F}_q^{k \times r}$ and $N_2 \in \mathbb{F}_q^{r \times k}$ be matrices with full rank such that $N = N_1 N_2$. One has

$$[J, L]_{S^{-1}NS} = [J, L]_{S^{-1}N_1 \cdot N_2 S} = [J, H]_{S^{-1}N_1} [H, L]_{N_2 S}.$$

We can now focus on the characterization of the maximal minors of the matrix $N_2 S$. The following considerations will also work for the matrix $S^{-1}N_1$ considering its transpose.

The minor $[H, L]_{N_2 S}$ is the determinant of a square matrix obtained by multiplying N_2 with the submatrix consisting of the columns of S indexed by L. Let L contain consecutive indices. By Lemma 3.2.13, the submatrix of S that we obtain together with N_2 satisfy the conditions of Theorem 3.2.14. It follows that $[H, L]_{N_2 S} \neq 0$.

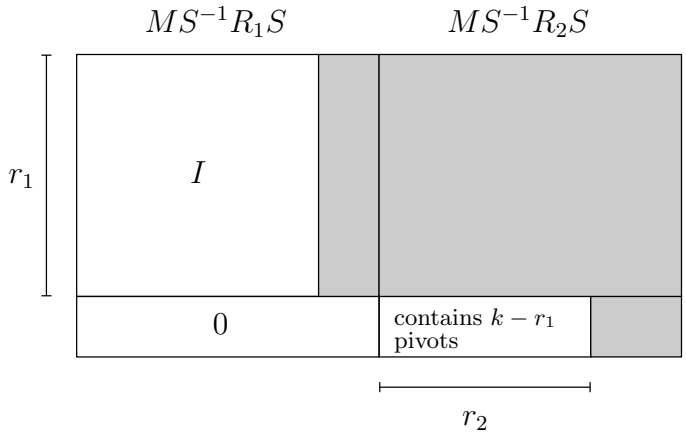
As a consequence we have that $[J, L]_{S^{-1}NS} \neq 0$ when both J and L are tuples of consecutive indices. □

Before proving Theorem 3.2.8, we first give a further definition.

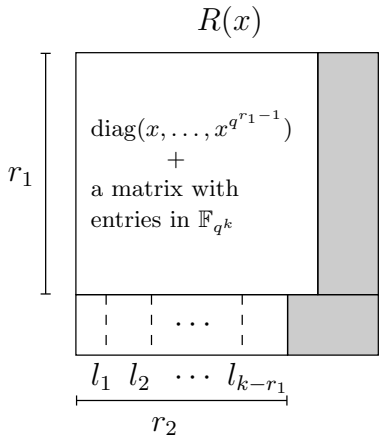
Definition 3.2.16. Let $N \in \mathbb{F}_q^{k\times k}$. We define the *non diagonal rank* of N as follows

$$\text{ndrank}(N) := \min\{r \in \mathbb{N} \mid [J,L]_N = 0 \ \forall J, L \in \{1,\dots,k\}^r,\ J \cap L = \emptyset\} - 1.$$

Proof. [Theorem 3.2.8] We first focus on the form of the matrix $R(x)$. Let $r_i := \text{rank}(R_i)$ for $i = 1, 2$. We deduce by Corollary 3.2.15 that the pivots of the matrix $MS^{-1}(R_1\ R_2)S$ are contained in the first r_1 columns and in a choice of $k - r_1$ of the first r_2 columns of $MS^{-1}R_2S$. The following picture depicts the matrix $MS^{-1}(R_1\ R_2)S$.



As a consequence, $R(x)$ has the following form



where $(l_1, \dots, l_{k-r_1}) \subset I$ is the tuple of indices of the columns corresponding to the pivots of $MS^{-1}R_2S$. Hence, for all $i \in \{1, \dots, k - r_1\}$ the

entries of columns l_i of $R(x)$ are all zero except for the entry l_i, which is $x^{q^{l_i-1}}$, and the entry r_1+i, which is 1.

Now consider the square submatrix $R'(x)$ of $R(x)$ of size $2r_1-k$ defined by the rows and columns indexed by

$$I' := I \setminus (l_1, \ldots, l_{k-r_1}, r_1+1, \ldots, k).$$

The matrix $R'(x)$ is a matrix containing unknowns only in the diagonal entries.

Let $\big(J;L\big)_{R'(x)}$ be a submatrix of $R'(x)$ such that $J \cap L = \emptyset$ and $s := |J| = |L|$. We can extend $\big(J;L\big)_{R'(x)}$ to the submatrix $\big(J \cup (r_1+1, \ldots, k); L \cup (l_1, \ldots, l_{k-r_1})\big)_{R(x)}$ of $R(x)$ for which it holds that

$$[J,L]_{R'(x)} = [J \cup (r_1+1, \ldots, k), L \cup (l_1, \ldots, l_{k-r_1})]_{R(x)}.$$

We obtain that

$$\begin{aligned} \operatorname{ndrank}(R'(x)) &\leq \operatorname{ndrank}(R(x)) - (k-r_1) \\ &\leq \frac{k-1}{2} - (k-r_1) = \frac{2r_1-k-1}{2}. \end{aligned} \tag{3.11}$$

Let $\mu \in \mathbb{F}_{q^k}$ be the unique element satisfying condition (3.8), it holds that $\operatorname{rank}(R'(\mu)) \leq \frac{k-1}{2} - (k-r_1)$. This implies that μ is a root of all $[J,L]_{R'(x)}$ such that $|J| = |L| = \frac{k+1}{2} - (k-r_1)$.

Consider $J', L' \subset I'$ to be tuples of indices such that

$$\begin{aligned} J' \cap L' = \emptyset,\ [J',L']_{R'(x)} \neq 0, \text{ and} \\ [J' \cup (j), L' \cup (l)]_{R'(x)} = 0 \text{ for any } j \neq l \in I' \setminus (J' \cup L'). \end{aligned} \tag{3.12}$$

The existence of a couple of tuples satisfying these conditions is ensured by the definition of $\operatorname{ndrank}(R'(x))$.

Let $K \subset I' \setminus (J' \cup L')$ with $|K| = \lfloor \frac{k+1}{2} \rfloor - (k-r_1) - s$. K is non empty since by (3.11)

$$|K| \geq \lfloor \frac{k+1}{2} \rfloor - (k-r_1) - \frac{2r_1-k-1}{2} = \lfloor \frac{k+1}{2} \rfloor - \frac{k-1}{2} > 0.$$

Define $J := J' \cup K$ and $L := L' \cup K$.

Combining conditions (3.12) and Corollary 3.2.11 we obtain that

$$[J,L][I',I'] - [J \cup (i), L \cup (i)][I' \setminus (i), I' \setminus (i)] = 0$$

for $i \in K$. It follows by Lemma 3.2.9 that the polynomial $[J,L]$ factors as follows

$$[J,L]_{R(x)} = [J \setminus K, L \setminus K]_{R(0)} \prod_{i \in K} \left(x^{q^i} - \mu_i\right).$$

with $\mu_i = \frac{[J\setminus(i), L\setminus(i)]_{R(0)}}{[J\setminus K, L\setminus K]_{R(0)}}$ and $\mu \in \left\{\mu_i^{q^{k-i}} \mid i \in K\right\}$. □

Algorithm 1 in section 3.3 shows an efficient way to find tuples satisfying (3.12).

3.2.2 The non singular case

We focus on the case where the received word $\mathcal{R} = \text{rowsp}\begin{pmatrix} R_1 & R_2 \end{pmatrix} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$ satisfies $R_1 \in GL_k(\mathbb{F}_q)$. We show that in this case we simplify the decoding algorithm.

The following is a reformulation of Corollary 3.2.15 for small rank matrices.

Corollary 3.2.17. *Let $N \in \mathbb{F}_q^{k\times k}$ be a matrix such that $\text{rank}(N) \leq \frac{k-1}{2}$ and $S \in GL_k(\mathbb{F}_{q^k})$ defined as in (3.10). then for any choice of $J, L \subset (1,\dots,k)$ of consecutive indices with $|J| = |L| = \text{rank}(N)$,*

$$[J,L]_{S^{-1}NS} \neq 0.$$

In particular $\text{ndrank}(S^{-1}NS) = \text{rank}(N)$.

Under this hypothesis, an alternative form of Theorem 3.2.6 holds.

Proposition 3.2.18. *Let $\mathcal{R} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$ be a subspace with*

$$\frac{k-1}{2} < \text{rank}(R_2) \leq \text{rank}(R_1) = k.$$

The following are equivalent:

- *$\mathcal{R}$ satisfies (3.7).*
- *There exists a unique $\mu \in \mathbb{F}_{q^k}$ such that*

$$\text{rank}(\Delta(\mu) - S^{-1}R_1^{-1}R_2S) = \text{ndrank}(S^{-1}R_1^{-1}R_2S)$$

where $\Delta(x)$ was defined in Theorem 3.2.6.

Proof. By Theorem 3.2.6 it is clear the equivalence between the first statement and the existence of a unique $\mu \in \mathbb{F}_{q^k}$ such that

$$\text{rank}(\Delta(\mu) - S^{-1}R_1^{-1}R_2S) \leq \frac{k-1}{2}.$$

Let $A = S\Delta(\mu)S^{-1}$, then by Corollary 3.2.17 it holds

$$\text{rank}(A - R_1^{-1}R_2) = \text{ndrank}(\Delta(\mu) - S^{-1}R_1^{-1}R_2S) = \text{ndrank}(S^{-1}R_1^{-1}R_2S).$$

□

The following corollary is the main result of this subsection.

Corollary 3.2.19. *Let* $\mathcal{R} = \operatorname{rowsp}\begin{pmatrix} R_1 & R_2 \end{pmatrix} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$ *satisfying* (3.7) *with* $k = \operatorname{rank}(R_1) \geq \operatorname{rank}(R_2) > \frac{k-1}{2}$ *and* $S \in GL_k(\mathbb{F}_{q^k})$ *a matrix diagonalizing* P. *Let* $R(x) := \Delta(x) - S^{-1}R_1^{-1}R_2S$. *Then, for any choice of tuples of consecutive indices* $J, L \subset (1,\ldots,k)$ *such that* $J \cap L = \emptyset$ *and* $|J| = |L| = \operatorname{ndrank}(S^{-1}R_1^{-1}R_2S)$ *it holds that for any* $i \in (1,\ldots,k)\setminus(J\cup L)$

$$\operatorname{rank}\left(R\left(\left(\frac{[J\cup(i), L\cup(i)]_{S^{-1}R_1^{-1}R_2S}}{[J,L]_{S^{-1}R_1^{-1}R_2S}}\right)^{q^{k-i}}\right)\right) \leq \frac{k-1}{2}.$$

Hence the unique $\mu \in \mathbb{F}_{q^k}$ *from Proposition 3.2.18 is*

$$\mu = \left(\frac{[J\cup(i), L\cup(i)]_{S^{-1}R_1^{-1}R_2S}}{[J,L]_{S^{-1}R_1^{-1}R_2S}}\right)^{q^{k-i}}$$

for any choice of $i \in (1,\ldots,k)\setminus(J\cup L)$.

Proof. By Proposition 3.2.18, there exists a unique μ for which

$$\operatorname{rank}(R(\mu)) = \operatorname{ndrank}(S^{-1}R_1^{-1}R_2S) \leq \frac{k-1}{2}.$$

Hence it suffices to consider minors of $R(x)$ of size $\operatorname{ndrank}(S^{-1}R_1^{-1}R_2S)+1$.

By Corollary 3.2.17, the minor

$$[J\cup(i), L\cup(i)]_{R(x)} = [J,L]_{S^{-1}R_1^{-1}R_2S}x^{q^i} - [J\cup(i), L\cup(i)]_{S^{-1}R_1^{-1}R_2S}$$

is not identically zero. Hence the root

$$\mu = \left(\frac{[J\cup(i), L\cup(i)]_{S^{-1}R_1^{-1}R_2S}}{[J,L]_{S^{-1}R_1^{-1}R_2S}}\right)^{q^{k-i}}$$

makes $\operatorname{rank}(R(\mu)) = \operatorname{ndrank}(S^{-1}R_1^{-1}R_2S)$. By Proposition 3.2.18 μ yields the unique solution to the decoding problem. □

3.3 Algorithms and complexity

We first give an algorithm that, given a non diagonal matrix, returns disjoint tuples $I, J \subset (1,\ldots,k)$ for which the related minor is nonzero and such that every bigger minor containing it and not involving entries of the diagonal is zero. The algorithm uses only row operations.

Lemma 3.3.1. *Algorithm 1 on page 51 works as desired.*

Proof. The algorithm eventually terminates since $|I|$ strictly decreases after every cycle of the while loop. Moreover, its complexity is bounded by the complexity of the Gaussian elimination algorithm which computes the row reduced echelon form of a matrix of $\mathbb{F}_q^{n\times n}$ in $O(n^3)$ operations.

We have to prove that the returned tuples $J, L \subset (1, \dots, k)$ satisfy the output conditions. First of all, the non diagonal condition of matrix M implies that, once terminated the procedure, $J, L \neq \emptyset$. The emptiness of $J \cap L$ follows from the fact that J, L are initialized to $\emptyset$ and each time we modify them, we get $J \cup (j)$ and $L \cup (l)$ where $j \neq l$ are not elements of $J \cap L$.

In order to continue we have to characterize the matrix N. The matrix changes as soon as we find coordinates $j, l \in I$ with $i \neq j$ for which $n_{jl} \neq 0$. The multiplication PN consists of the following row operations

- the i-th row of PN is the i-th row of N for $i \leq j$, and
- the i-th row of PN is the i-th row of N minus $\frac{n_{i,l}}{n_{j,l}}$ times the j-th row of N, where $N = (n_{j,l})_{1\leq j,l\leq k}$ for $i > j$.

It follows that the entries of the l-th column of PN are zero as soon as the row index is bigger than j.

We state that after each cycle of the while loop it holds that $[J, L]_N \neq 0$. We prove it by induction on the cardinality of J and L. Since the matrix M is not diagonal, the while loop will eventually produce tuples $J = (j)$ and $L = (l)$ with $j \neq l$ such that $[J, L]_M \neq 0$. Now suppose that we have J, L such that $J, L \neq \emptyset$, $J \cap L = \emptyset$ and $[J, L]_N \neq 0$ and there exist, following the algorithm, entries $j, l \in I$ with $j \neq l$ such that $n_{j,l} \neq 0$. From the previous paragraph, the only nonzero entry of the row with index j of $\big(J \cup (j); L \cup (l)\big)_N$, which by construction is the last one, is $n_{j,l}$, hence

$$[J \cup (j), L \cup (l)]_N = n_{j,l}[J, L]_N \neq 0.$$

In order to conclude that $[J, L]_M \neq 0$ it is enough to point out the row operations bringing $\big(J; M\big)_M$ to $\big(J; M\big)_N$ are rank preserving.

The property of maximality by containment of the minor $[J, L]_M$ is a direct consequence of the structure of the algorithm. □

Algorithm 2 on page 52 represents the decoding algorithm for spread codes in $\mathfrak{G}_{\mathbb{F}_q}(k, 2k)$ based on the previous section. Algorithm 3 on page 53 instead represents the decoding algorithm for spread codes in $\mathfrak{G}_{\mathbb{F}_q}(k, rk)$ where $r > 2$ and it is a consequence of Lemma 3.2.1.

Complexity of Algorithm 2

The complexity of Algorithm 2 is bounded by some operations on matrices which are performed on the field $\mathbb{F}_{q^k}$. The most expensive of the

operations is the computation of the rank of matrices of size $k \times k$, which can be performed with the help of the Gaussian elimination algorithm. We give the complexities as follows.

- The complexity of step 4. is $O(k^3)$ which corresponds to the computation of $\text{rank}(R(\mu))$.
- The complexity of step 5. is $O(k^4)$ which corresponds to the computation of $\text{rank}(R(\mu_i))$ for all $i \in K$.

An interested reader can find a comparison between this decoding procedure and the ones contained in [KK08b] and [SKK08] for Reed-Solomon like codes in the work [GMR11].

Algorithm 1: Modified Gaussian elimination

input : $M \in \mathbb{F}_q^{k\times k}$ non diagonal matrix.
output: $J, L \subset (1,\dots,k)$ such that $J, L \neq \emptyset$, $J \cap L = \emptyset$, $[J, L] \neq 0$ and $[J \cup (j), L \cup (l)] = 0$ for any $j \neq l \in (1,\dots,k) \setminus (J \cup L)$.

$J = L = \emptyset$, $I = (1,\dots,k)$, $j = 1$ and $N = (n_{j,l})_{1\leq j,l\leq k} = M$;
while $I \neq \emptyset$ **do**
  $t := 0$;
  for $l \in I$ *and* $l \neq j$ **do**
    if $n_{j,l} \neq 0$ *and* $t = 0$ **then**
      $J = J \cup (j), L = L \cup (l)$ and $I = I \setminus (j, l)$;
      $P = (p_{j',l'})_{1\leq j',l'\leq k}$ such that $p_{i,i} = 1$ for any $i \in \{1,\dots,k\}$,
      $p_{i,l} = -\frac{n_{i,l}}{n_{j,l}}$ for any $i \in I$ with $i > j$ and $p_{j',l'} = 0$ otherwise;
      $N = PN$;
      $t = 1$;
    end
  end
  if $t = 0$ **then** $I = I \setminus (j)$;
  $j = \min I$;
end
return J, L;

Algorithm 2: Decoding spread codes: case $n = 2k$

input : $\mathcal{R} = \text{rowsp}\begin{pmatrix} R_1 & R_2 \end{pmatrix} \in \mathfrak{G}_{\mathbb{F}_q}(k, 2k)$,
$P \in GL_k(\mathbb{F}_q)$ the companion matrix of $p \in \mathbb{F}_q[x]$ and
$S \in GL_k(\mathbb{F}_{q^k})$ its diagonalizing matrix.

output: $\mathcal{C} \in \mathcal{S} \subset \mathfrak{G}_{\mathbb{F}_q}(k, n)$ such that $d(\mathcal{R}, \mathcal{C}) < k$, if such a $\mathcal{C}$ exists.

Let $r_i := \text{rank}(R_i)$ for $i = 1, 2$.

1.
if *either* $r_1 = k$ *and* $S^{-1}R_1^{-1}R_2S$ *is diagonal or* $r_1 = 0$ *and* $r_2 = k$ **then**
  return $\mathcal{R} \in \mathcal{S}$;
end

2.
if *either* $r_1 \leq \frac{k-1}{2}$ *or* $r_2 \leq \frac{k-1}{2}$ **then** go to 3.
else if *either* $r_1 = k$ *or* $r_2 = k$ **then** go to 4.
else go to 5.

3. Case $r_1 \leq \frac{k-1}{2}$ `// the case` $r_2 \leq \frac{k-1}{2}$ `is similar.`
return $\text{rowsp}\begin{pmatrix} 0 & I \end{pmatrix}$;

4. Case $r_1 = k$ `// the case` $r_2 = k$ `is similar.`
$R(x) := \Delta(x) - S^{-1}R_1^{-1}R_2S$;
$s := \text{rank}\big((1, \ldots, \lfloor \frac{k-1}{2} \rfloor); (k - \lfloor \frac{k-1}{2} \rfloor + 1, \ldots, k)\big)_{R(0)}$;
$\mu := \frac{[(1,2,\ldots,s+1),(1,k-s,\ldots,k)]_{R(0)}}{[(2,\ldots,s+1),(k-s,\ldots,k)]_{R(0)}}$;
if $\text{rank}\left(R\left(\mu\right)\right) \leq \frac{k-1}{2}$ **then**
  return $\text{rowsp}\begin{pmatrix} I & S\Delta(\mu)S^{-1} \end{pmatrix} \in \mathcal{S}$;
  else return there exists no $\mathcal{C} \in \mathcal{S}$ such that $d(\mathcal{R}, \mathcal{C}) < k$;
end

5. Case $\frac{k-1}{2} < r_2 \leq r_1 < k$ `// the case` $r_1 \leq r_2$ `is similar.`
Find $M \in GL_k(\mathbb{F}_{q^k})$ such that $MS^{-1}(R_1\ R_2)S$ is in row reduced echelon form;
$R(x) := MS^{-1}R_1S\Delta(x) - MS^{-1}R_2S$;
Let $l_1, \ldots, l_{k-r_1} \in \{1, \ldots, k\}$ the columns of the pivots of $MS^{-1}R_2S$;
Let $I' := (1, \ldots, k) \setminus (l_1, \ldots, l_{k-r_1}, r_1 + 1, \ldots, k)$;
Apply Algorithm 1 on $\begin{pmatrix} I'; I' \end{pmatrix}_{R(x)}$ to find $J, L \subset I'$ and set $s := |J|$;
Let $K \subset I' \setminus (J \cup L)$ with $|K| = \lfloor \frac{k+1}{2} \rfloor - k + r_1 - s$;
$\mu_i := \left(\frac{[J \cup (i), L \cup (i)]_{R(0)}}{[J,L]_{R(0)}}\right)^{q^{k-i}}$ for $i \in K$;
if *there exists an* $i \in K$ *such that* $\text{rank}(R(\mu_i)) \leq \frac{k-1}{2}$ **then**
  return $\text{rowsp}\begin{pmatrix} I & S\Delta(\mu_i)S^{-1} \end{pmatrix}$;
  else return there exists no $\mathcal{C} \in \mathcal{S}$ such that $d(\mathcal{R}, \mathcal{C}) < k$;
end

Algorithm 3: Decoding spread codes: case $n = rk$, $r > 2$

input : $\mathcal{R} = \text{rowsp}\begin{pmatrix} R_1 & \cdots & R_r \end{pmatrix} \in \mathfrak{G}_{\mathbb{F}_q}(k, rk)$, $r > 2$,
$P \in GL_k(\mathbb{F}_q)$ the companion matrix of $p \in \mathbb{F}_q[x]$ and
$S \in GL_k(\mathbb{F}_{q^k})$ its diagonalizing matrix.

output: $\mathcal{C} \in \mathcal{S} \subset \mathfrak{G}_{\mathbb{F}_q}(k, rk)$ such that $d(\mathcal{R}, \mathcal{C}) < k$, if such a $\mathcal{C}$ exists.

Let $r_i = \text{rank}(R_i)$ for $i = 1, \ldots, r$;

if $r_i \leq \frac{k-1}{2}$ *for all* $i \in \{1, \ldots, r\}$ **then**
  return there exists no $\mathcal{C} \in \mathcal{S}$ such that $d(\mathcal{R}, \mathcal{C}) < k$
end

Let $j = \min\left\{i \in \{1, \ldots r\} \mid r_i > \frac{k-1}{2}\right\}$;

for $i \in \{1, \ldots, r\}$ *and* $r_i \leq \frac{k-1}{2}$ **do**
  $C_i = 0 \in \mathbb{F}_q^{k \times k}$;
end

for $j < i \leq r$ *and* $r_i > \frac{k-1}{2}$ **do**
  Apply Algorithm 2 with input $\mathcal{R} = \text{rowsp}\begin{pmatrix} R_j & R_i \end{pmatrix}$, P and S;
  if *Algorithm 2 returns no* $\mathcal{C}$ **then**
    return there exists no $\mathcal{C} \in \mathcal{S}$ such that $d(\mathcal{R}, \mathcal{C}) < k$;
    else let $C_i \in \mathbb{F}_q[P]$ such that $\mathcal{C} = \text{rowsp}\begin{pmatrix} I & C_i \end{pmatrix}$;
  end
end

return $\mathcal{C} = \text{rowsp}\begin{pmatrix} C_1 & \cdots C_r \end{pmatrix}$.

Chapter 4

Orbit codes

4.1 Definition and first properties

Definition 4.1.1. Let $k, n \in \mathbb{N}$ with $k \leq n$ and $U \in \mathbb{F}_q^{k\times n}$ a matrix with full rank, $\mathcal{U} := \text{rowsp}(U) \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$ and $A \in GL_n(\mathbb{F}_q)$. We define

$$\mathcal{U}A := \text{rowsp}(UA).$$

Because of the following lemma, the operation here defined is independent from the representation of $\mathcal{U}$.

Lemma 4.1.2. *Let* $U, U' \in \mathbb{F}_q^{k\times n}$ *be matrices such that* $\text{rowsp}(U) = \text{rowsp}(U')$. *Then* $\text{rowsp}(UA) = \text{rowsp}(U'A)$ *for any* $A \in GL_n(\mathbb{F}_q)$.

Define the following right group action on the Grassmannian:

$$\begin{array}{ccc} \mathfrak{G}_{\mathbb{F}_q}(k,n) \times GL_n(\mathbb{F}_q) & \to & \mathfrak{G}_{\mathbb{F}_q}(k,n) \\ (\mathcal{U}, A) & \mapsto & \mathcal{U}A \end{array}$$

Proposition 4.1.3. *The subspace distance is* $GL_n(\mathbb{F}_q)$*–invariant.*

Proof. The thesis is a direct consequence of Lemma 2.2.9 and of

$$\text{rank}\begin{pmatrix} U \\ V \end{pmatrix} = \text{rank}\left(\begin{pmatrix} U \\ V \end{pmatrix} A\right) = \text{rank}\begin{pmatrix} UA \\ VA \end{pmatrix}$$

for all $U, V \in \mathbb{F}_q^{k\times n}$ and $A \in GL_k(\mathbb{F}_q)$. □

Definition 4.1.4. Let $\mathcal{U} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$. The stabilizer group of $\mathcal{U}$ in $GL_n(\mathbb{F}_q)$ is defined as

$$Stab(\mathcal{U}) := \{A \in GL_n(\mathbb{F}_q) \mid \mathcal{U} \cdot A = \mathcal{U}\}.$$

Based on the stabilizer it is possible to define the following equivalence relation on $GL_n(\mathbb{F}_q)$. Let $A, B \in GL_n(\mathbb{F}_q)$, then

$$A \sim_{Stab(\mathcal{U})} B \iff \exists S \in Stab(\mathcal{U}) : A = SB.$$

Theorem 4.1.5. *Let $\mathcal{U} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$. Then, the sets $GL_n(\mathbb{F}_q)/Stab(\mathcal{U})$ and $\mathfrak{G}_{\mathbb{F}_q}(k,n)$ are in bijective correspondence.*

This theorem is a direct consequence of the fact that $GL_n(\mathbb{F}_q)$ acts transitively on the set $\mathfrak{G}_{\mathbb{F}_q}(k,n)$, which means that for any $\mathcal{U},\mathcal{V} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$ there exists an $L \in GL_n(\mathbb{F}_q)$ such that $\mathcal{V} = \mathcal{U}L$. For a further reading of actions of groups on sets, we refer the reader to [Rot95].

We now show another relation between the general linear group and stabilizers.

Proposition 4.1.6. *Let $k,n \in \mathbb{N}$ such that $0 < k \leq n$. Then*

$$GL_n(\mathbb{F}_q) = \cup_{\mathcal{U}\in\mathfrak{G}_{\mathbb{F}_q}(k,n)} Stab(\mathcal{U}) \iff k = n.$$

Proof. It is clear that $\cup_{\mathcal{U}\in\mathfrak{G}_{\mathbb{F}_q}(k,n)} Stab(\mathcal{U}) \subset GL_n(\mathbb{F}_q)$. Moreover, if $k = n$ then $Stab(\mathbb{F}_q^n) = GL_n(\mathbb{F}_q)$.

Let $k < n$, $p \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree k and $P \in GL_n(\mathbb{F}_q)$ its companion matrix. We claim that $P \notin \cup_{\mathcal{U}\in\mathfrak{G}_{\mathbb{F}_q}(k,n)} Stab(\mathcal{U})$. By contradiction assume there exists a $\mathcal{U} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$ such that $P \in Stab(\mathcal{U})$. Since $GL_n(\mathbb{F}_q)$ acts transitively on $\mathfrak{G}_{\mathbb{F}_q}(k,n)$, it follows that there exists an $L \in GL_n(\mathbb{F}_q)$ such that $\mathcal{U}L = \text{rowsp}\begin{pmatrix} I & 0 \end{pmatrix}$. From $P \in Stab(\mathcal{U})$ we get that $\mathcal{U}L(L^{-1}PL) = \mathcal{U}L$, i.e., $L^{-1}PL \in Stab(\mathcal{U}L)$. Since

$$Stab(\mathcal{U}L) = \left\{ \begin{pmatrix} M_1 & 0 \\ N & M_2 \end{pmatrix} \mid M_1 \in GL_k(\mathbb{F}_q),\ M_2 \in GL_{n-k}(\mathbb{F}_q) \right\},$$

it follows that

$$L^{-1}PL = \begin{pmatrix} M_1 & 0 \\ N & M_2 \end{pmatrix}$$

for some $M_1 \in GL_k(\mathbb{F}_q)$ and $M_2 \in GL_{n-k}(\mathbb{F}_q)$. It holds that the characteristic polynomial $\chi_{L^{-1}PL}$ is reducible, which is a contradiction since $\chi_{L^{-1}PL} = p$. □

Proposition 4.1.7. *Let $\mathcal{U},\mathcal{V} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$. Then $Stab(\mathcal{U})$ is conjugate to $Stab(\mathcal{V})$. This implies that*

$$|Stab(\mathcal{U})| = |Stab(\mathcal{V})|.$$

This proposition is also a direct consequence of the transitivity of $GL_n(\mathbb{F}_q)$ on $\mathfrak{G}_{\mathbb{F}_q}(k,n)$.

Definition 4.1.8. Let $\mathcal{U} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$ and $\mathcal{G} < GL_n(\mathbb{F}_q)$. Then

$$\mathcal{C} = \{\mathcal{U}A \mid A \in \mathcal{G}\}$$

is called an *orbit code*. An orbit code is *cyclic* if there exists a defining group which is cyclic.

The name orbit code arises because $\mathcal{G}$ is a group acting on $\mathfrak{G}_{\mathbb{F}_q}(k,n)$, i.e. the code is the orbit of the subspace $\mathcal{U}$ in $\mathfrak{G}_{\mathbb{F}_q}(k,n)$ under the action of $\mathcal{G}$.

Proposition 4.1.9. *Let $\mathcal{C} = \{\mathcal{U}A \mid A \in \mathcal{G}\}$ be an orbit code. It holds that*

$$|\mathcal{C}| = \frac{|\mathcal{G}|}{|\mathcal{G} \cap Stab(\mathcal{U})|}$$

and

$$d(\mathcal{C}) = \min_{A \in \mathcal{G} \setminus Stab(\mathcal{U})} d(\mathcal{U}, \mathcal{U}A).$$

Moreover, $d(\mathcal{U}, \mathcal{U}A_1) = d(\mathcal{U}, \mathcal{U}A_2)$ if $A_1 \sim_{Stab(\mathcal{U})} A_2$.

Proof. The cardinality follows from Proposition 4.1.7, whereas the distance between $\mathcal{U}_1, \mathcal{U}_2 \in \mathcal{C}$ is

$$d(\mathcal{U}_1, \mathcal{U}_2) = d(\mathcal{U}A_1, \mathcal{U}A_2) = d(\mathcal{U}, \mathcal{U}A_2A_1^{-1})$$

for some $A_1, A_2 \in \mathcal{G}$. □

A similar property holds for linear block codes in classical coding theory, where the minimum distance is the minimum of the distances between any non-zero vectors and the zero-vector. Hence this can be seen as another analog of linearity in the subspace setting, different from the one proposed in [EV08].

Definition 4.1.10. If $\mathcal{C} \subseteq \mathfrak{G}_{\mathbb{F}_q}(k,n)$, define the *dual code* as

$$\mathcal{C}^\perp := \{\mathcal{U}^\perp \in \mathfrak{G}_{\mathbb{F}_q}(n-k,n) \mid \mathcal{U} \in \mathcal{C}\}.$$

We use the name dual to point out the relation with the dual codes in classical coding theory. In [KK08b] this class of codes was first called *complementary codes* and it was shown that if $\mathcal{C}$ is a $[n, M, d(\mathcal{C}), k]$-code then $\mathcal{C}^\perp$ is a $[n, M, d(\mathcal{C}), n-k]$-code.

Theorem 4.1.11. *The dual code $\mathcal{C}^\perp$ of an orbit code $\mathcal{C}$ is again an orbit code.*

Proof. One immediately verifies that $(\mathcal{U}A)^\perp = \mathcal{U}^\perp (A^{-1})^t$. It follows that

$$\mathcal{C}^\perp = \{\mathcal{U}^\perp (A^{-1})^t \mid A \in \mathcal{G}\}$$

and $\{(A^{-1})^t \mid A \in \mathcal{G}\} = \{A^t \mid A \in \mathcal{G}\}$ is again a group. □

Example 4.1.12. Some already known network codes, such as spread codes and Reed–Solomon like codes, are orbit codes too. We focus here on the case of spread codes.

Spread codes. Let $n = rk > 0$ with $r > 1$, $p \in \mathbb{F}_q[x]$ a monic irreducible polynomial of degree k and $P \in GL_k(\mathbb{F}_q)$ its companion matrix. Consider $\mathcal{U} = \text{rowsp}\begin{pmatrix} I & 0 \end{pmatrix} \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$. Then, if $\mathcal{S} \subset \mathfrak{G}_{\mathbb{F}_q}(k,n)$ is defined as in Definition 3.1.10 and $\mathfrak{G}$ is the group generated by the matrices

$$\begin{pmatrix} I & A_2 & A_3 & \cdots & A_r \\ 0 & I & 0 & \cdots & 0 \\ 0 & 0 & I & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & I \end{pmatrix}, \begin{pmatrix} 0 & I & A_3 & \cdots & A_r \\ I & 0 & 0 & \cdots & 0 \\ 0 & 0 & I & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & I \end{pmatrix}, \ldots, \begin{pmatrix} 0 & \cdots & 0 & I \\ I & \cdots & 0 & 0 \\ & \ddots & & \vdots \\ 0 & \cdots & I & 0 \end{pmatrix}$$

where $A_2, \ldots, A_r \in \mathbb{F}_q[P]$, it holds that $\mathcal{S} = \{\mathcal{U}A \mid A \in \mathfrak{G}\}$.

In [TR11, Corollary 12] the authors proved that spread codes are cyclic orbit codes.

4.2 Cyclic subgroups of $GL_n(\mathbb{F}_q)$

In this section we investigate the cyclic subgroups of $GL_n(\mathbb{F}_q)$. The goal is to characterize them in a way such that is suitable for the study of orbit codes. More specifically we are interested in answering the question about when two cyclic groups are conjugate to each other.

Consider $GL_n(\mathbb{F}_q)$ and the following equivalence relation on it: given $A, B \in GL_n(\mathbb{F}_q)$ then

$$A \sim_c B \quad \iff \quad \exists L \in GL_n(\mathbb{F}_q) : \ A = L^{-1}BL.$$

A natural choice of representatives of the classes of $GL_n(\mathbb{F}_q)/\sim_c$ is given by the *rational canonical form*.

The following theorem states the existence and uniqueness of a rational canonical form.

Theorem 4.2.1 ([Her75, Chapter 6.7])**.** *Let $A \in GL_n(\mathbb{F}_q)$. Then there exists a matrix $L \in GL_n(\mathbb{F}_q)$ such that*

$$L^{-1}AL = \text{diag}(M_{p_1^{e_{11}}}, \ldots, M_{p_1^{e_{1r_1}}}, \ldots, M_{p_m^{e_{m1}}}, \ldots, M_{p_m^{e_{mr_m}}}) \tag{4.1}$$

is a block diagonal matrix where $p_i \in \mathbb{F}_q[x]$ are irreducible polynomials, $e_{ij} \in \mathbb{N}$ are such that $e_{i1} \geq \cdots \geq e_{ir_i}$, $\chi_A = \prod_{i,j} p_i^{e_{ij}}$ and $\mu_A = \prod_i p_i^{e_{i1}}$ represent respectively the characteristic and the minimal polynomials of A and $M_{p_i^{e_{ij}}}$ denotes the companion matrix of the polynomial $p^{e_{ij}}$. Moreover, the matrix (4.1) is unique for any choice of $A \in GL_n(\mathbb{F}_q)$.

Definition 4.2.2. Let $A \in GL_n(\mathbb{F}_q)$. The matrix (4.1) is called the *rational canonical form* of A and the polynomials $p_1^{e_{11}}, \ldots, p_1^{e_{1r_1}}, \ldots, p_m^{e_{m1}}, \ldots, p_m^{e_{mr_m}} \in \mathbb{F}_q[x]$ are its *elementary divisors*.

The following lemma motivates why rational canonical forms are a good choice of representatives for the classes of $GL_n(\mathbb{F}_q)/\sim_c$.

Lemma 4.2.3. *Let $A, B \in GL_n(\mathbb{F}_q)$. Then the following statements are equivalent:*

1. *$A \sim_c B$, and*
2. *A and B have the same rational canonical form.*

This lemma is well-known and is a consequence of the uniqueness of the rational canonical form.

We now want to extend the previous characterization to subgroups of $GL_n(\mathbb{F}_q)$. Consider the set of all subgroups of $GL_n(\mathbb{F}_q)$

$$\mathbf{G} := \{\mathfrak{G} \mid \mathfrak{G} < GL_n(\mathbb{F}_q)\}$$

and the following equivalence relation on it: given $\mathfrak{G}_1, \mathfrak{G}_2 \in \mathbf{G}$ then

$$\mathfrak{G}_1 \sim_c \mathfrak{G}_2 \quad \iff \quad \exists L \in GL_n(\mathbb{F}_q) : \ \mathfrak{G}_1 = L^{-1}\mathfrak{G}_2 L.$$

The following theorem extends the arguments of Lemma 4.2.3 to the case of cyclic subgroups.

Theorem 4.2.4. *Let $A, B \in GL_n(\mathbb{F}_q)$ and $\mathfrak{G}_A = \langle A\rangle, \mathfrak{G}_B = \langle B\rangle < GL_n(\mathbb{F}_q)$ be the two cyclic groups generated by them. Then, $\mathfrak{G}_A \sim_c \mathfrak{G}_B$ if and only if $|\mathfrak{G}_A| = |\mathfrak{G}_B|$ and there exists an $i \in \mathbb{N}$ with $\gcd(i, |\mathfrak{G}_B|) = 1$ such that $A \sim_c B^i$.*

Proof. $\boxed{\Rightarrow}$ Since $\mathfrak{G}_A \sim_c \mathfrak{G}_B$, it follows that there exists an $L \in GL_n(\mathbb{F}_q)$ such that $\mathfrak{G}_A = L^{-1}\mathfrak{G}_B L$, implying that the two groups have the same order. Moreover, it follows that the group homomorphism

$$\begin{array}{rcl} \varphi : \mathfrak{G}_A & \to & GL_n(\mathbb{F}_q) \\ A^i & \mapsto & LA^iL^{-1} \end{array}$$

is an isomorphism if restricted to the image of φ. As a consequence, the generator A of $\mathfrak{G}_A$ is mapped to a generator of $L\mathfrak{G}_A L^{-1} = \mathfrak{G}_B$, i.e., an element of $\{B^i \mid \gcd(i, |\mathfrak{G}_B|) = 1\}$. Then, there exists an $i \in \mathbb{N}$ with $\gcd(i, |\mathfrak{G}_B|) = 1$ such that $LAL^{-1} = B^i$, which implies that $A \sim_c B^i$.

$\boxed{\Leftarrow}$ From the hypothesis we know that $\langle B^i\rangle = \mathfrak{G}_B$ and that there exists $L \in GL_n(\mathbb{F}_q)$ such that $A = L^{-1}B^iL$. The statement follows as a direct consequence.

□

In order to give unique representatives for the classes of cyclic groups contained in $\mathbf{G}/\sim_c$ we need the following lemma.

Lemma 4.2.5. *Let $A \in GL_n(\mathbb{F}_q)$, $p_{A,1}^{e_{A,1}}, \dots, p_{A,m}^{e_{A,m}} \in \mathbb{F}_q[x]$ its elementary divisors, where $p_{A,j}$ for $j \in \{1, \dots, m\}$ are not necessarily distinct, and $\mathfrak{G}_A < GL_n(\mathbb{F}_q)$ the cyclic group generated by A. Then, for every $i \in \mathbb{N}$ with $\gcd(i, |\mathfrak{G}_A|) = 1$, the elementary divisors of A^i are exactly m many. If we denote them by $p_{A^i,1}^{e_{A^i,1}}, \dots, p_{A^i,m}^{e_{A^i,m}} \in \mathbb{F}_q[x]$, then, up to reordering, the order of $p_{A,j}$ is the same as that of $p_{A^i,j}$ and $e_{A,j} = e_{A^i,j}$ for $j = 1, \dots, m$.*

Proof. First we prove the case where the elementary divisor is unique. At the end of the proof we will give the main remark that implies the generalized statement.

Let $p_A^{e_A} \in \mathbb{F}_q[x]$ be the elementary divisor of a matrix $A \in GL_n(\mathbb{F}_q)$ and $k := n/e_A$. Let $\mathbb{F}_{q^k} := \mathbb{F}_q[x]/(p_A)$ be the splitting field of the polynomial p_A and $\mu \in \mathbb{F}_{q^k}$ a primitive element of it. There exists a $j \in \mathbb{N}$ such that $p_A = \prod_{u=0}^{k-1}(x - \mu^{jq^u})$. Since $p_A^{e_A}$ is the unique elementary divisor of the matrix A, it corresponds to the characteristic and the minimal polynomial of A. As a consequence we obtain that the Jordan normal form of A over $\mathbb{F}_{q^k}$ is

$$J_A = \operatorname{diag}\left(J_{A,\mu^j}^{e_a}, \dots, J_{A,\mu^{jq^{k-1}}}^{e_a}\right)$$

where $J_{A,\mu^{jq^u}}^{e_a} \in GL_{e_A}(\mathbb{F}_{q^k})$ is a unique Jordan block with diagonal entries μ^{jq^u} for $u = 0, \dots, k-1$.

By the Jordan normal form of A it follows that for every $i \in \mathbb{N}$ the characteristic polynomial of A^i is $p_{A^i} = (\prod_{u=0}^{k-1} x - \mu^{ijq^u})^{e_A}$. Let us now focus on the i's such that $\gcd(i, |\mathfrak{G}_A|) = 1$. A^i is then a generator of $\mathfrak{G}_A$, i.e., $p_{A^i} \in \mathbb{F}_q[x]$ is a monic irreducible polynomial whose order is the same as the one of p_A.

In order to conclude that $p_{A^i}^{e_A}$ is the elementary divisor of A^i we consider its rational canonical form. Assume by contradiction that the elementary divisors of A^i were more than one. Without loss of generality we can consider them to be two, i.e., $p_{A^i}^{e_{A,1}}$ and $p_{A^i}^{e_{A,2}}$. This means that its rational canonical form is $\mathrm{RCF}(A^i) = \operatorname{diag}(M_{p_{A^i}^{e_{A,1}}}, M_{p_{A^i}^{e_{A,2}}})$ where we use the operator RCF as an abbreviation for rational canonical form and $e_A = e_{A,1} + e_{A,2}$. For any $j \in \mathbb{N}$ we obtain that the matrix $\mathrm{RCF}((\mathrm{RCF}(A^i))^j)$ is a block diagonal matrix with at least two blocks. Let $j \in \mathbb{N}$ such that $ij \equiv 1 \pmod{|\mathfrak{G}_A|}$ and $L \in GL_n(\mathbb{F}_q)$ be a matrix such that $\mathrm{RCF}(A^i) = L^{-1}A^iL$, then

$$(\mathrm{RCF}(A^i))^j = (L^{-1}A^iL)^j = L^{-1}AL \sim_c A$$

implying that

$$\mathrm{RCF}(A) = \mathrm{RCF}((\mathrm{RCF}(A^i))^j)$$

This leads to a contradiction since $\mathrm{RCF}(A) = M_{p_A^{e_A}}$ has only one block. We conclude that $p_{A^i}^{e_A}$ is the elementary divisor of A^i.

The only difference in the case where $m > 1$ consists in the choice of the splitting field. Let $p_{A,1}^{e_{A,1}}, \dots, p_{A,m}^{e_{A,m}} \in \mathbb{F}_q[x]$ be the elementary divisors

of A, $p_{A,l_1}, \dots p_{A,l_r}$ with $l_1, \dots l_r \in \{1, \dots, m\}$ be the maximal of choice distinct polynomials from the elementary divisors and $d_i := \deg(p_{A,l_i})$ for $i \in \{1, \dots, r\}$. The splitting field on which the proof is based is the splitting field of $\prod_{t=1}^{r} p_{A,l_t}$ over $\mathbb{F}_q$, i.e., $\mathbb{F}_{q^{\mathrm{lcm}(d_1,\dots,d_r)}}$. □

We are now ready to characterize cyclic subgroups of $GL_n(\mathbb{F}_q)$ via the equivalence relation $\sim_c$ based only on their elementary divisors.

Theorem 4.2.6. *Let $A, B \in GL_n(\mathbb{F}_q)$ and $\mathfrak{G}_A, \mathfrak{G}_B \in \mathbf{G}$ the cyclic subgroups generated by them. Then, $\mathfrak{G}_A \sim_c \mathfrak{G}_B$ if and only if the following conditions hold:*

1. *A and B have the same number of elementary divisors, and*
2. *if $p_{A,1}^{e_{A,1}}, \dots, p_{A,m}^{e_{A,m}} \in \mathbb{F}_q[x]$ and $p_{B,1}^{e_{B,1}}, \dots, p_{B,m}^{e_{B,m}} \in \mathbb{F}_q[x]$ are the elementary divisors of A and B respectively, then, up to a reordering argument, the orders of $p_{A,j}$ and $p_{B,j}$ are the same and $e_{A,j} = e_{B,j}$ for $j = 1, \dots, m$.*

Proof. $\boxed{\Rightarrow}$ By Theorem 4.2.4, there exists a power $i \in \mathbb{N}$ with $\gcd(i, |\mathfrak{G}_A|) = 1$ such that $A \sim_c B^i$, i.e., they have the same elementary divisors. The statement follows with Lemma 4.2.5.

$\boxed{\Leftarrow}$ Let $p_{B,l_1}, \dots p_{B,l_r} \in \mathbb{F}_q[x]$ with $l_1, \dots l_r \in \{1, \dots, m\}$ be the maximal choice of pairwise coprime polynomials from the elementary divisors of B, $\mathbb{F}$ the splitting field of $\prod_{t=1}^{r} p_{B,l_t}$ and $\mu \in \mathbb{F}$ a primitive element of it. Consider the notation $d_j := \deg p_{B,l_j}$ for $j = 1, \dots, r$. Then, there exist $i_{B,1}, \dots, i_{B,r} \in \mathbb{N}$ such that $p_{B,l_j} = \prod_{u=0}^{d_j-1}(x - \mu^{i_{B,j}q^u})$ for $j = 1, \dots, r$. The same holds for the matrix A, i.e., there exist $i_{A,1}, \dots, i_{A,r} \in \mathbb{N}$ such that $p_{A,l_j} = \prod_{u=0}^{d_j-1}(x - \mu^{i_{A,j}q^u})$ for $j = 1, \dots, r$. By the condition on the orders, there exists a unique $i \in \mathbb{N}$ such that $i_{A,j} \equiv i \cdot i_{B,j} \pmod{\mathrm{ord}(p_{B,l_j})}$ for $j = 1, \dots, r$. It follows that the elementary divisors of B^i and the ones of A are the same, i.e., $A \sim_c B^i$.

□

The theorem states that we can uniquely represent the classes of cyclic subgroups in $\mathbf{G}/\sim_c$ by considering the cyclic subgroups generated by a rational canonical form based on the choice of a sequence of polynomials of the type $p_1^{e_1}, \dots, p_m^{e_m} \in \mathbb{F}_q[x]$ where the polynomials $p_1, \dots, p_m$ are irreducible and $\sum_{j=1}^{m} e_j \cdot \deg(p_j) = n$. Moreover, what matters in the choice of the polynomials p_j is only their degrees and orders.

Trivially, the following holds for the cardinality of a cyclic group.

Corollary 4.2.7. *Let $\mathfrak{G}_A = \langle A \rangle < GL_n(\mathbb{F}_q)$. Then*

$$|\mathfrak{G}_A| = \mathrm{lcm}\left(\mathrm{ord}\left(p_1^{e_1}\right), \dots, \mathrm{ord}\left(p_r^{e_r}\right)\right)$$

where $p_1^{e_1}, \dots, p_m^{e_m} \in \mathbb{F}_q[x]$ are the elementary divisors of the matrix A.

To conclude this section we give an example explaining why a straight forward generalization of Theorem 4.2.6 to any subgroup of $GL_n(\mathbb{F}_q)$ does not work.

Example 4.2.8. Let $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$ and $\mu \in \mathbb{F}_4$ a primitive element. Consider the following matrices over $\mathbb{F}_4$:

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \; B_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & -1 \end{pmatrix}, \text{ and } B_2 = \begin{pmatrix} \mu+1 & 1 & \mu \\ \mu & \mu & \mu+1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Although $B_1 \sim_c B_2$ since $\chi_{B_1} = \chi_{B_2} = x^3+x^2+1$, it holds that $|\langle A, B_1\rangle| = 168 \neq 60480 = |\langle A, B_2\rangle|$, meaning that the two groups are not conjugate.

4.2.1 Cyclic Orbit Codes

We now apply the results from the previous section to the characterization of cyclic codes. We start by giving an equivalence relation given by conjugation on the set of all orbit codes.

Definition 4.2.9. Let $\mathfrak{G}_1, \mathfrak{G}_2 < GL_n(\mathbb{F}_q)$ and $\mathcal{C}_1 := \{\mathcal{U}_1 A \mid A \in \mathfrak{G}_1\}, \mathcal{C}_2 := \{\mathcal{U}_2 A \mid A \in \mathfrak{G}_2\} \subseteq \mathfrak{G}_{\mathbb{F}_q}(k,n)$ be two orbit codes. We say that $\mathcal{C}_1$ and $\mathcal{C}_2$ are conjugate or simply $\mathcal{C}_1 \sim_c \mathcal{C}_2$ if there exists a matrix $L \in GL_n(\mathbb{F}_q)$ such that

$$\mathcal{U}_2 = \mathcal{U}_1 L \text{ and } \mathfrak{G}_2 = L^{-1}\mathfrak{G}_1 L,$$

i.e., $\mathcal{C}_2 = \{\mathcal{U}_1 AL \mid A \in \mathfrak{G}_1\} = \{\mathcal{U}_1 L(L^{-1}AL) \mid A \in \mathfrak{G}_1\}$. We use the notation $\sim_{c,\mathbb{F}}$ when the field on which we perform the conjugation is not clear from the context.

Remark 4.2.10. If $\mathcal{C}_1 := \{\text{rowsp}(U_1 A) \mid A \in \mathfrak{G}_1\}, \mathcal{C}_2 := \{\text{rowsp}(U_2 A) \mid A \in \mathfrak{G}_2\} \subseteq \mathfrak{G}_{\mathbb{F}_q}(k,n)$, i.e., when we define orbit codes starting from matrices $U_1, U_2 \in \mathbb{F}_q^{k\times n}$ instead from the subspaces $\mathcal{U}_1, \mathcal{U}_2 \in \mathfrak{G}_{\mathbb{F}_q}(k,n)$, then the equivalence relation needs an additional matrix $M \in GL_k(\mathbb{F}_q)$ such that $U_2 = MU_1 L$.

In order to further study properties of orbit codes, we need to introduce the notion of distance distribution for orbit codes. Due to Proposition 4.1.9, we are able to adapt the definition of weight enumerator from classical coding theory to orbit codes.

Definition 4.2.11. Let $\mathcal{C} = \{\mathcal{U}A \mid A \in \mathfrak{G} < GL_n(\mathbb{F}_q)\} \subseteq \mathfrak{G}_{\mathbb{F}_q}(k,n)$ be an orbit code. The distance distribution of $\mathcal{C}$ is the tuple $(D_0, \dots, D_k) \in \mathbb{N}^{k+1}$ such that

$$D_i := \frac{|\{A \in \mathfrak{G} \mid d(\mathcal{U}, \mathcal{U}A) = 2i\}|}{|\mathfrak{G} \cap Stab(\mathcal{U})|}.$$

As a consequence we obtain that $D_0 = 1$ and $\sum_{i=0}^{k} D_i = |\mathcal{C}|$. We are able to state the following theorem that characterizes conjugate orbit codes and that is a generalization of Theorem 9 from [TR11].

Theorem 4.2.12. *The binary relation $\sim_c$ on orbit codes is an equivalence relation. Moreover, let $\mathcal{C}_1, \mathcal{C}_2$ be two orbit codes such that $\mathcal{C}_1 \sim_c \mathcal{C}_2$, then $|\mathcal{C}_1| = |\mathcal{C}_2|$ and they have the same distance distribution.*

Proof. The fact that $\sim_c$ is an equivalence relation on orbit codes is a consequence of Theorem 4.2.4.

Let $\mathcal{C}_1 := \{\mathcal{U}A \mid A \in \mathfrak{G} < GL_n(\mathbb{F}_q)\}$ and $L \in GL_n(\mathbb{F}_q)$ such that $\mathcal{C}_2 = \{\mathcal{U}AL \mid A \in \mathfrak{G}\}$. The same cardinality is a consequence of the fact that given $A, B \in \mathfrak{G}$, then

$$\mathcal{U}AL = \mathcal{U}BL \iff \mathcal{U}A = \mathcal{U}B.$$

The same distance distribution follows from the distance preserving property of the $GL_n(\mathbb{F}_q)$ action on $\mathfrak{G}_{\mathbb{F}_q}(k, n)$, i.e., $d(\mathcal{U}L, \mathcal{U}AL) = d(\mathcal{U}, \mathcal{U}A)$. □

The importance of this last theorem is that two conjugate orbit codes are not distinguishable from the point of view of cardinality and distance distribution. Theorem 4.2.6 translates as follows in the language of orbit codes.

Corollary 4.2.13. *Every cyclic orbit code is conjugate to a cyclic orbit code defined by a cyclic group generated by a matrix in rational canonical form.*

Note that the corollary is weaker than Theorem 4.2.6 since it does not involve the elementary divisors of the defining matrix. This formulation is actually enough for our purposes. Indeed, thanks to Theorem 4.2.12 and Corollary 4.2.13, we can consider only cyclic orbit codes out of matrices in rational canonical form for the study of codes with good parameters.

We are now interested in these orbit codes.

Theorem 4.2.14. *Let $M := \operatorname{diag}(M_{p_1^{e_1}}, \ldots, M_{p_t^{e_t}}) \in GL_n(\mathbb{F}_q)$ be a matrix such that $p_i \in \mathbb{F}_q[x]$ are monic irreducible polynomials and $d_i := \deg(p_i^{e_i})$ for $i = 1, \ldots, t$. Let $\mathcal{U} = \operatorname{rowsp}\begin{pmatrix} U_1 & \cdots & U_t \end{pmatrix} \in \mathfrak{G}_{\mathbb{F}_q}(k, n)$ with $U_i \in \mathbb{F}_q^{k \times d_i}$ and where $\begin{pmatrix} U_1 & \cdots & U_t \end{pmatrix}$ is in row reduced echelon form. For any $i \in \{1, \ldots, t\}$, let $\bar{U}_i$ be a submatrix of U_i as depicted in Figure 4.1.*

If $\mathcal{C} := \{\mathcal{U}M^i \mid i \in \mathbb{N}\}$ and $\mathcal{C}_i := \{\operatorname{rowsp}(\bar{U}_i)M^j_{p_i^{e_i}} \mid j \in \mathbb{N}\}$, then

$$d(\mathcal{C}) \geq 2k - 2\sum_{i=1}^{t} \max_{j \in \mathbb{N}} \dim\left(\operatorname{rowsp}\left(\bar{U}_i\right) \cap \operatorname{rowsp}\left(\bar{U}_i M^j_{p_i^{e_i}}\right)\right), \tag{4.2}$$

and $|\mathcal{C}| := \operatorname{lcm}(|\mathcal{C}_1|, \ldots, |\mathcal{C}_t|)$.

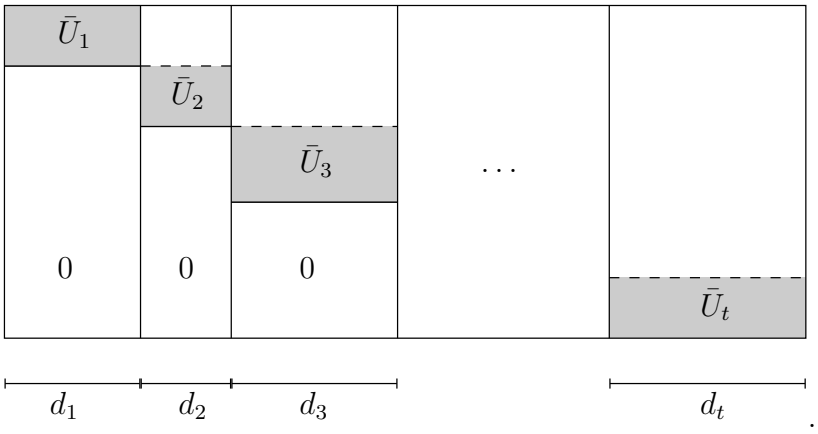


Figure 4.1: The matrix U in row reduced echelon form.

Proof. Consider the following projections

$$\begin{array}{rccc} \pi_i: & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^{d_i} \\ & (v_1,\ldots,v_n) & \longmapsto & (v_{l_{i-1}+1},\ldots,v_{l_i}) \end{array}$$

where $l_i = \sum_{j=1}^{i} d_i$ for $i = 1,\ldots,t$. Since $\begin{pmatrix} U_1 & \ldots & U_t \end{pmatrix}$ has full rank and is in row reduced echelon form, the matrices $\bar{U}_i$ have full rank. Let $\bar{\mathcal{U}}_i \subset \mathbb{F}_q^n$ be the space spanned by the rows of $\begin{pmatrix} U_1 & \ldots & U_t \end{pmatrix}$ corresponding to the ones of $\bar{U}_i$. Since $\bar{U}_i$ has full rank it follows that $\pi_i|_{\bar{\mathcal{U}}_i}$ is injective for $i = 1,\ldots,t$. As a consequence we obtain that for any $i = 1,\ldots,t$, if $m_i \in \mathbb{N}$ is such that

$$\dim\left(\bar{\mathcal{U}}_i \cap \bar{\mathcal{U}}_i M_{p_i^{e_i}}^{m_i}\right) \geq \dim\left(\bar{\mathcal{U}}_i \cap \bar{\mathcal{U}}_i M_{p_i^{e_i}}^{j}\right), \quad \forall j \in \mathbb{N}$$

and $\mathcal{V}_i := \bar{\mathcal{U}}_i \cap \bar{\mathcal{U}}_i M_{p_i^{e_i}}^{m_i}$, then

$$\pi_i(\mathcal{V}_i) \subseteq \operatorname{rowsp}(\bar{U}_i) \cap \operatorname{rowsp}(\bar{U}_i M_{p_i^{e_i}}^{m_i}).$$

It follows that

$$\dim(\mathcal{V}_i) \leq \max_{j\in\mathbb{N}} \dim(\operatorname{rowsp}(\bar{U}_i) \cap \operatorname{rowsp}(\bar{U}_i M_{p_i^{e_i}}^{j})).$$

Since $\mathcal{U} = \oplus_{i=1}^{t} \bar{\mathcal{U}}_i$ we conclude that

$$\begin{aligned} d(\mathcal{C}) &= 2k - 2\max_{j\in\mathbb{N}} \dim(\mathcal{U} \cap \mathcal{U}M^j) \\ &\geq 2k - 2\sum_{i=1}^{t} \max_{j\in\mathbb{N}} \dim\left(\operatorname{rowsp}\left(\bar{U}_i\right) \cap \operatorname{rowsp}\left(\bar{U}_i M_{p_i^{e_i}}^{j}\right)\right) \end{aligned}$$

The cardinality of $\mathcal{C}$ is a direct consequence of the fact that

$$\operatorname{diag}(M_{p_1^{e_1}},\ldots,M_{p_t^{e_t}})^i = \operatorname{diag}(M_{p_1^{e_1}}^i,\ldots,M_{p_t^{e_t}}^i)$$

and of the minimality of the least common multiple. □

Remark 4.2.15. The minimum distance of the code $\mathcal{C}$ can be generalized with the help of permutations. Let $\sigma : \{1, \ldots, t\} \to \{1, \ldots, t\}$ be a permutation and $\mathcal{C}_\sigma := \left\{\text{rowsp}\left(U_\sigma M_\sigma^i\right) \mid i \in \mathbb{N}\right\}$ where $U_\sigma = (U_{\sigma_1}, \ldots, U_{\sigma_t})$ and $M_\sigma = \text{diag}\left(M_{p_{\sigma_1}^{e_{\sigma_1}}}, \ldots, M_{p_{\sigma_t}^{e_{\sigma_t}}}\right)$. Since for any permutation we have that $\mathcal{C} \sim_c \mathcal{C}_\sigma$, by the previous theorem it follows that

$$d(\mathcal{C}) \geq \max_{\sigma \text{ perm.}} \left(2k - 2\sum_{i=1}^{t} \max_{j \in \mathbb{N}} \dim\left(\text{rowsp}\left(\bar{U}_{\sigma_i}\right) \cap \text{rowsp}\left(\bar{U}_{\sigma_i} M_{p_{\sigma_i}^{e_{\sigma_i}}}^j\right)\right)\right)$$
$$= \left(2k - 2 \min_{\sigma \text{ perm.}} \left(\sum_{i=1}^{t} \max_{j \in \mathbb{N}} \dim\left(\text{rowsp}\left(\bar{U}_{\sigma_i}\right) \cap \text{rowsp}\left(\bar{U}_{\sigma_i} M_{p_{\sigma_i}^{e_{\sigma_i}}}^j\right)\right)\right)\right).$$

where the matrices $\bar{U}_{\sigma_i}$ for $i = 1, \ldots, t$ respect Figure 4.1 but considering the row reduced echelon form of U_σ instead of the one of U.

It is possible to find examples for which the lower bound given by (4.2) is attained. The following lemmas depict these examples.

Lemma 4.2.16. *Let $M := \text{diag}(M_{p_1^{e_1}}, \ldots, M_{p_t^{e_t}}) \in GL_n(\mathbb{F}_q)$ be a matrix such that $p_i \in \mathbb{F}_q[x]$ are monic irreducible polynomials and $d_i := \deg(p_i^{e_i})$ for $i = 1, \ldots, t$. Let $k \leq d_i$ for $i = 1, \ldots, t$ and $\mathcal{U} := \text{rowsp}\begin{pmatrix} U_1 & \cdots & U_t \end{pmatrix} \in \mathfrak{G}_{\mathbb{F}_q}(k, n)$ where $U_i \in \mathbb{F}_q^{k \times d_i}$ are matrices having full rank for $i = 1, \ldots, t$. If we define $\mathcal{C} := \{\mathcal{U}M^i \mid i \in \mathbb{N}\}$ and $\mathcal{C}_i := \{\text{rowsp}(U_i) M_{p_i^{e_i}}^j \mid j \in \mathbb{N}\}$ and it holds that $\gcd(|\mathcal{C}_i|, |\mathcal{C}_j|) = 1$ for all $i \neq j$, then*

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

Proof. We only need to show that there exists a codeword of $\mathcal{C}$ that satisfies this minimum. Up to a permutation of $\{1, \ldots, t\}$ we can consider that the code $\mathcal{C}_1$ is satisfying the minimum distance. Let $g_1 \in \mathbb{N}$ be such that $d(\text{rowsp}(U_1), \text{rowsp}(U_1) M_{p_1^{e_1}}^{g_1}) = d(\mathcal{C}_1)$. Since the cardinalities of the codes $\mathcal{C}_i$ are pairwise coprime, it follows that there exists $g \in \mathbb{N}$ such that

$$g \equiv g_1 \pmod{|\mathcal{C}_1|} \quad \text{and} \quad g \equiv 0 \pmod{|\mathcal{C}_j|}$$

for $j = 2, \ldots, m$. We obtain that

$$d(\mathcal{U}, \mathcal{U}M^g) = d(\mathcal{U}, \mathcal{U}\text{diag}(M_{p_1^{e_1}}^{g_1}, I, \ldots, I)) = d(\mathcal{U}_1, \mathcal{U}_1 M_{p_1^{e_1}}^{g_1}) = d(\mathcal{C}_1)$$

□

Lemma 4.2.17. *Let $M := \text{diag}(M_{p_1^{e_1}}, \ldots, M_{p_t^{e_t}}) \in GL_n(\mathbb{F}_q)$ such that $p_i \in \mathbb{F}_q[x]$ are monic irreducible polynomials and $d_i := \deg(p_i^{e_i})$ for $i = 1, \ldots, t$. Let $k_i \leq d_i$, $\bar{U}_i \in \mathbb{F}_q^{k_i \times d_i}$ be matrices with full rank and $\mathcal{U} :=$*

$\mathrm{rowsp}(\mathrm{diag}(\bar{U}_1, \ldots, \bar{U}_t)) \in \mathfrak{G}_{\mathbb{F}_q}(k, n)$. *If we define* $\mathcal{C} := \{\mathcal{U}M^i \mid i \in \mathbb{N}\}$ *and* $\mathcal{C}_i := \{\mathrm{rowsp}(\mathcal{U}_i M_{p_i^{e_i}})^j \mid j \in \mathbb{N}\}$ *where* $\mathcal{U}_i = \mathrm{rowsp}(\bar{U}_i)$ *and it holds* $\gcd(|\mathcal{C}_i|, |\mathcal{C}_j|) = 1$ *for all* $i \neq j$*, then*

$$d(\mathcal{C}) = 2k - 2\sum_{i=1}^{t} \max_{j \in \mathbb{N}} \dim\left(\mathrm{rowsp}\left(\bar{U}_i\right) \cap \mathrm{rowsp}\left(\bar{U}_i M^j_{p_i^{e_i}}\right)\right).$$

Proof. Here we show a codeword of $\mathcal{C}$ which satisfies the relation. Let $g_1, \ldots, g_t \in \mathbb{N}$ be such that $\dim(\mathcal{U}_j) \cap \mathcal{U}_j M^{g_j}_{p_j^{e_j}})$ is maximal for $j = 1, \ldots, m$. Since the cardinalities of the codes are pairwise coprime, it follows that there exists a $g \in \mathbb{N}$ such that

$$g \equiv g_j \pmod{|\mathcal{C}_j|}$$

for any $j = 1, \ldots, t$. Then,

$$\begin{aligned} d(\mathcal{C}) &= d(\mathcal{U}, \mathcal{U}\mathrm{diag}(M_{p_1^{e_1}}, \ldots, M_{p_m^{e_m}})^g) \\ &= d(\mathcal{U}, \mathcal{U}\mathrm{diag}(M^{g_1}_{p_1^{e_1}}, \ldots, M^{g_m}_{p_m^{e_m}})) = 2k - 2\sum_{j=1}^{m} \dim(\mathcal{U}_j \cap \mathcal{U}_j M^{g_j}_{p_j^{e_j}}). \end{aligned}$$

□

4.3 Decoding cyclic orbit codes and DLP

As a textbook on the discrete logarithm problem (DLP) we refer the reader to Chapter 3.6 of [MvOV01]. There the reader can find the definition of the DLP as well as its use in cryptography and common known attacks. For the sake of completeness, we review some information relevant for our purpose, i.e., find a relation between the DLP and the problem of decoding cyclic orbit codes.

Definition 4.3.1. Let $\mathfrak{G}$ be a cyclic group of order l, $\alpha \in \mathfrak{G}$ a generator of $\mathfrak{G}$ and $\beta \in \mathfrak{G}$. The *discrete logarithm problem* (DLP) is the problem of finding an $m \in \mathbb{N}$ with $0 \leq m \leq l - 1$ such that $\beta = \alpha^m$.

We give here a standard generalization of the DLP.

Definition 4.3.2. Let $\mathfrak{G}$ be a finite group and $\alpha, \beta \in \mathfrak{G}$. A *generalization of the DLP* consists in finding an $m \in \mathbb{N}$ such that $\beta = \alpha^m$, provided that such an $m \in \mathbb{N}$ exists. In this case, as well as for the one of Definition 4.3.1, one uses the notation $m = \log_\alpha \beta$.

A particular case of this generalization is the DLP on matrices.

Definition 4.3.3. Let $\mathfrak{G} \subset GL_n(\mathbb{F}_q)$ be a cyclic subgroup of order l, $A \in \mathfrak{G}$ a generator of $\mathfrak{G}$ and $B \in \mathfrak{G}$. The *DLP on matrices* is the problem of finding an $m \in \mathbb{N}$ with $0 \leq m \leq l - 1$ such that $B = A^m$.

The DLP is considered to be computationally infeasible for a generic group of order bigger than 2^{160}. Indeed, a known algorithm for computing the discrete logarithm for general groups is the *Pollard's rho algorithm* which requires $O(\sqrt{l})$ group multiplications.

We translate our decoding problem of cyclic orbit codes in the language of the DLP.

Definition 4.3.4. Let $\mathfrak{G} \subset GL_n(\mathbb{F}_q)$ be a cyclic group, $A \in \mathfrak{G}$ a generator of it, $B \in GL_n(\mathbb{F}_q)$ and $U \in \mathbb{F}_q^{k\times n}$ a matrix with full rank. Let

$$r := \min_{i\in\mathbb{N}} \left\{ \operatorname{rank} \begin{pmatrix} U \\ UA^i \end{pmatrix} \mid \operatorname{rank} \begin{pmatrix} U \\ UA^i \end{pmatrix} \neq k \right\} \tag{4.3}$$

We define the *rank discrete logarithm problem* (RDLP) as the problem of finding an $m \in \mathbb{N}$ such that

$$\operatorname{rank} \begin{pmatrix} UB \\ UA^m \end{pmatrix} < \frac{k+r}{2},$$

provided that such an $m \in \mathbb{N}$ exists.

We can now prove the equivalence of the definition of the RDLP with the problem of decoding a cyclic orbit code.

Lemma 4.3.5. *The existence of a solution for the RDLP implies the existence of a solution for the decoding problem as defined in Definition 2.2.13 for a cyclic orbit code. Moreover, if a solution of the RDLP exists, then this solution is unique modulo $|\mathcal{C}|$.*

Proof. Consider the cyclic orbit code

$$\mathcal{C} := \{\mathcal{U}A^i \mid i \in \mathbb{N}\},$$

where $\mathcal{U} = \operatorname{rowsp}(U)$. Let $m \in \mathbb{N}$ be a solution of the RDLP. It holds that

$$\begin{aligned} d(\mathcal{U}B,\mathcal{U}A^m) &= 2\operatorname{rank} \begin{pmatrix} UB \\ UA^m \end{pmatrix} - 2k < r - k \\ &= \min_{i\in\mathbb{N}} \left\{ \frac{d(\mathcal{U},\mathcal{U}A^i)}{2} \mid d(\mathcal{U},\mathcal{U}A^i) \neq 0 \right\} = \frac{d(\mathcal{C})}{2} \end{aligned}$$

where we used (2.2) to translate the distance into the rank, r is defined in (4.3) and the last equality follows from Proposition 4.1.9.

The uniqueness is a consequence of the uniqueness of the decoding problem. □

The following picture depicts the RDLP.

In general, we expect the RDLP problem to be computationally difficult to solve. Naively, one can think to apply well known attacks for solving the DLP to the RDLP. We give hereinafter an adaptation of the *Baby–step giant–step algorithm* in order to solve the RDLP.

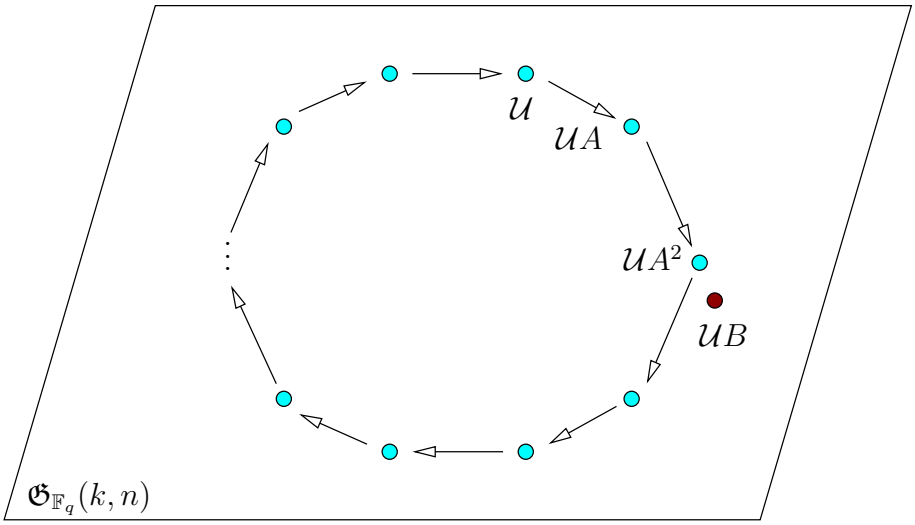


Figure 4.2: RDLP.

Remark 4.3.6 (Baby–step giant–step for RDLP). Let $\mathfrak{G} = \langle A \rangle \subset GL_n(\mathbb{F}_q)$ be a cyclic group, $U \in \mathbb{F}_q^{k\times n}$ be a matrix with full rank and $B \in GL_n(\mathbb{F}_q)$ such that there exists an $m \in \mathbb{N}$ for which

$$\operatorname{rank}\begin{pmatrix} UB \\ UA^m \end{pmatrix} < \frac{k+r}{2}.$$

Let $l := |\mathfrak{G}|$ and $t := \left\lceil \sqrt{l} \right\rceil$. Then, there exist $i, j \in \mathbb{N}$ with $0 \leq i, j \leq t$ such that $m = it + j$ and therefore

$$\frac{k+r}{2} > \operatorname{rank}\begin{pmatrix} UB \\ UA^m \end{pmatrix} = \operatorname{rank}\begin{pmatrix} UB \\ UA^{it+j} \end{pmatrix} = \operatorname{rank}\begin{pmatrix} UB(A^{-t})^i \\ UA^j \end{pmatrix}.$$

This algorithm requires physical space to store $\left\lceil \sqrt{l} \right\rceil$ matrices of $GL_n(\mathbb{F}_q)$ and $\left\lceil \sqrt{l} \right\rceil$ matrix multiplications and rank computations.

4.3.1 Error–free case

We now focus on a particular situation of the RDLP, which is the one where the $\mathcal{U}B$ lies in $\mathcal{C} = \{\mathcal{U}A^i \mid i \in \mathbb{N}\}$, i.e., there exists an $m \in \mathbb{N}$ such that $\operatorname{rank}\begin{pmatrix} UB \\ UA^m \end{pmatrix} = k$, i.e., $\operatorname{rowsp}(UB) \in \mathcal{C}$. This situation is related, in a network point of view, to an error free communication, i.e., the received codeword corresponds to the sent one. Despite the fact that $\operatorname{rowsp}(UB) \in \mathcal{C}$, this particular case of the RDLP, as well as the general one, cannot be

Algorithm 4: Baby–step giant–step for RDLP

input : $U \in \mathbb{F}_q^{k\times n}$ a matrix with full rank,
$A, B \in GL_n(\mathbb{F}_q)$ for which there exists $m \in \mathbb{N}$ such that
$\operatorname{rank}\begin{pmatrix} UB \\ UA^m \end{pmatrix} < r$.

output: $m \in \mathbb{N}$

$l := \operatorname{ord}(A)$ and $t := \left\lceil \sqrt{l} \right\rceil$

Construct a table with entries $(j, A^j) \in \mathbb{N} \times GL_n(\mathbb{F}_q)$ for $0 \leq j < t$

$A' := A^{n-t} = A^{-t}$ and $B' := B$

for *i=1,. . . ,t-1* **do**

  for *j=0,. . . ,t-1* **do**

    Compute $R := \operatorname{rank}\begin{pmatrix} UB' \\ UA^j \end{pmatrix}$ picking A^j from the table.

    if $R < \frac{k+r}{2}$ **then**

      return $m := it + j$

    end

  end

  $B' := B'A'$

end

considered as a classical DLP on matrices. The difference consists in the fact that $\operatorname{rowsp}(UB) \in \mathcal{C}$ does not imply that $B \in \langle A \rangle$, only that $B \sim_{Stab(\mathcal{U})} A^m$ for some $m \in \mathbb{N}$ where $\mathcal{U} = \operatorname{rowsp}(U)$.

We also show that for this particular case we obtain a member criterion for a received space to be an element of a cyclic orbit code.

In [MW97] the authors proved that there exists a probabilistic polynomial reduction of the DLP on matrices of $GL_n(\mathbb{F}_q)$ to the DLP in some extension fields of $\mathbb{F}_q$. In this subsection we show a similar result for this case of the RDLP.

Thanks to Section 4.2.1 we can focus our study on cyclic orbit codes defined by groups generated by a matrix in rational canonical form. As a first step we are going to focus on a particular conjugated group of a cyclic orbit code.

Theorem 4.3.7. *Let $\mathcal{C} = \{\mathcal{U}A^i \mid i \in \mathbb{N}\} \subset \mathfrak{G}_{\mathbb{F}_q}(k, n)$ be a cyclic orbit code where $A \in GL_n(\mathbb{F}_q)$ is in rational canonical form. Then, there exists an extension field $\mathbb{F} \supseteq \mathbb{F}_q$ and a code $\mathcal{C}_{\mathbb{F}} \subset \mathfrak{G}_{\mathbb{F}}(k, n)$ conjugate to $\mathcal{C}$ such that the pivots of all the codewords of $\mathcal{C}_{\mathbb{F}}$ are in the same position.*

Proof. Let $\mathbb{F}$ be the splitting field of the characteristic polynomial $\chi_A \in \mathbb{F}_q[x]$ of A and $S \in GL_n(\mathbb{F})$ a matrix such that $J_A = S^{-1}AS$ is the Jordan normal

form of A. By Theorem 4.2.12, we obtain that

$$\mathcal{C}_{\mathbb{F}} := \{\mathcal{U}A^iS \mid i \in \mathbb{N}\} = \{\mathcal{U}SJ_A^i \mid i \in \mathbb{N}\} \sim_{c,\mathbb{F}} \mathcal{C}.$$

Let $U_s \in \mathbb{F}^{k\times n}$ be a matrix with full rank and in row reduced echelon form such that $\mathcal{U}S = \text{rowsp}(U_s)$ and denote by $l_1, \ldots, l_k \in \{1, \ldots, n\}$ the indices of the columns containing the pivots of U_s. Since $\mathcal{U}SJ_A^i = \text{rowsp}(U_sJ_A^i)$, it is enough to prove that the pivots of $U_sJ_A^i$ lie in the columns $l_1, \ldots, l_k$ for any $i \in \mathbb{N}$. The matrix $U_sJ_A^i$ is not generally in row reduced echelon form but, in our case, it is enough to check that for all $i \in \mathbb{N}$ the entries (j, l) for $j \in \{1, \ldots, k\}$ and $l \in \{1, \ldots, n\}$ of the matrix $U_sJ_A^i$ satisfy the conditions

$$(j, l) = 0 \text{ for } l < l_j \quad \text{and} \quad (j, l_j) \neq 0. \tag{4.4}$$

for any $j \in \{1, \ldots, k\}$. If this would be true, then the row reduced form of $U_sJ_A^i$ would be

$$\big((1, \ldots, k); (l_1, \ldots, l_k)\big)^{-1}_{U_sJ_A^i} U_sJ_A^i.$$

The veracity of the conditions (4.4) is a direct consequence of the fact that J_A^i is an upper triangular matrix with diagonal entries λ_j^i for $j \in \{1, \ldots, k\}$ where $\lambda_1, \ldots, \lambda_k$ are the eigenvalues of A, and U_s is in row reduced echelon form. □

We can now state a theorem which relates the RDLP with the DLP when $A \in GL_n(\mathbb{F}_q)$ is a matrix diagonalizable over a certain extension field $\mathbb{F} \supseteq \mathbb{F}_q$.

Theorem 4.3.8. *Let $U \in \mathbb{F}_q^{k\times n}$ be a matrix with full rank, $A, B \in GL_n(\mathbb{F}_q)$ where A is diagonalizable over a certain extension field $\mathbb{F} \supseteq \mathbb{F}_q$ and $\mathcal{C} := \{\text{rowsp}(U)A^i \mid i \in \mathbb{N}\}$ is a cyclic orbit code. If there exists an $m \in \{0, \ldots, |\mathcal{C}|-1\}$ such that $\text{rank}\begin{pmatrix} UB \\ UA^m \end{pmatrix} = k$, then, the RDLP reduces polynomially over $\mathbb{F}$ to at most $k(n-k)$ instances of the DLP over some subgroups of the multiplicative groups $\mathbb{F}_{q^t}^*$ with $\mathbb{F} \supseteq \mathbb{F}_{q^t} \supseteq \mathbb{F}_q$.*

Proof. We first show that without loss of generality the matrix A can be considered in rational canonical form. This is a direct consequence of Corollary 4.2.13. Indeed, let $L \in GL_n(\mathbb{F}_q)$ be a matrix such that the matrix $L^{-1}AL$ is in rational canonical form. Then,

$$\text{rank}\begin{pmatrix} UB \\ UA^m \end{pmatrix} = \text{rank}\begin{pmatrix} UBL \\ UA^mL \end{pmatrix} = \text{rank}\begin{pmatrix} UL(L^{-1}BL) \\ UL(L^{-1}AL)^m \end{pmatrix}, \tag{4.5}$$

where $UL \in \mathbb{F}_q^{k\times n}$ is clearly a matrix with full rank. We conclude that the solution of the RDLP with parameters A, B and U is the same as the one of the RDLP with parameters $L^{-1}AL, L^{-1}BL$ and UL.

Now let A be a matrix in rational canonical form. Let $\chi_A = p_1^{e_1} \cdots p_r^{e_r} \in \mathbb{F}_q[x]$ be the characteristic polynomial of A where p_i are monic irreducible polynomials and $e_i \geq 1$ for $i = 1, \ldots, r$. The condition on A being diagonalizable over a certain extension field $\mathbb{F} \supseteq \mathbb{F}_q$ corresponds to the fact that the minimal polynomial $\mu_A \in \mathbb{F}_q[x]$ of A is of the form $\mu_A = p_1 \cdots p_r$. Consequently, matrix A is of the form

$$A = \mathrm{diag}(\underbrace{M_{p_1}, \ldots, M_{p_1}}_{e_1 \text{ times}}, \ldots, \underbrace{M_{p_r}, \ldots, M_{p_r}}_{e_r \text{ times}}),$$

where, for any $i \in \{1, \ldots, r\}$, the matrix M_{p_i} is the companion matrix of p_i. Let $\mathbb{F}$ be the splitting field of μ_A, $\lambda_i \in \mathbb{F}$ satisfying $p_i(\lambda_i) = 0$ and $d_i := \deg(p_i)$ for any $i \in \{1 \ldots, r\}$. Thanks to Proposition 3.2.12, a matrix diagonalizing A is of the form

$$S = \mathrm{diag}(\underbrace{S_1, \ldots, S_1}_{e_1 \text{ times}}, \ldots, \underbrace{S_r, \ldots, S_r}_{e_r \text{ times}}) \in GL_n(\mathbb{F})$$

where

$$S_i := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \lambda_i & \lambda_i^q & \lambda_i^{q^2} & \cdots & \lambda_i^{q^{d_i-1}} \\ \lambda_i^2 & \lambda_i^{2q} & \lambda_i^{2q^2} & \cdots & \lambda_i^{2q^{d_i-1}} \\ \vdots & \vdots & \vdots & & \vdots \\ \lambda_i^{d_i-1} & \lambda_i^{(d_i-1)q} & \lambda_i^{(d_i-1)q^2} & \cdots & \lambda_i^{(d_i-1)q^{d_i-1}} \end{pmatrix}.$$

It follows that

$$J_A := S^{-1}AS = \mathrm{diag}(\Lambda_1, \ldots, \Lambda_1, \ldots, \Lambda_r, \ldots, \Lambda_r) \in GL_n(\mathbb{F}),$$

where $\Lambda_i := S_i^{-1} M_{p_i} S_i = \mathrm{diag}(\lambda_i, \lambda_i^q, \ldots, \lambda_i^{q^{d_i-1}})$.

Substituting L with S in (4.5), we obtain that the solution as the RDLP with parameters $A, B \in GL_n(\mathbb{F}_q)$ and $U \in \mathbb{F}_q^{k \times n}$ is the same of the RDLP with parameters $J_A, S^{-1}BS \in GL_n(\mathbb{F})$ and $US \in \mathbb{F}^{k \times n}$. In the language of cyclic orbit codes and with the help of Lemma 4.3.5, we just shift the problem of decoding the received word $\mathrm{rowsp}(U)B$ in the code $\mathcal{C}$ to the one of decoding $\mathrm{rowsp}(U)BS$ in the conjugate code $\mathcal{C}_{\mathbb{F}} := \{\mathrm{rowsp}(U)SJ_A^i \mid i \in \mathbb{N}\}$.

Let $U_s \in \mathbb{F}^{k \times n}$ be a matrix in row reduced echelon form such that $\mathrm{rowsp}(U)S = \mathrm{rowsp}(U_s)$. It follows

$$\begin{aligned} \mathrm{rank} \begin{pmatrix} UB \\ UA^m \end{pmatrix} = k \quad &\iff \quad \mathrm{rowsp}(U)B = \mathrm{rowsp}(U)A^m \in \mathcal{C} \\ &\iff \quad \mathrm{rowsp}(U_s)S^{-1}BS = \mathrm{rowsp}(U_s)J_A^m \in \mathcal{C}_{\mathbb{F}}. \end{aligned}$$

We base our next step on Theorem 4.3.7. The matrix U_s is obtained by row reducing the matrix US. By Theorem 3.2.14, the first maximal minor of US is non zero, meaning that $U_s = \begin{pmatrix} I & U_s' \end{pmatrix}$.

Let $\mathbb{F}_{q^{d_i}} \cong \mathbb{F}_q[x]/(p_i) = \mathbb{F}_q[\lambda_i]$. We prove that solving the RDLP with parameters $J_A, S^{-1}BS \in GL_n(\mathbb{F})$ and $US \in \mathbb{F}^{k\times n}$ reduces to solving at most $k(n-k)$ instances of the DLP over some subgroups of the multiplicative groups $\mathbb{F}^*_{q^{\mathrm{lcm}(d_i,d_j)}}$ for $i, j \in \{1, \ldots, r\}$.

The proof is based on the fact that the row reduced echelon forms of UBS and UA^mS is the same since $\mathrm{rowsp}(UBS) = \mathrm{rowsp}(UA^mS)$ by the condition $\mathrm{rowsp}(UB) = \mathrm{rowsp}(UA^m)$. We base our reduction on this row reduced echelon form.

For simplicity of notation, we rename the eigenvalues of A as $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$ such that

$$J_A = \mathrm{diag}(\lambda_1, \ldots, \lambda_n). \tag{4.6}$$

It is direct consequence of (4.6) that

$$\lambda_i \in \mathbb{F}_{q^{d_r}} \quad \forall i \in \left\{ \sum_{l=1}^{r-1} e_l d_l + 1, \ldots, \sum_{l=1}^{r} e_l d_l \right\}. \tag{4.7}$$

By Theorem 4.3.7 it follows that the row reduced echelon form of $U_s J_A^m$ is

$$V_s = (\lambda_1^{-m}, \ldots, \lambda_k^{-m}) \cdot U_s \cdot \mathrm{diag}(\lambda_1^m, \ldots, \lambda_n^m) = \begin{pmatrix} I & V_s' \end{pmatrix}.$$

Let $U_s = (u_{jl})_{\substack{1\le j\le k \\ 1\le l\le n}}$ and $V_s = (v_{jl})_{\substack{1\le j\le k \\ 1\le l\le n}}$. For any $(j,l) \in \{1, \ldots, k\} \times \{1, \ldots, n\}$ it holds that

$$v_{jl} = u_{jl}\lambda_j^{-m}\lambda_l^m = u_{jl}(\lambda_j^{-1}\lambda_l)^m. \tag{4.8}$$

From this relations it follows that

$$u_{jl} \neq 0 \iff v_{jl} \neq 0.$$

Furthermore,

$$\frac{v_{jl}}{u_{jl}} = (\lambda_j^{-1}\lambda_l)^m = (\lambda_j^{-1}\lambda_l)^{m_{jl}} \in (\lambda_j^{-1}\lambda_l) \leq \mathbb{F}^*_{q^{\mathrm{lcm}(d_r,d_s)}}$$

where $\lambda_j \in \mathbb{F}^*_{q^r}$ and $\lambda_l \in \mathbb{F}^*_{q^s}$ from (4.7) and $m_{jl} \equiv m \pmod{\mathrm{ord}(\lambda_j^{-1}\lambda_l)}$. □

We show now that the discrete logarithm $m \in \{0, \ldots, |\mathcal{C}| - 1\}$ can be computed starting from the discrete logarithms

$$m_{jl} = \log_{\lambda_j^{-1}\lambda_l} \frac{v_{jl}}{u_{jl}}$$

for every $(j,l) \in \{1,\dots,k\} \times \{k+1,\dots,n\}$ such that $u_{jl} \neq 0$. From (4.8) we know that

$$m \equiv m_{jl} \pmod{\operatorname{ord}(\lambda_j^{-1}\lambda_l)}. \tag{4.9}$$

By applying the Chinese Remainder Theorem [Lan02, Theorem 2.1] there exists a unique $\bar{m} \in \{0,\dots,M-1\}$ satisfying all the relations (4.9), where

$$M = \operatorname{lcm}\left(\operatorname{ord}(\lambda_j^{-1}\lambda_l) \mid (j,l) \in \{1,\dots,k\} \times \{k+1,\dots,n\},\ u_{jl} \neq 0\right).$$

The searched discrete logarithm is then $m = \bar{m} \pmod{|\mathcal{C}|}$. Indeed

$$\begin{aligned}
\operatorname{rowsp}\left(\left(u_{jl}(\lambda_j^{-1}\lambda_k)^{m_{jl}}\right)_{\substack{1\le j\le k\\ 1\le l\le n}}\right) &= \operatorname{rowsp}\left(\left(u_{jl}\lambda_j^{-m_j}\lambda_k^{m_k}\right)_{\substack{1\le j\le k\\ 1\le l\le n}}\right)\\
&= \operatorname{rowsp}((\lambda_1^{-m_1},\dots,\lambda_k^{-m_k}) \cdot U_s \cdot \operatorname{diag}(\lambda_1^{m_1},\dots,\lambda_n^{m_n}))\\
&= \operatorname{rowsp}(U_s \operatorname{diag}(\lambda_1^{m_1},\dots,\lambda_n^{m_n})) = \operatorname{rowsp}(U_s J_A^{\bar{m}})\\
&= \operatorname{rowsp}(UA^{\bar{m}}S) = \operatorname{rowsp}(UA^mS).
\end{aligned}$$

where $m_j \equiv m \pmod{\lambda_i}$.

Algorithm 5 depicts the procedure presented in the proof of Theorem 4.3.8.

Algorithm 5: Solving the RDLP through DLP

input : $V \in \mathbb{F}_q^{k\times n}$ such that $\operatorname{rowsp}(V) \in \mathcal{C} = \{\mathcal{U}A^i \mid i \in \mathbb{N}\}$,
$S \in GL_n(\mathbb{F})$,
$U_s = \left(u_{jl}\right)_{\substack{1\le j\le k\\ 1\le l\le n}} \in \mathbb{F}^{k\times n}$ a matrix with full rank and in row reduced echelon form
$\lambda_1,\dots,\lambda_n \in \mathbb{F}$ the eigenvalues of A.

output: $m \in \mathbb{N}$ such that $\operatorname{rowsp}(V) = \operatorname{rowsp}(UA^m)$.

Compute $\left(v_{jl}\right)_{\substack{1\le j\le k\\ 1\le l\le n}} \in \mathbb{F}^{k\times n}$ that is the row reduced echelon form of VS;

for $j \in \{1,\dots,k\}$, $l \in \{k+1,\dots,n\}$ *and* $u_{jl} \neq 0$ **do**
  Compute $m_{jl} = \log_{\lambda_j^{-1}\lambda_l} \frac{v_{jl}}{u_{jl}} \in \{0,\dots,\operatorname{ord}(\lambda_j^{-1}\lambda_k)\}$
end

Use Gauss's Algorithm [MvOV01, Algorithm 2.121] to compute the $m \in \{0,\dots,M\}$ such that $m \equiv m_{jl} \pmod{\operatorname{ord}(\lambda_j^{-1}\lambda_k)}$.

Based on the Chinese Remainder Theorem, we can now establish a membership criterion for cyclic orbit codes.

Corollary 4.3.9 (Membership criterion)**.** *Let $U,V \in \mathbb{F}_q^{k\times n}$ be two matrices with full rank, $A \in GL_n(\mathbb{F}_q)$ be a diagonalizable matrix over a certain extension field $\mathbb{F} \supseteq \mathbb{F}_q$ and $\mathcal{C} := \{\operatorname{rowsp}(U)A^i \mid i \in \mathbb{N}\}$ be a cyclic orbit code.*

Let $S \in GL_n(\mathbb{F})$ *be a matrix such that* $S^{-1}AS = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ *and*

$$\big(u_{jl}\big)_{\substack{1\le j\le k\\ 1\le l\le n}} \text{ and } \big(v_{jl}\big)_{\substack{1\le j\le k\\ 1\le l\le n}} \in \mathbb{F}^{k\times n}$$

respectively the row reduced echelon form of US *and* VS*. Then,* $\mathrm{rowsp}(V) \in \mathcal{C}$ *if and only if it holds that*

$$v_{jl} = 0 \iff u_{jl} = 0 \quad \forall j \in \{1, \ldots, k\}, l \in \{1, \ldots, n\},$$

and

$$\log_{\lambda_j^{-1}\lambda_l} \frac{v_{jl}}{u_{jl}} \equiv \log_{\lambda_{j'}^{-1}\lambda_{l'}} \frac{v_{j'l'}}{u_{j'l'}} \pmod{\gcd\Big(\mathrm{ord}(\lambda_j^{-1}\lambda_l), \mathrm{ord}(\lambda_{j'}^{-1}\lambda_{l'})\Big)}$$

for any $j, j' \in \{1, \ldots, k\}$*,* $l, l' \in \{k+1, \ldots, n\}$ *and* $u_{jl}, u_{j'l'}$ *nonzero.*

Complexity

In order to study the complexity of Algorithm 5, we now face the DLP's contained in the for loop. We want to compute the discrete logarithms

$$m_{jl} = \log_{\lambda_j^{-1}\lambda_k} \frac{v_{jl}}{u_{jl}}$$

for $j \in \{1, \ldots, k\}$, $l \in \{k+1, \ldots, n\}$ and $u_{jl} \neq 0$.

As already specified, the DLP is in general computationally infeasible, meaning that a general instance of it is not solvable in acceptable time. The best known algorithm solving the DLP for any cyclic group is *Pollard's rho algorithm* [MvOV01, Algorithm 3.60] which requires $O(\sqrt{m})$, where m is the order of the cyclic group, and negligible amount of storage. There are some groups for which the DLP is feasible. The groups we are going to consider are the ones for which the order is smooth.

Definition 4.3.10 ([MvOV01, Definition 3.13]). Let $b \in \mathbb{N}^*$. An integer m is said to be *b–smooth*, or *smooth* with respect to a bound b, if all its prime factors are less than or equal to b.

Groups with smooth order received importance in cryptography with the paper [PH78], where the authors introduced the *Pohlig-Hellman algorithm* for computing discrete logarithms over $\mathbb{F}_p$, where p is a prime. The algorithm is efficient computationally as soon as $p-1$ is smooth, i.e. its prime factors are small. A generalization of this idea is the algorithm [MvOV01, Algorithm 3.63] which, based on the same idea of [PH78], works for every group. We illustrate here this algorithm.

Algorithm 6: Pohlig-Helmann algorithm for computing discrete logarithms, [MvOV01, Algorithm 3.63]

input : α a generator of a cyclic group $\mathfrak{G}$ of order d and $\beta \in \mathfrak{G}$.
output: $m = \log_\alpha \beta$

Find prime factorization of d: $d = \prod_{i=1}^{r} p_i^{e_i}$ where $e_i \geq 1$;
for $i \in \{1, \ldots, r\}$ **do**
  (*Compute* $m_i = \sum_{j=0}^{e_i-1} l_j p_i^j$, *where* $m_i \equiv m \pmod{p_i^{e_i}}$)
  Set $q = p_i$, $e = e_i$, $\gamma = 1$ and $l_{-1} = 0$;
  Compute $\bar{\alpha} = \alpha^{d/q}$;
  for $j \in \{0, \ldots e_i - 1\}$ **do**
    Compute $\gamma = \gamma \alpha^{l_{j-1} q^{j-1}}$ and $\bar{\beta} = (\beta \gamma^{-1})^{d/q^{j-1}}$;
    Compute $l_j = \log_{\bar{\alpha}} \bar{\beta}$ // DLP
  end
  Set $m_i = \sum_{j=0}^{e_i-1} l_j p_i^j$;
end
Use Gauss's algorithm [MvOV01, Algorithm 2.121] to compute the $m \in \{0, \ldots, d-1\}$ such that $m \equiv m_i \pmod{p^{e_i}}$ for $1 \leq i \leq r$.

The running time of the Pohlig-Hellman algorithm is $O(\sum_{i-1}^{r} e_i(\log d + \sqrt{p_i}))$ group multiplications where $\prod_{i=1}^{r} p_i^{e_i}$ is the prime factorization of d. In the case of smooth numbers, Algorithm 6 is feasible. The $\sqrt{p_i}$ is the complexity of computing a discrete logarithm via Pollard's rho algorithm over a cyclic group with p_i elements. It is possible to quicken the for algorithm by allowing some storage. By writing in a table the values $\left(j, (\alpha^{d/p_i})^j\right)$ for every $i \in \{1, \ldots, r\}$ and $j \in \{0, \ldots, p_i - 1\}$, the computation of $\log_{\bar{\alpha}} \bar{\beta}$ consists of only looking for the right entry in the table. In this case the complexity reduces to $O(\log d \sum_{i=1}^{r} e_i)$.

Example 4.3.11. We give an example of a cyclic orbit code with smooth cardinality based on spread codes. In [TR11, Section 3.1] spread codes are proven to be irreducible cyclic orbit codes, meaning that they are cyclic orbit codes defined by a cyclic subgroup generated by the companion matrix $A \in GL_n(\mathbb{F}_q)$ of an irreducible polynomial. Consequently, A is diagonalizable over $\mathbb{F}_{q^n}$. Let then $\mathcal{C} = \{\text{rowsp}(U)A^i \mid i \in \mathbb{N}\} \subset \mathfrak{G}_{\mathbb{F}_2}(10, 60)$ be a spread code for some $U \in \mathbb{F}_q^{10\times 60}$ with full–rank. Its cardinality is smooth since

$$\begin{aligned} |\mathcal{C}| &= \frac{2^{60}-1}{2^{10}-1} = 1127000493261825 \\ &= 3^2 \cdot 5^2 \cdot 11 \cdot 13 \cdot 41 \cdot 61 \cdot 331 \cdot 1321, \end{aligned}$$

meaning that its factors are rather small. The fact that A is diagonalizable allows us to use Algorithm 5 with input a matrix $V \in \mathbb{F}_q^{10\times 60}$ such that

$\text{rowsp}(V) \in \mathcal{C}$. Since $|\mathcal{C}|$ is smooth, we can use Pohlig-Helmann Algorithm in order to compute the discrete logarithms contained in Algorithm 5. In this case the required storage is negligible since it corresponds to storing 1786 elements of $\mathbb{F}_{2^{60}}$.

Conclusion

In the last subsection we show that for cyclic orbit codes with smooth cardinality it is possible to check if a received space is an element of the code in feasible time, allowing a negligible amount of storage. This leads to the natural conclusion that, although a complete decoding algorithm does not yet exist, cyclic orbit codes with smooth cardinality are in general a preferable choice for codes.

Bibliography

[ACLY00] R. Ahlswede, N. Cai, S.-Y.R. Li, and R.W. Yeung. Network information flow. *Information Theory, IEEE Transactions on*, 46(4):1204 –1216, July 2000.

[Die05] R. Diestel. *Graph theory*, volume 173 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, third edition, 2005.

[EKW10] A. Elsenhans, A. Kohnert, and A. Wassermann. Construction of codes for network coding. In *Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems – MTNS*, pages 1811–1814, Budapest, Hungary, 2010.

[Eli57] P. Elias. *List decoding for noisy channels*. Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Mass., Rep. No. 335, 1957.

[ES09] T. Etzion and N. Silberstein. Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams. *Information Theory, IEEE Transactions on*, 55(7):2909 –2919, July 2009.

[EV08] T. Etzion and A. Vardy. Error-correcting codes in projective space. In *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, pages 871–875, July 2008.

[FW86] P. Frankl and R. M. Wilson. The Erdős-Ko-Rado theorem for vector spaces. *J. Combin. Theory Ser. A*, 43(2):228–236, 1986.

[Gab85] È. M. Gabidulin. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii*, 21(1):3–16, 1985.

[GMR11] E. Gorla, F. Manganiello, and J. Rosenthal. An algebraic approach for decoding spread codes. *CoRR*, abs/1107.5523, 2011.

[GS99] V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and algebraic-geometry codes. *Information Theory, IEEE Transactions on*, 45(6):1757 –1767, September 1999.

[Gur04] V. Guruswami. *List Decoding of Error-Correcting Codes*, volume 3282 of *Lecture Notes in Computer Science*. Springer, 2004.

[GY08] M. Gadouleau and Z. Yan. On the decoder error probability of bounded rank-distance decoders for maximum rankdistance codes. *Information Theory, IEEE Transactions on*, 54(7):3202 –3206, July 2008.

[Her75] I. N. Herstein. *Topics in Algebra*. Xerox College Publishing, Lexington, Mass., second edition, 1975.

[Hir98] J. W. P. Hirschfeld. *Projective Geometries over Finite Fields*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second edition, 1998.

[KK08a] A. Kohnert and S. Kurz. Construction of large constant dimension codes with a prescribed minimum distance. In Jacques Calmet, Willi Geiselmann, and Jörn Müller-Quade, editors, *MMICS*, volume 5393 of *Lecture Notes in Computer Science*, pages 31–42. Springer, 2008.

[KK08b] R. Kötter and F.R. Kschischang. Coding for errors and erasures in random network coding. *Information Theory, IEEE Transactions on*, 54(8):3579–3591, August 2008.

[KM03] R. Koetter and M. Médard. An algebraic approach to network coding. *Networking, IEEE/ACM Transactions on*, 11(5):782 – 795, October 2003.

[Lan02] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[LN94] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and their Applications*. Cambridge University Press, Cambridge, London, 1994. Revised edition.

[LYC03] S.-Y.R. Li, R.W. Yeung, and N. Cai. Linear network coding. *Information Theory, IEEE Transactions on*, 49(2):371–381, February 2003.

[Men27] K. Menger. Zur allgemeinen kurventheorie. *Fund. Math*, 10(95-115):5, 1927.

[MGR08] F. Manganiello, E. Gorla, and J. Rosenthal. Spread codes and spread decoding in network coding. In *Proceedings of the 2008 IEEE International Symposium on Information Theory*, pages 851–855, Toronto, Canada, 2008.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North Holland, Amsterdam, 1977.

[MTR11] F. Manganiello, A.-L. Trautmann, and J. Rosenthal. On conjugacy classes of subgroups of the general linear group and cyclic orbit codes. In *Proceedings of the 2011 IEEE International Symposium on Information Theory*, Saint Petersburg, Russia, 2011.

[MV10] H. Mahdavifar and A. Vardy. Algebraic list-decoding on the operator channel. In *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, pages 1193 –1197, jun. 2010.

[MvOV01] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of applied cryptography*. CRC Press, 2001. http://www.cacr.math.uwaterloo.ca/hac/.

[MW97] A. J. Menezes and Y.-H. Wu. The discrete logarithm problem in GL(n, q). *Ars Combin.*, 47:23–32, 1997.

[PH78] S. Pohlig and M. Hellman. An improved algorithm for computing logarithms over and its cryptographic significance (corresp.). *Information Theory, IEEE Transactions on*, 24(1):106 – 110, jan 1978.

[PV05] F. Parvaresh and A. Vardy. Correcting errors beyond the Guruswami-Sudan radius in polynomial time. *Foundations of Computer Science, 2005. FOCS 2005. 46th Annual IEEE Symposium on*, pages 285–294, Oct. 2005.

[Rot95] J. J. Rotman. *An introduction to the theory of groups*, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth edition, 1995.

[RS60] I. S. Reed and G. Solomon. Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, 1960.

[Ska10] V. Skachek. Recursive code construction for random networks. *Information Theory, IEEE Transactions on*, 56(3):1378 –1382, March 2010.

[SKK08] D. Silva, F.R. Kschischang, and R. Kötter. A rank-metric approach to error control in random network coding. *Information Theory, IEEE Transactions on*, 54(9):3951–3967, Sept. 2008.

[Sta97] R. P. Stanley. *Enumerative combinatorics. Vol. 1.* Cambridge University Press, Cambridge, 1997. With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original.

[Sud97] M. Sudan. Decoding of Reed Solomon codes beyond the error-correction bound. *J. Complexity*, 13(1):180–193, 1997.

[TMR10] A.-L. Trautmann, F. Manganiello, and J. Rosenthal. Orbit codes - a new concept in the area of network coding. In *Information Theory Workshop (ITW), 2010 IEEE*, pages 1 –4, Dublin, Ireland, August 2010.

[TR11] A.-L. Trautmann and J. Rosenthal. A complete characterization of irreducible cyclic orbit codes. In *Proceedings of the Seventh International Workshop on Coding and Cryptography (WCC) 2011*, pages 219 – 223, 2011.

[vLW01] J. H. van Lint and R. M. Wilson. *A Course in Combinatorics*. Cambridge University Press, second edition, 2001.